x230-GP Series

ENTERPRISE POE+ GIGABIT EDGE SWITCHES

The Allied Telesis x230-GP Series of Layer 2+ Gigabit switches offer an impressive set of features in a compact design. Power over Ethernet Plus (PoE+) capability makes them ideal for powering access and security devices at the network edge.

PoE plus™ AlliedWare Plus™ OPERATING SYSTEM

Allied Telesis x230-GP Series switches provide optimal performance for connecting and remotely powering wireless access points, IP video surveillance cameras, and IP phones. The x230-10GP and x230-18GP provide 8 or 16 PoE+-capable Gigabit ports, and 2 SFP uplinks, for secure powered connectivity at the network edge.

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 x230-GP Series switches.

Network Access Control (NAC) gives unprecedented control over user access to the network, in order to mitigate threats to network infrastructure. Allied Telesis x230-GP 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. 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. Each of these can be configured to perform a variety of actions upon detection of a suspected attack.

EPSRing™

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. Allied Telesis x230-GP Series switches provide features to detect loops as soon as they are created. Loop detection and thrash limiting take immediate action to prevent network storms.

Manageable

The x230-GP runs the advanced AlliedWare Plus™ fully featured operating system, delivering a rich feature set and an industry-standard Command Line Interface (CLI). This reduces training requirements and is consistent across all AlliedWare Plus devices, simplifying network management.

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

AMF™

Powerful Network Management

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

ECO Friendly

The x230-GP Series supports Energy Efficient Ethernet, which automatically reduces the power consumed by the switch whenever there is no traffic on a port. This sophisticated feature can significantly reduce your operating costs by reducing the power requirements of the switch and any associated cooling equipment.

eco friendly

Features

- Comprehensive security features
- Easy management with Allied Telesis Management Framework (AMF)
- IEEE 803.3at PoE+ compliant (up to 30W per port)

Key Features

Power over Ethernet Plus (PoE+)

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

Allied Telesis Management Framework (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 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.

Ethernet Protection Switched Ring (EPSRing ™)

- EPSRing allows several x230-GP switches to join a protected ring capable of recovery within as little as 50ms. This feature is perfect for high availability in enterprise networks.

Access Control Lists (ACLs)

- The x230-GP 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 would be to provide traffic flow control.

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.

Storm protection

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

- Bandwidth limiting minimizes the effects of the storm by reducing the amount of flooding traffic.
- Policy-based storm protection is more powerful than bandwidth limiting. It restricts storm damage to within the storming VLAN, and it provides the flexibility to define the traffic rate that creates a broadcast storm. The action the device should take when it detects a storm can be configured, such as disabling the port from the VLAN or shutting the port down.
- Packet storm protection allows limits to be set on the broadcast reception rate, multicast frames and destination lookup failures. In addition, separate limits can be set to specify when the device will discard each of the different packet types.

Loop protection

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

Spanning Tree Protocol (STP) Root Guard

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

Bridge Protocol Data Unit (BPDU) protection

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

Tri-authentication

- Authentication options on the x230-GP 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.

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 this against the DHCP snooping database to ensure only clients with specific IP and/or MAC addresses can access the network. Combining DHCP snooping with other features, like dynamic ARP inspection, increases security in Layer 2 switched environments. This also provides a traceable history, which meets the growing legal requirements placed on service providers.

Strong passwords

- Enforcing strong passwords for key networking equipment users allows network administrators to increase security, and ensure a robust and reliable infrastructure.

Link aggregation

- Link aggregation allows a number of individual switch ports to be combined, forming a single logical connection of higher bandwidth. This provides a higher performance link, and also provides redundancy for a more reliable and robust network.

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, simplifying Quality of Service (QoS) configuration.

Find Me

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

IPv6 support

- With the depletion of IPv4 address space, IPv6 is rapidly becoming a mandatory requirement for many government and enterprise customers. To meet this need, now and into the future, the x230-GP Series supports IPv6 forwarding in hardware and features MLD snooping for efficient use of network bandwidth.

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 x230-GP switches with high performance EPSR connectivity to the x610 VCStack core. This topology provides recovery in as little as 50ms, if required. PoE powers IP phones without the need for separate power feeds.

