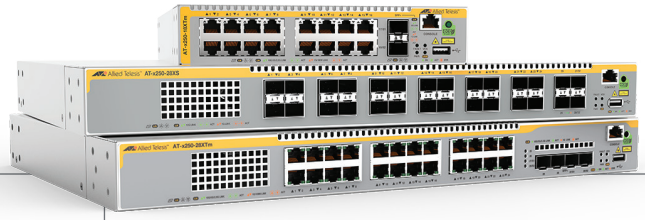
x250 Series

10 Gigabit Stackable Edge Switches



Allied Telesis x250 Series switches provide a superior high-speed access solution delivering up to 10G connectivity for next generation networks. The x250 Series fiber models support 1/10G (SFP and SFP+) on all ports, making them ideal for long-distance connections, and for high-capacity devices such as servers. The copper models support 1/2.5/5/10G (Multi-Gigabit) for flexible deployment options and the ability to support all end devices.

The x250 Series can form a virtual chassis stack (VCStack™) allowing 2 units to be managed as a single virtual device for simplicity and flexibility.

Resiliency

Converging network services means increasing demand for highly available networks with minimal downtime. VCStack, in conjunction with link aggregation, provides a network with no single point of failure, and provides access application resiliency.

Ethernet Protection Switched Ring (EPSRing™), and the standards-based G.8032 Ethernet Ring Protection, ensure distributed networks have high-speed access to online resources.

Secure

Network security is guaranteed, with powerful control over network traffic types, secure management options, and multi-layered security features.

Network Access Control (NAC) gives unprecedented control over user access to the network, in order to mitigate threats.

The x250 Series uses 802.1x port-based authentication, in partnership with standards-compliant dynamic VLAN assignment, to assess a user's adherence to network security policies and either grant access or offer remediation. Tri-authentication ensures the network is only accessed by known users and devices. Secure access is also available for guests.

Security from malicious network attacks is provided by features such as DHCP snooping, STP root guard, BPDU protection and access control lists. Each of these can be configured to perform a variety of actions upon detection of a suspected attack.

Network protection

Advanced storm protection features include bandwidth limiting, policy-based storm protection and packet storm protection.

Network storms are often caused by cabling errors that result in a loop. The x250 Series loop detection and thrash limiting take immediate action to prevent network storms.

Manageable

The x250 Series run the advanced AlliedWare Plus™ fully featured operating system, delivering a rich feature set and an industry-standard Command Line Interface (CLI). This reduces training requirements and is consistent across all AlliedWare Plus devices, simplifying network management.

The Device GUI (Graphical User Interface) is an easy-to-use and powerful management tool, with comprehensive monitoring facilities.

Future-proof

x250 Series switches are Software Defined Networking (SDN) ready and able to support OpenFlow v1.3.

Powerful network management

Autonomous Management Framework Plus (AMF Plus) automates many 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.

The x250 Series acting as AMF Plus members benefit from centralized management and network automation.

Cybersecurity

The x250 Series acting as AMF Plus members are compatible with our AMF-Security solution, which enables a self-defending network. The AMF–Sec controller responds immediately to any internal malware threats by instructing the x250 Series to isolate the affected part of the network, and quarantine the suspect device. Vista Manager EX alerts network administrators of threats that have been dealt with.

Key Features

- AlliedWare Plus fully featured OS
- AMF Plus member for network automation and management
- AMF-Security compatible
- 1/2.5/5/10G (Multi-Gigabit) connectivity on copper ports
- 1/10G (SFP and SFP+) connectivity on fiber ports
- VCStack 2 units at any speed
- EPSR & G.8032 high-speed resilient rings
- Active Fiber Monitoring
- Link Monitoring
- VLAN ACLs
- Precision Time Protocol (PTP) transparent mode
- Enhanced Transmission Selection (ETS)
- VLAN mirroring (RSPAN)
- Upstream Forwarding Only (UFO)
- OpenFlow for SDN
- NETCONF/RESTCONF with YANG data modelling

KEY FEATURES

Autonomous Management Framework Plus (AMF Plus)

AMF Plus 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 Plus secure mode encrypts all AMF traffic, provides unit and user authorization, and monitors network access to greatly enhance network security.

An AMF Plus license operating in the network provides all standard AMF network management and automation features, and also enables the AMF Plus intent-based networking features in Vista Manager EX (from version 3.10.1 onwards).

