x320 Series

Gigabit Layer 3 PoE++/PoE Pass-through Switches

The Allied Telesis x320 Series of Gigabit Layer 3 PoE++/PoE pass-through switches offer an impressive set of features in a compact design. Flexible Power over Ethernet capabilities make them ideal for IoT device connectivity in smart buildings and business environments.

AMF™   EPSRing™   ACTIVE Fiber Monitoring™
AT-VISTA MANAGER™ EX   AMF-Sec
R6 READY   eco friendly   PoE plus   AlliedWare Plus OPERATING SYSTEM

Overview

Allied Telesis x320 Series are secure and reliable, offering 8 x Gigabit PoE enabled ports and 2 x SFP uplinks. Advanced power connectivity features provide flexibility and value to meet the needs of today's connected business. The x320-10GH can provide up to 90 Watts of PoE power on all ports, while the x320-11GPT can be powered by PoE[1], and also pass PoE power through to connected end points. Each switch offers 8 x 10M/100M/1 Gigabit ports and flexible Gigabit uplinks.

Flexible PoE

The x320 Series support today's commonly used PoE standards, providing 15.4 Watts of PoE (802.3af), and 30 Watts of PoE+ (802.3at). In addition, the x320-10GH also supports providing 60 or 90 Watts of PoE++ (802.3bt).

Continuous PoE

Continuous PoE allows the x320 Series switches 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.

Network Management

Vista Manager™ EX bundled with Allied Telesis Autonomous Management Framework™ (AMF) meets the increasing management requirements of modern networks. While AMF allows an entire network to be securely and easily managed as a single virtual device, Vista Manager EX provides an intuitive and powerful graphical tool for monitoring and managing AMF wired, Autonomous Wave Control (AWC) wireless, and third party (SNMP) devices.

Cybersecurity

The x320 series acting as an AMF member is compatible with our AMF-Security solution, which enables a self-defending network. The AMF–Sec controller responds immediately to any internal malware threats by instructing the x320 to isolate the affected part of the network, and quarantine the suspect device. Vista Manager EX alerts networks administrators of threats that have been dealt with.

Network resiliency

Allied Telesis Ethernet Protection Switched Ring (EPSRing™), and the standards-based G.8032 Ethernet Ring Protection, ensure that distributed network segments have high-speed, resilient access to online resources and applications.

Secure

A secure network environment is guaranteed. The x320 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.

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 or a malfunction.

Environmentally friendly

The x320 Series supports Energy Efficient Ethernet (EEE), automatically reducing the power consumed by the switch whenever there is no traffic on a port. This sophisticated feature can significantly reduce operating costs by reducing the power requirements of the switch and any associated cooling equipment.

The x320 models are fan-less, providing silent operation, which makes them ideal for desktop or work area deployment.

Key Features

- AlliedWare Plus Enterprise-class operating system
- Allied Telesis Autonomous Management Framework™ (AMF)
- Vista Manager EX compatible
- AMF-Security compatible
- Full 30 Watts of PoE+
- Up to 90 Watts of PoE++ (x320-10GH only)
- PoE pass-through (x320-11GPT only)
- Continuous PoE
- EPSRing™ and G.8032 for resilient rings
- EPSR Master
- Energy Efficient Ethernet saves power
- Active Fiber Monitoring
- Static and dynamic routing
- Fanless design for silent operation
- Flexible deployment
- Wide operating temperature range
- Multicast Source Discovery Protocol (MSDP)
- Link Monitoring

[1] The x320-11GPT uses PD port 11 to receive PoE power, but cannot be powered by PoE if the AC adapter is connected

Key Features

Allied Telesis Autonomous 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.

▶ 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.

Power over Ethernet (PoE+, PoE++, and PoE pass-through)

▶ The x320-10GH supports providing up to 90 Watts (PoE++) on all ports. This enables powering high power devices such as high resolution PTZ cameras with heater/blowers for outdoor applications, enhanced infrared lighting and lighting controllers, remote Point of Sale (POS) kiosks, and more.

▶ The x320-11GPT can supply up to 30 Watts (PoE+) to connected devices. It can be powered by an AC power adapter, or by PoE. When deployed together, the x320-11GPT can be powered by the x320-10GH, while PoE pass-through enables power from the x320-10GH to pass through the x320-11GPT to power connected end points.

