IE560-12GSX

Industrial Ethernet, Stackable Layer 3 Switch

Overview

The IE560-12GSX compact distribution switch provides seamless and secure data transfer for critical infrastructure and industrial automation networks.

This hardened switch can withstand environmental conditions such as electromagnetic noise, wide temperature, humidity, vibration, and the risk of being exposed to flammable substances.

MACsec protects your critical data against sniffing exploits, spoofing, and manipulation, making secure communication possible between control centers and remote sites.

The IE560-12GSX provides network infrastructure for many vertical markets and related applications, such as:

- **Cranes & Logistics**
  Control of automated stacker cranes and other devices that boost the efficiency of dynamic warehouse environments.
- **Industrial automation and process control**
  Interconnection of machines, IoT devices, sensors, and more. Instant communications between systems and people enables improved efficiency and resilience in manufacturing environments.
- **Marine control and monitoring**
  Seamless communication for vessels, including high speed light water craft, and offshore units.
- **Oil and Gas**
  Integrated operations strategies in upstream and midstream processes that enhance remote surveillance and control capabilities.
- **Railway transportation (signalling and telecommunications)**
  Control signaling and telecommunication for improved safety, risk management, operating efficiency, and signage.
- **Railway transportation (power supply installations)**
  Substation automation and control systems which manage electric power delivery.
- **Smart grid**
  Self-sufficient systems for automatic mitigation of power outages, service disruptions, and power quality problems. Accommodating power generation options, such as distributed energy reserves, photo-voltaic, wind, and fuel cells.
- **Wastewater treatment**
  Industrial sewage treatment plants for efficient and reliable water purification. Control systems ensure process optimization by intelligent control, regulation, and monitoring.

IT/OT convergence

Improve productivity and decision-making by integrating your operational technology (OT) and information technology (IT). Use the intelligence of Industry 4.0 to collect, analysis, and manage all your data in real time.

Network automation and orchestration

Powerful automation options include Allied Telesis Autonomous Management Framework™ Plus (AMF Plus) and open standard-based northbound API.

For easy integration into complex networks consisting of physical, virtual, and multi-vendor devices, the IE560-12GSX features:

- NETCONF/RESTCONF + YANG data modelling for network automation.
- OpenFlow v1.3 for Software Defined Networking (SDN) orchestration.

Key Features

- 8 x 100/1000X SFP ports
- 4 x 1/10G SFP+ uplink ports
- EMC for power utilities (IEC 61850-3, IEEE 1613)
- AlliedWare Plus™ operating system
- Allied Telesis Autonomous Management Framework Plus™ (AMF Plus)
- NETCONF/RESTCONF with YANG data modelling
- OpenFlow v1.3 for SDN
- QoS with traffic shaping
- Efficient forwarding of multicast streams
- Routing capabilities (BGP, ECMP, OSPF, RIP, and static)
- Extensive features for cybersecurity and denial of service prevention
- MACsec encryption @256-bits, available on any port
- Active Fiber Monitoring (AFM)
- Virtual Chassis Stacking (VCStack™)
- High Availability networking (EPSRing™, ITU-T G.8032, MRP)
- Automation and control protocols (Modbus/TCP, PROFINET IO)
- Upstream Forwarding Only (UFO)
- Extended operating temp range: -40° C to 75° C (tested @85° C)
- Fanless design
- Graceful thermal shutdown
- Protection circuits
- Alarm monitoring with trigger facility
- Redundant power inputs
- Certified for hazardous location[1]

[1] Contact sales representative for availability.

KEY FEATURES

Network Automation

AMF Plus is a suite of tools that provide centralized control and network automation, as well as visual intent-based network management. It has the the intelligence to set-up, optimize, and maintain the network according to predefined goals and policies.

Powerful features like centralized management, auto backup, auto upgrade, auto provisioning and auto recovery enable plug-and-play networking and zero touch management.

Integration with our Vista Manager visual monitoring and management platform means AMF Plus also provides intent-based features like:

- Health monitoring to easily investigate, analyze, and improve overall network health.
- Smart ACLs to control and secure client resources.
- intent-based QoS to deal with network bandwidth contention.

AMF Plus is scalable and can be either deployed integrated into Allied Telesis equipment or on multi-tenant cloud architecture.

Northbound Interfaces

Open standard-based interfaces allow for easy integration with existing management systems.

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

OpenFlow is a key technology for SDN orchestration. SDN controllers and other tools support automated behavior in a network, and allow for the execution of customized applications and services.

Micro-segmentation for Network Security

Micro-segmentation enhances converged IT/OT network security by reducing the number of entry points for attackers or intruders. Isolating applications, data, and endpoints hampers the ability of intruders or malware to move within the network.

SDN network orchestration enables self-learning Artificial Intelligence to adapt and propagate security policies to mitigate evolving cyber threats.

MACsec data protection

Secure connectivity in critical infrastructure is essential. For example, power utilities can employ point-to-point tunnels protected by MACsec to ensure secure communications between control centers and remote sites.