High Speed

The x250 Series supports Multi-Gigabit (1/2.5/5/10G) speeds on copper and SFP and SFP+ (1/10G) speeds on fiber, for flexible high-density high-speed edge connectivity in next-generation networks.

Virtual Chassis Stacking (VCStack™)

Create a VCStack of two units with 40Gbps stacking bandwidth to each unit, which has dual links for increased 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.

Ethernet Protection Switched Ring (EPSRing™)

EPSRing allows several x250 switches to join a protected ring capable of recovery within as little as 50ms. This feature is perfect for 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.

NETCONF/RESTCONF

NETCONF/RESTCONF with YANG data modeling provides a standardized way to represent data and securely configure devices.

Access Control Lists (ACLs)

The x250 Series features industry-standard access control functionality through ACLs, which filter network traffic to control whether 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. An example of this would be to provide traffic flow control.

VLAN Access Control List (ACLs)

ACLs simplify access and traffic control across entire segments of the network. They can be applied to a VLAN as well as a specific port.

Easy To Manage

The AlliedWare Plus operating system incorporates an industry standard CLI, facilitating intuitive manageability.

With three distinct modes, the CLI is very secure, and the use of SSHv2 encrypted and strongly authenticated remote login sessions ensures CLI access is not compromised.

Storm protection

Advanced packet storm control features protect the network from broadcast storms:

Bandwidth limiting minimizes the effects of the storm by reducing the amount of flooding traffic.

Policy-based storm protection is more powerful than bandwidth limiting. It restricts storm damage to within the storming VLAN, with a defined traffic rate. The action the device should take when it detects a storm can be configured, such as disabling the port from the VLAN or shutting the port down.

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, called Loop Detection Frames (LDF), that the switch listens for. If a port receives an LDF packet, one can choose to disable the port, disable the link, or send an SNMP trap.

Spanning Tree Protocol (STP) Root Guard

STP root guard designates which devices can assume the root bridge role in an STP network. This stops an undesirable device from taking over this role, where it could either compromise network performance or cause a security weakness.

Bridge Protocol Data Unit (BPDU) protection

BPDU protection adds extra security to STP. It protects the spanning tree configuration by preventing malicious DoS attacks caused by spoofed BPDUs. If a BPDU packet is received on a protected port, the BPDU protection feature disables the port and alerts the network manager.

sFlow

sFlow monitors switched networks, and provides visibility to enable performance optimization, usage accounting/billing, and defense against security threats. Sampled packets sent to a collector provide a real-time view of network traffic.

Tri-authentication

Authentication options include 802.1x port authentication, web authentication for guest access, and MAC authentication for end points without an 802.1x supplicant. All three can be used simultaneously.

Upstream Forwarding Only (UFO)

UFO lets you manage which ports in a VLAN can communicate with each other, and which only have upstream access to services, for secure multi-user deployment.

TACACS+ Command Authorization

TACACS+ Command Authorization offers centralized control over which commands may be issued by each specific AlliedWare Plus device user. It complements authentication and accounting services for an AAA solution.

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.

Optical DDM

Most modern optical SFP/SFP+/XFP transceivers support Digital Diagnostics Monitoring (DDM) functions according to the specification SFF-8472. This enables real time monitoring of the various parameters of the transceiver, such as optical output power, temperature, laser bias current and transceiver supply voltage. Easy access to this information simplifies diagnosing problems with optical modules and fiber connections.

Active Fiber Monitoring

AFM prevents eavesdropping on fiber data or stacking links by monitoring received optical power. If an intrusion is detected, the link can be automatically shut down, or an alert sent.

VLAN Mirroring (RSPAN)

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

Find Me

In busy server rooms comprised of a large number of equipment racks, it can be quite a job finding the correct switch quickly among many similar units. The "Find Me" feature is a simple visual way to quickly identify the desired physical switch for maintenance or other purposes, by causing its LEDs to flash in a specified pattern.

Precision Time Protocol (PTP)

PTP (IEEE 1588v2) sychronizes clocks throughout the network with micro-second accuracy, supporting industrial automation and control systems.

Link Monitoring (Linkmon)

Linkmon enables network health monitoring by regularly sending probes over key links to gather metrics comprising latency, jitter, and probe loss. This supports pro-active network management, and can also be used with triggers to automate a change to device or network configuration in response to the declining health of a monitored link.

