AT-AR450S

Secure Ethernet Router

AT-AR450S

1 x 10/100B-TX WAN port
1 x 10/100B-TX DMZ port/second WAN port
5 x 10/100B-TX LAN ports
2 x asynchronous RS232 ports

The AT-AR450S is a secure Ethernet router offering versatility, integration, performance and security for medium-sized business and enterprise networks.

The AT-AR450S is a versatile one-rack unit (1RU) security router designed to provide up to Seven 10/100 Fast Ethernet interfaces and 2 asynchronous (RS-232) ports, making it a first class choice for Enterprise Solutions.

One 10/100Mbps WAN (Eth 0) Ethernet Port is offered for a broadband connection to the WAN network, and a 10/100Mbps Ethernet De-Militarised Zone (DMZ) (Eth1) Port provides a second local network publicly accessible from the Internet by authorised users. The DMZ port may also be used as a second Ethernet WAN port. The AT-AR450S Security Router also comes with five Layer-2 switched LAN ports and two dial-up asynchronous ports.

The two asynchronous (RS-232) ports provide 115kbps dial-up for external modems to either backup the dedicated link or provide top-up bandwidth for the network link. Full modem control is supported and both asynchronous ports can be multi-linked with PPP for extra bandwidth.

Security

Allied Telesis' high performance Stateful Inspection Firewall common to all routers and Layer 3 switches provides different levels of security to increase the overall security of business critical information. The AT-AR450S delivers up to 100 Mbps of firewall throughput with the ability to handle over 17,000 simultaneous sessions. With on board hardware encryption the Allied Telesyn AT-AR450S offers DES, 3DES and AES (Advanced Encryption Standard) hardware encryption using up to 256 bit key code. The AR450S has integrated hardware VPN acceleration delivering up to 95 Mbps of 3DES or AES VPN + NAT and Firewall throughput.

AES-Encrypted VPN

The AR450S supports the advanced Encryption Standard (AES). AES is a Federal Information Processing Standard (FIPS 197) that specifies a cryptographic algorithm for use by U.S. Government organizations to protect sensitive, unclassified information. This is the most advanced encryption to open a secure VPN channel.

VPN IPsec

IPsec (Internet Protocol Security) is a set of protocols for security at the network or packet processing layer. Early approaches to security were performed at the application layer of the communications model. IPsec is critical for secure virtual private networks and for remote user access through dial-up connections to private networks. A key advantage of IPsec over earlier implementations is that security (encryption and authentication) can be easily applied without requiring changes to individual user's computers.

There are two choices of security services with IPsec: Authentication Header (AH) and Encapsulating Security Payload (ESP).

AH provides authentication of the sender of data and ESP supports both authentication of the sender and encryption of data as well. The specific service information is inserted into the IP packet payload as a header. Separate key protocols can be selected, such as the ISAKMP protocol.

Key Features

- Stateful Inspection Firewall
- AES, 3DES, DES Hardware based Encryption
- 512 IPSEC/ISAKMP VPN tunnels
- Intrusion Detection and Attack Alert System
- Support Windows XP, 2000 VPN clients using pre-shared keys and also using X509 Certificates
- MD5 / SHA
- L2TP
- PPPoE
- Protection against Denial of Service attacks
- PAP/CHAP user authentication
- RADIUS/TACAS+ look-up
- SMTP and HTTP Proxy
- SSH / SSL
- 802.1X
- 5 Ethernet 10/100Mbps LAN Ports
- 1 Ethernet 10/100Mbps WAN Port
- 1 Ethernet 10/100Mbps DMZ Port
- 2 Async Ports

802.1Q VLAN

The AR450S Security Router is 802.1Q compliant. This enables the user to configure up to 64 VLANs with VLAN Identifier numbers (VID) between one and 4,094.

