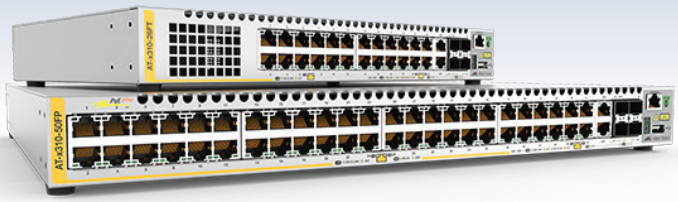
x310 Series

Stackable Access Switches



The Allied Telesis x310 Series Layer 3 stackable access switches offer an impressive set of features in a high-value package, ideal for applications at the network edge.

Overview

The Allied Telesis x310 Series provide a high performing and scalable access solution for today's networks. With a choice of 24-port and 48-port 10/100BASE-T versions with Gigabit uplinks, Power over Ethernet (PoE), plus the ability to stack up to four units, the x310 Series is perfect for demanding applications at the edge of enterprise networks.

Manageable

The x310 runs the advanced AlliedWare Plus™ fully featured Operating System delivering a rich feature set and an industry-standard Command Line Interface (CLI). The industry-standard CLI reduces training requirements and is consistent across all AlliedWare Plus devices, simplifying network management.

The built-in, web-based Graphical User Interface (GUI) is an easy-to-use and powerful management tool. With comprehensive monitoring facilities and the ability to view a virtual chassis as a single entity, the GUI is an essential part of network management.

Powerful network management

Meeting the increased management requirements of modern converged networks, Allied Telesis Autonomous Management Framework (AMF) automates everyday tasks including configuration management. The complete network can be managed as a single virtual device with powerful centralized management features. Growing the network can be accomplished with plug-and-play simplicity, and network node recovery is fully zero-touch.

AMF secure mode increases network security with management traffic encryption, authorization, and monitoring.

Reliable

The x310 was designed with reliability in mind, to guarantee the continued delivery of essential services. With the ability to stack up to four devices, maintenance and reconfiguration do not affect network uptime.

Secure

Advanced security features protect the network from the edge to the core. Unprecedented control over user access is provided with Network Access Control (NAC), to mitigate threats to network infrastructure. This ensures the network is accessed only by known users and devices, as each user's adherence to network security policies is checked.Secure access can also be provided for guests.

A secure network environment is guaranteed, with powerful control over network traffic types, secure management options, and other multi-layered security features built right into the x310 Series switches.

Future-proof

A future-proof network is ensured with the flexibility of the x310 Series, coupled with the ability to stack multiple units. All x310 models come with a comprehensive IPv6 feature set as standard, to ensure they are ready for future traffic demands.

x310 Series switches are Software Definided Networking (SDN) ready and are able to support OpenFlow v1.3.

ECO friendly

The x310 supports Energy Efficient Ethernet (EEE), which automatically reduces the power consumed by the switch whenever there is no traffic on a port. This sophisticated feature can significantly reduce your operating costs, by reducing the power requirements of the switch and any associated cooling equipment.

New Features

- AMF secure mode
- Active Fiber Monitoring
- OpenFlow for SDN
- VLAN Mirroring (RSPAN)
- VLAN ACLs
- G.8032 Ethernet Ring Protection
- Ethernet CFM

Key Features

Virtual Chassis Stacking (VCStack™)

- Create a VCStack of up to four units with 4 Gbps of stacking bandwidth to each unit. Stacking links are connected in a ring so each device has dual connections to further improve resiliency. VCStack provides a highly available system where network resources are spread out across stacked units, reducing the impact if one of the units fails. Aggregating switch ports on different units across the stack provides excellent network resiliency.

Allied Telesis Autonomous Management Framework™ (AMF)

- Allied Telesis Autonomous Management Framework (AMF) is a sophisticated suite of management tools that provide a simplified approach to network management. Common tasks are automated or made so simple that the every-day running of a network can be achieved without the need for highly-trained, and expensive, network engineers. Powerful features like centralized management, auto-backup, auto-upgrade, auto-provisioning and auto-recovery enable plug-and-play networking and zero-touch management.
- AMF secure mode encrypts all AMF traffic, provides unit and user authorization, and monitors network access to greatly enhance network security.

Ethernet Protection Switching Rings (EPSRing™)

- EPSRing allows several x310 switches to form a protected ring capable of recovery within as little as 50ms. This feature is perfect for high performance and high availability in enterprise networks.

G.8032 Ethernet Ring Protection

- G.8032 provides standards-based high-speed ring protection, that can be deployed stand-alone, or interoperate with Allied Telesis EPSR.
- Ethernet Connectivity Fault Monitoring (CFM) proactively monitors links and VLANs, and provides alerts when a fault is detected.

