Product Guide to Data Networks, Management Solutions and Security

A comprehensive offer by Alcatel-Lucent

Product Guide

November 2009

Introduction

Alcatel-Lucent provides the industry's best value in highly available, secure and easy-to-manage IP networks with a comprehensive, standards-based product portfolio. This product guide contains an overview of network infrastructure, management and security products.

Our network infrastructure product range includes:

- → Manageable layer-2/layer-3 LAN switches, both stackable and chassis-based, supporting Power-over-Ethernet and interface speeds up to 10 Gb/s
- → A highly scalable, wireless LAN solution supporting the latest high-speed (IEEE 802.11n draft v2.0) access
- → Unified services gateways enabling WAN access, at the same time providing a wealth of service from a single box
- → MPLS switches that support VPLS technology invented by Alcatel-Lucent, providing virtualization of network traffic without the overhead of layer-3 VPN

Our management product range includes:

- → Network and network element management systems
- → IP address management and (D)DNS management system
- → Consolidated service level management system

Our security product range includes:

- → Host integrity check solution to enforce end-system compliancy
- → A unique distributed firewall/VPN system capable of operating in stealth mode
- → Laptop information integrity and security solution
- → Application compliance and interaction security solution

In any network infrastructure, Alcatel-Lucent solutions provide security and availability to the operation of the processes relying on this network.

Alcatel-Lucent is proud to provide you with this product guide representing our enterprise networking, management and security offer, its key selling points, and benefits for your customers.

TABLE OF CONTENTS

Data Networks product range

The Alcatel-Lucent network infrastructure portfolio includes highly scalable and manageable products with embedded security for LANs, WLANs, WANs, and MANs.

Our LAN product family provides manageable layer-2/layer-3 LAN switches, both stackable and chassis-based, supporting Power-over-Ethernet and interface speeds up to 10 Gb/s, as well as comprehensive standards-based network access security.

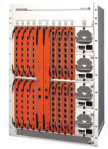
Our WLAN product family provides a highly scalable WLAN solution supporting the latest high-speed (IEEE 802.11n draft v2.0) access, as well as comprehensive standards-based network access security.

Our WAN and MAN product families provide unified services gateway routers that enable WAN access, at the same time providing a wealth of service from a single box. In addition, this product family includes MPLS switches that support VPLS technology invented by Alcatel-Lucent, providing virtualization of network traffic without the overhead of layer-3 VPN and Border Gateway Protocol.

OmniSwitch 9000

OmniSwitch 9600

OmniSwitch 9700



OmniSwitch 9800

The **Alcatel-Lucent OmniSwitch™ 9000 Chassis LAN Switch** (CLS) family is a series of layer-2 and layer-3 switches. They are designed to be feature-rich, yet value-priced, for use in the enterprise network in the distribution and access layers.

The OmniSwitch 9000 CLS family comprises four chassis (OmniSwitch 9600, OmniSwitch 9700, OmniSwitch 9702, and OmniSwitch 9800) and a common set of network interfaces to accommodate various connectivity needs and simplify inventory.

The OmniSwitch 9000 family addresses today's network needs for highly available infrastructure with large switching capacity and high 10 GigE Ethernet (10GigE) port densities to support the next generation of converged networks.

The OmniSwitch 9000 family provides the features required to sustain business applications:

- → High availability
- → High density for GigE and 10GigE interfaces
- → Wire-speed performance with low latency and flexible network policies such as quality of service (QoS)
- → Comprehensive security

These capabilities ensure an easy and economical way to upgrade or deploy a new Ethernet network. The large number of ports makes the OmniSwitch 9000 family suitable for two- or three-tier network designs — possible with the high-performance capability and density of GigE and 10GigE.

The OmniSwitch 9000 family also has a place in future network planning with its native and extensive support of IPv4/IPv6, addressing the need for migration from IPv4 to IPv6 or new IPv6 deployments. It provides advanced security and QoS features at an attractive price and is fully supported by the OmniVista™ 2500 Network Management System.

The OmniSwitch 9600 Chassis LAN Switch (CLS) is the smallest chassis (5.5 RU) of the OmniSwitch 9000 family. It is a five-slot chassis with one chassis management module (CMM) and four network interface (NI) modules, supporting an aggregation of up to 192 GigE ports or 24 10GigE ports. While CMM redundancy is not available on the OmniSwitch 9600, network resiliency is typically achieved with deployment of two OmniSwitch 9600 chassis.

The OmniSwitch 9600 reuses the OmniSwitch 9700 CMM and shares a common set of NI modules and power supplies with the rest of the OmniSwitch 9000 family. These benefits offer an easy upgrade path to the larger form factor if required.

The OmniSwitch 9700 Chassis LAN Switch (CLS) is the most popular chassis in the OmniSwitch 9000 family. It is a ten-slot chassis (11 RU) with two slots for CMMs and eight slots for NI modules, supporting an aggregation of up to 384 GigE ports (192 if Power-over-Ethernet (PoE) ports are included) or 48 10GigE ports.

Designed for continuous operation, the OmniSwitch 9700 CLS features "no single point of failure," supporting dual CMMs and redundant fans and power supplies.

Sparing for the OmniSwitch 9000 family is simplified because the OmniSwitch 9700 shares a common set of NI modules and power supplies with the rest of the OmniSwitch 9000 family. Additional subcomponents such as the fan tray and PoE shelf are also common with the OmniSwitch 9800 Chassis LAN Switch (CLS).

The OmniSwitch 9702 Chassis LAN Switch is a NEBS-ready variant of the OmniSwitch 9700.

The OmniSwitch 9800 CLS is the largest chassis in the OmniSwitch 9000 family. It is an 18-slot chassis (17 RU) with two slots for CMMs and 16 slots for NI modules, supporting an aggregation of up to 768 GigE ports (384 if PoE ports are considered) or 96 10GigE ports.

Designed for continuous operation, the OmniSwitch 9800 CLS features "no single point of failure," supporting dual CMMs and redundant fans and power supplies.

Sparing for the OmniSwitch 9000 family is simplified because the OmniSwitch 9800 shares a common set of NI modules and power supplies with the rest of the OmniSwitch 9000 family. Additional subcomponents such as the fan tray and PoE shelf are also common with the OmniSwitch 9700 CLS.

KEY SELLING POINTS

- → Prevent business interruption from failures with a combination of system's redundancy and resilient topology protocols:
  - ¬ The system's redundancy protects all critical functions, such as powering (redundant power supplies with AC and DC options), cooling (redundant fans) and switch management (redundant CMM in the OmniSwitch 9700/9800), with transparent failover.
  - ¬ The extensive support of layer-2 and layer-3 protocols are designed for always-available infrastructure.
- → Protect investment with a modular and scalable connectivity (GigE and 10GigE), but also with regular software updates to keep on track with evolving standards (IEEE, IETF and ITU), such as IPv6

- → Protect business assets against direct attacks on the infrastructure (malicious and denial-of-service attacks) and enforcement of IT policy for post- and pre-admission control (unique traffic anomaly detection)
- → Reduce energy costs with the system's low power dissipation (less than 2000 W in the worst case configuration, with 768 GigE ports)

KEY FEATURES

High availability

- → Smart continuous switching for nonstop operation in redundant CMM configuration
- → Passive backplane and redundant active components (power supply unit/fans/CMM)
- → Extensive layer-2 and layer-3 protocol support for spatial resiliency

High performance and scalability

- → Wire-rate processing for simultaneous L2/IPv4/IPv6 traffic (unicast and multicast)
- → High density with GigE (up to 768 ports) and 10GigE (up to 96 ports)
- → Enhanced forwarding – improves network response time through hardware-based forwarding at first packet, and elimination of CPU solicitation for access control list (ACL)/QoS demands

Comprehensive security

- → Flexible device/user authentication with Alcatel-Lucent Access Guardian (IEEE 802.1x/MAC/captive portal)
- → Built-in intrusion detection system (IDS) with traffic anomaly detection (TAD) and quarantine enforcement mechanism
- → Extensive support of user-oriented features of the Alcatel-Lucent Operating System (AOS), such as learned port security (LPS), port mapping, DHCP binding tables and unified network profile (UNP)

Convergence

- → Enhanced VoIP and video performance with policy-based QoS
- → Future-ready support for multimedia applications with wire-rate multicast
- → Full PoE support for IP phones, WLAN access points and video cameras with up to 2400 W of power through dedicated power shelves

TECHNICAL INFORMATION

OmniSwitch 9800
- 2 CMM slots
- 16 NI slots
- 4 positions for power supplies
- AC or DC power

OmniSwitch 9702 (NEBS)
- 2 CMM slots
- 8 NI slots
- 3 positions for power supplies
- AC or DC power

OmniSwitch 9700
- 2 CMM slots
- 8 NI slots
- 3 positions for power supplies
- AC or DC power

OmniSwitch 9600
- 1 CMM slot
- 4 NI slots
- 2 positions for power supplies
- AC or DC power

OmniSwitch 9000 network interfaces
- 24 RJ-45 GigE ports
- 24 RJ-45 GigE (PoE) ports
- 24 SFP GigE ports
- 48 RJ-45 GigE ports
- 20 RJ-45 Fast Ethernet ports + 2 SFP slots
- 6 XFP 10GigE ports
- 2 XFP 10GigE ports

IEEE standards
- IEEE 802.1D (STP)
- IEEE 802.1p (CoS)
- IEEE 802.1Q (VLANs)
- IEEE 802.1ad (VLAN stacking)
- IEEE 802.1ag (OAM)
- IEEE 802.1s (MSTP)
- IEEE 802.1w (RSTP)
- IEEE 802.1X (Port-based NAC)
- IEEE 802.3i (10Base-T)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (GigE Ethernet)
- IEEE 802.3ab (1000Base-T)
- IEEE 802.3ac (VLAN Tagging)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3af (Power-over-Ethernet)
- IEEE 802.3ae (10G Ethernet)

ITU-T recommendations
- ITU-T G.8032, June 2007 draft (Ethernet Ring Protection)

IETF RFCs

IPv4
- RFC 2003 IP/IP Tunneling
- RFC 2784 GRE Tunneling

OSPF
- RFC 1253/1850/2328 OSPFv2 and MIB
- RFC 1587/3101 OSPF NSSA Option
- RFC 1765 OSPF Database Overflow
- RFC 2154 OSPF MD5 Signature
- RFC 2370/3630 OSPF Opaque LSA
- RFC 3623 OSPF Graceful Restart

RIP
- RFC 1058 RIPv1
- RFC 1722/1723/2453/1724 RIPv2 and MIB
- RFC 1812/2644 IPv4 Router equirement
- RFC 2080 RIPng for IPv6

BGP
- RFC 1269/1657 BGP v3 and v4 MIB
- RFC 1403/1745 BGP/OSPF Interaction
- RFC 1771-1774/2842/2918/3392 BGP v4
- RFC 1965 BGP AS Confederations
- RFC 1966 BGP Route Reflection
- RFC 1997/1998 BGP Communities Attribute
- RFC 2042 BGP New Attribute
- RFC 2385 BGP MD5 Signature
- RFC 2439 BGP Route Flap Damping
- RFC 2545 BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
- RFC 2796 BGP Route Reflection
- RFC 2858 Multiprotocol Extensions for BGP-4
- RFC 3065 BGP AS Confederations

IP Multicast
- RFC 1075 DVMRP
- RFC 1112 IGMP v1
- RFC 2236/2933 IGMP v2 and MIB
- RFC 2362 PIM-SM

- RFC 2365 Multicast
- RFC 2715/2932 Multicast Routing MIB
- RFC 2934 PIM MIB for IPv4
- RFC 3376 IGMPv3
- RFC 5060 Protocol Independent Multicast MIB
- RFC 5132 IP Multicast MIB
- RFC 5240 PIM Bootstrap Router MIB

IPv6

- RFC 1886/3596 DNS for IPv6
- RFC 2292/2553/3493/3542 IPv6 Sockets
- RFC 2373/2374/3513/3587/4007/4193 IPv6 Addressing
- RFC 2452/2454 IPv6 MIB for TCP/UDP
- RFC 2460/2461/2462/2464 Core IPv6
- RFC 2463/2466/4443 ICMP v6 and MIB
- RFC 2893/3056/4213 IPv6 Transition Mechanisms
- RFC 3595 Flow Label Conventions

Manageability

- RFC 854/855 Telnet and Telnet Options
- RFC 959/2640 FTP
- RFC 1155/2578-2580 SMI v1 and SMI v2
- RFC 1157/2271 SNMP
- RFC 1212/2737 MIB and MIB-II
- RFC 1213/2011-2013 SNMP v2 MIB
- RFC 1215 Convention for SNMP Traps
- RFC 1350 TFTP Protocol
- RFC 1573/2233/2863 Private Interface MIB
- RFC 1643/2665 Ethernet MIB
- RFC 1901-1908/3416-3418 SNMP v2c
- RFC 2096 IP MIB
- RFC 2570-2576/3411-3415 SNMP v3
- RFC 2616/2854 HTTP and HTML
- RFC 2667 IP Tunneling MIB
- RFC 2668/3636 IEEE 802.3 MAU MIB
- RFC 2674 VLAN MIB
- RFC 3414 User-based Security Model
- RFC 4251 Secure Shell Protocol Architecture
- RFC 4252 The Secure Shell (SSH) Authentication Protocol
- RFC 4878 OAM Functions on Ethernet-Like Interfaces

Security

- RFC 1321 MD5
- RFC 2104 HMAC Message Authentication
- RFC 2138/2865/2868/3575/2618 RADIUS Authentication and Client MIB
- RFC 2139/2866/2867/2620 RADIUS Accounting and Client MIB
- RFC 2228 FTP Security Extensions
- RFC 2284 PPP EAP
- RFC 2869/2869bis RADIUS Extension

Quality of service

- RFC 896 Congestion Control
- RFC 1122 Internet Hosts
- RFC 2474/2475/2597/3168/3246 DiffServ
- RFC 3635 Pause Control

Others

- RFC 768 UDP
- RFC 791/894/1024/1349 IP and IP/Ethernet
- RFC 792 ICMP
- RFC 793/1156 TCP/IP and MIB
- RFC 826/903 ARP and Reverse ARP
- RFC 919/922 Broadcasting Internet Datagram
- RFC 925/1027 Multi-LAN ARP/Proxy ARP
- RFC 950 Subnetting
- RFC 951 Bootp
- RFC 1151 RDP
- RFC 1191 Path MTU Discovery
- RFC 1256 ICMP Router Discovery
- RFC 1305/2030 NTP v3 and Simple NTP
- RFC 1493 Bridge MIB
- RFC 1518/1519 CIDR
- RFC 1541/1542/2131/3396/3442 DHCP
- RFC 1757/2819 RMON and MIB
- RFC 2131/3046 DHCP/BootP Relay
- RFC 2132 DHCP Options
- RFC 2251 LDAP v3
- RFC 2338/3768/2787 VRRP and MIB
- RFC 3021 Using 31-bit Prefixes
- RFC 3060 Policy Core
- RFC 3176 sFlow

OmniSwitch 9000E

OmniSwitch 9700E

OmniSwitch 9800E

The **Alcatel-Lucent OmniSwitch™ 9000E** Chassis LAN Switch family comprises the OmniSwitch 9700E, OmniSwitch 9702E and the OmniSwitch 9800E. These are fully featured, high-availability and high-performance 10 Gigabit Ethernet (10GigE) chassis LAN switches designed for the core, data centers and campus networks.

The OmniSwitch 9000E family delivers wire-rate support of multiple virtual routing and forwarding (VRF), the foundation for network virtualization in the data center.

Network availability is enhanced through the in-service software upgrade (ISSU) capability such that emergency patching is achieved without taking the network down.

The OmniSwitch 9000E family protects current OmniSwitch investments by reusing existing and field-proven subcomponents from the OmniSwitch 9000 product line (such as the chassis, power supply units, and fan trays) and by leveraging the Alcatel-Lucent Operating System (AOS), which is common to all OmniSwitch products.

The OmniSwitch 9000E family has native and full support of IPv4/IPv6, addressing the need for migration from IPv4 to IPv6 or new IPv6 deployments. It also brings carrier technology such as MPLS into the enterprise campus.

The OmniSwitch 9000E provides advanced security and quality of service (QoS) features at an attractive price and is fully supported by the OmniVista™ 2500 Network Management System.

The OmniSwitch 9700E Chassis LAN Switch (CLS) is the most popular chassis in the OmniSwitch 9000E family. It is a ten-slot chassis (11 RU) with two slots for chassis management modules (CMMs) and eight slots for network interface (NI) modules, supporting an aggregation of up to 192 GigE ports or 16 10GigE ports.

Designed for continuous operation, the OmniSwitch 9700E CLS features "no single point of failure," supporting dual CMMs and redundant fans and power supplies.

Sparing for the OmniSwitch 9000E family is simplified because the OmniSwitch 9700E shares a common set of NI modules, power supplies and fan trays with the rest of the OmniSwitch 9000E family.

The OmniSwitch 9702E Chassis LAN Switch is a NEBS-ready variant of the OmniSwitch 9700E. The OmniSwitch 9702E also introduces a new backplane to accommodate higher performance for future modules.

The OmniSwitch 9800E Chassis LAN Switch (CLS) is the largest chassis in the OmniSwitch 9000E family. It is an 18-slot chassis (17 RU) with two slots for CMMs and 16 slots for NI modules, supporting an aggregation of up to 384 GigE ports or 32 10GigE ports.

Designed for continuous operation, the OmniSwitch 9800E CLS features "no single point of failure," supporting dual CMMs and redundant fans and power supplies.

Sparing for the OmniSwitch 9000E family is simplified because the OmniSwitch 9800E shares a common set of NI modules, power supplies and fan trays with the rest of the OmniSwitch 9000E family.

KEY SELLING POINTS

- → Prevent business interruption from failures with a combination of system's redundancy and resilient topology protocols:
  - ¬ The system's redundancy protects all critical functions, such as powering (redundant power supplies with AC and DC options), cooling (redundant fans) and switch management (redundant CMMs), with transparent failover and ISSU.
  - ¬ The AOS provides extensive support of layer-2 and layer-3 protocols to design always-available infrastructure.
- → Protect investment with a modular and scalable connectivity (GigE and 10GigE), but also with regular AOS software updates to keep on track with evolving standards (IEEE, IETF and ITU), such as IPv6 and MPLS
- → Protect business assets against direct attacks on the infrastructure (malicious and denial-of-service attacks) and enforcement of IT policy for post- and pre-admission control (unique traffic anomaly detection)
- → Reduce energy costs through the system's low power dissipation (less than 1500 W in the worst case configuration)

KEY FEATURES

High availability

- → Smart continuous switching for nonstop operation in redundant CMM configuration
- → ISSU for hitless patching
- → Passive backplane and redundant active components (power supply units, fans, CMM)
- → Extensive layer-2 and layer-3 protocol support for spatial resiliency

High performance and scalability

- → Wire-rate processing for simultaneous L2/IPv4/IPv6 traffic (unicast and multicast)

→ Extended scalability in network policies such as access control lists (ACLs) and QoS, and multicast flows for a better VoIP/video experience

→ Enhanced forwarding – improves network response time through hardware-based forwarding at first packet, and elimination of CPU solicitation for ACL/QoS demands

Comprehensive security

→ Flexible device/user authentication with Alcatel-Lucent Access Guardian (IEEE 802.1x/MAC/captive portal) with Host Integrity Check (HIC)

→ Built-in intrusion detection system (IDS) with traffic anomaly detection (TAD) and quarantine enforcement mechanism

→ Extensive support of AOS user-oriented features such as learned port security (LPS), port mapping, DHCP binding tables and unified network profile (UNP)

Large campus and metro network

→ Layer 2 deployment using stacked VLANs, including OA&M toolbox and multicast support

→ Layer 3 deployment using multiple virtual routing and forwarding (VRF)

→ IP/MPLS deployment using Virtual Private LAN Service (VPLS)

TECHNICAL INFORMATION

OmniSwitch 9800E

- 2 CMM slots
- 16 NI slots
- 4 positions for power supplies
- AC or DC power

OmniSwitch 9702E (NEBS)

- 2 CMM slots
- 8 NI slots
- 3 positions for power supplies
- AC or DC power

OmniSwitch 9700E

- 2 CMM slots
- 8 NI slots
- 3 positions for power supplies
- AC or DC power

OmniSwitch 9000E Network interfaces

- 24 RJ-45 GigE ports
- 24 SFP GigE ports
- 2 XFP 10GigE ports

IEEE standards

- IEEE 802.1D (STP)
- IEEE 802.1p (CoS)
- IEEE 802.1Q (VLANs)
- IEEE 802.1ad (VLAN stacking)
- IEEE 802.1ag (OAM)
- IEEE 802.1s (MSTP)
- IEEE 802.1w (RSTP)
- IEEE 802.1X (Port-based NAC)
- IEEE 802.3i (10Base-T)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (Gigabit Ethernet)
- IEEE 802.3ab (1000Base-T)
- IEEE 802.3ac (VLAN Tagging)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3ae (10G Ethernet)

ITU-T recommendations

- ITU-T G.8032, June 2007 draft (Ethernet Ring Protection)

IETF RFCs

IPv4

- RFC 2003 IP/IP Tunneling
- RFC 2784 GRE Tunneling

OSPF

- RFC 1253/1850/2328 OSPFv2 and MIB
- RFC 1587/3101 OSPF NSSA Option
- RFC 1765 OSPF Database Overflow
- RFC 2154 OSPF MD5 Signature
- RFC 2370/3630 OSPF Opaque LSA
- RFC 3623 OSPF Graceful Restart

RIP

- RFC 1058 RIPv1
- RFC 1722/1723/2453/1724 RIPv2 and MIB
- RFC 1812/2644 IPv4 Router Requirement
- RFC 2080 RIPng for IPv6

BGP

- RFC 1269/1657 BGP v3 and v4 MIB
- RFC 1403/1745 BGP/OSPF Interaction
- RFC 1771-1774/2842/2918/3392 BGP v4
- RFC 1965 BGP AS Confederations
- RFC 1966 BGP Route Reflection
- RFC 1997/1998 BGP Communities Attribute
- RFC 2042 BGP New Attribute
- RFC 2385 BGP MD5 Signature
- RFC 2439 BGP Route Flap Damping
- RFC 2545 BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
- RFC 2796 BGP Route Reflection
- RFC 2858 Multiprotocol Extensions for BGP-4
- RFC 3065 BGP AS Confederations

IP Multicast

- RFC 1075 DVMRP
- RFC 1112 IGMP v1
- RFC 2236/2933 IGMP v2 and MIB
- RFC 2362 PIM-SM
- RFC 2365 Multicast
- RFC 2715/2932 Multicast Routing MIB
- RFC 2934 PIM MIB for IPv4
- RFC 3376 IGMPv3
- RFC 5060 Protocol Independent Multicast MIB
- RFC 5132 IP Multicast MIB
- RFC 5240 PIM Bootstrap Router MIB

IPv6

- RFC 1886/3596 DNS for IPv6
- RFC 2292/2553/3493/3542 IPv6 Sockets
- RFC 2373/2374/3513/3587/4007/4193 IPv6 Addressing
- RFC 2452/2454 IPv6 MIB for TCP/UDP
- RFC 2460/2461/2462/2464 Core IPv6
- RFC 2463/2466/4443 ICMP v6 and MIB
- RFC 2893/3056/4213 IPv6 Transition Mechanisms
- RFC 3595 Flow Label Conventions

Manageability

- RFC 854/855 Telnet and Telnet Options
- RFC 959/2640 FTP
- RFC 1155/2578-2580 SMI v1 and SMI v2
- RFC 1157/2271 SNMP
- RFC 1212/2737 MIB and MIB-II
- RFC 1213/2011-2013 SNMP v2 MIB
- RFC 1215 Convention for SNMP Traps
- RFC 1350 TFTP Protocol
- RFC 1573/2233/2863 Private Interface MIB
- RFC 1643/2665 Ethernet MIB
- RFC 1901-1908/3416-3418 SNMP v2c
- RFC 2096 IP MIB
- RFC 2570-2576/3411-3415 SNMP v3
- RFC 2616/2854 HTTP and HTML
- RFC 2667 IP Tunneling MIB
- RFC 2668/3636 IEEE 802.3 MAU MIB
- RFC 2674 VLAN MIB
- RFC 3414 User-based Security Model
- RFC 4251 Secure Shell Protocol Architecture
- RFC 4252 The Secure Shell (SSH) Authentication Protocol
- RFC 4878 OAM Functions on Ethernet-Like Interfaces

Security

- RFC 1321 MD5
- RFC 2104 HMAC Message Authentication
- RFC 2138/2865/2868/3575/2618 RADIUS Authentication and Client MIB
- RFC 2139/2866/2867/2620 RADIUS Accounting and Client MIB
- RFC 2228 FTP Security Extensions
- RFC 2284 PPP EAP
- RFC 2869/2869bis RADIUS Extension

Quality of service

- RFC 896 Congestion Control
- RFC 1122 Internet Hosts
- RFC 2474/2475/2597/3168/3246 DiffServ
- RFC 3635 Pause Control

Others

- RFC 768 UDP
- RFC 791/894/1024/1349 IP and IP/Ethernet
- RFC 792 ICMP
- RFC 793/1156 TCP/IP and MIB
- RFC 826/903 ARP and Reverse ARP
- RFC 919/922 Broadcasting Internet Datagram
- RFC 925/1027 Multi-LAN ARP/Proxy ARP
- RFC 950 Subnetting
- RFC 951 BOOTP
- RFC 1151 RDP
- RFC 1191 Path MTU Discovery
- RFC 1256 ICMP Router Discovery
- RFC 1305/2030 NTP v3 and Simple NTP
- RFC 1493 Bridge MIB
- RFC 1518/1519 CIDR
- RFC 1541/1542/2131/3396/3442 DHCP
- RFC 1757/2819 RMON and MIB
- RFC 2131/3046 DHCP/BOOTP Relay
- RFC 2132 DHCP Options
- RFC 2251 LDAP v3
- RFC 2338/3768/2787 VRRP and MIB
- RFC 3021 Using 31-bit Prefixes
- RFC 3060 Policy Core
- RFC 3176 sFlow

MPLS

- RFC 3031/3032/3343/4182 MPLS
- RFC 3035/3036/3037/5036 LDP
- RFC 3478 LDP Graceful Restart
- RFC 4379 LSP Ping
- RFC 4762 VPLS using LDP

OmniSwitch 6850

OmniSwitch 6850-24X

OmniSwitch 6850-48

The **Alcatel-Lucent OmniSwitch™ 6850 Stackable LAN Switch** (SLS) family are fixed-configuration switches with layer-3 Gigabit Ethernet (GigE) and Power-over-Ethernet (PoE) capabilities. The OmniSwitch 6850 SLS products excel at the edge where they deliver line-rate gigabit switching and routing performance along with extensive network security features, enabling corporations to realize the full potential of secured networks.

They are advanced, stackable, triple-speed and 10G uplink switches that perform wire-rate layer-2 switching and layer-3 routing for both IPv4 and IPv6 natively, with optimal quality of service (QoS) for mission-critical applications.

Native IPv6, advanced QoS, security, and network management, along with a lifetime warranty, provide premium performance in the enterprise today while protecting customers' long-term capital interests — making this switch the best value in the industry.

KEY SELLING POINTS

- → Meet any customer configuration need and offer excellent investment protection and flexibility, as well as ease of deployment, operation and maintenance
- → Ensure network availability with a field-upgradable solution, reduce operating complexity and cost, and optimize response time for users and applications
- → Achieve outstanding performance when supporting real-time voice, data and video applications for converged scalable networks
- → Ensure efficient power management, reduce operating expenses and lower total cost of ownership (TCO) through the lowest power consumption in its class and dynamic PoE allocation, which delivers only the power needed by the attached device
- → Achieve enhanced security, fully integrated in the operating system and adaptive to user mobility, with comprehensive admission control, intrusion detection, containment and remediation at the edge of the network at no additional cost, allowing business continuity and preventing network outages

KEY FEATURES

- → Versatile features and models offering gigabit and 10-gigabit (10G) interfaces, IEEE 802.3af-compliant PoE, and 10/100 models upgradable to gigabit via a software license key without any network reconfiguration
- → Stacking capability for virtual chassis redundancy
- → External power supply choice (AC, DC, PoE) for flexible deployment and easier maintenance or power upgrade
- → Wire-rate performance for switching and routing at 10G and gigabit speeds
- → Advanced services incorporated in the operating system; for example, advanced QoS, access control lists (ACLs), bridging (layer 2) and routing (layer 3), VLAN stacking, and IPv6
- → Superior user and network security feature set
- → Suited for the edge, enterprise LAN wiring closets, aggregation layer in three-tier network, small enterprise core switching and metro Ethernet access — residential and business Ethernet services

TECHNICAL INFORMATION

OmniSwitch 6850-24(48)L

- 20 (44) RJ-45 Fast Ethernet ports
- Upgradable to 20 (44) GigE ports
- 4 Combo GigE ports
- 2 10G stack ports
- AC or DC, optional redundant power

OmniSwitch 6850-P24 (P48)L PoE

- 20 (44) RJ-45 Fast Ethernet (PoE) ports
- Upgradable to 20 (44) GigE ports
- 4 Combo GigE ports
- 2 10G stack ports
- AC, optional redundant power

OmniSwitch 6850-24(48)

- 20 (44) RJ-45 GigE ports
- 4 Combo GigE ports
- 2 10G stack ports
- AC or DC, optional redundant power

OmniSwitch 6850-P24 (P48) PoE

- 20 (44) RJ-45 GigE (PoE) ports
- 4 Combo GigE ports
- 2 10G stack ports
- AC, optional redundant power

OmniSwitch 6850-24(48)X

- 20 (48) RJ-45 GigE ports
- 4 (0) Combo GigE ports
- 2 XFP 10GigE ports
- 2 10G stack ports
- AC or DC, optional redundant power

OmniSwitch 6850-P24 (P48)X PoE

- 20 (48) RJ-45 GigE (PoE) ports
- 4 (0) Combo GigE ports
- 2 XFP 10GigE ports
- 2 10G stack ports
- AC, optional redundant power

OmniSwitch 6850-U24X

- 20 SFP Gigabit/Fast Ethernet ports
- 4 Combo GigE ports
- 2 XFP 10GigE ports
- 2 10G stack ports
- AC or DC, optional redundant power

IEEE standards

- IEEE 802.1D STP
- IEEE 802.1p CoS
- IEEE 802.1Q VLANs
- IEEE 802.1ad Provider Bridge QinQ (VLAN stacking)
- IEEE 802.1ag Connectivity Fault Management
- IEEE 802.1s MSTP
- IEEE 802.1w RSTP
- IEEE 802.1X Port-based Network Access Protocol
- IEEE 802.3i 10Base-T
- IEEE 802.3u Fast Ethernet
- IEEE 802.3x Flow Control
- IEEE 802.3z GigE
- IEEE 802.3ab 1000Base-T
- IEEE 802.3ac VLAN Tagging
- IEEE 802.3ad Link Aggregation
- IEEE 802.3af PoE
- IEEE 802.3ae 10G Ethernet

ITU-T recommendations

- ITU-T G.8032: Draft (June 2007) Ethernet Ring Protection

IETF RFCs

IPv4

- RFC 2003 IP/IP Tunneling
- RFC 2784 GRE Tunneling

BGP

- RFC 1269/1657 BGP v3 & v4 MIB
- RFC 1403/1745 BGP/OSPF Interaction
- RFC 1771-1774/2842/2918/3392 BGP v4
- RFC 1965 BGP AS Confederations
- RFC 1966 BGP Route Reflection
- RFC 1997/1998 BGP Communities Attribute
- RFC 2042 BGP New Attribute
- RFC 2385 BGP MD5 Signature
- RFC 2439 BGP Route Flap Damping
- RFC 2545 BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
- RFC 2796 BGP Route Reflection
- RFC 2858 Multiprotocol Extensions for BGP-4
- RFC 3065 BGP AS Confederations

OSPF

- RFC 1253/1850/2328 OSPF v2 and MIB
- RFC 1587/3101 OSPF NSSA Option
- RFC 1765 OSPF Database Overflow
- RFC 2154 OSPF MD5 Signature
- RFC 2370/3630 OSPF Opaque LSA
- RFC 3623 OSPF Graceful Restart

RIP

- RFC 1058 RIP v1
- RFC 1722/1723/2453/1724 RIP v2 and MIB
- RFC 1812/2644 IPv4 Router Requirements
- RFC 2080 RIPng for IPv6

IS-IS

- RFC 1142 OSI IS-IS for Intra-domain Routing Protocol
- RFC 1195 OSI IS-IS for Routing
- RFC 2763 Dynamic Host Name
- RFC 2966 Route Leaking
- RFC 3719 Interoperable Networks
- RFC 3787 Interoperable IP Networks Using IS-IS

IP Multicast

- RFC 1075 DVMRP
- RFC 1112 IGMP v1
- RFC 2236/2933 IGMP v2 and MIB
- RFC 2362 PIM-SM
- RFC 2365 Multicast
- RFC 2715/2932 Multicast Routing MIB
- RFC 2934 PIM MIB for IPv4
- RFC 3376 IGMPv3
- RFC 5060 Protocol Independent Multicast MIB
- RFC 5132 IP Multicast MIB
- RFC 5240 PIM Bootstrap Router MIB

IPv6

- RFC 1886 DNS for IPv6
- RFC 2292/2373/2374/2460/2462 IPv6 Addressing
- RFC 2461 NDP
- RFC 2463/2466 ICMP v6 and MIB
- RFC 2452/2454 IPv6 TCP/UDP MIB
- RFC 2464/2553/2893/3493/3513 IPv6 Transmission Mechanisms
- RFC 3056 IPv6 Tunneling
- RFC 3542/3587 IPv6
- RFC 3595 TC for Flow Label
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4193 Unique Local IPv6 Unicast Addresses

Manageability

- RFC 1350 TFTP Protocol
- RFC 854/855 Telnet and Telnet options
- RFC 1155/2578-2580 SMI v1 and SMI v2
- RFC 1157/2271 SNMP
- RFC 1212/2737 MIB and MIB-II
- RFC 1213/2011-2013 SNMP v2 MIB
- RFC 1215 Convention for SNMP Traps
- RFC 1573/2233/2863 Private Interface MIB
- RFC 1643/2665 Ethernet MIB
- RFC 1901-1908/3416-3418 SNMP v2c
- RFC 2096 IP MIB
- RFC 2570-2576/3411-3415 SNMP v3
- RFC 2616 /2854 HTTP and HTML
- RFC 2667 IP Tunneling MIB
- RFC 2668/3636 IEEE 802.3 MAU MIB
- RFC 2674 VLAN MIB
- RFC 3414 User-based Security Model
- RFC 4251 Secure Shell Protocol Architecture
- RFC 4252 The Secure Shell (SSH) Authentication Protocol
- RFC 4878 OAM Functions on Ethernet-Like Interfaces
- RFC 959/2640 FTP

Security

- RFC 1321 MD5
- RFC 2104 HMAC Message Authentication
- RFC 2138/2865/2868/3575/2618 RADIUS Authentication and Client MIB
- RFC 2139/2866/2867/2620 RADIUS Accounting and Client MIB
- RFC 2228 FTP Security Extensions
- RFC 2284 PPP EAP
- RFC 2869/2869bis RADIUS Extension

Quality of service

- RFC 896 Congestion Control
- RFC 1122 Internet Hosts
- RFC 2474/2475/2597/3168/3246 DiffServ
- RFC 3635 Pause Control

Others

- RFC 791/894/1024/1349 IP and IP/Ethernet
- RFC 792 ICMP
- RFC 768 UDP
- RFC 793/1156 TCP/IP and MIB
- RFC 826/903 ARP and Reverse ARP
- RFC 919/922 Broadcasting Internet Datagrams
- RFC 925/1027 Multi LAN ARP/ Proxy ARP
- RFC 950 Subnetting
- RFC 951 BOOTP
- RFC 1151 RDP
- RFC 1191 Path MTU Discovery
- RFC 1256 ICMP Router Discovery
- RFC 1305/2030 NTP v3 and Simple NTP
- RFC 1493 Bridge MIB
- RFC 1518/1519 CIDR
- RFC 1541/1542/2131/3396/3442 DHCP
- RFC 1757/2819 RMON and MIB
- RFC 2131/3046 DHCP/BOOTP Relay
- RFC 2132 DHCP Options
- RFC 2251 LDAP v3
- RFC 2338/3768/2787 VRRP and MIB
- RFC 3060 Policy Core
- RFC 3176 sFlow
- RFC 3021 Using 31-bit Prefixes

OmniSwitch 6855

OmniSwitch 6855-14

OmniSwitch 6855-U10

The **Alcatel-Lucent OmniSwitch™ 6855 Hardened LAN Switch** (HLS) models are industrial-grade, managed, Gigabit Ethernet (GigE) switches designed to operate reliably in harsh electrical and severe temperature environments.

This superior, rugged hardware design coupled with the widely deployed and field-proven Alcatel-Lucent Operating System (AOS) makes it ideal for industrial and mission-critical applications that require a wider range of operating temperatures, more stringent EMC/EMI requirements and an optimized feature set for high security, reliability, performance and easier management.

The OmniSwitch 6855 supports Power-over-Ethernet (PoE), which enables the provisioning of power to Ethernet devices, such as CCTV cameras, wireless access points, card readers and industrial sensors, at the edge of the network.

The target applications for these versatile LAN switches are power utilities, transportation and traffic control systems, industrial factory floor installations, video surveillance systems and outside installations, all requiring the benefits and performance of IP and Gigabit Ethernet.