Quality of Service

Enhanced Transmission Selection (ETS) provides quality of service by allocating bandwidth to important traffic classes, with the flexibility to share remaining bandwidth to maximize traffic throughput and performance.

Easy network upgrade

Increasing network performance by upgrading existing edge switches to the x250 Series is easy. AMF Plus auto-recovery enables a plug-and-play upgrade, as the x250 switches are auto-configured to match the previous devices.

10G edge connectivity

The increasing popularity of remote working and use of next-generation high-bandwidth applications such as video conferencing require ever faster networks.

As shown in diagram 1, the x250 Series supports up to 10G copper or fiber connectivity to end devices, to enable a fully-featured and secure solution that is cost-effective, flexible and future-proof.

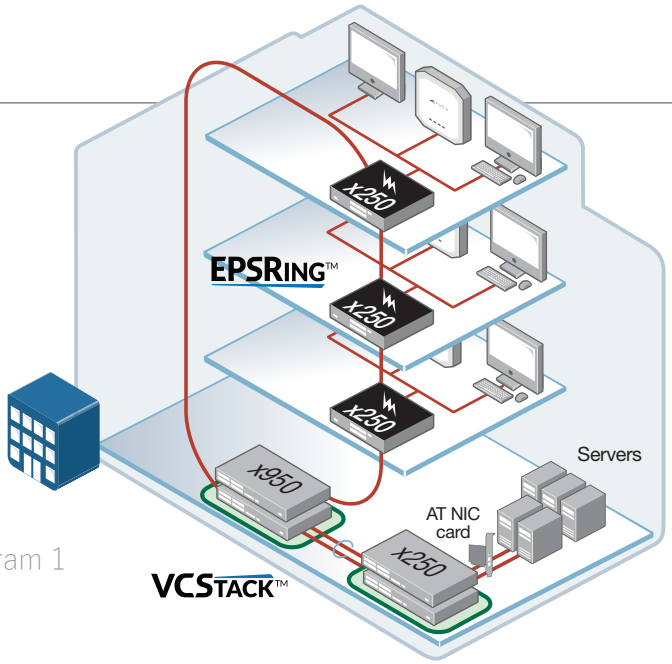


Diagram 1

High performing network flexibility

The x250 Series is available in both copper models with 1/2.5/5/10G (Multi-Gigabit) ports, or fiber models with 1/10G (SFP and SFP+) ports, for flexible distribution and edge deployment connecting any device, as shown in diagram 2.

VCStack enables deploying a single virtual unit comprised of 2 physical copper and/or fiber switches for a fully resilient solution. When combined with other advanced Allied Telesis products, such as x540L series distribution switches and the SBx908 GEN2 and x950 core switches, high-speed networks with 10G speeds all the way to the edge can be deployed.

AMF Plus provides an easy yet powerful solution for managing multiple devices with plug-and-play simplicity.