Industry-leading Quality of Service (QoS)

- Comprehensive low-latency wire-speed QoS provides flow-based traffic management with full classification, prioritization, traffic shaping and min/max bandwidth profiles. Enjoy boosted network performance and guaranteed delivery of business-critical Ethernet services and applications.

Loop protection

- Thrash limiting, also known as rapid MAC movement, detects and resolves network loops. It is highly user-configurable - from the rate of looping traffic to the type of action the switch should take when it detects a loop.
- With thrash limiting, the switch only detects a loop when a storm has occurred, which can potentially cause disruption to the network. To avoid this, loop detection works in conjunction with thrash limiting to send special packets that the switch listens for. If a port receives a special packet, you can choose to disable the port, disable the link, or send an SNMP trap.

Power over Ethernet Plus (PoE+)

- With PoE, a separate power connection to media endpoints such as IP phones and wireless access points is not necessary. PoE+ reduces costs and provides even greater flexibility, providing the capability to connect devices requiring more power (up to 30 Watts)—for example pan, tilt and zoom (PTZ) security cameras.

Link Layer Discovery Protocol – Media Endpoint Discovery (LLDP – MED)

- LLDP-MED extends LLDP basic network endpoint discovery and management functions. LLDP-MED allows for media endpoint specific messages, providing detailed information on power requirements, network policy, location discovery (for Emergency Call Services) and inventory.

Voice VLAN

- Voice VLAN automatically separates voice and data traffic into two different VLANs. This automatic separation places delay-sensitive traffic into a voice dedicated VLAN, which simplifies QoS configurations.

sFlow

- sFlow is an industry standard technology for monitoring high speed switched networks. It provides complete visibility into network use, enabling performance optimization, usage accounting/billing, and defense against security threats. Sampled packets sent to a collector ensure it always has a real-time view of network traffic.

Active Fiber Monitoring

- Active Fiber Monitoring prevents eavesdropping on fiber communications by monitoring received optical power. If an intrusion is detected, the link can be automatically shut down, or an operator alert can be sent.

UniDirectional Link Detection

- UniDirectional Link Detection (UDLD) is useful for monitoring fiber-optic links between two switches that use two single-direction fibers to transmit and receive packets. UDLD prevents traffic from being sent across a bad link by blocking the ports at both ends of the link in the event that either the individual transmitter or receiver for that connection fails.

Tri-authentication

- Authentication options on the x310 Series also include alternatives to 802.1x port-based authentication, such as web authentication to enable guest access and MAC authentication for end points that do not have an 802.1x supplicant. All three authentication methods—802.1x, MAC-based and Web-based—can be enabled simultaneously on the same port. This is called tri-authentication.

TACACS+ Command Authorization

- Centralize control of which commands may be issued by a specific user of an AlliedWare Plus device. TACACS+ command authorization complements authentication and accounting services for a complete AAA solution.

Access Control Lists (ACLs)

- AlliedWare Plus delivers industry-standard Access Control functionality through ACLs. ACLs filter network traffic to control whether routed packets are forwarded or blocked at the port interface. This provides a powerful network security mechanism to select the types of traffic to be analyzed, forwarded, or influenced in some way.

VLAN ACLs

- Simplify access and traffic control across entire segments of the network. Access Control Lists (ACLs) can be applied to a Virtual LAN (VLAN) as well as a specific port.

Premium Software License

- By default, the x310 Series offers a comprehensive Layer 2 and basic Layer 3 feature set that includes static routing and IPv6 management features. The feature set can easily be elevated to full Layer 3 by applying the premium software license. This adds dynamic routing protocols and Layer 3 multicasting capabilities.

VLAN Mirroring (RSPAN)

- VLAN mirroring allows traffic from a port on a remote switch to be analysed locally. Traffic being transmitted or received on the port is duplicated and sent across the network on a special VLAN.

Key Solutions

Network convergence

The convergence of network services in the Enterprise has led to increasing demand for highly available networks with minimal downtime. Diagram 1 shows x310 PoE+ switches with high performance EPSRing connectivity to the x930 VCStack network core. This topology provides recovery in as little as 50ms, if required. PoE+ powers end points without the need for separate power feeds.

