

IE210L Series

Industrial-Lite Ethernet Layer 2 Switches

The Allied Telesis IE210L Series of Industrial-Lite Ethernet Gigabit Layer 2 switches are built for enduring performance at high ambient temperatures, making them ideal for indoor IoT applications and physical security.



Overview

The Allied Telesis IE210L Series are wire-speed Layer 2 switches for industrial-lite Ethernet applications. With Power over Ethernet Plus (PoE+), and support for high operating temperatures of up to 65°C, IE210L switches tolerate the harsh and demanding environments found in industrial deployments.

These high-performing, cost-effective switches provide network managers with several key features, including port-based VLANs, IEEE 802.1p, QoS, port trunking/link aggregation, port mirroring, priority queues, and IEEE 802.1x security support.

With support for up to 16K MAC addresses, the IE210L Series is the ideal option for integrating management into any network solution.

Device management is provided via an industry-standard CLI, web-based Graphical User Interface (GUI), SNMP, Telnet and SSH, as well as the Allied Telesis Autonomous Management Framework™ (AMF).

Powerful network management

AMF meets the increased management requirements of modern converged networks, automating many everyday tasks including configuration management. AMF has powerful centralized management features that manage a complete network as a single virtual device. The network can be expanded 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. AMF Guestnode allows third-party devices, such as security cameras, to be part of an AMF network.

Secure

Network security is guaranteed, with powerful control over network traffic types, secure management options,

and other multi-layered security features built right into the IE210L.

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

Allied Telesis IE210L switches use 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, while secure access is also available for guests.

Security from malicious network attacks is provided by a comprehensive range of features, such as DHCP snooping, STP root guard, BPDU protection and Access Control Lists (ACLs). 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 network loop. IE210L switches provide features to detect loops as soon as they are created. Loop detection and thrash limiting take immediate action to prevent network storms.

Network resiliency

The convergence of network services in the Enterprise has led to increasing demand for highly-available networks with minimal downtime. The IE210L Series supports highly-stable and reliable network switching with a recovery time of less than 50ms.

You can customize the IE210L with the most appropriate mechanism and protocol to prevent network connection failure. Choices include Allied Telesis Ethernet Protection Switched Ring (EPSRing™), and the standard ITU-T G.8032.

Future-proof

The IE210L switches are Software-Defined Networking (SDN) ready and are able to support OpenFlow v1.3.

Key Features

- ▶ AlliedWare Plus™ functionality
- ▶ Allied Telesis Autonomous Management Framework™ (AMF) node
- ▶ Active Fiber Monitoring (AFM)
- ▶ Ethernet Protection Switched Ring (EPSRing™) Master/Transit
- ▶ Ethernet Ring Protection Switching (ITU-T G.8032)
- ▶ Ethernet CFM (IEEE 802.1ag)
- ▶ IEEE 802.3at PoE+ sourcing (30W)
- ▶ OpenFlow for SDN
- ▶ sFlow
- ▶ TACACS+ Command Authorization
- ▶ UDLD
- ▶ VLAN / Double tagging (Q-in-Q)
- ▶ VLAN Mirroring (RSPAN)
- ▶ Built-in AC power supply unit

Key Features

Allied Telesis Autonomous Management Framework™ (AMF)

- ▶ 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.
- ▶ AMF Guest node allows Allied Telesis wireless access points and further switching products, as well as third-party devices such as IP phones and security cameras, to be part of an AMF network.

Software-Defined Networking (SDN)

- ▶ OpenFlow is a key technology that enables the use of SDN to build smart applications that unlock value and reduce cost.

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.
- ▶ As a Layer 2+ switch, a static route can be added to allow a user in a different subnet to manage the switch.

ICT Network Resiliency

- ▶ EPSRing™ and ITU-T G.8032 enable a protected ring capable of recovery within as little as 50ms; these features are perfect for high performance and high availability.
- ▶ Spanning Tree Protocol (STP), RSTP, MSTP, static Link Aggregation Group (LAG), and dynamic Link Aggregation Control Protocol (LACP) are all supported.