The 802.1Q specification establishes a standard method for inserting VLAN membership information into Ethernet frames. VLANs can span many switches. VLANs between switches are achieved by inserting a tag with a VID between one and 4,094 into each frame. A VID must be assigned for each VLAN. By assigning the same VID to VLANs on many switches, one or more VLANs (broadcast domains) can be extended across a large network.

The AR450S can firewall between VLANs thus providing protection within the enterprise network from internal attacks.

Firewall

Allied Telesis' state of the art Stateful Inspection Firewall provides a high level of security by providing full application-layer awareness without breaking the client/server model. Allied Telesis' Stateful Inspection Firewall:

- Offers per packet dynamic access control (stateful inspection) for all traffic reaching the firewall
- Protects against a wide range of Denial of Service (DOS) attacks, including Ping of Death, Smurf attacks, port scans, fragment attacks and IP Spoofing
- Sends automatic email alerts to initiate appropriate action

Software QoS

The AlliedWare™ operating system provides advanced Quality of Service (QoS) and traffic shaping features. There are five key QoS features available on the AT-AR450S:

- Bandwidth Metering
- RED Curves
- Mixed Scheduling
- Virtual Bandwidth
- Dynamic Application Recognition (DAR)

Software QoS also supports eight queues per interface. DAR is used to snoop for session setup exchanges and dynamically create classifiers that match the voice and video packets in the session. For more information, see the Allied Telesis Advanced QoS White Paper available on our website.

Triggered Events and Scripts

A trigger sets off an ordered sequence of scripts and router commands to be executed when a certain event occurs, providing a powerful mechanism for automating the execution of router commands in response to specific events. Each trigger may reference multiple scripts and any script can be used by any trigger. Using this feature, the AT-AR450S can, for example, send an email alert to the network manager when trouble occurs, or it can automatically shut down an interface to protect against suspected attacks. The scripting facility enables sequences of commands to be stored in a script and replayed at any time, allowing the AR450S to be easily configured or quickly re-configured. This is useful when developing a complex configuration, making the same configuration change to several different routers, Layer 3 switches or security appliances, or introducing a configuration change that must occur at a particular time. Scripts can be created on a PC and uploaded to the router, or they can be created using the router's own integrated text editor. Scripts can be activated either from the command line or from a trigger.

World Class Operating System and Management Software

AlliedWare™

AlliedWare is Allied Telesis' feature rich operating system (OS) that serves as the foundation for its entire line of Layer 3 routers and switches. Robust and reliable, the AlliedWare OS offers a breadth of functionality for any application. AlliedWare is a common OS that ensures the AT-AR450S Security Router is able to interoperate seamlessly with other Allied Telesis security appliances, fixed function, modular routers and Layer 3 switches, allowing operational investment protection for training, management and monitoring. A standards-based implementation assures full interoperability with all other major network equipment vendors.

AT-AR450S Security Router is shipped "ready to run" with AlliedWare, a comprehensive software suite that includes all the features, management capabilities and performance today's networks demand.

Feature licences give access to a set of progressive features:

- The Advanced Layer 3 Upgrade provides a set of the cutting edge protocols such as IPv6, BGP4 and Load Balancer

Graphical User Interface (GUI)

The AR450S' Graphical User Interface (GUI) allows for swift, pain free configuration and management.

The following major new features are incorporated in the AR450S GUI:

- Easy configuration wizard for connection to the Internet
- PPP over Ethernet configuration and monitoring
- DHCP server configuration and monitoring
- Firewall configuration and monitoring, ability to view events, logs and device status
- IPsec configuration

AlliedView™ (Optional)

AlliedView™ is a Java-based device management solution from Allied Telesis that provides a user-friendly, windows based environment to manage the AT-AR450S Security Router, as well as the complete line-up of Allied Telesis managed devices. Whether managing a large network distributed across multiple sites or a small network with only a handful of nodes, AlliedView™ provides the tools needed to effectively monitor and proactively manage Allied Telesis' intelligent networking products.