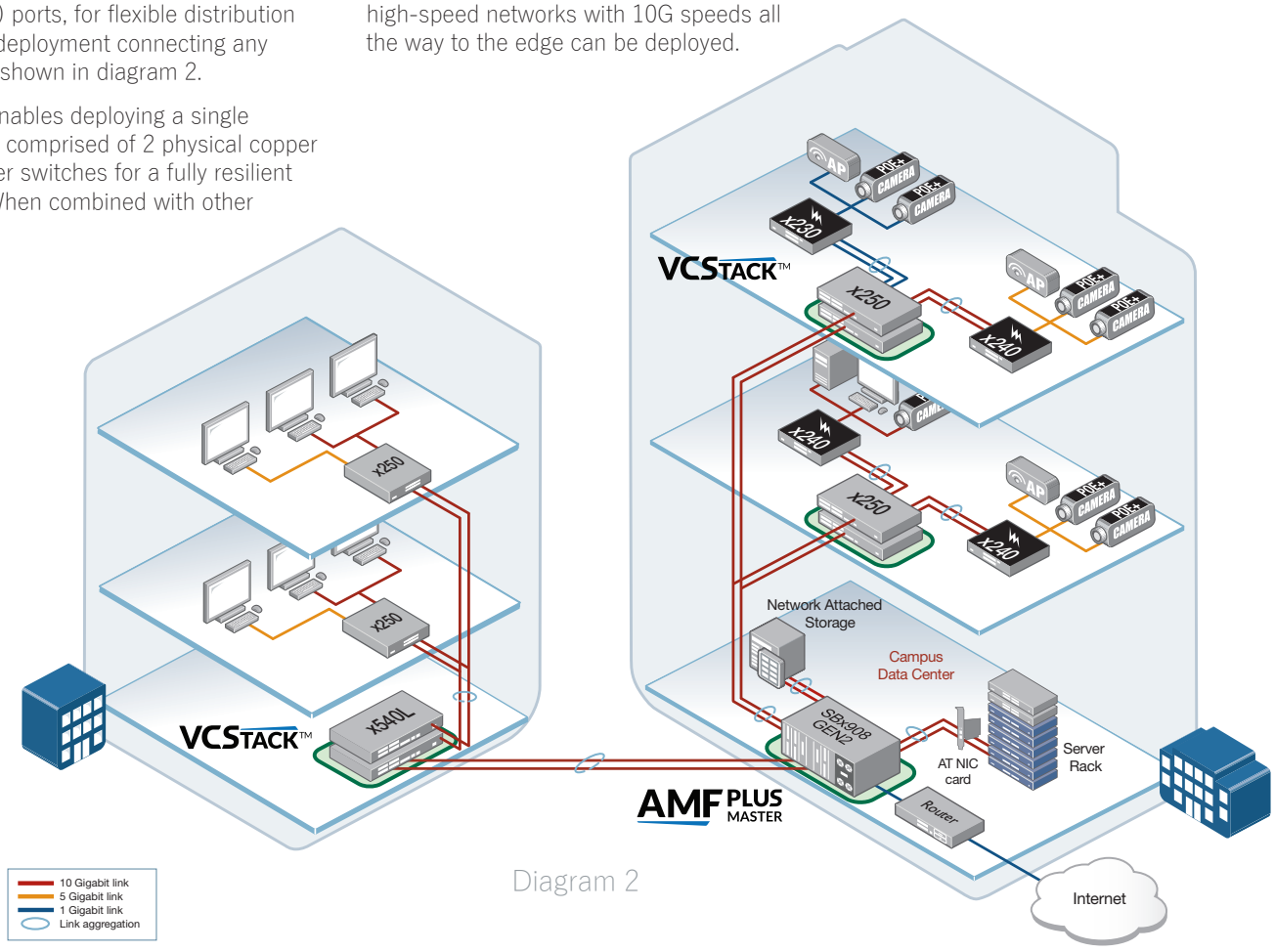


Diagram 2

SPECIFICATIONS

Product Specifications

	100/1000T/2.5/5/10G (RJ-45) copper ports	1/10 Gigabit sfp+ ports	Total Ports	Switching Fabric	Forwarding Rate
x250-18XTm	16	2	18	360Gbps	267.9Mpps
x250-28XTm	24	4	28	560Gbps	416.7Mpps
x250-18XS	-	18	18	360Gbps	267.9Mpps
x250-28XS	-	28	28	560Gbps	416.7Mpps

Physical Specifications

	Width	Depth	Height	Weight
x250-18XTm	210 mm (8.27 in)	346 mm (13.62 in)	42.5 mm (1.67 in)	TBD
x250-28XTm	440 mm (17.32 in)	290 mm (11.41 in)	44 mm (1.73 in)	4.0 kg (8.8 lb)
x250-18XS	210 mm (8.27 in)	346 mm (13.62 in)	42.5 mm (1.67 in)	2.7 kg (5.9 lb)
x250-28XS	440 mm (17.32 in)	290 mm (11.41 in)	44 mm (1.73 in)	3.8 kg (8.3 lb)

Power and Noise

	Max Power Consumption	Max Heat dissipation	Noise
x250-18XTm	110W	360 BTU/h	41-58 db
x250-28XTm	160W	540 BTU/h	46-63 db
x250-18XS	70W	236 BTU/h	39-48 db
x250-28XS	86W	293 BTU/h	39-52 db

Latency (microseconds)

	Port Speed			
	1Gbps	2.5Gbps	5Gbps	10Gbps
x250-18XTm	4.86µs	7.23µs	4.63µs	3.49µs
x250-28XTm	4.48µs	8.43µs	5.72µs	2.73µs
x250-18XS	3.65µs	-	-	1.84µs
x250-28XS	3.59µs	-	-	1.60µs

