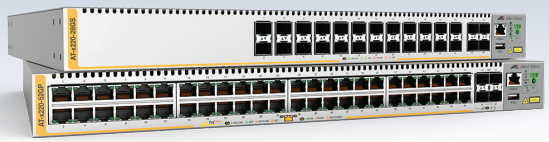
x220 Series

Gigabit Edge Switches



The Allied Telesis x220 Series are fully-managed high-performing Gigabit Layer 3 switches. Integrated security features, plus 28 SFP or 48 Gigabit copper ports, make them the ideal choice for long-distance fiber or high-density copper connectivity at the edge of the network.

Overview

The x220-28GS features 24 x 100/1000X SFP slots and 4 x 100/1000X SFP uplinks to provided extended reach at the network edge in distributed environments. Secure data transfer is ensured with Allied Telesis Active Fiber Monitoring (AFM) preventing data eavesdropping on all short and long-distance fiber links.

The x220-52GP/GT have 48 x 10/100/1000T RJ-45 copper ports and 4x 100/1000X SFP uplinks. The Power over Ethernet Plus (PoE+) model (52GP) is an ideal solution for connecting and remotely powering wireless access points, IP video surveillance cameras and IP phones.

A comprehensive feature-set provides an excellent access solution for today's networks, with high performance gigabit throughput.

Resilient

Allied Telesis Ethernet Protection Switched Ring (EPSRing™) enables distributed network segments to have resilient high-speed access to online resources and applications, and provides continuous traffic flow even during unscheduled outages.

Powerful network management

Meeting the increased management requirements of modern converged networks, Allied Telesis Autonomous Management Framework™ (AMF) automates many everyday tasks including configuration management. The entire 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.

AMF secure mode increases network security with management traffic encryption, authorization and monitoring.

Secure

Network security is guaranteed, with powerful control over all traffic types, secure management options, and other multi-layered security features built right into the x220 Series.

Network Access Control (NAC) gives unprecedented control over user access to the network, successfully mitigating threats to network infrastructure.

The x220 Series 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.

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. The x220 Series provides features to detect loops as soon as they are created. Loop detection and thrash limiting take immediate action to prevent network storms.

Key Features

- Allied Telesis Autonomous Management Framework™ (AMF)
- Active Fiber Monitoring
- AlliedWare Plus operating system
- EPSR™ and G.8032 high-speed ring connectivity
- Management stacking
- Static routing and RIP
- DHCP snooping
- IEEE 802.1x/MAC/Web authentication support
- PoE+ supplies up to 30W per port
- PoE power budget of 740 Watts
- Continuous PoE

Effortless management

The x220 Series 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.

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

Active Fiber Monitoring (AFM)

- AFM 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.

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 pan, tilt and zoom security cameras.

Continuous PoE

- Continuous PoE allows the switch to be restarted without affecting the supply of power to connected devices. Smart lighting, security cameras, and other PoE devices will continue to operate during a software upgrade on the switch.

Ethernet Protection Switched Ring (EPSRing™)

- EPSRing allows several x220 switches to form a protected ring capable of recovery within as little as 50ms. This feature is perfect for high availability in enterprise networks.

G.8032 Ethernet Ring Protection

- G.8032 provides standards-based high-speed ring protection, that can be deployed standalone, or interoperate with Allied Telesis EPSR.
- Ethernet Connectivity Fault Monitoring (CFM) proactively monitors links and VLANs, and provides alerts when a fault is detected.

Access Control Lists (ACLs)

- The x220 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.

VLAN ACLs

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

Easy To Manage

- The AlliedWare Plus operating system incorporates an industry standard CLI, facilitating intuitive manageability.
- With three distinct modes, the CLI is very secure, and the use of SSHv2 encrypted and strongly authenticated remote login sessions ensures CLI access is not compromised.

Storm protection

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

- Bandwidth limiting minimizes the effects of the storm by reducing the amount of flooding traffic.
- Policy-based storm protection is more powerful than bandwidth limiting. It restricts storm damage to within the storming VLAN, 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 x220 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

- Centralize control of which commands may be issued by a specific user of an AlliedWare Plus device. TACACS+ command authorization complements authentication and accounting services for a complete AAA solution.

