Alcatel-Lucent OmniSwitch 6575-MP16

Compact Hardened Ethernet Switches

The Alcatel-Lucent OmniSwitch® 6575-MP16 is a ruggedized, fully manageable and fan-less Gigabit Ethernet switch. Designed for industrial Ethernet applications, the hardened OmniSwitch 6575-MP16 offers a wall mountable switch that is ideal for a wide variety of industrial applications such as intelligent transportation, railway, smart cities and utilities.

OS6575-MP16

The 6575-MP16 is a hardened, compact, fan-less gigabit Ethernet switches that has been designed specifically for industrial applications. The switches run on the widely deployed and field-proven Alcatel-Lucent Operating System (AOS) that offers high security, reliability, performance and easy management. These switches are designed to operate in extended temperatures, offer higher EMI/EMC tolerance, provide a flexible range of power input options and deliver high surge protection.

The OS6575-MP16 offers advanced PoE capabilities with 60W PoE per port and Fast / Perpetual PoE support to power range of modern devices from PTZ IP cameras on toll booths, LED lights and building management gateways in smart buildings to industrial control systems. This switch is easy to deploy and offer out-of-the- box plug-and-play, Zero-touch provisioning, network automation and disaster recovery options. With support for MACSec-256 on all ports, the OS6575-MP16 enables end-to-end encrypted networks. The OS6575-MP16 offers advanced system- and network-level resiliency features and convergence through standardized protocols in a space-efficient form factor.

These versatile industrial switches are ideal for deployment in transportation and traffic control systems, utilities, IP surveillance systems and outdoor installations, among other applications.

Key Features	Benefits
• Resilient ruggedized hardware design	• Operates at a wider temperature range from -40° C to +75° C, withstands greater shock, vibrations, temperature and EMI/EMC variance
• Convection cooled fan-less models	• Fan-less operation increases resiliency and maximizes uptime for converged mission-critical networks
• Designed for industrial applications	• Operates at a wider temperature range from -40°C to +75°C, withstands greater shock, vibrations, surge and EMI/EMC variance • Redundant power supply inputs with a 6 pin M23 connector for 2 power inputs • Alarm relays to connect external alarm systems • Compact wall mountable design
• Advanced Industrial PoE capabilities with support for 60W IEEE 802.3bt PoE and Fast PoE / Perpetual PoE	• Enables converged deployments and is ideal for all type of PoE application requirements from outdoor wireless APs to PTZ surveillance cameras and video displays • Fast PoE allows the PoE power to be supplied to the connected devices within a matter of seconds as soon as the switch is powered up • Perpetual PoE maintains the power to connected PoE devices when a switch is rebooted
• Virtual chassis technology to connect multiple switches to create a single chassis-like entity	• Increases system redundancy, resiliency and high availability while simplifying network deployment, operations and management
• Auto-fabric technology to simplify installation and service provisioning	• Enables zero-touch provisioning and network automation with automatic protocol and topology discovery • Prevent human mistakes by automating standardized and replicable configurations
• Built in resiliency and redundancy • M23 connector supports 2 power sources, not hot-swappable • Delivers redundant ring topologies using industry standard protocols	• Field upgradable, highly redundant network solution maximizes network uptime
• SDN-ready ¬ Supports RESTful API commands and MIBs ¬ Embedded scripting capabilities	• Allows creation of specialized services which ensures future readiness and enables interoperability with third-party solutions • REST APIs provide access to all AOS CLI and, with advanced embedded scripting capabilities using Python and Bash, it enables fast deployment of new network services and the ability to adopt new applications
• MACSec-256 support on all ports	• MACSec encryption support provides a secure network access ensuring data confidentiality and integrity
• Switch backup and restore	• Simplifies switch replacement in field and minimizes network downtime using USB drive • USB encryption ensures optimal security

Alcatel-Lucent OmniSwitch 6575-MP16 model

The OmniSwitch 6575-MP16 offers an extensive selection of Gigabit fixed-configuration switches with up to 60 watts of PoE per port and power supply options that accommodate the most demanding requirements. The model can be mounted on a wall.