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.

Access Control Lists (ACLs)

- ▶ The IE210L Series features industry-standard access control functionality through ACLs. ACLs 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 is traffic flow control.
- ▶ Simplify access and traffic control across entire segments of the network. ACLs can be applied to a Virtual LAN (VLAN) as well as a specific port.

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 equipments, network policy, location discovery (for Emergency Call Services) and inventory.

VLAN Translation

- ▶ VLAN Translation allows traffic arriving on a VLAN to be mapped to a different VLAN on the outgoing paired interface.
- ▶ In Metro networks, it is common for a network Service Provider (SP) to give each customer their own unique VLAN, yet at the customer location give all customers the same VLAN-ID for tagged packets to use on the wire. SPs can use VLAN Translation to change the tagged packet's VLAN-ID at the customer location to the VLAN-ID for tagged packets to use within the SP's network.
- ▶ This feature is also useful in Enterprise environments where it can be used to merge two networks together, without manually reconfiguring the VLAN numbering scheme. This situation can occur if two companies have merged and the same VLAN-ID is used for two different purposes.

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.

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

- ▶ DHCP servers allocate IP addresses to clients, and the switch keeps a record of addresses issued on each port. IP source guard checks against this DHCP snooping database to ensure only clients with specific IP and/or MAC address can access the network. DHCP snooping can be combined 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.

Power over Ethernet Plus (PoE+)

- ▶ With PoE, a separate power connection to media endpoints such as 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) such as pan, tilt and zoom security cameras.

Security (Tri-Authentication)

- ▶ Authentication options on the IE210L Series 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, resulting in tri-authentication.

TACACS+ Command Authorization

- ▶ Provides centralized control of which commands can be issued by specific users of an AlliedWare Plus device. TACACS+ command authorization complements authentication and accounting services for a complete AAA solution.

UniDirectional Link Detection (UDLD)

- ▶ 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.

Premium Software License

- ▶ By default, the IE210L Series offers a comprehensive Layer 2 feature set. This feature set can easily be upgraded with premium software licenses.

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 IE210L switches with high-performance EPSR connectivity together in one network ring. This topology provides recovery in as little as 50 ms, if required.

Network flexibility

Flexible network deployment is facilitated by compact 10 and 18 port IE210L PoE+ models, as required in a factory network with a high temperature environment. Diagram 2 shows the IE210L series in multiple ring network topology, serving different domains.