KEY SELLING POINTS

- → Withstand greater shock, vibrations, wider temperature range and harsh EMI/EMC environments with uninterrupted traffic and zero communication errors in this purpose-built, industrial strength switch
- → Enable converged networks in challenged environments to connect and power CCTV cameras, IP phones, and wireless access points with PoE support
- → Support real-time voice, data and video applications. The switches provide first packet wire-speed classification and processing for all packets, giving a noticeable performance boost to converged enterprise networks.
- → Achieve a faster convergence time in a ring configuration, with support for the Ethernet Ring Protection (ERP) protocol
- → Provide resiliency through a superior architecture, offering physical redundancy at all levels

- Fully secure the network at the edge, at no additional cost, by supporting the network proactive and reactive capabilities that are provided through the Alcatel-Lucent Access Guardian™, traffic anomaly detection and the Alcatel-Lucent OmniVista™ 2500 NMS Quarantine Manager
- Reduce enterprise-wide costs through hardware consolidation to achieve network segmentation and security without additional hardware installation

KEY FEATURES

- Ruggedized hardware design
- Convection cooling for fan-less models or temperature-triggered fans
- Diverse power supply options: external, redundant, hot-swappable, AC and DC
- Wide choice of models offering different port densities: 10, 14, 24GigE, copper while supporting a variety of fiber types: single-mode, multi-mode, short- and long-haul optics, allowing distances up to 70 km
- Redundancy at all levels including power supplies, software and hot-swappable small form factor pluggable (SFP) modules
- PoE support on all copper models
- Wire-rate switching and routing at gigabit speeds
- Advanced services incorporated in the operating system: quality of service (QoS), access control lists (ACLs), layer 2/layer 3, VLAN stacking and IPv6
- Extensive security features for network access control, policy enforcement and attack containment
- Hardware-based virtual routing and forwarding (VRF) support

TECHNICAL INFORMATION

OmniSwitch 6855-14(D)

- 8 RJ-45 GigE ports
- 4 RJ-45 GigE (PoE) ports
- 2 SFP ports for GigE
- AC (or DC), optional redundant power

OmniSwitch 6855-24(D/DL)

- 16 RJ-45 GigE ports
- 4 RJ-45 GigE (PoE) ports
- 4 Combo GigE ports
- AC (or DC 48/24V), optional redundant power

OmniSwitch 6855-U10(D)

- 2 RJ-45 GigE ports
- 8 SFP ports for GigE
- AC (or DC), optional redundant power

OmniSwitch 6855-U24(D/DL)

- 22 SFP ports for GigE
- 2 Combo GigE ports
- AC (or DC 48/24V), optional redundant power

OmniSwitch 6855-U24X (D/DL)

- 22 SFP ports for GigE
- 2 Combo GigE ports
- 2 SFP+ 10GigE or 10G stacking ports
- AC (or DC 48/24V), optional redundant power

IEEE standards

- IEEE 802.1D STP
- IEEE 802.1p CoS
- IEEE 802.1Q VLANs
- IEEE 802.1ad Provider Bridge QinQ (VLAN stacking)
- IEEE 802.1ag Connectivity Fault Management
- IEEE 802.1s MSTP
- IEEE 802.1w RSTP
- IEEE 802.1X Port-based Network Access Protocol
- IEEE 802.3i 10Base-T
- IEEE 802.3u Fast Ethernet
- IEEE 802.3x Flow Control
- IEEE 802.3z GigE
- IEEE 802.3ab 1000Base-T
- IEEE 802.3ac VLAN Tagging
- IEEE 802.3ad Link Aggregation
- IEEE 802.3af Power-over-Ethernet
- IEEE 802.3ae 10G Ethernet

ITU-T recommendations

- ITU-T G.8032: Draft (June 2007) Ethernet Ring Protection

IETF RFCs

IPv4

- RFC 2003 IP/IP Tunneling
- RFC 2784 GRE Tunneling

OSPF

- RFC 1253/1850/2328 OSPF v2 and MIB
- RFC 1587/3101 OSPF NSSA Option
- RFC 1765 OSPF Database Overflow
- RFC 2154 OSPF MD5 Signature
- RFC 2370/3630 OSPF Opaque LSA
- RFC 3623 OSPF Graceful Restart

RIP

- RFC 1058 RIP v1
- RFC 1722/1723/2453/1724 RIP v2 and MIB
- RFC 1812/2644 IPv4 Router Requirement
- RFC 2080 RIPng for IPv6

BGP

- RFC 1269/1657 BGP v3 and v4 MIB
- RFC 1403/1745 BGP/OSPF Interaction
- RFC 1771-1774/2842/2918/3392 BGP v4
- RFC 1965 BGP AS Confederations
- RFC 1966 BGP Route Reflection
- RFC 1997/1998 BGP Communities Attribute
- RFC 2042 BGP New Attribute
- RFC 2385 BGP MD5 Signature
- RFC 2439 BGP Route Flap Damping
- RFC 2545 BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
- RFC 2796 BGP Route Reflection
- RFC 2858 Multiprotocol Extensions for BGP-4
- RFC 3065 BGP AS Confederations

IP Multicast

- RFC 1075 DVMRP
- RFC 1112 IGMP v1
- RFC 2236/2933 IGMP v2 and MIB
- RFC 2362 PIM-SM
- RFC 2365 Multicast
- RFC 2715/2932 Multicast Routing MIB
- RFC 2934 PIM MIB for IPv4
- RFC 3376 IGMPv3
- RFC 5060 Protocol Independent Multicast MIB
- RFC 5132 IP Multicast MIB
- RFC 5240 PIM Bootstrap Router MIB

IPv6

- RFC 1886 DNS for IPv6
- RFC 2292/2373/2374/2460/2462 Ipv6 Addressing
- RFC 2461 NDP
- RFC 2463/2466 ICMP v6 and MIB
- RFC 2452/2454 IPv6 TCP/UDP MIB
- RFC 2464/2553/2893/3493/3513 IPv6 Transmission Mechanisms
- RFC 3056 IPv6 Tunneling
- RFC 3542/3587 IPv6
- RFC 3595 TC for Flow Label
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4193 Unique Local IPv6 Unicast Addresses

Manageability

- RFC 1350 TFTP Protocol
- RFC 854/855 Telnet and Telnet Options
- RFC 1155/2578-2580 SMI v1 and SMI v2
- RFC 1157/2271 SNMP
- RFC 1212/2737 MIB and MIB-II
- RFC 1213/2011-2013 SNMP v2 MIB
- RFC 1215 Convention for SNMP Traps
- RFC 1573/2233/2863 Private Interface MIB
- RFC 1643/2665 Ethernet MIB
- RFC 1901-1908/3416-3418 SNMP v2c
- RFC 2096 IP MIB
- RFC 2570-2576/3411-3415 SNMP v3
- RFC 2616/2854 HTTP and HTML
- RFC 2667 IP Tunneling MIB
- RFC 2668/3636 IEEE 802.3 MAU MIB
- RFC 2674 VLAN MIB
- RFC 3414 User-based Security Model
- RFC 4251 Secure Shell Protocol Architecture
- RFC 4252 The Secure Shell (SSH) Authentication Protocol
- RFC 4878 OAM Functions on Ethernet-Like Interfaces
- RFC 959/2640 FTP

Security

- RFC 1321 MD5
- RFC 2104 HMAC Message Authentication
- RFC 2138/2865/2868/3575/2618 RADIUS Authentication and Client MIB
- RFC 2139/2866/2867/2620 RADIUS Accounting and Client MIB
- RFC 2228 FTP Security Extensions
- RFC 2284 PPP EAP
- RFC 2869/2869bis RADIUS Extension

Quality of service

- RFC 896 Congestion Control
- RFC 1122 Internet Hosts
- RFC 2474/2475/2597/3168/3246 DiffServ
- RFC 3635 Pause Control

Others

- RFC 791/894/1024/1349 IP and IP/Ethernet
- RFC 792 ICMP
- RFC 768 UDP
- RFC 793/1156 TCP/IP and MIB
- RFC 826/903 ARP and Reverse ARP
- RFC 919/922 Broadcasting Internet Datagram
- RFC 925/1027 Multi-LAN ARP/Proxy ARP
- RFC 950 Subnetting
- RFC 951 BOOTP
- RFC 1151 RDP
- RFC 1191 Path MTU Discovery
- RFC 1256 ICMP Router Discovery
- RFC 1305/2030 NTP v3 and Simple NTP
- RFC 1493 Bridge MIB
- RFC 1518/1519 CIDR
- RFC 1541/1542/2131/3396/3442 DHCP
- RFC 1757/2819 RMON and MIB
- RFC 2131/3046 DHCP/BOOTP Relay
- RFC 2132 DHCP Options
- RFC 2251 LDAP v3
- RFC 2338/3768/2787 VRRP and MIB
- RFC 3060 Policy Core
- RFC 3176 sFlow
- RFC 3021 Using 31-bit Prefixes

OmniSwitch 6400

OmniSwitch 6400-24

OmniSwitch 6400-U24

The new **Alcatel-Lucent OmniSwitch™ 6400 Stackable Gigabit LAN Switch** (SGS) is an extension to the existing OmniSwitch family of products that support triple speed applications, L2+ and an extensive array of networking features. The OmniSwitch 6400 addresses small- to medium-sized business (SMB) needs for converged voice, data and video networks as well as service providers' requirements for residential and business Ethernet access. Designed for optimized flexibility, scalability and low power consumption, the OmniSwitch 6400 provides an outstanding edge solution for highly available, self-protective, easily managed and eco-friendly networks.

The OmniSwitch 6400 SGS family comprises five stackable models that have built-in security, resiliency and enhanced OA&M management capabilities, making them ideal for any networking environment. This latest Alcatel-Lucent product offering supports the familiar and field-proven Alcatel-Lucent Operating System (AOS) functionality for effortless deployment within our available customer base while offering extended features to address new customer requirements. The OmniSwitch 6400 is the right fit for customers looking for improved edge performance, high availability, integrated security with easy deployment and management — all in one cost-effective platform.

The OmniSwitch 6400 was designed for use in a variety of markets and to complete the Alcatel-Lucent Ethernet access, SMB and branch office solution offerings with a best-of-breed, stackable LAN switch. This switch family offers the capacity enterprises and service providers need when advanced layer-3 or 10-gigabit (10G) uplinks are not required. Compared with the Alcatel-Lucent OmniSwitch™ 6250 Stackable LAN Switch, the OmniSwitch 6400 provides gigabit performance.

KEY SELLING POINTS

- → Uses AC or DC power
- → Offers high availability using stacking functions, redundant power and complete element redundancy
- → Offers a variety of Power-over-Ethernet (PoE), non-PoE gigabit and fiber models: Includes the 24- and 48-port (PoE and non-PoE) triple-speed copper versions and a 24-port fiber model
- → Supports advanced layer-2 switching with basic layer-3 routing at wire-rate speeds and Alcatel-Lucent extensive AOS functionality
- → Features always-on robust infrastructure, optimal response time for users and applications, and investment protection

- Allows business continuity and prevents network outages with edge network security and control
- Offers scalable and versatile configuration with effortless deployment meeting SMB, branch office or service provider preferences
- Stackable, fixed configuration chassis in a 1U form factor can be optionally equipped with Alcatel-Lucent-approved small form factor pluggable (SFP) transceivers supporting short, long and very long distances

KEY FEATURES

- Choice of 24 ports, 48 ports, PoE, non-PoE and fiber models
- Scalability from 24 to 384 ports by stacking up to eight units with dedicated stacking ports
- AOS field-proven software with management through web interface (WebView), CLI and Simple Network Management Protocol (SNMP)
- Ethernet OA&M support for service configuration and monitoring
- Support by Alcatel-Lucent OmniVista™ 2500 Network Management System (NMS)
- Alcatel-Lucent 5620 Service Aware Manager (SAM) applications (for service providers)

Security features

- Auto-sensing network access control through the Access Guardian framework (802.1X, MAC, rules)
- Automated containment and quarantine with the Alcatel-Lucent OmniVista 2500 NMS Quarantine Manager™ integrated in the OmniVista 2500 NMS
- Advanced quality of service (QoS) and access control lists (ACLs) for traffic control

Performance and redundancy features

- Advanced layer-2+ features with basic layer-3 routing for both IPv4 and IPv6
- Triple-speed (10/100/1000) user interfaces and Gigabit Ethernet fiber interfaces (SFP) supporting 100Base-X or 1000Base-X optical transceivers
- Wire-rate switching and routing performance
- High availability with virtual chassis concept, redundant stacking links, primary/secondary unit failover, hot-swappable power options and configuration rollback

TECHNICAL INFORMATION

OmniSwitch 6400-24(48)

- 20 (44) RJ-45 GigE ports
- 4 Combo GigE ports
- 2 10G stack ports
- AC, optional redundant power

OmniSwitch 6400-P24(P48) PoE

- 20 (44) RJ-45 GigE (PoE) ports
- 4 Combo GigE ports
- 2 10G stack ports
- AC, optional redundant power

OmniSwitch 6400-U24

- 22 SFP Gigabit/Fast Ethernet ports
- 2 Combo GigE ports
- 2 10G stack ports
- AC, optional redundant power

OmniSwitch 6400-U24D

- 22 SFP Gigabit/Fast Ethernet ports
- 2 Combo GigE ports
- 2 10G stack ports
- DC, optional redundant power

IEEE standards

- IEEE 802.1D (STP)
- IEEE 802.1p (CoS)
- IEEE 802.1Q (VLANs)
- IEEE 802.1ad (Provider Bridge) QinQ (VLAN stacking)
- IEEE 802.1ag (Connectivity Fault Management)
- IEEE 802.1s (MSTP)
- IEEE 802.1w (RSTP)
- IEEE 802.1X (Port-based Network Access Protocol)
- IEEE 802.3i (10Base-T)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (GigE)
- IEEE 802.3ab (1000Base-T)
- IEEE 802.3ac (VLAN Tagging)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3af (Power-over-Ethernet)

ITU-T recommendations

- ITU-T G.8032: Draft (June 2007) Ethernet Ring Protection

IETF RFCs

IPv4

- RFC 2003 IP/IP Tunneling
- RFC 2784 GRE Tunneling

RIP

- RFC 1058 RIP v1
- RFC 1722/1723/2453/1724 RIP v2 and MIB
- RFC 1812/2644 IPv4 Router Requirements
- RFC 2080 RIPng for IPv6

IP Multicast

- RFC 1112 IGMP v1
- RFC 2236/2933 IGMP v2 and MIB
- RFC 2365 Multicast
- RFC 3376 IGMPv3

IPv6

- RFC 1886 DNS for IPv6
- RFC 2292/2373/2374/2460/2462 Advanced Sockets API for IPv6
- RFC 2461 NDP
- RFC 2463/2466 ICMP v6 and MIB
- RFC 2452/2454 IPv6 TCP/UDP MIB
- RFC 2464/2553/2893/3493/3513 Transmission of IPv6 Packets over Ethernet Networks
- RFC 3056 IPv6 Tunneling
- RFC 3542/3587 IPv6

Manageability

- RFC 1350 TFTP Protocol
- RFC 854/855 Telnet and Telnet options
- RFC 1155/2578-2580 SMI v1 and SMI v2
- RFC 1157/2271 SNMP
- RFC 1212/2737 MIB and MIB-II
- RFC 1213/2011-2013 SNMP v2 MIB
- RFC 1215 Convention for SNMP Traps
- RFC 1573/2233/2863 Private Interface MIB
- RFC 1643/2665 Ethernet MIB
- RFC 1901-1908/3416-3418 SNMP v2c
- RFC 2096 IP MIB
- RFC 2570-2576/3411-3415 SNMP v3
- RFC 2616/2854 HTTP and HTML
- RFC 2667 IP Tunneling MIB
- RFC 2668/3636 IEEE 802.3 MAU MIB
- RFC 2674 VLAN MIB
- RFC 3414 User-based Security Model
- RFC 4251 Secure Shell Protocol Architecture
- RFC 4252 The Secure Shell (SSH) Authentication Protocol

- RFC 4878 OAM Functions on Ethernet-Like Interfaces
- RFC 959/2640 FTP

Security

- RFC 1321 MD5
- RFC 2104 HMAC Message Authentication
- RFC 2138/2865/2868/3575/2618 RADIUS Authentication and Client MIB
- RFC 2139/2866/2867/2620 RADIUS Accounting and Client MIB
- RFC 2228 FTP Security Extensions
- RFC 2284 PPP EAP
- RFC 2869/2869bis RADIUS Extension

Quality of service

- RFC 896 Congestion Control
- RFC 1122 Internet Hosts
- RFC 2474/2475/2597/3168/3246 DiffServ
- RFC 3635 Pause Control

Others

- RFC 791/894/1024/1349 IP and IP/Ethernet
- RFC 792 ICMP
- RFC 768 UDP
- RFC 793/1156 TCP/IP and MIB
- RFC 826/903 ARP and Reverse ARP
- RFC 919/922 Broadcasting Internet Datagrams
- RFC 925/1027 Multi LAN ARP/Proxy ARP
- RFC 950 Subnetting
- RFC 951 BOOTP
- RFC 1151 RDP
- RFC 1191 Path MTU Discovery
- RFC 1256 ICMP Router Discovery
- RFC 1305/2030 NTP v3 and Simple NTP
- RFC 1493 Bridge MIB
- RFC 1518/1519 CIDR
- RFC 1541/1542/2131/3396/3442 DHCP
- RFC 1757/2819 RMON and MIB
- RFC 2131/3046 DHCP/BOOTP Relay
- RFC 2132 DHCP Options
- RFC 2251 LDAP v3
- RFC 2338/3768/2787 VRRP and MIB
- RFC 3060 Policy Core
- RFC 3176 sFlow
- RFC 3021 Using 31-bit Prefix

OmniSwitch 6250

OmniSwitch 6250-8M

OmniSwitch 6250-24/P24/24M/24MD

The **Alcatel-Lucent OmniSwitch™ 6250 Stackable Fast Ethernet Switch** (SFES) is a layer-2+ LAN family of switches for both the enterprise and Ethernet access segments. Enterprise models address the small and medium-sized enterprise edge and branch office environments, while the metro models address the residential and business Ethernet access supplied by service providers.

With an optimized design for flexibility and scalability as well as low power consumption, the OmniSwitch 6250 runs on the field-proven Alcatel-Lucent Operating System (AOS), providing an outstanding edge solution for highly available, self-protective, easily managed and eco-friendly networks.

The Alcatel-Lucent OmniSwitch 6250 family is an evolution of the current Alcatel-Lucent OmniStack™ 6200 Stackable LAN Switch family, embedding the latest technology and AOS innovations.

Solutions benefiting from the OmniSwitch 6250 family of switches are:

- → Edge of small-to-medium-sized networks
- → Branch office enterprise workgroups
- → Residential/metro Ethernet triple-play applications

All models in the Alcatel-Lucent OmniSwitch 6250 family are stackable, half-rack width (8.5 in./21.59 cm), fixed-configuration chassis in a 1U form factor. A variety of Power-over-Ethernet (PoE) (enterprise) and non-PoE (enterprise and metro) models are offered. They can be optionally equipped with Alcatel-Lucent-approved small form factor pluggable (SFP) transceivers supporting short, long and very long distances.

KEY SELLING POINTS

- → Provides simplified selection with only two enterprise models (non-PoE and PoE):
  - ¬ Reduces sparing and inventory costs
  - ¬ Allows for any mix of PoE and non-PoE, up to 416 ports
- → Small form factor and low noise output makes the OmniSwitch 6250 ideal for collocation environments. The low power consumption reduces operating expenses and cooling costs, lowering operational expenditures and resulting in faster return on investment (ROI).

- Leads the industry in price/feature-performance ratio and offers customers a cost-efficient network technology upgrade without being forced to move to a higher priced layer-2+ gigabit solution
- Provides outstanding features and performance for supporting scalable real-time voice, data and video applications for converged networks
- Allows existing AOS customers/users immediate familiarity with the product from day one, reducing their total cost of ownership (TCO) and training costs. New users may choose one of the several methods of switch access most beneficial to their needs.
- Lifetime warranty eliminates service program costs and ongoing service renewals, lowering TCO and allowing customers to reach ROI targets more quickly.

KEY FEATURES

- Innovative models with half-rack width make for greater variety of switch combinations
- Highly efficient and optimized in their form factor, power consumption and acoustic output
- Developed to satisfy customer requests for feature-rich, cost-effective 10/100 stackable switch built on the latest technologies
- AOS-based, field-proven software with management through web interface (WebView), CLI and Simple Network Management Protocol (SNMP)
- Supported by Alcatel-Lucent OmniVista™ 2500 Network Management System (NMS) and Alcatel-Lucent 5620 Service Aware Manager (SAM) applications for service providers

Security features

- Auto-sensing network access control (NAC) through the Alcatel-Lucent Access Guardian framework (multi-client/VLAN 802.1X, MAC, rules)
- Advanced QoS and access control lists (ACLs) for traffic control, including an embedded denial of service (DoS) engine to filter out unwanted traffic attacks
- Web-based authentication (captive portal)

Performance and redundancy features

- Advanced layer-2+ features with basic layer-3 routing for both IPv4 and IPv6 wire-rate switching and routing performance
- High availability with virtual chassis concept, redundant stacking links, primary/secondary unit failover, hot-swappable power options and configuration rollback

Features for small-to-mid-sized enterprise edge, branch or small business scenarios

- → Feature-rich Fast Ethernet switches at the LAN edge where gigabit speed is not required
- → Very flexible media options with PoE, non-PoE
- → Two combo ports on each unit, individually configurable for connectivity to servers, aggregating switches or data centers
- → Scalable up to 384 10/100 and 32 GigE ports per 8U rack space
- → Highly optimized in their form factor and acoustic output for collocation environments
- → Wire speed layer-2+ and basic layer-3 switching
- → Intelligent, secure and available networking for demanding applications

Features for residential and business Ethernet access services

- → Ethernet services: Virtual LAN (VLAN) stacking, SVLAN, CVLAN
- → Ethernet OA&M for management and troubleshooting
- → Extensive QoS capability guaranteed delivery: flow-based management, tri-color marking
- → IPTV multicast for video services delivery
- → Metro edge security features for traffic containment: private VLAN, Dynamic Host Configuration Protocol (DHCP) and Internet Group Management Protocol (IGMP) snooping, Access Guardian
- → Supported by industry-leading Alcatel-Lucent 5620 SAM
- → Compliant with MEF 9 and 14

TECHNICAL INFORMATION

OmniSwitch 6250-24

- 24 RJ-45 Fast Ethernet ports
- 2 Combo GigE ports
- 2 2.5-Gigabit HDMI stack ports
- AC, optional redundant power

OmniSwitch 6250-P24 Power over Ethernet

- 24 RJ-45 Fast Ethernet (PoE+) ports
- 2 Combo GigE ports
- 2 2.5-Gigabit HDMI stack ports
- AC, optional redundant power

OmniSwitch 6250-24M(D)

- 24 RJ-45 Fast Ethernet ports
- 2 Combo GigE ports
- 2 SFP GigE or 2.5-Gigabit stacking ports
- AC (or DC), optional redundant power

OmniSwitch 6250-8M

- 8 RJ-45 Fast Ethernet ports
- 2 Combo GigE ports
- 2 SFP GigE or 2.5-Gigabit stacking ports
- AC, optional redundant power

IEEE standards

- IEEE 802.1D (STP)
- IEEE 802.1p (CoS)
- IEEE 802.1Q (VLANs)
- IEEE 802.1ad (Provider Bridge) Q-in-Q (VLAN stacking)
- IEEE 802.1ag (Connectivity Fault Management)
- IEEE 802.1s (MSTP)
- IEEE 802.1w (RSTP)
- IEEE 802.1X (Port-based Network Access Protocol)
- IEEE 802.3i (10Base-T)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (GigE)
- IEEE 802.3ab (1000Base-T)
- IEEE 802.3ac (VLAN Tagging)

- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3af (Power-over-Ethernet)
- IEEE 802.3at (Power-over-Ethernet)
- IEEE 802.ah (Ethernet first mile)

IETF RFCs

IPv4
- RFC 2003 IP/IP Tunneling
- RFC 2784 GRE Tunneling

RIP
- RFC 1058 RIP v1
- RFC 1722/1723/2453/1724 RIP v2 and MIB
- RFC 1812/2644 IPv4 Router Requirements
- RFC 2080 RIPng for IPv6

IP Multicast
- RFC 1112 IGMP v1
- RFC 2236/2933 IGMP v2 and MIB
- RFC 2365 Multicast
- RFC 3376 IGMPv3 for IPv6

IPv6
- RFC 1886 DNS for IPv6
- RFC 2292/2373/2374/2460/2462 Advanced Sockets API for IPv6
- RFC 2461 NDP
- RFC 2463/2466 ICMP v6 and MIB
- RFC 2452/2454 IPv6 TCP/UDP MIB
- RFC 2464/2553/2893/3493/3513 Transmission of IPv6 Packets over Ethernet Networks
- RFC 3056 IPv6 Tunneling
- RFC 3542/3587 IPv6
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4193 Unique Local IPv6 Unicast Addresses

Manageability
- RFC 1350 TFTP Protocol
- RFC 854/855 Telnet and Telnet options
- RFC 1155/2578-2580 SMI v1 and SMI v2
- RFC 1157/2271 SNMP
- RFC 1212/2737 MIB and MIB-II
- RFC 1213/2011-2013 SNMP v2 MIB
- RFC 1215 Convention for SNMP Traps
- RFC 1573/2233/2863 Private Interface MIB
- RFC 1643/2665 Ethernet MIB
- RFC 1901-1908/3416-3418 SNMP v2c
- RFC 2096 IP MIB
- RFC 2570-2576/3411-3415 SNMP v3
- RFC3414 User-based Security Model
- RFC 2616/2854 HTTP and HTML
- RFC 2667 IP Tunneling MIB
- RFC 2668/3636 IEEE 802.3 MAU MIB
- RFC 2674 VLAN MIB
- RFC 4251 Secure Shell Protocol Architecture
- RFC 4252 The Secure Shell (SSH) Authentication Protocol
- RFC 959/2640 FTP

Security
- RFC 1321 MD5
- RFC 2104 HMAC Message Authentication
- RFC 2138/2865/2868/3575/2618 RADIUS Authentication and Client MIB
- RFC 2139/2866/2867/2620 RADIUS Accounting and Client MIB
- RFC 2228 FTP Security Extensions
- RFC 2284 PPP EAP
- RFC 2869/2869bis RADIUS Extension

Quality of service
- RFC 896 Congestion Control
- RFC 1122 Internet Hosts
- RFC 2474/2475/2597/3168/3246 DiffServ
- RFC 3635 Pause Control

Others
- RFC 791/894/1024/1349 IP and IP/Ethernet
- RFC 792 ICMP
- RFC 768 UDP
- RFC 793/1156 TCP/IP and MIB
- RFC 826/903 ARP and Reverse ARP
- RFC 919/922 Broadcasting Internet Datagram
- RFC 925/1027 Multi-LAN ARP/Proxy ARP
- RFC 950 Sub-netting
- RFC 951 BOOTP
- RFC 1151 RDP
- RFC 1191 Path MTU Discovery
- RFC 1256 ICMP Router Discovery
- RFC 1305/2030 NTP v3 and Simple NTP
- RFC 1493 Bridge MIB
- RFC 1518/1519 CIDR
- RFC 1541/1542/2131/3396/3442

DHCP
- RFC 1757/2819 RMON and MIB
- RFC 2131/3046 DHCP/BOOTP Relay
- RFC 2132 DHCP Options
- RFC 2251 LDAP v3
- RFC 3060 Policy Core
- RFC 3176 sFlow
- RFC 3021 Using 31-bit prefixes

OmniStack 6200

OmniStack 6212

OmniStack 6248

The **Alcatel-Lucent OmniStack™ 6200 Stackable LAN Switch** (SLS) is a family of stackable Ethernet switches that address enterprise and residential networking needs. The OmniStack 6200 family consists of seven different, stackable, layer-2+ switches: 12-, 24- and 48-port Fast Ethernet switches with and without Power over Ethernet (PoE). There is also a version that can contain up to 26 optical fiber transceivers. The switches securely support advanced quality of service (QoS) with advanced user and traffic classification capabilities for exceptional video, voice and data performance. These compact switches have a one unit (1U) high form factor that supports an all-in-one stackable design. The OmniStack 6200 family comes with a comprehensive set of features making it perfect for:

- → Enterprise workgroups
- → LAN wiring closets
- → Edge deployments
- → Small/medium-sized businesses and branch offices
- → Deployments requiring PoE

The OmniStack 6212 and OmniStack 6224 are a perfect fit for environments with severe noise restrictions because they offer a fan-less design.

This switch family provides a superior architecture with four usable Gigabit Ethernet (GigE) ports that support stacking and multi-gigabit uplink connectivity without sacrificing user ports.

- → Every OmniStack 6200 switch comes with two 10/100/1000 copper RJ-45 ports that can be used with standard Ethernet cabling for fault-tolerant dedicated stacking links or as gigabit ports in a standalone configuration.
- → They also come with two additional gigabit combo ports that provide ports for upstream connectivity to the network or to high-speed servers. Combo ports provide the user the ability to attach via standard copper Ethernet cabling or fiber using industry standard optical transceivers.

This means every OmniStack 6200 switch comes with four simultaneously operational wire-speed GigE ports.

The OmniStack 6200 can be stacked with mix and match of any model up to eight units high supporting a fault-tolerant stack loop. The copper RJ-45 10/100/1000 ports used for stacking use standard Category 5 Ethernet cabling and RJ-45 connectors for dedicated stacking between elements supporting one primary plus one secondary management entity.

KEY SELLING POINTS

- → Cost-effective enterprise workgroup switch for small and medium-sized enterprise networks
- → Highly available network edge for key applications such as IP voice communications by providing PoE, wire-speed QoS and security
- → Reduces the complexity and costs associated with training, configuration and maintenance by offering industry-standard CLI and simplified stack management with standard Ethernet cabling
- → Supports service providers' requirements for the network edge with VLAN stacking, multicast TV VLANs for user service differentiation and efficient bandwidth usage with better operator control and security

KEY FEATURES

Availability/performance

- → Superior architecture with 24/48 ports Fast Ethernet and four usable gigabit ports that support stacking and multi-gigabit uplink
- → 801.s, 802.1w Spanning Tree for loop-free topology, link redundancy and sub-second failover
- → Advanced QoS for user traffic and user service differentiation

Manageability/ease-of-deployment

- → Fan-less designs for OmniStack 6212 and OmniStack 6224 models. Perfect fit for office environment with noise restrictions
- → Industry-standard CLI, Simple Network Management Protocol (SNMP) and web browser for easier operations
- → IEEE 802.1ab and LLDP-MED extensions for network discovery, topology and easier VoIP deployment

Security

- → Per-port and per-user 802.1X and MAC authentication
- → Guest VLAN, private VLAN for limiting network access to unauthorized clients
- → Dynamic Host Configuration Protocol (DHCP) snooping and dynamic Address Resolution Protocol (ARP) inspection for IP address control and protection

Ethernet access services

- → Per-service VLAN stacking with per-port and inner VLAN classification
- → Multicast TV VLAN registration for maximum bandwidth efficiency between edge and core

TECHNICAL INFORMATION

OmniStack 6212/6224/6248

- 12/24/48 RJ-45 Fast Ethernet ports
- 2 Combo Gigabit/Fast Ethernet ports
- 2 SFP Gigabit/Fast Ethernet ports
- AC, optional redundant power

OmniStack 6212P/6224P/6248P PoE

- 12/24/48 RJ-45 Fast Ethernet (PoE) ports
- 2 Combo Gigabit/Fast Ethernet ports
- 2 SFP Gigabit/Fast Ethernet ports
- AC, optional redundant power

OmniStack 6224U

- 24 SFP Fast Ethernet ports
- 2 Combo Gigabit/Fast Ethernet ports
- 2 SFP Gigabit/Fast Ethernet ports
- AC, optional redundant power

Safety agency approvals

- UL 60950-1, USA
- CSA-C22.2 No. 60950-1-03, Canada
- EN 60950-1: 2001; all deviations (CE Mark), Europe
- IEC 60950-1:2001; all national deviations (CB Mark), other countries
- TUV-GS Mark, Germany
- EN60825-1 Laser
- EN60825-2 Laser
- CDRH Laser

IEEE Standards

- IEEE 802.1D (STP)
- IEEE 802.1p (CoS)
- IEEE 802.1Q (VLANs)
- IEEE 802.1ad (VLAN stacking)
- IEEE 802.1s (MSTP)
- IEEE 802.1w (RSTP)
- IEEE 802.1X (Port-based NAC)
- IEEE 802.3i (10Base-T)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (Gigabit Ethernet)
- IEEE 802.3ab (1000Base-T)
- IEEE 802.3ac (VLAN Tagging)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3af (Power-over-Ethernet)

IETF standards

IP Multicast

- RFC 1112 IGMP v1
- RFC 2236 IGMP v2

Manageability

- RFC 1350 TFTP Protocol
- RFC 1157 SNMP
- RFC 1907 SNMP v2
- RFC 1212/2737 MIB and MIB-II
- RFC 1213/2011-2013 SNMP v2 MIB
- RFC 1215 Convention for SNMP Traps
- RFC 1573/2233/2863 Private Interface MIB
- RFC 1643/2665 Ethernet MIB
- RFC 2096 IP MIB
- RFC 2616/2854 HTTP and HTML
- RFC 2668 IEEE 802.3 MAU MIB
- RFC 2674 VLAN MIB
- RFC 4251 Secure Shell Protocol Architecture
- RFC 2012 UDP MIB
- RFC 2573 SNMP Target MIB, SNMP Notification MIB
- RFC 2574 SNMP User-Based SM MIB
- RFC 2575 SNMP View Based ACM MIB
- RFC 2576 SNMP Community MIB

Security

- RFC 2618 RADIUS

Others

- RFC 791/894/1024/1349 IP and IP/Ethernet
- RFC 792 ICMP
- RFC 768 UDP
- RFC 793/1156 TCP/IP and MIB
- RFC 826 ARP
- RFC 2030 SNTP
- RFC 1493 Bridge MIB
- RFC 1541 DHCP
- RFC 1757 RMON and MIB
- RFC 2132 DHCP Options

Electromagnetic emission certification and immunity

- FCC Part 15 (CFR 47) Class A
- VCCI Class A, Japan
- EN 55022 Class A, EN 55024 Class A
- EN 61000-4-2 ESD, EN 61000-4-3 Radiated Immunity, EN 61000-4-4 EFT, EN 61000-4-5 Surge, EN 61000-4-6 Low Frequency Common Immunity, EN 61000-4-8, EN 61000-4-11 Voltage Dips and Sags

Environmental compliance

- EU 2002/95/EC RoHS (with lead exemption)
- EU 2002/91/EC WEEE

OmniAccess 6000

OmniAccess 6000

The **Alcatel-Lucent OmniAccess™ 6000** is a high-performance, fully featured, modular WLAN switch able to aggregate up to 2048 campus-connected access points (APs). The OmniAccess 6000 provides a true user-centric network experience, delivering follow-me connectivity, identity-based access and application continuity services.

The OmniAccess 6000 offers a scalable design that supports large deployments and can be easily implemented as an overlay without disruption to the existing wired network. Advanced Voice over WLAN (VoWLAN) features such as call admission control (CAC), voice-aware radio frequency (RF) management and strict over-the-air quality of service (QoS) allow the OmniAccess 6000 to deliver mobile VoIP capabilities.

The OmniAccess 6000 is managed through the integrated management capability of the Alcatel-Lucent OmniAccess Wireless Operating System or the Alcatel-Lucent OmniVista™ 3600 Air Manager.

KEY SELLING POINTS

- → Platforms support multiple supervisor engines designed to handle heavy traffic loads generated by IEEE 802.11n APs
- → Can control up to 2048 campus-connected APs while offering a pay-as-you-grow model. The OmniAccess 6000 AP capacity can grow by adding supervisor modules and/or adding software licenses.
- → Allows for overlay deployments without disruption to the existing wireline infrastructure
- → Simplifies management by minimizing the number of network elements
- → Provides analysis of the RF environment to facilitate deployment with self-tuning APs and to facilitate operation of the network with virtual real-time site survey
- → Integrates both wireless networking and wireless intrusion detection and prevention, thus reducing the cost of wireless infrastructure and cost of operating the wireless network
- → Prevents unauthenticated users from accessing the corporate wireless network while safely supporting guest users, contractors and corporate users
- → Decreases management burden of security through role-based security
- → 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

- → Improves voice quality through support of QoS mechanisms such as Wi-Fi multimedia (WMM), differentiated services code point (DSCP) marking and prioritization and CAC
- → Improves end users' voice experience by maximizing battery life with protocols such as Unscheduled Automatic Power Save Delivery (U-APSD)
- → Provides unmatched voice security through embedded stateful firewall
- → Allows for seamless hand-off of voice terminal as users move from AP to AP

KEY FEATURES

- → High performance
- → Scalable architecture
- → Centralized WLAN switching
- → Dynamic RF management
- → Integrated wireless intrusion prevention
- → User-centric security with stateful firewall
- → Real-time location tracking
- → QoS, extended battery capabilities, seamless roaming for support of voice terminals

TECHNICAL INFORMATION

Performance and capacity

- Campus-connected APs: Up to 2048
- Remote APs: Up to 8192
- 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 Gb/s
- Encrypted throughput (3DES): Up to 32 Gb/s
- Encrypted throughput (AES-CCM): Up to 16 Gb/s

WLAN security and control

- 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 generic routing encapsulation (GRE)
- CAPWAP-compatible and upgradeable
- Distributed WLAN mode for remote AP deployments
- Simultaneous centralized and distributed WLAN support

Identity-based security

- 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

- 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 Application Layer Gateways (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 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 ring tone generation (RFC 3960)
- Per-user and per-role rate limits (bandwidth contracts)

Adaptive radio management (ARM)

- 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

- 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
- Ad hoc WLAN network detection and containment
- Windows client bridging and wireless bridge detection
- Denial of service (DoS) 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

- 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
- 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 DoS 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

- 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 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 Dynamic Host Configuration Protocol (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

- 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

- 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 W per PSU

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

- AC input voltage: 90 V AC to 132 V AC, 170 V AC to 264 V AC
- AC input frequency: 47 Hz to 63 Hz
- AC input current: 5 A at 110 V AC

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

- AC input voltage: 85 V AC to 264 V AC, auto-sensing
- AC input frequency: 47 Hz to 63 Hz
- AC input current: 5 A at 110 V AC

Operating specifications and dimensions

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

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), 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 mark, cTUVus, GS, CB, C-tick, Anatel, NOM, MIC, IQC

OmniAccess 4000

OmniAccess 4504

OmniAccess 4603GW

The **Alcatel-Lucent OmniAccess™ 4000** family of high-performance WLAN switches are fixed form factor controllers designed for advanced WLAN services. At the same time they offer a cost-effective price point for small to large networks.