MACsec is a Layer 2 protocol that relies on GCM-AES cipher suites encryption to offer integrity, confidentiality, and origin authentication.

This protects against data packet sniffing exploits, spoofing, and manipulation.

The advantages are:

- Secure communication beyond the link layer
- Line-rate throughput
- Microsecond latency
- Set-and-forget management
- Near-zero overhead
- Low total cost of ownership

The IE560-12GSX features MACsec encryption on any port.

High Availability

Virtual Chassis Stacking (VCStack™) is when two or more Allied Telesis switches are configured to operate as a single switch.

VCStack™ provides a highly available system where network resources are spread 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.

The IE560-12GSX features VCStack™ of up to four devices.

EPSRing™ and ITU-T G.8032 ERPS enable a protected ring capable of recovery within as little as 50ms. These features are perfect for high performance and high availability.

High-availability automation networks are supported with Media Redundancy Protocol (MRP) as defined by IEC62439-2.

MRP in ring networks allows up to 50 devices to have guaranteed and deterministic switchover behavior.

Spanning Tree protocols RSTP and MSTP, along with static LAGs and the dynamic Link Aggregation Control Protocol (LACP), support high availability in star network topologies.

Automation and Control Protocols

Automation and control protocols enable the integration of our solutions with OT-related supervisory and control systems.

PROFINET IO is a communication protocol for data exchange between I/O controllers, like SCADA and PLC, with I/O devices over Ethernet networks.

Supporting PROFINET certification,[1] the IE560-12GSX has I/O device properties that provide diagnostic data.

Communication channel support:

- Standard TCP/IP (PROFINET NRT): suitable for non-deterministic functions, such as parametrization, video/audio transmissions and data transfer to higher level IT systems.
- Real Time (PROFINET RT): TCP/IP layers are bypassed in order to have deterministic performance for automation applications.

Modbus/TCP is intended for supervision and control of automation equipment. It is a variant of the MODBUS protocol using TCP/IP for communications on Ethernet networks.

The IE560-12GSX supports read/write register access and heartbeat functionality for efficient process control of both SCADA and slave devices.

Precise Time Synchronization (IEEE 1588)

The IEEE 1588 Precise Time Protocol (PTP) is a fault tolerant method that enables clock synchronization in packet-based networks. This deterministic communication method provides precise timing for automation applications and measurement systems.

In power systems, time synchronization is required for synchrophasor measurements, protective line measurements, analog measurements, and SCADA time stamping.

Synchrophasors are instruments that measure the magnitude and phase angle of line voltage and current at multiple locations across the power grid. These measurements enable detection of instabilities so appropriate action can be taken.

SCADA systems require IED events to be logged with 1ms accuracy, which is achieved using PTP for timing distribution.

The IE560-12GSX supports PTP power profiles as a Transparent Clock, and performs an active role in Ethernet networks to reduce the effects of link delay and residence time.[2]

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 services and applications.

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 (AFM)

Active Fiber Monitoring prevents eavesdropping on fiber communications by monitoring received optical power. If the switch detects an intruder, it can automatically shut down the port or transmit an alert.

VLAN Mirroring (RSPAN)

VLAN mirroring provides for local analysis of traffic on ports in remote switches. Traffic being transmitted or received on a monitored port is duplicated and sent across the network on a special VLAN.

VLAN Translation

VLAN Translation allows traffic arriving on a VLAN to be mapped to a different VLAN on the outgoing paired interface.

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.

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.

Dynamic Host Configuration Protocol (DHCP) Snooping

The switch keeps a record of the IP addresses of the devices on its ports, including those addresses allocated by DHCP servers. IP source guard checks against this DHCP snooping database to ensure only clients with specific IP and/or MAC addresses can access the network. DHCP snooping works with other features, like dynamic ARP inspection, to increase security in Layer 2 switched environments, and also provides a traceable history which meets the growing legal requirements placed on service providers.

[1] Contact sales representative for availability.

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

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

Port Based DHCP IP Address Assignment

DHCP server port-based address allocation ensures a replacement device receives the same IP address - even though the client-identifier or client hardware address has changed.

That supports Industrial Automation and Control Systems (IACS), which are very sensitive to operation outages. When devices such as sensors and actuators fail, the must be replaced immediately.

Assigning the same IP address to the replaced device allows the OT supervisory system to take control and resume operation as quickly as possible, minimizing downtime.

Alarm Monitoring and Trigger facility

The IE560-12GSX features the alarm facility to monitor the switch's environment and respond problem as they occur.

Example of alarm events include:

- Main power supply failure
- Over-temperature
- Port link down
- Alarm Input

Triggers based on alarm changes provide a smart/friendly mechanism for automatic and timed management of your device by activating the execution of commands in response to certain events.

Alarm Input/Output

Alarm Input and Output responds to an event instantly and automatically with predefined actions. The 2-pin terminal blocks may be connected to sensors and actuator relays.

Alarm Input receives signals from external devices like motion sensors and magnets that trigger specific actions when something changes.