PWR300 (External Power Supply)

▶ This PWR300 is the external Power Supply Unit (PSU) for x320-10GH. One PWR300 will power the switch and provide PoE power. Up to three PWR300 PSUs can be used to increase the available PoE power, and enable power supply redundancy.

Flexible deployment

▶ The x320 Series can operate from -10 to +55 degrees Celsius, and with a fanless design, and using the PoE passthrough feature, are ideally suited for flexible deployment in the ceiling of smart buildings and any other areas of the business premises.

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 x320 switches to form a high-speed protected ring, capable of recovery within as little as 50ms. This feature is perfect for high performance and high availability in enterprise networks. x320 Series switches can act as the EPSR Master.

▶ Super-Loop Protection (SLP) enables a link between two EPSR nodes to be in separate EPSR domains, improving redundancy and network fault resiliency.

G.8032 Ethernet Ring Protection

▶ G.8032 provides standards-based high-speed ring protection, that can be deployed stand-alone, or interoperate with Allied Telesis EPSR.

▶ Ethernet Connectivity Fault Monitoring (CFM) proactively monitors links and VLANs, and provides alerts when a fault is detected.

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. Boosted network performance and guaranteed delivery of business-critical Ethernet services and applications are provided. Time-critical services such as voice and video take precedence over non-essential services such as file downloads, maintaining responsiveness of Enterprise applications

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.

Open Shortest Path First (OSPFv2, OSPFv3)

▶ OSPF is a scalable and adaptive routing protocol for IP networks. The addition of OSPFv3 provides support for IPv6 and further strength for next generation networking.

sFlow

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

Active Fiber Monitoring (AFM)

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

Tri-authentication

▶ Authentication options on the x320 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.

TACACS+ Command Authorization

▶ TACACS+ Command Authorization offers centralized control over which commands may be issued by each specific AlliedWare Plus device user. It complements authentication and accounting services for a complete AAA solution.

Premium Software License

▶ By default, the x320 Series offers a comprehensive Layer 2 and Lite Layer 3 feature set that includes static routing and IPv6 management features. The feature set can easily be elevated to Basic Layer 3 by applying the premium software license. This adds dynamic routing protocols and Layer 3 multicasting capabilities.

VLAN Access Control List (ACLs)

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

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 Loop Detection Frame (LDF) packets that the switch listens for. If a port receives an LDF packet, you 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.

Multicast Source Discovery Protocol (MSDP)

▶ MSDP enables two or more PIM-SM (Sparse Mode) domains to share information on active multicast sources, for more efficient forwarding of multicast traffic.

Link Monitoring (Linkmon)

▶ Linkmon enables network health monitoring by regularly sending probes over key links to gather metrics comprising latency, jitter, and probe loss. This supports pro-active network management, and can also be used with triggers to automate a change to device or network configuration in response to the declining health of a monitored link.