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.

VLAN Mirroring (RSPAN)

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

Find Me

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

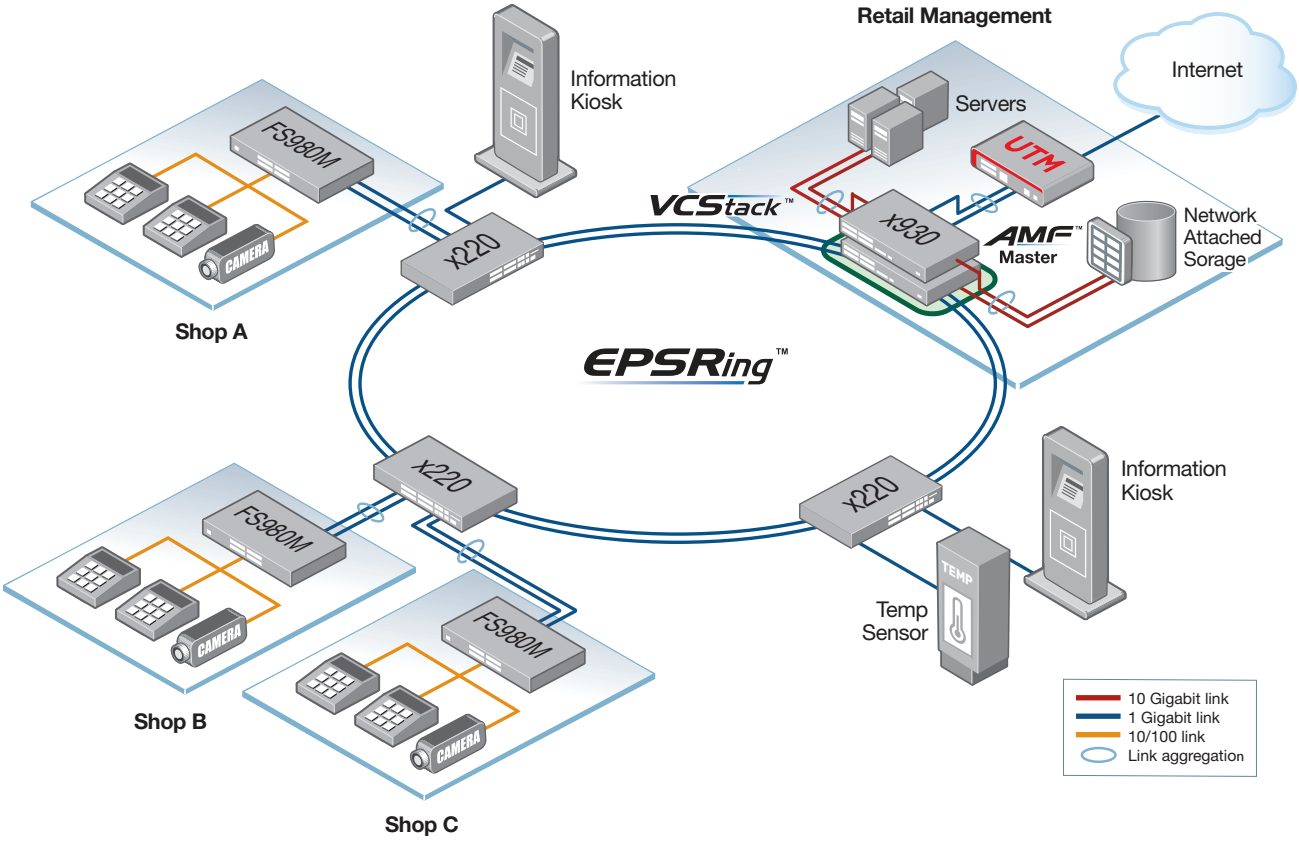
IPv6 Support

- 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 x220 Series supports IPv6 forwarding in hardware and features MLD snooping for efficient use of network bandwidth.

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.