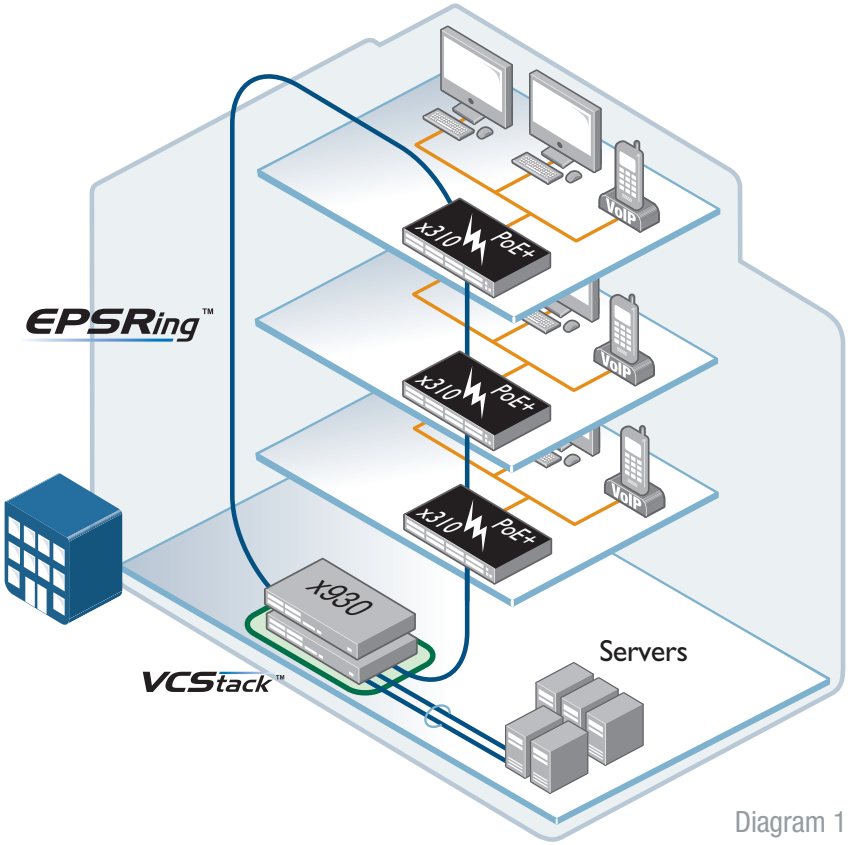


Diagram 1

Network flexibility

Multiple x310 units can form a single virtual unit with VCStack, as shown in Diagram 2. This greatly simplifies management and provides a scalable and future-proof network. Management of the network is simple, since all SwitchBlade and x-series switches run the advanced AlliedWare Plus operating system, with an industry standard CLI.

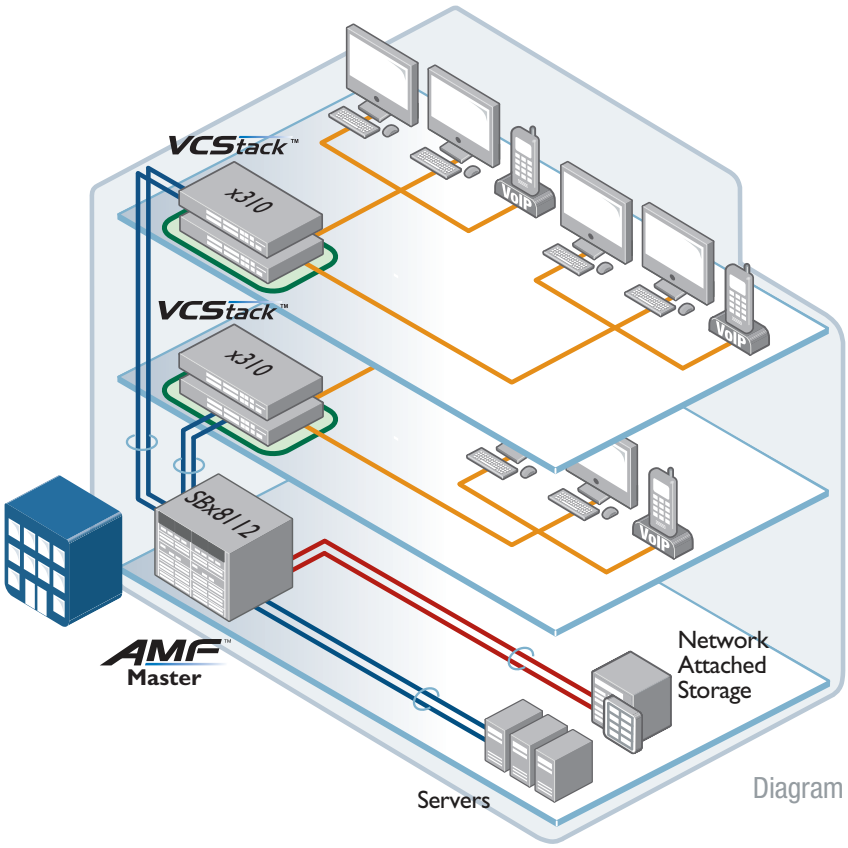


Diagram 2

Product Specifications

PRODUCT	10/100BASE-T (RJ-45) COPPER PORTS	100/1000 COMBO UPLINK PORTS	1 GIGABIT STACKING PORTS	POE CAPABLE PORTS	SWITCHING CAPACITY	FORWARDING RATE
x310-26FT	24	2	2	-	12.8 Gbps	9.5 Mpps
x310-50FT	48	2	2	-	17.6 Gbps	13.1 Mpps
x310-26FP	24	2	2	24	12.8 Gbps	9.5 Mpps
x310-50FP	48	2	2	48	17.6 Gbps	13.1 Mpps

