



x210 Series

ENTERPRISE EDGE SWITCHES

Allied Telesis $\times 210$ Series Layer 2+ switches offer an impressive set of features in an affordable package, ideal for applications at the network edge.



The Allied Telesis x210 Series is a reliable and value-packed solution for today's networks. With a choice of 9-, 16- and 24-port versions, each with one or more SFP uplinks, the x210 Series switches are ideal for applications at the edge of the network where security and manageability are the key requirements.

Secure

Network security is guaranteed, with powerful control over network traffic types, secure management options, and other multi-layered security features built right into the x210 Series switches.

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

Allied Telesis x210 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.

Network Protection

Advanced storm protection features include bandwidth limiting, policy-based storm protection and packet storm protection.

Network storms are often caused by cabling errors that result in a network loop. Allied Telesis ×210 Series switches provide features to detect loops as soon as they are created. Loop detection and thrash limiting take immediate action to prevent network storms.

Manageable

The ×210 runs the advanced AlliedWare Plus™ fully featured operating system, delivering a rich feature set and an industry-standard CLI, which reduces training requirements and is consistent across all AlliedWare Plus devices, simplifying network management. The CLI allows automation of configuration tasks, as commands may be used in scripts. In addition, triggers provide a powerful management mechanism, automating script execution in response to specific events.

Features

- » Comprehensive security features
- » Easy management
- » Silent operation
- » Future-proof

Investment Protection

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 x2IO Series supports IPv6 forwarding in hardware and features MLD snooping for efficient use of network bandwidth.

Silent Fan-less Operation

The x210 Series features compact models that are highly reliable and run silently, making them the ideal choice for placement on a desktop or in a dusty environment, without affecting their expected lifetime.

Key Features

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 tran.

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.

Access Control Lists (ACLs)

» The x210 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.

Tri-authentication

» Authentication options on the x210 Series also include alternatives to 802.1x port-based authentication, such as web authentication, to enable guest access and MAC authentication for end points that do not have an 802.1x supplicant. All three authentication methods—802.1x, MAC-based and Web-based—can be enabled simultaneously on the same port, resulting in tri-authentication.

Dynamic Host Configuration Protocol (DHCP) Snooping

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

Strong Passwords

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

EPSRing™ (Ethernet Protection Switched Ring)

» EPSRing allows several x210 switches to join a protected ring capable of recovery within as little as 50ms. This feature is perfect for high availability in enterprise networks.

Link Aggregation

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

Voice VLAN

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

Find Me

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

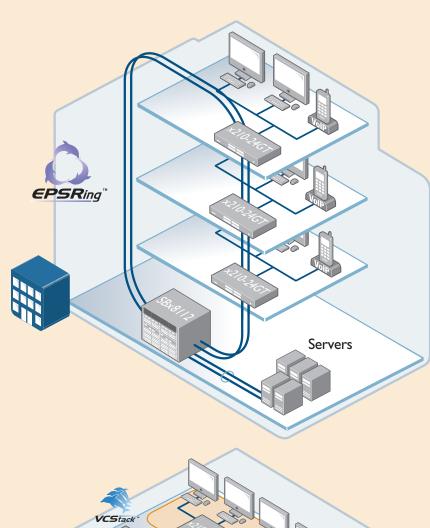


2 | x210 Series alliedtelesis.com

Key Solutions

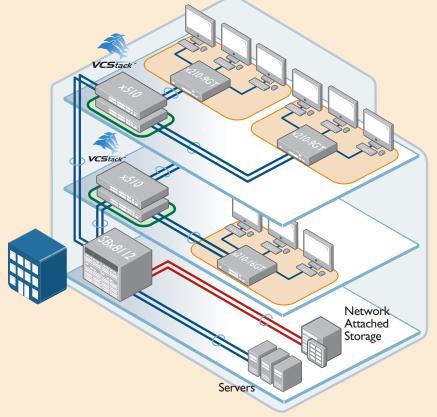
Network Convergence

The convergence of network services in the Enterprise has led to increasing demand for highly available networks with minimal downtime. Diagram I shows x210-24GT switches with high performance EPSR connectivity to the SwitchBlade® x8112 core chassis. This topology provides recovery in as little as 50ms, if required. Management of the network is simplified as all x-series switches run the advanced AlliedWare Plus operating system, with an industry-standard CLI.



Network Flexibility

Flexible network deployment is facilitated by the smaller 9- and 16-port x210 models, shown in diagram 2. Whisper quiet with a fanless design, they can be placed in work areas and on desks without disrupting staff.



the solution : the network x210 Series | 3

Product Specifications

PRODUCT	10/100/1000T (RJ-45) COPPER PORTS	SFP AND 10/100/1000T COMBO PORTS	100/1000X SFP PORTS	TOTAL PORTS	SWITCHING FABRIC	FORWARDING RATE	
AT-x210-9GT	8	-	1	9	24 Gbps	13.4 Mpps	
AT-x210-16GT	14	2	-	16	36 Gbps	23.8 Mpps	
AT-x210-24GT	20	4	-	24	48 Gbps	35.7 Mpps	

Physical Specifications

PRODUCT	HEIGHT	WIDTH	DEPTH	MOUNTING	WEIGHT	
THODOUT				MOONTHA	UNPACKAGED	PACKAGED
AT-x210-9GT	38 mm (1.50 in)	263 mm (10.35 in)	179 mm (7.05 in)	Desktop	1.4 kg (3.09 lb)	
AT-x210-16GT	44 mm (1.73 in)	341 mm (13.42 in)	210 mm (8.27 in)	Desktop	2.0 kg (4.41 lb)	
AT-x210-24GT	44 mm (1.73 in)	440 mm (17.32 in)	210 mm (8.27 in)	Rack-mount	2.7 kg (5.95 lb)	

Performance

- » Up to 8K MAC addresses
- » 256 VLANs (4K VLAN IDs)
- » 128MB DDR SDRAM
- » 64MB flash memory
- » Packet Buffer memory: 512KB
- » Supports 9kB jumbo frames
- » Wirespeed forwarding