Key Solutions

VCStack™

AMF™ Master

Legend:
- 1 Gigabit link
- PoE++
- PoE pass-through
- Link aggregation
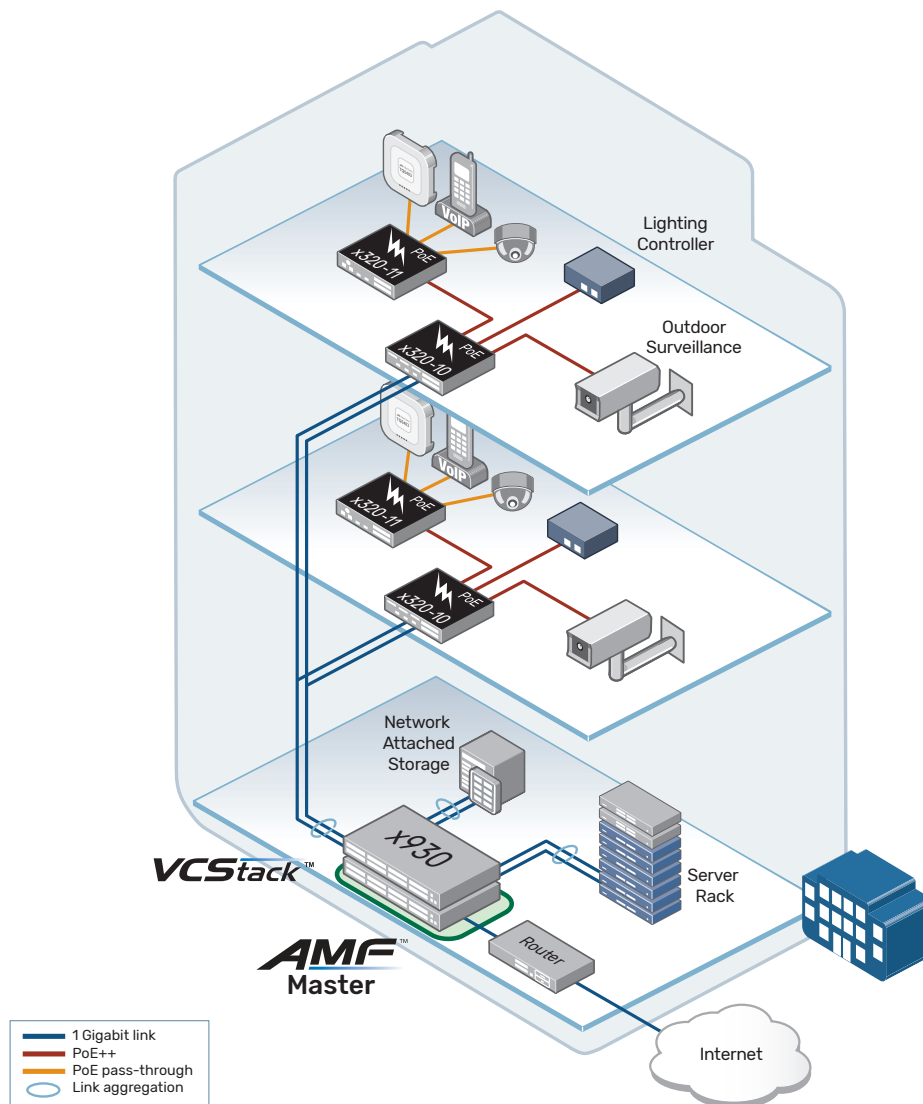
Enable today's smart buildings with flexible PoE

More than ever, PoE powered devices are converging on the Enterprise network to enable smooth business operation, with central management of building security and systems, as well as online user connectivity. The x320 Series are ideal for these modern business networks, with flexible PoE provision to connect and power a wide range of network and IoT devices.

The x320-10GH provides up to 90 Watts of PoE power per port, and as shown in the diagram can support high-power devices such as high resolution outdoor PTZ cameras with heater/blowers, advanced LED lighting controllers and more.

The x320-11GPT can supply up to 30 Watts of PoE power to connected devices, and can itself be powered by PoE or an AC adapter.

As shown in the diagram, the x320-10GH can use PoE to power the x320-11GPT, and also pass PoE power though it to connected devices such as IP phones, wireless access points and so on.

With their fanless design for silent operation, and supporting a wide temperature range, the x320 series offer very flexible deployment options. They can be DIN rail mounted in ceiling and other building spaces, and when powered by PoE the x320-11GPT doesn't require a separate power connection to operate. Used alongside PoE pass-through to connect and power end points, the x320 Series are an ideal solution for today's smart buildings and converged business networks.

x320 Series | Gigabit Layer 3 PoE++/PoE Pass-through Switches

Specifications

PRODUCT	10/100/1000T (RJ-45) POE+ ENABLED PORTS	10/100/1000T (RJ-45) POE++ ENABLED PORTS	10/100/1000T (RJ-45) POE-IN PORT	1000X SFP PORTS	SWITCHING FABRIC	FORWARDING RATE
x320-10GH	-	8	-	2	24Gbps	14.9Mpps
x320-11GPT	8	-	1	2	24Gbps	16.4Mpps

Performance
▶ Supports 10KB L2 jumbo frames
▶ Wire speed multicasting
▶ 4094 configurable VLANs
▶ Up to 16K MAC addresses
▶ Up to 2K multicast entries
▶ 512MB DDR3 SDRAM, 128MB NAND flash memory
▶ Packet buffer memory: 1.5MB

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

Expandability
▶ Versatile licensing options for additional features

Flexibility and Compatibility
▶ 1G-SFP ports on x320 will support any combination of Allied Telesis 100Mbps and 1000Mbps SFP modules listed in this document under Ordering Information
▶ Port speed and duplex configuration can be set manually or by auto-negotiation

