x330 Series

Gigabit Layer 3 Access Switches

The Allied Telesis x330 Series Layer 3 Gigabit switches offer an impressive set of features in a compact fanless design, making them an ideal access solution for modern applications.

Overview

The Allied Telesis x330 Series provide an excellent access solution supporting Gigabit to the desktop for maximum performance. With Multi-Gigabit and 10 Gigabit copper and fiber uplinks, and a fanless design for silent operation, the x330 Series are ideal for the edge of business networks in the IoT era. With support for Layer 3 routing protocols, the x330 Series can also be deployed as distribution or small branch office core switches.

Manageable

The x330 Series run 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 management.

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

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 x330 Series acting as AMF members are 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 x330 Series 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 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 x330 Series provide features to detect loops as soon as they are created. Loop detection and thrash limiting take immediate action to prevent network storms.

Secure

Network security is guaranteed, with powerful control over network traffic types, secure management options, and other multi-layered security features built right in.

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

Allied Telesis x330 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.

Resilient

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.

Future-proof

The x330 Series are Software Defined Networking (SDN) ready and able to support OpenFlow v1.3.

ECO friendly

The x330 Series support Energy Efficient Ethernet, which automatically reduces the power consumed by the switch whenever there is no traffic on a port.

The x330 Series are fanless, 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
- 10G copper and fiber uplinks
- Multi-Gigabit (1/2.5/5/10G) port for flexible uplink options
- EPSRing™ and G.8032 for resilient rings
- EPSR Master
- Energy Efficient Ethernet saves power
- Upstream Forwarding Only (UFO)
- Active Fiber Monitoring
- Static and dynamic routing
- Fanless design for silent operation
- Web-based Device GUI
- Multicast Source Discovery Protocol (MSDP)
- Link Monitoring

Key Features

Allied Telesis Autonomous Management Framework™ (AMF)

- AMF is a sophisticated suite of management tools that provide a simplified approach to network management. Common tasks are automated or made so simple that the every-day running of a network can be achieved without the need for highly-trained, and expensive, network engineers. Powerful features like centralized management, auto-backup, auto-upgrade, auto-provisioning and auto-recovery enable plug-and-play networking and zero-touch management

Virtual Chassis Stacking (VCStack™)

- The x330-20GTX and x330-28GTX can form a VCStack of up to six switches, with 40 Gbps of stacking bandwidth. VCStack provides a highly-available system in which network resources are spread out across stacked units, minimizing the impact should any unit fail.

Ethernet Protection Switched Ring (EPSRing™)

- EPSRing allows several x330 switches to join a protected ring capable of recovery within as little as 50ms. This feature is perfect for high availability in enterprise networks.
- The x330 Series can act as the ESPR Master, or be deployed as an EPSR transit node.

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.

Access Control Lists (ACLs)

- The x330 Series feature 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. Access Control Lists (ACLs) can be applied to a Virtual LAN (VLAN) as well as a specific port.

Upstream Forwarding Only (UFO)

- UFO lets you manage which ports in a VLAN can communicate with each other, and which only have upstream access to services, for secure multi-user deployment.

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 3 switch, a static route can be added to allow a user in a different subnet to manage the switch.
- The Device GUI enables graphical monitoring and management of the switch, simplifying administration

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.

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.

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 a real-time view of network traffic.

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.

Tri-authentication

- Authentication options on the x330 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

- 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 x330 Series offer a comprehensive Layer 2 and basic Layer 3 feature set that includes static routing and IPv6 management features. The feature set can easily be elevated to full Layer 3 by applying the premium software license. This adds dynamic routing protocols and Layer 3 multicasting capabilities.

Unidirectional Link Detection

- 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 either the individual transmitter or receiver for that connection fails.

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.

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.