Reliability

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

Flexibility and Compatibility

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

Diagnostic Tools

- » Find-Me device locator
- » Ping polling for IPv4 and IPv6
- » Port mirroring
- » TraceRoute for IPv4 and IPv6

IPv6 Features

- » Device management over IPv6 networks with SNMPv6, Telnetv6 and SSHv6
- » NTPv6

Management

- » 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
- » Comprehensive SNMP MIB support for standardsbased device management
- » Built-in text editor
- » Event-based triggers allow user-defined scripts to be executed upon selected system events
- » VLAN creation based on protocol, port or subnet

Quality of Service

- » 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 gueue congestion control
- » Strict priority, weighted round robin or mixed scheduling

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)
- » Loop protection: loop detection and thrash limiting
- » PVST+ compatibility mode
- » RRP snooping
- » STP root guard

Security Features

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

Environmental Specifications

- » Operating temperature range:
- x210-9GT: 0°C to 50°C (32°F to 122°F)

x210-9GT: 0°C to 45°C (32°F to 113°F) with AT-SPLX40 or AT-SPZX80

x210-16GT: 0°C to 40°C (32°F to 104°F)

x210-16GT: 0°C to 35°C (32°F to 95°F) with AT-SPLX40 or AT-SPZX80 or AT-SPFX/2 or

x210-24GT: 0°C to 40°C (32°F to 104°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
- » Certification: UL, cUL, TUV

Restrictions on Hazardous Substances (RoHS) Compliance

- » EU RoHS compliant
- » China RoHS compliant

Country of Origin

» Singapore

Power and Noise Characteristics

RFC 4443 Internet Control Message Protocol (ICMPv6)

RFC 4862 IPv6 Stateless Address Auto-Configuration

IPv6 socket API for source address selection RFC 5095 Deprecation of type 0 routing headers in IPv6

RFC 4291 IPv6 addressing architecture

RFC 4861 Neighbor discovery for IPv6

(SLAAC)

RFC 5014

PRODUCT	AVERAGE POWER CONSUMPTION	MAX POWER CONSUMPTION	AVERAGE HEAT DISSIPATION	MAX HEAT DISSIPATION	NOISE
AT-x210-9GT	8.6W	12W	28.4 BTU/hr	41.7 BTU/hr	Fan-less
AT-x210-16GT	16W	19W	55.9 BTU/hr	64.5 BTU/hr	Fan-less
AT-x210-24GT	25W	28W	85.3 BTU/hr	94.8 BTU/hr	Fan-less