Network flexibility

Flexible network deployment is facilitated by the compact 10 and 18 port x230-GP switches, as shown in the Campus network in diagram 2. With the growth of wireless networking and digital security, the x230-GP Series are ideal supplying connectivity and power at the network edge, supporting the full 30 watts of PoE+. AMF provides an easy yet powerful solution for managing multiple devices with plug-and-play simplicity.

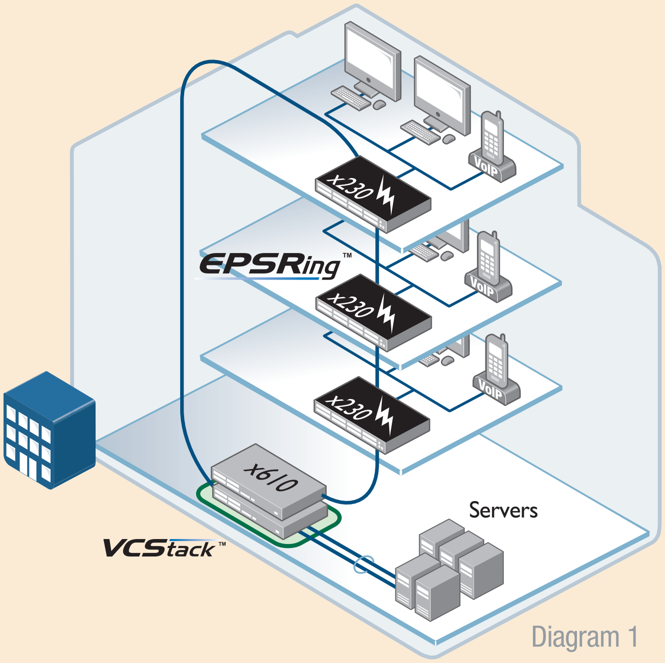

Diagram 1

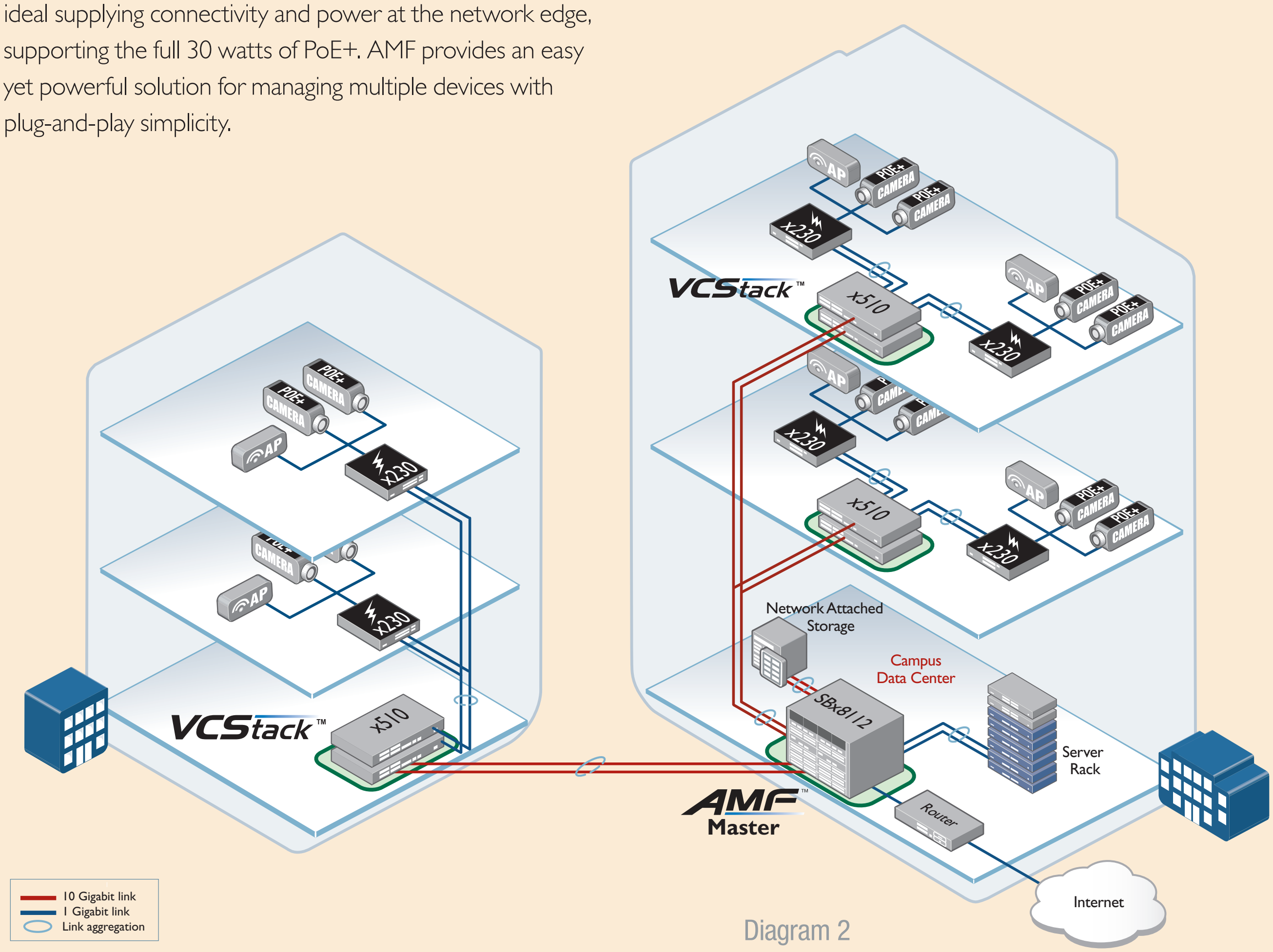

Diagram 2

Product Specifications

PRODUCT	10/100/1000T (RJ-45) COPPER PORTS	100/1000X SFP PORTS	TOTAL PORTS	SWITCHING FABRIC	FORWARDING RATE
AT-x230-10GP	8	2	10	20 Gbps	14.9 Mpps
AT-x230-18GP	16	2	18	36 Gbps	26.8 Mpps

Physical specifications

PRODUCT	HEIGHT	WIDTH	DEPTH	WEIGHT	
				UNPACKAGED	PACKAGED
AT-x230-10GP	42.5 mm (1.67 in)	210 mm (8.27 in)	275 mm (10.83 in)	2.1 kg (4.6 lb)	3.3 kg (7.3 lb)
AT-x230-18GP	44 mm (1.73 in)	341 mm (13.42 in)	231 mm (9.09 in)	3.0 kg (6.6 lb)	4.2 kg (9.3 lb)

Performance

- Up to 16K MAC addresses
- 256MB DDR SDRAM
- 64MB flash memory
- Packet Buffer memory: 1.5MB
- Supports 10KB jumbo frames
- Wirespeed forwarding

Reliability

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

Flexibility and compatibility

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

Diagnostic tools

- Built-In Self Test (BIST)
- Find-me device locator
- Cable fault locator (TDR)
- Automatic link flap detection and port shutdown
- Ping polling for IPv4 and IPv6
- Port mirroring
- TraceRoute for IPv4 and IPv6