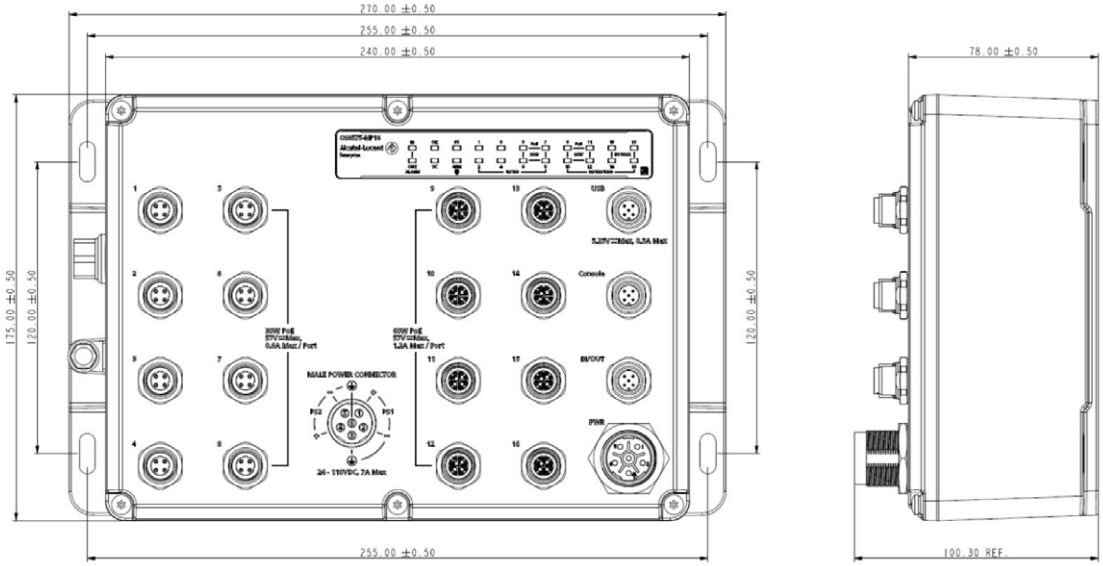
All the models in the OS6575 family support IEEE 802.3bt compliant 60W PoE, MACSec-256 and alarm relays.

Switch	100Mbit ports (D-code)	100Mbit ports with PoE (D-code)	1Gbit ports with PoE (X-code)	1Gbit ports with Bypass (X-code)	Description
OS6575-MP16	4	4	4	4	Hardened GigE fan-less switch. 4x10/100 BaseT IEEE 802.3at 30W PoE D-code, 4 x 10/100/1000 BaseT IEEE 802.3bt 60W X-code, 4 x 10/100 BaseT D-code, 4 x 10/100/1000 BaseT X-code with Bypass Function.

Technical specifications

Product matrix	OS6575-MP16
Operating temperature	-40°C to 75°C (-40°F to 167°F)
Fans	0
File system flash	4 GB
RAM	2 GB
Max switching capacity	17.6 Gb/s
Forwarding capacity	13.09 Mpps
Weight (no power supply attached)	3.4 Kg (7.5 lbs)
Height	270 mm (10.63 in)
Width	175 mm (6.89 in)
Depth (no power supply attached)	78 mm (3.07 in)
MACsec-256-capable ports	All ports
USB port (5V@.5A)	1 M12 A-code
Console port	1 M12 A-code
Alarm relay contacts	1 in, 1 out
Power input	2 in 1 M23 connector
Max PoE budget	120W
Protection	IP67
Altitude	13,000 ft
Storage temperature	-40°C to 85°C (-40°F to 185°F)
Humidity (operating and storage)	5% to 95% non-condensing
Power consumption (idle)	~13 W
Power consumption (full load)	~17 W
Heat dissipation (BTU/hr)	148 BTU/hr
Maximum surge protection	2 KV
MTBF (hours) (switch only)	219000 hours
Mounting options	Wall

Switch dimensions



OS6575-MP16

Product specifications and measurements

Per-port LEDs

- Non-PoE ports - Green: link/activity
- PoE ports - Amber: link/activity

System LEDs

- OK: Green/Amber operational status of the switch
- VC: Green/Amber master or slave role in VC configuration. Number of blinks identifies stacking unit number
- PS: Green/Amber - status of the primary or secondary power supply
- ALRM IN: Red when alarm in
- ALRM OUT: Red when alarm out
- GRN: Green when in power saving mode