Allical/Mare Plus Operating System	01	uda and Busta sala	Managan		Ovelity of	: Camilaa	
Authentication Pure Operating System SMAPPI, v.c. and v.3 EEE 802.1 Mills Lagor Biscolary Protocol (LLDP) content savice version 54.3 Feb. 2474 Diffsor ynaccolaron for the controled baid retreated Feb. 2474 Diffsor ynaccolaron for the controled baid retreated Feb. 2474 Diffsor ynaccolaron for the controled baid retreated Feb. 2474 Diffsor ynaccolaron for for quasiport information for TCPPI based internets Feb. 2475 Diffsor ynaccolaron for for quasiport information for TCPPI based internets Feb. 2576 Diffsor ynaccolaron for forwarding (AF) Diffsor ynaccolaron for forwarding (AF) Diffsor ynaccolar	Standards and Protocols		Management		Quality of Service		
Authentication	Alliad\Ma	o Blue Operating System					
Autheritication RFC 1321 MDS Missage-Digist algorithm RFC 1321 MDS Missage-Digist algorithm RFC 1321 MDS Missage-Digist algorithm RFC 13221 MDS Missage-Digist algorithm RFC 13221 MDS Missage-Digist algorithm RFC 13221 MDS Missage-Digist algorithm RFC 1323 MDS Missage-Digist algorithm RFC 1323 MDS Missage-Digist algorithm RFC 1323 MDS Missage-Digist algorithm RFC 1324 MDS Missage-Digist algorithm RFC 1324 MDS Missage-Digist algorithm RFC 1324 MDS Missage-Digist algorithm RFC 1325 MDS Missage-Digist algorithm			,		RFG 2211	•	
March Marc	version 5.4.	3		. , ,	DEC 0474		
Fig. 1367 MOS Message Debast algorithm Fig. 1367 Sericals Missagement Protocol (SMMP) Fig. 1367 Concise Missagement Protocol (SMMP) Fig. 1367 Concise Missagement of TOP/IP-based international control marker Fig. 2367 A flow-rate three-color marker Fig. 2368 A flow-rate three-color marker Fig. 2369 Fig. 2369 A flow-rate three-color marker Fig. 2369 Fig. 2369 A flow-rate three-color marker Fig. 2369 Students / Missage flow flow flow flow flow flow flow flow	Authentic	ation	KFC 1155				
PRC 1287			DEC 1157				
Encryption FIPS 180 Secure Hash standard GRM-1) BFC 1215 Secure Hash standard GRM-1) BFC 1215 Connection for defining traps for use with the SMAP Secure Hash standard GRM-1 Sec						• , ,	
Pincy patient	111 0 1020	ii authentication using keyeu MD3				0	
FIPS 186 Did largerturer standard (RSA) PiPS 46-3 Data Encryption Standard (DES and 30ES) PiPC 1275 SMMP MLX protocol and MIB EEE 80.21 Multiple Spanning Tree Protocol (RSTP) EEE 80.23 Multiple	Encryptic	nn .	RFG 1213				
First Firs			DE0 4045		RFU 3246	DiffServ Expedited Forwarding (EF)	
Ethernet		, ,	KFU 1215		Resilienc	v Features	
Ethernet EFE 802_1 Multiple Spanning Tree Protocol (MSTP) EFE 802_1 Logical Link Control (LLC) EFE 802_2 Logical Link Control (LLC) EFE 802_3 Ethernet EFE 802_3		0 0 ,	DE0 4007				
EER 802.1 Kull-is aggregation (static and LACP) FEE 802.2 Logical Link Control (LLC) FEE 802.2 Logical Link Control (LLC) FEE 802.2 Logical Link Control (LLC) FEE 802.3 Sink Control (RSTP) FEE 802.3 Sink Control (LLC) FEE 802.3 Sink Control	1110400	Data Energytion otandard (DEO and ODEO)		•		ů .	
EEE 80.2 Light Land Land Chron (LLC)	Ethernet						
EEE 80.2 Logical Link Control (LLC)		XLink angregation (static and LACP)		ě .	ILLL 002.1W	napid Spanning free Frotocol (norr)	
IEEE 802.3 bit flower that the protocol (P) IEEE 802.3 bit flower that the protocol (ICMP) IEEE 802.3 bit flower that the p		,		· ·	Security F	eatures	
February		, ,		· ·	-		
EEE 802.3u TOBASE X Static and dynamic link aggregation FPC 2576 CoMunication FPC 2579 Textual conventions for SMIv2 IEEE 802.3x TOBASE X Flow control - full duplex operation FPC 2580 Fex 2580 Common es tatements for SMIv2 IEEE 802.3x TOBASE X Flow control - full duplex operation FPC 2580 Common es tatements for SMIv2 IEEE 802.3x TOBASE X Flow control - full duplex operation FPC 2580 Common es tatements for SMIv2 IEEE 802.3x TOBASE X Flow control - full duplex operation FPC 2680 Common es tatements for SMIv2 IEEE 802.1x Dort-based network access control FPC 2546 FPC 2781 Common es tatements for SMIv2 IEEE 802.1x Dort-based network access control FPC 2546 FPC 2547 Common es tatements for SMIv2 IEEE 802.1x Dort-based network access control FPC 2546 FPC 2547 Common es tatements for SMIv2 IEEE 802.1x Dort-based network access control FPC 2546 FPC 2547 Common es tatements for SMIv2 IEEE 802.1x Dort-based network access control FPC 2546 FPC 2547 Common es tatements for SMIv2 IEEE 802.1x Dort-based network access control FPC 2546 FPC 2547 Common es tatements for SMIv2 IEEE 802.1x Turnly supplicant authentication Total Common es tatements for SMIv2 IEEE 802.1x Turnly supplicant authentication Total Common es tatements for SMIv2 IEEE 802.1x Turnly supplicant authentication IEEE 802.1x Turnly supplicant authent				•		ŭ	
EREB 802.3 x Flow control - full duplex operation RFC 2579 Tester 802.3 x Flow control - full duplex operation RFC 2579 RFC 2570 RFC 2570 RFC 2570 RFC 2571 RFC 2572 RFC 2571 RFC 2572 RF			RFC 2578	9			
IEEE 802.3x Flow control -full duplex operation RFC 2580 Conformance statements for SMIW2 IEEE 802.3x 1000BASE-X RFC 2670 Definitions of managed objects for bridges with raffic dasses, multicast filtering and VLAN RFC 2546 Tas protocol V1.0 RFC 2741 Agent extensions RFC 2746 Tas protocol V1.0 RFC 2746 Tas protocol V1.0 RFC 2746 RFC 2746 RFC 2746 RFC 2746 RFC 2746 RFC 2747 Agent extensibility (AgentX) protocol RFC 2746 RFC				,	ILLL 002.1X		
IEEE 802.3z 1000BASE-X				Textual conventions for SMIv2	IEEE 902 1V	,	
IPV4 Features First Design Fir		·	RFC 2580	Conformance statements for SMIv2			
PV4 Features	IEEE 002.32	1000BASE-X	RFC 2674	Definitions of managed objects for bridges with		•	