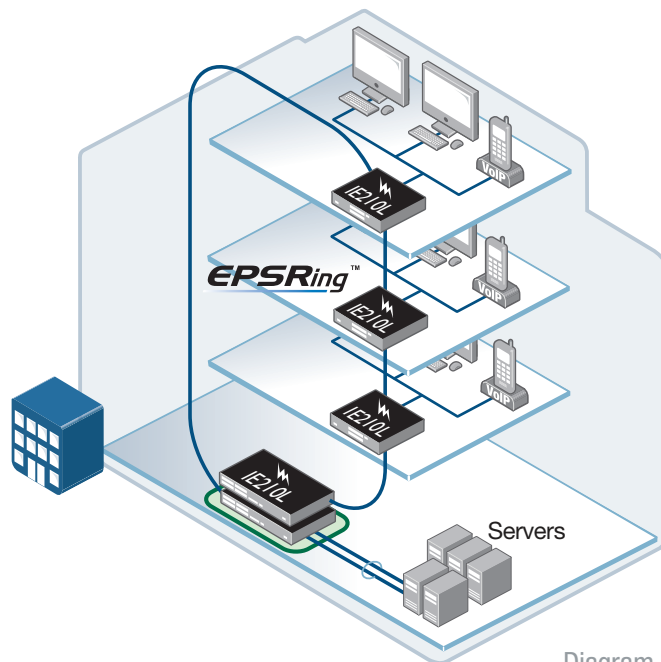


Diagram 1

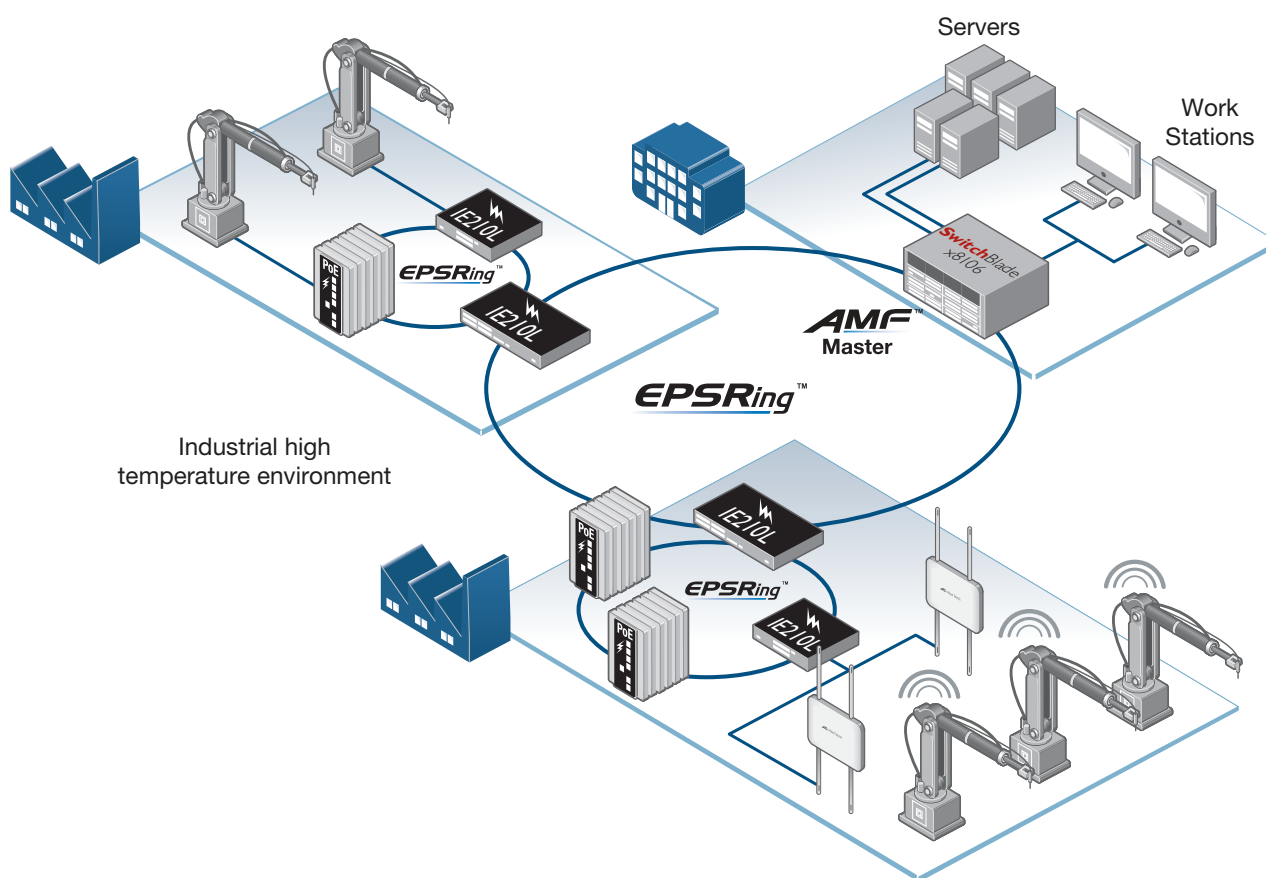


Diagram 2

Specifications

| PRODUCT | 10/100/1000T (RJ-45) COPPER PORTS | 100/1000X SFP PORTS | TOTAL PORTS | POE+ ENABLE PORTS | SWITCHING FABRIC | FORWARDING RATE |
|-------------|-----------------------------------|---------------------|-------------|-------------------|------------------|-----------------|
| IE210L-10GP | 8 | 2 | 10 | 8 | 20Gbps | 14.9Mpps |
| IE210L-18GP | 16 | 2 | 18 | 16 | 36Gbps | 26.8Mpps |

