IE500 Series

Industrial Ethernet, Stackable Layer 3 Switch

Our ruggedized IE500 Industrial Ethernet switches are built for enduring performance in harsh environments, such as those found in manufacturing, transportation and physical security. Offering high throughput, rich functionality and advanced security features, IE500 switches deliver the performance and reliability demanded by industrial deployments in the Internet of Things (IoT) age.

Overview

The Allied Telesis IE500 Series are wirespeed Layer 3 switches for industrial Ethernet applications. With a wide operating temperature range of between -40°C and 75°C, they tolerate harsh and demanding environments, such as those found in industrial and outdoor deployment.

Device management is provided via Industry-standard CLI, SNMP, Telnet, SSH, or Allied Telesis Management Framework™ (AMF). AMF is unique to Allied Telesis managed devices, offering simplified device provisioning, recovery and firmware upgrade management.

Performance

The IE500 Series of high performance and cost-effective managed switches meets the high reliability requirements of industrial network operations. These robust switches provide network managers with several key features, using the simple web-based management function, including port-based VLANs, IEEE 802.1p, QoS, port mirroring, priority queues, and IEEE 802.1x security support. With support for up to 16K MAC addresses, the IE500 Series is the ideal option for integrating management into any network solution.

Secure

Advanced security features protect the network. Unprecedented control over user access is provided with Network Access Control (NAC), mitigating threats to network infrastructure. This ensures the network is accessed only by known users and devices — all users’ adherence to network security policies is checked, and then either access is granted or remediation is offered. Secure access can also be provided for guests. A secure network environment is guaranteed. The IE500 Series offers powerful control over network traffic types, secure management options, loop guard to protect against cabling mistakes, and tri-authentication for comprehensive access control.

High Network Resiliency

The convergence of network services in the enterprise has led to increasing demand for highly available networks with minimal downtime. VCVStack, in conjunction with link aggregation, provides a network with no single point of failure and an easy solution for resiliency in access applications.

The IE500 Series supports highly stable and reliable network switching with a recovery time of less than 50ms. You can customize the IE500 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.

The IE500 Series can form a VCVStack of up to four units for enhanced resiliency and simplified device management. Full EPSRing support and VCVStack LD (Long Distance), which enables stacks to be created over long distance fiber links, make the IE500 Series the perfect choice for distributed environments.

Future-proof

The IE500 Series ensures a future-proof network, with superior flexibility coupled with the ability to stack multiple units. All IE500 Series models feature 1/10 Gigabit uplinks ports and a comprehensive IPv6 feature set, to ensure they are ready for future network traffic demands. These models are Software Defined Networking (SDN) ready and are able to support OpenFlow v1.3.
Key Features

Allied Telesis Management Framework (TM) (AMF)
- Allied Telesis Management Framework (AMF) is a sophisticated suite of management tools that provide a simplified approach to network management. Common tasks are automated or made so simple that the everyday 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.

VCStack (Virtual Chassis Stacking)
- Create a VCStack of up to four units with 400Gbps of stacking bandwidth to each unit. Stacking links are connected in a ring so each device has dual connections to further improve resiliency. VCStack provides a highly available system where network resources are spread out across stacked units, reducing the impact if one of the units fails. Aggregating switch ports on different units across the stack provides excellent network resiliency.
- Long-distance stacking allows a VCStack to be created over longer distances, perfect for a distributed network environment.

High Availability
- EPSRing and ITU-T G.8032 allow to form a protected ring capable of recovering within as little as 50ms. These features are perfect for high performance and high availability.
- Spanning-Tree protocol compatible; RSTP, MSTP; static Link Aggregation Group (LAG) and dynamic Link Aggregation Control Protocol (LACP) support.

Industry-leading Quality of Service (QoS)
- Comprehensive low-latency wire-speed QoS provides flow-based traffic management with full classification, prioritization, traffic shaping and min/max bandwidth profiles. Enjoy boosted network performance and guaranteed delivery of business-critical Ethernet services and applications. Time-critical services such as voice and video take precedence over non-essential services such as file downloads, maintaining responsiveness of your applications.

Loop Protection
- Thrash limiting, also known as rapid MAC movement, detects and resolves network loops. It is highly user-configurable — from the rate of looping traffic to the type of action the switch should take when it detects a loop.
- With thrash limiting, the switch only detects a loop when a storm has occurred, which can potentially cause disruption to the network. To avoid this, loop detection works in conjunction with trash limiting to send special Loop Detection Frame (LDF) packets that the switch listens for. If a port receives an LDF packet, it can choose to disable the port, disable the link, or send an SNMP trap. This feature can help to detect loops before a network storm occurs, avoiding the risk and inconvenience of traffic disruption.