Performance

- Up to 32K MAC addresses
- Up to 16 static or RIP routes
- 2GB DDR SDRAM
- 4094 configurable VLANs
- 256MB flash memory
- Packet Buffer memory: 8MB
- Supports 10KB L2 jumbo frames
- Wirespeed forwarding

Reliability

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

Flexibility and compatibility

- 10G SFP+ ports will support any combination of Allied Telesis 1000Mbps SFP and 10GbE SFP+ modules and direct attach cables listed in this document under Ordering Information

Diagnostic tools

- Active Fiber Monitoring detects tampering on optical links
- Find-me device locator
- Connectivity Fault Management (CFM) for use with G.8032 ERPS
- Link Monitoring
- Automatic link flap detection and port shutdown
- Optical Digital Diagnostic Monitoring (DDM)
- Ping polling for IPv4 and IPv6
- Port mirroring
  - No limit on mirrored ports
  - Up to 7 mirror (analyzer) ports
- VLAN mirroring (RSPAN)
- TraceRoute for IPv4 and IPv6
- Uni-Directional Link Detection (UDLD)

IPv4 Features

- Equal Cost Multi Path (ECMP) routing
- Static and RIP routing for IPv4
- UDP broadcast helper (IP helper)
- Directed broadcast forwarding
- DHCP client, relay and server for IPv4
- Black hole routing
- DNS relay
- Route redistribution (RIP)
- Policy-based routing

IPv6 Features

- DHCPv6 client and relay
- IPv4 and IPv6 dual stack
- IPv6 hardware ACLs
- Device management over IPv6 networks with SNMPv6, Telnetv6 and SSHv6
- Static unicast routing for IPv6
- Log to IPv6 hosts with Syslog v6

Management

- Autonomous Management Framework Plus (AMF Plus) enables powerful centralized management and zero-touch device installation and recovery
- Console management port on the front panel for ease of access
- NETCONF/RESTCONF northbound interface with YANG data modelling
- Eco-friendly mode allows ports and LEDs to be disabled to save power
- Industry-standard CLI with context-sensitive help
- Management stacking allows up to 32 devices to be managed from a single console
- 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
- Web-based Graphical User Interface (GUI)

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
- Queue scheduling options for strict priority, weighted round robin or mixed scheduling
- IP precedence and DiffServ marking based on layer 2, 3 and 4 headers
- Enhanced Transmission Selection (ETS)

Resiliency Features

- SFP+ stacking ports can be configured as 10G Ethernet ports
- Control Plane Prioritization (CPP) ensures the CPU always has sufficient bandwidth to process network control traffic
- Dynamic link failover (host attach)
- EPSR (Ethernet Protection Switched Rings) with SuperLoop Protection (SLP)

- Ethernet Ring Protection Switching (ITU-T G.8032 ERPS)
- Flexi-stacking - use any port-speed to stack
- Link aggregation (LACP) on LAN ports
- Long-distance stacking with 10G SFP+ modules (LD-VCStack)
- Loop protection: loop detection and thrash limiting
- PVST+ compatibility mode
- RRP snooping
- Spanning Tree Protocols (STP, RSTP, MSTP)
- STP root guard
- VCStack fast failover minimizes network disruption

Security Features

- Access Control Lists (ACLs) based on layer 3 and 4 headers
- Configurable ACLs for management traffic
- Auth fail and guest VLANs
- Authentication, Authorization and Accounting (AAA) for TACACS+ and RADIUS
- 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
- Local RADIUS server for user and device authentication
- Network Access and Control (NAC) features manage endpoint security
- Port-based learn limits (intrusion detection)
- RADIUS group selection per VLAN or port
- Secure Copy (SCP)
- Secure File Transfer Protocol (SFTP) client
- Strong password security and encryption
- Simple Certificate Enrollment Protocol (SCEP) supports secure management
- Tri-authentication: MAC-based, web-based and IEEE 802.1x

VLAN Features

- Private VLANs provide security and port isolation for multiple customers using the same VLAN
- Upstream Forwarding Only (UFO)
- VLAN ID translation
- Voice VLAN

Environmental Specifications

- Operating temperature range:
  0°C to 50°C (32°F to 122°F)
  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:
  3,000 meters maximum (9,843 ft)