Key Solutions



Distributed retail network

The growth of large retail shopping complexes, and open-air malls (as shown in the diagram above) have increased the need for high performing networks. The convergence of data from visitor information kiosks, monitoring sensors, security management, and point of sale systems requires a resilient solution.

The x220 Series supports Allied Telesis Ethernet Protection Switched Ring (EPSRing) to ensure distributed network segments have high-speed access to online systems. Continuous traffic flow is enabled with failover in a little as 50ms in the case of an unscheduled device outage or link failure.

With 28 SFP ports, the x220-28GS extends network reach to enable access connectivity right around the retail precinct, or similarly an education campus, manufacturing plant, or large distributed business. All fiber links are kept secure with Active Fiber Monitoring, which detects attempted data eavesdropping and protects against intrusion.

To simplify and automate network management, Allied Telesis Autonomous Management Framework automatically backs-up the entire network, and provides plug-and-play network growth and zero-touch unit replacement.

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 x220 switches with high performance EPSR connectivity to the SwitchBlade x8106 core chassis. This topology provides recovery in as little as 50ms, if required.

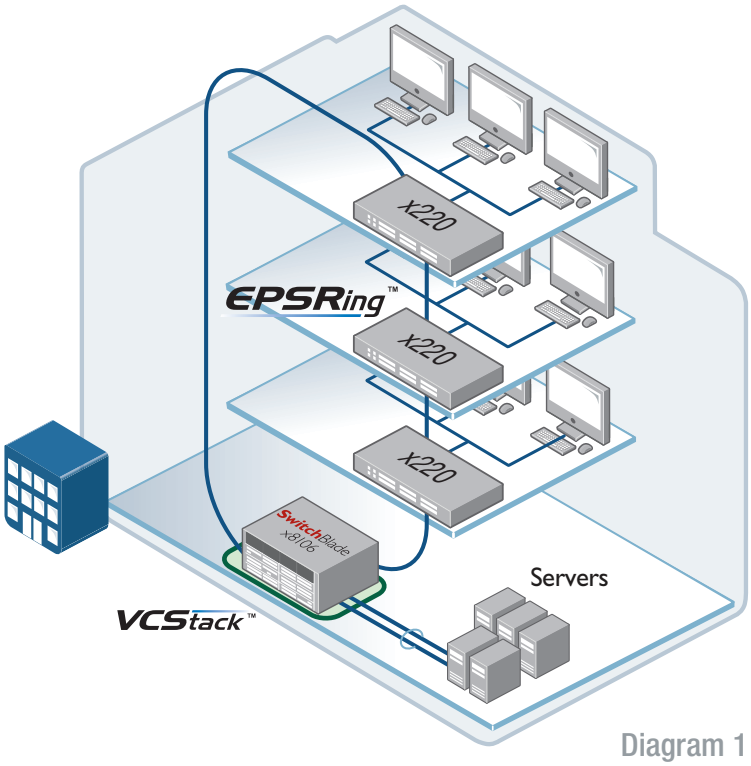


Diagram 1

Network flexibility

Flexible network deployment is facilitated by the x220 PoE+ models, as shown in the Campus network in diagram 2. With the growth of wireless networking and digital security, the x220 PoE+ models 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.