VLAN Translation

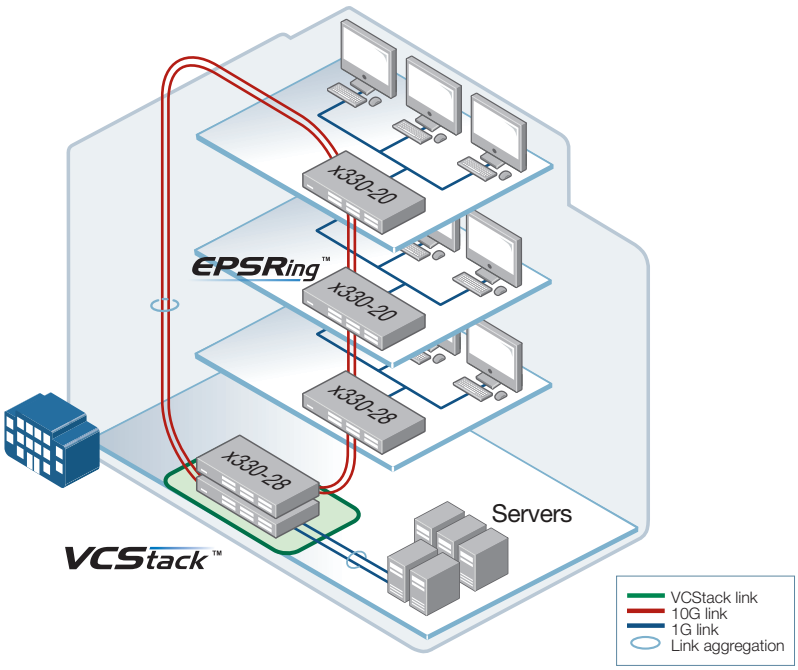
- VLAN Translation allows traffic arriving on a VLAN to be mapped to a different VLAN on the outgoing interface.
- Service Providers can provide customers with a unique VLAN ID, which can be changed for data transfer through the SP's network.
- In the Enterprise, it can be used to merge two networks together, without manually reconfiguring the VLAN numbering scheme.

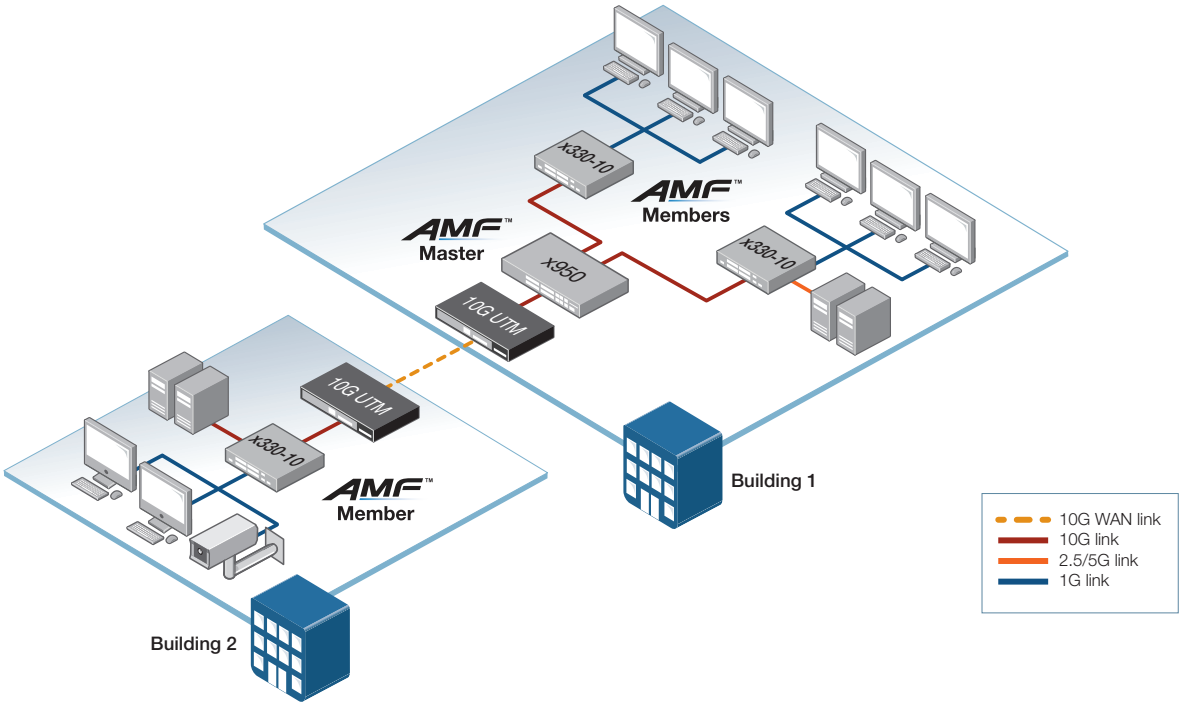
Key Solutions

Resilient small network core

The x330-20GTX and x330-28GTX can form a VCStack of up to 6 switches to provide load-sharing and network redundancy for flexible deployment. With the addition of dynamic routing and multicasting capability, the x330-20GTX and x330-28GTX are ideal as a resilient small network core solution.