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

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

UniDirectional Link Detection (UDLD)
- 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 the individual transmitter or receiver for that connection fails.

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 the Network Service Provider to give each customer their own unique VLAN, yet at the customer location, give all the customers the same VLAN-ID for tagged packets to use on the wire. VLAN-ID translation can be used by the Service Provider to change the tagged packet’s VLAN-ID at the customer location to the VLAN-ID for tagged packets to use within the NSP’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.

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

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.

Security (Tri-authentication)
- Authentication options on the IE500 Series also include alternatives to IEEE 802.1x port-based authentication, such as web authentication, to enable guest access and MAC authentication for endpoints that do not have an IEEE 802.1X supplicant. All three authentication methods—IEEE 802.1X, MAC-based and Web-based—can be enabled simultaneously on the same port for tri-authentication.

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

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.

Alarm Input/Output
- Alarm Input/Output are useful for security integration solution; they respond to events instantly and automatically by a pre-defined event scheme, and notify alert message to the monitoring control center. The 2-pin terminal blocks may be connected to sensors and actuator relays. Alarm Input receives signal from external devices like motion sensor and magnets; that will trigger subsequent actions if something changes. Alarm output controls external device upon a event (i.e. sirens, strobes, PTZ camera).

Premium Software License
- By default, the IE500 Series offers a comprehensive Layer 2 and basic Layer 3 feature set that includes static routing and IPv6 management features. The feature set can easily be upgraded with premium software licenses.
IE500 Series | Industrial Ethernet, Stackable Layer 3 Switch

Specifications

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>10/100/1000T COPPER PORTS</th>
<th>1000/1000X SFP PORTS</th>
<th>1/10 GIGABIT STACKING PORTS</th>
<th>SWITCHING FABRIC</th>
<th>FORWARDING RATE (64-BYTE PACKETS)</th>
<th>STACKING BANDWIDTH</th>
<th>POE SOURCING PORTS</th>
<th>POE BUDGET</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE510-28GISX</td>
<td>-</td>
<td>24</td>
<td>4 (2 if stacked)</td>
<td>2*</td>
<td>128Gbps</td>
<td>95.2Mpps</td>
<td>40Gbps</td>
<td>-</td>
</tr>
</tbody>
</table>

* Stacking ports can be configured as additional 1G/10G Ethernet ports when unit is not stacked

Performance

- **MAC address**: 16K entries
- **Packet Buffer**: 2 MB/byte (16 Mbits)
- **Priority Queues**: 8
- **Simultaneous VLANs**: 4K
- **VLAN ID range**: 1 – 4094
- **Multicast groups**: 1K (layer 2), 256 (layer 3)
- **Routers**: 2K (IPv4), 512 (IPv6)
- **VLANs ID range**: 1 – 4094
- **Priority Queues**: 8
- **Packet Buffer**: 2 MBytes (16 Mbits)
- **Jumbo frames**: 13KB jumbo packets
- **Port no.**
  - 1
  - 2

Other Interfaces

- **Type**
  - Serial console (UART)
  - Alarm Input
  - USB2.0 (Host Controller Class)
  - Type A receptacle
  - Alarm Output
  - RJ-45 female
- **Port no.**
  - 1
  - 2
- **Connector**
  - 2-pin Terminal Block
- **Connector**
  - RJ-45 female

Reliability

- Modular AlliedWare™ operating system
- Redundant power input
- Full environmental monitoring of temperature and internal voltages: SNMP traps alert network managers in case of any failure

Expandability

- Stack up to four units in a VCStack
- Premium license option for additional features

Flexibility and Compatibility

- Gigabit SFP ports will support any combination of Allied Telesis 1000Mbps and 1000Mbps SFP modules listed in this document under Ordering Information
- 10G SFP+ ports will support any combination of Allied Telesis 10000Mbps SFP and 10GBE SFP+ modules and direct attach cables listed in this document under Ordering Information
- Stacking ports can be configured as 10G Ethernet ports
- Port speed and duplex configuration can be set manually or by auto-negotiation

Diagnostic Tools

- Active Fiber Monitoring detects tampering on optical links
- Automatic link flap detection and port shutdown
- Built-In Self Test (BIST)
- Cable fault locator (TDF)
- Event logging via Syslog over IPv4
- Find-me device locator