Scalability numbers and speeds

- Wire rate at Layer 2 and Layer 3 on all ports
- Jumbo frame size: 9,216 bytes
- Total number of MAC addresses: 32,000
- Total number of IPv4 routes: 8,000
- Number of VLANs: 4,000

Virtual chassis

- Maximum number of units in a VC: 4
- Supports remote VC connection

Compliance and certifications

Commercial safety

- IEC 62368-1
- UL 62368-1 3rd Edition
- IEC 62368-1; all national deviations
- EN 62368-1; all deviations
- CAN/CSA-C22.2 No. 62368-1
- NOM-019 SCFI, Mexico
- AS/NZ TS-001 and 62368-1:2000, Australia
- UL-AR, Argentina
- UL-GS Mark, Germany
- CU, EAC, Russia
- ANATEL, Brazil
- CCC, China
- KCC Korea
- BSMI, Taiwan
- EN 60825-1 Laser
- EN 60825-2 Laser
- CDRH Laser
- RoHS and WEEE directives compliant
- REACH directive

Commercial EMI/EMC

- 47 CRF FCC Part 15: 2015 Subpart B (Class A)VCCI (Class A, with UTP Cables)
- ICES–003:2012 Issue 5, Class A
- AS/NZS 3548 (Class A) – C-Tick
- CE marking for European countries (Class A)
- CE emission
  - ¬ EN50581 (RoHS Recast)
  - ¬ EN 55032 (EMI & EMC requirement)
  - ¬ EN 55035 (Immunity Characteristics)
  - ¬ EN 61000-3-2 (Harmonic Current emissions)
  - ¬ EN 61000-3-3
  - ¬ EN 61000-4-2
  - ¬ EN 61000-4-3
  - ¬ EN 61000-4-4
  - ¬ EN 61000-4-5 (Surge Immunity, Class 4)
  - ¬ EN 61000-4-6
  - ¬ EN 61000-4-8
  - ¬ EN 61000-4-9
  - ¬ EN 61000-4-11
  - ¬ IEEE802.3: Hi-pot Test (2.25 KV DC on all Ethernet ports)

Industrial

Industrial environmental

- IEC 60870-2-2 (operational temperature)
- IEC 60068-2-1 (temperature type test – cold)
- IEC 60068-2-2 (temperature type test – hot)
- IEC 60721-3-1: Class 1K5 (storage temperature)
- IEC 60068-2-30: 5% to 95% non-condensing humidity
- IEC 60255-21-2 (mechanical shock)
- IEC 60255-21-1 (vibration)
- IEC 60068-2-6 (sinusoidal vibration)
- IEC 60068-2-27 (shock testing)

Industrial safety

- UL 61010
- EN 50021

- Hazardous location
  - ISA 12.12.01 (UL 1604) (Class I, Div 2, groups A-D)
  - CSA22.2/213 (Class I, Div 2, groups A-D)
- IP67

Industrial emission

- EN 55032 (Emission Standard)
- EN 61000-3-2
- EN 61000-3-3
- EN 61805-3
- EN 55035 (Immunity Standard)
- EN 61000-4-2 to EN 61000-4-8
- EN 61000-4-11
- EN 61000-4-12
- EN 61000-4-16
- EN 61000-4-17
- EN 61000-4-29
- IEC 60255-5

Industry specific

Railway applications

- EN 50121-4
- EN 50155:2017
- EN 61373
- EN 62236-4
- EN 61000-6-2
- EN 61000-6-4

Intelligent transportation (road)