The x330 series support EPSR master capability with no feature license required. With EPSRing, the x330 series can deliver high-performance resilient ring connectivity with automatic recovery in as little as 50ms.





Flexible deployment

The fanless and compact design of the x330-10GTX makes it ideal for use in office spaces where quiet operation is required. Advanced network control features ensure secure always-on access to online resources and applications.

10 Gigabit uplinks from the x330-10GTX edge switches provides maximum throughput, and business buildings can be connected with secure 10G WAN connectivity for high performance. The flexible x330 series are capable of connecting at 2.5G and 5G Multi-Gigabit speeds, which enables fully flexible deployment that maximizes network and building infrastructure.

Specifications

Performance

- Supports 10KB L2 jumbo frames for 2.5G connections, or 12KB for all other connection speeds
- Wire speed multicasting
- 4094 configurable VLANs
- 16K MAC addresses
- 1GB DDR3 SDRAM, 256MB NAND flash memory
- Packet buffer memory: 2MB

Reliability

- Modular AlliedWare Plus operating system
- Temperature and internal voltages. SNMP traps alert network managers in case of any failure

Expandability

- Create a VCStack of up to six x330-20GTX and x330-28GTX switches
- Versatile licensing options for additional features

Flexibility and Compatibility

- 10G SFP+ ports will support any combination of Allied Telesis 1000Mbps SFP and 10GbE SFP+ modules and direct attach cables listed in this document under Ordering Information
- The 1/2.5/5/10G Multi-Gigabit port enables flexible uplink options, and support for legacy cabling
- Port speed and duplex configuration can be set manually or by auto-negotiation
- Front-panel SFP+ stacking ports can be configured as 1G/10G Ethernet ports

Diagnostic Tools

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

IPv4 Features

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

IPv6 Features

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

Management

- Industry-standard CLI with context-sensitive help
- Built-in text editor and powerful CLI scripting engine
- Comprehensive SNMP MIB support for standards-based device management
- Console management port on the front panel for ease of access
- Event-based triggers allow user-defined scripts to be executed upon selected system events
- Eco-friendly mode allows ports and LEDs to be disabled to save power
- USB interface allows software release files, configurations and other files to be stored for backup and distribution to other devices
- Front panel 7-segment LED provides at-a-glance status and fault information
- Web-based Graphical User Interface (GUI)
- Autonomous Management Framework (AMF) enables powerful centralized management and zero-touch device installation and recovery.

Quality of Service

- IP precedence and DiffServ marking based on Layer 2, 3 and 4 headers
- Queue scheduling options for strict priority, weighted round robin or mixed scheduling
- Taildrop for queue congestion control
- Extensive remarking capabilities
- Policy-based QoS based on VLAN, port, MAC and general packet classifiers
- Type of Services (ToS) IP precedence and DiffServ marking based on layer 2, 3 and 4 headers
- Limit bandwidth per port or per traffic class down to 64kbps
- 8 priority queues with a hierarchy of high priority queues for real time traffic, and mixed scheduling, for each switch port
- Policy-based storm protectionl
- Wirespeed traffic classification with low latency essential for VoIP and real-time streaming media applications

Resiliency Features

- EPSRing (Ethernet Protection Switched Rings) with Super Loop Protection (SLP) and enhanced recovery
- STP root guard
- Loop protection: thrash limiting and loop detection
- Dynamic link failover (host attach)
- Control Plane Prioritization (CPP) ensures the CPU always has sufficient bandwidth to process network control traffic
- PVST+ compatibility mode
- BPDU forwarding
- VCStack fast failover minimizes network disruption
- SFP+ stacking ports can be configured as 10G Ethernet ports