The switches share a common set of advanced features to offer best-in-class security and accommodate demanding applications such as Voice over WLAN (VoWLAN). In addition, these WLAN switches simplify the deployment, monitoring and troubleshooting of the WLAN infrastructure.

The switches aggregate network traffic from access points (APs), process it and deliver it to the network.

The OmniAccess 4000 line of WLAN switches includes multiple models, designed to support the varying requirements of differently sized wireless networks such as campus, branch office, or small business networks. The OmniAccess 4302, 4304, 4306, 4306G/GW, 4308, 4504, 4324, 4604 and 4704 are fully featured WLAN switches designed from the ground up to support the traffic load of IEEE 802.11n high-speed wireless networks with the ability to aggregate up to 8, 8, 16, 16, 32, 48, 64 and 128 APs respectively.

KEY SELLING POINTS

- → User-centric network experience delivers follow-me connectivity and identity-based access
- → Application continuity services with seamless voice hand-off
- → Built-in stateful firewall and centralized cryptography for best-in-class security
- → Integrated mesh capability for WLAN bridging and backhauling
- → Remote AP management for extension of corporate Wi-Fi® network to small branches or home offices

KEY FEATURES

- → Easy to deploy as an overlay without disruption to the wired network
- → Centralized security policies, control and management
- → Adaptive radio frequency management
- → Identity-based security

- → Quarantine of unsafe traffic
- → Reach of Wi-Fi network extended with wireless mesh capability
- → Built-in wireless intrusion detection and prevention
- → Integrated location tracking capability for Wi-Fi clients and Wi-Fi asset tags
- → VoWLAN capabilities with application-aware adaptive networking
- → Support for IEEE 802.11 a/b/g/n APs

TECHNICAL INFORMATION

OmniAccess 4302

- Maximum LAN-connected APs: 8
- Maximum remote APs: 8
- Maximum number of users: 100
- (MAC) addresses: 4096
- 10/100Base-T ports: 1
- 10/100/1000Base-T ports: 1
- Form factor/footprint: Desktop
- Active firewall sessions: 32,000
- Concurrent IPSec tunnels: 100
- Firewall throughput: 1 Gb/s
- Encrypted throughput (3DES, AESCBC256): 200 Mb/s
- Encrypted throughput (AES-CCM): 200 Mb/s
- Maximum power consumption: 12 W

OmniAccess 4306

- Maximum LAN-connected APs: 8
- Maximum remote APs: 32
- Maximum number of users: 128
- MAC addresses: 2048
- 10/100Base-T ports: 8
- 10/100/1000Base-T ports: 1
- USB ports: 1
- ExpressCard® Technology slot: Yes
- Form factor/footprint: Desktop
- Active firewall sessions: 8192
- Concurrent IPSec tunnels: 128
- Firewall throughput: 800 Mb/s
- Encrypted throughput (3DES, AESCBC256): 400 Mb/s
- Encrypted throughput (AES-CCM): 320 Mb/s
- PoE+ ports: 4
- Maximum power consumption: 115 W

OmniAccess 4306G

- Maximum LAN-connected APs: 16
- Maximum remote APs: 64
- Maximum number of users: 256
- MAC addresses: 2048
- 10/100/1000Base-T ports: 6
- Gigabit SFP ports: 2
- USB ports: 4
- ExpressCard® Technology slot: Yes
- Form factor/footprint: Desktop
- Active firewall sessions: 16,384
- Concurrent IPSec tunnels: 256
- Firewall throughput: 2 Gb/s
- Encrypted throughput (3DES, AESCBC256): 1.6 Gb/s
- Encrypted throughput (AES-CCM): 800 Mb/s
- PoE+ ports: 4
- Maximum power consumption: 126 W

OmniAccess 4306GW

- Maximum LAN-connected APs: 17
- Maximum remote APs: 64
- Integrated AP: Yes
- Maximum number of users: 256
- MAC addresses: 2048
- 10/100/1000Base-T ports: 6
- Gigabit SFP ports: 2
- USB ports: 4
- ExpressCard Technology slot: Yes
- Form factor/footprint: Desktop
- Active firewall sessions: 16,384
- Concurrent IPSec tunnels: 256
- Firewall throughput: 2 Gb/s
- Encrypted throughput (3DES, AESCBC256): 1.6 Gb/s
- Encrypted throughput (AES-CCM): 800 Mb/s
- PoE+ ports: 4
- Maximum power consumption: 126 W

OmniAccess 4308

- Maximum LAN-connected APs: 16
- Maximum remote APs: 16
- Maximum number of users: 256
- MAC addresses: 4096
- 10/100Base-T ports: 8
- 10/100/1000Base-T ports: 1 (on T model)
- Gigabit SFP ports: 1 (on SX model)
- ExpressCard® Technology slot: No
- Form factor/footprint: 1 RU
- Active firewall sessions: 64,000
- Concurrent IPSec tunnels: 256
- Firewall throughput: 1 Gb/s
- Encrypted throughput (3DES, AESCBC256): 200 Mb/s
- Encrypted throughput (AES-CCM): 200 Mb/s
- PoE ports: 8
- Serial over Ethernet (SoE): Yes
- Maximum power consumption: 200 W

OmniAccess 4324

- Maximum LAN-connected APs: 48
- Maximum remote APs: 48
- Maximum number of users: 768
- MAC addresses: 4096
- 10/100Base-T ports: 24
- 10/100/1000Base-T ports: 0
- Gigabit SFP ports: 2
- Form factor/footprint: 1 RU
- Active firewall sessions: 64,000
- Concurrent IPSec tunnels: 768
- Firewall throughput: 2 Gb/s
- Encrypted throughput (3DES, AESCBC256): 400 Mb/s
- Encrypted throughput (AES-CCM): 400 Mb/s
- PoE ports: 24
- SoE: Yes
- Maximum power consumption: 300 W

OmniAccess 4504

- Maximum LAN-connected APs: 32
- Maximum remote APs: 128
- Maximum number of users: 512
- MAC addresses: 64,000
- Gigabit combo ports: 4
- Form factor/footprint: 1 RU
- Active firewall sessions: 128,000
- Concurrent IPSec tunnels: 512
- Firewall throughput: 3 Gb/s
- Encrypted throughput (3DES, AESCBC256): 1.6 Gb/s
- Encrypted throughput (AES-CCM): 800 Mb/s
- Maximum power consumption: 35 W

OmniAccess 4604

- Maximum LAN-connected APs: 64
- Maximum remote APs: 256
- Maximum number of users: 1024
- MAC addresses: 64,000
- Gigabit combo ports: 4
- Form factor/footprint: 1 RU
- Active firewall sessions: 128,000
- Concurrent IPSec tunnels: 1024
- Firewall throughput: 4 Gb/s
- Encrypted throughput (3DES, AESCBC256): 4 Gb/s
- Encrypted throughput (AES-CCM): 2 Gb/s
- Maximum power consumption: 45 W

OmniAccess 4704

- Maximum LAN-connected APs: 128
- Maximum remote APs: 512
- Maximum number of users: 2048
- MAC addresses: 64,000
- Gigabit combo ports: 4
- Form factor/footprint: 1 RU
- Active firewall sessions: 128,000
- Concurrent IPSec tunnels: 2048
- Firewall throughput: 4 Gb/s
- Encrypted throughput (3DES, AESCBC256): 8 Gb/s
- Encrypted throughput (AES-CCM): 4 Gb/s
- Maximum power consumption: 60 W

All OmniAccess WLAN switches

- Operating temperature: 0°C to 40°C (32°F to 104°F)
- Storage temperature: -40°C to +70°C (-40°F to +158°F)
- Humidity: Non-condensing 5% to 95%
- Encryption types: WER, TKIP, DES, AES-CCMP, 3DES, AES-CBC, xSec
- Authentication types: WPA-Enterprise, WPA-PSK, WPA2-Enterprise, WPA2-PSK, 802.1x, MAC address, captive portal
- Management capabilities: SNMP, Web, CLI using SSH, Telnet and console port

OmniAccess Access Points


OmniAccess AP85


OmniAccess AP70


OmniAccess AP61


OmniAccess AP125

The **Alcatel-Lucent OmniAccess™ family of wireless access points** (APs) are designed to support the varying requirements of mobile enterprise networks from large campuses to small branch offices. The APs aggregate wireless user traffic onto the enterprise network and direct this traffic to OmniAccess WLAN switches.

The OmniAccess wireless APs are offered in both indoor and outdoor models, with dual and single radio configurations. This broad portfolio of APs addresses the needs of a wide array of environments including:

- → Indoor and outdoor dual radio deployments
- → Indoor single radio deployments
- → Challenging radio frequency (RF) indoor deployments
- → Ceiling deployments
- → Workspace deployments
- → Telecommuter deployments
- → Harsh environment/factory floor deployments
- → Secure outdoor wireless bridging deployments

KEY SELLING POINTS

- → Multifunction APs providing simultaneously WLAN access, air monitoring, and wireless intrusion detection and prevention
- → Multipurpose APs with the ability to support remote AP operation or mesh AP operation
- → High-speed wireless with up to 300 Mb/s of throughput per radio on the OmniAccess AP120 series
- → IEEE 802.3af powered
- → High availability with dual Ethernet ports on the OmniAccess AP70 and OmniAccess AP120 series
- → Support for antenna diversity for enhanced antenna sensitivity
- → Flexible mounting options with support for wall, ceiling and plenum deployments

KEY FEATURES

- → IEEE 802.11a, 802.11b and 802.11g support
- → IEEE 802.11n support (OmniAccess AP120 series)
- → Software upgrade to 802.11n for the OmniAccess 12x abg series

- → RP-SMA antenna interfaces supported on OmniAccess AP60, OmniAccess AP70, OmniAccess AP120 and OmniAccess AP124
- → Quad N-Type female antenna interfaces supported on OmniAccess AP85 series
- → 10/100 Base-TX (RJ-45) auto-sensing Ethernet interface(s) with support for Power-over-Ethernet (PoE) (802.3af) and Serial-over-Ethernet (SoE) (OmniAccess AP60/61, OmniAccess AP65, OmniAccess AP70 and OmniAccess AP85TX)
- → Dual 10/100/1000Base-T (RJ-45) auto-sensing Ethernet interfaces with support for IEEE 802.3af PoE or 802.3at, PoE + (OmniAccess AP12x series)
- → DC power connector for external (optional) country-specific AC adapter kits

TECHNICAL INFORMATION

Operating mode

- Multiservice WLAN AP
  - ¬ 802.11a or 802.11b/g (OmniAccess AP60/61, OmniAccess AP120abg/121abg)
  - ¬ Concurrent 802.11a + b/g (OmniAccess AP65, OmniAccess AP70, OmniAccess AP85, OmniAccess AP124abg/125abg)
  - ¬ 802.11a/n or 802.11b/g/n (OmniAccess AP120/121)
  - ¬ Concurrent 802.11a/n + b/g/n (OmniAccess AP124/125)
- Air Monitor
- Hybrid combination of AP/Air Monitor
- Remote AP
- Mesh AP

RF management

- Automatic transmit power and channel management control with auto coverage hole correction via Adaptive Radio Management (ARM)

Advanced features

- Wi-Fi multimedia (WMM) QoS
- 802.1p and DSCP to WMM AC tagging
- Upstream traffic prioritization/priority queuing
- Call admission control (CAC)
- Traffic classification/session bandwidth reservation (T-SPEC/TCLAS)
- Unscheduled Automatic Power Save Delivery (U-APSD)
- Stateful session awareness (soft voice client QoS)
  - ¬ SIP
  - ¬ Alcatel-Lucent NOE
  - ¬ Cisco Skinny
  - ¬ Vocera
- Spectralink Voice Prioritization (SVP)
- Support for Proxy-ARP and multicast filtering

Wireless radio specifications

(common to all APs)

- Supported frequency bands (country-specific restrictions apply)
  - ¬ 2.400 GHz to 2.4835 GHz
  - ¬ 5.150 GHz to 5.250 GHz
  - ¬ 5.250 GHz to 5.350 GHz
  - ¬ 5.470 GHz to 5.725 GHz
  - ¬ 5.725 GHz to 5.850 GHz
- Available channels: WLAN switch-managed, dependent on configured regulatory domain
- Modulations
  - ¬ 802.11b: Direct-Sequence Spread-Spectrum (DSSS)
  - ¬ 802.11a/g: Orthogonal Frequency Division Multiplexing (OFDM)
- Transmit power: Configurable in increments of 0.5 dBm
- Association rates (Mb/s)
  - ¬ 802.11b: 11, 5.5, 2, 1 with automatic fallback
  - ¬ 802.11a/g: 54, 48, 36, 24, 18, 12, 9, 6 with automatic fallback

802.11n wireless radio specifications

(OmniAccess AP120/AP121/ AP124/AP125 only)

- AP type: 3 x 3 Multiple-In, Multiple-Out (MIMO)
- Modulations
  - ¬ 802.11b: DSSS
  - ¬ 802.11a/g: OFDM
  - ¬ 802.11n: 802.11n draft 2.0
- Association rates (Mb/s)
  - ¬ 802.11n: MCS0 to MCS15 (6.5 Mb/s to 300 Mb/s)
- 802.11n High-Throughput (HT) support: HT 20/40
- 802.11n Packet Aggregation: A-MPDU, A-MSDU

Antenna

OmniAccess AP60

- Dual, RP-SMA interfaces for external antenna support (supports spatial diversity)

OmniAccess AP61

- Integral antennas
  - ¬ Dual, omni-directional multi-band dipole (supports spatial diversity)
  - ¬ Antenna max gain
    - – 2.4 GHz to 2.5 GHz: 2.8 dBi
    - – 5.150 GHz to 5.350 GHz: 3.9 dBi
    - – 5.950 GHz: 4.0 dBi

OmniAccess AP65

- Integral antennas
  - ¬ Dual, omni-directional multi-band dipole (supports spatial diversity)
  - ¬ Antenna max gain
    - – 2.4 GHz to 2.5 GHz: 3.3 dBi
    - – 5.150 GHz to 5.250 GHz: 3.19 dBi
    - – 5.350 GHz: 3.53 dBi
    - – 5.470 GHz: 3.69 dBi
    - – 5.875 GHz: 3.90 dBi

OmniAccess AP70

- Quad, RP-SMA interfaces (2 per radio) for external antennas and Integral antennas
  - ¬ Dual, omni-directional multi-band dipole (supports spatial diversity)
  - ¬ Gain
    - – 2.4 GHz to 2.5 GHz: 4.46 dBi
    - – 5.150 GHz: 7.21 dBi
    - – 5.350 GHz: 6.49 dBi
    - – 5.850 GHz: 5.23 dBi

OmniAccess AP85TX/FX/LX

- Quad, N-type female interfaces (2 per radio) for external antenna support (supports spatial diversity)

OmniAccess AP120/AP120abg/ AP124/AP124abg:

- Three RP-SMA interfaces for external antenna support (supports up to 3 x 3 MIMO with spatial diversity)

OmniAccess AP121/AP121abg/ AP125/AP125abg

- Integral antennas
  - ¬ Tri, omni-directional multi-band dipole antenna elements (supports up to 3 x 3 MIMO with spatial diversity)
  - ¬ Antenna max gain
    - – 2.4 GHz to 2.5 GHz: 3.2 dBi
    - – 5.150 GHz to 5.875 GHz: 5.2 dBi

Interfaces

OmniAccess AP60/AP61/AP65

- 1 x 10/100Base-T Ethernet (RJ-45), auto-sensing link speed and MDI/ MDX (with PoE and SoE capability)

OmniAccess AP70

- 2 x 10/100Base-T Ethernet (RJ-45), auto-sensing link speed and MDI/ MDX (with PoE and SoE capability) and 1 x USB

OmniAccess AP85TX

- 1 x 10/100Base-T Ethernet (RJ-45), auto-sensing link speed and MDI/ MDX (with PoE and SoE capability)

OmniAccess AP85FX

- 1 x 100Base-FX multi-mode, 1310 nm wavelength dual-fiber LC interface (2 km reach) and console interface

OmniAccess AP85LX

- 1 x 100Base-LX single-mode, 1310 nm wavelength dual-fiber LC interface (10 km reach) and console interface

OmniAccess AP12x series

- 2 x 100/1000Base-T Ethernet (RJ-45), auto-sensing link speed and MDI/ MDX (with PoE capability) and 1 x RJ-45 console interface

Power

OmniAccess AP60/61

- 48 V DC 802.3af PoE
- 5 V/1.5 A DC power interface

OmniAccess AP65

- 48 V DC 802.3af PoE
- 5 V/2 A DC power interface

OmniAccess AP70

- 48 V DC 802.3af PoE
- 5 V/2.5 A DC power interface

OmniAccess AP85TX

- 48 V DC 802.3af PoE
- 12 V DC for external solar supplied power (maximum power draw 9.6 W at 12 V DC)

OmniAccess AP85FX/LX

- 1 x 12 V DC up to 2.0 A (for external DC solar-supplied power)
- 1 x 90 V to 288 V AC/500 mA auto-sensing power interface with transient surge suppression

OmniAccess AP120/121

- 48 V DC 802.3af
- 5 V DC/2.4 A DC power interface

OmniAccess AP124/125

- 48 V DC 802.3af or 802.3at or PoE+
- 5 V DC/3.2 A DC power interface

Operating temperatures

- OmniAccess AP60/61, OmniAccess AP65, OmniAccess AP70, OmniAccess AP12x series: 0°C to 50°C (32°F to 122°F)
- OmniAccess AP85TX/FX/LX: -30°C to +55°C (-22°F to +131°F)

Regulatory

OmniAccess AP60/61, OmniAccess AP65, OmniAccess AP70

- FCC Part 15
- Industry Canada
- VCCI
- MIC
- PSE mark – adapters/cords
- Anatel
- NOM/COFETEL
- SRRC
- GS Mark
- CE Mark
- R&TTE Directive – 1995/5/EC
- Low Voltage Directive – 72/23/EEC
- EN 300 328
- EN 301 893
- EN 301 489
- UL/IEC/EN 60950-1:2001 CB, cULus
- AS/NZS 4268, 4771
- Medical EN 60601-1, -2
- UL2043 Listed

OmniAccess AP85 series

- FCC Part 15
- Industry Canada
- VCCI
- MIC
- Anatel
- NOM/COFETEL
- SRRC
- GS Mark
- CE Mark
- R&TTE Directive – 1995/5/EC
- Low Voltage Directive – 72/23/EEC
- EN 300 328
- EN 301 893
- EN 301 489
- UL/IEC/EN 60950-1:2001
- CB, cULus
- AS/NZS 4268, 4771
- ATEX Zone 2
- IEC 60529 IP68

OmniAccess AP12x series

- FCC Part 15
- Industry Canada
- MIC
- Anatel
- NOM/COFETEL
- SRRC/CCC
- GS Mark
- CE Mark
- R&TTE Directive – 1995/5/EC
- Low Voltage Directive – 72/23/EEC
- EN 300 328
- EN 301 893
- EN 301 489
- UL/IEC/EN 60950-1:2001
- CB, cULus
- AS/NZS 4268, 4771
- UL2043-compliant

OmniAccess 700

OmniAccess 780

OmniAccess 740

The **Alcatel-Lucent OmniAccess™ 700[1] Unified Services Gateway** (USG) family of routers integrate enterprise security, core networking technologies and adaptive services into a single, highly available system for branch office networking.

The OmniAccess 700 USG family of routers are multiservice networking devices designed to reduce the cost and complexity of managing branch office networks. The OmniAccess 700 USG product family consolidates multiple hardware and software networking solutions typically required for a branch site, and delivers switching and routing, various WAN connectivity (legacy T1/E1, IP, serial), remote management, unparalleled serviceability, VoIP, and security functionality in an easy-to-manage platform.

[1] The OmniAccess 740 and 780, now called OmniAccess 5740/5780 respectively, are still referred to as OA740 and OA780 in the price list, on product labels, and in certification documents.

The Alcatel-Lucent OmniAccess 780 USG has six interface slots and the Alcatel-Lucent OmniAccess 740 USG has two interface slots. Both platforms support a selection of interface modules such as 10/100/1000 Ethernet layer 2, T1, E1, and serial synchronous (V.35, X.21, TIA/EIA-232).

Typical deployment solutions that benefit from the versatile OmniAccess 700 USG router family are:

- → Converged medium and large branch offices
- → Aggregation of multiple branch sites that have differing WAN connectivity
- → Multi-T1 (or serial links) Internet access and corporate Frame Relay
- → Head office location for smaller organizations

KEY SELLING POINTS

- → **Purpose built:** Software and hardware architecture specifically designed to provide a rich and extensive suite of features and services that branch offices require
- → **Modular:** Leverages a highly modular design that allows the addition of new services on an as-needed basis
- → **Enhances uptime:** The Alcatel-Lucent ModuLive operating system enables in-service upgrades and configuration changes to ensure that a fault in one service causes minimal or no disruption to other services

- **Efficient:** Provides true service unification, saves CPU resources, minimizes latency through the system, and unifies VoIP functionality with low latency and high-throughput performance with minimal packet loss
- **High availability:** Regardless of the state of the system, remote system administration can repair a majority of network issues, eliminating the need for on-site intervention
- **Redundancy:** Remote office Voice Resiliency (RoVR) enables redundancy at multiple levels (call server, Virtual Router Redundancy Protocol (VRRP), WAN links) to provide always-on voice functionality for small branches
- **Privacy and security:** Maintains separate routing and forwarding tables to extend the privacy and security of an MPLS VPN down to the customer edge (CE), (that is, small branches), enabling a cheaper, future-proof and secure multi-VPN virtual routing and forwarding (VRF) (multi-VPN VRF CE) solution
- **Enhanced security:** Security-first architecture delivers a comprehensive set of security features such as stateful firewall, VPN and intrusion detection system/intrusion prevention system (IDS/IPS)
- **Open platform:** Enables the integration of customer and partner applications as needed

KEY FEATURES

- **Unified services and features:** Consolidation of multiple services and protocols such as LAN switching, WAN routing, firewall, VPNs, IDS/IPS, and VoIP on a single system that is managed by a unified network management interface
- **Flexible and expandable:** Choice of two modular platforms (six-slot chassis and two-slot chassis) that support a selection of interface modules such as 10/100/1000 Ethernet layer 2, T1, E1, and serial synchronous (V.35, X.21, TIA/EIA-232)
- **Modular software design:** Alcatel-Lucent ModuLive operating system enhances mission-critical application delivery and insulates the system to prevent failure of any one service
- **Single-pass packet processing:** Alcatel-Lucent OnePass provides global classification of packets for all services down to an application's payload level
- **Redundancy:** The Alcatel-Lucent LifeLine management framework embeds dedicated management processors in each line card to enable an N+1 redundant architecture and multiple access mechanisms to reach the system
- **Unified VoIP services with survivability:** Call admission control (CAC), advanced QoS, differentiated services code point (DSCP) classification and marking, Session Initiation Protocol (SIP) and New Office Environment (NoE) application layer gateway (ALG), RoVR

- → **SIP proxy:** Local and PSTN call routing during WAN link outage
- → **Robust routing services:** VRRP, Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), generic routing encapsulation (GRE), Internet Group Management Protocol (IGMP), Protocol Independent Multicast (PIM), Policy-based Routing (PBR), Multi-VPN VRF CE
- → **Advanced security services:** Stateful firewall, network address translation (NAT), destination network address translation (DNAT), IPSec VPN, IDS/IPS, distributed denial of service (DDoS) protection
- → **Software Application Service Engine (ASE):** Server-on-a-stick architecture provides secure third-party application support with common management
- → **High availability and resiliency:** Supports on-line insertion and removal (OIR) for various modules

TECHNICAL INFORMATION

Hardware

- OmniAccess 780 USG – Modular chassis with six interface slots
- OmniAccess 740 USG – Modular chassis with two interface slots
- Interface cards:
  - ¬ 8-port 10/100/1000 Mb/s Ethernet
  - ¬ 4-port T1/E1
  - ¬ 4-port serial (V.35, X.21, TIA/EIA-232)
- Core processor: Services engine (SE) with two ports 10/100/1000 Mb/s Ethernet built-in
- Hot-swappable line cards
- RAM (default/max): 512 MB/1 GB
- Flash memory: 512 MB
- IPv6-ready hardware

T1/E1 specification overview

- T1/E1 or fractional T1/E1 network interfaces
- Interface connectors: Four 100-ohm RJ-48C connectors
- Data rates:
  - ¬ Non-channelized T1/E1, up to 2 Mb/s
  - ¬ Channelized T1/E1, up to 24 and 32 x 64 kb/s respectively
- Maximum transmission unit (MTU): 1500 bytes
- High-Level Data Link Control (HDLC), Point-to-Point Protocol (PPP) and Frame Relay encapsulation, Multilink PPP (MLPPP) and Multilink Frame Relay (MLFR)
- Fully manageable through CLI, HTTP and Simple Network Management Protocol (SNMP)

T1 interface

- Transmit bit rate: 1.544 Mb/s +/-32 ppm
- Receive bit rate: 1.544 Mb/s +/-32 ppm
- Line code: alternate mark inversion (AMI), Bipolar Eight Zero Substitution (B8ZS)
- Framing format: D4 super frame (SF) and extended super frame (ESF)
- Output level line build-out (LBO): 0 dB, -7.5 dB, -15 dB, -22.5 dB
- Data terminal equipment (DTE)/data communication equipment (DCE) interface: ITU T G.704/structured or fractional service

E1 interface

- Transmit bit rate: 2.048 Mb/s +/-50 ppm
- Receive bit rate: 2.048 Mb/s +/-50 ppm
- Data rate: 1.984 Mb/s (framed mode)
- Line code: High Density Bipolar 3 (HDB3), AMI
- Framing format: CRC4, non-CRC4
- Output level: Short haul/long haul
- DTE/DCE interface: ITU-T G.704/ structured or fractional service, G.703

Channel service unit (CSU)/ data service unit (DSU)

- Selectable cable length: 0 ft to 110 ft, 110 ft to 220 ft, 220 ft to 330 ft, 330 ft, 440 ft to 550 ft, 550 ft to 660 ft
- CSU LBO: 0 dB, -7.5 dB, -15 dB, -22.5 dB
- CSU receive signal level: 0 dB to -36 dB

Diagnostics

- Digital diagnostic loopback
- Payload loopback
- Line loopback
- Red, yellow and alarm indication signal (AIS)
- Transmission of AIS and yellow alarm signal

LEDs

- Active – green/off
- Fault – red/off
- LA (local alarm) – amber/off
- RA (remote alarm) – amber/off
- CD (carrier detect) – green/off
- LB (loopback) – green/off

Routing

- Static routes
- RIP v1/v2 dynamic routing
- OSPF/BGP dynamic routing
- 64,000 total routes per system
- Multicast routing – PIM
- IGMP (v1, v2)
- GRE tunnels
- VRRP
- Policy-based routing
- Multi-VRF CE
- 32 VRF instances per system
- Number of routes per instance: No limit, only total number of routes limit in system applies
- RFC 3021 support – 31-bit mask
- Packet forward rate (64-byte packets): 930 kp/s
- Forwarding performance: 2 Gb/s
- Maximum number of BGP peers: 200
- Maximum number of virtual local area networks (VLANs): 4096

Firewall

- Stateful packet inspection and filtering access control list (ACL)
- NAT (source and destination NAT)
- Denial of service (DoS) and DDoS protection
- Protocol anomaly: IP, Transmission Control Protocol (TCP), User Datagram Protocol (UDP)
- ALGs: Trivial File Transfer Protocol (TFTP), FTP, Network File System (NFS), Domain Name Service (DNS), Real Time Streaming Protocol (RTSP), SIP, Dynamic Host Configuration Protocol (DHCP), NOE
- Common classification for all services
- Firewall performance: 2 Gb/s
- Concurrent sessions: 128,000

QoS

- QoS on bundled interfaces (MLFR, MLPPP)
- QoS on sub-interfaces (per-PVC QoS)
- Auto QoS configuration for 802.1p L3/4 traffic policy definition, voice
- Interface egress queues: 16 queues per interface
- Priority scheduling
- Weighted fair queuing
- Class-based queuing
- Hierarchical queuing: Up to four levels
- Ingress policing
- Egress shaping
- DSCP/type of service (TOS) marking
- Weighted Random Early Detection (WRED)
- Differentiated Services (DiffServ): RFC 3246, 2597, 2445
- 802.1p Classification and Marking
- 802.1Q Classification

VPN (IPSec)

- Site-to-site VPN tunnels: Up to 15,003
- Tunnel interfaces
- DES (56-bit), 3DES (168-bit), and AES (128-bit, 192-bit, 256-bit) encryptions
- Message-Digest Algorithm 5 (MD5) and Secure Hash Algorithm 1 (SHA-1) authentication
- Internet key exchange (IKE) with pre-shared key or public key infrastructure (PKI)
- Perfect forward secrecy (DH groups): 1, 2, 5
- IP Security (IPSec) NAT traversal
- AES performance: 180 Mb/s
- Maximum concurrent VPN tunnels: 1500

IDS/IPS

- Detection mode
- Prevention mode
- Automatic signature updates
- Group-based IDS/IPS: Priority/protocol/intrusion type

WAN protocols

- PPP
- MLPPP
- Frame Relay support with FRF.12 fragmentation
- MLFR
- Link Frame Interleaving (LFI) (Frame Relay and MLPPP)
- HDLC
- Password Authentication Protocol (PAP)/Challenge Handshake Authentication Protocol (CHAP) authentication
- Point-to-Point Protocol over Ethernet (PPPoE) client support
- DSL interface via external DSL modem LAN protocols
- Spanning Tree Protocol (STP)
- Bridging
- IEEE 802.1Q VLANs
- Per-VLAN STP (PVST+)
- Integrated Routing and Bridging (IRB)

Network services

- DHCP relay/server
- DNS client
- TFTP server/client
- FTP client
- Secure Shell (SSH) server/client
- HTTP server
- Transparent firewall

VoIP

- SIP ALGs
- Priority scheduling
- Dynamic Pinholing in firewall
- DSCP classification and marking
- TFTP server for booting IP phones
- DHCP options for phones provisioning
- LFI support for reducing jitter and delay

CAC support for VoIP calls

- Busy signal to over-the-limit call attempt
- Static configuration of number of calls limit per interface or link
- Automatic management of allowed number of calls based on dynamic bandwidth utilization measurement and link capacity

VoIP security

- ALG support for voice signaling and supporting protocols
- Protection against attacks: DDoS, IP spoofing, stateful inspection, packet assembler/disassembler (PAD)

RoVR

- SIP proxy: Local and PSTN call routing during WAN link outage
- PSTN fallback via external media gateway (Mediatrix, AudioCodes)
  - ¬ 5-call server support
  - ¬ Call features in RoVR mode
  - ¬ Call routing
  - ¬ Call forward
  - ¬ Call hold/resume
  - ¬ Transfer
  - ¬ Conference
  - ¬ Don't disturb
  - ¬ Call waiting
  - ¬ Caller ID information on call waiting
  - ¬ Caller ID/caller ID blocking
  - ¬ ROVR mode notification to User Agent
  - ¬ Special dial tone in RoVR mode

System management

- Alcatel-Lucent OmniVista™ management enhanced support
- Initial Alcatel-Lucent 5620 Service Aware Manager (SAM) integration support
- CLI (console, USB, backup modem, Telnet, SSH)
- Web user interface (HTTP, HTTPS)
- SNMP (v1,v2, v3)
- Local administrator database
- AAA – RADIUS, TACACS+
- Syslog forwarding: External, up to four servers

- Standard and custom MIBs
- Ping, traceroute
- Hitless component upgrades via Alcatel-Lucent ModuLive software platform
- Management plane for Alcatel-Lucent Lifeline framework
- License Manager
- GUI wizards for complex configurations
  - ¬ Advanced QoS configuration GUI wizard
  - ¬ Firewall configuration wizard
  - ¬ IPSec configuration wizard
  - ¬ Universal serial interface configuration GUI
  - ¬ MLPPP/Frame Relay configuration GUI
  - ¬ VRF configuration GUI

OmniAccess 780 USG

Dimensions

- Height: 13.34 cm (5.25 in.)
- Width: 44.45 cm (17.5 in.)
- Depth: 43.18 cm (17 in.)
- Weight: 22.7 kg (50 lb) fully configured
- Rack-mountable: 19-inch standard

Power

- Power supply: 100 V AC to 240 V AC, 400 W per supply, 4 A
- Power consumption: Max 400 W
- Redundant power supply support

OmniAccess 740 USG

Dimensions

- Height: 4.45 cm (1.75 in.)
- Width: 44.45 cm (17.5 in.)
- Depth: 43.18 cm (17 in.)
- Weight: 12.8 kg (25 lb) fully configured
- Rack-mountable: 19-in. standard

Power

- Power supply: 100 V AC to 240 V AC, 250 W per supply, 3 A
- Power consumption: Max 250 W

Environment

- Operating temperature: 0°C to 45°C (32°F to 113°F)
- Non-operating temperature: -25°C to +70°C (-13°F to +158°F)
- Operating humidity: 10% to 90% (non-condensing)
- Operating altitude: 3048 m (10,000 ft)
- Non-operating altitude: 4572 m (15,000 ft)

Certifications/ agency approvals

Networking

- 47, CFR Part 68 and ACTA adopted technical criteria
- CS 03 Issue 8, Part II
- TBR 12 and 13
- AS/ACTF S016: 2001
- T1 (DS1) JATE – 1.544 Mb/s digital interface
- E1 JATE – 2.048 Mb/s digital interface

EMC

- FCC Part 15, Subpart A
- ICES 003
- EN 55022:1998/A1:2000
- AS/NZS 3548: 1995+A1: 1997 +A2: 1997
- VCCI V-3/2000.04

Regulatory compliance

- FCC Part 15 Class A
- FCC Part 68, TIA-968-A-2
- CS-03 Issue 8, Part II
- TBR 12, TBR 13
- [FCC# 6TGUSA-46505_DE-N]

Safety

- US (UL 60950-1: 2003, First Ed.)
- Canada (CSA 22.2 No. 60950-1-03 First Ed.)
- Europe (EN 60950)
- Other countries (IEC 60950, CB Scheme)

Telecommunications standards

- ITU-T G.703, G.704
- ANSI T1.102, T1.403
- AT&T Publication 62411

IEEE standards

- IEEE 802.1D 2004 (STP)
- IEEE 802.1X (Port-based Network Access Control)

- IEEE 802.1x (EAP)
- IEEE 802.1Q (Tagging)
- IEEE 802.2 (Logical Link Control)
- IEEE 802.3 (Carrier Sense Multiple Access with Collision Detection – Ethernet CSMA-CD)
- IEEE 802.3ab (1000Base-T)
- IEEE 802.3i (10Base-T)
- IEEE 802.3u (100Base-T)
- IEEE 802.3z (1000Base-X)

IETF RFCs

- RFC 768 UDP
- RFC 783 TFTP rev2
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 854 Telnet
- RFC 919 IP Bcast
- RFC 959 FTP
- RFC 966 Host groups, A Multicast Extension to the Internet Protocol
- RFC 1042 A Standard for the Transmission of IP Datagrams over IEEE 802 Networks
- RFC 1054 Host Extensions for IP Multicasting
- RFC 1058 RIP
- RFC 1105 Border Gateway Protocol (BGP)
- RFC 1112 Host Extensions for IP Multicasting
- RFC 1131 OSPF Specification
- RFC 1157 SNMP v1
- RFC 1163 Border Gateway Protocol (BGP)
- RFC 1166 Internet Numbers
- RFC 1191 Path MTU Discovery
- RFC 1234 PPP Authentication Protocols
- RFC 1247 OSPF v2
- RFC 1305 NTPv3
- RFC 1315 MIB for FR DTE
- RFC 1332 PPP IPCP
- RFC 1334 PPP Authentication PAP
- RFC 1350 TFTP rev2
- RFC 1364 BGP OSPF Interaction
- RFC 1397 Default Route Advertisement in BGP2 and BGP3 Versions of the Border Gateway Protocol
- RFC 1403 BGP OSPF Interaction
- RFC 1519 CIDR
- RFC 1583 OSPF v2
- RFC 1586 OSPF over FR
- RFC 1587 OSPF NSSA option
- RFC 1618 PPP over ISDN
- RFC 1654 BGP-4
- RFC 1657 Definitions of Managed Objects for BGP-4 using SMIv2
- RFC 1661 Point-to-Point Protocol (PPP)
- RFC 1662 PPP in HDLC-like Framing
- RFC 1701 GRE
- RFC 1702 Generic Routing Encapsulation over IPv4 networks
- RFC 1721 RIP Version 2 Protocol Analysis
- RFC 1722 RIP Version 2 Protocol Applicability Statement
- RFC 1745 BGP4/IDRP for IP – OSPF Interaction
- RFC 1765 OSPF Database Overflow
- RFC 1771 BGP-4
- RFC 1812 Requirements for IPv4 Routers
- RFC 1817 CIDR and Classful Routing
- RFC 1853 IP in IP Tunneling
- RFC 1858 Security Considerations for IP Fragment Filtering
- RFC 1878 Variable Length Subnet Table for IPv4 (VLSM)
- RFC 1907 SNMP v2 Management Information Base
- RFC 1965 Autonomous Confederations for BGP
- RFC 1990 The PPP Multilink Protocol (MP)
- RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
- RFC 1997 BGP Communities Attribute
- RFC 2082 RIP-2 MD5 Authentication
- RFC 2096 IP Forwarding Table MIB
- RFC 2117 Protocol Independent Multicast-Sparse Mode (PIM-SM)
- RFC 2131 Dynamic Host Configuration Protocol (DHCP)
- RFC 2178 OSPF v2
- RFC 2236 IGMPv2
- RFC 2283 Multiprotocol Extensions for BGP-4
- RFC 2328 OSFPv2
- RFC 2338 VRRP (IP v4)
- RFC 2362 PIM-SM Protocol Specification
- RFC 2367 PF_KEY Key Management API, Version 2
- RFC 2370 OSPF v2 Opaque LSA Option
- RFC 2401 Security Architecture for the Internet Protocol

- RFC 2402 IP Authentication Header
- RFC 2406 IP Encapsulating Security Payload (ESP)
- RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408 Internet Security Association and Key Management Protocol
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 2411 IP Security Document Roadmap
- RFC 2412 OAKLEY Key Determination Protocol
- RFC 2427 Multiprotocol Interconnect over Frame Relay
- RFC 2439 BGP Route Flap Damping
- RFC 2453 RIPv2
- RFC 2474 DiffServ Precedence
- RFC 2571 An Architecture for Describing SNMP Management Frameworks
- RFC 2573 SNMP Applications
- RFC 2574 SNMP v3 User-based Security Model
- RFC 2575 View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
- RFC 2578 Structure of Management Information Version 2 (SMIv2)
- RFC 2579 Textual Conventions for SMIv2
- RFC 2580 Conformance Statements for SMIv2
- RFC 2597 DiffServ Expedited Forwarding (EF)
- RFC 2598 DiffServc Assured Forwarding (AF)
- RFC 2784 Generic Routing Encapsulation (GRE)
- RFC 2796 BGP Route Reflection: An Alternative to full mesh IBGP
- RFC 2842 Capabilities Advertisement with BGP-4
- RFC 2858 Multiprotocol Extensions to BGP-4
- RFC 2863 The Interfaces Group MIB
- RFC 2890 Key and Sequence Number Extensions to GRE
- RFC 2908 The Internet Multicast Address Allocation Architecture
- RFC 2918 Route Refresh Capability for BGP-4
- RFC 3065 Autonomous Confederations for BGP
- RFC 3101 OSPF NSSA option
- RFC 3137 OSPF Stub Router Advertisement
- RFC 3164 BSD Syslog Protocol
- RFC 3246 An Expedited Forwarding PBH
- RFC 3392 Capabilities Advertisement with BGP-4
- RFC 3410 Introduction and Applicability Statement for Internet Standard Management Framework
- RFC 3411 Architecture for Describing SNMP Management
- RFC 3416 SNMP v2 Protocol Operations
- RFC 3417 SNMP v2 Transport Mappings
- RFC 3418 SNMP v2 Management Information Base
- RFC 3509 OSPF Alternative Implementations
- RFC 3706 A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3715 IPSec-Network Address Translation (NAT) Compatibility Requirements
- RFC 3748 PPP Extensible Authentication Protocol (EAP)
- RFC 3768 VRRP (IP v4)
- RFC 3947 Negotiation of NAT-Traversal in the IKE
- RFC 3948 UDP Encapsulation of IPSec ESP Packets
- RFC 4302 IP Authentication Header
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 4456 BGP Route Reflection: An Alternative to full mesh IBGP
- RFC 4601 PIM-SM Protocol Specification (Revised)
- RFC 4632 CIDR Internet Address Assignment & Aggregation Plan
- RFC 4760 Multiprotocol Extensions to BGP-4
- RFC 4835 Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)

OmniAccess 5510

OmniAccess 5510-TE

OmniAccess 5510-SR

The **Alcatel-Lucent OmniAccess™ 5510 Unified Services Gateway** (USG) router is a compact and affordable, purpose-built platform for secure, wire-speed delivery of voice and data services to small offices. It has been specifically designed to meet the requirements of small and medium-sized businesses (SMBs), small enterprise branch offices and carrier-provided managed services applications for simultaneous delivery of secure voice and data services. This cost-effective platform provides consistent wire-speed throughput with no degradation in performance, even when multiple services are enabled.