Performance

- 4 Gbps of stacking bandwidth
- Supports 12KB Jumbo frames
- Wirespeed multicasting
- Up to 16K MAC addresses
- Up to 64 multicast entries
- 512MB DDR SDRAM
- 64MB flash memory
- Packet Buffer memory: x310-26 - 1.5MB
  x310-50 - 3MB

Reliability

- Modular AlliedWare Plus operating system
- Full environmental monitoring of PSU, fans, temperature and internal voltages. SNMP traps alert network managers in case of any failure

Power Characteristics

- AC Voltage: 90 to 260V (auto-ranging)
- Frequency: 47 to 63Hz

Expandability

- Stackable up to four units in a VCStack

Flexibility and compatibility

- Gigabit SFP ports on x310 Series will support any combination of Allied Telesis 100Mbps and 1000Mbps SFP modules listed in this document under Ordering Information
- Port speed and duplex configuration can be set manually or by auto-negotiation

Diagnostic Tools

- Active Fiber Monitoring detects tampering on optical links
- Built-In Self Test (BIST)
- Cable fault locator (TDR)
- UniDirectional Link Detection (UDLD)
- Find-me device locator
- Automatic link flap detection and port shutdown
- Optical Digital Diagnostic Monitoring (DDM)
- Ping polling for IPv4 and IPv6
-
- TraceRoute for IPv4 and IPv6

IPv4 Features

- Black hole routing
- Directed broadcast forwarding
- DNS relay
- Route redistribution (OSPF, RIP)
- Static unicast and multicast routes for IPv4
- UDP broadcast helper (IP helper)

IPv6 Features

- DHCPv6 client and relay
- IPv4 and IPv6 dual stack
- IPv6 hardware ACLs and QoS
- Device management over IPv6 networks with SNMPv6, Telnetv6 and SSHv6
- NTPv6 client and server
- Static unicast and multicast routes for IPv6

Management

- Front panel 7-segment LED provides at-a-glance status and fault information
- Autonomous Management Framework (AMF) enables powerful centralized management and zero-touch device installation and recovery
- Console management port on the front panel for ease of access
- Eco-friendly mode allows ports and LEDs to be disabled to save power
- Web-based Graphical User Interface (GUI)
- Industry-standard CLI with context-sensitive help
- Powerful CLI scripting engine
- Comprehensive SNMP MIB support for standards-based device management
- Built-in text editor
- Event-based triggers allow user-defined scripts to be executed upon selected system events
- USB interface allows software release files, configurations and other files to be stored for backup and distribution to other devices

Quality of Service (QoS)

- 8 priority queues with a hierarchy of high priority queues for real time traffic, and mixed scheduling, for each switch port
- Limit bandwidth per port or per traffic class down to 64kbps
- Wirespeed traffic classification with low latency essential for VoIP and real-time streaming media applications
- Policy-based QoS based on VLAN, port, MAC and general packet classifiers
- Policy-based storm protection
- Extensive remarking capabilities
- Taildrop for queue congestion control
- Strict priority, weighted round robin or mixed scheduling
- IP precedence and DiffServ marking based on layer 2, 3 and 4 headers

Resiliency

- Control Plane Prioritization (CPP) ensures the CPU always has sufficient bandwidth to process network control traffic
- Dynamic link failover (host attach)
- Ethernet Protection Switched Rings (EPSR) with SuperLoop Protection (SLP) and enhanced recovery for extra resiliency
- Loop protection: loop detection and thrash limiting
- PVST+ compatibility mode
- STP root guard
- VCStack fast failover minimizes network disruption

Security

- Access Control Lists (ACLs) for IPv4 and IPv6 based on layer 3 and 4 headers, per VLAN or port
- Configurable ACLs for management traffic
- Auth-fail and guest VLANs
- Authentication, Authorisation and Accounting (AAA)
- Bootloader can be password protected for device security
- BPDU protection
- DHCP snooping, IP source guard and Dynamic ARP Inspection (DAI)
- DoS attack blocking and virus throttling
- Dynamic VLAN assignment
- MAC address filtering and MAC address lock-down
- Network Access and Control (NAC) features manage endpoint security
- Port-based learn limits (intrusion detection)
- Private VLANs provide security and port isolation for multiple customers using the same VLAN
- Secure Copy (SCP)
- Strong password security and encryption
- Tri-authentication: MAC-based, web-based and IEEE 802.1x
- RADIUS group selection per VLAN or port
- RADIUS Proxy