Hardware Features

Two 10/100Mbps Ethernet ports.

- Eth0 is a WAN (Wide Area Network) port and
- Eth1 is a DMZ (De-Militarized Zone) port

Five 10/100Mbps Ethernet LAN ports

802.1q tagged VLANs, with support for up to any 64 VLAN IDs of a possible 4094 (LAN ports only)

Automatic MDI/MDI-X crossover with user override via software commands (LAN ports only)

400MHz CPU

64MB SDRAM

16MB of Flash memory enabling storage of 2 software releases

2 x asynchronous (RS-232)

On-board hardware security processor enabling the following advanced encryption function:

- Complete processing of IPsec header and trailer
- Support for 3DES, DES, DES-MAC, AES, SHA-1 and MD-5
- PKI acceleration for Diffie-Hellman, RSA and DSA
- D-H negotiation (with 1024-bit modulus, 180-bit exponent)
- 1024-bit sign and verify RSA and DSA.

MDI/MDI-X

The WAN and DMZ ports are wired as MDI. The 5 LAN ports are wired as MDI-X. The 5 LAN ports also have MDI/MDI-X auto-crossover.

AT-AR450S | Secure Ethernet Router

Main Memory – SDRAM
64MB SDRAM fitted as standard..

FLASH Memory
16MB used for software and configuration data storage.

Universal AC Power Supply
The AR450S has a universal AC input connector and a power switch on its rear panel. The router requires a power input of 100-240 VAC at 50-60Hz.

Real Time Clock (RTC)
The RTC keeps track of current date and time. During times when the system has been powered down, a backup battery supplies power to the RTC.

Software Features
- Secure VPN option
- IPsec (AES, 3DES, DES, DES-MAC, MD5, SHA-1)
- Stateful Inspection Firewall
- Network Address Translation (NAT)
- CLI, PAP and CHAP
- RADIUS, TACACS
- PKI for IKE/IPsec
- SSL
- SecureShell remote management
- UPnP v1.0
- Generic Routing Encapsulation
- Dynamic IP address assignment
- L2TP (Layer 2 Tunneling Protocol)
- DHCP
- PPPoE
- IP packet filtering
- IP multihoming
- Demand IP and IPX
- IPX/SPX spoofing
- Spanning tree on Bridge Ports
- BAP/BACP (Bandwidth Allocation Protocol)
- PPP multilink
- Callback
- IP/IPX and bridge filtering
- Advanced routing protocols OSPF, BGP4, RIP and RIPv2
- Multicast protocols DVMRP, PIM-SM, PIM-DM
- SNMP management v2c and SNMPv3
- GUI
- OSI
- Load Balancer
- IPv6
- IP and IPX routing
- RSVP
- VRRP
- IP Packet prioritization
- STAC data compression (s/w only)

Reliability
System MTBF: 90,000 hours min
PSU MTBF: 150,000 hours min
Base MTBF: 533,000 hours min

Power Characteristics
100-240vAC, 50 - 60Hz

Physical Characteristics
1U rack mount, Depth 190mm, Width 305mm
Weight 1.75 kg (3.75lbs)

Regulatory Approvals
EMC Emissions: EN55022 class A, FCC class A , VCCI class A, AS/NZS CISPR22 class A
Immunity: EN55024
Safety: UL60950, CAN/CSA-C22.2NO. 60950-00, EN60950
Listing: UL, cUL, TUV

Environmental Conditions
Operating temperature range:
0°C – 40°C (32°F – 104°F)
Storage temperature range:
-25°C – 70°C (-13°F – 158°F)
Relative humidity range:
5 – 95% non-condensing