Diagnostic Tools
▶ Active Fiber Monitoring detects tampering on optical links
▶ Built-In Self Test (BIST)
▶ Cable fault locator (TDR)
▶ Connectivity Fault Management (CFM) - Continuity Check Protocol (CCP) for use with G.8032 ERPS
▶ Find-me device locator
▶ Automatic link flap detection and port shutdown
▶ Optical Digital Diagnostic Monitoring (DDM)
▶ Ping polling for IPv4 and IPv6
▶ Port mirroring
▶ Trace Route for IPv4 and IPv6
▶ Uni-Directional Link Detection (UDLD)

IPv4 Features
▶ Black hole routing
▶ Directed broadcast forwarding
▶ DNS relay
▶ Equal Cost Multi Path (ECMP) routing
▶ Policy-based routing
▶ Route maps and redistribution (OSPF and RIP)
▶ Static unicast and multicast routing for IPv4
▶ UDP broadcast helper (IP helper)

IPv6 Features
▶ DHCPv6 client and relay
▶ DNSv6 client and relay
▶ IPv4 and IPv6 dual stack
▶ IPv6 aware storm protection and QoS
▶ IPv6 hardware ACLs
▶ Device management over IPv6 networks with SNMPv6, Telnetv6 and SSHv6
▶ NTPv6 client and server
▶ Static unicast and multicast routing for IPv6
▶ Log to IPv6 hosts with Syslog v6
▶ IPv6 Ready certified

Management
▶ Allied Telesis Autonomous 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
▶ 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
▶ USB interface allows software release files, configurations and other files to be stored for backup and distribution to other devices
▶ Management stacking allows up to 24 devices to be managed from a single console

Quality of Service
▶ 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
▶ Wire speed traffic classification with low latency essential for VoIP and real-time streaming media applications
▶ IPv6 QoS support
▶ Policy-based QoS based on VLAN, port, MAC and general packet classifiers
▶ Policy-based storm protection
▶ Extensive remarking capabilities
▶ Queue scheduling options for Strict priority, weighted round robin or mixed scheduling
▶ Type of Services (ToS) 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 Super-Loop Protection (SLP) and enhanced recovery for extra resiliency
▶ Loop protection: loop detection and thrash limiting
▶ PVST+ compatibility mode
▶ STP root guard

Security Features
▶ Access Control Lists (ACLs) based on layer 3 and 4 headers
▶ Configurable auth-fail and guest VLANs
▶ Dynamic ACLs assigned via port authentication
▶ ACL Groups enable multiple hosts/ports to be included in a single ACL, reducing configuration
▶ 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)
▶ 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
▶ Learn limits (intrusion detection) for single ports or LAGs
▶ Private VLANs provide security and port isolation for multiple customers using the same VLAN
▶ RADIUS group selection per VLAN or port
▶ Secure Copy (SCP)
▶ Secure File Transfer (SFTP) client
▶ Strong password security and encryption
▶ Tri-authentication: MAC-based, web-based and IEEE 802.1x
▶ Web-based authentication

Environmental Specifications
▶ Operating temperature range: -10°C to 55°C (14°F to 131°F)
▶ 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: 3,000 meters maximum (9,843 ft)

Electrical Approvals and Compliances
▶ EMC: EN55032 class A, FCC class A, VCCI class A, ICES-003 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
▶ Certification: UL, cUL

Restrictions on Hazardous Substances (RoHS) Compliance
▶ EU RoHS compliant
▶ China RoHS compliant

x320 Series | Gigabit Layer 3 PoE++/PoE Pass-through Switches

Physical Specifications

PRODUCT	WIDTH X DEPTH X HEIGHT	MOUNTING	WEIGHT		PACKAGED DIMENSIONS
			UNPACKAGED	PACKAGED	
x320-10GH	210 x 180 x 42.5 mm (8.26 x 7.08 x 1.67 in)	Rack-mount	1.6 kg	2.7 kg	417 x 336 x 151 mm (16.42 x 13.23 x 1.67 in)
x320-11GPT	210 x 180 x 42.5 mm (8.26 x 7.08 x 1.67 in)	Rack-mount	1.6 kg	3.5 kg	417 x 336 x 151 mm (16.42 x 13.23 x 1.67 in)