Environmental specifications

- Operating Temperature Range:
  0°C to 45°C (32°F to 113°F) for AT-x310-26FT (fanless)
  0°C to 50°C (32°F to 122°F) for AT-x310-26FP/50FP/50FT
  Derated by 1°C per 305 meters (1,000 ft)
- Storage Temperature Range:
  -25°C to 70°C (-13°F to 158°F)
- Operating Relative Humidity Range:
  5% to 90% non-condensing
- Storage Relative Humidity Range:
  5% to 95% non-condensing
- Operating Altitude:
  3,048 meters maximum (10,000 ft)

Electrical approvals and compliances

- EMC: EN55022 class A, FCC class A, VCCI class A
- Immunity: EN55024, EN61000-3-levels 2 (Harmonics), and 3 (Flicker) – AC models only

Safety

- Standards: UL60950-1, CAN/CSA-C22.2 No. 60950-1-03, EN60950-1, EN60825-1, AS/NZS 60950.1
- Certification: UL, cUL

Restrictions on Hazardous Substances (RoHS) Compliance

- EU RoHS Compliant
- China RoHS Compliant

Physical specifications

PRODUCT	WIDTH X DEPTH X HEIGHT	MOUNTING	WEIGHT		PACKAGED DIMENSIONS
			UNPACKAGED	PACKAGED	
x310-26FT	340 x 215 x 44 mm (13.38 x 8.46 x 1.73 in)	1RU Rack Mount	2.4 kg (5.3 lb)	3.6 kg (7.9 lb)	48 x 30 x 10 cm (18.9 x 11.8 x 3.9 in)
x310-50FT	440 x 310 x 44 mm (17.32 x 12.20 x 1.73 in)	1RU Rack Mount	4.6 kg (10.2 lb)	6.1 kg (13.5 lb)	56 x 51 x 15 cm (22.1 x 20.1 x 5.9 in)
x310-26FP	440 x 360 x 44 mm (17.32 x 14.17 x 1.73 in)	1RU Rack Mount	5.4 kg (11.9 lb)	6.9 kg (15.2 lb)	56 x 51 x 15 cm (22.1 x 20.1 x 5.9 in)
x310-50FP	440 x 360 x 44 mm (17.32 x 14.17 x 1.73 in)	1RU Rack Mount	5.8 kg (12.8 lb)	7.3 kg (16.1 lb)	56 x 51 x 15 cm (22.1 x 20.1 x 5.9 in)

Power characteristics

PRODUCT	NO POE LOAD			FULL POE+ LOAD			MAX POE POWER	MAX POE PORTS AT 15W PER PORT	MAX POE+ PORTS AT 30W PER PORT
	MAX POWER CONSUMPTION	MAX HEAT DISSIPATION	NOISE	MAX POWER CONSUMPTION	MAX HEAT DISSIPATION	NOISE			
x310-26FT	24W	81 BTU/hr	Fanless	-	-	-	-	-	-
x310-50FT	48W	164 BTU/hr	33.4 dBA	-	-	-	-	-	-
x310-26FP	50W	168 BTU/hr	38.2 dBA	460W	308 BTU/hr	60.0 dBA	370W	24	12
x310-50FP	61W	209 BTU/hr	42.8 dBA	472W	349 BTU/hr	60.4 dBA	370W	24	12

Standards and Protocols

AlliedWare Plus Operating System

Version 5.4.9-1

Cryptographic Algorithms

FIPS Approved Algorithms

Encryption (Block Ciphers):

- AES (ECB, CBC, CFB and OFB Modes)
- 3DES (ECB, CBC, CFB and OFB Modes)

Block Cipher Modes:

- CCM
- CMAC
- GCM
- XTS

Digital Signatures & Asymmetric Key Generation:

- DSA
- ECDSA
- RSA

Secure Hashing:

- SHA-1
- SHA-2 (SHA-224, SHA-256, SHA-384. SHA-512)

Message Authentication:

- HMAC (SHA-1, SHA-2(224, 256, 384, 512)

Random Number Generation:

- DRBG (Hash, HMAC and Counter)

Non FIPS Approved Algorithms

RNG (AES128/192/256)
DES
MD5

Ethernet Standards

IEEE 802.2 Logical Link Control (LLC)
IEEE 802.3 Ethernet
IEEE 802.3af Power over Ethernet (PoE)
IEEE 802.3at Power over Ethernet plus (PoE+)
IEEE 802.3az Energy Efficient Ethernet (EEE)
IEEE 802.3u 100BASE-X
IEEE 802.3x Flow control - full-duplex operation
IEEE 802.3z 1000BASE-X