RFC 791 Internet Protocol (IP) RFC 792 Internet Control Message Protocol (ICMP) RFC 792 Internet Control Message Protocol (ICMP) RFC 826 Address Resolution Protocol (ARP) RFC 826 Address Resolution Protocol (ARP) RFC 827 Address Resolution Protocol (ARP) RFC 828 Address Resolution Protocol (ARP) RFC 829 Standard for the transmission of IP datagrams over Ethernet networks over Ethernet activations in the protocol p	IDv4 Foot	TIMO O		traffic classes, multicast filtering and VLAN		•	
RFC 792 Internet Control Message Protocol (ICMP) RFC 826 Address Resolution Protocol (ARP) RFC 826 Address Resolution Protocol (ARP) RFC 827 REVIEW R				extensions			
RFC 826 Address Resolution Protocol (ARP) RFC 847 Standard for the transmission of IP datagrams over Ethernet networks RFC 919 Broadcasting Internet datagrams RFC 920 Broadcasting Internet datagrams in the presence of Subnets RFC 931 Subnetwork addressing scheme RFC 932 Subnetwork addressing scheme RFC 932 Subnetwork addressing scheme RFC 933 Subnetwork addressing scheme RFC 946 Internet standard subnetting procedure RFC 947 Subnetwork addressing of IP datagrams over IEEE 802 networks RFC 948 RFC 949 Section for IP datagrams over IEEE 802 networks RFC 9411 SNMP applications RFC 9412 Subnetwork addressing scheme RFC 9413 SNMP applications RFC 9414 Subnetwork addressing scheme RFC 9415 SNMP Applications SNMP RFC 9415 SNMP applications SNMP RFC 9415 SNMP applications SNMP RFC 9415 SNMP applications RFC 9415 SNMP Applications RFC 9415 SNMP Applications RFC 9415 SNMP RFC 9415 SNMP Applications RFC 9415 SNMP RFC 9415 S		, ,	RFC 2741	Agent extensibility (AgentX) protocol		, ,	
RFC 894 Standard for the transmission of IP datagrams over Ethernet networks vere thement networks and standard grams over Ethernet networks and standard grams over Ethernet networks and standard grams are produced in the		. ,	RFC 2819	RMON MIB (groups 1,2,3 and 9)			
over Ethernet networks RFC 919 Broadcasting Internet datagrams RFC 919 Broadcasting Internet datagrams in the presence of subnets RFC 922 Subnetwork addressing scheme RFC 932 Subnetwork addressing scheme RFC 932 Subnetwork addressing scheme RFC 934 Subnetwork addressing scheme RFC 935 Subnetwork addressing scheme RFC 936 Subnetwork addressing scheme RFC 937 Subnetwork addressing scheme RFC 938 Subnetwork addressing scheme RFC 930 Simple procedure RFC 930 Simple RFC 930 Trivial File Transfer Protocol (TFTP) RFC 1910 Internet host requirements SNMP SNMP RFC 1930 Simple RFC 930 Simple RFC 9310 Simple RFC 930 Simple RFC 9310 Simple National Broadcasting in the subnetwork of the protocol operations for the RFC 9310 Simple National Broadcasting in the subnetwork of the protocol (SMTP) RFC 1931 Dictoration RFC 930 Simple RFC 9310 Simple National Broadcasting National Broadcasting National Broadcasting National Protocol (SMTP) RFC 930 Simple National Broadcasting National Protocol (SMTP) RFC 930 Simple National Broadcasting National Protocol (SMTP) RFC 930 Simple National Protocol (SMTP) RF		` ,	RFC 2863				
FFC 912 Broadcasting Internet datagrams FFC 913 Broadcasting Internet datagrams in the presence of subnets FFC 922 Broadcasting Internet datagrams in the presence of subnets FFC 932 Subnetwork addressing scheme FFC 930 Internet standard subnetting procedure FFC 930 Internet standard subnetting procedure FFC 940 Standard for the transmission of IP datagrams over IEEE 802 networks FFC 9412 Subnetwork addressing scheme FFC 9413 SNMP applications FFC 1042 Standard for the transmission of IP datagrams over IEEE 802 networks FFC 9414 User-based Security Model (USM) for SNMPV SNMP Presented the suppress go ahead option FFC 1041 User-based Security Model (USM) for SNMPV SNMP Presented Standard for the transmission of IP datagrams over IEEE 802 networks FFC 1041 User-based Security Model (USM) for SNMPV SNMP Presented Standard for the transmission of IP datagrams over IEEE 802 networks FFC 1041 Viscovery FFC 1122 Internet host requirements FFC 1124 Internet host requirements FFC 1125 Internet host requirements FFC 1126 ICMP router discovery messages FFC 1518 An architecture for IP address allocation with CIDR FFC 1519 Classless Inter-Domain Routing (CIDR) FFC 1510 Classless Inter-Domain Routing (CIDR) FFC 1510 Requirements for IPv4 routers FFC 1510 Requ	RFC 894	•	RFC 3164	Syslog protocol			
BFC 919 Broadcasting internet datagrams FFC 932 Subnetwork addressing scheme FFC 932 Subnetwork addressing scheme FFC 9341 Internet strandard subnetting procedure FFC 935 Subnetwork addressing scheme FFC 9412 Standard for the transmission of IP datagrams over IEEE 802 networks FFC 1042 Standard for the transmission of IP datagrams over IEEE 802 networks FFC 1045 Standard for the transmission of IP datagrams over IEEE 802 networks FFC 1046 Internet standard subnetting procedure FFC 1047 Computing the Internet checksum FFC 3413 SNMP applications FFC 1041 Computing the Internet checksum FFC 1341 User-based Security Model (USM) for SNMPV3 FFC 1051 Internet host requirements FFC 1191 Path MTU discovery FFC 1256 ICMP router discovery messages FFC 1356 ICMP router discovery messages FFC 1350 Classless Inter-Domain Routing (CIDR) FFC 1351 Classless Inter-Domain Routing (CIDR) FFC 1363 FFC 1363 Eternet 2418 FFC 1364 Requirements for IPv4 routers FFC 1918 IP addressing FFC 4318 Definitions of managed objects for the FFC 2450 Path MTU discovery for IPv6 FFC 2450 Definitions of managed objects for remote ping, received and lookup operations FFC 2450 DNS extensions to support IPv6 FFC 2450 Internet processing and dispatching for the SMMP FFC 3450 SMMP applications FFC 3451 SMMP applications FFC 3451 SMMP applications FFC 3451 DNS extensions to support IPv6 FFC 2450 DNS extensions to support IPv6			RFC 3176		RFC 4254	Secure Shell (SSHv2) connection protocol	