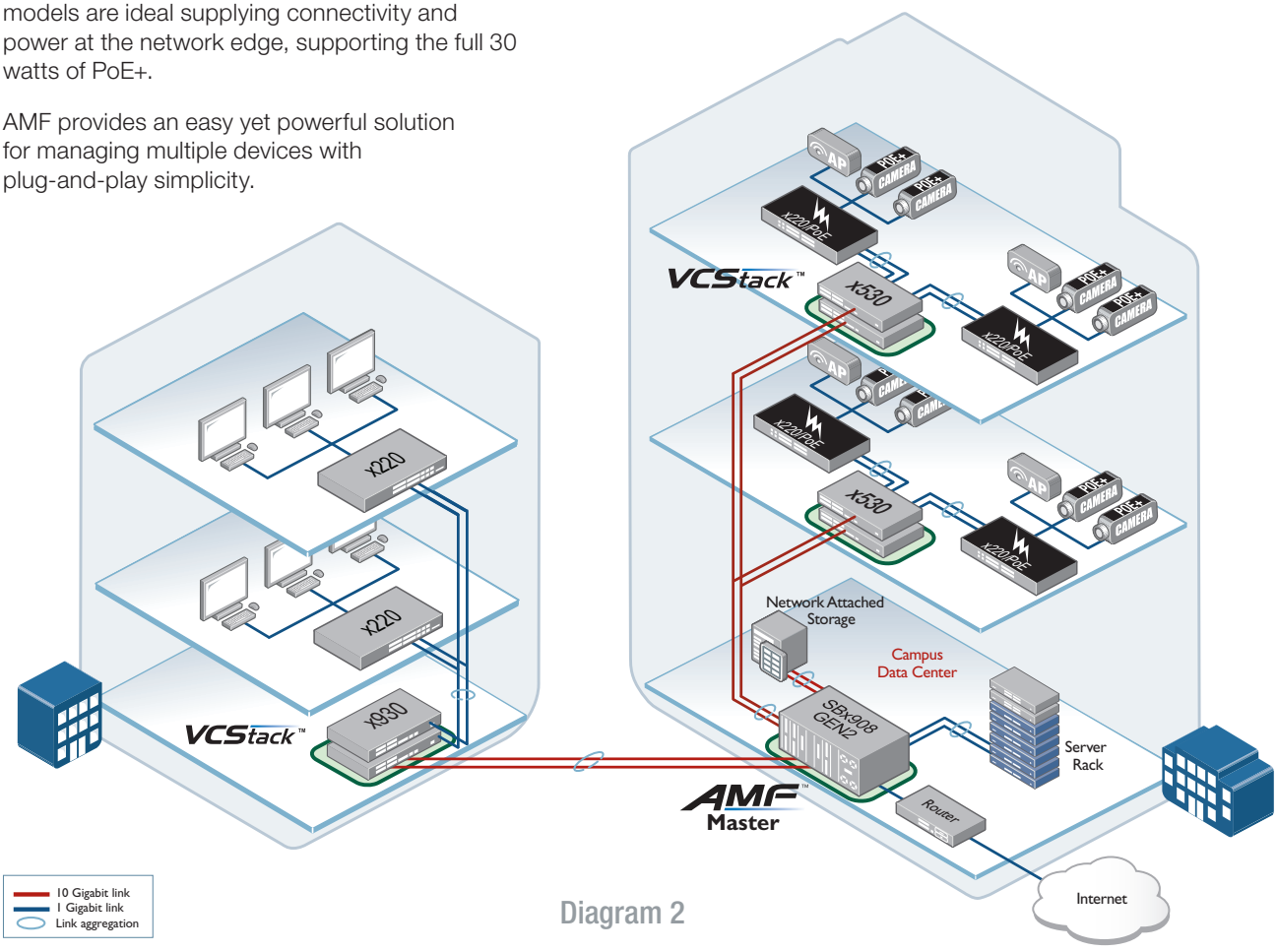


Diagram 2

Product Specifications

PRODUCT	10/100/1000T COPPER PORTS	100/1000X SFP PORTS	TOTAL PORTS	POE+ ENABLED PORTS	SWITCHING FABRIC	FORWARDING RATE
x220-28GS	-	28	28	-	56Gbps	41.7Mpps
x220-52GP	48	4	52	48	104Gbps	77.4Mpps
x220-52GT	48	4	52	-	104Gbps	77.4Mpps

Performance

- Up to 16K MAC addresses
- Routes: 16 (IPv4), 16 (IPv6)
- Up to 2K multicast entries
- 512MB DDR SDRAM
- 128MB flash memory
- 4094 configurable VLANs
- Packet Buffer memory: 1.5MB(28GS), 3MB(52GT)
- 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 1000T, 100X, 100FX, 100BX, 1000X, 1000SX, 1000LX, 1000ZX or 1000ZX CWDM SFPs

Diagnostic tools

- Active Fiber Monitoring detects tampering on optical links
- Built-In Self Test (BIST)
- 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