The OmniAccess 5510 USG comprises a range of fixed-configuration models that provide secure data connectivity for T1/E1, serial and xDSL WAN interfaces. Each model comes with four 10/100 switched Ethernet RJ-45 ports and one 10/100 RJ-45 Ethernet expansion port. It supports built-in hardware VPN encryption that enhances VPN encryption performance.

Typical deployment solutions that will benefit from the versatile OmniAccess 5510 USG router are:

- All-in-one secure WAN connectivity/access for SMBs
- Unified networking services for small enterprise branch offices
- Carrier-provided managed services applications
- Basic Internet connectivity or secure VPN communications

KEY SELLING POINTS

- **Flexible configuration:** Different models with a variety of WAN connectivity options enable customer to meet various deployment scenarios
- **Simple and easy deployment:** Rack-friendly and desktop-friendly options allow fast installation in a variety of enterprise environments
- **Simplifies the network:** Provides the same services and features as multiple devices in a single, resilient, low-cost, small footprint platform
- **Enhances uptime:** The Alcatel-Lucent ModuLive operating system enables in-service upgrades and configuration changes to ensure that a fault in one service causes minimal or no disruption to other services
- **Efficient:** Provides true service unification, saves CPU resources, minimizes latency through the system, and unifies VoIP

functionality with low latency, high-throughput performance with minimal packet loss

- **Redundancy:** Remote office Voice Resiliency (RoVR) enables redundancy at multiple levels (call server, Virtual Router Redundancy Protocol (VRRP), WAN links) to provide always-on voice functionality for small branches
- **Privacy and security:** Maintains separate routing and forwarding tables to extend the privacy and security of an MPLS VPN down to the customer edge (CE) (that is, small branches), enabling a cheaper, future-proof and secure multi-VPN virtual routing and forwarding (VRF) (Multi-VPN VRF CE) solution
- **Enhanced security:** Security-first architecture delivers a comprehensive set of security features such as stateful firewall, VPN and intrusion detection system/intrusion prevention system (IDS/IPS)
- **Environment friendly:** Low-power, fanless design consumes less power and makes it suitable for noise-sensitive environment

KEY FEATURES

- **Unmatched flexibility:** Choice of T1/E1, serial, ADSL (Annex A and B) WAN interface models
- **Streamlined form factor:** Choice of half-rack width or desktop deployment with fanless design provide a variety of deployment options
- **Flexible services:** Provides the same services and feature richness as high-end USG routers in a streamlined form factor
- **Modular software design:** Alcatel-Lucent ModuLive operating system enhances mission-critical application delivery and insulates the system to prevent failure of any one service
- **Single-pass packet processing:** Alcatel-Lucent OnePass provides global classification of packets for all services down to an application's payload level
- **Unified VoIP services survivability:** Call admission control (CAC), advanced quality of service (QoS), differentiated services code point (DSCP) classification and marking, Session Initiation Protocol (SIP) and New Office Environment (NoE) application layer gateway (ALG), RoVR
- **SIP proxy:** Local and PSTN call routing during WAN link outage
- **Robust routing services:** VRRP, Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), generic routing encapsulation (GRE), Internet Group Management Protocol (IGMP), Protocol Independent Multicast (PIM), Policy-based Routing (PBR), Multi-VPN VRF CE
- **Advanced security services:** Stateful firewall, network address translation (NAT), destination network address translation (DNAT), IPSec VPN, IDS/IPS, distributed denial of service (DDoS) protection

TECHNICAL INFORMATION

The Alcatel-Lucent OmniAccess 5510 USG offers fixed-configuration models with different WAN connectivity options.

- All models have integrated:
  - ¬ 4-port 10/100 Ethernet LAN switch
  - ¬ 1-port 10/100 Ethernet WAN/LAN expansion
  - ¬ 1 USB port
  - ¬ 1 console port
- All models have an external AC or DC power supply
- In addition there are various integrated WAN interfaces:
  - ¬ Model 5510-TE: One T1/E1 interface
  - ¬ Model 5510-SR: One Universal serial interface (X.21, V.35, TIA/EIA-232)
  - ¬ Model 5510-AA: One ADSL2+ interface, Annex A (ADSL over POTS)
  - ¬ Model 5510-AB: One ADSL2+ interface, Annex B (ADSL over ISDN)

Routing

- Static routes
- RIP v1/v2 dynamic routing
- OSPF/BGP dynamic routing
- Multicast routing – PIM
- IGMP (v1, v2)
- GRE tunnels
- VRRP
- PBR
- IPv6 routing-ready hardware

Multi-VRF CE

- 32 VRF instances per system
- Number of routes per instance: No limit, only total number of routes limit in system applies
- RFC 3021 support – 31-bit mask firewall
- Stateful packet inspection and filtering access control list (ACL)
- NAT (source and destination)
- Denial of service (DoS) and DDoS protection
- Protocol anomaly: IP, Transmission Control Protocol (TCP), User Datagram Protocol (UDP)
- ALGs: Trivial File Transfer Protocol (TFTP), FTP, Network File System (NFS), Domain Name Service (DNS), Real Time Streaming Protocol (RTSP), SIP, Dynamic Host Configuration Protocol (DHCP), NOE
- Common classification for all services

QoS

- QoS on bundled interfaces: Multilink Frame Relay (MLFR), Multilink Point-to-Point Protocol (MLPPP)
- QoS on sub-interfaces (per-PVC QoS)
- Auto QoS configuration for 802.1p L3/4 traffic policy definition, voice
- L3/4 traffic policy definition
- Interface egress queues: 16 queues per interface
- Priority scheduling
- Weighted fair queuing
- Class-based queuing
- Hierarchical queuing: Up to four levels
- Ingress policing
- Egress shaping
- DSCP/type of service (TOS) marking
- Weighted Random Early Detection (WRED)
- Differentiated Services (DiffServ): RFC 3246, 2597, 2445
- 802.1p Classification and Marking
- 802.1Q Classification

VPN (IPSec)

- Site-to-site VPN tunnels
- Tunnel interfaces
- DES (56-bit), 3DES (168-bit), and AES (128-bit, 192-bit, 256-bit) encryptions
- Message-Digest Algorithm 5 (MD5) and Secure Hash Algorithm (SHA-1) authentication
- Internet key exchange (IKE) with pre-shared key or public key infrastructure (PKI)
- Perfect forward secrecy (DH groups): 1, 2, 5
- IP Security (IPSec) NAT traversal

IDS/IPS

- Detection mode
- Prevention mode
- Automatic signature updates
- Group-based IDS/IPS: Priority/protocol/intrusion type

WAN protocols

- PPP
- Frame Relay with FRF.12 fragmentation
- Link Frame Interleaving (LFI) (Frame Relay and MLPPP)
- HDLC
- Password Authentication Protocol (PAP)/Challenge Handshake Authentication Protocol (CHAP) authentication
- Point-to-Point Protocol over Ethernet (PPPoE) client support

LAN protocols

- STP
- Bridging
- IEEE 802.1Q VLANs
- Integrated routing and bridging (IRB)

Network services

- DHCP relay/server
- DNS client
- TFTP server/client
- FTP client
- Secure Shell (SSH) server/client
- HTTP server
- Transparent firewall

VoIP support

- SIP ALGs
- Priority scheduling
- Dynamic Pinholing in firewall
- DSCP classification and marking
- TFTP server for booting IP phones
- DHCP options for phones provisioning

VoIP security

- ALG support for voice signaling and supporting protocols
- Protection against attacks: DDoS, IP spoofing, stateful inspection, packet assembler/disassembler (PAD)

CAC support for VoIP calls

- Busy signal to over-the-limit call attempt
- Static configuration of number of calls limit per interface or link
- Automatic management of allowed number of calls based on dynamic bandwidth utilization measurement and link capacity

RoVR

- SIP proxy: Local and PSTN call routing during WAN link outage
- PSTN fallback via external media gateway (Mediatrix, AudioCodes)

System management

- CLI (console, USB, backup modem, Telnet, SSH)
- Web user interface (HTTP, HTTPS)
- Simple Network Management Protocol (SNMP) (v1, v2, v3)
- Local administrator database
- AAA – RADIUS, TACACS+
- Syslog forwarding: External, up to four servers
- Standard and custom MIBs
- Ping, traceroute
- Hitless component upgrades via Alcatel-Lucent ModuLive software platform
- Management plane for Alcatel-Lucent Lifeline framework
- License Manager
- GUI wizards for complex configurations
  - ¬ Advanced QoS configuration GUI wizard
  - ¬ Firewall configuration wizard
  - ¬ IPSec configuration wizard
  - ¬ Universal serial interface configuration GUI
  - ¬ MLPPP/Frame Relay configuration GUI
  - ¬ VRF configuration GUI

Dimensions and power

- Weight: 1 kg (2 lb)
- Dimensions:
  - ¬ Height: 3.85 cm (1.5 in.)
  - ¬ Width: 21.22 cm (8.35 in.)
  - ¬ Depth: 20.04 cm (7.88 in.)
- Rack-mountable: 19-in. standard (half-rack width)

- Power supplies:
  - ¬ AC: 100 V AC to 240 V AC
  - ¬ DC: 20 V AC to 60 V DC

Environmental

- Operating temperature: 0°C to 50°C (32°F to 113°F)
- Non-operating temperature: -25°C to +70°C (-13°F to +158°F)
- Operating altitude: From sea level up to 3048 m (10,000 ft)
- Non-operating altitude: From sea level up to 4572 m (15,000 ft)
- Operating humidity: 10% to 90% (non-condensing)
- Convection cooled, no fan

Certifications

Networking

- 47, CFR Part 68 and ACTA adopted technical criteria
- CS 03 Issue 8, Part II
- TBR 12 and 13
- AS/ACTF S016: 2001
- T1 (DS1) JATE – 1.544 Mb/s digital interface
- E1 JATE – 2.048 Mb/s digital interface

EMC

- FCC Part 15, Subpart A
- ICES 003
- EN 55022:1998/A1:2000
- AS/NZS 3548: 1995+A1: 1997 +A2: 1997
- VCCI V-3/2000.04

Regulatory compliance

- FCC Part 15 Class A
- FCC Part 68, TIA-968-A-2
- CS-03 Issue 8, Part II
- TBR 12, TBR 13
- FCC# 6TGUSA-46505_DE-N

Safety

- US (UL 60950-1: 2003, First Ed.)
- Canada (CSA 22.2 No. 60950-1-03 First Ed.)
- Europe (EN 60950)
- Other countries (IEC 60950, CB Scheme)

IEEE standards

- IEEE 802.1D 2004 (STP)
- IEEE 802.1X (Port-based Network Access Control)
- IEEE 802.1x (EAP)
- IEEE 802.1Q/q (Tagging)
- IEEE 802.1p (CoS)
- IEEE 802.1AB (Station and Media Access Control Connectivity Discovery)
- IEEE 802.2 (Logical Link Control)
- IEEE 802.3 (Carrier Sense Multiple Access with Collision Detection -Ethernet CSMA-CD)
- IEEE 802.3ab (1000-T)
- IEEE 802.3i (10Base-T)
- IEEE 802.3u (100Base-T)
- IEEE 802.3z (1000-X)

IETF RFCs

IPv4

- RFC 2784 GRE Tunneling

RIP

- RFC 1058 RIP v1
- RFC 1721/1721/2453 RIP v2
- RFC 1812 IPv4 Router Requirement
- RFC 2082 RIP-2 MD5 Authentication

OSPF

- RFC 1131 OSPF Specification
- RFC 1247/1583/2178/2328 OSPF v2
- RFC 2370 OSPF v2 Opaque LSA option
- RFC 1586 OSPF over FR
- RFC 1587/3101 OSPF NSSA Option
- RFC 3137 OSPF Stub Router Advertisement
- RFC 1765 OSPF Database Overflow
- RFC 2439 BGP Route Flap Damping
- RFC 3509 OSPF Alternative Implementations

BGP

- RFC 1105/1163 Border Gateway Protocol (BGP)
- RFC 1654/1771 BGP-4
- RFC 1364/1403 BGP OSPF Interaction
- RFC 1397 Default Route Advertisement in BGP2 and BGP3 Versions of the BGP
- RFC 1965/3065 Autonomous Confederations for BGP
- RFC 1657 Definitions of Managed Objects for BGP-4 using SMIv2
- RFC 2283/2858/4760 Multiprotocol Extensions for BGP-4
- RFC 1997 BGP Communities Attribute
- RFC 1745 BGP4/IDRP for IP – OSPF Interaction
- RFC 2796/4456 BGP Route Reflection - An Alternative to Full Mesh IBGP
- RFC 2842/3392 Capabilities Advertisement with BGP-4

- RFC 2918 Route Refresh Capability for BGP-4

IP multicast

- RFC 1112/1054 Host Extensions for IP Multicasting
- RFC 2117 PIM-SM
- RFC 2908 The Internet Multicast Address Allocation Architecture
- RFC 2236 IGMP v2
- RFC 2362 PIM-SM Protocol Specification
- RFC 4601 PIM-SM Protocol Specification (Revised)

Advanced routing

- RFC 1701/2784 Generic Routing Encapsulation (GRE)
- RFC 1702 Generic Routing Encapsulation over IPv4 Networks
- RFC 2890 Key and Sequence Number Extensions to GRE
- RFC 2338/3768 VRRP (IPv4)
- Multi-VRF CE

Security

- RFC 2401 Security Architecture for the Internet Protocol
- RFC 1858 Security Considerations for IP Fragment Filtering
- RFC 2402 IP Authentication Header
- RFC 2406 IP Encapsulating Security Payload (ESP)
- RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408 Internet Security Association and Key Management Protocol
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 2411 IP Security Document Roadmap
- RFC 2412 OAKLEY Key Determination Protocol
- RFC 2367 PF_KEY Key Management API, Version 2
- RFC 3706 A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3715 IPSec-Network Address Translation (NAT) Compatibility Requirements
- RFC 3748 PPP Extensible Authentication Protocol (EAP)
- RFC 3947 Negotiation of NAT-Traversal in the IKE
- RFC 3948 UDP Encapsulation of IPSec ESP Packets
- RFC 4302 IP Authentication Header
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 4835 Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)

Voice and QoS

- RFC 3261 Session Initiation Protocol (SIP)
- RFC 2474 DiffServ Precedence
- RFC 2597 DiffServ Expedited Forwarding (EF)
- RFC 2598 DiffServc Assured Forwarding (AF)
- RFC 3246 An Expedited Forwarding PBH

WAN connectivity

- RFC 1234 PPP Authentication Protocols
- RFC 1990 The PPP Multilink Protocol (MP)
- RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
- RFC 2427 Multiprotocol Interconnect over Frame Relay
- RFC 1315 MIB for FR DTE
- RFC 1332 PPP IPCP
- RFC 1334 PPP Authentication PAP
- RFC 1618 PPP over ISDN
- RFC 2516 PPPoE
- RFC 1661 Point-to-Point Protocol (PPP)
- RFC 3021 Using 31-bit Prefixes on IPv4 Point-to-Point Links
- RFC 1662 PPP in HDLC-like Framing

Manageability

- RFC 2571 An Architecture for Describing SNMP Management Frameworks
- RFC 2573 SNMP Applications
- RFC 3411 Architecture for Describing SNMP Management
- RFC 2575 View-based Access Control Model (VACM) for SNMP
- RFC 2578/2579/2580 Structure of Management Information Version 2 (SMIv2)
- RFC 1157 SNMPv1
- RFC 3416 SNMP v2 Protocol Operations
- RFC 3417 SNMP v2 Transport Mappings
- RFC 3418 SNMP v2 Management Information Base
- RFC 1907 SNMP v2 Management Information Base
- RFC 2574 SNMP v3 User-based Security Model
- RFC 2863 The Interfaces Group MIB

Others

- RFC 791/966/919/1042/1166 Internet and IP / Ethernet
- RFC 768/792/793/826/854/959 UDP, ICMP, TCP, ARP, Telnet, FTP
- RFC 1853 IP in IP Tunneling
- RFC 783 TFTP rev2
- RFC 1191 Path MTU Discovery
- RFC 1305 NTPv3
- RFC 1350 TFTP rev2
- RFC 1519 CIDR
- RFC 1817 CIDR and Classful Routing
- RFC 4632 CIDR Internet Address Assignment and Aggregation Plan
- RFC 1878 Variable Length Subnet Table For IPv4 (VLSM)
- RFC 2096 IP Forwarding Table MIB
- RFC 2131 Dynamic Host Configuration Protocol (DHCP)
- RFC 3164 BSD Syslog Protocol
- RFC 3410 Introduction and Applicability Statement for Internet Standard Management Framework

7705 Service Aggregation Router

7705 SAR

The **Alcatel-Lucent 7705 Service Aggregation Router** (SAR) delivers industry-leading IP/MPLS and pseudowire capabilities in a compact platform that has the ability to reliably groom and aggregate multiple media, service and transport protocols onto an economical packet transport infrastructure.

Industry-leading scalability and density is provided in the 7705 SAR-8, a two-rack unit (2U) version of the 7705 SAR that supports up to 96 T1/E1 any service any port (ASAP) ports. The platform can optionally be configured with redundant control and switch modules (CSMs) and uplinks. The Alcatel-Lucent 7705 SAR-8 has eight slots; two are allocated for CSMs, with the remaining six being available for user traffic adapter cards.

The 7705 SAR-F is a fixed-configuration version of the SAR; it has a one rack unit (1U) high form factor and supports up to 16 T1/E1 ASAP ports. The ASAP ports can be configured to support ATM, Inverse Multiplexing over ATM (IMA), TDM and Multilink Point-to-Point Protocol (MLPPP).

The 7705 SAR-F has six 10/100 Base-T autosensing Ethernet ports, plus two ports that support 10/100/1000 Base-TX using small form-factor pluggable optics (SFPs).

KEY SELLING POINTS

- → **Cost effective:** Transition from PDH-based connectivity to Ethernet and/or IP-based networking infrastructures to greatly reduce recurring operating expenditures such as line lease costs
- → **Resilient:** Advanced resiliency features improve network uptime and allow critical services to be offered
- → **Performance:** Rapid fault detection and powerful commissioning and troubleshooting tools improve productivity of operations staff and reduce network down time
- → **Compact:** Reduces equipment instances needed to carry multiple traffic streams through multiprotocol and convergence capabilities (with flexible and granular quality of service)
- → **Configurable:** Alleviates the burden of complex pre-engineering and future scenario planning with a modular, flexible architecture
- → **Tough:** Compact, rugged form factor is well suited for remote sites where deployment conditions are not ideal
- → **Information integrity:** Accurate synchronization avoids data underflows, overflows and transmission "slips"

→ **Consistent:** Creates service and operational continuity by using a common operating system across all service routers to minimize approval for use test cycles, eliminate all issues related to release and feature backward compatibility, and allow for rapid fault isolation

KEY FEATURES

→ **Upgrade path:** Economical upgrade path from T1/E1-based backhaul to economical and flexible packet-based transport

→ **Dependable:** One-for-one hitless CSM failover (7705 SAR-8), synchronization redundancy, network uplink resiliency, and power feed redundancy

→ **Powerful management tools:** Service-aware OA&M capabilities complemented by the Alcatel-Lucent 5620 Service Aware Manager (SAM) management portfolio for GUI-based network and element configuration, provisioning, and fault and performance management

→ **Convergence:** Dense adaptation of multiple converged services onto an economical packet infrastructure

→ **Dynamic routing**: Extends IP/MPLS capabilities to small site hubs and network edge in a compact form factor

→ **Data integrity:** Redundancy and independent validation of accuracy facilitates data synchronization functions

TECHNICAL INFORMATION

7705 SAR-8

Modules and adapter cards

- CSM
- 8-port Ethernet adapter card (six ports of 10/100 Ethernet, two ports of 10/100/1000 Ethernet), DS3 point-to-point trunking is supported with an SFP device
- 16-port T1/E1 ASAP adapter card
- 4-port OC-3/STM-1 clear channel adapter card

Redundancy and resiliency

- Control
- Fabric
- Synchronization
- Uplinks
- MPLS tunnel
- Pseudowires
- Power feeds
- Cooling fans

Physical dimensions

- Height: 8.9 cm (3.5 in.) (2 RU)
- Depth: 25.4 cm (10 in.)
- Width: 43.9 cm (17.3 in.)
- Rack-mountable in a 48.2 cm rack, 30 cm depth (standard 19-in. equipment rack with 12-in. depth)

Power

- Two feeds: -48/-60 V DC or two feeds: +24 V DC
- Certified AC power solution available: 100 V AC to 240 V AC

Note: +24 V DC operation requires hardware introduced at Release 2.0

Cooling

- One tray of eight fans with redundancy

Operating environment

- Normal operating temperature range: -40°C to +65°C (-40°F to +149°F) sustained (with fan module introduced in Release 2.0)
- Normal operating temperature range: -5°C to +45°C (23°F to 113°F) (with pre-Release 2.0 fan module)
- Short term (96 hours) extended temperature range: -5°C to +55°C (23°F to 131°F) (with pre-Release 2.0 fan module)
- Normal humidity: 5% to 85%
- Short term (96 hours) extended humidity range: 5% to 95%

7705 SAR-F

Modules and adapter cards

- N/A – Fixed configuration with integrated CSM, six ports of 10/100 Ethernet, two ports of 10/100/1000 Ethernet and 16 T1/E1 ASAP ports, DS3 point-to-point trunking is supported with an SFP device

Redundancy and resiliency

- Synchronization
- Uplinks
- MPLS tunnel
- Pseudowires
- Power feeds
- Cooling fans

Physical dimensions

- Height: 4.45 cm (1.75 in.) (1 RU)
- Depth: 25.4 cm (10 in.)
- Width: 43.9 cm (17.3 in.)
- Rack-mountable in a 48.2 cm rack, 30 cm depth (standard 19 in. equipment rack with 12 in. depth)

Power

- Two feeds: -48/-60 V DC or two feeds: +24 V DC
- Certified AC power solution available: 100 V AC to 240 V AC

Cooling

- Built-in five-fan array with redundancy

Operating environment

- Normal operating temperature range: -40°C to +65°C (-40°F to +149°F) sustained
- Normal humidity: 5% to 95% non-condensing

SAR specifications

Services

- TDM pseudowires
  - ¬ RFC 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)
  - ¬ RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
- ATM pseudowires
  - ¬ RFC 4717 Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks
  - ¬ N:1 cell mode, virtual circuit connection and virtual path connection
  - ¬ ATM IMA
- Ethernet pseudowires
  - ¬ RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks
  - ¬ Raw and tagged mode
  - ¬ MEF 9- and MEF 14-certified
- IP pseudowires
  - ¬ PPP (as per RFC 1661) and MLPPP (as per RFC 1990) access to IP pseudowires
  - ¬ Ethernet (null, tagged) access to IP pseudowires

Synchronization

- External reference timing
- Line timing
- Adaptive timing
- Synchronous Ethernet
- Built-in Stratum-3 clock
- Hardware-ready to support IEEE 1588v2

Traffic management and QoS

- Hierarchical queuing
- Multi-tier scheduling
- Profiled (in and out of profile) scheduling
- Queue type-based scheduling
- Ingress policing and egress shaping
- Up to eight queues per service
- Memory allocation per queue (CBS, MBS per queue)
- Premium, assured and best-effort forwarding classes
- Weighted Random Early Detection (WRED) on ingress and egress
- Classification based on:
  - ¬ Layer 1/Layer 2/Layer 2.5 and/or Layer 3 header
  - ¬ Timeslot/port
  - ¬ Ethernet port/virtual local area network (VLAN)
  - ¬ ATM service category (CBR/rt-VBRrt-VBR/UBR)
  - ¬ ATM VC
  - ¬ Ethernet 802.1p/VLAN
  - ¬ IP differentiated services code point (IP DSCP)/MPLS EXP
- Marking based on:
  - ¬ Layer 2 (802.1p)
  - ¬ Layer 2.5 (EXP) both for tunnel and Pseudowire Emulation Edge to Edge (PWE3)
  - ¬ Layer 3 differentiated services (DiffServ)

Security (node access)

- User ID/password-based authentication and authorization
  - ¬ Exponential login backoff for brute force attacks
  - ¬ Local or remote storing of user information
- Remote authentication/authorization via RADIUS and TACACS
- Secure Shell (SSH) v2, Secure File Transfer Protocol (SFTP) and Simple Network Management Protocol (SNMP) version 3
  - ¬ Secure open interfaces
- Syslog
  - ¬ Capture security logs on local or remote server
- Alarm on suspicious sequence of operations
- Nodal attack
- Basic firewall with filtering of control plane traffic
- Denial of service (DoS) attack prevention (rate-limiting and prioritization)
- Data security
- Transfer over peer-to-peer tunnel (MPLS)
- Message-Digest Algorithm 5 (MD5) authentication
- Sequence numbers prevent replaying of data
- Statistics available on suspicious behavior

Management

- Fully featured, industry-standard CLI
- Service assurance tools, including label switched path (LSP) ping, LSP traceroute, Source Discovery Protocol (SDP) ping, and Virtual Circuit Connection Verification (VCCV)
- ATM In-band Management
- SSH and Telnet
- FTP, Trivial File Transfer Protocol (TFTP) and Secure Copy Protocol (SCP)
- RADIUS (AAA)
- TACACS+
- SNMP v2/v3

Safety, EMC and telecom regulatory compliance

Safety

- UL/CSA 60950-1
- IEC/EN 60950-1
- AS/NZS 60950-1
- IEC/EN 60825-1 and 2 (Laser Safety)

EMC

- EN 55022 1998 (Class A)
- FCC Part 15 2008 (Class A)
- ICES-003 Issue 4 2004 (Class A)
- EN 300 386 V1.3.3
- AS/NZS CISPR 22:2002 (Class A)
- GR-1089 Issue 4
- RRL Notice No. 2007-69 (Class A)
- RRL Notice No. 2007-99

Telecom

- IC CS-03 Issue 9
- ACTA TIA-968-A
- MIC No: 2004-15 (S. Korea)
- MIC No: 2005-96 (S. Korea)
- AS/ACIF S016 (Australia/ New Zealand)
- EU Directive 2002/96/EC WEEE
- EU Directive 2002/95/EC RoHS
- China: Ministry of Information
- Industry order No. 39 - CRoHS

Standards and protocols

Standards compliance

- IEEE 802.1p/Q (VLAN Tagging)
- IEEE 802.3 (10Base-T)
- IEEE 802.3u (100Base-TX)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (1000Base-SX/LX)

Protocol support

LDP

- RFC 5036 LDP Specification

MPLS

- RFC 3031 Multiprotocol Label Switching Architecture
- RFC 3032 MPLS Label Stack Encoding
- RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures

RSVP-TE and Fast Reroute

- RFC 2430 A Provider Architecture DiffServ & TE
- RFC 2702 Requirements for Traffic Engineering over MPLS
- RFC 2747 RSVP Cryptographic Authentication
- RFC 3097 RSVP Cryptographic Authentication
- RFC 3209 Extensions to RSVP for Tunnels
- RFC 4090 Fast Reroute Extensions to RSVP-TE for LSP Tunnels

OSPF

- RFC 1765 OSPF Database Overflow
- RFC 2328 OSPF Version 2
- RFC 2370 Opaque LSA Support
- RFC 2740 OSPF for IPv6 (OSPFv3) draft-ietf-ospfospfv3-update-14.txt
- RFC 3101 OSPF NSSA Option
- RFC 3137 OSPF Stub Router Advertisement
- RFC 3623 Graceful OSPF Restart – GR Helper
- RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2
- RFC 4203 Shared Risk Link Group (SRLG) sub-TLV

BFD

- Bidirectional Forwarding Detection Management Information Base draft-ietf-bfd-mib-00.txt
- Bidirectional Forwarding Detection draft-ietf-bfd-base-05.txt
- BFD IPv4 and IPv6 (Single Hop) draft-ietf-bfd-v4v6-1hop-06.txt
- BFD for Multi-hop Paths draft-ietf-bfd-multihop-06.txt

GRE

- RFC 2784 Generic Routing Encapsulation (GRE)

Differentiated services

- RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
- RFC 2597 Assured Forwarding PHB Group
- RFC 2598 An Expedited Forwarding PHB
- RFC 3140 Per Hop Behavior Identification Codes

TCP/IP

- RFC 768 User Datagram Protocol
- RFC 1350 The TFTP Protocol (Revision 2)
- RFC 791 Internet Protocol
- RFC 792 Internet Control Message Protocol
- RFC 793 Transmission Control Protocol
- RFC 826 Ethernet Address Resolution Protocol
- RFC 854 Telnet Protocol Specification
- RFC 1812 Requirements for IPv4 Routers

PPP

- RFC 1332 PPP Internet Protocol Control Protocol (IPCP)
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 1989 PPP Link Quality Monitoring
- RFC 1990 The PPP Multilink Protocol (MP)

ATM

- RFC 2514 Definitions of Textual Conventions and OBJECTIDENTITIES for ATM Management, February 1999
- RFC 2515 Definition of Managed Objects for ATM Management, February 1999
- af-tm-0121.000 Traffic Management Specification Version 4.1, March 1999
- ITU-T Recommendation I.610 – B-ISDN operation and maintenance principles and functions version 11/95
- ITU-T Recommendation I.432.1 – B-ISDN user-network interface – Physical layer specification: General characteristics
- Telcordia GR-1248-CORE – Generic Requirements for Operations of ATM Network Elements (NEs), Issue 3, June 1996
- Telcordia GR-1113-CORE – Asynchronous Transfer Mode (ATM) Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1, July 1994

Pseudowires

- RFC 4385 Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
- RFC 4447 Pseudowire Setup and Maintenance using the Label Distribution Protocol (LDP)
- RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks
- RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
- RFC 4717 Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks
- RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
- RFC 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)

RADIUS

- RFC 2865 Remote Authentication Dial In User Service (RADIUS)
- RFC 2866 RADIUS Accounting

SSH

- SSH Protocol Architecture draft-ietf-secsh-architecture.txt
- SSH Authentication Protocol draft-ietf-secsh-userauth.txt
- SSH Transport Layer Protocol draft-ietf-secsh-transport.txt
- SSH Connection Protocol draft-ietf-secsh-connection.txt
- SSH Transport Layer Encryption Modes draft-ietf-secsh-newmodes.txt

TACACS+

- IETF draft-grant-tacacs-02.txt

Network management

- ITU-T X.721: Information technology-OSI-Structure of management information
- ITU-T X.734: Information technology-OSI-Systems management: Event report management function
- ITU-T M.3100/3120 Equipment and Connection Models
- TMF 509/613 Network Connectivity Model
- RFC 1157 SNMPv1
- RFC 1907 SNMPv2-MIB
- RFC 2011 IP-MIB
- RFC 2012 TCP-MIB
- RFC 2013 UDP-MIB
- RFC 2138 RADIUS
- RFC 2571 SNMP-Framework-MIB
- RFC 2572 SNMP-MPD-MIB
- RFC 2573 SNMP-Applications
- RFC 2574 SNMP-User-Based-SM-MIB
- RFC 2575 SNMP-View-Based-ACM-MIB
- RFC 2576 SNMP-COMMUNITYMIB
- RFC 2665 Ethernet-Like-MIB
- RFC 2819 RMON-MIB
- RFC 2863 The Interfaces Group-MIB
- RFC 2864 Inverted-Stack-MIB
- RFC 3014 Notification-Log-MIB
- RFC 3273 HCRMON-MIB
- RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
- RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413 Simple Network Management Protocol (SNMP) Applications
- RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 3418 SNMP MIB
- draft-ietf-disman-alarm-mib-04.txt
- draft-ietf-mpls-ldp-mib-07.txt
- IANA-ifType-MIB Plus support for an extensive range of proprietary MIBs.

7710 Service Router

7710 SRc4

The **Alcatel-Lucent 7710 Service Router** (SR) is a feature-rich multi-service router that is a member of the full suite of Alcatel-Lucent MPLS-based routers, and is available in modular and compact form factors. It is ideally suited as a backbone node in a smaller network, a local node for a large enterprise office, or as a WAN layer-3 access point in a layer-2 network. It provides a wide variety of Ethernet, SONET and SDH, ATM circuit emulation service (CES), and TDM interfaces.