Alarm Output controls external devices like strobes and sirens when an event occurs.

Protection Circuits

Optimized protection circuits guard against the following abnormal conditions:

- Reverse input voltage polarity
- Over- and under-voltage
- Over-current, peak-current and short-circuit
- Over-temperature

Dual power inputs

The redundant power inputs are for higher system reliability and to allow UPS emergency power over an extended period of time.

Hazardous Locations

Hazardous locations include areas where flammable liquids, gases, vapors, or combustible dust exists in enough quantity to potentially cause an explosion or fire. Many applications, especially in the chemical, petrochemical (oil and gas), and mining industries require explosion protected equipment.

The IE560-12GSX is designed for use in hazardous locations in accordance with US National Electric Code Publication 70 (NEC 70) and the European ATEX directive.[1]

Premium Software License

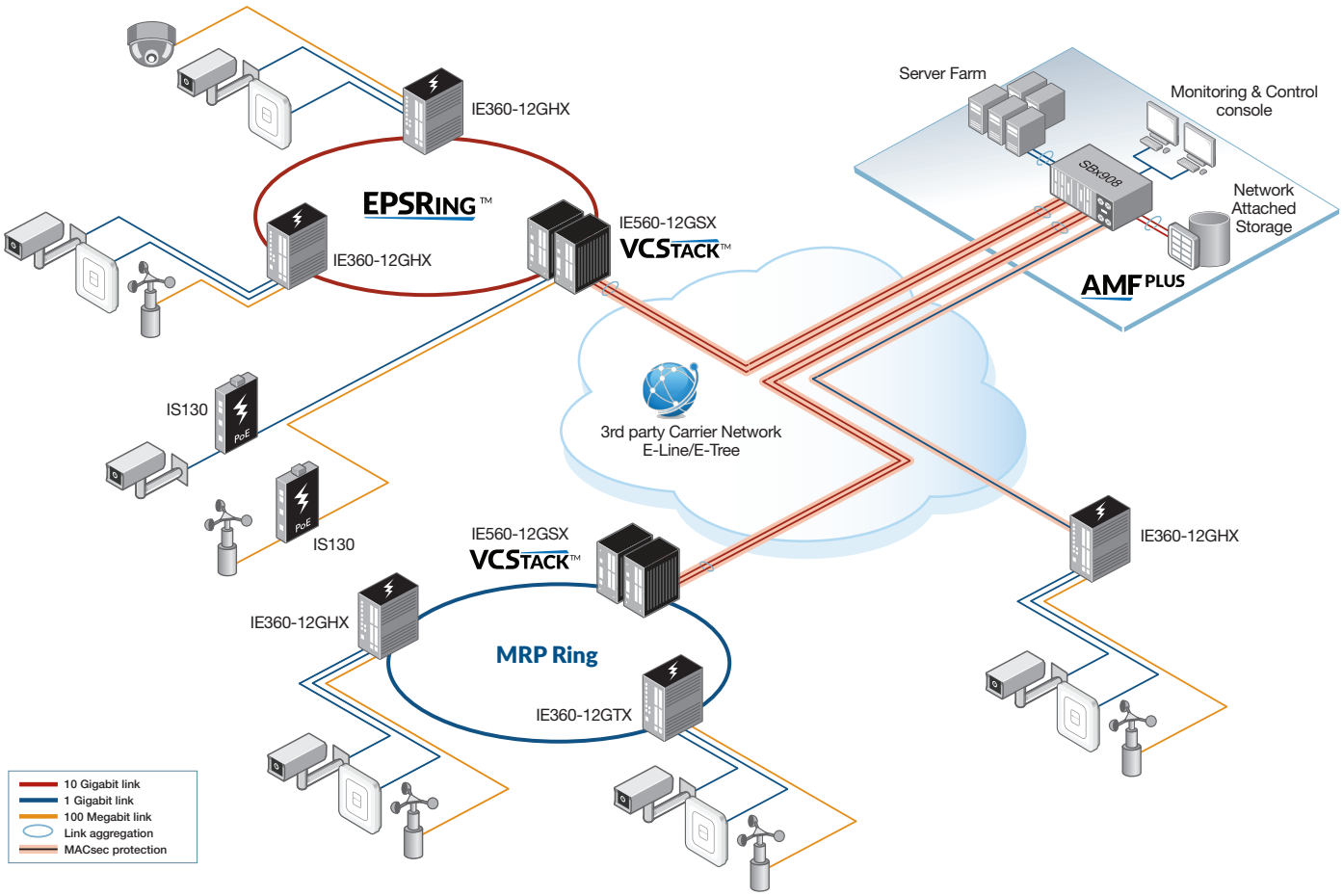
By default, the IE560-12GSX offers a comprehensive feature set that includes Layer 2 switching, static routing and IPv6 management features.

The feature set can easily be upgraded with premium software licenses.

[1] Contact sales representative for availability.

KEY SOLUTION

Industrial Network



Energy systems are a critical infrastructure of modern society that serve as the backbone for economic activity, security, and consumers' daily lives.