Power Characteristics

PRODUCT	MAXIMUM POE POWER	MAXIMUM POE PORTS SUPPORTED					NO POE LOAD		FULL POE LOAD	
		POE (7.5W)	POE (15.4W)	POE+ (30W)	POE++ (60W)	POE++ (90W)	MAX POWER CONSUMPTION (W)	MAX HEAT DISSIPATION (BTU/H)	MAX POWER CONSUMPTION (W)	MAX HEAT DISSIPATION (BTU/H)
x320-10GH	240W (1 x PWR300 PSU)	8	8	8	4	2	21	71	320	218
	480W (2 x PWR300 PSUs)	8	8	8	8	5			600	409
	720W (3 x PWR300 PSUs)	8	8	8	8	8			880	600
x320-11GPT	0W (switch powered by 30W PoE)[1]	0	0	0	0	0	22	75	98 (using AC power adapter)	350 (using AC power adapter)
	31.6W (switch powered by 60W PoE)[1]	4	2	1	0	0				
	46.2W (switch powered by 90W PoE)[1]	6	3	1	0	0				
	62W (switch powered by AC Adaptor)	8	4	2	0	0				

Latency (microseconds)

PRODUCT	PORT SPEED	
	100MBPS	1GBPS
x320-10GH	5.4μs	3.0μs
x320-11GPT	5.5μs	3.0μs

Standards and Protocols

AlliedWare Plus Operating System
Version 5.5.1

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

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)

Non FIPS Approved Algorithms
RNG (AES128/192/256)
DES
MD5

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

Ethernet 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 up to 30W (PoE+)
IEEE 802.3bt Power over Ethernet Plus 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 Features
RFC 768   User Datagram Protocol (UDP)
RFC 791   Internet Protocol (IP)
RFC 792   Internet Control Message Protocol (ICMP)
RFC 793   Transmission Control Protocol (TCP)
RFC 826   Address Resolution Protocol (ARP)
RFC 894   Standard for the transmission of IP datagrams over Ethernet networks
RFC 919   Broadcasting Internet datagrams
RFC 922   Broadcasting Internet datagrams in the presence of subnets
RFC 932   Subnetwork addressing scheme
RFC 950   Internet standard subnetting procedure
RFC 951   Bootstrap Protocol (BootP)
RFC 1027   Proxy ARP
RFC 1035   DNS client
RFC 1042   Standard for the transmission of IP datagrams over IEEE 802 networks
RFC 1071   Computing the Internet checksum
RFC 1122   Internet host requirements
RFC 1191   Path MTU discovery
RFC 1256   ICMP router discovery messages
RFC 1518   An architecture for IP address allocation with CIDR
RFC 1519   Classless Inter-Domain Routing (CIDR)
RFC 1542   Clarifications and extensions for BootP
RFC 1591   Domain Name System (DNS)
RFC 1812   Requirements for IPv4 routers
RFC 1918   IP addressing
RFC 2581   TCP congestion control

IPv6 Features
RFC 1981   Path MTU discovery for IPv6
RFC 2460   IPv6 specification
RFC 2464   Transmission of IPv6 packets over Ethernet networks
RFC 3056   Connection of IPv6 domains via IPv4 clouds
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
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
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 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)

[1] The x320-11GPT uses PD port 11 to receive PoE power, but cannot be powered by PoE if the AC adapter is connected

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 2787	Definitions of managed objects for VRRP
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
RFC 6527	Definitions of managed objects for VRRPv3

Multicast Support

Bootstrap Router (BSR) mechanism for PIM-SM
IGMP query solicitation
IGMP snooping (IGMPv1, v2 and v3)
IGMP snooping fast-leave
IGMP/MLD multicast forwarding (IGMP/MLD proxy)
MLD snooping (MLDv1 and v2)
PIM for IPv6

RFC 1112	Host extensions for IP multicasting (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 3618	Multicast Source Discovery Protocol (MSDP)
RFC 3810	Multicast Listener Discovery v2 (MLDv2) for IPv6
RFC 3956	Embedding the Rendezvous Point (RP) address in an IPv6 multicast address
RFC 3973	PIM Dense Mode (DM)
RFC 4541	IGMP and MLD snooping switches
RFC 4601	Protocol Independent Multicast - Sparse Mode (PIM-SM): protocol specification (revised)
RFC 4604	Using IGMPv3 and MLDv2 for source-specific multicast
RFC 4607	Source-specific multicast for IP