- NEMA TS-2

Federal certifications

- Trade Agreements Act (TAA)*

Detailed product features

Simplified manageability and configuration

- Intuitive CLI in a scriptable Python and BASH environment via console, Telnet or Secure Shell (SSH) v2 over IPv4/IPv6
- Powerful WebView graphical web interface via HTTP and HTTPS over IPv4/IPv6
- Network Automation and Programmability Abstraction Layer with Multivendor (NAPALM) support
- Fully programmable RESTful web services interface with XML and JSON support. API enables access to CLI and individual MIB objects
- Integrated with Alcatel-Lucent OmniVista® products for network management
- Integrated with Nokia Network Services Platform (NSP) for network management
- Full configuration and reporting using SNMPv1/2/3 to facilitate third-party network management over IPv4/IPv6
- File upload using USB, TFTP, FTP, SFTP or SCP using IPv4/IPv6
- Human-readable ASCII-based configuration files for off-line editing, bulk configuration and out-of-the-box auto-provisioning
- Non-volatile memory for start-up configuration
- Multiple microcode image support with fallback recovery
- Dynamic Host Configuration Protocol (DHCP) relay for IPv4/IPv6
- IEEE 802.1AB Link Layer Discover Protocol (LLDP) with Media Endpoint Discover (MED) extensions
- Network Time Protocol (NTP)
- DHCPv4 and DHCPv6 server managed by Nokia VitalQIP® DNS/DHCP IP Address Management
- Access to the AOS console via USB Adapter with Bluetooth technology provides wireless management access, eliminating the need of console cables
- Configurable per-port PoE priority, max power and time-of-day policy for PoE power allocation

Cloud ready with OmniVista® Cirrus

- Alcatel-Lucent OmniVista® Cirrus offers a secure, resilient and scalable cloud-based network management. It offers hassle free network deployment and easy service roll-out with advanced analytics for smarter decision making. It provides IT-friendly unified access with secure authentication and policy enforcement for users and devices.

Monitoring and troubleshooting

- Local (on the flash) and remote server logging (Syslog): event and command logging
- IP tools: ping and trace route
- Dying Gasp support via SNMP and syslog messages
- Loopback IP address support for management per service
- Management virtual routing and forwarding (VRF) support
- Policy- and port-based mirroring
- Remote port mirroring
- sFlow v5 and Remote Monitoring (RMON)
- Unidirectional Link Detection (UDLD), Digital Diagnostic Monitoring (DDM) and Time Domain Reflectometry (TDR)

Resiliency and high availability

- Unified management, control and virtual chassis technology
- Virtual chassis 1+N redundant supervisor manager
- Virtual chassis In-Service Software Upgrade (ISSU)
- Remote virtual chassis - Up to 10-km fault-tolerant remote stacking supported
- Smart continuous switching technology
- ITU-T G.8032/Y1344 2010: Ethernet Ring Protection
- High availability automation network: Media Redundancy protocol (IEC 62439-2)
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) encompasses IEEE 802.1D Spanning Tree Protocol (STP) and IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- Per-VLAN spanning tree (PVST+) and 1x1 STP mode
- IEEE 802.3ad/802.1AX Link Aggregation Control Protocol (LACP) and static LAG groups across modules
- Dual-home link support for sub-second link protection without STP
- Virtual Router Redundancy Protocol (VRRP) with tracking capabilities
- IEEE protocol auto-discovery
- Bidirectional Forwarding Detection (BFD) for fast failure detection and reduced re- convergence times in a IPv4/IPv6 routed environment
- Redundant and hot-swappable power supplies
- Built-in CPU protection against malicious attacks
- Split virtual chassis protection: Auto-detection and recovery of virtual chassis splitting due to one or more VFL or stack element failures*

Advanced security

Switch software security

- AOS secured diversified code solution is available on OmniSwitch 6575, hardening it at both the software source code and binary executable levels to enhance overall network security
- AOS secured diversified code protects networks from intrinsic vulnerabilities, code exploits, embedded malware, and potential back doors that could compromise mission-critical operations

- AOS secured diversified code is a proactive, defense approach toward network security that continuously defines and implements value-add capabilities to address both current and future threats