Performance

- ▶ Up to 16K MAC addresses
- ▶ Up to 512 multicast entries
- ▶ 512MB DDR3-SDRAM
- ▶ 2048 configurable VLANs
- ▶ 128MB NOR Flash memory
- ▶ Packet buffer memory: 1.5MB
- ▶ Supports 10KB jumbo frames
- ▶ Wire-speed 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

- ▶ SFP ports will support any combination of 10/100/1000T, 100X, 100FX, 100BX, 1000X, 1000SX, 1000LX, 1000ZX or 1000ZX CWDM SFPs

Diagnostic tools

- ▶ Active Fiber Monitoring detects tampering on optical links
- ▶ Automatic link flap detection and port shutdown
- ▶ Built-In Self Test (BIST)
- ▶ Connectivity Fault Management (CFM) - Continuity Check Protocol (CCP) for use with G.8032 ERPS
- ▶ Cable fault locator (TDR)
- ▶ Event logging via SYSlog over IPv4
- ▶ Find-me device locator
- ▶ Optical Digital Diagnostics Monitoring (DDM)
- ▶ Automatic link flap detection and port shutdown
- ▶ Ping polling for IPv4 and IPv6
- ▶ Port and VLAN mirroring (RSPAN)
- ▶ TraceRoute for IPv4 and IPv6
- ▶ UniDirectional Link Detection (UDLD)

IPv4 Features

- ▶ Black hole routing
- ▶ Directed broadcast forwarding
- ▶ DHCP server and relay
- ▶ DNS relay
- ▶ UDP broadcast helper (IP helper)

IPv6 Features

- ▶ DHCPv6 relay, DHCPv6 client
- ▶ Device management over IPv6 networks with SNMPv6, Telnetv6 and SSHv6
- ▶ IPv4 and IPv6 dual stack
- ▶ IPv6 hardware ACLs
- ▶ NTPv6 client and server

Management

- ▶ Allied Telesis 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 with built-in text editor
- ▶ SD/SDHC memory card socket allows software release files, configurations and other files to be stored for backup and distribution to other devices
- ▶ Configurable logs and triggers provide an audit trail of SD card insertion and removal
- ▶ Comprehensive SNMP MIB support for standards-based device management
- ▶ Management stacking allows up to 24 devices to be managed from a single console
- ▶ Event-based triggers allow user-defined scripts to be executed upon selected system events

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 Switching Ring (EPSR) with SuperLoop Prevention (EPSR-SLP)
- ▶ Ethernet Ring Protection Switching (G.8032 ERPS)
- ▶ Loop protection: loop detection and thrash limiting
- ▶ PVST+ compatibility mode
- ▶ Spanning Tree Protocol (STP) root guard

Security

- ▶ Access Control Lists (ACLs) based on layer 3 and 4 headers
- ▶ Access Control Lists (ACLs) for management traffic

- ▶ Authentication, Authorisation and Accounting (AAA)
- ▶ Auth fail and guest VLANs
- ▶ BPDU protection
- ▶ Bootloader can be password protected for device security
- ▶ 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
- ▶ 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

Software-Defined Networking

- ▶ OpenFlow v1.3 including support for connection interruption, control plane encryption and inactivity probe

Environmental Specifications

- ▶ Operating temperature range:
0°C to 65°C (32°F to 149°F)
Derated by 1°C per 305 meters (1,000 ft)
- ▶ Storage temperature range:
-30°C to 70°C (-22°F to 158°F)
- ▶ Operating relative humidity range:
5% to 95% 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: EN55032 class A, FCC class A, VCCI class A, ICES-003 class A
- ▶ Immunity: EN55024, EN61000-3-2 (harmonic), EN61000-3-3 (flicker)