Electrical approvals and compliances

- EMC: ETSI EN300-386, EN300-132-2, FCC class A, VCCI class A
- Immunity: EN55024, EN61000-3-levels 2 (Harmonics), and 3 (Flicker) – AC models only

Safety

- Standards: UL62368-1, CAN/CSA-C22.2 No. 60950-1-03, EN60950-1, EN60825-1, AS/NZS 60950.1
- Certifications: UL, cUL, UL-EU

Restrictions on Hazardous Substances (RoHS) Compliance

- EU RoHS compliant
- China RoHS compliant

STANDARDS & PROTOCOLS

AlliedWare Plus Operating System

Version 5.5.6

Authentication

RFC 1321 MD5 Message-Digest algorithm
RFC 1828 IP authentication using keyed MD5

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

IEEE 802.2 Logical Link Control (LLC)
IEEE 802.3 Ethernet
IEEE 802.3ab1000BASE-T
IEEE 802.3ae10 Gigabit Ethernet
IEEE 802.3an10GBASE-T
IEEE 802.3azEnergy Efficient Ethernet (EEE)
IEEE 802.3bz2.5GBASE-T and 5GBASE-T ("multi-gigabit")
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 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 1518 An architecture for IP address allocation with CIDR
RFC 1519 Classless Inter-Domain Routing (CIDR)
RFC 1591 Domain Name System (DNS)
RFC 1812 Requirements for IPv4 routers
RFC 1918 IP addressing
RFC 2581 TCP congestion control
RFC 3021 Using 31-Bit Prefixes on IPv4 Point-to-Point Links

IPv6 Features

RFC 1981 Path MTU discovery for IPv6
RFC 2460 IPv6 specification
RFC 2464 Transmission of IPv6 packets over Ethernet networks
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

Management

AMF MIB and SNMP traps
AT Enterprise MIB
Optical DDM MIB
SNMP support SNMPv1, v2c and v3
ANSI/TIA-1057 LLDP-Media Endpoint Detection
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 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 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 The Syslog protocol

Multicast support

IGMP snooping (IGMPv1, v2 and v3)
IGMP snooping fast-leave
MLD snooping (MLDv1 and v2)
RFC 4541 IGMP and MLD snooping switches

Quality of Service (QoS)

IEEE 802.1p Priority tagging
IEEE 802.1Qaz Enhanced Transmission Selection (ETS)
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.8032 / Y.1344 Ethernet Ring Protection Switching (ERPS)
IEEE 802.1ag CFM Continuity Check Protocol (CCP)
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

Routing Information Protocol (RIP)

RFC 1058 Routing Information Protocol (RIP)
RFC 2082 RIP-2 MD5 authentication
RFC 2453 RIPv2

Security Features

SSH remote login
SSLv2 and SSLv3
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 5176 RADIUS Change of Authorization (CoA)
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
RFC 8446 Transport Layer Security (TLS) v1.3
RFC 8894 Simple Certificate Enrollment Protocol (SCEP)

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 client
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 3396 Encoding long options in DHCPv4
RFC 3646 DNS configuration options for DHCPv6
RFC 3993 Subscriber-ID suboption for DHCP relay agent option
RFC 4330 Simple Network Time Protocol (SNTP) version 4
RFC 4954 SMTP service extension for authentication
RFC 5905 Network Time Protocol (NTP) version 4

VLAN support

IEEE 802.1ad Provider bridges (VLAN stacking, Q-in-Q)
IEEE 802.1Q Virtual LAN (VLAN) bridges
IEEE 802.1v VLAN classification by protocol and port
IEEE 802.3ac VLAN tagging

Feature Licenses

	Description	Includes	Stack Licensing
AT-FL-x250-APP	VLAN Q-in-Q and PTP license	■ VLAN Q-in-Q ■ PTP Transparent Mode ■ VLAN translation	■ One license per stack member
AT-FL-x250-OF13-1YR	OpenFlow license	■ OpenFlow v1.3 for 1 year	■ Not supported on a stack
AT-FL-x250-OF13-5YR	OpenFlow license	■ OpenFlow v1.3 for 5 years	■ Not supported on a stack