Security Features

- MAC address filtering and MAC address lock-down
- Port-based learn limits (intrusion detection)
- Access Control Lists (ACLs) based on layer 3 and 4 headers
- Private VLANs provide security and port isolation for multiple customers using the same VLAN
- Secure Copy (SCP)
- BPDU protection
- Network Access and Control (NAC) features manage endpoint security
- Dynamic VLAN assignment
- Tri-authentication: MAC-based, web-based and IEEE 802.1x
- DoS attack blocking and virus throttling
- DHCP snooping, IP source guard and Dynamic ARP Inspection (DAI)
- Strong password security and encryption
- Auth fail and guest VLANs
- Secure File Transfer Protocol (SFTP) client
- Authentication, Authorisation and Accounting (AAA)
- Bootloader can be password protected for device security
- Configurable ACLs for management traffic
- RADIUS group selection per VLAN or port

Environmental Specifications

- Operating temperature range: 0°C to 50°C (32°F to 122°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: 3,048 meters maximum (10,000 ft)

Software Defined Networking (SDN)

- OpenFlow v1.3 with support for encryption, connection interruption and inactivity probe

Electrical Approvals and Compliances

- EMC: EN55032 class A, FCC class A, VCCI class A, ICES-003 class A
- Immunity: EN55035, EN61000-3-levels 2 (Harmonics), and 3 (Flicker) – AC models only

Safety

- Standards: UL62368-1, CAN/CSA-C22.2 No.62368-1, EN62368-1, EN60825-1, AS/NZS62368.1
- Certification: UL, cUL

Restrictions on Hazardous Substances (RoHS) Compliance

- EU RoHS compliant
- China RoHS compliant

Product Specifications

PRODUCT	10/100/1000T (RJ-45) COPPER PORTS	1/2.5/5/10GT COPPER PORT	1/10G SFP+ PORT	TOTAL PORTS	SWITCHING FABRIC	FORWARDING RATE
x330-10GTX	8	1	1	10	56Gbps	41.6Mpps
x330-20GTX	16	2	2	20	72Gbp	83.3Mpps
x330-28GTX	24	2	2	28	128Gbp	95.2Mpps

Physical Specifications

PRODUCT	WIDTH X DEPTH X HEIGHT	MOUNTING	WEIGHT		PACKAGED DIMENSIONS
			UNPACKAGED	PACKAGED	
x330-10GTX	263 x 179 x 38 mm (10.35 x 7.04 x 1.497 in)	Rack-mount	1.6 kg (3.53 lb)	2.97 kg (6.55 lb)	462 x 258 x 107 mm (18.19 x 10.15 x 4.21 in)
x330-20GTX	341 x 231 x 44 mm (13.42 x 9.09 x 1.73 in)	Rack-mount	3.0 kg (6.61 lb)	4.42 kg (9.74 lb)	530 x 360 x 120 mm (20.86 x 14.17 x 4.72 in)
x330-28GTX	341 x 231 x 44 mm (13.42 x 9.09 x 1.73 in)	Rack-mount	3.1 kg (6.84 lb)	4.42 kg (9.74 lb)	530 x 360 x 120 mm (20.86 x 14.17 x 4.72 in)

Latency (microseconds)

PRODUCT	PORT SPEED				
	100MBPS	1GBPS	2.5GBPS	5GBPS	10GBPS
x330-10GTX	6.22	3.68	3.24	2.86	1.73
x330-20GTX	7.32	3.73	3.48	3.13	1.87
x330-28GTX	7.18	3.71	3.39	3.04	1.82

Power Characteristics

PRODUCT	MAX POWER CONSUMPTION(W)	MAX HEAT DISSIPATION(BTU/H)
x330-10GTX	21	71
x330-20GTX	28	96
x330-28GTX	33	114

Standards and Protocols

AlliedWare Plus Operating System

Version 5.5.2-2

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 802.3ae 10 Gigabit Ethernet
IEEE 802.3az Energy Efficient Ethernet (EEE)
IEEE 802.3bz 2.5GBASE-T and 5GBASE-T ("multi-gigabit")
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 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 2787 Definitions of managed objects for VRRP
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 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 4502 RMON 2
RFC 4560 Definitions of managed objects for remote ping, traceroute and lookup operations
RFC 5424 The Syslog protocol
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 and PIM SSM 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
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
RFC 5340 OSPFv3 for IPv6 (partial support)