BFC 922 Broadcasting internet datagrams in the presence of subhets RFC 932 Subnetwork addressing scheme RFC 934 Subnetwork addressing scheme RFC 3412 Message processing and dispatching for the SMMP RFC 855 Telnet option specifications RFC 1042 Standard for the transmission of IP datagrams over IEEE 802 networks RFC 1071 Computing the Internet checksum RFC 3414 User-based Security Model (USM) for SMMPv3 RFC 1071 Computing the Internet checksum RFC 3415 View-based Access Control Model (VACM) for Internet host requirements RFC 1122 Internet host requirements RFC 1124 Internet host requirements RFC 3415 View-based Access Control Model (VACM) for SMMP RFC 1256 ICMP router discovery messages RFC 3416 Version 2 of the protocol operations for the SMMP RFC 2418 Internet for IP address allocation with CIDR RFC 1812 Requirements for IPv4 routers RFC 3417 Transport mappings for the SMMP RFC 2554 SMTP service extension for authentication RFC 1812 Requirements for IPv4 routers RFC 1812 Requirements for IPv4 routers RFC 1818 Path MTU discovery for IPv6 RFC 1819 IP addressing RFC 4318 Definitions of managed objects for bridges RFC 1819 IPv6 specification RFC 4318 Definitions of managed objects for bridges RFC 2464 Transmission of IPv6 packets over Ethernet networks RFC 4310 IPv6 specification RFC 3417 Internet host requirements for IPv6 RFC 4318 Definitions of managed objects for bridges with a pethal MUI discovery for IPv6 RFC 2460 IPv6 specification RFC 4318 Definitions of managed objects for bridges with a pethal MUI discovery for IPv6 RFC 3439 Definitions of managed objects for bridges with a pethal MUI discovery for IPv6 RFC 3459 DNS extensions to support IPv6 RFC 3450 IGMP snooping Multicast Support Multicast Su				•	Camilana		
presence of subnets RFC 932 Subnetwork addressing scheme RFC 935 Internet standard subnetting procedure RFC 1042 Standard for the transmission of IP datagrams over IEEE 802 networks RFC 3413 SMMP applications RFC 1071 Computing the Internet checksum RFC 3414 User-based Security Model (USM) for SNMPy3 RFC 1071 Computing the Internet checksum RFC 3415 SNMP applications RFC 1071 Computing the Internet checksum RFC 3414 User-based Security Model (USM) for SNMPy3 RFC 1072 Internet host requirements RFC 1191 Path MTU discovery RFC 1256 ICMP router discovery messages RFC 3416 Version 2 of the protocol operations for the SNMP RFC 3417 Transport mappings for the SNMP RFC 3418 NIB for SNMP RFC 3418 RFC 3418 IP addressing RFC 1310 DHCPv4 (server, relay and client) RFC 1918 Path MTU discovery RFC 1619 Classless Inter-Domain Routing (CIDR) RFC 1718 Path Sequirements for IPv4 routers RFC 3418 RFC 3418 Definitions of managed objects for the Ethernet-like interface types RFC 1918 Path MTU discovery for IPv6 RFC 4318 Definitions of managed objects for bridges RFC 4320 IPv6 specification RFC 2464 Transmission of IPv6 packets over Ethernet RFC 3418 Definitions of managed objects for remote ping, RFC 3418 Definitions of managed objects for remote ping, RFC 3414 Definitions of managed objects for remote ping, RFC 3415 Definitions of managed objects for remote ping, RFC 3416 Definitions of managed objects for remote ping, RFC 3417 Usual LAN (VLAN) bridges RFC 3418 Definitions of managed objects for remote ping, RFC 3418 Definitions of managed objects for remote ping, RFC 3418 Definitions of managed objects for remote ping, RFC 3418 Definitions of managed objects for remote ping, RFC 3418 Definitions of managed objects for remote ping, RFC 3418 Definitions of managed objects for remote ping, RFC 3418 Definitions of managed objects for remote ping, RFC 3418 Definitions of managed objects for remote ping, RFC 3418 Definitions of managed objects for remote ping, RFC 3418 Definitions of managed objects for remote ping, RFC 3418 Definitio	RFC 922		RFC 3411			Talant austral annification	
Increst standard subnetting procedure RFC 932 Internet standard subnetting procedure RFC 9412 Standard for the transmission of IP datagrams over IEEE 802 networks RFC 1071 Computing the Internet checksum RFC 3413 User-based Security Model (USM) for SNMPV RFC 1172 Internet host requirements RFC 3415 View-based Access Control Model (VACM) for SNMP RFC 1191 Path MTU discovery RFC 1256 ICMP router discovery messages RFC 3416 Version 2 of the protocol operations for the CIDR RFC 1519 Classless Inter-Domain Routing (CIDR) RFC 1510 Requirements for IPv4 routers RFC 1911 Path MTU discovery 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 2131 DHCPv4 (server, relay and client) SNMP RFC 2421 DHCPv4 (server, relay and client) RFC 3416 Version 2 of the protocol operations for the SNMP RFC 3417 Transport mappings for the SNMP RFC 2421 DHCPv4 (server, relay and client) RFC 3418 RFC 3418 MIB for SNMP RFC 3418 RFC 3418 Definitions of managed objects for the Ethernet-like interface types RFC 1921 Simple Mail Transfer Protocol (SMTP) RFC 2421 Simple Mail Transfer Protocol (SMTP) RFC 3430 Simple Network Time Protocol (SMTP) RFC 3431 Definitions of managed objects for bridges RFC 3448 Default address selection for IPv6 RFC 3450 Definitions of managed objects for remote ping, reworks RFC 3448 Default address selection for IPv6 RFC 3450 DNS extensions to support IPv6 IGMP query solicitation IGMP snooping Multicast Support IGMP snooping Multicast Support Voice over IP ILDP-MED ANSI/TIA-1057 Voice VLAN		•		ů,			