IPv6 features

- DHCPv6 client
- Device management over IPv6 networks with SNMPv6, Telnetv6, SSHv6 and Syslogv6
- 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
- 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
- Built-in text editor
- 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)
- EPSRing (Ethernet Protection Switched Rings) with enhanced recovery for extra resiliency
- Loop protection: loop detection and thrash limiting
- PVST+ compatibility mode
- RRP snooping
- STP root guard

Security

- Access Control Lists (ACLs) based on layer 3 and 4 headers
- Configurable auth-fail and guest VLANs
- Authentication, Authorization and Accounting (AAA)
- Bootloader can be password protected for device security
- BPDU protection
- DHCP snooping, IP source guard and Dynamic ARP Inspection (DAI)
- Dynamic VLAN assignment
- Network Access and Control (NAC) features manage endpoint security
- Port-based learn limits (intrusion detection)
- Private VLANs provide security and port isolation for multiple customers using the same VLAN
- Secure Copy (SCP)
- Strong password security and encryption
- Tri-authentication: MAC-based, web-based and IEEE 802.1x

Environmental specifications

- Operating temperature range:

  x230-10GP: 0°C to 50°C (32°F to 122°F)

  x230-18GP: 0°C to 50°C (32°F to 122°F)

  Derated by 1°C per 305 meters (1,000 ft)
- Storage temperature range:

  -25°C to 70°C (-13°F to 158°F)

  Operating relative humidity range:

  5% to 90% non-condensing
- Storage relative humidity range:

  5% to 95% non-condensing
- Operating altitude:

  3,048 meters maximum (10,000 ft)

Electrical approvals and compliances

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

Safety

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

Restrictions on Hazardous Substances (RoHS) Compliance

- EU RoHS compliant
- China RoHS compliant

Country of origin

- China

Power characteristics

100-240 VAC, 50-60Hz, 2.4A maximum

PRODUCT	NO POE LOAD			FULL POE+ LOAD			MAX POE POWER	MAX POE PORTS AT 15W PER PORT	MAX POE+ PORTS AT 30W PER PORT
	MAX POWER CONSUMPTION	MAX HEAT DISSIPATION	NOISE	MAX POWER CONSUMPTION	MAX HEAT DISSIPATION	NOISE			
AT-x230-10GP	16W	55 BTU/hr	33 dBA	161W	126 BTU/hr	41 dBA	120W	8	4
AT-x230-18GP	21W	72 BTU/hr	34 dBA	296W	169 BTU/hr	42 dBA	240W	16	8

Standards and Protocols

AlliedWare Plus Operating System

Version 5.4.5

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 802.1AX Link aggregation (static and LACP)
IEEE 802.2 Logical Link Control (LLC)
IEEE 802.3 Ethernet
IEEE 802.3ab 1000BASE-T
IEEE 802.3ad Static and dynamic link aggregation
IEEE 802.3af Power over Ethernet (PoE)
IEEE 802.3at Power over Ethernet plus (PoE+)
IEEE 802.3az Energy Efficient Ethernet (EEE)
IEEE 802.3u 100BASE-X
IEEE 802.3x Flow control - full-duplex operation
IEEE 802.3z 1000BASE-X

IPv4 standards

RFC 791 Internet Protocol (IP)
RFC 792 Internet Control Message Protocol (ICMP)
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 1256 ICMP router discovery messages
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

IPv6 standards

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 3596 DNS extensions to support IPv6
RFC 4007 IPv6 scoped address architecture
RFC 4193 Unique local IPv6 unicast addresses
RFC 4291 IPv6 addressing architecture
RFC 4443 Internet Control Message Protocol (ICMPv6)
RFC 4861 Neighbor discovery for IPv6
RFC 4862 IPv6 Stateless Address Auto-Configuration (SLAAC)
RFC 5014 IPv6 socket API for source address selection
RFC 5095 Deprecation of type 0 routing headers in IPv6

Management

AMF MIB and SNMP traps
AT Enterprise MIB
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 2011 SNMPv2 MIB for IP using SMIv2
RFC 2012 SNMPv2 MIB for TCP using SMIv2
RFC 2013 SNMPv2 MIB for UDP using SMIv2
RFC 2096 IP forwarding table 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 3164 Syslog protocol
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 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

Multicast support

IGMP query solicitation
IGMP snooping (IGMPv1, v2 and v3)
IGMP snooping fast-leave
MLD snooping (MLDv1 and v2)

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

IEEE 802.1D MAC bridges
IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)

Security

SSH remote login
SSLv2 and SSLv3
TACACS+ accounting and authentication
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 2246 TLS protocol v1.0
RFC 2818 HTTP over TLS ("HTTPS")
RFC 2865 RADIUS
RFC 2866 RADIUS accounting
RFC 2868 RADIUS attributes for tunnel protocol support
RFC 3280 Internet X.509 PKI 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 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

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 802.1Q 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

Ordering Information

AT-x230-10GP
L2+ switch with 8 x 10/100/1000T PoE ports and 2 x 100/1000X SFP ports

AT-RKMT-J14
Rack mount kit for x230-10GP

AT-x230-18GP
L2+ switch with 16 x 10/100/1000T PoE ports and 2 x 100/1000X SFP ports

AT-RKMT-J13
Rack mount kit for x230-18GP

SFP modules

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

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

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

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

AT-SPTX
1000T 100 m copper

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

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

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

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

AT-SPLX10/I
1000LX GbE single-mode 1310 nm fiber up to 10 km industrial temperature

AT-SPBD10-13
1000LX GbE Bi-Di (1310 nm Tx, 1490 nm Rx) fiber up to 10 km

AT-SPBD10-14
1000LX GbE Bi-Di (1490 nm Tx, 1310 nm Rx) fiber up to 10 km

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

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

Allied Telesis

the **solution :** the **network**

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

alliedtelesis.com