With the migration to smart grids, there are an increased number of potentially vulnerable entry points through which the grid can be disrupted. A critical infrastructure must therefore employ sophisticated and scalable security measures to prevent malicious attacks.

Operators of Essential Services (OES) either operate self-owned private networks, or lease services from carriers/service providers. OES have adopted MACsec (IEEE 802.1AE) to protect multiple communication flows over the same physical link. It can be used as an alternative to IPsec, as it can protect multicast, broadcast, and non-IP packets.

Key Solutions

MACsec secures communication between an operation center and remote sites with line-rate throughput, as a Layer 2 security protocol that provides point-to-point security on Ethernet links. Data remains encrypted and secure during the entire transmission between sender and receiver even if there are multiple hops in between.

The IE560-12GSX supports MACsec with the Advanced Encryption Standards CGM-AES-256, which are the most powerful symmetric encryption algorithms that use a 256-bit key to scramble data into an unreadable format.

SPECIFICATIONS

Product Specifications

	100M/1000X SFP Ports	1/10 Gigabit SFP+ Ports	Total Ports	Switching Fabric	Forwarding Rate
IE560-12GSX	8 w/ MACsec	4 w/ MACsec	12	96Gbps	71.4Mpps

Physical Specifications

	Width	Depth	Height	Weight	Enclosure	Mounting	Protection Rate
IE560-12GSX	91 mm (3.58 in)	158 mm (6.23 in)	153 mm (6.027 in)	DIN rail: 2.2 kg (4.88 lbs) Wall mount: 2.1 kg (4.64 lbs)	Aluminum/Stainless Steel Sheet Metal shell	DIN rail, wall mount	IP30

Power Characteristics

	Input Voltage	Cooling	Max Power Consumption	Max Heat Dissipation	Noise
IE560-12GSX	18~57V DC	Fanless	30W	108.2 BTU/h	Fanless

Latency (microseconds)

	Port Speed		
	100Mbps	1Gbps	10Gbps
IE560-12GSX	14.61µs	4.58µs	1.78µs

Performance

RAM memory	2GB DDR4 SDRAM
ROM memory	1GB flash
MAC address	16K entries
Packet Buffer	2 MBytes (16 Mbits)
Priority Queues	8
Simultaneous VLANs	4K
VLAN ID range	1–4094
Jumbo frames	12KB L2 jumbo frames
Multicast groups	1,023 (Layer 2 and Layer 3)

Other Interfaces

Type	Serial console (UART)
Port no.	1
Connector	RJ-45 female
Type	USB2.0 (Host Controller Class)
Port no.	1
Connector	Type A receptacle
Type	Alarm input (2mA @5.0Vdc)
Port no.	1
Connector	2-pin Terminal Block
Type	Alarm output (1A @48Vdc)
Port no.	1
Connector	2-pin Terminal Block

Flexibility and Compatibility

- SFP ports support any combination of Allied Telesis 100Mbps and 1Gbps SFP modules listed in this document under Ordering Information

Reliability

- Modular AlliedWare™ operating system
- Protection circuits against abnormal operations
- Redundant power input
- Full environmental monitoring of temperature and internal voltage levels
- Enhanced Thermal Shutdown

Industrial Automation

- IEEE 1588 PTP one-step variant
- IEEE 1588 PTP two-step variant[1]
- IEEE 1588 PTP End-to-End Transparent Clock
- IEEE 1588 PTP Peer-to-Peer Transparent Clock[1]
- IEEE 1588 PTP profile: Default
- IEEE 1588 PTP profile: Power (IEEEC C37.238)[1]
- IEEE 1588 PTP profile: Power (IEC 61850-9-3)[1]
- Modbus/TCP with master/slave heartbeats facility
- PROFINET IO non-real-time and real-time (NRT/RT)[2]

Management Features

- Allied Telesis Autonomous Management Framework™ Plus (AMF Plus) node
- NETCONF/RESTCONF northbound interface with YANG data modelling[2]
- OpenFlow northbound interface
- Web-based Graphical User Interface (GUI)
- Industry-standard CLI with context-sensitive help
- Powerful CLI scripting engine
- Built-in text editor
- Event-based triggers allow user-defined scripts to be executed upon selected system events
- Link Layer Discovery Protocol (LLDP)
- Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED)
- SNMPv1/v2c/v3 support
- Comprehensive SNMP MIB support for standard based device management
- Console management port on the front panel for ease of access
- Front panel LEDs provide at-a-glance PSU status, PoE status, and fault information
- Eco-friendly mode allows ports and LEDs to be disabled to save power
- USB interface allows software release files, configurations, and other files to be stored for backup and distribution to other devices
- Recessed Reset button

IPv4 Features

- Black hole routing
- Directed broadcast forwarding
- Equal Cost Multi Path (ECMP) routing
- Dynamic routing (OSPF, RIP, and BGP)
- Static unicast and multicast routes for IPv4
- UDP broadcast helper (IP helper)