IP features

- IPv4 static routing and RIP
- 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
- Industry-standard CLI with context-sensitive help
- Powerful CLI scripting engine with built-in text editor
- Web-based Graphical User Interface (GUI)
- USB interface allows software release files, configurations and other files to be stored for backup and distribution to other devices
- 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 Features

- 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 Features

- Access Control Lists (ACLs) based on layer 3 and 4 headers, per VLAN or port
- Configurable ACLs for management traffic
- Dynamic ACLs assigned via port authentication
- ACL Groups enable multiple hosts/ports to be included in a single ACL, reducing configuration
- 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
- 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
- Secure Copy (SCP)
- Strong password security and encryption
- Tri-authentication: MAC-based, web-based and IEEE 802.1x
- RADIUS group selection per VLAN or port

Environmental specifications

- Operating temperature range:
  0°C to 50°C (32°F to 122°F)
  Derated by 1°C per 305 meters (1,000 ft)
- Storage temperature range:
  -25°C to 70°C (-13°F to 158°F)
- Operating relative humidity range:
  5% to 90% non-condensing
- Storage relative humidity range:
  5% to 95% non-condensing
- Operating altitude:
  3,048 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

Standards and Protocols

AlliedWare Plus Operating System

Version 5.5.0-1

Cryptographic Algorithms

FIPS Approved Algorithms

Encryption (Block Ciphers):

- AES (ECB, CBC, CFB and OFB Modes)
- 3DES (ECB, CBC, CFB and OFB Modes)

Block Cipher Modes:

- CCM
- CMAC
- GCM
- XTS

Digital Signatures & Asymmetric Key Generation:

- DSA
- ECDSA
- RSA

Secure Hashing:

- SHA-1
- SHA-2 (SHA-224, SHA-256, SHA-384. SHA-512)

Message Authentication:

- HMAC (SHA-1, SHA-2(224, 256, 384, 512)

Random Number Generation:

- DRBG (Hash, HMAC and Counter)

Physical Specifications

PRODUCT	WIDTH X DEPTH X HEIGHT	MOUNTING	WEIGHT		PACKAGED DIMENSIONS
			UNPACKAGED	PACKAGED	
x220-28GS	441 x 323 x 44 mm (17.36 x 12.72 x 1.73 in)	1RU Rack-mount	4.3 kg (9.47 lbs)	6.1 kg (13.45 lbs)	575 x 445 x 150 mm (22.64 x 17.52 x 5.90 in)
x220-52GP	441 x 359 x 44 mm (17.36 x 14.13 x 1.73 in)	1RU Rack-mount	5.8 kg (12.79 lbs)	7.8 kg (17.20 lbs)	575 x 520 x 150 mm (22.64 x 20.47 x 5.90 in)
x220-52GT	441 x 323 x 44 mm (17.36 x 12.72 x 1.73 in)	1RU Rack-mount	4.5 kg (9.92 lbs)	6.4 kg (14.12 lbs)	575 x 445 x 150 mm (22.64 x 17.52 x 5.90 in)

Power and Noise Characteristics

PRODUCT	NO POE LOAD			FULL POE+ LOAD (PWR800)				POE SOURCING PORTS	
	MAX POWER CONSUMPTION	MAX HEAT DISSIPATION	NOISE	MAX POWER CONSUMPTION	MAX HEAT DISSIPATION	NOISE	POE POWER BUDGET	POE (15W)	POE+ (30W)
x220-28GS	52W	179 BTU/h	39 dBA	-	-	-	-	-	-
x220-52GP	48W	164 BTU/h	42 dBA	909W	577 BTU/h	42 dBA	740W	48	24
x220-52GT	47W	160 BTU/h	39 dBA	-	-	-	-	-	-

Noise: tested to ISO7779; front bystander position

Latency (microseconds)

PRODUCT	PORT SPEED		
	10MPS	100MBPS	1GBPS
x220-28GS	39.6µs	6.8µs	3.8µs
x220-52GP	35.1µs	5.5µs	2.6µs
x220-52GT	35.1µs	5.5µs	2.6µs