Quality of Service

- Eight 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

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 Switched Rings (EPSRing™) with SuperLoop Protection (SLP)
- Ethernet Ring Protection Switching (ITU-T G.8032)
- Link Aggregation Control Protocol (LACP)
- Long-Distance stacking (VCStack LD)
- Loop protection: loop detection and thrashing limit
- Multiple Spanning Tree Protocol (MSTP)
- PVST+ compatibility mode
- Rapid Spanning Tree Protocol (RSTP)
- Spanning Tree Protocol (STP) with root guard
- Stacking ports can be configured as 10G Ethernet ports
- Virtual Router Redundancy Protocol (VRRPv3)

Multicasting

- Internet Group Membership Protocol (IGMPv1/v2/v3)
- IGMP proxy
- IGMP snooping with fast leave and no timeout feature
- IGMP static groups
- Multicast Listener Discovery (MLDv1/v2)
- MLD snooping
- Protocol Independent Multicast (PIM)
- PIM Dense Mode (DM) for IPv4 and IPv6
- PIM Sparse Mode (SM) for IPv4 and IPv6
- PIM Dense Mode to Sparse Mode translation

Security Features

- Access Control Lists (ACLs) based on layer 3 and 4 headers
- Auth-fail and guest VLANs
- Configurable ACLs for management traffic
- Authentication, Authorization and Accounting (AAA)
- Bootloader can be password protected for device security
- BPDU protection
IE500 Series | Industrial Ethernet, Stackable Layer 3 Switch

- 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 lockdown
- Network Access and Control (NAC) features manage endpoint security
- Port-based link 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

Environmental Specifications
- Operating temperature range: -40°C to 75°C (-40°F to 167°F)
- 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: up to 3,000 meters (9,842 ft)

Physical Specifications

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>WIDTH</th>
<th>HEIGHT</th>
<th>DEPTH</th>
<th>WEIGHT</th>
<th>ENCLOSURE</th>
<th>MOUNTING</th>
<th>PROTECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE510-28GSX-80</td>
<td>440 mm</td>
<td>44 mm</td>
<td>300 mm</td>
<td>4.8 Kg</td>
<td>metal shell</td>
<td>rack mount</td>
<td>IP30</td>
</tr>
</tbody>
</table>

Power and Noise Characteristics

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>INPUT VOLTAGE</th>
<th>COOLING</th>
<th>MAX NO POE POWER</th>
<th>MAX NO POE HEAT DISSIPATION</th>
<th>NOISE</th>
<th>MAX FULL POWER</th>
<th>MAX FULL HEAT DISSIPATION</th>
<th>NOISE</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE510-28GSX-80</td>
<td>±48V DC, ±60V DC</td>
<td>fan</td>
<td>74W **</td>
<td>252 BTU/h **</td>
<td>45 dBA</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Latency (microseconds)

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>PORT SPEED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>100MBPS</td>
</tr>
<tr>
<td>IE510-28GSX-80</td>
<td>14.5µs</td>
</tr>
</tbody>
</table>

Standards and Protocols

AlliedWare Plus Operating System
Version 5.4.7*

*Available in Q1 2017

Authentication
RFC 1321 Digest algorithm
RFC 1514 IP authentication using keyed MD5

Encryption
FIPS 191 Secure Hash standard (SHA-1)
FIPS 196 Data Encryption Standard (DES)

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 825 Address Resolution Protocol (ARP)
RFC 894 Standard for the transmission of IP datagrams over Ethernet networks
RFC 919 Broadcast Internet datagrams
RFC 922 Booting Internet datagrams in the presence of subnets
RFC 932 Subnetwork addressing scheme
RFC 950 Internet standard subnetworking procedure
RFC 951 Bootstrap Protocol (BooP)
RFC 1027 Proxy ARP
RFC 1035 DNS client

IPv6 Features
RFC 1481 Path MTU discovery (IPv6)
RFC 2460 IPv6 specification
RFC 2464 Transmission of IPv6 packets over Ethernet networks
RFC 3056 Connection of IPv6 domains via IPv4 clouds
RFC 3448 Default address selection for IPv6
RFC 3596 DNS extensions to support IPv6
RFC 4007 IPv6 scoped address architecture

Electrical/Mechanical Approvals

Compliance Mark
CE, FCC, VCCI

Safety
EN/IEC/UL 60950-1
US CSA-C22.2 no. 60950-1

EMC
CISPR 32
EN55024
EN55032 Class A
EN61000-3-2
EN61000-3-3
EN61000-4-2 (ESD)
EN61000-4-3 (RS)
EN61000-4-4 (EFT)
EN61000-4-5 (Surge)
EN61000-4-6 (ES)
EN61000-4-8
EN61000-4-11
FCC Part 15B, Class A
ICES-003, Class A
VCCI, Class A