IPv4 Features

RFC 768 User Datagram Protocol (UDP)
RFC 791 Internet Protocol (IP)
RFC 792 Internet Control Message Protocol (ICMP)
RFC 793 Transmission Control Protocol (TCP)
RFC 826 Address Resolution Protocol (ARP)
RFC 894 Standard for the transmission of IP datagrams over Ethernet networks
RFC 919 Broadcasting Internet datagrams
RFC 922 Broadcasting Internet datagrams in the presence of subnets
RFC 932 Subnetwork addressing scheme
RFC 950 Internet standard subnetting procedure
RFC 951 Bootstrap Protocol (BootP)
RFC 1027 Proxy ARP
RFC 1035 DNS client
RFC 1042 Standard for the transmission of IP datagrams over IEEE 802 networks
RFC 1071 Computing the Internet checksum
RFC 1122 Internet host requirements
RFC 1191 Path MTU discovery
RFC 1256 ICMP router discovery messages
RFC 1518 An architecture for IP address allocation with CIDR
RFC 1519 Classless Inter-Domain Routing (CIDR)
RFC 1542 Clarifications and extensions for BootP
RFC 1591 Domain Name System (DNS)
RFC 1812 Requirements for IPv4 routers
RFC 1918 IP addressing
RFC 2581 TCP congestion control

IPv6 Features

RFC 1981 Path MTU discovery for IPv6
RFC 2460 IPv6 specification
RFC 2464 Transmission of IPv6 packets over Ethernet networks
RFC 2711 IPv6 router alert option
RFC 3484 Default address selection for IPv6
RFC 3587 IPv6 global unicast address format
RFC 3596 DNS extensions to support IPv6
RFC 4007 IPv6 scoped address architecture
RFC 4193 Unique local IPv6 unicast addresses
RFC 4213 Transition mechanisms for IPv6 hosts and routers
RFC 4291 IPv6 addressing architecture
RFC 4443 Internet Control Message Protocol (ICMPv6)
RFC 4861 Neighbor discovery for IPv6
RFC 4862 IPv6 Stateless Address Auto-Configuration (SLAAC)
RFC 5014 IPv6 socket API for source address selection
RFC 5095 Deprecation of type 0 routing headers in IPv6
RFC 5175 IPv6 Router Advertisement (RA) flags option
RFC 6105 IPv6 Router Advertisement (RA) guard

Management

AT Enterprise MIB including AMF MIB and SNMP traps
Optical DDM MIB
SNMPv1, v2c and v3
IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
RFC 1155 Structure and identification of management information for TCP/IP-based Internets
RFC 1157 Simple Network Management Protocol (SNMP)
RFC 1212 Concise MIB definitions
RFC 1213 MIB for network management of TCP/IP-based Internets: MIB-II
RFC 1215 Convention for defining traps for use with the SNMP
RFC 1227 SNMP MUX protocol and MIB
RFC 1239 Standard MIB
RFC 1724 RIPv2 MIB extension
RFC 2578 Structure of Management Information v2 (SMIv2)
RFC 2579 Textual conventions for SMIv2
RFC 2580 Conformance statements for SMIv2
RFC 2674 Definitions of managed objects for bridges with traffic classes, multicast filtering and VLAN extensions
RFC 2741 Agent extensibility (AgentX) protocol
RFC 2787 Definitions of managed objects for VRRP
RFC 2819 RMON MIB (groups 1,2,3 and 9)
RFC 2863 Interfaces group MIB
RFC 3176 sFlow: a method for monitoring traffic in switched and routed networks

RFC 3411 An architecture for describing SNMP management frameworks
RFC 3412 Message processing and dispatching for the SNMP
RFC 3413 SNMP applications
RFC 3414 User-based Security Model (USM) for SNMPv3
RFC 3415 View-based Access Control Model (VACM) for SNMP
RFC 3416 Version 2 of the protocol operations for the SNMP
RFC 3417 Transport mappings for the SNMP
RFC 3418 MIB for SNMP
RFC 3621 Power over Ethernet (PoE) MIB
RFC 3635 Definitions of managed objects for the Ethernet-like interface types
RFC 3636 IEEE 802.3 MAU MIB
RFC 4022 MIB for the Transmission Control Protocol (TCP)
RFC 4113 MIB for the User Datagram Protocol (UDP)
RFC 4188 Definitions of managed objects for bridges
RFC 4292 IP forwarding table MIB
RFC 4293 MIB for the Internet Protocol (IP)
RFC 4318 Definitions of managed objects for bridges with RSTP
RFC 4560 Definitions of managed objects for remote ping, traceroute and lookup operations
RFC 5424 Syslog protocol
RFC 6527 Definitions of managed objects for VRRPv3