Safety

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

Restrictions on Hazardous Substances (RoHS) Compliance

- ▶ EU RoHS compliant
- ▶ China RoHS compliant

Physical Specifications

| PRODUCT | WIDTH X DEPTH X HEIGHT | WEIGHT | PACKAGED DIMENSIONS | WEIGHT |
|-------------|---|-----------------|--|------------------|
| IE210L-10GP | 210 x 275 x 42.5 mm (8.27 x 10.83 x 1.67 in) | 2.1 kg (4.6 lb) | 43 x 36 x 15 cm (16.93 x 14.17 x 5.90 in) | 3.45 kg (7.6 lb) |
| IE210L-18GP | 341 x 231 x 44 mm (13.42 x 9.09 x 1.73 in) | 3.0 kg (6.6 lb) | 43 x 36 x 15 cm (16.93 x 14.17 x 5.90 in) | 4.35 kg (9.6 lb) |

Latency (microseconds)

| PRODUCT | PORT SPEED | | |
|-------------|------------|---------|-------|
| | 10MBPS | 100MBPS | 1GBPS |
| IE210L-10GP | 55µs | 7.8µs | 3.4µs |
| IE210L-18GP | 56µs | 7.9µs | 3.4µs |

Power and Noise Characteristics: 100-240V AC, 50-60Hz, 2.4A max (10GP), 4.2A max (18GP)

| PRODUCT | NO POE LOAD | | | FULL POE+ LOAD | | | MAX POE POWER | POE SOURCING PORTS | | |
|-------------|-----------------------|----------------------|----------------------------|-----------------------|----------------------|---|---------------|--------------------|-----------|------------|
| | MAX POWER CONSUMPTION | MAX HEAT DISSIPATION | NOISE | MAX POWER CONSUMPTION | MAX HEAT DISSIPATION | NOISE | | POE (7.5W) | POE (15W) | POE+ (30W) |
| IE210L-10GP | 16W | 55 BTU/h | 33 dBA (at 30C ambient) | 180W | 126 BTU/h | 60 dBA (at 50C ambient and 124W POE output) | 124W | 8 | 8 | 4 |
| IE210L-18GP | 21W | 72 BTU/h | 34 dBA (at 30C ambient) | 330W | 169 BTU/h | 60 dBA (at 50C ambient and 124W POE output) | 247W | 16 | 16 | 8 |

Noise: tested to ISO7779; front bystander position

Standards and Protocols

AlliedWare Plus Operating System

Version 5.4.9

Authentication

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

Encryption

- 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 802.3ab1000BASE-T
- IEEE 802.3af Power over Ethernet (PoE)
- IEEE 802.3at Power over Ethernet plus (PoE+)
- IEEE 802.3azEnergy 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 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 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 3596 DNS extensions to support IPv6
- RFC 3587 IPv6 global unicast address format
- 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 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 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

Multicast Support

- IGMP query solicitation
- IGMP snooping (IGMPv1, v2 and v3)
- IGMP snooping fast-leave
- MLD snooping (MLDv1 and v2)
- RFC 1112 Host extensions for IP multicasting (IGMPv1)
- RFC 2236 Internet Group Management Protocol v2 (IGMPv2)
- RFC 2715 Interoperability rules for multicast routing protocols
- RFC 3306 Unicast-prefix-based IPv6 multicast addresses
- RFC 3376 IGMPv3
- RFC 4541 IGMP and MLD snooping switches

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 802.1ag 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

Security Features

- SSH remote login
- SSLv2 and SSLv3
- TACACS+ Accounting, Authentication and Authorisation (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
- 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

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 3315 DHCPv6 client
- RFC 4330 Simple Network Time Protocol (SNTP) version 4
- 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