Access control

- Alcatel-Lucent Access Guardian framework for comprehensive user-policy-based NAC
- Autosensing IEEE 802.1X multi-client, multi-VLAN support
- MAC-based authentication for non-IEEE 802.1X hosts
- Web based authentication (captive portal): a customizable web portal residing on the switch
- User Network Profile (UNP) simplifies NAC by dynamically providing pre-defined policy configuration to authenticated clients — VLAN, ACL, BW
- Secure Shell (SSH) with public key infrastructure (PKI) support
- Terminal Access Controller Access-Control System Plus (TACACS+) client
- Centralized Remote Access Dial-In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAP) administrator authentication
- Centralized RADIUS for device authentication and network access control authorization
- Learned Port Security (LPS) or MAC address lockdown
- Access Control Lists (ACLs); flow-based filtering in hardware (Layer 1 to Layer 4)
- DHCP v4 & v6 Snooping, DHCP IP and Address Resolution Protocol (ARP) spoof protection
- DHCPv6 guard and DHCPv6 Client guard
- ARP poisoning detection
- IP v4 &v6 Source Filtering as a protective and effective mechanism against ARP attacks
- Bring Your Own Device (BYOD) provides on-boarding of guest, IT/non-IT issued and silent devices. Restriction/ remediation of traffic from non-compliant devices. Uses RADIUS CoA to dynamically enforce User Network Profiles based on authentication, profiling, posture check of devices
- LLDP Security mechanism for rogue device detection and restriction

Network control

- AOS secured diversified code solution is available on OmniSwitch 6575, hardening it at both the software source code and binary executable levels to enhance overall network security
- AOS secured diversified code protects networks from intrinsic vulnerabilities, code exploits, embedded malware, and potential back doors that could compromise mission- critical operations

QoS

- Priority queues: Eight hardware-based queues per port for flexible QoS management
- Traffic prioritization: Flow-based QoS Flow-based traffic policing and bandwidth management
- 32-bit IPv4/128-bit IPv6 non-contiguous mask classification
- Egress traffic shaping
- DiffServ architecture
- Congestion avoidance: Support for end- to-end head-of-line (E2E-HOL) blocking prevention, IEEE 802.1Qbb Priority- based Flow Control (PFC) and IEEE 802.3x Flow Control (FC)
- Auto-QoS support for Generic Object Oriented Substation Events (GOOSE) messages

Layer 3 routing and multicast

IPv4 routing

- Multiple VRF and inter-VRF route leaking
- Static routing
- Routing Information Protocol (RIP) v1 and v2
- Open Shortest Path First (OSPF) v2 with Graceful Restart
- Intermediate System to Intermediate System (IS-IS) with Graceful Restart
- Border Gateway Protocol (BGP) v4 with Graceful Restart
- Generic Routing Encapsulation (GRE) and IP/IP tunneling
- Virtual Router Redundancy Protocol (VRRPv2)
- DHCP relay (including generic UDP relay)
- Address Resolution Protocol (ARP)
- Policy-based routing and server load balancing
- DHCPv4 server

IPv6 routing

- Multiple VRF and inter-VRF route leaking
- Internet Control Message Protocol version 6 (ICMPv6)
- Static routing
- Routing Information Protocol Next Generation (RIPng)
- Open Shortest Path First (OSPF) v3 with Graceful Restart
- Intermediate System to Intermediate System (IS-IS) with Graceful Restart
- Multi-Topology IS-IS (M-ISIS)
- BGP v4 multiprotocol extensions for IPv6 routing (MP-BGP)
- Graceful Restart extensions for OSPF and BGP
- Virtual Router Redundancy Protocol version 3 (VRRPv3)
- Neighbor Discovery Protocol (NDP)
- Policy-based routing and server load balancing
- DHCPv6 server
- DHCPv6 Relay and UDPv6 relay

IPv4/IPv6 multicast

- Internet Group Management Protocol (IGMP) v1/v2/v3 snooping
- Protocol Independent Multicast – Sparse- Mode (PIM-SM), Source Specific Multicast (PIM-SSM)
- Protocol Independent Multicast – Dense- Mode (PIM-DM), Bidirectional Protocol Independent Multicast (PIM-BiDir)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Multicast Listener Discovery (MLD) v1/v2 snooping
- PIM to DVMRP gateway support

Fluent network for voice, video and data

- SIP profile for QOS, priority tuning for end-to-end processing*
- Multicast DNS Relay: Bonjour protocol support for wired Airgroup

Advanced Layer 2 services

- Ethernet services support using IEEE 802.1ad Provider Bridges (also known as Q-in-Q or VLAN stacking
- Ethernet OAM (802.1ag, ITU-T Y.1731): Connectivity Fault Management (L2 ping and link trace)
- Ethernet in first mile: Link OAM (802.3ah)
- Fabric virtualization services IEEE 802.1aq