Multicast Support

Bootstrap Router (BSR) mechanism for PIM-SM
IGMP query solicitation
IGMP snooping (IGMPv1, v2 and v3)
IGMP snooping fast-leave
IGMP/MLD multicast forwarding (IGMP/MLD proxy)
MLD snooping (MLDv1 and v2)
PIM SM and PIM SSM for IPv6
RFC 1112 Host extensions for IP multicasting (IGMPv1)
RFC 2236 Internet Group Management Protocol v2 (IGMPv2)
RFC 2710 Multicast Listener Discovery (MLD) for IPv6
RFC 2715 Interoperability rules for multicast routing protocols
RFC 3306 Unicast-prefix-based IPv6 multicast addresses
RFC 3376 IGMPv3
RFC 3810 Multicast Listener Discovery v2 (MLDv2) for IPv6
RFC 3956 Embedding the Rendezvous Point (RP) address in an IPv6 multicast address
RFC 3973 PIM Dense Mode (DM)
RFC 4541 IGMP and MLD snooping switches
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

Open Shortest Path First (OSPF)

OSPF link-local signaling
OSPF MD5 authentication
Out-of-band LSDB resync
RFC 1245 OSPF protocol analysis
RFC 1246 Experience with the OSPF protocol
RFC 1370 Applicability statement for OSPF
RFC 1765 OSPF database overflow
RFC 2328 OSPFv2
RFC 2370 OSPF opaque LSA option
RFC 2740 OSPFv3 for IPv6
RFC 3101 OSPF Not-So-Stubby Area (NSSA) option
RFC 3509 Alternative implementations of OSPF area border routers
RFC 3623 Graceful OSPF restart
RFC 3630 Traffic engineering extensions to OSPF
RFC 4552 Authentication/confidentiality for OSPFv3
RFC 5329 Traffic engineering extensions to OSPFv3
RFC 5340 OSPFv3 for IPv6 (partial support

Quality of Service (QoS)

IEEE 802.1p Priority tagging
RFC 2211 Specification of the controlled-load network element service
RFC 2474 DiffServ precedence for eight queues/port
RFC 2475 DiffServ architecture
RFC 2597 DiffServ Assured Forwarding (AF)
RFC 2697 A single-rate three-color marker
RFC 2698 A two-rate three-color marker
RFC 3246 DiffServ Expedited Forwarding (EF)

Resiliency Features

ITU-T G.8023 / Y.1344 Ethernet Ring Protection Switching (ERPS)
IEEE 802.1AX Link aggregation (static and LACP)
IEEE 802.1D MAC bridges
IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
IEEE 802.3ad Static and dynamic link aggregation
RFC 5798 Virtual Router Redundancy Protocol version 3 (VRRPv3) for IPv4 and IPv6

Routing Information Protocol (RIP)

RFC 1058 Routing Information Protocol (RIP)
RFC 2080 RIPng for IPv6
RFC 2081 RIPng protocol applicability statement
RFC 2082 RIP-2 MD5 authentication
RFC 2453 RIPv2

Security Features

SSH remote login
SSLv2 and SSLv3
TACACS+ Accounting, Authentication and Authorization (AAA)
IEEE 802.1X authentication protocols (TLS, TTLS, PEAP and MD5)
IEEE 802.1X multi-supplicant authentication
IEEE 802.1X port-based network access control
RFC 2560 X.509 Online Certificate Status Protocol (OCSP)
RFC 2818 HTTP over TLS ("HTTPS")
RFC 2865 RADIUS authentication
RFC 2866 RADIUS accounting
RFC 2868 RADIUS attributes for tunnel protocol support
RFC 2986 PKCS #10: certification request syntax specification v1.7
RFC 3546 Transport Layer Security (TLS) extensions
RFC 3579 RADIUS support for Extensible Authentication Protocol (EAP)
RFC 3580 IEEE 802.1x RADIUS usage guidelines
RFC 3748 PPP Extensible Authentication Protocol (EAP)
RFC 4251 Secure Shell (SSHv2) protocol architecture
RFC 4252 Secure Shell (SSHv2) authentication protocol
RFC 4253 Secure Shell (SSHv2) transport layer protocol
RFC 4254 Secure Shell (SSHv2) connection protocol
RFC 5246 Transport Layer Security (TLS) v1.2
RFC 5280 X.509 certificate and Certificate Revocation List (CRL) profile
RFC 5425 Transport Layer Security (TLS) transport mapping for Syslog
RFC 5656 Elliptic curve algorithm integration for SSH
RFC 6125 Domain-based application service identity within PKI using X.509 certificates with TLS
RFC 6614 Transport Layer Security (TLS) encryption for RADIUS
RFC 6668 SHA-2 data integrity verification for SSH