Environmental Compliance
RoHS
China RoHS
WEEE

Noise: tested to ISO7779; front bystander position
Management

AMF MB and SNMP traps
AT Enterprise MB
Optical DDM MB
SMTPv1, v2, 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 1213 MB for network management of TCP/IP-based Internets: MB-2
RFC 1215 Convention for defining traps for use with the SNMP
RFC 1227 SNMP MIB protocol and MB
RFC 1239 Standard MB
RFC 1274 RIPv2 MB extension
RFC 2001 IPv6 MB for IPv6 using SMIPv2
RFC 2012 IPv6 MB for TCP using SMIPv2
RFC 2013 SMIPv2 MB for UDP using SMIPv2
RFC 2096 IP forwarding table MB
RFC 2578 Structure of Management Information v2 (SMIPv2)
RFC 2579 Textual conventions for SMIPv2
RFC 2674 Definitions of managed objects for bridges with traffic classes, multicast filtering and VLAN extensions
RFC 2741 Agent extensibility (AgentX) protocol
RFC 2787 Definitions of managed objects for VRRP
RFC 2819 RMIPv MB (groups 1, 2, 3, and 9)
RFC 2863 Interfaces MB group
RFC 3164 Syslog protocol
RFC 3176 MPLS signaling protocol
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 MB for SNMP
RFC 3621 Power over Ethernet (PoE) MB
RFC 3835 Definitions of managed objects for the Ethernet-like interface types
RFC 3636 IEEE 802.3 MII MB
RFC 4188 Definitions of managed objects for bridges
RFC 4318 Definitions of managed objects for bridges with RSTP
RFC 4560 Definitions of managed objects for remote ping, traceroute, and lookup operations
RFC 6527 Definitions of managed objects for VRFv3

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 (IGMPv3/MLD proxy)
MLD snooping (MLDv1 and v2)
PIM-SM and SSM for IPv6
RFC 1112 Host extensions for IP multicast (IGMPv1)
RFC 2236 Internet Group Management Protocol v2 (IGMPv2)
RFC 2710 Multicast Listener Discovery (MLD) for IPv6
RFC 2715 Interoperability rules for multicast routing protocols
RFC 3306 Unicast prefix-based IPv6 multicast addresses
RFC 3376 IGMPv3
RFC 3810 Multicast Listener Discovery v2 (MLDV2) for IPv6
RFC 3956 Embedding the Rendezvous Point (RP) address in an IPv6 multicast address
RFC 3973 PIM Dense Mode (DMI)
RFC 4541 IGMP and MLD snooping switches
RFC 4604 Using IGMPv3 and MLDv2 for source-specific multicast
RFC 4607 Source-specific multicast for IPv6

Open Shortest Path First (OSPF)

OSPF link-local signaling
OSPF MD5 authentication
OSPF rest signaling
Out-of-band L2DB 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 3191 OSPF Not So Stubby Area (NSSA) option
RFC 3509 Alternative implementations of OSPF area border routers
RFC 3623 Graceful OSPF restart
RFC 3632 Traffic engineering extensions to OSPF
RFC 4552 Authentication/forwarding for OSPFv3
RFC 5329 Traffic engineering extensions to OSPFv3

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)

Resilience Features

IEEE 802.1aq CDP Connectivity Fault Management - Continuity Check Protocol (CCP)
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 Ethernet ring protection switching
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 MDS authentication
RFC 2453 RIPv2

Security Features

SSH remote login
SSLv2 and SSLv3
TCACCS+ accounting and authentication
IEEE 802.1X authentication protocols (TLS, TTLS, PEAP, MD5)
IEEE 802.1X multi-supplicant authentication
IEEE 802.1X port-based network access control
RFC 2918 HTTP over TLS (“HTTPS”)
RFC 2965 RADIUS
RFC 2966 RADIUS accounting
RFC 2968 RADIUS attributes for tunnel protocol support
RFC 3280 Internet X.509 Certificate and Certificate Revocation List (CRL) profile
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 PEP Extensible Authentication Protocol (EAP)
RFC 4251 Secure Hash (SHA) protocol architecture
RFC 4252 Secure Hash (SHA) authentication protocol
RFC 4253 Secure Hash (SHA) transport layer protocol
RFC 4254 Secure Hash (SHA) connection protocol
RFC 5248 TLS v1.2