IPv6 Features

- Device management over IPv6 networks with SNMPv6, Telnetv6 and SSHv6
- IPv4 and IPv6 dual stack
- IPv6 hardware ACLs
- Dynamic routing (OSPFv3, RIPng, and BGP+)
- Static unicast routing for IPv6
- IPv6 Ready certified

Multicasting Features

- Internet Group Management Protocol (IGMPv1/v2/v3)
- IGMP snooping with fast leave
- IGMP query solicitation
- Multicast Listener Discovery (MLDv1/v2)
- MLDv2 for IPv6
- MLD snooping
- IGMP/MLD proxy (multicast forwarding)
- Protocol Independent Multicast - Dense Mode (PIM-DM)
- Protocol Independent Multicast - Sparse Mode (PIM-SM)

[1] Contact sales representative for availability.
[2] Refer to the public GitHub for the supported YANG models.

Quality of Service

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

Resiliency Features

- Control Plane Prioritization (CPP) ensures the CPU always has sufficient bandwidth to process network control traffic
- Dynamic link failover (host attach)
- Ethernet Protection Switching Ring (EPSR™) with SuperLoop Prevention (EPSR-SLP™)
- Ethernet Ring Protection Switching (ITU-T G.8032 ERPS)
- Link Aggregation Control Protocol (LACP)
- Loop detection and thrash limiting
- Media Redundancy Protocol (MRP)
- Multiple Spanning Tree Protocol (MSTP)
- PVST+ compatibility mode
- Rapid Spanning Tree Protocol (RSTP)
- Router Redundancy Protocol (RRP) snooping
- Spanning Tree Protocol (STP) root guard
- Virtual Router Redundancy Protocol (VRRPv3)
- Virtual Chassis Stacking (VCStack™) up to 4 equipment

Security Features

- Access Control Lists (ACLs) based on layer 3 and 4 headers
- Authentication, Authorization and Accounting (AAA)
- Auth-fail and guest VLANs
- Configurable ACLs for management traffic
- BPDU protection
- DHCP snooping, IP source guard and Dynamic ARP Inspection (DAI)
- DoS attack blocking and virus throttling
- Dynamic VLAN assignment
- HTTP over TLS (HTTPS)
- MAC address filtering and MAC address lockdown
- MACsec encryption (cipher suite: CGM-AES-128, CGM-AES-256)
- Network Access and Control (NAC) features manage endpoint security
- Password protected bootloader
- Port-based learn limits (intrusion detection)
- Private VLANs and port isolation for multiple customers using the same VLAN
- RADIUS local server (100 users) and accounting
- Secure Copy (SCP)
- Strong password security and encryption
- TACACS+ authentication and accounting
- Tri-authentication: MAC-based, web-based and IEEE 802.1X

Virtual LAN Features

- Generic VLAN Registration Protocol (GVRP)
- VLAN stacking, Q-in-Q
- VLAN translation
- Upstream Forwarding Only (UFO)

Services

- Domain Name System (DNS) client and relay
- DNSv6 client and relay
- Dynamic Host Configuration Protocol (DHCP) server and relay
- DHCPv6 server and relay
- HyperText Transfer Protocol (HTTP/1.1)
- Network Time Protocol (NTP) for IPv4 and IPv6
- Simple Mail Transfer Protocol (SMTP)
- Secure Shell (SSHv2/v3)
- TELNET
- Trivial File Transfer Protocol (TFTP)

Diagnostic Tools

- Active Fiber Monitoring (AFM) detects tampering on optical links
- Automatic link flap detection and port shutdown
- Built-In Self-Test (BIST)
- Cable fault locator (TDR)
- Connectivity Fault Management (CFM), Continuity Check Protocol (CCP) for use with ITU-T G.8032 ERPS
- Event logging via Syslog over IPv4
- Find-me device locator
- Optical Digital Diagnostic Monitoring (DDM)
- Ping polling for IPv4 and IPv6
- Port mirroring
- No limit on mirrored ports
- Up to 4 mirror (analyzer) ports for received traffic
- 1 mirror (analyzer) port for transmitted traffic
- VLAN mirroring (RSPAN)
- sFlow
- TraceRoute for IPv4 and IPv6
- UniDirectional Link Detection (UDLD)

Environmental Specifications[3]

- Operating temperature range:[4]
  -40°C to 75°C (-40°F to 167°F)
  +85°C (dry heat endurance test for 20 hours)
- Storage temperature range:
  -40°C to 85°C (-40°F to 185°F)
- Operating humidity range:
  5% to 95% non-condensing
- Storage humidity range:
  5% to 95% non-condensing
- Operating altitude:
  3,000 meters maximum (9,843 ft)

Mechanical

- EN 50022, EN 60715 standardized mounting on rails

[3] Refer to the Installation Guide for the full list of environmental tests.

[4] Refer to the Installation Guide for more details on the safety approved power ratings and thermal conditions.