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 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 (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	STACK LICENSING
AT-FL-x330-01	x330 Premium license	▶ OSPF[1] (256 routes) ▶ PIMv4-SM, DM and SSM v4 ▶ RIPng[2] (256 routes) ▶ OSPFv3[2] (256 routes) ▶ PIM-SMv6/SSMv6 ▶ MLD v1/v2 ▶ VLAN double tagging (Q-in-Q) ▶ VLAN translation	▶ One license per stack member
AT-FL-x330-8032	ITU-T G.8032 license	▶ G.8032 ring protection ▶ Ethernet CFM	▶ One license per stack
AT-FL-x330-0F13-1YR	OpenFlow license	▶ OpenFlow v1.3 for 1 year	▶ Not supported on a stack
AT-FL-x330-0F13-5YR	OpenFlow license	▶ OpenFlow v1.3 for 5 years	▶ Not supported on a stack

[1] The standard switch software supports 1,000 IPv4 Static, 256 RIP, and 64 OSPF routes
[2] The standard switch software supports 1,000 IPv6 Static, and no RIPng or OSPFv3 routes

Ordering Information

Model availability can vary between regions. Please check to see which models are available in your region.

AT-x330-10GTX-xx
8-port 10/100/1000T switch, with 1 x 1/2.5/5/10G copper port, 1 x SFP/SFP+ port, and 1 fixed PSU

AT-x330-20GTX-xx
16-port 10/100/1000T switch, with 2 x 1/2.5/5/10G copper ports, 2 x SFP/SFP+ ports, and1 fixed PSU

AT-x330-28GTX-xx
24-port 10/100/1000T switch, with 2 x 1/2.5/5/10G copper ports, 2 x SFP/SFP+ ports, and 1 fixed PSU

AT-RKMT-J05
Rack Mount Tray for x330-10GTX

AT-RKMT-J13
Rack Mount Kit for x330-20GTX and x330-28GTX

AT-BRKT-J23
Wall mount kit for x330-10GTX

AT-BRKT-J24
Wall mount kit for x330-20GTX and x330-28GTX

AT-VT-Kit3
Management Cable (USB to Serial Console)

AT-STND-J03
Stand-kit for AT-x330-28GTX

Where x = 10 for US power cord
30 for UK power cord
40 for Australian power cord
50 for European power cord

[3] Trade Act Agreement compliant

10G SFP+ Modules

Any 10G SFP+ module or cable can be used for stacking with the front panel 10G ports

AT-SP10SR
10GSR 850 nm short-haul, 300 m with MMF

AT-SP10SR/I
10GSR 850 nm short-haul, 300 m with MMF industrial temperature

AT-SP10LR20/I
10GER 1310 nm long-haul, 20 km with SMF industrial temperature

AT-SP10TM
1G/2.5G/5G/10G, 100m copper, TAA[3]

AT-SP10BD10/I-12
10 GbE Bi-Di (1270 nm Tx, 1330 nm Rx) fiber up to 10 km industrial temperature, TAA[3]

AT-SP10BD10/I-13
10 GbE Bi-Di (1330 nm Tx, 1270 nm Rx) fiber up to 10 km industrial temperature, TAA[3]

AT-SP10BD20-12
10 GbE Bi-Di (1270 nm Tx, 1330 nm Rx) fiber up to 20 km, TAA[3]

AT-SP10BD20-13
10 GbE Bi-Di (1330 nm Tx, 1270 nm Rx) fiber up to 20 km, TAA[3]

AT-SP10TW1
1 meter SFP+ direct attach cable

AT-SP10TW3
3 meter SFP+ direct attach cable

1000Mbps SFP Modules

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

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

AT-SPLX10a
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 (LC) GbE Bi-Di (1310 nm Tx, 1490 nm Rx) fiber up to 10 km

AT-SPBD10-14
1000LX (LC) GbE Bi-Di (1490 nm Tx, 1310 nm Rx) fiber up to 10 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 (LC) GbE single-mode Bi-Di (1310 nm Tx, 1490 nm Rx) fiber up to 40 km, industrial temperature

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

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

AT-SPTX
10/100/1000 TX (RJ45), up to 100 m

617-000688 RevF