Designed for service provider and mission-critical enterprise customers, the Alcatel-Lucent 7710 SR delivers unmatched service richness, service assurance and velocity. The 7710 SR gives service providers, cable multiple system operators (MSOs) and enterprise customers a competitive edge by optimizing their infrastructure build-outs with a fully featured router that has a smaller footprint.

Optimized for the delivery of high-performance data, voice and video services, the Alcatel-Lucent 7710 SR is available in two chassis sizes to support up to four and up to 12 interface positions (depending on the model) and a wide variety of interface types and speeds.

As a member of the industry-leading Alcatel-Lucent portfolio, the 7710 SR uses the Alcatel-Lucent Service Router Operating System (SR OS), which has the proven performance and reliability capabilities to meet service provider and mission-critical application requirements for future-proof, innovative, profitable service delivery over IP/MPLS platforms.

KEY SELLING POINTS

- → **Powerful routing:** Capitalizes on all the hardware and software strengths of the Alcatel-Lucent 7750 Service Router product family
- → **Flexible:** Provides a broad range of interface types using Alcatel-Lucent 7710 Service Router Compact Media Adapter (CMA) and service router Media Dependent Adapter (MDA) including lower-speed interfaces
- → **Modular:** Supports the same applicable optical/electrical small form-factor pluggables (SFP) available on the 7750 Service Router product family
- → **Consistent:** Creates service and operational continuity by using a common operating system across all service routers, to minimize approval for use test cycles, eliminate all issues related to release and feature backward compatibility, and allow for rapid fault isolation

- **Reliable and efficient:** Facilitates full system redundancy and lower aggregation speeds in metro area networks
- **Reduced footprint:** Functions as smaller points of presence (POPs) in distributed hub sites and enterprise customer offices
- **Ease of maintenance:** Minimizes troubleshooting time with service and network level OA&M tools

KEY FEATURES

- **Advanced services:** Virtual Private LAN Service (VPLS), Virtual Private Wire Service (VPWS), Virtual Private Routed Networks (VPRNs) based on RFC 4364 and IPv6-based services
- **Service tunneling:** Enable layer-2 and layer-3 services on a single platform with the flexibility of any service over any port (ASAP) over a wide range of interfaces including channelized DS1/E1, DS3/E3, Ethernet, SONET/SDH (PoS) and ATM interfaces
- **Multiservice edge:** Frame Relay/ATM/Ethernet pseudowire services (VPWS), Ethernet/Frame Relay/ATM service interworking, Ethernet, Frame Relay and ATM access to VPLS, IP VPNs and Internet services with service-aware quality of service (QoS) to maintain stringent service level agreements (SLAs) and ensure a seamless migration to emerging services
- **Quality of service:** Service-based QoS allows for service-based queuing, which enables shaping, policing and marking of different traffic flows on a per-service basis
- **Hierarchical QoS:** Hierarchical QoS (H-QoS) uses an advanced scheduling mechanism, with multiple levels and instances of queuing, shaping, policing and marking, to prioritize different services over the same connection and combine all services into overall SLAs
- **High availability:** Nonstop services and nonstop routing that provide unparalleled availability and reliability. Nonstop services ensure that VPLS-based services and VPRNs are not affected when there is a control and forwarding module (CFM) switch-over on the Alcatel-Lucent 7710 SR. With nonstop routing, Label Distribution Protocol (LDP) adjacencies, and sessions the database remains intact if there is a switchover.
- **Operations, administration and maintenance:** Unmatched service-aware OA&M tools, and mirroring deliver the service assurance capabilities needed to reduce mean-time-to-repair (MTTR) and ensure a predictable end-user experience
- **Enhanced troubleshooting tools:** In-service software upgrade (ISSU) minimizes down time between minor release upgrades. The service assurance agent (SAA), which consists of OA&M and debugging tools, allows network operators to collect statistics such as loss, jitter, latency, response time and packet loss. Multicast troubleshooting tools include multicast functions that allow network operators to assess the distribution of IP multicast traffic, trace multicast paths in the network, and calculate performance metrics of the network.

- **Security:** Service-based filtering using access control list (ACL) support on a per-service or per-interface basis
- **Accounting and billing:** Service-based accounting and billing collects statistics on a per-service basis, not just a per-port basis
- **Network management:** The Alcatel-Lucent 7710 SR is fully supported by the Alcatel-Lucent 5620 Service Aware Manager (SAM) and 5650 Control Plane Assurance Manager (CPAM), which simplify the provisioning, management and trouble-shooting of IP/MPLS networks

TECHNICAL INFORMATION

7710 SR-c12

Throughput

- 24 Gb/s (half-duplex) forwarding capacity

CMAs/MDAs per system

Any one of the following options:

- Up to eight CMAs and two MDAs
- Up to six CMAs and three MDAs
- Up to four CMAs and four MDAs
- Up to two CMAs and five MDAs
- Up to six MDAs

Redundancy

- Redundancy on all common system elements
- Nonstop routing, including BGP, OSPFv3, IS-IS, RIP, RSVP-TE, LDP, T-LDP
- In-service insertion and removal of system components and physical interfaces

Physical dimensions

- Height: 22.2 cm (8.7 in.)
- Width: 44.4 cm (17.5 in.)
- Depth: 60.0 cm (23.6 in.)

Power

- -40 V DC to -75 V DC (nominal)
- 85 V AC to 265 V AC

Cooling

- Horizontal forced airflow

7710 SR-c4

Throughput

- 18 Gb/s (half-duplex) forwarding capacity

CMAs/MDAs per system

Any one of the following options:

- Up to four CMAs
- One MDA and up to two CMAs
- Up to two MDAs

Redundancy

- Redundancy on power modules and fans
- In-service insertion and removal of system components and physical interfaces

Physical dimensions

- Height: 13.3 cm (5.3 in.)
- Width: 44.4 cm (17.5 in.)
- Depth: 55.9 cm (22.0 in.)

Power

- -40 V Dc to -75 V DC (nominal)
- 85 V AC to 265 V AC

Cooling

- Horizontal forced airflow

Interfaces

CMAs

- 8-port Channelized DS1/E1 (n x 64 kb/s) RJ-48C 32 64
- 8-port T1/E1 ATM RJ-48C 32 64
- 4-port DS3/E3 1.0/2.3 Connectors 16 32
- 8-port 10/100Base-T Ethernet RJ-45 32 64
- 1-port Gigabit Ethernet SFP 4 8
- 2-port OC-3c/OC-12c/STM-1/STM-4 SFP 8 16
- 1-port CH OC-3/STM-1 CES SFP 1 2
- 1-port Gigabit Ethernet CMA-XP SFP 4 8
- 10-port Gigabit Ethernet CMA-XP SFP 20 80
- 20-port Gigabit Ethernet CMA-XP SFP 40 160
- 20-port Gigabit Ethernet CMA-XP Copper RJ-45 40 160

Ethernet MDAs

- 20-port 100Base-FX SFP 40 120
- 20-port 10/100/1000Base-TX SFP 40 120
- 60-port 10/100Base-TX 5 x mini RJ-21 120 360

- 5-port Gigabit Ethernet SFP 10 30
- 20-port Gigabit Ethernet SFP 40 120

Packet over SONET/SDH (POS) MDAs

- 8-port OC-3c/STM-1c SFP 16 48
- 2-port OC-48c/STM-16c SFP 4 12

ASAP MDAs

- 4-port CH DS3/E3 ASAP Mini SMB 8 8
- 12-port CH DS3/E3 ASAP Mini SMB 24 24
- 4-port CH OC-3/STM-1 ASAP SFP 8 8
- 1-port CH OC-12/STM-4 ASAP SFP 2 2

CES MDAs

- 1-port CH OC-12 CES SFP 1 2
- 4-port CH OC3-CES SFP 4 8

ATM MDAs

- 4-port ATM OC-3c/STM-1c/OC-12c/ STM-4c (Multirate) SFP 4 8

Safety standards and compliance agency certifications

Safety

- EN 60590-1
- IEC 60950-1 CB Scheme
- CSA/UL 60950-1 NRTL
- FDA CDRH 21-CFR 1040
- EN 60825-1
- EN 60825-1/2
- IEC 60825-1
- IEC 60825-2

EMC

- ICES-003 Class A
- FCC Part 15 Class A
- EN 300 386
- EN 55022
- EN 55024
- EN 61000-4-2
- EN 61000-4-3
- EN 61000-4-4
- EN 61000-4-5
- EN 61000-4-6
- EN 61000-4-11
- IEC CISPR 22
- AS/NZS CISPR 22

Immunity

- EN 61000-3-2 Power Line Harmonics
- EN 61000-3-3 Voltage Fluctuations and Flicker
- EN 61000-4-2 Electric Static Discharge
- EN 61000-4-3 Radiated Immunity
- EN 61000-4-4 EFT
- EN 61000-4-5 Surge
- EN 61000-4-6 Low Frequency Common Immunity
- EN 61000-4-11 Voltage Dips and Sags

Telecom

- Telcordia GR-253-CORE Issue 3
- IEEE 802.3 (Gigabit Ethernet, Ethernet)
- ANSI T1.105.03
- ANSI T1.105.06
- ANSI T1.105.09
- ANSI T1.403 (DS1)
- ANSI T1.404 (DS3)
- ITU-T G.957
- ITU-T G.825
- ITU-T G.824
- ITU-T G.823
- ITU-T G.813
- ITU-T G.707
- ITU-T G.703

Environmental

- ETS 300 019-1-1, Storage Tests, Class 1.2
- ETS 300 019-1-2, Transportation Tests, Class 2.3
- ETS 300 019-1-3, Operational Tests, Class 3.2
- ETS 300 019-2-4, pr A1 Seismic

Environmental specifications

- Operating temperature: 0°C to 40°C (32°F to 104°F)
- Relative humidity: 15% to 85% (non-condensing)
- Operating altitude: Sea level to 3048 m (10,000 ft)

Electronic equipment devices

- WEEE
- RoHS
- R&TTE
- China CRoHS

Certifications

- Network Equipment Building System (NEBS) level 3
  - ¬ Telcordia GR-63-CORE, Issue 4, June 2006
  - ¬ Telcordia GR-1089-CORE, Issue 3, March 2006
  - ¬ ATT-TP-76200
- CE

Standards compliance

- IEEE 802.1ab-REV/D3 (Station and Media Access Control Connectivity Discovery)
- IEEE 802.1d (Bridging)

- IEEE 802.1p/Q (VLAN Tagging)
- IEEE 802.1s (Multiple Spanning Tree)
- IEEE 802.1w (Rapid Spanning Tree Protocol)
- IEEE 802.1x (Port-based Network Access Control)
- IEEE 802.1ad (Provider Bridges)
- IEEE 802.1ah (Provider Backbone Bridges)
- IEEE 802.1ag (Service Layer OAM)
- IEEE 802.3ah (Ethernet in the First Mile)
- IEEE 802.1ak (Multiple MAC Registration Protocol)
- IEEE 802.3 (10Base-T)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3ae (10 Gb/s Ethernet)
- IEEE 802.3ah (Ethernet OAM)
- IEEE 802.3u (100Base-TX)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (1000Base-SX/LX)
- ITU-T Y.1731 (OAM functions and mechanisms for Ethernet-based networks)

Synchronous Ethernet

- ITU-T G.8261 - g.pactiming – Timing and synchronization aspects of packet networks
- ITU-T G.8262 - g.paclock – Timing characteristics of Ethernet equipment slave clock (EEC)
- ITU-T G.8264 - g.pacmod – Distribution of timing through packet networks and Ethernet Sync Status Message (ESSM)

Protocol support

OSPF

- RFC 1765 OSPF Database Overflow
- RFC 2328 OSPF Version 2
- RFC 2370 Opaque LSA Support
- RFC 2740 OSPF for IPv6 (OSPFv3) draft-ietf-ospfospfv3-update-14.txt
- RFC 3101 OSPF NSSA Option
- RFC 3137 OSPF Stub Router Advertisement
- RFC 3623 Graceful OSPF Restart – GR Helper
- RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2
- RFC 4203 For Shared Risk Link Group (SRLG) sub-TLV

BGP

- RFC 1397 BGP Default Route Advertisement
- RFC 1772 Application of BGP in the Internet
- RFC 1965 Confederations for BGP
- RFC 1997 BGP Communities Attribute
- RFC 2385 Protection of BGP Sessions via MD5
- RFC 2439 BGP Route Flap Dampening
- RFC 2547bis BGP/MPLS VPNs
- draft-ietf-idr-rfc2858bis-09.txt
- RFC 2918 Route Refresh Capability for BGP-4
- RFC 3107 Carrying Label Information in BGP-4
- RFC 3392 Capabilities Advertisement with BGP4
- RFC 4271 BGP-4 (previously RFC 1771)
- RFC 4360 BGP Extended Communities Attribute
- RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs) (previously RFC 2547bis BGP/MPLS VPNs)
- RFC 4456 BGP Route Reflection: Alternative to Full-mesh IBGP (previously RFC 1966 & 2796)
- RFC 4724 Graceful Restart Mechanism for BGP – GR Helper
- RFC 4760 Multi-protocol Extensions for BGP
- RFC 4893 BGP Support for Four-octet AS Number Space
- RFC 5065 Confederations for BGP (obsoletes 3065)

IS-IS

- RFC 1142 OSI IS-IS Intra-domain Routing Protocol (ISO 10589)
- RFC 1195 Use of OSI IS-IS for routing in TCP/IP and Dual Environments
- RFC 2763 Dynamic Hostname Exchange for IS-IS
- RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
- RFC 2973 IS-IS Mesh Groups
- RFC 3373 Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
- RFC 3567 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
- RFC 3719 Recommendations for Interoperable Networks using IS-IS

- RFC 3784 Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)
- RFC 3787 Recommendations for Interoperable IP Networks
- RFC 3847 Restart Signaling for IS-IS – GR Helper
- RFC 4205 for Shared Risk Link Group (SRLG) TLV
- draft-ietf-isis-igp-p2p-over-lan-05.txt

LDP

- RFC 3036 LDP Specification
- RFC 3037 LDP Applicability
- RFC 3478 Graceful Restart Mechanism for LDP – GR Helper
- RFC 5283 LDP Extension for Inter-Area LSP
- draft-jork-ldp-igp-sync-03.txt

IPv6

- RFC 1981 Path MTU Discovery for IPv6
- RFC 2375 IPv6 Multicast Address Assignments
- RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
- RFC 2461 Neighbor Discovery for IPv6
- RFC 2462 IPv6 Stateless Address Auto Configuration
- RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification
- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels
- RFC 2545 Use of BGP-4 Multiprotocol Extension for IPv6 Inter-Domain Routing
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
- RFC 2740 OSPF for IPv6
- RFC 3306 Unicast-Prefix-based IPv6 Multicast Addresses
- RFC 3315 Dynamic Host Configuration Protocol for IPv6
- RFC 3587 IPv6 Global Unicast Address Format
- RFC 3590 Source Address Selection for the Multicast Listener Discovery (MLD) Protocol
- RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4291 IPv6 Addressing Architecture
- RFC 4659 BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
- RFC 5072 IP Version 6 over PPP
- draft-ietf-isis-ipv6-05.txt
- draft-ietf-isis-wg-multi-topology-xx.txt

Multicast

- RFC 1112 Host Extensions for IP Multicasting (Snooping)
- RFC 2236 Internet Group Management Protocol (Snooping)
- RFC 2362 Protocol Independent Multicast-Sparse Mode (PIM-SM)
- RFC 3376 Internet Group Management Protocol, Version 3 (Snooping)
- RFC 3618 Multicast Source Discovery Protocol (MSDP)
- RFC 3446 Anycast Rendezvous Point (RP) Mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)
- RFC 3956: Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address
- RFC 4601 Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification (Revised)
- RFC 4604 Using IGMPv3 and MLDv2 for Source-Specific Multicast
- RFC 4607 Source-Specific Multicast for IP
- RFC 4608 Source-Specific Protocol Independent Multicast in 232/8
- RFC 4610 Anycast-RP Using Protocol Independent Multicast (PIM)
- draft-ietf-pim-sm-bsr-06.txt
- draft-rosen-vpn-mcast-08.txt
- draft-ietf-mboned-msdp-mib-01.txt
- draft-ietf-l3vpn-2547bis-mcast-07.txt: Multicast in MPLS/BGP IP VPNs
- draft-ietf-l3vpn-2547bis-mcast-bgp-05.txt: BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs

MPLS

- RFC 3031 MPLS Architecture
- RFC 3032 MPLS Label Stack Encoding (REV 3443)
- RFC 4182 Removing a Restriction on the Use of MPLS Explicit NULL
- RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
- RFC 5332 MPLS Multicast Encapsulations

RIP

- RFC 1058 RIP Version 1
- RFC 2082 RIP-2 MD5 Authentication
- RFC 2453 RIP Version 2

RSVP-TE

- RFC 2430 A Provider Architecture DiffServ & TE
- RFC 2702 Requirements for Traffic Engineering over MPLS
- RFC 2747 RSVP Cryptographic Authentication
- RFC 3097 RSVP Cryptographic Authentication
- RFC 3209 Extensions to RSVP for Tunnels
- RFC 3564 Requirements for Differentiated Services-aware TE
- RFC 4090 Fast Reroute Extensions to RSVP-TE for LSP Tunnels
- RFC 4124 Protocol Extensions for Support of Differentiated Services-aware MPLS Traffic Engineering
- RFC 4125 Maximum Allocation Bandwidth Constraints Model for Differentiated Services-aware MPLS Traffic Engineering
- RFC 4875 Extensions to Resource Reservation Protocol – Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)
- MPLS Traffic Engineering Soft Preemption; draft-ietf-mpls-soft-preemption-14.txt
- Graceful Shutdown in GMPLS Traffic Engineering Networks; draft-ietf-ccamp-mpls-graceful-shutdown-06.txt
- Graceful Shutdown in GMPLS Traffic Engineering Networks; draft-ietf-mpls-p2mp-lsp-ping-06.txt

Differentiated services

- RFC 2474 Definition of the DS Field in the IPv4 and IPv6 Headers (Rev)
- RFC 2597 Assured Forwarding PHB Group (rev3260)
- RFC 2598 An Expedited Forwarding PHB
- RFC 3140 Per-Hop Behavior Identification Codes

TCP/IP

- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 854 Telnet
- RFC 951 BOOTP (rev)
- RFC 1350 The TFTP Protocol
- RFC 1519 CIDR
- RFC 1542 Clarifications and Extensions for the Bootstrap Protocol
- RFC 1812 Requirements for IPv4 Routers
- RFC 2347 TFTP Option Extension
- RFC 2328 TFTP Blocksize Option
- RFC 2349 TFTP Timeout Interval and Transfer Size option
- RFC 2401 Security Architecture for Internet Protocol
- Bidirectional Forwarding Detection Management Information Base; draft-ietf-bfd-mib-00.txt
- Bidirectional Forwarding Detection; draft-ietf-bfd-base-05.txt
- BFD IPv4 and IPv6 (Single Hop); draft-ietf-bfd-v4v6-1hop-06.txt
- BFD for Multihop Paths; draft-ietf-bfd-multihop-06.txt

VRRP

- RFC 2787 Definitions of Managed Objects for the Virtual Router Redundancy Protocol
- RFC 3768 Virtual Router Redundancy Protocol
- draft-ietf-vrrp-unified-spec-02.txt: Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6

PPP

- RFC 1332 PPP IPCP
- RFC 1377 PPP OSINLCP
- RFC 1638/2878 PPP BCP
- RFC 1661 PPP (rev RFC2151)
- RFC 1662 PPP in HDLC-like Framing
- RFC 1877 PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
- RFC 1989 PPP Link Quality Monitoring
- RFC 1990 The PPP Multilink Protocol (MP)
- RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
- RFC 2516 A Method for Transmitting PPP over Ethernet

- RFC 2615 PPP over SONET/SDH
- RFC 2686 The Multi-Class Extension to Multi-Link PPP

Frame relay

- FRF.1.2 – PVC User-to-Network Interface (UNI) Implementation Agreement
- FRF.5 – Frame Relay/ATM PVC Network Interworking Implementation
- ANSI T1.617 Annex D, DSS1 – Signaling Specification for Frame Relay Bearer Service
- FRF2.2 – PVC Network-to-Network Interface (NNI) Implementation Agreement
- FRF.12 – Frame Relay Fragmentation Implementation Agreement
- FRF.16.1 – Multilink Frame Relay UNI/NNI Implementation Agreement
- ITU-T Q.933 Annex A – Additional procedures for Permanent Virtual Connection (PVC) status management

ATM

- RFC 1626 Default IP MTU for use over ATM AAL5
- RFC 2514 Definitions of Textual Conventions and OBJECT_IDENTITIES for ATM Management
- RFC 2515 Definition of Managed Objects for ATM Management
- RFC 2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5
- AF-TM-0121.000 Traffic Management Specification Version 4.1
- ITU-T Recommendation I.610 – B-ISDN Operation and Maintenance Principles and Functions version 11/95
- ITU-T Recommendation I.432.1 – BISDN user network interface – Physical layer specification: General characteristics
- Telcordia GR-1248-CORE – Generic Requirements for Operations of ATM Network Elements (NEs), Issue 3
- Telcordia GR-1113-CORE – Bellcore, Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1
- AF-ILMI-0065.000 Integrated Local Management Interface (ILMI) Version 4.0
- AF-TM-0150.00 Addendum to Traffic Management v4.1 optional minimum desired cell rate indication for UBR
- AF-PHY-0086.001 Inverse Multiplexing for ATM (IMA) Specification Version 1.1

DHCP

- RFC 1534 Interoperation between DHCP and BOOTP
- RFC 2131 Dynamic Host Configuration Protocol (REV)
- RFC 3046 DHCP Relay Agent Information Option (Option 82)

VPLS

- RFC 4762 Virtual Private LAN Services Using LDP (previously draft-ietf-l2vpn-vpls-ldp-08.txt)
- draft-ietf-l2vpn-vpls-mcast-reqts-04.txt

Pseudowire

- RFC 3916 Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)
- RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3)
- RFC 4385 Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
- RFC 4446 IANA Allocations for PWE3
- RFC 4447 Pseudowire Setup and Maintenance Using LDP (draft-ietf-pwe3-control-protocol-17.txt)
- RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks (draft-ietf-pwe3-ethernet-encap-11.txt)
- RFC 4619 Encapsulation Methods for Transport of Frame Relay over MPLS Networks (draft-ietfpwe3-frame-relay-07.txt)
- RFC 4717 Encapsulation Methods for Transport ATM over MPLS Networks (draft-ietf-pwe3-atmencap-10.txt)
- RFC 4816 PWE3 ATM Transparent Cell Transport Service (draft-ietf-pwe3-cell-transport-04.txt)
- RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
- draft-ietf-l2vpn-vpws-iw-oam-02.txt
- draft-ietf-pwe3-oam-msg-map-05-txt
- draft-ietf-l2vpn-arp-mediation-04.txt
- draft-ietf-pwe3-ms-pw-arch-02.txt
- draft-ietf-pwe3-segmented-pw-05.txt
- draft-hart-pwe3-segmented-pw-vccv-02.txt
- draft-muley-dutta-pwe3-redundancy-bit-02.txt
- draft-muley-pwe3-redundancy-02.txt

- MFA Forum 9.0.0 The Use of Virtual Trunks for ATM/MPLS Control Plane Interworking
- MFA Forum 12.0.0 Multiservice Interworking – Ethernet over MPLS
- MFA forum 13.0.0 Fault Management for Multiservice Interworking v1.0
- MFA Forum 16.0.0 Multiservice Interworking – IP over MPLS

ANCP/L2CP

- draft-ietf-ancp-framework-01.txt
- draft-ietf-ancp-protocol-00.txt

Circuit emulation

- RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
- RFC 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN) MEF-8 Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks, October 2004
- RFC 5287 Control Protocol Extensions for the Setup of Time Division Multiplexing (TDM) Pseudowires in MPLS Networks

SONET/SDH

- Telcordia GR-253-CORE SONET Transport Systems: Common Generic Criteria, Issue 3, September 2000
- ITU-T G.841 Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum 1, issued in July 2002

RADIUS

- RFC 2865 Remote Authentication Dial In User Service
- RFC 2866 RADIUS Accounting

SSH

- draft-ietf-secsh-architecture.txt SSH Protocol Architecture
- draft-ietf-secsh-userauth.txt SSH Authentication Protocol
- draft-ietf-secsh-transport.txt SSH Transport Layer Protocol
- draft-ietf-secsh-connection.txt SSH Connection Protocol
- draft-ietf-secsh-newmodes.txt SSH Transport Layer Encryption Modes

TACACS+

- draft-grant-tacacs-02.txt

Network management

- ITU-T X.721: Information technology – OSI - Structure of Management Information
- ITU-T X.734: Information technology – OSI - Systems Management: Event Report Management Function
- ITU-T M.3100/3120 Equipment and Connection Models
- TMF 509/613 Network Connectivity Model
- RFC 1157 SNMPv1
- RFC 1215 A Convention for Defining Traps for use with the SNMP
- RFC 1657 BGP4-MIB
- RFC 1724 RIPv2-MIB
- RFC 1850 OSPF-MIB
- RFC 1907 SNMPv2-MIB
- RFC 2011 IP-MIB
- RFC 2012 TCP-MIB
- RFC 2013 UDP-MIB
- RFC 2096 IP-FORWARD-MIB
- RFC 2138 RADIUS
- RFC 2206 RSVP-MIB
- RFC 2452 IPv6 Management Information Base for the Transmission Control Protocol
- RFC 2454 IPv6 Management Information Base for the User Datagram Protocol
- RFC 2465 Management Information Base for IPv6: Textual Conventions and General Group
- RFC 2558 SONET-MIB
- RFC 2571 SNMP-FRAMEWORK-MIB
- RFC 2572 SNMP-MPD-MIB
- RFC 2573 SNMP-TARGET-&-NOTIFICATION-MIB
- RFC 2574 SNMP-USER-BASED-SMMIB
- RFC 2575 SNMP-VIEW-BASEDACM-MIB
- RFC 2576 SNMP-COMMUNITY-MIB
- RFC 2665 EtherLike-MIB
- RFC 2819 RMON-MIB
- RFC 2863 IF-MIB
- RFC 2864 INVERTED-STACK-MIB
- RFC 2987 VRRP-MIB
- RFC 3014 NOTIFICATION-LOGMIB
- RFC 3019 IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol
- RFC 3164 Syslog
- RFC 3273 HCRMON-MIB

- RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
- RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413 Simple Network Management Protocol (SNMP) Applications
- RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 3418 SNMP MIB
- draft-ietf-disman-alarm-mib-04.txt
- draft-ietf-ospf-mib-update-04.txt
- draft-ietf-mpls-lsr-mib-06.txt
- draft-ietf-mpls-te-mib-04.txt
- draft-ietf-mpls-ldp-mib-07.txt
- draft-ietf-isis-wg-mib-05.txt
- IANA-IFType-MIB
- IEEE8023-LAG-MIB

7750 Service Router


7750 SR-12


7750 SR-c12


7750 SR-7


7750 SR-1

The **Alcatel-Lucent 7750 Service Router** (SR) is a superior multi-service edge router that is purpose-built for mission-critical enterprise and vertical market customers, service providers and cable multiple system operators (MSOs) looking to deliver a new wave of services on a single IP/MPLS network.

Optimized for the delivery of high-performance data, voice and video services, the Alcatel-Lucent 7750 SR is available in five chassis sizes whose capacities range from 40 Gb/s to 2 terabits — all of which offer a wide range of interfaces with unmatched density and service performance. They are the 7750 SR-1, 7750 SR-7, 7750 SR-12 and the 7750 SR-c12.

Leveraging the strength of the Alcatel-Lucent Service Router Operating System (SR OS), the 7750 SR delivers the flexibility to achieve the service continuity, service richness and service assurance critical to customer satisfaction and market leadership.

KEY SELLING POINTS

- **Purpose-built platform:** Enables the efficient and cost-effective delivery of a new generation of differentiated voice, video and data services
- **Reliable:** Integrates full system redundancy and industry-leading nonstop routing and nonstop switching
- **Future-proof:** Flexible form factors and network asset portability across the service router portfolio result in optimal CAPEX investment with extended asset longevity and depreciation cycles
- **Performance:** Sophisticated packet processing capabilities and service headroom result in maximized network asset yields with no hidden CAPEX owing to line card or platform proliferation
- **Efficient:** Reduced OPEX and accelerated time-to-market through rapid service provisioning and advanced OA&M tools
- **Fast and secure:** Improved service level guarantees through a comprehensive approach to high availability using purpose-built hardware and software, which provides industry-leading performance and comprehensive security capabilities
- **Consistent:** Creates service and operational continuity by using a common operating system across all service routers, to minimize approval for use test cycles, eliminate all issues related to release and feature backward compatibility, and allow for rapid fault isolation

KEY FEATURES

- **Advanced services:** Enables Virtual Private LAN Service (VPLS), Virtual Private Wire Service (VPWS), Virtual Private Routed Networks (VPRNs) based on RFC 4364 and IPv6 services.
- **Service tunneling:** Enable layer-2 and layer-3 services on a single platform with the flexibility of any service over any port (ASAP) over a wide range of interfaces including DS3/E3, Ethernet, SONET/SDH (PoS), Frame Relay and ATM interfaces. Additional interface options include OC-3/STM-1 support on the ASAP interface card and a combination interface card supporting gigabit and 10-gigabit (10G) ports.
- **Multiservice edge:** Comprehensive service continuity with Frame Relay/ATM/Ethernet pseudowire services (VPWS), Ethernet/Frame Relay/ATM service interworking, Ethernet, Frame Relay and ATM access to VPLS, IP VPNs and Internet services with service-aware quality of service (QoS) to maintain stringent service level agreements (SLAs) and ensure a seamless migration to emerging services.
- **Quality of service:** Service-based QoS allows for service-based queuing, which enables shaping, policing and marking of different traffic flows on a per-service basis. Enhancements include class-based forwarding allowing service packets to be directed over specific Resource Reservation Protocol (RSVP) label switched paths (LSPs) based on their forwarding class. Label Distribution Protocol (LDP) over RSVP with Traffic Engineering (RSVP-TE) allows end-to-end LDP tunnels to inherit RSVP-TE properties.
- **Hierarchical QoS:** Hierarchical QoS (H-QoS) uses an advanced scheduling mechanism, with multiple levels and instances of queuing, shaping, policing and marking to prioritize different services over the same connection and combine all services into overall SLAs.
- **Service scaling:** Concurrently supports tens of thousands of layer-2 and layer-3 services, more than 2 million Border Gateway Protocol (BGP) routes and up to 32,000 LSPs per system. Enhancements include pseudowire switching to scale VPWS and VPLS over multi-area networks and LDP over RSVP-TE to avoid a full mesh of end-to-end RSVP-TE tunnels between provider edge (PE) routers.
- **High availability:** Nonstop services and nonstop routing that provide unparalleled availability and reliability. Nonstop services ensure that VPLS-based services and VPRNs are not affected when there is a control processing module (CPM) switchover on the 7750 SR. With nonstop routing, LDP adjacencies, sessions and the database remain intact if there is a switchover. Other differentiating high availability features include multi-chassis link aggregation (LAG) and pseudowire redundancy.
- **Operations, administration and maintenance:** Service assurance capabilities such as administration and maintenance toolkit and mirroring are integrated to reduce mean-time-to-repair (MTTR) and ensure a predictable end-user experience.

- **Enhanced troubleshooting tools:** In-service software upgrade (ISSU) minimizes down time between minor release upgrades. The service assurance agent (SAA), which consists of OA&M and debugging tools, allows network operators to collect statistics such as loss, jitter, latency, response time and packet loss. Multicast troubleshooting allows network operators to assess the distribution of IP multicast traffic, to trace multicast paths in the network and to calculate performance metrics of the network.
- **Security:** Critical path method queuing eliminates the effect of one peer consuming the system resources and service-based filtering uses access control lists (ACLs) to filter on a per-service or per-interface basis.
- **Accounting and billing:** Service-based accounting and billing collects statistics on a per-service basis, not just a per-port basis.
- **Network management:** The Alcatel-Lucent 7750 SR is fully supported by the Alcatel-Lucent 5620 Service Aware Manager (SAM) and 5650 Control Plane Assurance Manager (CPAM), which simplify the provisioning, management and troubleshooting of IP/MPLS networks.

TECHNICAL INFORMATION

7750 SR-12

System throughput
- Switch fabric: Up to 1 Tb (half-duplex)
- Slot capacity: Up to 50 Gb/s (full-duplex)

Input/Output Modules (IOMs) supported
- IOM-2
- IOM3-XP

Number of IOMs supported per chassis
- 10 – Any mix of IOM-2 or IOM3-XP

Number of half-slot of MDAs per chassis
- 20 – Any mix of MDA or MDA-XP

Integrated Media Modules (IMMs) supported
- 4-port 10GigE (XFP) IMM
- 8-port 10GigE (XFP) IMM
- 48-port GigE (SFP) IMM
- 48-port GigE (10/100/1000Base-T) IMM

Redundancy
- SF/CPM, power, fans

Hot-swappable modules
- SF/CPM, power, fans, IOM, MDA, IMM, Integrated Service Adapter (ISA)

Dimensions
- Height: 62.2 cm (24.5 in.)
- Width: 44.4 cm (17.5 in.)
- Depth: without cable: 64.5 cm (25.4 in.); with cable: 76.5 cm (30.1 in.)

Weight
- Empty: 33.1 kg (73 lb)
- Loaded: 136 kg (300 lb) approx.

Power
- -40 V DC to -72 V DC (nominal)
- 90 A to 162 A
- 1+1 redundancy

Cooling
- Front-to-back air flow

7750 SR-7

System throughput
- Switch fabric: Up to 500 Gb/s (half-duplex)
- Slot capacity: Up to 50 Gb/s (full-duplex)

IOMs supported
- IOM-2
- IOM3-XP

Number of IOMs supported per chassis
- Five – Any mix of IOM-2 or IOM3-XP

Number of half-slot of MDAs per chassis
- 10 – Any mix of MDA or MDA-XP

IMMs supported
- 4-port 10GigE (XFP) IMM
- 8-port 10GigE (XFP) IMM
- 48-port GigE (SFP) IMM
- 48-port GigE (10/100/1000Base-T) IMM

Redundancy
- SF/CPM, power, fans

Hot-swappable modules
- SF/CPM, power, fans, IOM, MDA, IMM, ISA

Dimensions
- Height: 35.5 cm (14.0 in.)
- Width: 44.4 cm (17.5 in.)
- Depth: 59.7 cm (25.5 in.)

Weight
- Empty: 27.2 kg (60 lb)
- Loaded: 70.3 kg (155 lb) approx.

Power
- -40 V DC to -72 V DC (nominal)
- 52 A to 93 A
- 1+1 redundancy

Cooling
- Side-to-back air flow

7750 SR-1

System throughput
- Switch fabric: Up to 40 Gb/s (half-duplex)
- MDA half-slot capacity: Up to 10 Gb/s (full-duplex)

IOMs supported
- Integrated IOM and SF/CPM

Number of IOMs supported per chassis
- Not applicable

Number of half-slot MDAs per chassis
- Two – Any mix of MDA or MDA-XP

IMMs supported
- None

Redundancy
- Power

Hot-swappable modules
- Power, integrated IOM and SF/CPM, MDA

Dimensions
- Height: 6.6 cm (2.6 in.)
- Width: 44.4 cm (17.5 in.)
- Depth: 56.4 cm (22.2 in.)

Weight
- Empty: 12.3 kg (27 lb)
- Loaded: 13.2 kg (29 lb) approx.