- Shortest Path Bridging (SPB-M)
- In-band management for SPB-M
- Ethernet network-to-network interface (NNI) and user network interface (UNI)
- Service Access Point (SAP) profile identification
- Service VLAN (SVLAN) and Customer VLAN (CVLAN) support
- VLAN translation and mapping including CVLAN to SVLAN
- Port mapping
- DHCP Option 82: Configurable relay agent information
- Multiple VLAN Registration Protocol (MVRP)
- HA-VLAN for Layer 2 clusters such as MS-NLB and active-active Firewall clusters*
- Customer Provider Edge (CPE) test head traffic generator and analyzer tool
- TR-101 Point-to-Point Protocol over Ethernet (PPPoE) Intermediate Agent allowing for the PPPoE network access method
- Service Assurance Agent (SAA) for proactively measuring network health, reliability and performance
- Jumbo frame support
- Bridge Protocol Data Unit (BPDU) blocking
- STP Root Guard
- STP Loop-Guard
- Loopback Detection to auto-detect and prevent L2 loops

Supported standards

IEEE standards

- IEEE 802.1D STP
- IEEE 802.1p CoS
- IEEE 802.1Q VLANs
- IEEE 802.1ab (LLDP)
- IEEE 802.1ag (OA&M)
- IEEE 802.1ad Provider Bridges Q-in-Q/ VLAN stacking
- IEEE 802.1ak (Multiple VLAN Registration Protocol (MVRP)
- IEEE 802.1s MSTP
- IEEE 802.3i 10BASE-T
- IEEE 802.1w RSTP
- IEEE 802.3x Flow Control
- IEEE 802.3z Gigabit Ethernet
- IEEE 802.3ab 1000Base-T
- IEEE 802.3ac VLAN Tagging
- IEEE 802.3ad/802.1AX Link Aggregation
- IEEE 802.3ae 10 GigE
- IEEE 802.3af Power over Ethernet
- IEEE 802.3at PoE Plus
- IEEE 802.3bt PoE (60W)

ITU-T recommendations

- ITU-T G.8032/Y.1344 2010: Ethernet Ring Protection (ERPv2)
- ITU-T Y.1731 OA&M fault and performance management

IEC standards

- IEC 62439-2 Media Redundancy Protocol

IETF RFCs

IPv4

- RFC 2003 IP/IP Tunneling
- RFC 2131 Dynamic Host Configuration Protocol (DHCPv4)
- RFC 2784 GRE Tunneling
- RFC 4022/2452 MIB for IPv4 TCP
- RFC 4087 IP Tunnel MIB
- RFC 4113/2454 MIB for IPv4 UDP
- RFC 4292/4293 IPv4 MIBs

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

OSPF

- RFC 1765 OSPF Database Overflow
- RFC 1850/2328/4570 OSPF v2 and MIB
- RFC 2154 OSPF MD5 Signature
- RFC 2370/3630 OSPF Opaque LSA
- RFC 2740/5340 OSPFv3 for IPv6
- RFC 3101 OSPF NSSA Option
- RFC 3623/5187 OSPF Graceful Restart
- RFC 5838 MIB for OSPFv3
- RFC 4552 Authentication for OSPFv3
- RFC 5709 OSPFv2 HMAC-SHA Cryptographic Authentication

BGP

- RFC 1269/1657/4273 BGP v3 and v4 MIB
- RFC 1403/1745 BGP/OSPF Interaction
- RFC 1771-1774/2842/2918/3392/4271 BGP v4
- RFC 1965 BGP AS Confederations
- RFC 1966/2796 BGP Route Reflection
- RFC 1997/1998/4360 BGP

Communities attribute

- RFC 2042/5396 BGP New Attribute
- RFC 2385 BGP MD5 Signature
- RFC 2439 BGP Route Flap Damping
- RFC 2545 BGP-4 Multiprotocol Extensions for IPv6 Routing
- RFC 2858/4760 Multiprotocol Extensions for BGP-4
- RFC 3065 BGP AS Confederations
- RFC 4456 BGP Route Reflection
- RFC 4486 Subcodes for BGP Cease Notification
- RFC 4724 Graceful Restart for BGP
- RFC 3392/5492/5668/6793 BGP 4-Octet ASN
- RFC 5082 Generalized TTL Security Mechanism (GTSM)