Services

RFC 854 Telnet protocol specification
RFC 855 Telnet option specifications
RFC 857 Telnet echo option
RFC 858 Telnet suppress go ahead option
RFC 1091 Telnet terminal-type option
RFC 1350 Trivial File Transfer Protocol (TFTP)
RFC 1985 SMTP service extension
RFC 2049 MIME
RFC 2131 DHCPv4 (server, relay and client)
RFC 2132 DHCP options and BootP vendor extensions
RFC 2616 Hypertext Transfer Protocol - HTTP/1.1
RFC 2821 Simple Mail Transfer Protocol (SMTP)
RFC 2822 Internet message format
RFC 3046 DHCP relay agent information option (DHCP option 82)
RFC 3315 DHCPv6 client
RFC 3993 Subscriber-ID suboption for DHCP relay agent option
RFC 4330 Simple Network Time Protocol (SNTP) version 4
RFC 5905 Network Time Protocol (NTP) version 4

VLAN Support

IEEE 802.1Q Virtual LAN (VLAN) bridges
IEEE 802.1v VLAN classification by protocol and port
IEEE 802.3ac VLAN tagging

Voice over IP (VoIP)

LLDP-MED ANSI/TIA-1057
Voice VLAN

Ordering Information

Feature Licenses

NAME	DESCRIPTION	INCLUDES	STACK LICENSING
AT-FL-x310-01	x310 premium license	▶ RIP (64 routes) ▶ OSPF (64 routes) ▶ PIMv4-SM, DM and SSM ▶ EPSR master ▶ RIPng (64 routes) ▶ OSPFv3 (64 routes) ▶ PIMv6-SM and SSM ▶ UDLD ▶ VRRP	▶ One license per stack member
AT-FL-x310-0F13-1YR	OpenFlow license	▶ OpenFlow v1.3 for 1 year	▶ Not supported on a stack
AT-FL-x310-0F13-5YR	OpenFlow license	▶ OpenFlow v1.3 for 5 years	▶ Not supported on a stack
AT-FL-x310-8032	ITU-T G.8032 license	▶ G.8032 ring protection ▶ Ethernet CFM	▶ One license per stack member

Switches

AT-x310-26FT-xx
24-port 10/100BASE-T switch with 2 combo ports (100/1000X SFP or 10/100/1000T) and 2 stacking ports

AT-x310-50FT-xx
48-port 10/100BASE-T switch with 2 combo ports (100/1000X SFP or 10/100/1000T) and 2 stacking ports

AT-x310-26FP-xx
24-port 10/100BASE-T PoE+ switch with 2 combo ports (100/1000X SFP or 10/100/1000T) and 2 stacking ports

AT-x310-50FP-xx
48-port 10/100BASE-T PoE+ switch with 2 combo ports (100/1000X SFP or 10/100/1000T) and 2 stacking ports

Where xx = 10 for US power cord
20 for no power cord
30 for UK power cord
40 for Australian power cord
50 for European power cord

SFP modules

AT-SPFX/2
100FX multi-mode 1310 nm fiber up to 2 km

AT-SPFX/15
100FX single-mode 1310 nm fiber up to 15 km

AT-SPFXBD-LC-13
100BX Bi-Di (1310 nm Tx,1550 nm Rx) fiber up to 10 km

AT-SPFXBD-LC-15
100BX Bi-Di (1550 nm Tx,1310 nm Rx) fiber up to 10 km

AT-SPSX
1000SX GbE multi-mode 850 nm fiber up to 550 m

AT-SPSX/I
1000SX GbE multi-mode 850 nm fiber up to 550 m industrial temperature

AT-SPEX
1000X GbE multi-mode 1310 nm fiber up to 2 km

AT-SPLX10
1000LX GbE single-mode 1310 nm fiber up to 10 km

AT-SPLXI0/I
1000LX GbE single-mode 1310 nm fiber up to 10 km industrial temperature

AT-SPBDI0-13
1000LX GbE Bi-Di (1310 nm Tx, 1490 nm Rx) fiber up to 10 km

AT-SPBDI0-14
1000LX GbE Bi-Di (1490 nm Tx, 1310 nm Rx) fiber up to 10 km

AT-SPLX40
1000LX GbE single-mode 1310 nm fiber up to 40 km

AT-SPZX80
1000ZX GbE single-mode 1550 nm fiber up to 80 km

AT-SPBD20-13/I
1000BX GbE Bi-Di (1310 nm Tx, 1550 nm Rx) fiber up to 20 km

AT-SPBD20-14/I
1000BX GbE Bi-Di (1490 nm Tx, 1310 nm Rx) fiber up to 20 km

AT-SP10TW1
1 meter SFP direct attach cable

AT-SP10TW3
3 meter SFP direct attach cable

AT-SP10TW7
7 meter SFP direct attach cable

(Note that any Allied Telesis direct attach cable can also be used for stacking)

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com

© 2019 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.
617-000510 RevZD