Power
- 110 V AC or 220 V AC
- -40 V DC to -72 V DC (nominal)
- 10 A to 6 A
- 1+1 redundancy
- AC available with external shelf

Cooling
- Side-to-back air flow

Physical interface
- SF/CPM
  - ¬ 7750 SR-12 – 1 Tb/s (half-duplex)
  - ¬ 7750 SR-7 – 500 Gb/s (half-duplex)
- IOMs
  - ¬ IOM3-XP – 50 Gb/s (full-duplex)
  - ¬ IOM-2 – 20 Gb/s (full-duplex)
- IMMs
  - ¬ 50 Gb/s (full duplex)
- Integrated IOM and SF/CPM (7750 SR-1 only)

Interface types

MDA-type ports per MDA interface type
- Ethernet MDA-XPs
- 1000Base 10/20 SFP
- 10/100/1000Base 20 RJ-45
- 10GBase (LAN/WAN PHY) 1/2/4 XFP

Ethernet MDAs
- 10/100/1000Base 20 RJ-45
- 100Base-FX 20 SFP
- 10/100Base-TX 60 5 x mini RJ-21
- 1000Base 5/10/20 SFP

- 10GBase/1000Base 1+10 XFP/SFP
- 10GBase (LAN/WAN PHY) 1 Simplex SC
- 10GBase (tunable optics) 1 LC
- 10GBase (LAN PHY) 1/2 XFP

High-scale MDAs
- 1000Base 10 SFP
- 10GBase 1 XFP

POS MDAs
- OC-3c/STM-1c 8/16 SFP
- OC-3c/STM-1c/OC-12c/STM-4c (Multirate) 8/16 SFP
- OC-48c/STM-16c 2/4 SFP
- OC-192c/STM-64c 1 Simplex SC

ASAP MDAs
- Chan. DS3/E3 ASAP
- Chan. OC-3/STM-1 ASAP 4 SFP
- Chan. OC-12/STM-4 ASAP 1 SFP

CES MDAs
- Chan. OC-3/STM-1 CES 1/4 SFP
- Chan. OC-12/STM-4 CES 1 SFP

ATM MDAs
- ATM OC-3c/STM-1c/OC-12c/STM-4c (Multirate) 4 SFP
- ATM OC-3c/STM-1c 16 SFP

Other
- Versatile Service Module

CMA-type ports per CMA interface type
- 1000Base CMA-XP 1/5 SFP
- Chan. DS1/E1 8 RJ-48
- DS3/E3 4 1.0/2.3 Connectors
- 10/100Base-TX 8 RJ-45
- 1000Base 1 SFP
- Chan. OC-3/STM-1 CES 1 SFP
- OC-3c/STM-1c/OC-12c/STM-4c (Multirate) 2 SFP
- ATM T1/E1 IMA 8 RJ-48C

IMM-type ports per IMM interface type
- 10GBase 4/5/8 XFP
- 10/100/1000Base 48 SFP
- 10/100/1000Base 48 RJ-45

Software support

Services
- IP VPN (RFC 4364)
- IPv6-based IP VPN
- VPWS point-to-point Layer 2 VPN
- VPLS multipoint Layer 2 VPN (RFC 4762)
- Direct Internet access
- CES
- Mobile transport
- IP multicast support with VPRN using "draft Rosen"
- Pseudowire Emulation Edge to Edge (PWE3) using "draft Martini" encapsulation
- Generic routing encapsulation (GRE)
- Provider backbone bridge (PBB) based on IEEE 802.1ah
- PBB and VPLS integration
- Synchronous Ethernet ITU Sync-E G.8261, G.8261, G.8264 standards compliant
- Synchronous Ethernet ITU Sync-E G.8263 for synchronous status messaging (SSM) is hardware ready

QoS
- Per-service QoS with per-service queuing, shaping and policing
- Hierarchical queuing and scheduling
- Ingress and egress buffering (up to 200 ms at 25 Gb/s in each direction)
- Committed information rate (CIR), peak information rate (PIR), maximum burst size (MBS) queue parameters
- Thousands of ingress and egress operations
- Programmable queues with CIR/PIR enforcement
- Premium, assured and best-effort forwarding classes
- IEEE 802.1p filtering/marking/re-marking
- IETF differentiated services code point (DSCP) filtering/marking/re-marking
- Weighted Random Early Detection (WRED) on ingress and egress
- Packet marking (DiffServ)
- Traffic shaping and policing (ingress and egress)
- Digital subscriber line access multiplexer (DSLAM) ID as a secondary shaper
- Packet and byte counter statistics (ingress and egress)

Security
- Wirespeed ACLs
- Message-Digest Algorithm 5 (MD5) password encryption and authentication for routing protocols
- Classification and prioritization of control traffic

- Secure Shell (SSH) v1/v2 and Secure Copy (SCP)
- IEEE 802.1x port-based authentication
- Prevention of unauthorized communication between DSL subscribers
- DHCP-based automatic IP/MAC filter and static Address Resolution Protocol (ARP) cache population for DSL subscribers
- Dedicated management Ethernet routing instance
- Control processor module queuing (CPMQ); separate hardware-based CPM queues allocated on a per-peer basis
- Inbound and outbound LDP label binding filtering
- Limitation of MAC address moves between VPLS instances
- CPM filter based on MAC criteria

Lawful intercept

- Highly flexible Intercept Access Point (IAP) mirroring supports lawful intercept (LI) mirroring on a per-subscriber, per-service, per-flow and per-network IAP basis
- Full content mirroring includes signaling, routing and switched data traffic
- Flexible packet size for mirrored LI traffic enables full or partial packets to be mirrored
- Local and remote LI mirroring
- Layer-2 and layer-3 services LI mirroring of both routed (layer 3) and switched (layer 2) services, which include IP VPN, Internet Enhanced Service (IES), virtual leased line (VLL), VPLS and CES
- Comprehensive set of LI mirroring-capable interfaces supports subscriber- and classification-based interception mirroring across a wide set of interfaces – supported interfaces include TDM, ATM, Frame Relay, SONET/SDH, Ethernet, VLAN, link aggregation group, and CES.
- Configurable QoS for mirrored LI traffic locally on the network element and across the network
- The data plane supports line-rate switching for the traffic aggregate – the total original and mirrored traffic

Management

- Alcatel-Lucent 5620 SAM provides extensive Fault, Configuration, Accounting, Performance, and Security (FCAPS)
- Alcatel-Lucent 5650 CPAM provides control plane management solution
- Alcatel-Lucent 5670 Reporting and Analysis Manager (RAM) enables network-wide, application-aware visibility and planning insight for TPSDA managed online services
- Fully featured industry CLI, including service CLI
- SSH v1/v2 and Telnet
- FTP, TFTP and SCP
- RADIUS (AAA)
- TACACS+
- SNMP v1, v2c and v3
- Local and remote port/service/flow mirroring
- Service assurance tools, including service ping, SDP ping, LSP ping, MAC ping and MAC traceroute
- Path maximum transmission unit (MTU) size measurement
- Round-trip delay, jitter, loss measurement (SAA)

Safety standards and compliance agency certifications

Safety

- EN 60590-1
- IEC 60950-1 CB Scheme
- CSA/UL 60950-1 NRTL
- FDA CDRH 21-CFR 1040
- EN 60825-1
- EN 60825-1/2
- IEC 60825-1
- IEC 60825-2

EMC

- ICES-003 Class A
- FCC Part 15 Class A
- EN 300 386
- EN 55022
- EN 55024
- EN 61000-4-2
- EN 61000-4-3
- EN 61000-4-4
- EN 61000-4-5
- EN 61000-4-6
- EN 61000-4-11
- IEC CISPR22
- AS/NZS CISPR 22

Immunity

- EN 61000-3-2 Power Line Harmonics
- EN 61000-3-3 Voltage Fluctuations and Flicker
- EN 61000-4-2 Electric Static Discharge
- EN 61000-4-3 Radiated Immunity
- EN 61000-4-4 EFT

- EN 61000-4-5 Surge
- EN 61000-4-6 Low Frequency Common Immunity
- EN 61000-4-11 Voltage Dips and Sags

Telecom

- Telcordia GR-253-CORE Issue 3
- IEEE 802.3 (Gigabit Ethernet, Ethernet)
- ANSI T1.105.06
- ANSI T1.105.09
- ANSI T1.403 (DS1)
- ANSI T1.404 (DS3)
- ITU-T G.957
- ITU-T G.825
- ITU-T G.824
- ITU-T G.823
- ITU-T G.813
- ITU-T G.707
- ITU-T G.703

Environmental

- ETS 300 019-1-1, Storage Tests, Class 1.2
- ETS 300 019-1-2, Transportation Tests, Class 2.3
- ETS 300 019-1-3, Operational Tests, Class 3.2
- ETS 300 019-2-4, pr A1 Seismic

Environmental specifications

- Operating temperature: 0°C to 40°C (32°F to 104°F)
- Relative humidity: 15% to 85% (operating)
- Relative humidity: 5% to 90% (non-condensing)
- Operating altitude: sea level to 3048 m (10,000 ft)

Electronic equipment devices

- WEEE
- RoHS
- R&TTE
- China CRoHS

Certifications

- Network Equipment Building System (NEBS) Level 3
  - ¬ Telcordia GR-63-CORE, Issue 4, June 2006
  - ¬ Telcordia GR-1089-CORE, Issue 3, March 2006
  - ¬ ATT-TP-76200
- CE

Standards compliance

- IEEE 802.1d (Bridging)
- IEEE 802.1p/Q (VLAN Tagging)
- IEEE 802.1s (Multiple Spanning Tree)
- IEEE 802.1w (Rapid Spanning Tree Protocol)
- IEEE 802.1x (Port-based Network Access Control)
- IEEE 802.1ad (Provider Bridges)
- IEEE 802.1ah (Provider Backbone Bridges)
- IEEE 802.1ag (Service Layer OAM)
- IEEE 802.3ah (Ethernet in the First Mile)
- IEEE 802.1ak (Multiple MAC Registration Protocol)
- IEEE 802.3 (10Base-T)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3ae (10Gbps Ethernet)
- IEEE 802.3ah (Ethernet OAM)
- IEEE 802.3u (100Base-TX)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (1000Base-SX/LX)

Protocol support

OSPF

- RFC 1765 OSPF Database Overflow
- RFC 2328 OSPF Version 2
- RFC 2370 Opaque LSA Support
- RFC 2740 OSPF for IPv6 (OSPFv3) draft-ietf-ospfospfv3- update-14.txt
- RFC 3101 OSPF NSSA Option
- RFC 3137 OSPF Stub Router Advertisement
- RFC 3623 Graceful OSPF Restart – GR Helper
- RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2
- RFC 4203 Shared Risk Link Group (SRLG) sub-TLV

BGP

- RFC 1397 BGP Default Route Advertisement
- RFC 1772 Application of BGP in the Internet
- RFC 1965 Confederations for BGP
- RFC 1997 BGP Communities Attribute
- RFC 2385 Protection of BGP Sessions via MD5
- RFC 2439 BGP Route Flap Dampening
- RFC 2547bis BGP/MPLS VPNs draft-ietf-idr-rfc2858bis-09.txt
- RFC 2918 Route Refresh Capability for BGP-4
- RFC 3392 Capabilities Advertisement with BGP4
- RFC 4271 BGP-4 (previously RFC 1771)
- RFC 4360 BGP Extended Communities Attribute

- RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs) (previously RFC 2547bis BGP/MPLS VPNs)
- RFC 4456 BGP Route Reflection: Alternative to Full-mesh IBGP (previously RFC 1966 and 2796)
- RFC 4724 Graceful Restart Mechanism for BGP – GR Helper
- RFC 4760 Multi-protocol Extensions for BGP (previously RFC 2858)
- RFC 5065 Confederations for BGP (obsoletes 3065)

IS-IS

- RFC 1142 OSI IS-IS Intra-domain Routing Protocol (ISO 10589)
- RFC 1195 Use of OSI IS-IS for routing in TCP/IP and dual environments
- RFC 2763 Dynamic Hostname Exchange for IS-IS
- RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
- RFC 2973 IS-IS Mesh Groups
- RFC 3373 Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
- RFC 3567 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
- RFC 3719 Recommendations for Interoperable Networks using IS-IS
- RFC 3784 Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)
- RFC 3787 Recommendations for Interoperable IP Networks
- RFC 3847 Restart Signaling for IS-IS – GR helper
- RFC 4205 for Shared Risk Link Group (SRLG) TLV
- draft-ietf-isis-igp-p2p-over-lan-05.txt

LDP

- RFC 3036 LDP Specification
- RFC 3037 LDP Applicability
- RFC 3478 Graceful Restart Mechanism for LDP – GR Helper
- draft-jork-ldp-igp-sync-03.txt

IPv6

- RFC 1981 Path MTU Discovery for IPv6
- RFC 2375 IPv6 Multicast Address Assignments
- RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
- RFC 2461 Neighbor Discovery for IPv6
- RFC 2462 IPv6 Stateless Address Auto configuration
- RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification
- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels
- RFC 2545 Use of BGP-4 Multiprotocol Extension for IPv6 Inter-Domain Routing
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
- RFC 2740 OSPF for IPv6
- RFC 3306 Unicast-Prefix-based IPv6 Multicast Addresses
- RFC 3315 Dynamic Host Configuration Protocol for IPv6
- RFC 3587 IPv6 Global Unicast Address Format
- RFC3590 Source Address Selection for the Multicast Listener Discovery (MLD) Protocol
- RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4291 IPv6 Addressing Architecture
- RFC 4659 BGP-MPLS IP Virtual Private Network (VPN) extension for IPv6 VPN
- RFC 5072 IP Version 6 over PPP
- draft-ietf-isis-ipv6-05.txt
- draft-ietf-isis-wg-multi-topology-xx.txt

Multicast

- RFC 1112 Host Extensions for IP Multicasting (Snooping)
- RFC 2236 Internet Group Management Protocol (Snooping)
- RFC 3376 Internet Group Management Protocol, Version 3 (Snooping)
- RFC 2362 Protocol Independent Multicast-Sparse Mode (PIM-SM)
- RFC 3618 Multicast Source Discovery Protocol (MSDP)
- RFC 3446 Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)

- RFC 4601 Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification
- RFC 4604 Using IGMPv3 and MLDv2 for Source-Specific Multicast
- RFC 4607 Source-Specific Multicast for IP
- RFC 4608 Source-Specific Protocol Independent Multicast in 232/8
- RFC 4610 Anycast-RP using Protocol Independent Multicast (PIM)
- draft-ietf-pim-sm-bsr-06.txt
- draft-rosen-vpn-mcast-08.txt
- draft-ietf-mboned-msdp-mib-01.txt

MPLS

- RFC 3031 MPLS Architecture
- RFC 3032 MPLS Label Stack Encoding (REV3443)
- RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
- RFC 4182 Removing a Restriction on the use of MPLS Explicit NULL

RIP

- RFC 1058 RIP Version 1
- RFC 2082 RIP-2 MD5 Authentication
- RFC 2453 RIP Version 2

RSVP-TE

- RFC 2430 A Provider Architecture DiffServ & TE
- RFC 2702 Requirements for Traffic Engineering over MPLS
- RFC 2747 RSVP Cryptographic Authentication
- RFC 3097 RSVP Cryptographic Authentication
- RFC 3209 Extensions to RSVP for Tunnels
- RFC 4090 Fast Reroute Extensions to RSVP-TE for LSP Tunnels

Differentiated services

- RFC 2474 Definition of the DS Field in the IPv4 and IPv6 Headers (Rev)
- RFC 2597 Assured Forwarding PHB Group (rev3260)
- RFC 2598 An Expedited Forwarding PHB
- RFC 3140 Per-Hop Behavior Identification Codes

TCP/IP

- RFC 768 UDP
- RFC 1350 The TFTP Protocol (Rev 2)
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 854 Telnet
- RFC 951 BootP (rev)
- RFC 1519 CIDR
- RFC 1542 Clarifications and Extensions for the Bootstrap Protocol
- RFC 1812 Requirements for IPv4 Routers
- RFC 2347 TFTP Option extension
- RFC 2328 TFTP Blocksize option
- RFC 2349 TFTP Timeout Interval and Transfer Size option
- RFC 2401 Security Architecture for Internet Protocol
- draft-ietf-bfd-mib-00.txt Bidirectional Forwarding Detection Management Information Base
- draft-ietf-bfd-base-05.txt Bidirectional Forwarding Detection
- draft-ietf-bfd-v4v6-1hop-06.txt BFD IPv4 and IPv6 (Single Hop)
- draft-ietf-bfd-multihop-06.txt BFD for Multi-hop Paths

VRRP

- RFC 2787 Definitions of Managed Objects for the Virtual Router Redundancy Protocol
- RFC 3768 Virtual Router Redundancy Protocol

PPP

- RFC 1332 PPP IPCP
- RFC 1377 PPP OSINLCP
- RFC 1638/2878 PPP BCP
- RFC 1661 PPP (rev RFC 2151)
- RFC 1662 PPP in HDLC-like Framing
- RFC 1989 PPP Link Quality Monitoring
- RFC 1990 The PPP Multilink Protocol (MP)
- RFC 2516 A Method for Transmitting PPP Over Ethernet
- RFC 2615 PPP over SONET/SDH
- RFC 2686 The Multi-Class Extension to Multi-Link PPP
- RFC 1877 PPP Internet Protocol Control Protocol Extensions for Name Server Addresses

Frame relay

- FRF.1.2 – PVC User-to-Network Interface (UNI) Implementation Agreement
- FRF.5 – Frame Relay/ATM PVC Network Interworking Implementation
- ANSI T1.617 Annex D, DSS1 – Signaling Specification for Frame Relay Bearer Service
- FRF2.2 – PVC Network-to-Network Interface (NNI) Implementation Agreement
- ITU-T Q.933 Annex A – Additional procedures for Permanent Virtual Connection (PVC) status management

ATM

- RFC 1626 Default IP MTU for Use over ATM AAL5
- RFC 2514 Definitions of Textual Conventions and OBJECT_IDENTITIES for ATM Management
- RFC 2515 Definition of Managed Objects for ATM Management
- RFC 2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5
- AF-TM-0121.000 Traffic Management Specification Version 4.1
- ITU-T Recommendation I.610 – B-ISDN operation and maintenance principles and functions version 11/95
- ITU-T Recommendation I.432.1 – B-ISDN user-network interface – Physical layer specification: General characteristics
- Telcordia GR-1248-CORE – Generic Requirements for Operations of ATM Network Elements (NEs), Issue 3
- Telcordia GR-1113-CORE – Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1
- AF-ILMI-0065.000 Integrated Local Management Interface (ILMI) Version 4.0
- AF-TM-0150.00 Addendum to Traffic Management v4.1 optional minimum desired cell rate indication for UBR
- AF-PHY-0086.001, Inverse Multiplexing for ATM (IMA) Specification Version 1.1

DHCP

- RFC 2131 Dynamic Host Configuration Protocol (REV)
- RFC 3046 DHCP Relay Agent Information Option (Option 82)
- RFC 1534 Interoperation between DHCP and BOOTP

VPLS

- RFC 4762 Virtual Private LAN Services Using LDP (previously draft-ietf-l2vpn-vpls-ldp-08.txt)
- draft-ietf-l2vpn-vpls-mcast-reqts-04.txt

Pseudowire

- RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3)
- RFC 4385 Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
- RFC 3916 Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)
- RFC 4717 Encapsulation Methods for Transport ATM over MPLS Networks (draft-ietf-pwe3-atmencap-10.txt)
- RFC 4816 PWE3 ATM Transparent Cell Transport Service (draft-ietf-pwe3-cell-transport-04.txt)
- RFC 4448 Encapsulation Methods for Transport of Ethernet over PLS Networks (draft-ietf-pwe3-ethernet-encap-11.txt)
- RFC 4619 Encapsulation Methods for Transport of Frame Relay over MPLS Networks (draft-ietfpwe3-frame-relay-07.txt)
- RFC 4446 IANA Allocations for PWE3
- RFC 4447 Pseudowire Setup and Maintenance Using LDP (draft-ietf-pwe3-control-protocol-17.txt)
- RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
- draft-ietf-l2vpn-vpws-iw-oam-02.txt
- draft-ietf-pwe3-oam-msg-map-05-txt
- draft-ietf-l2vpn-arp-mediation-04.txt
- draft-ietf-pwe3-ms-pw-arch-02.txt
- draft-ietf-pwe3-segmented-pw-05.txt
- draft-hart-pwe3-segmented-pw-vccv-02.txt
- draft-muley-dutta-pwe3-redundancy-bit-02.txt
- draft-muley-pwe3-redundancy-02.txt
- MFA Forum 9.0.0 The Use of Virtual Trunks for ATM/MPLS Control Plane Interworking
- MFA Forum 12.0.0 Multiservice Interworking – Ethernet over MPLS
- MFA forum 13.0.0 Fault Management for Multiservice Interworking v1.0
- MFA Forum 16.0.0 Multiservice Interworking – IP over MPLS

ANCP/L2CP

- draft-ietf-ancp-framework-01.txt

Circuit emulation

- RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
- RFC 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)
- MEF-8 Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks, October 2004
- draft-ietf-pwe3-tdm-control-protocol-extensi-02.txt

SONET/SDH

- Telcordia GR-253-CORE SONET Transport Systems: Common Generic Criteria, Issue 3, September 2000
- ITU-T G.841 Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum 1 issued in July 2002
- Telcordia GR-253-CORE - SONET Transport Systems: Common Generic Criteria, Issue 3, September 2000

RADIUS

- RFC 2865 Remote Authentication Dial In User Service
- RFC 2866 RADIUS Accounting

SSH

- draft-ietf-secsh-architecture.txt SSH Protocol Architecture
- draft-ietf-secsh-userauth.txt SSH Authentication Protocol
- draft-ietf-secsh-transport.txt SSH Transport Layer Protocol
- draft-ietf-secsh-connection.txt SSH Connection Protocol
- draft-ietf-secsh-newmodes.txt SSH Transport Layer Encryption Modes

TACACS+

- draft-grant-tacacs-02.txt

Network management

- ITU-T X.721: Information technology – OSI - Structure of Management Information
- ITU-T X.734: Information technology – OSI - Systems Management: Event Report Management Function
- ITU-T M.3100/3120 Equipment and Connection Models
- TMF 509/613 Network Connectivity Model
- RFC 1157 SNMPv1
- RFC 1215 A Convention for Defining Traps for use with the SNMP
- RFC 1657 BGP4-MIB
- RFC 1724 RIPv2-MIB
- RFC 1850 OSPF-MIB
- RFC 1907 SNMPv2-MIB
- RFC 2011 IP-MIB
- RFC 2012 TCP-MIB
- RFC 2013 UDP-MIB
- RFC 2096 IP-FORWARD-MIB
- RFC 2138 RADIUS
- RFC 2206 RSVP-MIB
- RFC 2452 IPv6 Management Information Base for the Transmission Control Protocol
- RFC 2454 IPv6 Management Information Base for the User Datagram Protocol
- RFC 2465 Management Information Base for IPv6: Textual Conventions and General Group
- RFC 2558 SONET-MIB
- RFC 2571 SNMP-FRAMEWORKMIB
- RFC 2572 SNMP-MPD-MIB
- RFC 2573 SNMP-TARGET-&-NOTIFICATION-MIB
- RFC 2574 SNMP-USER-BASED-SMMIB
- RFC 2575 SNMP-VIEW-BASEDACM-MIB
- RFC 2576 SNMP-COMMUNITY-MIB
- RFC 2665 EtherLike-MIB
- RFC 2819 RMON-MIB
- RFC 2863 IF-MIB
- RFC 2864 INVERTED-STACK-MIB
- RFC 2987 VRRP-MIB
- RFC 3014 NOTIFICATION-LOGMIB
- RFC 3019 IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol
- RFC 3164 Syslog
- RFC 3273 HCRMON-MIB
- RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
- RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413 Simple Network Management Protocol (SNMP) Applications

- RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 3418 SNMP MIB
- draft-ietf-disman-alarm-mib-04.txt
- draft-ietf-ospf-mib-update-04.txt
- draft-ietf-mpls-lsr-mib-06.txt
- draft-ietf-mpls-te-mib-04.txt
- draft-ietf-mpls-ldp-mib-07.txt
- draft-ietf-isis-wg-mib-05.txt
- IANA-IFType-MIB
- IEEE8023-LAG-MIB
- Plus support for an extensive array of proprietary protocols

7450 Ethernet Service Switch

7450 ESS-6

7450 ESS-1

The **Alcatel-Lucent 7450 Ethernet Service Switch** (ESS) is a feature-rich MPLS-based switch/router designed to aggregate and switch voice, video and data traffic in mission-critical enterprise and service provider networks. It is ideally suited as a backbone and aggregation node in a network providing layer-2 connectivity for multiple locations and providing access to the layer-3 WAN access points.

The 7450 ESS overcomes the limitations imposed by traditional Ethernet switches with features like Hierarchical QoS (H-QoS) and MPLS resiliency. It sets a new market standard for the delivery of Ethernet business services such as Virtual Private Wire Service (VPWS/VLL) and Virtual Private LAN Service (VPLS).

The scalable performance and port density provided by the 7450 ESS is available in five chassis configurations including the 12-slot 7450 ESS-12, 7-slot 7450 ESS-7, 6-slot 7450 ESS-6, 6-slot 7450 ESS-6v, and 1-slot 7450 ESS-1.

KEY SELLING POINTS

- **Flexible:** H-QoS enables network managers to support users that require different service classes
- **Configurable:** Product sizes and densities are available to match any requirements
- **Dependable:** Improved network stability, scalability, availability and performance when compared to existing layer 2/3 Ethernet switches through a combination of MPLS, bridged Ethernet, stacked VLANs and Spanning Tree Protocols
- **Upgrade path:** Inherent product scalability coupled with a programmable architecture ensures forklift-free upgrades and reduces truck rolls (no technician deployment)
- **Fault tolerant:** Diagnostics and mirroring are implemented through built-in end-to-end Ethernet OA&M tools
- **Fast deployment:** Ethernet services with advanced provisioning tools reduces the time from installation to network operation

KEY FEATURES

- **Service-oriented:** Supports a service-oriented architecture (SOA) by using service level agreement (SLA)-based Ethernet services with filtering, shaping and quality of service (QoS) on a per-service basis, while scaling to support tens of thousands of users

- → **Virtualization:** Deploys IETF implementations of VPWS and VPLS
- → **High availability:** Includes nonstop services, nonstop routing, MPLS, Fast Reroute and in-service software upgrade (ISSU) to guarantee network uptime
- → **Flexible billing:** Deterministic, tiered or usage-based billing options
- → **Small footprint:** Leads the Industry in rack density (by 2-3 times per rack) when compared to competing layer-2/layer-3 Ethernet switches with 10 Gb/s architecture
- → **Future-proof:** Enables quick and painless adaptation and upgrades to new and evolving standards using programmable fast path

TECHNICAL INFORMATION

Synchronous Ethernet (Sync-E) standards support

- ITU-T G.8261 - g.pactiming – Timing and synchronization aspects of packet networks
- ITU-T G.8262 - g.paclock – Timing characteristics of Ethernet equipment slave clock (EEC)
- ITU-T G.8263 - g.paclock.bis – Synchronous status messaging (SSM) echo support
- ITU-T G.8264 - g.pacmod – Distribution of timing through packet networks

Safety standards and compliance agency certifications

Safety

- EN 60590-1
- IEC 60950-1CB Scheme
- CSA/UL 60950-1 NRTL
- FDA CDRH 21-CFR 1040
- EN 60825-1
- EN 60825-1/2
- IEC 60825-1
- IEC 60825-2

EMC

- ICES-003 Class A
- FCC Part 15 Class A
- EN 300 386
- EN 55022
- EN 55024
- EN 61000-4-2
- EN 61000-4-3
- EN 61000-4-4
- EN 61000-4-5
- EN 61000-4-6
- EN 61000-4-11
- IEC CISPR22
- AS/NZS CISPR 22

Immunity

- EN 61000-3-2 Power Line Harmonics
- EN 61000-3-3 Voltage Fluctuations and Flicker
- EN 61000-4-2 Electric Static Discharge
- EN 61000-4-3 Radiated Immunity
- EN 61000-4-4 EFT
- EN 61000-4-5 Surge
- EN 61000-4-6 Low Frequency Common
- EN 61000-4-11 Voltage Dips and Sags

Telecom

- Telcordia GR-253-CORE Issue 3
- IEEE 802.3 (Gigabit Ethernet, Ethernet)
- ANSI T1.105.03
- ANSI T1.105.06
- ANSI T1.105.09
- ANSI T1.403 (DS1)
- ANSI T1.404 (DS3)
- ITU-T G.957
- ITU-T G.825
- ITU-T G.824
- ITU-T G.823
- ITU-T G.813
- ITU-T G.707
- ITU-T G.703

Environmental

- ETS 300 019-1-1, Storage Tests, Class 1.2
- ETS 300 019-1-2, Transportation Tests, Class 2.3
- ETS 300 019-1-3, Operational Tests, Class 3.2
- ETS 300 019-2-4, per A1 Seismic

Environmental specifications

- Operating temperature: 0°C to 40°C (32°F to 104°F)
- Relative humidity: 15% to 85% (non-condensing)
- Operating altitude: sea level to 3048 m (10,000 ft)

Electronic equipment devices

- WEEE
- RoHS
- R&TTE
- China CRoHS

Certifications

- Network Equipment Building System (NEBS) Level 3
  - ¬ Telcordia GR-63-CORE, Issue 4, June 2006
  - ¬ Telcordia GR-1089-CORE, Issue 3, March 2006
  - ¬ ATT-TP-76200
- CE

Standards compliance

- IEEE 802.1ab-REV/D3 (Station and Media Access Control Connectivity Discovery)
- IEEE 802.1d (Bridging)
- IEEE 802.1p/Q (VLAN Tagging)
- IEEE 802.1s (Multiple Spanning Tree)
- IEEE 802.1w (Rapid Spanning Tree Protocol)
- IEEE 802.1x (Port-based Network Access Control)
- IEEE 802.1ad (Provider Bridges)
- IEEE 802.1ah (Provider Backbone Bridges)
- IEEE 802.1ag (Service Layer OAM)
- IEEE 802.3ah (Ethernet in the First Mile)
- IEEE 802.1ak (Multiple MAC Registration Protocol)
- IEEE 802.3 (10Base-T)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3ae (10Gbps Ethernet)
- IEEE 802.3ah (Ethernet OAM)
- IEEE 802.3u (100Base-TX)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (1000Base-SX/LX)
- ITU-T Y.1731 (OAM functions and mechanisms for Ethernet-based networks)

Protocol support

OSPF

- RFC 1765 OSPF Database Overflow
- RFC 2328 OSPF Version 2
- RFC 2370 Opaque LSA Support
- RFC 3101 OSPF NSSA Option
- RFC 3137 OSPF Stub Router Advertisement
- RFC 3623 Graceful OSPF Restart – GR helper
- RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2
- RFC 4203 for Shared Risk Link Group (SRLG) sub-TLV

BGP

- RFC 1397 BGP Default Route Advertisement
- RFC 1772 Application of BGP in the Internet
- RFC 1965 Confederations for BGP
- RFC 1997 BGP Communities Attribute
- RFC 2385 Protection of BGP Sessions via MD5
- RFC 2439 BGP Route Flap Dampening
- RFC 2547bis BGP/MPLS VPNs
- RFC 4760 Multiprotocol Extensions for BGP-4
- RFC 2918 Route Refresh Capability for BGP-4
- RFC 3392 Capabilities Advertisement with BGP4
- RFC 4271 BGP-4 (previously RFC 1771)
- RFC 4456 BGP Route Reflection: Alternative to Full-mesh IBGP (previously RFC 1966 & 2796)
- RFC 4724 Graceful Restart Mechanism for BGP – GR Helper
- RFC 4760 Multi-protocol Extensions for BGP
- RFC 4893 BGP Support for Four-octet AS Number Space
- RFC 5065 Confederations for BGP (obsoletes 3065)

IS-IS

- RFC 1142 OSI IS-IS Intra-domain Routing Protocol (ISO 10589)
- RFC 1195 Use of OSI IS-IS for routing in TCP/IP & dual environments
- RFC 2763 Dynamic Hostname Exchange for IS-IS
- RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
- RFC 2973 IS-IS Mesh Groups
- RFC 3373 Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies

- RFC 3567 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
- RFC 3719 Recommendations for Interoperable Networks using IS-IS
- RFC 3784 Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)
- RFC 3787 Recommendations for Interoperable IP Networks
- RFC 3847 Restart Signaling for IS-IS – GR Helper
- RFC 4205 IS-IS Extensions in Support of GMPLS for Shared Risk Link Group (SRLG) TLV
- RFC 5309 Point-to-Point Operation over LAN in Link State Routing Protocols

LDP

- RFC 3036 LDP Specification
- RFC 3037 LDP Applicability
- RFC 3478 Graceful Restart Mechanism for LDP – GR Helper
- RFC 5283 LDP Extension for Inter-Area LSP
- draft-jork-ldp-igp-sync-03

MPLS

- RFC 3031 MPLS Architecture
- RFC 3032 MPLS Label Stack Encoding (REV3443)
- RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
- RFC 4182 Removing a Restriction on the use of MPLS Explicit NULL

RIP

- RFC 1058 RI P Version 1
- RFC 2082 RIP-2 MD5 Authentication
- RFC 2453 RI P Version 2

RSVP-TE

- RFC 2430 A Provider Architecture DiffServ & TE
- RFC 2702 Requirements for Traffic Engineering over MPLS
- RFC2747 RSVP Cryptographic Authentication
- RFC3097 RSVP Cryptographic Authentication
- RFC 3209 Extensions to RSVP for Tunnels
- RFC 3564 Requirements for Diff-Serv-aware TE
- RFC 4090 Fast reroute Extensions to RSVP-TE for LSP Tunnels
- RFC 4124 Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering
- RFC 4125 Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering
- draft-ietf-mpls-soft-preemption-14.txt MPLS Traffic Engineering Soft Preemption
- draft-ietf-ccamp-mpls-graceful-shutdown-06.txt Graceful Shutdown in GMPLS Traffic Engineering Networks

Differentiated services

- RFC 2474 Definition of the DS Field the IPv4 and IPv6 Headers (Rev)
- RFC 2597 Assured Forwarding PHB Group (rev3260)
- RFC 2598 An Expedited Forwarding PHB
- RFC 3140 Per-Hop Behavior Identification Codes

TCP/IP

- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 854 Telnet
- RFC 951 BootP
- RFC 1350 The TFTP Protocol
- RFC 1519 CIDR
- RFC 1542 Clarifications and Extensions for the Bootstrap Protocol
- RFC 1812 Requirements for IPv4 Routers
- RFC 2347 TFTP Option Extension
- RFC 2328 TFTP Blocksize Option
- RFC 2349 TFTP Timeout Interval and Transfer Size option
- RFC 2401 Security Architecture for Internet Protocol
- draft-ietf-bfd-mib-00.txt Bidirectional Forwarding Detection Management Information Base
- draft-ietf-bfd-base-05.txt Bidirectional Forwarding Detection
- draft-ietf-bfd-v4v6-1hop-06.txt BFD IPv4 and IPv6 (Single Hop)
- draft-ietf-bfd-multihop-06.txt BFD for Multihop Paths

VRRP

- RFC 2787 Definitions of Managed Objects for the Virtual Router Redundancy Protocol
- RFC 3768 Virtual Router Redundancy Protocol

PPP

- RFC 1332 PPP IPCP
- RFC 1377 PPP OSINLCP
- RFC 1638/2878 PPP BCP
- RFC 1661 PPP (rev RFC2151)
- RFC 1662 PPP in HDLC-like Framing
- RFC 1877 PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
- RFC 1989 PPP Link Quality Monitoring
- RFC 1990 The PPP Multilink Protocol (MP)
- RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
- RFC 2516 A Method for Transmitting PPP Over Ethernet
- RFC 2615 PPP over SONET/SDH

DHCP

- RFC 2131 Dynamic Host Configuration Protocol (REV)
- RFC 3046 DHCP Relay Agent Information Option (Option 82)
- RFC 1534 Interoperation between DHCP and BOOTP

VPLS

- RFC 4762 Virtual Private LAN Services Using LDP (previously draft-ietf-l2vpn-vpls-ldp-08.txt)
- draft-ietf-l2vpn-vpls-mcast-reqts-04.txt

PSEUDOWIRE

- RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3)
- RFC 3916 Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)
- RFC 4385 Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
- RFC 4446 IANA Allocations for PWE3
- RFC 4447 Pseudowire Setup and Maintenance Using LDP (draft-ietf-pwe3-control-protocol-17.txt)
- RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks (draft-ietf-pwe3-ethernet-encap-11.txt)
- RFC 4717 Encapsulation Methods for Transport ATM over MPLS Networks (draft-ietf-pwe3-atmencap-10.txt)
- RFC 4816 PWE3 ATM Transparent Cell Transport Service (draft-ietf-pwe3-cell-transport-04.txt)
- RFC 4619 Encapsulation Methods for Transport of Frame Relay over MPLS Networks (draft-ietfpwe3-frame-relay-07.txt)
- RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
- draft-ietf-l2vpn-vpws-iw-oam-02.txt
- draft-ietf-pwe3-oam-msg-map-05-txt
- draft-ietf-l2vpn-arp-mediation-04.txt
- draft-ietf-pwe3-ms-pw-arch-05.txt
- draft-ietf-pwe3-segmented-pw-11.txt
- draft-hart-pwe3-segmented-pw-vccv-02.txt
- draft-muley-dutta-pwe3-redundancy-bit-02.txt
- draft-muley-pwe3-redundancy-02.txt
- MFA Forum 9.0.0 The Use of Virtual trunks for ATM/MPLS Control Plane Interworking
- MFA Forum 12.0.0 Multiservice Interworking – Ethernet over MPLS
- MFA forum 13.0.0 Fault Management for Multiservice Interworking v1.0
- MFA Forum 16.0.0 Multiservice Interworking – IP over MPLS

ANCP/L2CP

- draft-ietf-ancp-framework-01.txt
- draft-ietf-ancp-protocol-00.txt

SONET/SDH

- GR-253-CORE SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000
- ITU-T G.841 Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum 1 issued in July 2002

RADIUS

- RFC 2865 Remote Authentication Dial In User Service
- RFC 2866 RADIUS Accounting

SSH

- draft-ietf-secsh-architecture.txt SSH Protocol Architecture
- draft-ietf-secsh-userauth.txt SSH Authentication Protocol
- draft-ietf-secsh-transport.txt SSH Transport Layer Protocol
- draft-ietf-secsh-connection.txt SSH Connection Protocol
- draft-ietf-secsh-newmodes.txt SSH Transport Layer Encryption Modes

TACACS+

- draft-grant-tacacs-02.txt

Network management

- ITU-T X.721: Information technology – OSI - Structure of Management Information
- ITU-T X.734: Information technology – OSI - Systems Management: Event Report Management Function
- ITU-T M.3100/3120 Equipment and Connection Models
- TMF 509/613 Network Connectivity Model
- RFC 1157 SNMPv1
- RFC 1215 A Convention for Defining Traps for use with the SNMP
- RFC 1657 BGP4-MIB
- RFC 1724 RIPv2-MIB
- RFC 1850 OSPF-MIB
- RFC 1907 SNMPv2-MIB
- RFC 2011 IP-MIB
- RFC 2012 TCP-MIB
- RFC 2013 UDP-MIB
- RFC 2096 IP-FORWARD-MIB
- RFC 2138 RADIUS
- RFC 2206 RSVP-MIB
- RFC 2558 SONET-MIB
- RFC 2571 SNMP-FRAMEWORKMIB
- RFC 2572 SNMP-MPD-MIB
- RFC 2573 SNMP-TARGET-&-NOTIFICATION-MIB
- RFC 2574 SNMP-USER-BASED-SMMIB
- RFC 2575 SNMP-VIEW-BASED-ACM-MIB
- RFC 2576 SNMP-COMMUNITY-MIB
- RFC 2665 EtherLike-MIB
- RFC 2819 RMON-MIB
- RFC 2863 IF-MIB
- RFC 2864 INVERTED-STACK-MIB
- RFC 2987 VRRP-MIB
- RFC 3014 NOTIFICATION-LOG-MIB
- RFC 3164 Syslog
- RFC 3273 HCRMON-MIB
- RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
- RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413 Simple Network Management Protocol (SNMP) Applications
- RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 3418 SNMP MIB
- draft-ietf-disman-alarm-mib-04.txt
- draft-ietf-ospf-mib-update-04.txt
- draft-ietf-mpls-lsr-mib-06.txt
- draft-ietf-mpls-te-mib-04.txt
- draft-ietf-mpls-ldp-mib-07.txt
- draft-ietf-isis-wg-mib-05.txt
- IANA-IFType-MIB
- IEEE8023-LAG-MIB
- Plus support for a complete array of proprietary MIBs

Management solutions product range

Alcatel-Lucent has a wide portfolio of management infrastructure products that run on industry-standard operating systems and provide network management for LANs, WLANs, WANs and MANs, as well as comprehensive service level management and IP address management.