RFC 1042 Standard for the transmission of IP datagrams over IEEE 802 networks RFC 1071 Computing the Internet checksum RFC 3413 SMMP applications RFC 3415 SMMP applications RFC 3415 SMMP applications RFC 3415 SMMP applications RFC 3416 View-based Security Model (USM) for SNMPV3 RFC 1122 Internet host requirements RFC 1121 Internet host requirements RFC 1122 Internet host requirements RFC 1121 Internet host requirements RFC 1122 Internet host requirements RFC 1123 Internet host requirements RFC 1124 Internet host requirements RFC 1125 ICMP router discovery RFC 1256 ICMP router discovery messages RFC 1126 ICMP router discovery messages RFC 1127 An architecture for IP address allocation with CIDR RFC 1128 An architecture for IP address allocation with CIDR RFC 1129 Classless Inter-Domain Routing (CIDR) RFC 3418 MIB for SNMP RFC 3418 RFC 3418 MIB for SNMP RFC 3418 RFC 3419 IP addressing RFC 3419 IP addressing RFC 3410 Internet message format RFC 3			RFC 3412	•		·	
Standard for the transmission of IP datagrams over IEEE 802 networks RFC 1071 RFC 1071 RFC 1071 RFC 1071 RFC 1122 Internet host requirements RFC 3415 RFC 3415 RFC 3415 RFC 3415 RFC 3416 RFC 3416 RFC 3416 RFC 3416 RFC 3417 RFC 3416 RFC 3418 RFC 3416 RFC 3417 RFC 3418 RFC 3418 RFC 3418 RFC 3419 RFC 3416 RFC 3416 RFC 3417 RFC 3417 RFC 3418 RFC 3418 RFC 3418 RFC 3418 RFC 3418 RFC 3418 RFC 3419 RFC 3419 RFC 3419 RFC 3419 RFC 3419 RFC 3410 RFC 3410 RFC 3416 RFC 3416 RFC 3416 RFC 3416 RFC 3416 RFC 3416 RFC 3417 RFC 3418 RFC 3418		• ,	100112			•	
Over IEEE 802 networks RFC 3414 User-based Security Model (USM) for SNMPV3 RFC 1350 Trivial Firansfer Protocol (FFTP) RFC 1122 Internet host requirements RFC 3415 View-based Access Control Model (VACM) for SNMP RFC 1350 Trivial Firansfer Protocol (FFTP) RFC 1256 IcMP router discovery messages RFC 1319 Path MTU discovery messages RFC 1518 An architecture for IP address allocation with CIDR RFC 1519 Classless Inter-Domain Routing (CIDR) RFC 1519 Classless Inter-Domain Routing (CIDR) RFC 1812 Requirements for IPv4 routers RFC 1918 IP addressing RFC 3636 Effectives RFC 3636 IEEE 802.3 MAU MIB RFC 3636 IEEE 802.3 MAU MIB RFC 2460 IPv6 specification RFC 2460 IPv6 specification RFC 2464 Transmission of IPv6 RFC 2484 Default address selection for IPv6 RFC 3596 DNS extensions to support IPv6 RFC 3596 DNS extensions to support IPv6 RFC 3491 Unique local IPv6 scoped address architecture IGMP snooping IGMP snooping RFC 3414 User-based Security Model (USM) for SNMP/ RFC 3415 View-based Access Control Model (VACM) for SNMP RFC 1935 SMTP service extension RFC 1981 Path MTU discovery messages RFC 3416 Network Time Protocol (SMTP) RFC 3418 Definitions of managed objects for the Ethernet-like interface types RFC 3418 Definitions of managed objects for bridges RFC 3418 Definitions of managed objects for bridges RFC 3418 Definitions of managed objects for bridges RFC 3418 Definitions of managed objects for remote ping, traceroute and lookup operations RFC 3420 VLAN taggling Nulticast Support RFC 3430 Definitions of managed objects for remote ping, traceroute and lookup operations RFC 3431 Definitions of managed objects for remote ping, traceroute and lookup operations RFC 3434 Default address selection for IPv6 RFC 3434 Default address selection for IPv6 RFC 3434 Default address architecture RFC 3434 Default address architecture RFC 3434 Default address architecture RFC 3435 Definitions of managed objects for remote ping, traceroute and lookup operations RFC 3434 Default address selection for IPv6 RFC 3434 Default address selecti	RFC 1042	•	BEC 3413				
RFC 1071 Computing the Internet checksum RFC 1122 Internet host requirements RFC 1125 Internet host requirements RFC 1126 Internet host requirements RFC 1256 ICMP router discovery messages RFC 1256 ICMP router discovery messages RFC 1518 An architecture for IP address allocation with CIDR RFC 1519 Classless Inter-Domain Routing (CIDR) RFC 3418 MIB for SMMP RFC 2821 Simple Mail Transfer Protocol (SMTP) RFC 1812 Requirements for IPv4 routers RFC 1918 IP addressing RFC 1918 Path MTU discovery for IPv6 RFC 2810 Definitions of managed objects for bridges RFC 1918 Path MTU discovery for IPv6 RFC 2460 IPv6 specification RFC 2464 Transmission of IPv6 packets over Ethernet networks RFC 3484 Default address selection for IPv6 RFC 3484 Default address selection for IPv6 RFC 3495 INdicast Support IPv6 scoped address architecture RFC 3497 Ilpique local IPv6 scoped address architecture RFC 3497 Ilpique local IPv6 scoped address architecture RFC 3497 Ilpique local IPv6 scoped address architecture RFC 1918 Ilpique local IPv6 scoped address architecture RFC 3497 Ilpique local IPv6 unicast addresses RFC 3497 Ilpique local IPv6 unicast addresses RFC 3498 Ilpique local IPv6 unicast addresses RFC 3497 Ilpique local IPv6 unicast addresses						31 1	
RFC 1121 Internet nost requirements RFC 1191 Path MTU discovery RFC 1256 ICMP router discovery messages RFC 3416 Version 2 of the protocol operations for the SNMP RFC 2413 DHCPv4 (server, relay and client) SNMP RFC 2414 DHCPv4 (server, relay and client) SNMP RFC 2415 DHCP options and BootP vendor extensions RFC 1518 An architecture for IP address allocation with CIDR RFC 1519 Classless Inter-Domain Routing (CIDR) RFC 1812 Requirements for IPv4 routers RFC 1812 Requirements for IPv4 routers RFC 1918 IP addressing RFC 3418 MIB for SNMP RFC 3636 IEEE 802.3 MAU MIB RFC 3636 IEEE 802.3 MAU MIB RFC 1918 Path MTU discovery for IPv6 RFC 2418 Definitions of managed objects for bridges RFC 1910 IPv6 specification RFC 2460 IPv6 specification RFC 2464 Transmission of IPv6 packets over Ethernet networks RFC 3484 Default address selection for IPv6 RFC 3485 DFS extensions to support IPv6 RFC 3486 DNS extensions to support IPv6 RFC 3497 Illique local IPv6 scoped address architecture IGMP query solicitation RFC 3498 Illique local IPv6 injects addresses Internet notice of the protocol operations of the protocol operation operation operations of the protocol operation operation operations oper						, ,	