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 Tripl File Transfer Protocol (TFTP)
RFC 1985 SMTP service extension
RFC 2049 MIME
RFC 2131 DHCPv4 (server, relay and client)
RFC 2132 DHCP options and BootPv4 vendor extensions
RFC 2554 SMTP service extension for authentication
RFC 2616 HyperText Transfer Protocol - HTTP/1.1
RFC 2621 Simple Mail Transfer Protocol (SMTP)
RFC 2622 Internet message format
RFC 3046 DHCP relay agent information option (DHCP option 82)
RFC 3315 DHCPv6 (server, relay and client)
RFC 3633 IPv6 prefix options for DHCPv6
RFC 3646 DNS configuration options for DHCPv6
RFC 3993 Subscriber-ID option for DHCPv6 relay agent option
RFC 4330 Simple Network Time Protocol (SNTP) version 4
RFC 5806 Network Time Protocol (NTP) version 4

VLAN Support

RFC 1583 Provider bridges (VLAN stacking, Q-in-Q)
RFC 1610 Virtual LAN (VLAN) bridges
IEEE 802.1v VLAN classification by port and port
IEEE 802.3ac VLAN tagging

Voice over IP (VoIP)

RFC 2216 LLDP-MED - ANSI/TIA-1057
Voice VLAN
### Feature Licenses

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>INCLUDES</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT-FL-IE5-L2-01</td>
<td>IE500 series Layer-2 Premium license</td>
<td>EPSR Master, VLAN Translation, VLAN double tagging (QinQ), UDLD</td>
</tr>
<tr>
<td>AT-FL-IE5-L3-01</td>
<td>IE500 series Layer-3 Premium license</td>
<td>OSPF, OSPFv3, PIM-SM, DM and SSM, PIMv6-SM and SSM, RIPv2, RIPng, VRRP</td>
</tr>
<tr>
<td>AT-FL-IE5-G8032</td>
<td>IE500 series license for ITU-T G.8032</td>
<td>ITU-T G.8032, Ethernet CFM</td>
</tr>
</tbody>
</table>

### Ordering Information

**AT-IE510-28GSX-80**
24x 100/1000X SFP, 4x 1/10G SFP+, Industrial Ethernet, Stackable Layer 3 Switch

**Supported SFP Modules**

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

**10Gbps SFP+ modules**
- **AT-SP10TW1** 1 meter SFP+ direct attach cable
- **AT-SP10TW3** 3 meter SFP+ direct attach cable
- **AT-SP10TW7** 7 meter SFP+ direct attach cable
- **AT-SP10ER40/I** 10Gbps ER SFP+, 40 km
- **AT-SP10LR** 10Gbps LR SFP+, 10 km
- **AT-SP10LR/I** 10 Gigabit Small Form-Factor, 20 km
- **AT-SP10LR20/I** 10 Gigabit Small Form-Factor, 20 km
- **AT-SP10LRM** 10Gbps LRM SFP+, 550 m
- **AT-SP10SR** 10Gbps SR SFP+, 300 m
- **AT-SP10SR/I** 10Gbps SR SFP+, 300 m
- **AT-SP102R80/I** 10Gbps ZR SFP+, 80 km

**1Gbps SFP modules**
- **AT-SPBD10-13** 1000LX single-mode BiDi SFP, 10 km
- **AT-SPBD10-14** 1000LX single-mode BiDi SFP, 10 km
- **AT-SPBD20-13/I** Small Form Pluggable, 20 km industrial temperature
- **AT-SPBD20-14/I** Small Form Pluggable, 20 km industrial temperature
- **AT-SPEX** 1000X (LC) SFP, 2 km
- **AT-SPLX10** 1000LX (LC) SFP, 10 km
- **AT-SPLX10/I** 1000LX (LC) SFP, 10km, industrial temperature
- **AT-SPLX40** 1000LX (LC) SFP, 40 km

**100Mbps SFP modules**
- **AT-SPFX/2** 100FX (LC) SFP, 2 km
- **AT-SPFX/15** 100FX (LC) SFP, 15 km

**100Mbps SFP modules**
- **AT-SPFXB-D-LC-13** 100FX (LC) single-mode BiDi SFP, 15 km
- **AT-SPFXB-D-LC-15** 100FX (LC) single-mode BiDi SFP, 15 km

**1Gbps SFP modules**
- **AT-SPSX** 1000SX (LC) SFP, 550 m
- **AT-SPSX/I** 1000SX (LC) SFP, 550 m, industrial temperature
- **AT-SPTX** 1000T SFP, 100 m
- **AT-SPZX80** 1000ZX (LC) SFP, 80 km