ORDERING INFORMATION

AT-x250-18XTm	16-port 100M/1/2.5/5/10G stackable copper switch with 2 x SFP/SFP+ports, and a single fixed PSU
AT-x250-28XTm	24-port 100M/1/2.5/5/10G stackable copper switch with 4 x SFP/SFP+ports, and a single fixed PSU
AT-x250-18XS	18-port SFP/SFP+ stackable fiber switch, with a single fixed PSU
AT-x250-28XS	28-port SFP/SFP+ stackable fiber switch, with a single fixed PSU
AT-BRKT-J24	Wall mount bracket
AT-RKMT-J14	Rack mount kit for x250-18XTm and x250-18XS
AT-RKMT-J15	Rack mount kit to install two devices side by side in a 19-inch equipment rack - x250-18XTm and x250-18XS
AT-STND-J03	Stand-kit for x250-xx

Accessories

10GbE SFP+ Modules

Any 10G SFP+ module or cable can be used for stacking with the front panel 10G ports

AT-SP10SR	10GSR 850 nm short-haul, 300 m with MMF
AT-SP10SR/I	10GSR 850 nm short-haul, 300 m with MMF industrial temperature
AT-SP10LRa/I	10GLR 1310 nm medium-haul, 10 km with SMF industrial temperature TAA[1]
AT-SP10ER40a/I	10GER 1310 nm long-haul, 40 km with SMF industrial temperature
AT-SP10ZR80/I	10GER 1550 nm long-haul, 80 km with SMF industrial temperature
AT-SP10TM/I	1G/2.5G/5G/10G, 100 m copper, industrial temperature, TAA[5]
AT-SP10BD10/I-12	10 GbE Bi-Di (1270 nm Tx, 1330 nm Rx) fiber up to 10 km industrial temperature, TAA[1]
AT-SP10BD10/I-13	10 GbE Bi-Di (1330 nm Tx, 1270 nm Rx) fiber up to 10 km industrial temperature, TAA[1]
AT-SP10BD20-12	10 GbE Bi-Di (1270 nm Tx, 1330 nm Rx) fiber up to 20 km, TAA[1]
AT-SP10BD20-13	10 GbE Bi-Di (1330 nm Tx, 1270 nm Rx) fiber up to 20 km, TAA[1]
AT-SP10BD40/I-12	10 GbE Bi-Di (1270 nm Tx, 1330 nm Rx) fiber up to 40 km industrial temperature, TAA[1]
AT-SP10BD40/I-13	10 GbE Bi-Di (1330 nm Tx, 1270 nm Rx) fiber up to 40 km industrial temperature, TAA[1]
AT-SP10BD80/I-14	10 GbE Bi-Di (1490 nm Tx, 1550 nm Rx) fiber up to 80 km industrial temperature, TAA[1]
AT-SP10BD80/I-15	10 GbE Bi-Di (1550nm Tx, 1490 nm Rx) fiber up to 80 km industrial temperature, TAA[1]
AT-SP10TW1	1 meter SFP+ direct attach cable
AT-SP10TW3	3 meter SFP+ direct attach cable

1000Mbps SFP Modules

AT-SPSX	1000SX GbE multi-mode 850 nm fiber up to 550 m
AT-SPLX10a	1000LX GbE single-mode 1310 nm fiber up to 10 km
AT-SPLX10a/I	1000LX GbE single-mode 1310 nm fiber up to 10 km industrial temperature
AT-SPBD10-13	1000LX GbE Bi-Di (1310 nm Tx, 1490 nm Rx) fiber up to 10 km
AT-SPBD10-14	1000LX GbE Bi-Di (1490 nm Tx, 1310 nm Rx) fiber up to 10 km
AT-SPBD20-13/I	1000BX GbE Bi-Di (1310 nm Tx, 1490 nm Rx) fiber up to 20 km industrial temperature
AT-SPBD20-14/I	1000BX GbE Bi-Di (1490 nm Tx, 1310 nm Rx) fiber up to 20 km industrial temperature
AT-SPBD40-13/I	1000LX GbE single-mode Bi-Di (1310 nm Tx, 1490 nm Rx) fiber up to 40 km, industrial temperature
AT-SPBD40-14/I	1000LX GbE single-mode Bi-Di (1490 nm Tx, 1310 nm Rx) fiber up to 40 km, industrial temperature
AT-SPLX40	1000LX GbE single-mode 1310 nm fiber up to 40 km
AT-SPTXc	10/100/1000 TX (RJ45), up to 100 m

[1] Trade Act Agreement compliant