RFC 1916 Fath MTU discovery messages RFC 3416 Version 2 of the protocol operations for the SNMP RFC 2131 DHCP/4 (server, relay and client) RFC 1518 An architecture for IP address allocation with CIDR RFC 3418 MIB for SNMP RFC 2554 SMTP service extension for authentication RFC 1519 Classless Inter-Domain Routing (CIDR) RFC 3418 MIB for SNMP RFC 2554 SMTP service extension for authentication RFC 1812 Requirements for IPv4 routers RFC 3636 Definitions of managed objects for the Ethernet-like interface types RFC 2822 Internet message format RFC 1918 IP addressing RFC 3636 IEEE 802.3 MAU MIB RFC 5905 Network Time Protocol (SNTP) version 4 RFC 1918 Path MTU discovery for IPv6 RFC 4318 Definitions of managed objects for bridges RFC 2460 IPv6 specification RSTP IEEE 802.10 Virtual LAN (VLAN) bridges RFC 2464 Transmission of IPv6 packets over Ethernet networks RFC 4560 Definitions of managed objects for remote ping, traceroute and lookup operations IEEE 802.3 ac VLAN tagging RFC 3484 Default address selection for IPv6 RFC 3493 IEEE 802.3 ac VLAN tagging RFC 3493 Unique local IPv6 upicast addresses IGMP snooping IGMP snooping Voice VLAN RFC 3493 Unique local IPv6 upicast addresses IGMP snooping IGMP snooping Voice VLAN RFC 3491 Internet message format RFC 4560 RFC 4318 RFC 4318 Internet message format RFC 4330 Simple Mail Transfer Protocol (SMTP) RFC 2822 Internet message format RFC 4330 Simple Network Time Protocol (SMTP) version 4 RFC 5905 Network Time Protocol (NTP) version 4 RFC 2825 Internet message format RFC 4330 Simple Network Time Protocol (SMTP) RFC 4330 Simple Network Time Protocol (NTP) version 4 RFC 4318 Definitions of managed objects for bridges with RFC 4330 RFC 4330 Simple Network Time Protocol (NTP) version 4 RFC 430 RFC 4330 Simple Network Time Protocol (NTP) version 4 RFC 4330 RFC 4330 RFC 4330 RFC 4330 RFC 4330 RFC 4330	RFC 1122	Internet host requirements	111 0 0 4 10	, ,			
RFC 1256 ICMP router discovery messages RFC 1518 An architecture for IP address allocation with CIDR RFC 1519 Classless Inter-Domain Routing (CIDR) RFC 1519 Classless Inter-Domain Routing (CIDR) RFC 1812 Requirements for IPv4 routers RFC 1918 IP addressing RFC 3635 Etter 82.3 MAU MIB RFC 3636 IEEE 802.3 MAU MIB RFC 4318 Definitions of managed objects for the Ethernet-like interface types RFC 1981 Path MTU discovery for IPv6 RFC 4318 Definitions of managed objects for bridges RFC 1981 Path MTU discovery for IPv6 RFC 2460 IPv6 specification RFC 2461 Transmission of IPv6 packets over Ethernet networks RFC 3484 Default address selection for IPv6 RFC 3480 Default address selection for IPv6 RFC 3481 Default address architecture RFC 4007 IPv6 scoped address architecture		Path MTU discovery	BEC 3/16				
RFC 1518 An architecture for IP address allocation with CIDR RFC 3417 Transport mappings for the SNMP RFC 3418 MIB for SNMP RFC 3418 MIB for SNMP RFC 3418 RFC 3418 MIB for SNMP RFC 3430 Simple Mail Transfer Protocol (SMTP) version 4 RFC 3430 Simple Metwork Time Protocol (SNTP) version 4 RFC 3430 Simple Network Time Protocol (SNTP) version 4 RFC 3430 Simple Network Time Protocol (SNTP) version 4 RFC 3430 Network Time Protocol (NTP) version 4 RFC 3430 Simple Network Time Protocol (SNTP) version 4 RFC 3430 Simple Network Time Protocol (SNTP) version 4 RFC 3430 Simple Network Time Protocol (SNTP) version 4 RFC 3430 Simple Network Time Protocol (SNTP) version 4 RFC 3430 Simple Network Time Protocol (SNTP) version 4 RFC 3430 Simple Network Time Protocol (SNTP) version 4 RFC 3430 Simple Network Time Protocol (SNTP) version 4 RFC 3430 Simple Network Time Protocol (SNTP) version 4 RFC 3430 Simple Network Time Protocol (SNTP) version 4 RFC 3430 Simple Network Time Protocol (SNTP) version 4 RFC 3430 Simple Network Time Protocol (SNTP) version 4 RFC 3430 Simple Network Time Protocol (SNTP) version 4 RFC 3430 Simple Network Time Protocol (SNTP) version 4 RFC 3430 Simple Network Time Protocol (SNTP) version 4 RFC 3440 Definitions of managed objects for bridges RFC 4330 VLAN Support IEEE 802.10 VILAN (VLAN) bridges IEEE 802.10 VILAN classification by protocol and port traceroute and lookup operations IEEE 802.3 VLAN tagging Woice over IP LIDP-MED ANSI/TIA-1057 Voice VLAN	RFC 1256	ICMP router discovery messages	111 0 3410	·			
RFC 1519 Classless Inter-Domain Routing (CIDR) RFC 1812 Requirements for IPv4 routers RFC 1918 IP addressing RFC 3635 Definitions of managed objects for the Ethernet-like interface types RFC 1918 IP addressing RFC 3636 IEEE 802.3 MAU MIB RFC 3636 IEEE 802.3 MAU MIB RFC 4330 Simple Network Time Protocol (SNTP) version 4 RFC 4330 Simple Network Time Protocol (SNTP) version 4 RFC 1918 RFC 4330 Simple Network Time Protocol (SNTP) version 4 RFC 4330 Simple Network Time Protocol (NTP) version 4 RFC 4330 Simple Network Time Protocol	RFC 1518	An architecture for IP address allocation with	DEC 2/17			•	
RFC 1812 Requirements for IPv4 routers RFC 1918 IP addressing RFC 3635 Definitions of managed objects for the Ethernet-like interface types RFC 1918 IP addressing RFC 3636 IEEE 802.3 MAU MIB RFC 3636 IEEE 802.3 MAU MIB RFC 3636 IEEE 802.3 MAU MIB RFC 3637 Definitions of managed objects for bridges RFC 1981 Path MTU discovery for IPv6 RFC 2460 IPv6 specification RFC 2460 Transmission of IPv6 packets over Ethernet networks RFC 3484 Default address selection for IPv6 RFC 3484 Default address selection for IPv6 RFC 3596 DNS extensions to support IPv6 RFC 3596 DNS extensions to support IPv6 RFC 4007 IPv6 scoped address architecture RFC 4007 IPv6 scoped address architecture RFC 4007 IPv6 support IPv6 IPv6 scoped address architecture IGMP query solicitation IGMP snooping IEEE 802.1 Victual LAN (VLAN) bridges IEEE 802.1 VLAN tagging Voice over IP LLDP-MED ANSI/TIA-1057 Voice VLAN Internet message format RFC 2822 Internet shring the internet message format RFC 2828 Internet shring the internet message format RFC 2828 Internet shring the internet message format RFC 2828 Internet shrin		CIDR					