Our management product range includes:

- → LAN and LAN switch management system, designed to manage the OmniSwitch™ series, yet open to other SNMP-manageable elements
- → WLAN management system, designed to manage the OmniAccess WLAN series, yet open to managing other vendors' Wi-Fi® systems
- → MAN management system, designed to manage the Service Router, Ethernet Service Switch and OmniSwitch series, yet open to manage other SNMP-manageable elements
- → Service level management system, designed to provide comprehensive performance reporting for network infrastructure, IP telephony, call center, applications and end systems.
- → IP address management system, not only for clear IP address management, but also to provide DNS, ENUM, NTP and TFTP services

OmniVista 2500

OmniVista 2500 Network Management System

The **Alcatel-Lucent OmniVista™ 2500 Network Management System** (NMS) provides a comprehensive set of components and tools that simplify the management of Alcatel-Lucent Enterprise portfolio and third-party networking devices.

The OmniVista 2500 NMS allows managers to monitor network activity, configure and troubleshoot each device, and provision and manage an entire network from a single platform. In a single application, the OmniVista 2500 NMS reduces the complex deployment and administration of Alcatel-Lucent Enterprise solutions — from network management to network security.

The OmniVista 2500 NMS has a true client/server architecture, allowing multiple users to access its services simultaneously either through a Java-based client or through web browser applications.

KEY SELLING POINTS

- **Unified cohesive management and network-wide visibility:** Provides a common GUI with which network administrators can perform monitoring and configuration operations across multiple devices, using a single touch. The intuitive GUI also provides an extensive set of configuration operations and reporting capabilities for all network activities and events.
- **Scalable architecture:** Provides simultaneous client sessions based on an extensible architecture suitable for large infrastructures, allowing the OmniVista 2500 NMS environment to be tailored to the user's network and budget needs.
- **Bulk operations:** Manages device configuration and standardization through CLI scripting automation. The Resource Manager provides device configuration backup and restore automation for disaster recovery, as well as firmware and software upload for version management control.
- **Role-based management with User Network Profile configuration:** Includes the Access Guardian, the OmniVista 2500 NMS component for end-user network security management including authentication, host integrity compliance check and resource access definition.
- **Policy-based approach for network access control and QoS:** OneTouch™ and Expert modes are available for creating, distributing and updating policies from a centralized framework, across multiples switches.

- **Centralized control of switch administration access rights and network administrator credentials:** Offers OneTouch setup of user login, password and partitioned management (user credentials and access rights).
- **Network quarantine:** Eliminates threats and security risks from misbehaving devices by providing automation for quarantine and isolation. The 2500 NMS Quarantine Manager™ simplifies intrusion detection and notification by providing Traffic Anomaly Detection configuration for visibility of network behavior anomalies. It simplifies enforcement and definition of a network security perimeter.

KEY FEATURES

- Centralized, cohesive network operations and security management with a common, intuitive look and feel
- Network-wide topology view, including contextual integration with element manager
- Alarms monitoring and notification with advanced filtering capabilities and smart responders for fast notification and remediation
- Centralized and automated network device configuration simplifies provisioning with CLI scripting automation
- Location-based troubleshooting tools for quick network connectivity problem resolution
- Device configuration backup/restore and software version management for configuration management operations
- Policy-based access control list (ACL) and quality of service (QoS) for voice and data performance optimization and network resource access enforcement with simplified or expert modes
- Centralized control of network device administration access rights and network administrator credentials
- Global end-user network profile and security configuration for role-based access to resources and management of credentials
- Template-like approach for simplified configuration of Traffic Anomaly Detection
- Network quarantine for security perimeter enforcement to automatically contain potential threats
- Northbound interface/web services interfaces for easy application integration with IT dashboard applications developed in-house

TECHNICAL INFORMATION

OmniVista 2500 NMS Server

Supported platforms and operating system

- Microsoft® Windows® 2008 (32-bit)
- Sun™ Solaris™ 2.10 (32-bit and 64-bit)
- Red Hat® Enterprise Linux® ES
- Novell® SUSE™ Linux (32-bit and 64-bit)

Minimum CPU and disk space

- Intel® Pentium® 4 with 2 GHz or higher (for Windows and Linux)
- Sun UltraSPARC® 5 processor or higher (Sun Solaris)

Minimum RAM and disk space

- 2 GB RAM or higher
- 5 GB free disk space
- OmniVista 2500 NMS Client

Supported platforms and operating systems

- Microsoft Windows Vista® Business edition
- Microsoft Windows XP Pro
- Sun Solaris 2.10 (32-bit and 64-bit)
- Red Hat Enterprise Linux ES
- Novell SUSE (32-bit and 64-bit)

Supported web browsers

- Microsoft Internet Explorer® 7.0
- Mozilla® Firefox® 3.5

Minimum CPU and disk space

- Intel Pentium 4 with 2 GHz or higher (for Windows and Linux)
- Sun UltraSPARC 5 processor or higher (Sun Solaris)

Minimum RAM and disk space

- 2 GB RAM or higher
- 5 GB free disk space

5620 Service Aware Manager

5620 Service Aware Manager

The **Alcatel-Lucent 5620 Service Aware Manager** (SAM) takes enterprises and service providers well beyond the traditional boundaries of element, network and service management. It enables unified, end-to-end management of IP/MPLS and Carrier Ethernet networks and the services they deliver. Rapid provisioning reduces time-to-market and increases flexibility when launching new services. Proactive troubleshooting helps resolve problems before they affect users.

The 5620 SAM offers a modular, extensible and scalable architecture that can be customized to fit specific operational environments. It consists of four modules that provide:

- → Element management for traditional FCAPS functionality
- → Network infrastructure configuration, service provisioning, scripting and customer management
- → Service assurance including physical, network and service topology views and OA&M service-diagnostics tools
- → Operations Support System (OSS) integration with external applications

Enterprises and service providers can further enhance the 5620 SAM's management capabilities with the Alcatel-Lucent 5650 Control Plane Assurance Manager (CPAM), Alcatel-Lucent 5670 Reporting and Analysis Manager (RAM), Alcatel-Lucent custom service portals, and pre-certified OSS partner application integrations.

KEY SELLING POINTS

- → Introduce new services and technologies rapidly with accelerated and reliable provisioning that minimizes the risk of misconfiguration and reduces time-to-market
- → Prevent potential service-affecting problems proactively before they impact users
- → Resolve problems quickly and simply
- → Collect statistics efficiently for flexible billing and service level agreement (SLA) options
- → Provide unmatched operational scalability to support network and service growth
- → Increase productivity and flexibility with a management solution that easily adapts to allow cost-effective integration into the existing operational environment, enhancing workflows and processes

KEY FEATURES

- → Easy-to-use GUI that accelerates configuration and provisioning tasks. Automation further accelerates tasks and minimizes the time and costs associated with the errors that commonly occur when a command line interface is used.
- → Common provisioning for layer-2 and layer-3 services to reduce the cost of delivering different service types
- → Extensive service assurance capabilities that allow proactive identification of problems before they affect customers
- → Powerful troubleshooting tools that help to quickly pinpoint the root cause of problems to speed resolution
- → Templates that allow simplified integration with existing processes and workflows
- → Open interfaces that enable integration with custom web portals, Operations Support Systems (OSSs) and Business Support Systems (BSSs)

TECHNICAL INFORMATION

Operating environment

The Alcatel-Lucent 5620 SAM, Release 7.0, operates on:

- Sun Solaris™ 10 x 86 for Sun Microsystems AMD-based platforms (preferred platform)
- Sun Solaris 10 for Sun Microsystems SPARC® platforms
- Microsoft® Windows® 2000/2003/ XP Professional (32-bit) operating system
- Microsoft Windows Vista® Business and Ultimate (32-bit editions) for 5620 SAM client only

Contact your Alcatel-Lucent representative for 5620 SAM platform sizing recommendations.

VitalSuite

VitalSuite

The **Alcatel-Lucent VitalSuite™ Performance Management Software** is an award-winning multivendor, multitechnology performance management solution. It comprises three advanced software modules: Alcatel-Lucent VitalNet Network Performance Management Software, VitalSuite Real Time Event Analysis Software for network infrastructure monitoring with advanced real-time thresholds and VitalART™ for wizard-based customizable report generation. This comprehensive, fully integrated solution is a cost-effective package that provides both historical and near-real-time views into everything from complex contact center transactions to VoIP traffic to mission-critical applications and network resources. It proactively monitors, measures and optimizes performance at every level of IT operations.

The Alcatel-Lucent VitalSuite Performance Management Software solution offers three advanced modules:

Alcatel-Lucent VitalApps Application Performance Management Software and Real Time Fault Detecting and Troubleshooting Software monitors and manages application performance for business-critical applications. It proactively gives network-wide real-time visibility for tracking, analyzing and predicting the behavior of network-based applications such as e-mail, web server, DNS, and in-house applications per user transaction. Application managers can monitor traffic volumes, application transaction response time and other critical data for evaluating performance and ensuring maximum availability. With drill-down capabilities, operations staff can quickly identity and solve issues.

Alcatel-Lucent VitalNet Network Performance Management Software/VitalSuite Real Time Event Analysis Software provides critical network information necessary to preempt problems, optimize resources and plan for maximum return on network investments. For your multivendor, multifunction network devices, VitalNet Network Performance Management Software/VitalSuite Real Time Event Analysis Software provides:

- → Regular updates of network monitoring through auto-discovery of network resources, minimizing need for administrator to perform manual updates to maintain a complete network view
- → Centralized visibility to help monitor, analyze, manage and predict the network infrastructure (for example, from routers, switches, servers to VoIP and Genesys) to help benchmark network behavior, efficiently troubleshoot network problems and optimize performance of network devices
- → Portal capability to restrict information access for the entire network or limited network view for a single user (driven by user profile).

- → Hourly, daily, weekly, and monthly performance and planning data in text and graphical reports for trending and capacity planning
- → Advanced VoIP solutions that address the complete deployment cycle, from readiness assessment, to pre-production testing, to production rollout and tuning. VitalNet (VoIP Agent) can generate tests calls and measure VoIP performance as well as help baseline performance and proactively threshold then troubleshoot VoIP problems.
- → Basic and advanced thresholding and alerting capabilities on performance data to help identify network resources that have exceeded defined network service levels

Alcatel-Lucent VitalART software is a comprehensive web-based tool that enables you to generate advanced custom presentation-quality reports and graphs by extracting monitored data from your VitalNet and VitalApps Performance Management Software products. With VitalART, administrators no longer need to export files to complex and expensive commercial reporting packages. The flexible formatting power and user-friendly scheduling capabilities of VitalART allow easy transformation of application and network performance data to custom reports with user-defined metrics in tables and charts to help increase IT staff productivity.

VitalSuite is a sophisticated information delivery system that allows IT organizations to provide internal users and/or customers with secure views into the quality of services they receive. The VitalSuite web-based portal lets you create and display virtually any aspect of network and application performance: wireless, LAN, WAN, server, ATM, VoIP or Frame Relay quality indices; top applications and events; even specific e-business transactions such as order entry or credit authorization. Everyone, from executives to engineers, can create unique displays tailored to their network operational model and individual needs.

In conclusion, VitalSuite provides the critical network information necessary to preempt problems, optimize resources and plan for maximum return on network investments. This market-leading management solution provides near-real-time, end-to-end, web-based visibility into geographically dispersed, multivendor, multi-technology converged infrastructure. It enables IT managers to monitor, analyze, manage and predict service performance from a single centralized location.

KEY SELLING POINTS

- → Access at-a-glance personalized performance data that is aligned with an IT operational model with multivendor and multitechnology support
- → Preempt potential network problems with real-time network-wide visibility
  - ¬ Network-wide visibility: Monitor performance across the entire IT infrastructure via maps, paths, domains, groups, services

- → Simplify analysis and planning for every organizational level with drill-down reports
- → Proactively track performance problems to their source, maximizing uptime
- → Increase VoIP quality by efficiently identifying the root cause using advanced VoIP performance monitoring solution with capability to generate VoIP traffic
- → Monitor application and network infrastructure environment using unique Genesys™ Contact Center with specialized data collection from Genesys servers
- → Strengthen support of critical business transactions with applications performance monitoring
  - ¬ Enhanced end-user experience: Access real-time data to identify performance issues before they affect users
- → Protect network investments with enhanced operational performance
- → Realize rapid ROI with immediate system deployment and access to performance data
  - ¬ Fast, easy deployment: Help network managers identify potential trouble spots, verify SLA compliance and optimize resource utilization
- → Protect investment: Use built-in toolkit to speed integration with existing management systems and emerging technologies
- → Implement carrier-class management capabilities priced to suit enterprise IT budgets – cost-effective price to performance

KEY FEATURES

- → **Industry-leading scalability:** VitalSuite can scale from single-server deployments to monitor small networks to multi-server deployments that monitor network and service quality across today's largest environments. Customers can start small and grow as needed.
- → **Comprehensive multivendor VoIP performance monitoring:** Includes collection and analysis of individual VoIP call records from leading VoIP platforms including Avaya, Cisco, and Alcatel-Lucent (streaming call records from OmniPCX™). VitalSuite also supports active VoIP monitoring via synthetic VoIP transactions using the VitalSuite VoIP Agent capability, or Cisco IP SLA operations.
- → Centralized application and network visibility via web-based GUI with a single administration interface for user accounts administration, domain and group definition, and threshold definitions. VitalSuite heat charts provide an intuitive, at-a-glance indicator of application and/or network performance problems with efficient drill-downs to additional performance details. Customized reports provide the ability to view both application and network data in the same report.

VitalApps

- **Embedded Alcatel-Lucent VitalAgent™ client software:** Pinpoints application-related problems on desktops, notebooks and servers
- **Patented passive flow analysis:** Provides real-time demarcation of every application transaction by client, network and server time
- **VPN tunnel monitoring and reporting:** Tracks tunnel setup and usage time and generates tunnel-problem alerts
- **Powerful fault detection and management:** Unique heat charts and summary reports isolate trouble spots at a glance (by domain and group)
- **Centralized alarm console:** Proactively receives alarms for application and network faults and performance shortfalls
- **End-to-end application performance monitoring:** Provides end-user perspective using active and passive monitoring. Mid-Tier Agent gives insight concerning incoming and outgoing traffic from the server.
- **Extensibility:** Provides the ability to add support for in-house applications
- **Events forwarding:** Allows event reports to be automatically generated and forwarded to popular industry-leading trouble ticketing system or fault management system for further actions
- **Remote diagnostics:** Allows administrator to visit remote desktops to see problems exactly as end users see them

VitalNet/VitalSuite Real Time Event Analysis Software

- **Flexible, multivendor and multitechnology support:** Monitors diverse resource types and more than 600 devices from more then 50 different vendors including the Alcatel-Lucent OmniPCX, Cisco and Avaya IP-PBX deployments
- **Advanced VoIP solution:** Extensive VoIP monitoring: For example OmniPCX streaming call record data collection, VoIP traffic generation, and ability to provision detailed mean opinion score (MOS) parameters to calculate MOS
- **Contact center monitoring:** Provides contact center infrastructure monitoring (VoIP, Genesys servers, and routers/switches)
- **Versatile reporting:** Provides real-time statistics for efficient, on-target troubleshooting, continuous operations data for monitoring service quality, high-level summaries and long-term trends for capacity planning
- **Fully automated monitoring:** Auto-discovery capability and continuous gathering of network-wide performance criteria for data and VoIP converged networks including VoIP leading quality indicators (MOS)
- Instantaneous event notification via e-mail, graphical screen displays (alarms page, network path and topology) and trap messages

- **Powerful event analysis:** Advanced tools to filter, analyze and summarize raw performance data, and present it in easy-to-use graphical displays with quick drill-down from high-level views to detailed information. High-level displays include heat charts, traffic charts, network topology maps, and personalized MyVital portal views
- **Simplified reporting:** Pre-aggregation of raw data, domain management and user-defined retention period makes trending and capacity planning easy
- **Flexible network visibility:** Extensive set of access control mechanisms provide customization views of network performance data to a broad range of users and/or customers
- **Versatile thresholding:** Offers default, user-configurable, multi-level, rate-based, time-based and adaptive (learned from historical data) thresholds, device-specific or network-wide
- **Extensive data collection:** Collects data from WAN, LAN, servers, firewall, Genesys Contact Center, VoIP and other network elements
- **Quick extensibility:** MIBWorks and DataWorks provide a way to add data collection for new devices

VitalART

- **Fully integrated reporting tool:** Provides access to all VitalSuite Performance Management Software data sets, calculations, multi-level domain and group definitions; automatically discovers new collector data added
- **Powerful custom reporting tool:** Supports a wide variety of table and chart types with robust cataloging, viewing, exporting and scheduling options
- **100% web-based report administration package:** Provides reports that can be private or published across the organization
- **Easy to use:** Out-of-the-box functionality via a wizard-based structure and step-by-step operating procedures
- **Advanced capabilities:** User-defined metrics, filtering, sorting, constraints, aggregation, percentile, top N, side-by-side charts, conditional charts, and multi-pass reporting

TECHNICAL INFORMATION

- N-tier architecture for unsurpassed scalability (single-server or multi-server deployment)
- Failover backup poller
- Northbound APIs for integration

VitalApps

- Server system requirements
  - ¬ Microsoft® Windows® 2003 with Microsoft SQL 2005
- VitalAgent system requirements
  - ¬ Windows 2000, XP SP2, Vista® Business
- Mid-Tier Agent system requirements
  - ¬ Windows 2000, XP SP2, Vista Business, Windows 2000/2003 Server, Sun Solaris™ 10, HP-UX® 11 and Linux® (Red Hat 4)
- Monitored applications
  - ¬ Internet (HTTP, HTTPS, and web-based applications such as DNS)
  - ¬ Groupware (E-mail, IBM® Lotus® Notes®, file and print services)

- ¬ Database (Oracle®, Microsoft SQL, Sybase® and LDAP)
- ¬ Infrastructure (VPN, DNS and security)
- ¬ Custom in-house applications such as those using Java™

VitalNet/VitalSuite Real Time Event Analysis Software

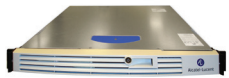
- Server system requirements
  - ¬ Windows 2003 with Microsoft SQL 2005
  - ¬ Sun Solaris 10 with Oracle 10
- VoIP Agent system requirements
  - ¬ Windows 2000, XP SP2, Vista Business
- Supports SNMP v1, v2 and v3
- Monitored network elements (multivendor)
  - ¬ Routers and switches
  - ¬ WAN and LAN
  - ¬ Servers
  - ¬ VoIP
  - ¬ Firewalls
  - ¬ Genesys Contact Center
  - ¬ DSL
  - ¬ WLAN and WiMAX
  - ¬ Wireless

VitalART

- Server system requirements
  - ¬ Windows 2003 with Microsoft SQL 2005
  - ¬ Sun Solaris 10 with Oracle 10
- VitalSuite client system requirements: Internet Explorer® 7 or Firefox® 2.0 on Windows 2000, XP SP2 and Windows Vista Business
- VitalSuite supported environment for MIBWorks, DataWorks, Automon, TTK and VSEdit: Windows XP SP2
  - ¬ MIBWorks – SNMP Data Collecting Customization
  - ¬ DataWorks – Bulk Data Collection Customization
  - ¬ Automon – Application Traffic Generation
  - ¬ TTK – Application Transaction Customization Support
  - ¬ VSEdit – Open API from VitalSuite

VitalQIP

VitalQIP



VitalQIP Appliance Manager 1000 platform

The **Alcatel-Lucent VitalQIP™ DNS/DHCP IP Management Software** integrated with the VitalQIP Appliance Manager provides a seamless, cost-effective way to maintain your network by providing customized hardware with an automated software upgrade and monitoring platform.

Market-leading VitalQIP DNS/DHCP IP Management Software helps you efficiently configure, automate, integrate and administer IP services across your entire network — locally or globally. This powerful management software centralizes planning and administration, enabling you to rapidly provision address space and reliably deliver critical IP address and name services.

Compatible with multiple technologies and platforms, it helps you streamline management tasks with a comprehensive suite of integrated tools and user interfaces. VitalQIP software is widely deployed in high-volume distributed network environments, where it has demonstrated its ability to support demanding applications with millions of individual IP addresses and hundreds of thousands of domains.

Built-in support for master and slave DNS servers, as well as dynamic DNS updates, helps you avoid network outages and automate address and name assignments. Running the system on the Alcatel-Lucent DHCP server eliminates any single point of failure with many-to-one failover capability: a single secondary DHCP server can serve as the back-up for multiple primary DHCP servers. This helps ensure that IP services are delivered to users as specified, reducing your network hardware requirements and simplifying network administration.

The system consolidates all IP address information in a single location, ensuring that diverse, geographically dispersed administrators managing your network can access the same IP database. This eliminates duplication of administrative effort and allows you to maintain a consistent, network-wide IP inventory. VitalQIP software supports both Alcatel-Lucent and other vendor DNS and DHCP servers, allowing you to readily configure and deploy IP services across your distributed network and synchronize VitalQIP data updates in real time.

KEY SELLING POINTS

Lower personnel costs

→ Accurate, centralized IP network inventory reduces address assignment errors and links IP device addresses to domain names. It also improves network moves/adds/changes processes by providing IP address visibility to the individual object level, not just subnet block.

- → Reduction in infrastructure support costs
- → Reduction in address assignment process and departmental costs
- → Reduction in disaster recovery costs

Lower down-time costs

- → Improvement in availability of network infrastructure
- → Reductions in operator errors and misconfigurations

Reduce company risk and improve business operations

- → Risk reduction due to employee turnover
- → Improvement in overall network operational efficiencies
- → Reduced troubleshooting time and support costs due to inaccurate configuration

Increase productivity

- → Maintenance of consistent, accurate IP inventory
- → Operating expenses controlled through automation
- → High availability for clients/subscribers
- → High performance access for clients/subscribers
- → Optional integrated VitalQIP Appliance Manager Platforms to take advantage of the off-the-shelf hardware/software solution with extended capabilities for efficient patch management and processing as well as DNS high availability

Provision new services quickly

- → Performance-proven in today's most demanding networks (third-party benchmarked)
- → Address space rapidly provisioned, and critical IP name and services reliably delivered throughout the network
- → Industry-leading Dynamic Host Configuration Protocol (DHCP) server performance benchmarked by third party (Exodus Labs)

KEY FEATURES

- → VitalQIP DNS/DHCP IP Management Software is the industry's leading IP management software product.
- → Automation of IP address assignment increases end-user productivity and reduces manual processes as well as help desk calls.
- → Accurate, centralized IP network inventory reduces address assignment errors and links IP device addresses to domain names. It also improves network moves/adds/changes processes by providing IP address visibility to the individual object level, not just subnet block.
- → Subnetting tools simplify and improve accuracy of subnetting operations and reduce the requirement to remember binary arithmetic.
- → Extremely scalable

- Hierarchical GUI allows viewing of IP network by domain, network, subnet, subnet organization, DNS server, DHCP server, and even a user-definable hierarchy. This allows use of the software across a multitude of constituencies with varying perspectives, hot buttons, and backgrounds. Flexible administrator network resource visibility also increases security and improves accountability.
- DHCP failover capabilities and multiple DNS server redundancy maximize availability of IP address and name services to clients, keeping them productive despite failures.
- Flexibility to support existing BIND or Microsoft environments with full integration lowers startup and ongoing costs.
- Support for DNS Bind Views and DNSSEC
- Multivendor/multiplatform support: Integration with Microsoft Active Directory® directory service
- ENUM and VoIP
  - Network allocation: Simplifies address allocation
  - Discovery tools: Allow you to know everything that is on the network and how it is being managed
  - IPV4/IPv6-compliant: Dual-stacked due to mandates, other vendors and products requiring v6 addresses, etc.
- Workflow: Easy-to-use workflow management tools that help create, automate and implement IP address processes and policies

VitalQIP Appliance Manager Platforms

- Seamless, cost-effective way to maintain the network with secured, customized hardware with automated software upgrades and monitoring
- Increased service availability
- Highest performing appliances in the market
- Multiple models to meet any requirement
- Increased service availability: Eliminate problems relating to maintaining remote servers
- Improved security: Appliances eliminate operating system vulnerabilities
- Simple software upgrades:
  - Import new packages from Alcatel-Lucent download site
  - Point and click deployment and rollback
  - Update hundreds of appliances with a single operation
- Improved monitoring: Centralize reporting and analysis for device- and application-level logs
- Leading-edge Intel-based hardware
- Support for anycast
- NTP and TFTP

TECHNICAL INFORMATION

VitalQIP Enterprise Server 7.2

Processor and memory

- Microsoft® Windows® 2003 SP2 Standard and Enterprise Server (32-bit and 64-bit): Intel® Pentium® 4 (>1 GHz), >1 GB RAM
- Windows 2003 R2 SP2 Standard and Enterprise Server (32-bit and 64-bit): Intel Pentium 4 (>1 GHz), >1 GB RAM
- Red Hat® Linux® 5.2 or higher (32-bit and 64-bit): any x86(>500 MHz), >1 GB RAM
- Sun Solaris™ 9 (32-bit and 64-bit): UltraSPARC® (>500 MHz), >1 GB RAM
- Sun Solaris 10 (32-bit and 64-bit): UltraSPARC (>500 MHz), >1 GB RAM

Disk space

- 500 MB disk space (does not include disk space required for data segments)

VitalQIP Remote Server and Distributed Services 7.2

Processor and memory

- Windows 2003 SP2 Standard and Enterprise Server (32-bit and 64-bit): Intel Pentium 4 (>500 MHz), >256 MB RAM
- Windows 2003 R2 SP2 Standard and Enterprise Server (32-bit and 64-bit): Intel Pentium 4 (>500 MHz), >256 MB RAM
- Red Hat Linux 5.2 or higher (32-bit and 64-bit): any x86 (>300 MHz), >256 MB RAM
- Sun Solaris 9 (32-bit and 64-bit): UltraSPARC (>300 MHz), >256 MB RAM
- Sun Solaris 10 (32-bit and 64-bit): UltraSPARC (>300 MHz), >256 MB RAM

Disk space

- 300 MB disk space

VitalQIP Client (GUI and CLI) 7.2

Processor and memory

- Windows 2003 SP2 Standard and Enterprise Server (32-bit and 64-bit): x86 (>500 MHz), >256 MB RAM
- Windows 2003 R2 SP2 Standard and Enterprise Server (32-bit and 64-bit): x86 (>500 MHz), >256 MB RAM
- Windows 2008 Standard and Enterprise Server (32-bit and 64-bit): x86 (>500 MHz), >256 MB RAM
- Windows Vista® Enterprise and XP Professional (32-bit and 64-bit): x86 (>500 MHz), >256 MB RAM
- Red Hat Linux 5.2 or higher (32-bit and 64-bit): any x86 (>300 MHz), >256 MB RAM
- Sun Solaris 9 (32-bit and 64-bit): UltraSPARC (>300 MHz), >256 MB RAM
- Sun Solaris 10 (32-bit and 64-bit): UltraSPARC (>300 MHz), >256 MB RAM

Disk space

- 300 MB disk space
- Not to include Sybase® or Oracle® client

VitalQIP Web Client 7.2

Browser-based

- Microsoft Internet Explorer® 7.x or higher
- Mozilla® Firefox® 2.x or higher

VitalQIP Appliance Manager 1.5 – Hardware models

Model 500

- AMM 500
- AMS 500

Model 1000

- AMM 1000
- ESM 1000
- AMS 1000

Model 5000

- AMM 5000
- ESM 5000

More specific guidelines for sizing hardware are available from Alcatel-Lucent.

OmniVista 3600

OmniVista 3600 Air Manager

The **Alcatel-Lucent OmniVista™ 3600 Air Manager** is a wireless LAN management software suite that provides centralized visibility, configuration and control over today's wireless networks. The OmniVista 3600 reduces the cost of operating the wireless infrastructure, improves network performance, improves reliability for wireless end users, and makes the network more secure.

The OmniVista 3600 is a true operations management solution that delivers a full set of capabilities including real-time user and device monitoring, centralized configuration and compliance management. These management solutions are designed for the entire IT staff, providing every team member with customized monitoring views and the detailed information needed for his or her job. Most importantly, they provide complete visibility and transparency, so IT can see exactly where users are and how the network is performing at all times.

In addition to serving the Alcatel-Lucent OmniAccess™ wireless product line, the OmniVista 3600 Air Manager supports the WLAN infrastructure of multiple vendors, thus providing a centralized operations platform for a heterogeneous WLAN network through all phases of its life cycle.

KEY SELLING POINTS

- → Provides Level One and Level Two Help Desk with all relevant user information to troubleshoot and fix a WLAN problem in very little time
- → Enhances security through availability of forensic information pertaining to user activity over the wireless network
- → Provides accurate assessment of performance and network capacity over time; allows for proactive planning of network upgrade for increased capacity
- → Provides efficient and fast RF troubleshooting information by correlating between RF heat map, interference map and user location
- → Offers flexibility in deployment strategy with the ability to gradually migrate third-party equipment while using OmniVista 3600 as the common centralized management platform

- → Prevents a large number of security incidents resulting from improper configuration of wireless equipment with its audit capability
- → Detects one of the most dangerous and yet common threats from wireless LANs — rogue access points
- → Simplifies firmware distribution task for large organizations

KEY FEATURES

- → User, session and device monitoring with bandwidth usage, RF signal strength, QoS data, and roaming history
- → Storage of nearly 2 years of historical data, user roaming patterns and detailed capacity reports
- → Real-time location information
- → Management of multiple vendors' wireless solutions
- → Compliance audits and configuration policy enforcement
- → Rogue access point detection and classification
- → Automatic distribution, scheduling and verification of firmware updates

TECHNICAL INFORMATION

Operating system

To ensure hardware capability, the server hardware should support Red Hat® Enterprise Linux®. The Alcatel-Lucent OmniVista 3600 Air Manager includes a default operating system based on CentOS. Optionally, Red Hat Enterprise Linux may be chosen. Only 32-bit Red Hat Enterprise Linux installations are supported. Not supported are 64-bit operating system installations.

Hardware platform

The hardware platform sizing is based on the number of managed devices and practical use of the OmniVista 3600 Air Manager Core Platform, Rogue AP Detection Module and the Visual RF Module.

Processor and memory

- 100 managed devices: Intel® Xeon® L5310, AMD Opteron™ 2210, 4 GB RAM
- 200 managed devices: Intel Xeon L5310, AMD Opteron 8216, 6 GB RAM
- 500 managed devices: Intel Xeon E5420, AMD Opteron 8222, 8 GB RAM
- 1000 managed devices: Intel Xeon E5450, AMD Opteron 8222, 12 GB RAM
- 2500 managed devices: Intel Xeon E5460, 16GB RAM

Disk storage

- 100 managed devices: 7.5 GB to 15 GB (15,000 rpm)
- 200 managed devices: 15 GB to 30 GB (15,000 rpm)
- 500 managed devices: 38 GB to 75 GB (15,000 rpm, multiple disks in RAID)
- 1000 managed devices: 75 GB to 150 GB (15,000 rpm, multiple disks in RAID)
- 2500 managed devices: 187 GB to 375 GB (15,000 rpm, multiple disks in RAID)

More specific guidelines for sizing hardware are available from Alcatel-Lucent.

Security product range

Alcatel-Lucent has a wide portfolio of network security products designed to provide the security required to protect valuable information and daily operation in IT. The products range from a distributed firewall through end-system integrity check to remote disabling of lost laptops.

Our security product range includes:

- → Host integrity check system, to enforce end-system compliancy
- → A unique distributed firewall/VPN system capable of operating in stealth mode
- → Laptop information integrity and security system
- → Application compliance and interaction security system

VPN Firewall Brick

VPN Firewall Brick 700

VPN Firewall Brick 1200

The **Alcatel-Lucent VPN Firewall Brick™** security portfolio is a virtually impenetrable perimeter security solution that provides advanced next-generation features designed to secure today's emerging converged IP-based networks. Incorporating unique security features from Bell Labs, the portfolio is built around a highly scalable centralized management platform, which enables cost-effective and rapid deployment of security solutions suited to enterprise, government and service provider network security strategies.