Standards and Protocols
Software Release 2.9.1

BGP-4
RFC 1771 Border Gateway Protocol 4
RFC 1966 BGP Route Reflection
RFC 1997 BGP Communities Attribute
RFC 1998 Multi-home Routing
RFC 2385 Protection of BGP Sessions via the TCP MD5 Signature Option
RFC 2439 BGP Route Flap Damping
RFC 2858 Multiprotocol Extensions for BGP-4
RFC 2918 Route Refresh Capability for BGP-4
RFC 3065 Autonomous System Confederations for BGP
RFC 3392 Capabilities Advertisement with BGP-4

Encryption
RFC 1321 MD5
RFC 2104 HMAC
RFC 2451 The ESP CBC-Mode Cipher Algorithms
FIPS 180 SHA-1
FIPS 186 RSA
FIPS 197 AES
FIPS 46-3 DES
FIPS 46-3 3DES

Ethernet
RFC 894 Ethernet II Encapsulation
IEEE 802.1D MAC Bridges
IEEE 802.1G Remote MAC Bridging
IEEE 802.1Q Virtual LANs
IEEE 802.2 Logical Link Control
IEEE 802.3ac VLAN TAG
IEEE 802.3u 100BASE-T
IEEE 802.3x Full Duplex Operation

General Routing
RFC 768 UDP
RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 903 Reverse ARP
RFC 925 Multi-LAN ARP
RFC 950 Subnetting, ICMP
RFC 1027 Proxy ARP
RFC 1035 DNS
RFC 1055 SLIP
RFC 1122 Internet Host Requirements
RFC 1142 OSI IS-IS Intra-domain Routing Protocol
RFC 1144 Van Jacobson's Compression
RFC 1256 ICMP Router Discovery Messages
RFC 1288 Finger
RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
RFC 1334 PPP Authentication Protocols
RFC 1377 The PPP OSI Network Layer Control Protocol (OSINLCP)
RFC 1378 The PPP AppleTalk Control Protocol (ATCP)
RFC 1518 CIDR
RFC 1519 CIDR
RFC 1542 BootP
RFC 1552 The PPP Internetworking Packet Exchange Control Protocol (IPXCP)
RFC 1570 PPP LCP Extensions
RFC 1582 RIP on Demand Circuits

RFC 1598 PPP in X.25
RFC 1618 PPP over ISDN
RFC 1661 The Point-to-Point Protocol (PPP)
RFC 1701 GRE
RFC 1702 GRE over IPv4
RFC 1762 The PPP DECnet Phase IV Control Protocol (DNCP)
RFC 1812 Router Requirements
RFC 1877 PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
RFC 1918 IP Addressing
RFC 1962 The PPP Compression Control Protocol (CCP)
RFC 1968 The PPP Encryption Control Protocol (ECP)
RFC 1974 PPP Stac LZS Compression Protocol
RFC 1978 PPP Predictor Compression Protocol
RFC 1989 PPP Link Quality Monitoring
RFC 1990 The PPP Multilink Protocol (MP)
RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
RFC 2125 The PPP Bandwidth Allocation Protocol (BAP) / The PPP Bandwidth Allocation Control Protocol (BACP)
RFC 2131 DHCP
RFC 2390 Inverse Address Resolution Protocol
RFC 2516 A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2661 L2TP
RFC 2822 Internet Message Format
RFC 2878 PPP Bridging Control Protocol (BCP)
RFC 3022 Traditional NAT
RFC 3046 DHCP Relay Agent Information Option
RFC 3232 Assigned Numbers
RFC 3993 Subscriber-ID Sub-option for DHCP Relay Agent Option
IPX Router Specification, v1.2, Novell, Inc., Part Number 107-000029-001
AppleTalk
ISO 10589, ISO 10589 Technical Corrigendums 1, 2, 3, ISO Intermediate System-to-Intermediate System
ISO 8473, relevant parts of ISO 8348(X.213), ISO 8343/Add2, ISO 8648, ISO 8648, ISO TR 9577 Open System Interconnection
ISO 9542 End System to Intermediate System Protocol
draft-ietf-ipsec-nat-t-ike-08.txt Negotiation of NAT-Traversal in the IKE
draft-ietf-ipsec-udp-encaps-08.txt UDP Encapsulation of IPsec Packets
http://www.iana.org/assignments/bootp-dhcp-parameters BootP and DHCP parameters