RFC 1918 IP addressing	RFC 1519	Classless Inter-Domain Routing (CIDR)					
Paddressing	RFC 1812	Requirements for IPv4 routers	RFU 3033			ů .	
PV6 Features RFC 4188 Definitions of managed objects for bridges RFC 9905 NetWork Time Production (NTF) Version 4	RFC 1918	IP addressing	DE0 0000	31		Simple Network Time Protocol (SNTP) version 4	
RFC 1981 Path MTU discovery for IPv6 RFC 4318 Definitions of managed objects for bridges with RFC 2460 IPv6 specification RFC 2460 Transmission of IPv6 packets over Ethernet networks RFC 3484 Default address selection for IPv6 Description RFC 2460 Definitions of managed objects for remote ping, traceroute and lookup operations RFC 3484 Default address selection for IPv6 RFC 3596 DNS extensions to support IPv6 IPv6 scoped address architecture IGMP query solicitation IGMP snooping RFC 4318 Definitions of managed objects for remote ping, traceroute and lookup operations RFC 3484 Default address selection for IPv6 RFC 4007 IPv6 scoped address architecture IGMP query solicitation IDMP snooping VLAN Support IEEE 802.10 Virtual LAN (VLAN) bridges IEEE 802.12 VLAN classification by protocol and port IEEE 802.3ac VLAN tagging Voice over IP LLDP-MED ANSI/TIA-1057 Voice VLAN Voice VLAN					RFC 5905	Network Time Protocol (NTP) version 4	
RFC 2460 IPv6 specification IPv6 specification IPv6 specification IPv6 packets over Ethernet networks IEEE 802.10 Virtual LAN (VLAN) bridges RFC 3484 Default address selection for IPv6 RFC 3596 DNS extensions to support IPv6 RFC 4007 IPv6 scoped address architecture IGMP query solicitation IGMP snooping RFC 4560 Definitions of managed objects for remote ping, traceroute and lookup operations IEEE 802.1v VLAN classification by protocol and port IEEE 802.3ac VLAN tagging Wulticast Support Voice over IP LLDP-MED ANSI/TIA-1057 Voice VLAN							
RFC 2464 Transmission of IPv6 packets over Ethernet networks RFC 3484 Definitions of managed objects for remote ping, networks RFC 3484 Default address selection for IPv6 RFC 3596 DNS extensions to support IPv6 RFC 4007 IPv6 scoped address architecture RFC 4560 Definitions of managed objects for remote ping, traceroute and lookup operations IEEE 802.1v VLAN classification by protocol and port IEEE 802.3ac VLAN tagging Voice over IP IGMP query solicitation IPv6 scoped address architecture RFC 4131 Unique local IPv6 unjects addresses IGMP snooping Voice VLAN		,	RFC 4318			•	
RFC 3484 Default address selection for IPv6 RFC 3596 DNS extensions to support IPv6 RFC 4007 IPv6 scoped address architecture IGMP query solicitation IGMP snooping Voice VLAN IEEE 802.3ac VLAN tagging Voice over IP LLDP-MED ANSI/TIA-1057 Voice VLAN		•	DEC 4500			, , ,	
RFC 3484 Default address selection for IPv6 RFC 3596 DNS extensions to support IPv6 IGMP query solicitation LLDP-MED ANSI/TIA-1057 RFC 4007 IPv6 scoped address architecture IGMP snooping Voice VLAN	RFC 2464	Transmission of IPv6 packets over Ethernet	KFC 4560			, · · · · · · · · · · · · · · · · · · ·	
RFC 3596 DNS extensions to support IPv6 Multicast Support RFC 4007 IPv6 scoped address architecture IGMP query solicitation LLDP-MED ANSI/TIA-1057 RFC 4131 Unique local IPv6 unicast addresses IGMP snooping Voice VLAN		networks		traceroute and lookup operations	IEEE 802.3a	c VLAN tagging	
RFC 4007 IPv6 scoped address architecture IGMP query solicitation LLDP-MED ANSI/TIA-1057 RFC 4103 Unique local IPv6 unjects addresses IGMP snooping Voice VLAN	RFC 3484	Default address selection for IPv6	B. 4				
RFC 4193 Unique local IPv6 unicast addresses IGMP snooping Voice VLAN	RFC 3596	DNS extensions to support IPv6		• •			
RFC 4193 Unique local IPv6 unicast addresses IGMP snooping Voice VLAN	RFC 4007	IPv6 scoped address architecture				ANSI/ ITA-1057	
	RFC 4193				Voice VLAN		

the solution: the network ×210 Series | 5

MLD snooping (v1 and v2)

×210 Series | Enterprise Edge Switches









Ordering Information

AT-x210-9GT-xx

L2+ switch with 8 x 10/100/1000T ports and one SFP port

AT-RKMT-J05

Rack mount kit for x210-9GT

AT-x210-16GT-xx

L2+ switch with 14 x 10/100/1000T ports and 2 combo ports (SFP and 10/100/1000T)

AT-x210-24GT-xx

L2+ switch with 20 x 10/100/1000T ports and 4 combo ports (SFP and 10/100/1000T)

SFP Modules

AT-SPFX/2

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

AT-SPFX/I5

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

AT-SPFXBD-LC-13

100BX Bi-Di (1310 nm Tx, 1550 nm Rx) fiber up to 10 km $\,$

AT-SPFXBD-LC-15

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

AT-SPTX

1000T 100 m copper

AT-SPSX

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

AT-SPSX/I

1000SX GbE multi-mode 850 nm fiber up to 550 m industrial temperature

AT-SPEX

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

AT-SPLXI0

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-I3

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

AT-SPBDI0-I4

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

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

Allied Telesis

the solution: the network

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