IS-IS

- RFC 1142/1195/3719/3787/5308 IS-IS v4
- RFC 2763/2966/3567/3373 Adjacencies and route management
- RFC 5120 M-ISIS: Multi Topology IS-IS
- RFC 5306 Graceful Restart
- RFC 5309/draft-ietf-isis-igp-p2p-over-lan Point to point over LAN
- RFC 6329 IS-IS Extensions Supporting IEEE 802.1aq SPB
- RFC 5304 IS-IS Cryptographic Authentication
- RFC 5310 IS-IS Generic Cryptographic Authentication

IP Multicast

- RFC 1075/draft-ietf-idmr-dvmrp-v3-11. txt DVMRP
- RFC 2362/4601/5059 PIM-SM
- RFC 2365 Multicast
- RFC 2710/3019/3810/MLD v2 for IPv6
- RFC 2715 PIM and DVMRP interoperability
- RFC 2933 IGMP MIB
- RFC 3376 IGMPv3 (includes IGMP v2/v1)
- RFC 3569 Source-Specific Multicast (SSM)
- RFC 3973 Protocol Independent Multicast- Dense Mode (PIM-DM)
- RFC 4541 Considerations for IGMP and MLD Snooping Switches
- RFC 5015 BiDIR PIM
- RFC 5060 Protocol Independent Multicast MIB
- RFC 5132 Multicast Routing MIB
- RFC 5240 PIM Bootstrap Router MIB

IPv6

- RFC 1981 Path MTU Discovery
- RFC 2460 IPv6 Specification
- RFC 2461 NDP
- RFC 2464 IPv6 over Ethernet
- RFC 2465 MIB for IPv6: Textual Conventions (TC) and General Group
- RFC 2466 MIB for IPv6: ICMPv6 Group
- RFC 2711 Router Alert Option
- RFC 3056 6to4 Tunnels
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

- RFC 3484 Default Address Selection
- RFC 3493/2553 Basic Socket API
- RFC 3542/2292 Advanced Sockets API
- RFC 3587/2374 Global Unicast Address Format
- RFC 3595 TC for IPv6 Flow Label
- RFC 3596/1886 DNS for IPv6
- RFC 4007 Scoped Address
- RFC 4022/2452 MIB for IPv6 TCP
- RFC 4113/2454 MIB for IPv6 UDP
- RFC 4193 Unique Local Addresses
- RFC 4213/2893 Transition Mechanisms
- RFC 4291/3513/2373 Addressing Architecture (uni/any/multicast)
- RFC 4292/4293 IPv6 MIBs
- RFC 4301/2401 Security Architecture
- RFC 4302/2402 IP Authentication Header
- RFC 4303/2406 IP Encapsulating Security Payload (ESP)
- RFC 4443/2463 ICMPv6
- RFC 4861/2461 Neighbor Discovery*
- RFC 4862/2462 Stateless Address Autoconfiguration
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6*

Manageability

- RFC 854/855 Telnet and Telnet options
- RFC 959/2640 FTP
- RFC 1350 TFTP Protocol
- 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 1867 Form-based File Upload in HTML
- RFC 1901-1908/3416-3418 SNMP v2c
- RFC 2096 IP MIB
- RFC 2131 DHCP Server/Client
- RFC 2388 Returning Values from Forms: multipart/form-data
- RFC 2396 Uniform Resource Identifiers (URI): Generic Syntax
- RFC 2570-2576/3410-3415/3584 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 3023 XML Media Types
- RFC 3414 User-based Security Model
- RFC 3826 (AES) Cipher Algorithm in the SNMP User-based Security Model
- RFC 4122 A Universally Unique IDentifier (UUID) URN Namespace
- RFC 4234 Augmented BNF for Syntax Specifications: ABNF
- RFC 4251 Secure Shell Protocol Architecture
- RFC 4252 The Secure Shell (SSH) Authentication Protocol
- RFC 4253 SSH Transport Layer Protocol
- RFC 4254 SSH Connection Protocol
- RFC 4627 JavaScript Object Notation (JSON)
- RFC 6585 Additional HTTP Status Codes