Compliance	IE360
Compliance Mark	ATEX,[6] CE, FCC, ICES, RCM, UKCA, UL, VCCI
Hazardous Substances Compliance	RoHS, China-RoHS, JGSSI, REACH, SCIP, TSCA, WEEE
Safety[7]	AS/NZS 62368-1 CAN/CSA C22.2 No.60950-22 CAN/CSA C22.2 No.61010-1[6] CAN/CSA C22.2 No.61010-2-201[6] CAN/CSA C22.2 No.62368-1[6] EN/IEC/UL 60950-22 EN/IEC/UL 61010-1 EN/IEC/UL 61010-2-201 EN/IEC/UL 62368-1
Electromagnetic Immunity	EN 55035 IEC 61000-6-2
Electrostatic discharge (ESD)	EN/IEC 61000-4-2, contact discharge: 6kV (level 3) air discharge: 8kV (level 3)
Radiated susceptibility (RS)	EN/IEC 61000-4-3, radiated immunity: 10V/m (level 3) 20V/m (level X)
Electrical fast transient (EFT)	EN/IEC 61000-4-4, signal port: 4kV (level X) DC power port: 4kV (level 4)
Lighting/surge immunity (Surge)	EN/IEC 61000-4-5, installation class 3 for outdoor DC power ports: line-to-earth: 2kV (level 3) line-to-line: 1kV (level 3)
Conducted immunity (CS)	EN/IEC 61000-4-6, 10V (level 3)
Power Frequency Magnetic Field	EN/IEC 61000-4-8, 100A/m cont. (level 5) 1,000A/m for 1s (level 5)
Mains frequency voltage	EN/IEC 61000-4-16, DC power ports: 30V cont. (level 4) 300V for 1s (level 4)
Damped oscillatory wave	EN/IEC 61000-4-18, signal ports: common mode: 2.5kV (level 3) differential mode: 1.0kV (level 3) DC power ports: common mode: 2.5kV (level 3) differential mode: 1.0kV (level 3)
DC voltage dips and Interruption	EN/IEC 61000-4-29, voltage dips: ΔU 30% for 0,1s ΔU 60% for 0,1s voltage interruption: ΔU 100% for 0,05s[8]
Electromagnetic Emissions	AS/NZS CISPR 32, class A CISPR 32, class A EN 55032, class A EN 50121-4 / IEC 62236-4, class A EN 50121-5 / IEC 62236-5, class A EN/IEC 61000-6-4, class A FCC 47 CFR Part 15, subpart B, class A ICES-03, class A ICES-GEN, class A IEC 61850-3 VCCI, class A
Industry	
Marine	DNV[6]
Power utility automation	IEC 61850-3 IEEE 1613
PROFINET IO	PI conformance class B (CC-B)[6] IEC 61158-1, IEC 61158-5-10, IEC 61158-6-10 (fieldbus type 10) IEC 61784-1, IEC 61784-2 (communication profile CPF 3)
Railway applications	
Fixed installation for power supply	EN 50121-5, IEC 62236-5 EN 50125-2, IEC 62498-2
Signalling and telecommunication	EN 50121-4, IEC 62236-4 EN 50125-3, IEC 62498-3
Traffic controller assemblies	NEMA TS 2[6]

[4] Refer to the Installation Guide for more details on the safety approved power ratings and thermal conditions.
[5] Requires primary and redundant power supplies.
[6] Contact sales representative for availability.

Compliance	IE360
Environmental	
Shock	IEC60068-2-27 operational: 20g, 11ms, half-sine non-operational: 65g, 11ms, half-sine IEC 50125-3 Section 4.13.2 20 m/s^2, 11ms, mean and peak IEC 60255-21-2 response: 10g, 11ms, half sine non-operational: 30g, 11ms, half sine (withstand) 10g, 16ms (bump, DIN rail mount) 20g, 16 ms (bump, wall mount)
Vibration	IEC60068-2-6 operational: 2g, @10-500Hz non-operational: 2g, @10-500Hz IEC 50125-3 Section 4.13.1 2.3 m/s^2, 5-2000 Hz IEC 60255-21-1 response: 1g, @10-150Hz endurance: 2g, @10-500Hz
Seismic	IEC 60255-21-3 2g x-axis, 1g y-axis, 1-35 Hz, single axis sine
Hazardous location	II 3G Ex ec IIC T4 Gc[6]
c-UL-us	UL listed Industrial Control Equipment; see UL File XXXXX UL listed for Class I, Division 2, Group A, B, C, D; see UL File XXXXX UL listed for Class I, Zone Hazardous Locations; see UL File XXXXX
ATEX Directive 2014/34/EU	EN 60079-0 EN 60079-7 (Increased Safety)

[6] Contact sales representative for availability.