IP Multicasting

RFC 1075 DVMRP
RFC 1112 Host Extensions
RFC 2236 IGMPv2
RFC 2362 PIM-SM
RFC 2715 Interoperability Rules for Multicast Routing Protocols
RFC 3973 PIM-DM
draft-ietf-idmr-dvmrp-v3-9 DVMRP

IPsec

RFC 1829 IPsec algorithm
RFC 1828 IP Authentication using Keyed MD5
RFC 2395 IPsec Compression - LZS
RFC 2401 Security Architecture for IP
RFC 2402 AH - IP Authentication Header
RFC 2403 IPsec Authentication - MD5
RFC 2404 IPsec Authentication - SHA-1
RFC 2405 IPsec Encryption - DES
RFC 2406 ESP - IPsec encryption
RFC 2407 IPsec DOI
RFC 2408 ISAKMP
RFC 2409 IKE
RFC 2410 IPsec encryption - NULL
RFC 2411 IP Security Document Roadmap
RFC 2412 OAKLEY
RFC 3173 IPComp - IPsec compression

IPv6

RFC 1981 Path MTU Discovery for IPv6
RFC 2080 RIPng for IPv6
RFC 2365 Administratively Scoped IP Multicast
RFC 2375 IPv6 Multicast Address Assignments
RFC 2460 IPv6
RFC 2461 Neighbour Discovery for IPv6
RFC 2462 IPv6 Stateless Address Autoconfiguration
RFC 2463 ICMPv6
RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
RFC 2465 Allocation Guidelines for Ipv6 Multicast Addresses Management Information Base for IP Version 6: Textual Conventions and General Group
RFC 2466 Management Information Base for IP Version 6: ICMPv6 Group
RFC 2472 IPv6 over PPP
RFC 2526 Reserved IPv6 Subnet Anycast Addresses
RFC 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels
RFC 2710 Multicast Listener Discovery (MLD) for IPv6
RFC 2711 IPv6 Router Alert Option
RFC 2851 Textual Conventions for Internet Network Addresses
RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers
RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
RFC 3307 Allocation Guidelines for IPv6 Multicast Addresses
RFC 3315 DHCPv6
RFC 3484 Default Address Selection for IPv6
RFC 3513 IPv6 Addressing Architecture
RFC 3587 IPv6 Global Unicast Address Format
RFC 3596 DNS Extensions to support IPv6
RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6

Management

RFC 1155 MIB
RFC 1157 SNMP
RFC 1212 Concise MIB definitions
RFC 1213 MIB-II
RFC 1493 Bridge MIB
RFC 1643 Ethernet MIB
RFC 1657 Definitions of Managed Objects for BGP-4 using SMIv2
RFC 2011 SNMPv2 MIB for IP using SMIv2
RFC 2012 SNMPv2 MIB for TCP using SMIv2
RFC 2096 IP Forwarding Table MIB
RFC 2576 Coexistence between V1, V2, and V3 of the Internet-standard Network Management Framework
RFC 2578 Structure of Management Information Version 2 (SMIv2)
RFC 2579 Textual Conventions for SMIv2
RFC 2580 Conformance Statements for SMIv2
RFC 2665 Definitions of Managed Objects for the Ethernet-like Interface Types
RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions (VLAN)
RFC 2790 Host MIB
RFC 2819 RMON (groups 1,2,3 and 9)
RFC 2856 Textual Conventions for Additional High Capacity Data Types
RFC 2863 The Interfaces Group MIB
RFC 3164 Syslog Protocol
RFC 3289 Management Information Base for the Differentiated Services Architecture
RFC 3410 Introduction and Applicability Statements for Internet-Standard Management Framework
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 the SNMP
RFC 3416 Version 2 of the Protocol Operations for SNMP
RFC 3417 Transport Mappings for the SNMP
RFC 3418 MIB for SNMP
RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs
RFC 3768 VRRP
draft-ietf-bridge-8021x-00.txt Port Access Control MIB
CDP
IEEE 802.1AB LLDP