Non FIPS Approved Algorithms

RNG (AES128/192/256)
DES
MD5

Ethernet Standards

IEEE 802.2 Logical Link Control (LLC)
IEEE 802.3 Ethernet
IEEE 802.3ab 1000BASE-T
IEEE 802.3af Power over Ethernet (PoE)
IEEE 802.3at Power over Ethernet (PoE+)
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 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 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 1724 RIPv2 MIB extension
RFC 2578 Structure of Management Information v2 (SMIv2)
RFC 2579 Textual conventions for SMIv2
RFC 2580 Conformance statements for SMIv2
RFC 2674 Definitions of managed objects for bridges with traffic classes, multicast filtering and VLAN extensions
RFC 2741 Agent extensibility (AgentX) protocol
RFC 2819 RMON MIB (groups 1,2,3 and 9)
RFC 2863 Interfaces group MIB
RFC 3176 sFlow: a method for monitoring traffic in switched and routed networks
RFC 3411 An architecture for describing SNMP management frameworks
RFC 3412 Message processing and dispatching for the SNMP
RFC 3413 SNMP applications
RFC 3414 User-based Security Model (USM) for SNMPv3
RFC 3415 View-based Access Control Model (VACM) for SNMP
RFC 3416 Version 2 of the protocol operations for the SNMP
RFC 3417 Transport mappings for the SNMP
RFC 3418 MIB for SNMP
RFC 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 Syslog protocol

Multicast Support

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

Routing Information Protocol (RIP)

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

Security Features

SSH remote login
SSLv2 and SSLv3
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 authentication
RFC 2866 RADIUS accounting
RFC 2868 RADIUS attributes for tunnel protocol support
RFC 2986 PKCS #10: certification request syntax specification v1.7
RFC 3546 Transport Layer Security (TLS) extensions
RFC 3579 RADIUS support for Extensible Authentication Protocol (EAP)
RFC 3580 IEEE 802.1x RADIUS usage guidelines
RFC 3748 PPP Extensible Authentication Protocol (EAP)
RFC 4251 Secure Shell (SSHv2) protocol architecture
RFC 4252 Secure Shell (SSHv2) authentication protocol
RFC 4253 Secure Shell (SSHv2) transport layer protocol
RFC 4254 Secure Shell (SSHv2) connection protocol
RFC 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 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

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

Feature Licenses

NAME	DESCRIPTION	INCLUDES
AT-FL-x220-8032	ITU-T G.8032 license	▶ G.8032 ring protection ▶ Ethernet CFM
AT-FL-x220-CPOE	Continuous PoE license	▶ Continuous PoE power for x220-52GP only

Ordering Information

19 inch rack-mount brackets included

AT-x220-28GS-xx
28-port 100/1000X SFP switch

AT-x220-52GP-xx
48-port 10/100/1000T-POE+ switch with 4 SFP uplink ports and single fixed PSU

AT-x220-52GT-xx
48-port 10/100/1000T switch with 4 SFP uplink ports and single fixed PSU

Where xx = 10 for US power cord
20 for no power cord
30 for UK power cord
40 for Australian power cord
50 for European power cord

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[1]
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-SPLXI0/I
1000LX GbE single-mode 1310 nm fiber up to 10 km industrial temperature

AT-SPBDI0-13
1000LX GbE Bi-Di (1310 nm Tx, 1490 nm Rx) fiber up to 10 km

AT-SPBDI0-14
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

AT-SPBD20-13/I[2]
1000BX GbE Bi-Di (1310 nm Tx, 1490 nm Rx) fiber up to 20 km

AT-SPBD20-14/I[2]
1000BX GbE Bi-Di (1490 nm Tx, 1310 nm Rx) fiber up to 20 km

AT-SPBD40-13/I
1000LX GbE single-mode Bi-Di (1310 nm Tx, 1490 nm Rx) fiber up to 40 km, industrial temperature

AT-SPBD40-14/I
1000LX GbE single-mode Bi-Di (1490 nm Tx, 1310 nm Rx) fiber up to 40 km, industrial temperature

[1]The tri-speed AT-SPSX only supports Gigabit connectivity in the x220-28GS
[2] Only supported in the x220-28GS

617-000639 RevJ