Security

- RFC 1321 MD5
- RFC 1826/1827/4303/4305 Encapsulating Payload (ESP) and crypto algorithms
- RFC 2104 HMAC Message Authentication
- RFC 2138/2865/2868/3575/2618 RADIUSAuthentication and Client MIB
- RFC 3576 Dynamic Authorization Extensions to RADIUS
- RFC 2139/2866/2867/2620 RADIUS Accounting and Client MIB
- RFC 2228 FTP Security Extensions
- RFC 2284 PPP EAP
- RFC 2869/2869bis RADIUS Extension
- RFC 4301 Security Architecture for IP

Security - With Common Criteria enabled

- RFC 5280 - Internet X.509 PKI Certificate and CRL Profile
- RFC 2560 - X.509 Internet PKI Online Certificate Status Protocol - OCSP
- RFC 2986 - PKCS #10: Certification Request Syntax Specification v 1.7
- RFC 5246 - TLS Protocol v 1.2
- RFC 4346 - TLS Protocol v 1.1
- RFC 3268 - AES Cipher suites for TLS
- RFC 6125 - Representation and Verification of Domain-Based Application Service Identity within Internet PKIX Certificates in the Context of TLS
- draft-ietf-radext-radsec-12 - TLS encryption for RADIUS

QoS

- RFC 896 Congestion Control
- RFC 1122 Internet Hosts
- RFC 2474/2475/2597/3168/3246 DiffServ
- RFC 2697 srTCM
- RFC 2698 trTCM
- RFC 3635 Pause Control

Others

- RFC 791/894/1024/1349 IP and IP/Ethernet
- RFC 792 ICMP
- RFC 768 UDP
- RFC 2581 TCP Congestion Control
- RFC 826 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 1305/2030/5905 NTP v4 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 2581 TCP Congestion Control
- 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
- RFC 3621 Power Ethernet MIB
- RFC 4562 MAC-Forced Forwarding

Ordering information

Orderable part	Description
OS6575-MP16-00	Hardened GigE fan-less switch. 4x10/100 BaseT IEEE 802.3at 30W PoE D-code, 4 x 10/100/1000 BaseT IEEE 802.3bt 60W X-code, 4 x 10/100 BaseT D-code, 4 x 10/100/1000 BaseT X-code with Bypass Function, alarm relay A-code, RS232 A-code, USB port A-code, FPoE/PPoE and up to 120W PoE budget. Include user manual & Wall mounting hardware.
OmniSwitch 6575-MP16 Cable	
M12-Console-5P	M12 5pin A-code to RS232(F/F), 1m 5pk
M12-Alarm-6P	M12 5pin A-code(F) to bare cable, 1m 6pk
M12-USB-2P	M12 5pin A-code(F) to USB Plug, 0.5m 2pk
M12-DC-M-8P	M12 4pin D-code (M/M), 0.5m 8pk
M12-DC-RJ45M-8P	M12 4pin D-code to RJ45 (M/M), 0.5m 8pk
M12-DC-RJ45F-8P	M12 4pin D-code to RJ45 (M/F), 0.5m 8pk
M12-XC-M-8P	M12 8pin X-code (M/M), 0.5m 8pk
M12-XC-RJ45M-8P	M12 8pin X-code to RJ45 (M/M), 0.5m 8pk
M12-XC-RJ45F-8P	M12 8pin X-code to RJ45 (M/F), 0.5m 8pk
M23-PWRCONN-5P	M23 6pin(F) power conn (w/o cable) 5pk
OmniSwitch 6575 software	
OS-SW-MACSEC	Site license to enable MACSec on OS6575 models. One license per customer at no cost.

Warranty

The OmniSwitch 6575 family comes with a Limited Lifetime Hardware Warranty.

Services and support

For more information about our Professional services, Support services and Managed services, please go to https://www.al-enterprise.com/en/services

Please visit our website to learn more: https://www.al-enterprise.com/en/products/switches/omniswitch-6575