STANDARDS & PROTOCOLS

AlliedWare Plus Operating System

Version 5.5.5-1

Authentication

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

Automation and Control

Modbus/TCP
IEC 61158 Industrial communication networks - Fieldbus specifications - PROFINET
IEC 61784 Industrial communication networks - communication profile - PROFINET
IEEE 1588-2019 Precision Clock Synchronization Protocol
IEC/IEEE 61850-9-3:2016 Precision time protocol profile for power utility automation
IEEE C37.238-2017 Precision time protocol profile for power system applications

Border Gateway Protocol (BGP)

BGP dynamic capability
BGP outbound route filtering
RFC 1772 Application of the Border Gateway Protocol (BGP) in the Internet
RFC 1997 BGP communities attribute
RFC 2439 BGP route flap damping
RFC 2545 Use of BGP-4 multiprotocol extensions for IPv6 inter-domain routing
RFC 2918 Route refresh capability for BGP-4
RFC 3882 Configuring BGP to block Denial-of-Service (DoS) attacks
RFC 4271 Border Gateway Protocol 4 (BGP-4)
RFC 4360 BGP extended communities
RFC 4456 BGP route reflection - an alternative to full mesh iBGP
RFC 4724 BGP graceful restart
RFC 4760 Multiprotocol Extensions for BGP-4
RFC 5065 Autonomous system confederations for BGP
RFC 5492 Capabilities Advertisement with BGP-4
RFC 5925 The TCP Authentication Option
RFC 6793 BGP Support for Four-Octet Autonomous System (AS) Number Space
RFC 7606 Revised Error Handling for BGP UPDATE Messages

Encryption (Management Traffic Only)

FIPS 180-1 Secure Hash standard (SHA-1)
FIPS 186 Digital signature standard (RSA)
FIPS 46-3 Data Encryption Standard (DES and 3DES)

Ethernet

IEEE 802.2 Logical Link Control (LLC)
IEEE 802.3 Ethernet
IEEE 802.3ab 1000BASE-T
IEEE 802.3ae 10 Gigabit Ethernet
IEEE 802.3an 10GBASE-T
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 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 Plus MIB and traps

Optical DDM MIB
SNMPv1, v2c and v3
ANSI/TIA-1057 Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)
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 2011 SNMPv2 MIB for IP using SMIv2
RFC 2012 SNMPv2 MIB for TCP using SMIv2
RFC 2013 SNMPv2 MIB for UDP using SMIv2
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 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 The Syslog protocol
RFC 6020 YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)
RFC 6241 Network Configuration Protocol (NETCONF)
RFC 6244 Architecture for Network Management Using NETCONF and YANG
RFC 6527 Definitions of managed objects for VRRPv3
RFC 7950 The YANG 1.1 Data Modeling Language
RFC 8040 RESTCONF Protocol

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 SSM for IPv6
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 3590 Source Address Selection for the Multicast Listener Discovery (MLD) Protocol
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 4604 Using IGMPv3 and MLDv2 for source-specific multicast
RFC 4607 Source-specific multicast for IP
RFC 7761 Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol specification

Open Shortest Path First (OSPF)

OSPF link-local signaling
OSPF MD5 authentication
OSPF restart signaling
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

IEC 62439-2 Media Redundancy Protocol (MRP)
IEEE 802.3ad Static and dynamic link aggregation
EEE 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)
ITU-T G.8032 / Y.1344 Ethernet Ring Protection Switching (ERPS)
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, Authorization (AAA)
IEEE 802.1AE MAC Security (MACsec), cipher suite GCM-AES-128, GCM-AES-256, GCM-AES-1XPN-256
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 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 3579 RADIUS support for Extensible Authentication Protocol (EAP)
RFC 3580 IEEE 802.1x RADIUS usage guidelines
RFC 3748 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 CoA (Change of Authorization)
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 The TFTP protocol (revision 2)
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 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 3396 Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)
RFC 3633 IPv6 prefix options for DHCPv6
RFC 3646 DNS configuration options for DHCPv6
RFC 3993 Subscriber-ID suboption for DHCP relay agent option
RFC 4954 SMTP Service Extension for Authentication
RFC 5905 Network Time Protocol (NTP) version 4

VLAN LAN Features

Generic VLAN Registration Protocol (GVRP)
Voice VLAN
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
AT-IE560-FL01	IE560-12GSX Premium license	■ BGP, BGP+ (256 routes) ■ OSPF (256 routes) ■ OSPFv3 (256 routes) ■ PIM-SM, DM and SSM (256 routes) ■ PIMv6-SM and SSM (256 routes) ■ RIP (256 routes) ■ RIPng (256 routes)

ORDERING INFORMATION

The DIN rail and wall mount kits are included.

AT-IE 560-12GSX-xx	8x 100/1000X SFP, 4x 1G/10G SFP+ Industrial Ethernet, Stackable Layer 3 Switch
Power Supplies	
AT-IE048-120-20	120W @48Vdc, Industrial AC/DC power supply, DIN rail mount (5 years warranty)
AT-SDR120-48	120W @48Vdc, Industrial AC/DC power supply, DIN rail mount

Where xx = 80 standard Country of Origin
980 TAA compliant Country of Origin

Accessories

Refer to the installation guide for the recommended Maximum Operating Temperature according to the selected SFP module.