Alcatel-Lucent VPN Firewall Brick solutions provide superb performance and low total cost of ownership (TCO), while maximizing IT staff resources through time-saving and work-saving features. In addition, the flexibility, availability and scalability the VPN Firewall Brick family simplifies the deployment and management of diverse applications including:

- VPN services for site-to-site and remote access
- Specialized VoIP security services for SIP, H.323 and the Alcatel-Lucent OmniPCX™ Enterprise Communication Server
- Bandwidth management capabilities
- Secure data center web and application hosting
- Storage network security solution
- Mobile data security
- Packet data gateway and packet data interworking functions for dual-mode wireless, Wi-Fi® VPNs and VoIP/data security

The VPN Firewall Brick portfolio forms a unique three-tier security architecture that includes:

VPN Firewall Brick platforms: A suite of security appliances that integrate extensive application layer inspection, denial-of-service (DoS) protection, protocol anomaly detection and firewall functionality with advanced VPN capabilities that are well suited for environments from small offices to data centers

Alcatel-Lucent Security Management Server (SMS): Software for robust, tightly synchronized firewall, VPN, service quality, VLAN and virtual firewall policy management

Alcatel-Lucent IPSec Client: Software that provides secure remote access VPN services for mobile workforce and telecommuters

KEY SELLING POINTS

- Proven and scalable, the Alcatel-Lucent VPN Firewall Brick security management server employs a unique client/server design that provides centralized staging, real-time monitoring, and no-touch management of all VPNs as well as security and service quality assurance
- Enables stealth-like, defense security that conventional router-based firewalls cannot match
- Patented Bell Labs DoS attack protection, high-speed content security and premium authentication services that have had no occurrences of reported CERT® advisories and have no management backdoors
- Maximize service quality via flexible class-based queuing (CBQ) technology with server-level and user-level limits and guarantees
- Native high-availability architecture with no single point of failure
- Transparent interaction with third-party software, proxy servers, routers or other devices utilizing content filtering functions such as command blocking, URL filtering and virus scanning
- Range of systems available to support up to 3 million simultaneous sessions, 1100 virtual firewalls, and 20,000 VPN tunnels
- Virtually impenetrable to hacker attacks; frees memory for other functions such as packet processing and policy management
- Enables easy assignment and enforcement of security policies for diverse user groups
- Allows implementation of secure, mission-critical applications without costly, time-intensive network reconfiguration
- Saves IT staff time and effort by eliminating ongoing feature-licensing expenses and simplifying installation, management and upgrades
- Reduces the need to purchase additional equipment with high-performance and high-capacity features
- Integrated application-layer filters provide deep packet inspection, protocol anomaly detection and DoS protection
- Advanced security features secure SIP, H.323 and Alcatel-Lucent OmniPCX Enterprise Communication Server installations

KEY FEATURES

- Simplified management
- Full-featured bridging
- Advanced security safeguards
- Uniquely granular bandwidth management
- Carrier-grade reliability
- Rules-based routing
- High-performance packet processing
- Ultra-thin, highly secure operating system

- → Virtual firewall and VLAN support
- → Plug-and-play deployment
- → Low TCO
- → Stateful deep packet inspection technology
- → Specialized VoIP and converged network security capabilities

TECHNICAL INFORMATION

Processor/memory

- 3.6 GHz processor with 2 GB of RAM for VPN Firewall Brick 1200 HS Security Appliance AC and DC models
- 3.2 GHz processor with 1 GB of RAM for VPN Firewall Brick 1200 Security Appliance AC model
- Dual Core 2.2 GHz processor with 1 GB of RAM for VPN Firewall Brick 700 Security Appliance
- 650 MHz processor with 128 MB of RAM for VPN Firewall Brick 150 Security Appliance
- 466 MHz processor with 64 MB of RAM for VPN Firewall Brick 50 Security Appliance

LAN/VPN interfaces

VPN Firewall Brick 1200 HS Security Appliance AC and DC models

- 14 10/100/1000 copper ports
- Six GigE mini-GBIC small form-factor pluggable (SFP) ports
- One VPN encryption accelerator

VPN Firewall Brick 1200 Security Appliance AC model

- Eight 10/100/1000 copper ports
- Two GigE mini-GBIC SFP ports
- One VPN encryption accelerator

VPN Firewall Brick 700 Security Appliance AC and DC models

- Eight 10/100/1000 copper ports
- One VPN encryption accelerator

VPN Firewall Brick 700 SFP Security Appliance AC model

- Two 10/100/1000 copper ports
- Six GigE SFP ports
- One VPN encryption accelerator

VPN Firewall Brick 700 Basic Security Appliance AC model

- Eight 10/100/1000 copper ports

VPN Firewall Brick 150 Security Appliance

- Four 10/100 copper ports
- On-board VPN encryption accelerator

VPN Firewall Brick 50 Security Appliance

- Three 10/100 copper ports
- On-board VPN encryption accelerator

Other ports

- VPN Firewall Brick 1200 and 700: SVGA video, DB9 serial, PS/2 keyboard, 4 x USB
- VPN Firewall Brick 150: SVGA video, DB9 serial, parallel, 2 x USB
- VPN Firewall Brick 50: DB9 serial, 1 x USB

Performance

VPN Firewall Brick 1200 HS AC or HS DC

- Concurrent sessions: 3 million
- New sessions/second: 45,000
- Rules: 30,000 (shared among all virtual firewalls)
- Maximum cleartext throughput: 4.75 Gb/s (1460-byte UDP packets)
- Maximum cleartext PPS throughput: 2,200,000 pps (78-byte UDP packets)
- Maximum 3DES and AES 256 throughput with hardware encryption acceleration
  - ¬ 1.7 Gb/s (1460-byte UDP packets)
- Maximum 3DES and AES 256 PPS throughput with hardware encryption acceleration
  - ¬ 480,000 pps (78-byte UDP packets)

VPN Firewall Brick 1200 AC

- Concurrent sessions: 2 million
- New sessions/second: 30,000
- Rules: 30,000 (shared among all virtual firewalls)
- Maximum cleartext throughput: 4.1 Gb/s (1460-byte UDP packets)
- Maximum cleartext PPS throughput: 2,016,000 pps (78-byte UDP packets)

- Maximum 3DES and AES 256 throughput with hardware encryption: 1.1 Gb/s (1460-byte UDP packets)
- Maximum 3DES and AES 256 PPS throughput with hardware encryption: 332,000 pps (78-byte UDP packets)

VPN Firewall Brick 700

- Concurrent sessions: 1 million
- New sessions/second: 20,000
- Rules: 30,000 (shared among all virtual firewalls)
- Max clear text throughput: 2.5 Gb/s (1514-byte UDP packets)
- Max clear text PPS throughput: 800,000 pps (78-byte UDP packets)
- Max 3DES throughput with software encryption (VPN Firewall Brick 700 Basic): 109 Mb/s (1514-byte UDP packets), 105 Mb/s (1460-byte UDP packets)
- Max 3DES throughput with hardware encryption acceleration (VPN Firewall Brick 700 VPN and 700 VPN SFP): 388 Mb/s (1514-byte UDP packets), 374 Mb/s (1460 byte UDP packets)
- Max AES throughput with software encryption (VPN Firewall Brick 700 Basic): 218 Mb/s (1514-byte UDP packets), 210 Mb/s (1460-byte UDP packets)
- Max AES throughput with hardware encryption acceleration (VPN Firewall Brick 700 VPN and 700 VPN SFP): 363 Mb/s (1514-byte UDP packets), 374 Mb/s (1460-byte UDP packets)

VPN Firewall Brick 150

- Concurrent sessions: 245,000
- New sessions/second: 20,000
- Rules: 30,000 (shared among all virtual firewalls)
- Maximum clear text throughput: 330 Mb/s (1514-byte UDP packets), 100,000 pps (78-byte UDP packets)
- Maximum 3DES throughput: 140 Mb/s (1024-byte UDP packets without LZS compression), 52,000 pps (78-byte UDP packets)
- Maximum AES 256 throughput: 140 Mb/s (1024-byte UDP packets without LZS compression), 52,000 pps (78-byte UDP packets)

VPN Firewall Brick 50

- Concurrent sessions: 135,000
- New sessions/second: 1600
- Rules: 10,000 (shared among all virtual firewalls)
- Maximum clear text throughput: 195 Mb/s (1514-byte UDP packets), 88,000 pps (78-byte UDP packets)
- Maximum 3DES throughput with hardware encryption acceleration: 75 Mb/s (1460-byte UDP packets without LZS compression), 9200 pps (78-byte UDP packets)
- Maximum AES 256 throughput with hardware encryption acceleration: 60 Mb/s (1024-byte UDP packets without LZS compression), 9200 pps (78-byte UDP packets without LZS compression)

Virtualization

- VPN Firewall Brick 1200 HS AC or DC: Maximum number of virtual firewalls: 1100
- VPN Firewall Brick 1200 AC: Maximum number of virtual firewalls: 500
- VPN Firewall Brick 700: Maximum number of virtual firewalls: 350
- VPN Firewall Brick 140: Maximum number of virtual firewalls: 150
- VPN Firewall Brick 50: Maximum number of virtual firewalls: 50
- Number of VLANs supported: 4094
- VLAN domains: Up to 16 per VLAN trunk
- VPN Firewall Brick partitions: Allows for virtualization of customer IP address range, including support for overlapping IP addresses

Modes of operation

- Bridging and/or routing on all interfaces
- All features supported with bridging
- IP routing with static routes
- 802.1Q VLAN tagging supported inbound and outbound on any combination of ports
- Layer-2 VLAN bridging
- Network address translation (NAT)
- Port address translation (PAT)
- Policy-based NAT and PAT (per rule)
- Supports virtual IP addresses for both address translation and VPN tunnel endpoints
- Point-to-Point Protocol over Ethernet (PPPoE) and DHCP-assignable interface/VLAN addresses
- Redundant DHCP relay capabilities
- Dynamic registration of mobile VPN Firewall Brick security appliance address for centralized remote management
- Nested zone rule sets for common firewall
- Policies for all VPN Firewall Bricks in the zone
- Link aggregation
- Mobile VPN Firewall Brick using integrated DHCP client

Services supported

- BOOTP, HTTP, IRC, netstat, POP3, SNMP, TFTP, PPTP, DNS, HTTPS, Kerberos, NNTP, RIP, SSH, WHO, RADIUS, EIGRP, IDENT, LDAP, NTP, RIP2, Syslog, Shell, X.11, EXEC, GMP, login, OSPF, rlogin, Telnet, talk, H.323, SIP, FTP, IMAP, Mbone, ping, rsh, traceroute, Lotus Notes, VoIP/SIP, Gopher, IPSec, NetBIOS, PointCast, MTP, SQL*Net
- Any IP protocol (user-definable)
- Any IP protocol + layer-4 ports (user-definable)
- Support for non-IP protocols as defined by SAP/Ethertype

Layer-7 application support

- Application filter architecture supports layer-7 protocol inspection (deep packet inspection) for command and protocol validation, protocol anomaly detection, dynamic channel pinholes and application layer address translation. Application filters include HTTP, FTP, RPC, TFTP, H.323/H.323 RAS, SMTP, Oracle SQL*Net, NetBIOS, ESP, DHCP Relay, DNS, GTP, Alcatel-Lucent OmniPCX™ Enterprise New Office Environment (NOE), and SIP

Firewall attack detection and protection

- Generalized Day Zero anomaly-based flood protection with patent-pending intelligent cache management protection
- SYN flood protection to specifically protect inbound servers, for example Web servers, from inbound TCP SYN floods
- Strict TCP validation to ensure TCP session state enforcement, validation of sequence and acknowledgement numbers
- Rejection of bad TCP flag combinations
- Initial sequence number (ISN) rewriting for weak TCP stack implementations
- Fragment flood protection with robust fragment reassembly, ensures no partial or overlapping fragments are transmitted
- Generalized IP packet validation including detection of malformed packets
- DoS mitigations for over 190 DoS attacks, including ping of death, land attack, tear drop attack, etc.
- Drops bad IP options as well as source route options
- Connection rate limits to minimize effects of new attacks

QoS/bandwidth management

- Classified by physical port, virtual firewall, firewall rule, session bandwidth guarantees – Into and out of virtual firewall, allocated in bits/second
- Bandwidth limits – Into and out of virtual firewall, allocated in bits/second, packets/ session, sessions/second
- Type of service (ToS)/Differentiated Services (DiffServ) marking and matching
- Integrated with application layer filters

Content security

- HTTP filter keyword support integrated with HTTP application filter
- Basic content filtering with configurable whitelist/blacklist and content keyword matching.
- URL redirection for blacklist sites
- Rules-based routing feature for HTTP, SMTP and FTP features (Security Management Server v9.1 or later)
  - ¬ Interoperates with all third-party anti-virus, anti-spam, and content filtering systems
  - ¬ Redirects only protocol-specific packets to third-party systems performing anti-virus, anti-spam and content filtering services
- Application-layer protocol command recognition and filtering
- Application-layer command line length enforcement
- Unknown protocol command handling
- Extensive session-oriented logging for application-layer commands and replies
- Hostile mobile code blocking (Java™, ActiveX™)

Firewall user authentication

- Browser-based authentication allows authentication of any user protocol
- Built-in internal database: User limit 10,000
- Local passwords, RADIUS, RSA SecurID®
- User assignable RADIUS attributes
- Certificate authentication

VPN

- Maximum number of dedicated VPN tunnels: 7500
- Manual key, IKEv1, IKEv2, DoD PKI, X.509
- 3DES (168-bit), DES (56-bit)
- AES (128-bit, 192-bit, 256-bit)
- SHA-1 and MD5 authentication/integrity
- Replay attack protection
- Remote access VPN
- Site-to-site VPN
- IPSec NAT Traversal/UDP encapsulated IPSec
- IKEv2 IPSec NAT Traversal and dead peer detection
- LZS compression
- Spliced and nested tunneling
- Fully meshed or hub-and-spoke site-to-site VPN

VPN authentication

- Local passwords, RADIUS, SecurID, X.509 digital certificates
- PKI certificate requests (PKCS 12)
- Automatic LDAP certificate retrieval
- Department of Defense (DoD) PKI

High availability

- VPN Firewall Brick security appliance to VPN Firewall Brick security appliance active/passive failover with full synchronization
- 400-ms device failure detection and activation
- Session protection for firewall, VoIP and VPN
- Link failure detection
- Alarm notification on failover
- Encryption and authentication of session synchronization traffic
- Self-healing synchronization links
- Pre-emption and IP tracking for improved health state checking
- Seamless system upgrade with no down time for redundant deployments

Diagnostic tools

- Out-of-band debugging and analysis via serial port/modem/terminal server
- Centralized, secure remote console to any VPN Firewall Brick
- Support for ping, traceroute, and packet trace with filters
- Remote VPN Firewall Brick security appliance bootstrapping
- Real-time log viewer analysis tool
- Java-based navigator for remote access to management system

Three-tier management architecture

- Centralized, carrier-class, active/active management architecture with Alcatel-Lucent Security Management Server (SMS) software
- Secure VPN Firewall Brick to SMS communications with Diffie-Helman and 3DES encryption, SHA-1 authentication and integrity and digital certificates for VPN Firewall Brick security appliance/Alcatel-Lucent SMS authentication
- Up to 100 simultaneous administrators securely managing all aspects of up to 20,000 VPN Firewall Brick units in a hierarchical management cluster
- Secure, reliable, redundant real-time alarms, logs, reports

Certifications

- ICSA V4.1 Firewall Certification
- ICSA V1.2 IPSec Certification
- FIPS 140-2 Certification (Pending on Brick 700)
- EAL-4+ Certification (Pending on Brick 700)
- NEBS Level 3 (compliant with Telecordia GR-1089-CORE and GR-63-CORE) in process for Brick 1200 HS DC version.

Mean time between failures (MTBF)

- VPN Firewall Brick 1200 Basic: 129,801 hours
- VPN Firewall Brick 1200HS AC: 128,820 hours
- VPN Firewall Brick 1200HS DC: 128,833 hours
- VPN Firewall Brick 700 Basic: 62,025 hours
- VPN Firewall Brick 700 VPN AC: 62,036 hours

- VPN Firewall Brick 700 VPN SFP AC: 58,539 hours
- VPN Firewall Brick 700 VPN DC: 61,301 hours
- VPN Firewall Brick 150: 218,999 hours
- VPN Firewall Brick 50: 409,688 hours
- Telecordia SR-332 at Standard Reference Conditions

Dimensions

VPN Firewall Brick 1200 Models

- Height: 8.9 cm (3.5 in.)
- Width: 48.3 cm (19 in.)
- Depth: 48.3 cm (19 in.)
- Rack-mountable per EIA-310 specification
- Weight: 20 kg (44 lb)
- Shipping weight: 22 kg (50 lb)

VPN Firewall Brick 700 Models

- Height: 4.45 cm (1.75 in.)
- Width: 43.18 cm (17 in.)
- Depth: 48.26 cm (19 in.)
- Rack-mountable per EIA-310 specification.
- Weight: 8.16 kg (18 lb) (without power supplies)
- DC power supply weight: 1.088 kg (2.4 lb)
- AC power supply weight: 1.088 kg (2.4 lb)

VPN Firewall Brick 150 model

- Height: 4.5 cm (1.75 in)
- Width: 27.9 cm (11 in.)
- Depth: 18.2 cm (7.18 in.)
- Rack-, wall-, or table-mountable
- Weight: 1.4 kg (3 lb)
- Shipping weight: 2.3 kg (5 lb)

VPN Firewall Brick 50 model

- Height: 2.8 cm (1.1 in.)
- Width: 21.6 cm (8.5 in.)
- Depth: 15 cm (5.9 in.)
- Wall- or table-mountable
- Weight: 1.0 kg (2 lb, 3 oz)
- Shipping weight: 2.2 kg (4 lb, 12 oz)

Cooling

- VPN Firewall Brick 1200: Chassis fan (intake and exhaust), power supply fans
- VPM Firewall Brick 700: Active cooling for CPU and power supply
- VPN Firewall Brick 150: Chassis fan
- VPN Firewall Brick 50: Passive cooling

Operating altitude

- Up to 4000 m (13,123 ft)

Environmental

VPN Firewall Brick 1200 and 700 Models

Operating

- Normal operating temperature: 0°C to 45°C (32°F to 113°F)
- Shock: 2.5 g at 15 ms to 20 ms on any axis
- Relative humidity: 5% to 85% at 40°C (104°F) (non-condensing)
- Vibration: 5 g at 2 Hz to 200 Hz on any axis

Non-operating

- Temperature: -40°C to +70°C (-40°F to +158°F)
- Shock: 35 g at 15 ms to 20 ms on any axis
- Relative humidity: 5% to 95% at 40°C (104°F) (non-condensing)
- Vibration: 5 g at 2 Hz to 200 Hz on any axis

VPN Firewall Brick 150 and 50 Models

Operating

- Normal operating temperature: 0°C to 50°C (32°F to 122°F)
- Shock: 2.5 g at 15 ms to 20 ms on any axis
- Relative humidity: 10% to 95% at 40°C (104°F) (non-condensing)
- Vibration: 5 g at 2 Hz to 200 Hz on any axis

Non-operating

- Temperature: -20°C to +70°C (-4°F to +158°F)
- Shock: 35 g at 15 ms to 20 ms on any axis
- Relative humidity: 10% to 95% at 40°C (104°F) (non-condensing)
- Vibration: 5 g at 2 Hz to 200 Hz on any axis

Power

VPN Firewall Brick 1200 AC models

- Hot-swappable, internal dual AC to DC power supply: 500 W max
- Auto-ranging: 100 V AC to 240 V AC, 47 Hz to 63 Hz
- Consumption: 8 A at 120 V AC; 5 A at 240 V AC

VPN Firewall Brick 1200 DC model

- Hot-swappable, internal dual DC to DC power supply: 500 W max
- Input range: -36 V DC to -72 V DC
- Consumption: 10 A at -48 V DC, 8 A at -60 V DC

VPN Firewall Brick 700 AC models

- Internal AC to DC power supply: Rated 450 W max
  - ¬ Hot-swappable when optional second supply installed.
- Range: 90 V to 264 V
- Typical consumption: 160 W

VPN Firewall Brick 700 DC Model

- Internal DC to DC power supply: Rated 450 W max
  - ¬ Hot-swappable when optional second supply installed
- Range: -40 V DC to -60 V DC
- Typical consumption: 160 W

VPN Firewall Brick 150 Model

- External AC to DC power supply: 50 W max
- Input CV mode: 100 V AC to 240 V AC, 47 Hz to 63 Hz, 64 W
- Consumption: 2.8 A at 115 V AC; 1.4 A at 230 V AC

VPN Firewall Brick 150 Model

- External AC to DC power supply: 25 W max
- Input CV mode: 100 V AC to 240 V AC, 47 Hz to 63 Hz, 64 W
- Consumption: 1.2 A at 115 V AC; .6 A at 230 V AC

Alcatel-Lucent Security Management Server

Software requirements

- Sun Solaris™ 2.9 or 2.10 on SPARC® processors
- Red Hat® Linux® version RHEL4 and RHEL5 support on x86 processors
- Microsoft Windows® XP Professional, Windows Server 2003, or Windows Vista® Business

Hardware requirements

SPARC

- 500 MHz UltraSPARC® or better
- 512 MB of memory or more

Linux RHEL4/5

- 2 GHz dual-core or better
- 1 GB of memory or more

Windows XP/2003

- 500 MHz Pentium® III or better
- 512 MB of memory or more

Vista

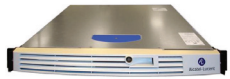
- 800 MHz Pentium III or better
- 1 GB of memory or more

Common

- Swap space at least as large as system memory
- 4 GB free disk space in file system partition where software is to be installed
- 50 MB free disk space in root partition
- One 10/100 Ethernet interface
- CD-ROM drive
- USB port and serial port
- Video card capable of supporting minimum resolution of 1024 x 768 (65,535 colors)

OmniAccess 3500

MiFi 2352



Gateway server

The **Alcatel-Lucent OmniAccess™ 3500 Nonstop Laptop Guardian** (NLG) is the market's only, always-on, secure, independent mobile platform that provides 24/7 visibility, control and access to mobile laptops worldwide. Its mobile security platform leverages 3G networks, GPS, a self-powered and self-contained computing system and an automatic VPN to allow enterprises to securely manage, track and control their laptops, even when they are turned off or are offline.

At the heart of the OmniAccess 3500 NLG is a secure, always-on computing system on a 3G wireless data device. This device acts as the laptop's ignition key, providing multi-factor authentication for the VPN connection and delivering 24/7 connectivity to a dedicated management system located in the enterprise.

As soon as the device is connected to the computer, it looks for connectivity across all media and automatically establishes a VPN tunnel. By automatically establishing a secure connection, mobile laptops have the same level of security as desktops inside the enterprise. When the card is not inserted, it is still accessible to receive content and commands (remote kill, patches, updates, pre-fetched application content, etc).

Encryption keys are stored on the device, safeguarding confidential laptop data. If a laptop is stolen or misplaced, the enterprise IT manager can immediately disable the encryption key in the device, making the laptop data unreadable. If the laptop is later located, the encryption key can be re-enabled to restore all laptop data.

All employee laptops become part of a trusted network no matter if they are connected, how they are connected or where they are located.

Today, there are many solutions to maintain and protect desktop computers; however, mobile laptops offer a variety of concerns that existing solutions cannot combat. Enterprise IT organizations must address these concerns. The OmniAccess 3500 NLG mobile security platform specializes in providing a trusted, always-on, easy-to-use solution for both IT and end users that:

- → Protects sensitive data 24/7 and provides remote kill capabilities
- → Offers an always-on VPN solution and multi-factor authentication
- → Uses 3G networks and GPS for increased mobility, enhanced productivity tools, maintenance and location-based services.

KEY SELLING POINTS

- → Delivers always-on mobile security platform with always-on remote management even when a laptops is off or offline
- → Provides 24/7 visibility and control using always-on 3G communications to mobile laptops back to the management portal
- → Reduces liability of lost or stolen laptops with always-on remote lock and kill capabilities
- → Improves compliance and policy enforcement through automatic VPN without user interaction and ensures 100 percent policy enforcement
- → Increases productivity with off-hours patch downloads and application pre-fetch for users by automatically maintaining software systems
- → Emulates an interactive smart device for multi-factor authentication
- → Capitalizes on mobility benefits provided by broadband wireless networks using automatic, cost-effective and non-invasive security management, which eliminates the end user from the security equation
- → Facilitates laptop recovery using GPS location tracking and integration with LBS

KEY FEATURES

- → An embedded CPU and self-contained, hardened Linux operating system
- → A rechargeable battery that supplies power to the device when it is on standby or shutdown
- → 3G communications virtually anywhere there is mobile phone reception
- → Non-volatile flash memory to store software updates, patches or downloads while the laptop is powered off
- → GPS capability for locating lost or stolen laptops and location-based services
- → Secure communications over the enterprise VPN with no additional software required on the laptop
- → Smartcard emulation for Microsoft Windows® authentication enabling integration with full-disk encryption solutions

TECHNICAL INFORMATION

The Alcatel-Lucent OmniAccess 3500 Nonstop Laptop Guardian has two key components:

- An always-on wireless data device featuring a built-in CPU, hardened operating system, storage, rechargeable battery, GPS capability, VPN client and 3G communications.*
- A gateway appliance that is deployed on the enterprise premises to terminate the secure tunnels and to manage user credentials and security policies. A standard enterprise gateway (for up to 16,000 users) and mid-range gateway (for small and medium-sized businesses with up to 500 users) are available.

* Available as a PCMCIA card from Alcatel-Lucent or a USB solution by Novatel Wireless (MiFi)

InfoExpress CyberGatekeeper

InfoExpress CyberGatekeeper

Alcatel-Lucent offers a seamless, secure and scalable enterprise network access control (NAC) solution through its embedded network security framework. This framework includes a comprehensive security solution for verifying endpoint integrity through host integrity checking (HIC). The solution is the result of integration between the InfoExpress CyberGatekeeper and the Alcatel-Lucent OmniSwitch™ 6400 Stackable Gigabit LAN Switch (SGS), the Alcatel-Lucent OmniSwitch 6850 Stackable LAN Switch (SLS) and any edge switches using the Alcatel-Lucent Operating System (AOS), Release 6.3.4 or later.

The InfoExpress CyberGatekeeper can be used either in conjunction with the Alcatel-Lucent OmniSwitch integration or as a seamless overlay with other Alcatel-Lucent or third-party systems. The CyberGatekeeper is a one-stop HIC and NAC product for enterprises. HIC capabilities screen endpoints and allow them to access the network only if they meet specific security policy requirements.

The CyberGatekeeper supports both HIC desktop agent and agentless (web-based agent) methods. It allows the management of endpoint requirement policy across all user connection modes (wired, wireless or remote VPN), all user types (employee, contractor or guest), and a broad range of devices and platforms (Microsoft® Windows®, Linux®, Mac OS devices).

The CyberGatekeeper can be deployed seamlessly in just a few hours, with minimal network changes. The product is available in an appliance/software version and a software-only version.

KEY SELLING POINTS

- → Ensures 100 percent of network endpoints are compliant (patch levels, configurations and application settings) or they are quarantined until remediated
- → Separates authentication mechanism from security
  - ¬ 802.1x not a requirement for HIC
  - ¬ Endpoints can be plugged into phones and still be secured
- → Will not interfere with existing VoIP deployments
- → Keeps rogue devices off the network
- → Reduces vulnerabilities: Security solutions, operating system and patches are assured to be running and up-to-date
- → Lowers help desk costs: Automatic remediation of non-compliant PCs

- → Improves security compliance/auditing scorecard
- → Reduces risks associated with improperly configured computers
- → Integrates with existing patch management solutions to preserve software investments
- → Reduces support costs by maintaining standard configurations across desktops
- → Agents are permanently installed or provided on-demand via a web browser
- → Dynamic enforcement via access control lists (ACLs), not VLAN or IP address changes
- → Central policy management delivers consistent user experience
- → Continuous surveillance of endpoint configuration

KEY FEATURES

- → Automatically manages the security fitness of endpoints
- → Operates independently of authentication mechanism and network access controls
- → Auto-remediation through automatic installation of missing patches, fully interoperable with third-party remediation/patch management solutions
- → InfoExpress CyberGatekeeper integration with the Alcatel-Lucent OmniSwitch integrates and enforces endpoint compliance at the very first entry point to the network, the edge switch
- → InfoExpress CyberGatekeeper HIC policy server provides a single management platform to define, manage and monitor endpoint security fitness compliance
- → Compatible with Microsoft Windows, Mac OS, and Linux

TECHNICAL INFORMATION

OmniSwitch products supporting HIC integration

- Alcatel-Lucent OmniSwitch 6400 Stackable Gigabit LAN Switch (SGS) and Alcatel-Lucent OmniSwitch 6850 Stackable LAN Switch (SLS) families with Alcatel-Lucent Operating System (AOS), Release 6.3.4 or later

CGS-1000 CyberGatekeeper Server Appliance

- Hardware revision: 1000-sm1a
- Software revision: 6.02
- Compliance: RoHS, UL, FCC
- Power requirements: 5 A Max (100 V to 240 V 50/60 Hz, single power supply)
- Network interfaces: Dual 1000BT full-duplex RJ-45 (copper)
- Audit connections: Rated up to 10,000 for policies with 500 audited conditions
- Enforcement modules
  - ¬ CGSI (HIC): Max 100 client switches
  - ¬ EAP (RADIUS Proxy): Max 100 client switches
  - ¬ Dynamic NAC: Max 200 managed subnets
  - ¬ Bridge (in-line): Max 800 Mb/s (CGR-1000 dedicated bridge enforcement)

CGM CyberGatekeeper Manager Software Suite

- Includes Policy Manager and Reporting Server
- Requires Microsoft Windows 2003 Server® and Microsoft SQL Server® 2005/2008 database software
- Hardware specifications to support an implementation vary depending on total number of endpoints, policy complexity, and data retention period. The following sample configuration is provided only as a guide for supporting a 3000-endpoint implementation

Web server (dedicated)

Windows 2003 Server SP1, IIS

- Processor and memory: Intel® Core™2 Quad 2.4 GHz, 3.0 GB of RAM
- Disk subsystem: RAID 5, 7200 rpm disks, minimum 80 GB for operating system and application

Database SQL server (dedicated)

Windows 2003 (64-bit) Server SP1, SQL Server 2005/2008

- Processor and memory: Intel Core 2 Quad 2.4 GHz, 8 GB of RAM
- Disk subsystem: RAID 5, 7200 rpm disks, minimum 100 GB for DB
- Expected average database size: 45 GB

OmniAccess 8550

OmniAccess 8500

The **Alcatel-Lucent OmniAccess™ 8550 Web Services Gateway** (WSG) is a network appliance that secures automated business processes to meet corporate governance obligations. It protects sensitive corporate data from misuse and ensures data is always available when and where it is needed.

The OmniAccess 8550 WSG is a critical component for any organization that needs to secure or automate business processes within the organization, or with partners and when using web services deployed on a services-oriented architecture (SOA). This is accomplished by using Alcatel-Lucent patent pending, web services runtime message inspection technology, which provides IT system interoperability for corporate-wide security and regulatory compliance.

The OmniAccess 8550 WSG significantly reduces the total cost of ownership for information systems, which leads to a significant competitive advantage.

KEY SELLING POINTS

- **Stateful policy enforcement:** Enforce conformance to policy at runtime for all user transactions in an application session, ensuring conformance to regulations
- **Consolidated audit trail:** Audit trail of all access to web services
- **Application data protection:** Application data is kept private and is only released with appropriate authorization and encryption
- **Identity interoperability:** Acceptance of user validation from partners while meeting all traceability and user privacy requirements
- **Service virtualization:** Virtual services published to external security domains protecting the internal application architecture
- **Service mediation:** Message data and security token translation
- **High availability (HA):** Automatic, seamless, stateful failover for paired nodes

KEY FEATURES

- Corporate governance
- Partner extranet
- Information system interoperability
- Business-critical features

TECHNICAL INFORMATION

Compliance

- HTTP 1.0/1.1
- TLSv1/SSLv3
- DES, 3DES, AES, RC4, SHA-1, MD5
- RSA, DSA, X509, Diffie-Hellman
- SAML 1.2
- WSSE 1.0
- SOAP 1.1/1.2
- XSLT 1.0
- Xpath 1.0
- IEEE 802.3, 802.3u, 802.3ab

Fortinet

FortiGate Series

Fortinet® offers an array of multi-threat security solutions that help businesses of all sizes meet their security challenges and enable a safe and clean communications environment. Fortinet built its comprehensive security platform from the ground up to provide multiple layers of threat protection and management. This translates into increased deployment flexibility, better security through integration and a future-proof solution that can easily scale with business requirements.

Using Fortinet's ASIC innovation and its performance acceleration capabilities, FortiGate® systems detect and eliminate the most damaging, content-based threats from e-mail and web traffic such as viruses, worms, intrusions and inappropriate web content, in real time without degrading network performance.

FortiGate systems integrate the industry's broadest suite of security protection products — including firewall, VPN, antivirus, intrusion prevention systems (IPS), web filtering, anti-spam and traffic shaping — that are deployed either individually or combined for a comprehensive, unified threat management solution.

KEY SELLING POINTS

- → Offers certified protection with maximum performance and scalability with a powerful, complete content inspection firewall
- → Detects and eliminates viruses, worms and spyware in real time. Scans incoming and outgoing e-mail attachments (SMTP, POP3, IMAP) and all FTP and HTTP traffic, including web-based e-mail
- → Delivers alerts based on a customizable database of more than 1400 known attack signatures. FortiGate multi-threat security stops attacks that evade conventional host-based anti-virus systems, with real-time response to fast-spreading threats.
- → Enables blacklisting of web sites and domains, keyword scanning of e-mails (configurable on a per-user basis) and the ability to leverage a dynamic scoring system using a number of criteria
- → Processes all web content against known malicious URLs to block inappropriate material and malicious scripts including Java™ applets, cookies, and ActiveX® scripts entering the network. Fortinet categorizes more than 25 million domains and billions of web pages to ensure its customers can avoid malware on the Internet.

- Provides secure communication tunnels between networks and clients using industry-standard IP Security (IPSec), Secure Sockets Layer (SSL) and Transport Layer Security (TLS), Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Tunneling Protocol (L2TP)-based VPN support. Fortinet's ASIC-accelerated VPN capabilities allow enterprises to use the Internet as the public infrastructure and a variety of specialized protocols to support private communications through it.
- Helps users control network traffic to optimize or guarantee performance, low latency, and/or bandwidth with Fortinet's traffic shaping. The FortiOS™ firmware offers packet classification, queue disciplines, policy enforcement, congestion management, quality of service and fairness.

KEY FEATURES

- Firewall
- Anti-virus gateway
- Intrusion prevention
- Anti-spam
- Web filtering
- VPN
- Traffic shaping
- Data leakage prevention

TECHNICAL INFORMATION

Summary system information

Large enterprise and managed service provider systems

- FortiGate-5140 – 14-slot chassis, AC or DC power
- FortiGate-5050 – five-slot chassis, AC or DC power
- FortiGate-5020 – two-slot chassis, AC power
- FortiGate-5001 – Threat Management blade with GigE and SFP options
- FortiGate-5005 – Threat Management blade with six SFP and two FortiAccel SFP ports
- FortiSwitch-5003 – Switch Fabric Blade with GigE and SFP options
- FortiController-5208 – Load Balancer blade

Enterprise appliances

- FortiGate-3810 – 8 x 10/100/1000 ports, 2 x SFP ports and two single-width, two double-width expansion slots
- FortiGate-3600 – 8 x 10/100/1000 ports, 2 x SFP ports and one single-width expansion slot
- FortiGate-3016 – 2 x 10/100/1000 ports, 16 x SFP ports and one single-width expansion slot
- FortiGate-1000A – 10 x 10/100/1000 ports
- FortiGate-1000FA – 10 x 10/100/1000 ports, 2 x SFP ports
- FortiGate-800 – 4 x 10/100, 4 x 10/100/1000 ports
- FortiGate-800F – 4 x 10/100, 4 x SFP ports
- FortiGate-620B – 20 x 10/100/1000 ports and one single-width expansion slot
- FortiGate-500A – 8 x 10/100 ports and 2 x 10/100/1000 ports
- FortiGate-400A – 4 x 10/100 ports and 2 x 10/100/1000 ports
- FortiGate-310B – 10 x 10/100/1000 ports
- FortiGate-300A – 4 x 10/100 ports and 2 x 10/100/1000 ports
- FortiGate-224B – 26 x 10/100 ports and 2 x 10/100/1000 ports
- FortiGate-200A – 8 x 10/100 ports

SMB/ROBO/SOHO appliances

- FortiGate-110C/111C – 8 x 10/100 ports and 2 x 10/100/1000 ports

- FortiGate-100A – 6 x 10/100 ports
- FortiGate-80C/80CM – 6 x 10/100 ports and 2 x10/100/1000 ports
- FortiWiFi-80CM – 6 x 10/100 ports, 2 x 10/100/1000 ports and 1 x Wi-Fi b/g/n
- FortiGate-60CM – 6 x 10/100 ports and 2 x 10/100/1000 ports
- FortiWiFi-60CM – 6 x 10/100 ports, 2 x 10/100/1000 ports and 1 x Wi-Fi a/b/g
- FortiGate-50B/51B – 5 x 10/100 ports
- FortiWiFi-50B – 5 x 10/100 ports and 1 x Wi-Fi b/g
- FortiGate-30B – 4 x 10/100 ports
- FortiWiFi-30B – 5 x 10/100 ports and 1 x Wi-Fi b/g

Summary performance information

Large enterprise and managed service provider systems

- FortiGate-5140 – up to 182 Gb/s cleartext, 98 Gb/s IPSec VPN
- FortiGate-5050 – up to 65 Gb/s cleartext, 35 Gb/s IPSec VPN
- FortiGate-5020 – up to 28 Gb/s cleartext, 14 Gb/s IPSec VPN

Enterprise appliances

- FortiGate-3810 – 7 Gb/s (37 Gb/s with AMC) cleartext, 1 Gb/s (19 Gb/s with AMC) IPSec VPN
- FortiGate-3600 – 6 Gb/s (10 Gb/s with AMC) cleartext, 0.8 Gb/s (3.8 Gb/s with AMC) IPSec VPN
- FortiGate-3016 – 16 Gb/s (20 Gb/s with AMC) cleartext, 12 Gb/s (15 Gb/s with AMC) IPSec VPN
- FortiGate-1000A/FA – 2 Gb/s cleartext, 600 Mb/s IPSec VPN
- FortiGate-800/800F – 1 Gb/s cleartext, 200 Mb/s IPSec VPN
- FortiGate-620B – 16 Gb/s (20 Gb/s with AMC) cleartext, 12 Gb/s (15 Gb/s with AMC) IPSec VPN
- FortiGate-500A – 600 Mb/s cleartext, 150 Mb/s IPSec VPN
- FortiGate-400A – 500 Mb/s cleartext, 140 Mb/s IPSec VPN
- FortiGate-310B – 8 Gb/s (12 Gb/s with AMC) cleartext, 6 Gb/s (9 Gb/s with AMC) IPSec VPN
- FortiGate-300A – 400 Mb/s cleartext, 120 Mb/s IPSec VPN
- FortiGate-224B – 150 Mb/s cleartext, 70 Mb/s IPSec VPN
- FortiGate-200A – 150 Mb/s cleartext, 70 Mb/s IPSec VPN

SMB/ROBO/SOHO appliances

- FortiGate-110C/111C – 500 Mb/s cleartext, 100 Mb/s IPSec VPN
- FortiGate-100A – 100 Mb/s cleartext, 40 Mb/s IPSec VPN
- FortiGate-80C/80CM – 350 Mb/s cleartext, 80 Mb/s IPSec VPN
- FortiWiFi-80CM – 350 Mb/s cleartext, 80 Mb/s IPSec VPN
- FortiGate-60CM – 100 Mb/s cleartext, 64 Mb/s IPSec VPN
- FortiWiFi-60CM – 100 Mb/s cleartext, 64 Mb/s IPSec VPN
- FortiGate-50B/51B – 50 Mb/s cleartext, 48 Mb/s IPSec VPN
- FortiWiFi-50B – 50 Mb/s cleartext, 48 Mb/s IPSec VPN
- FortiGate-30B – 30 Mb/s cleartext, 5 Mb/s IPSec VPN
- FortiWiFi-30B – 30 Mb/s cleartext, 5 Mb/s IPSec VPN

For more information

Should you require further information about Alcatel-Lucent Enterprise solutions, products or services:

→ Contact your Alcatel-Lucent representative

→ Visit the public Internet web site at:

www.enterprise.alcatel-lucent.com

Alcatel-Lucent Enterprise business partners may visit the Alcatel-Lucent Business Partner web site at:

www.businesspartner.alcatel-lucent.com

Business partners in North America may visit the specific North American Business Partner web site at:

www.alcatel-lucent.com/us/partners

Data Networks, Management Solutions and Security

www.alcatel-lucent.com

Alcatel·Lucent