Open Shortest Path First (OSPF)

OSPF link-local signaling
OSPF MD5 authentication
OSPF restart signaling
Out-of-band LSDB resync

RFC 1245	OSPF protocol analysis
RFC 1246	Experience with the OSPF protocol
RFC 1370	Applicability statement for OSPF
RFC 1765	OSPF database overflow
RFC 2328	OSPFv2
RFC 2370	OSPF opaque LSA option
RFC 2740	OSPFv3 for IPv6
RFC 3101	OSPF Not-So-Stubby Area (NSSA) option
RFC 3509	Alternative implementations of OSPF area border routers
RFC 3623	Graceful OSPF restart
RFC 3630	Traffic engineering extensions to OSPF
RFC 4552	Authentication/confidentiality for OSPFv3
RFC 5329	Traffic engineering extensions to OSPFv3

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
RFC 5798	Virtual Router Redundancy Protocol version 3 (VRRPv3) for IPv4 and IPv6

Routing Information Protocol (RIP)

RFC 1058	Routing Information Protocol (RIP)
RFC 2080	RIPng for IPv6
RFC 2081	RIPng protocol applicability statement
RFC 2082	RIP-2 MD5 authentication
RFC 2453	RIPv2

Security Features

SSH remote login
SSLv2 and SSLv3
TACACS+ Accounting, Authentication and Authorization (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 2246	TLS protocol v1.0
RFC 2818	HTTP over TLS ("HTTPS")
RFC 2865	RADIUS authentication
RFC 2866	RADIUS accounting
RFC 2868	RADIUS attributes for tunnel protocol support
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 (server, relay and client)
RFC 2132	DHCP options and BootP vendor extensions
RFC 2616	Hypertext Transfer Protocol - HTTP/1.1
RFC 2821	Simple Mail Transfer Protocol (SMTP)
RFC 2822	Internet message format
RFC 3046	DHCP relay agent information option (DHCP option 82)
RFC 3315	DHCPv6 (server, relay and client)
RFC 3633	IPv6 prefix options for DHCPv6
RFC 3646	DNS configuration options for DHCPv6
RFC 3993	Subscriber-ID suboption for DHCP relay agent option
RFC 4330	Simple Network Time Protocol (SNTP) version 4
RFC 5905	Network Time Protocol (NTP) version 4

VLAN Support

Generic VLAN Registration Protocol (GVRP)
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 (VoIP)

LLDP-MED   ANSI/TIA-1057
Voice VLAN

Feature Licenses

NAME	DESCRIPTION	INCLUDES
AT-FL-x320-01	x320 premium license	▶ OSPF (256 routes) ▶ PIMv4-SM, DM, and SSM ▶ RIPng (256 routes) ▶ OSPFv3 (256 routes) ▶ PIMv6-SM and SSM ▶ MLD v1/v2 ▶ VLAN double tagging (Q-in-Q)
AT-FL-x320-8032	ITU-T G.8032 license	▶ G.8032 ring protection ▶ Ethernet CFM
AT-FL-x320-CPOE	Continuous PoE license	▶ Continuous PoE power

Ordering Information

Switches

19 inch rack-mount brackets included

AT-x320-10GH

8-port 10/100/1000T PoE++ switch with 2 SFP ports, and 3 external PSU ports[2]

AT-x320-11GPT

8-port 10/100/1000T PoE+ switch with 2 SFP ports, one AC adapter port[3], and one PoE-in port[4] (supporting PD and PoE pass-through)

Power Supplies

AT-PWR300-xx

300W PoE power supply (for x320-10GH and GS980EM/10H switches)

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

[2] PWR300 power supplies for the x320-10GH must be ordered separately
[3] The x320-11GPT ships with an AC power adapter
[4] The x320-11GPT can be powered by PoE from 30W (class 4) to 90W (class 8)

SFP Modules

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-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
1000BX GbE Bi-Di (1310 nm Tx, 1490 nm Rx) fiber up to 20 km

AT-SPBD20-14/I
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

Allied Telesis™