AT-VT-Kit3	Management cable (USB to serial console)
10Gbps SFP+ Modules	
AT-SP10BD10/I-12	10 km, 10G BiDi SFP, LC, SMF, (1270 Tx/1330 Rx)
AT-SP10BD10/I-13	10 km, 10G BiDi SFP, LC, SMF, (1330 Tx/1270 Rx)
AT-SP10BD20-12	20 km, 10G SFP, LC, SMF, TAA[7] (1270 Tx/1330 Rx)
AT-SP10BD20-13	20 km, 10G SFP, LC, SMF, TAA[7] (1330 Tx/1270 Rx)
AT-SP10BD40/I-12	40 km, 10G SFP, LC, SMF, I-Temp, TAA[7] (1270 Tx/1330 Rx)
AT-SP10BD40/I-13	40 km, 10G SFP, LC, SMF, I-Temp, TAA[7] (1330 Tx/1270 Rx)
AT-SP10BD80/I-14	80 km, 10G SFP, LC, SMF, I-Temp, TAA[7] (1490 Tx/1550 Rx)
AT-SP10BD80/I-15	80 km, 10G SFP, LC, SMF, I-Temp, TAA[7] (1550 Tx/1490 Rx)

AT-SP10ER40a/I	40 km, 10G SFP, LC, SMF, 1550 nm, I-Temp, TAA[7]
AT-SP10LRa/I	10 km, 10G SFP, LC, SMF,1310 nm, I-Temp, TAA[7]
AT-SP10SR	300 m, 10G SFP, LC, MMF,850 nm, TAA[7]
AT-SP10SR/I-90	300 m, 10G SFP, LC, MMF,850 nm, I-Temp, TAA[7]
AT-SP10TM	20 m, 1/10G SFP, RJ-45, I-Temp, TAA[7]
AT-SP10ZR80/I	80 km, 10G SFP, LC, SMF,1550 nm, I-Temp
1000Mbps SFP Modules	
AT-SPBD10-13	10 km, 1G BiDi SFP, LC, SMF, I-Temp (1310 Tx/1490 Rx)
AT-SPBD10-14	10 km, 1G BiDi SFP, LC, SMF, I-Temp (1490 Tx/1310 Rx)
AT-SPBD20-13/I	20 km, 1G BiDi SFP, SC, SMF, I-Temp, (1310 Tx/1490 Rx)
AT-SPBD20-14/I	20 km, 1G BiDi SFP, SC, SMF, I-Temp, (1490 Tx/1310 Rx)

[7] Trade Act Agreement compliant (TAA)

1000Mbps SFP Modules	
AT-SPBD20LC/I-13	20 km, 1G BiDi SFP, LC, SMF, I-Temp, TAA[7] (1310 Tx/1490 Rx)
AT-SPBD20LC/I-14	20 km, 1G BiDi SFP, LC, SMF, I-Temp, TAA[7] (1490 Tx/1310 Rx)
AT-SPBD40-13/I	40 km, 1G BiDi SFP, LC, SMF, I-Temp, (1310 Tx/1490 Rx)
AT-SPBD40-14/I	40 km, 1G BiDi SFP, LC, SMF, I-Temp, (1490 Tx/ 1310 Rx)
AT-SPEX/E-90	2 km, 1000EX SFP, LC, MMF, 1310 nm, Ext. Temp, TAA[7]
AT-SPLX10a	10 km, 1000LX SFP, LC, SMF, 1310 nm, TAA[7]
AT-SPLX10/I	10 km, 1000LX SFP, LC, SMF, 1310 nm, I-Temp
AT-SPLX10/E-90	10 km, 1000LX SFP, LC, SMF, 1310 nm, Ext. Temp, TAA[7]
AT-SPLX40	40 km, 1000LX SFP, LC, SMF, 1310 nm
AT-SPLX40/E-90	10 km, 1000LX SFP, LC, SMF, 1310 nm, Ext. Temp, TAA[7]
AT-SPSX-90	550 m, 1000SX SFP, LC, MMF, 850 nm, TAA[7]
AT-SPSX/I-90	550 m, 1000SX SFP, LC, MMF, 850 nm, I-Temp, TAA[7]
AT-SPSX/E-90	550 m, 1000SX SFP, LC, MMF, 850 nm, Ext. Temp, TAA[7]
AT-SPTX-90	100 m, 10/100/1000T SFP, RJ-45, TAA[7]
AT-SPTX/I	100 m, 10/100/1000T SFP, RJ-45, I-Temp
AT-SPZX120/I	120 km, 1000LX SFP, LC, SMF, 1550 nm, I-Temp, TAA[7]
100Mbps SFP Modules	
AT-SPFX/2-90	2 km, 100FX SFP, LC, MMF, 1310 nm, TAA[7]
AT-SPFX30/I-90	30 km, 100FX SFP, LC, SMF, 1310 nm, I-Temp, TAA[7]
Direct Attach Cables (DAC)	
AT-SP10TW1	Twinax direct attach cable (1 meter)
AT-SP10TW3	Twinax direct attach cable (3 meters)

[7] Trade Act Agreement compliant (TAA)