Voice over IP

- LLDP-MED ANSI/TIA-1057
- Voice VLAN

Feature Licenses

| NAME | DESCRIPTION | INCLUDES |
|--------------------|--|---|
| AT-FL-IE2L-L2-1 | IE210L Series Layer 2 Premium license | <ul style="list-style-type: none">▶ EPSR Master▶ VLAN translation▶ VLAN double tagging (Q-in-Q)▶ UDLD▶ PTP Transparent Mode |
| AT-FL-IE2-G8032 | IE210L Series G.8032 license | <ul style="list-style-type: none">▶ ITU-T G.8032▶ Ethernet CFM |
| AT-FL-IE2-OF13-1YR | IE210L Series OpenFlow license for 1 year | <ul style="list-style-type: none">▶ OpenFlow v1.3 |
| AT-FL-IE2-OF13-5YR | IE210L Series OpenFlow license for 5 years | <ul style="list-style-type: none">▶ OpenFlow v1.3 |



Ordering Information

AT-IE210L-10GP

8x 10/100/1000T, 2x 100/1000X SFP, Industrial Ethernet, Layer 2 Switch, PoE+ Support

AT-IE210L-18GP

16x 10/100/1000T, 2x 100/1000X SFP, Industrial Ethernet, Layer 2 Switch, PoE+ Support

AT-RKMT-J13

Rack mount kit for IE210L-18GP

AT-RKMT-J14

Rack mount kit for IE210L-10GP

Supported SFP Modules

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

1000Mbps SFP Modules

AT-SPBD10-13

10 km, 1G BiDi SFP, LC, SMF (1310Tx/1490Rx)

AT-SPBD10-14

10 km, 1G BiDi SFP, LC, SMF (1490Tx/1310Rx)

AT-SPBD20-13/I

20 km, 1G BiDi SFP, SC, SMF, I-Temp (1310Tx/1490Rx)

AT-SPBD20-14/I

20 km, 1G BiDi SFP, SC, SMF, I-Temp (1490Tx/1310Rx)

AT-SPBD20LC/I-13

20 km, 1G BiDi SFP, LC, SMF, I-Temp (1310Tx/1490Rx)

AT-SPBD20LC/I-14

20 km, 1G BiDi SFP, LC, SMF, I-Temp (1490Tx/1310Rx)

AT-SPEX

2 km, 1000EX SFP, LC, MMF, 1310 nm

AT-SPEX/E

2 km, 1000EX SFP, LC, MMF, 1310 nm, Ext. Temp

AT-SPLX10

10 km, 1000LX SFP, LC, SMF, 1310 nm

AT-SPLX10/I

10 km, 1000LX SFP, LC, SMF, 1310 nm, I-Temp

AT-SPLX10/E

10 km, 1000LX SFP, LC, SMF, 1310 nm, Ext. Temp

AT-SPLX40

40 km, 1000LX SFP, LC, SMF, 1310 nm

AT-SPLX40/E

40 km, 1000LX SFP, LC, SMF, 1310 nm, Ext. Temp

AT-SPSX

550 m, 1000SX SFP, LC, MMF, 850 nm

AT-SPSX/I

550 m, 1000SX SFP, LC, MMF, 850 nm, I-Temp

AT-SPSX/E

550 m, 1000SX SFP, LC, MMF, 850 nm, Ext. Temp

AT-SPTX

100 m, 10/100/1000T SFP, RJ-45

AT-SPTX/I

100 m, 10/100/1000T SFP, RJ-45, I-Temp

100Mbps SFP Modules

AT-SPFX/2

2 km, 100FX SFP, LC, MMF, 1310 nm

AT-SPFX/15

15 km, 100FX SFP, LC, SMF, 1310 nm

AT-SPFXBD-LC-13

15 km, 100FX BiDi SFP, LC, SMF (1310 Tx/1550 Rx)

AT-SPFXBD-LC-15

15 km, 100FX BiDi SFP, LC, SMF (1550 Rx/1310 Tx)