OSPF

RFC 1245 OSPF protocol analysis
RFC 1246 Experience with the OSPF protocol
RFC 1586 OSPF over Frame Relay
RFC 1587 The OSPF NSSA Option
RFC 1793 Extending OSPF to Support Demand Circuits
RFC 2328 OSPFv2
RFC 3101 The OFPS Not-so-Stubby Area (NSSA) Option

Quality of Service

RFC 2205 Reservation Protocol
RFC 2211 Controlled-Load
RFC 2474 DCSP in the IPv4 and IPv6 Headers
RFC 2475 An Architecture for Differentiated Services
RFC 2597 Assured Forwarding PHB Group
RFC 2697 A Single Rate Three Color Marker
RFC 2698 A Two Rate Three Color Marker
RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior)
IEEE 802.1p Priority Tagging

RIP

RFC 1058 RIPv1
RFC 2082 RIP2 MD5 Authentication
RFC 2453 RIPv2

Security

RFC 959 FTP
RFC 1413 IDP

RFC 1492 TACACS
RFC 1779 X.500 String Representation of Distinguished Names
RFC 1858 Fragmentation
RFC 2284 EAP
RFC 2510 PKI X.509 Certificate Management Protocols
RFC 2511 X.509 Certificate Request Message Format
RFC 2559 PKI X.509 LDAPv2
RFC 2585 PKI X.509 Operational Protocols
RFC 2587 PKI X.509 LDAPv2 Schema
RFC 2865 RADIUS
RFC 2866 RADIUS Accounting
RFC 2868 RADIUS Attributes for Tunnel Protocol Support
RFC 3280 X.509 Certificate and CRL profile
RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines
draft-grant-tacacs-02.txt TACACS+
Draft-IETF-PKIX-CMP-Transport-Protocols-01 Transport Protocols for CMP
draft-ylonen-ssh-protocol-00.txt SSH Remote Login Protocol
IEEE 802.1x Port Based Network Access Control
PKCS #10 Certificate Request Syntax Standard
Diffie-Hellman

Services

RFC 854 Telnet Protocol Specification
RFC 855 Telnet Option Specifications
RFC 856 Telnet Binary Transmission
RFC 857 Telnet Echo Option
RFC 858 Telnet Suppress Go Ahead Option
RFC 932 Subnetwork addressing scheme
RFC 951 BootP
RFC 1091 Telnet terminal-type option
RFC 1179 Line printer daemon protocol
RFC 1305 NTPv3
RFC 1350 TFTP
RFC 1510 Network Authentication
RFC 1542 Clarifications and Extensions for the Bootstrap Protocol
RFC 1945 HTTP/1.0
RFC 1985 SMTP Service Extension
RFC 2049 MIME
RFC 2068 HTTP/1.1
RFC 2156 MIXER
RFC 2217 Telnet Com Port Control Option
RFC 2821 SMTP

SSL

RFC 2246 The TLS Protocol Version 1.0
draft-freier-ssl-version3-02.txt SSLv3

About Allied Telesis

Allied Telesis was founded in 1987 and now has offices around the globe, over 2,800 employees and over $500M of worldwide annual revenue. The attributes which have led Allied Telesis to achieve its leading position in the enterprise, operator and connectivity business segments can be summarised by four key elements: its business focus on networking technology for professional markets, where Allied Telesis has proved to be the only company capable of providing a total end-to-end solution at a high price/performance ratio; the ability to handle every aspect of its own products from design to marketing; the development of components and solutions which accommodate flexible, efficient and reliable network construction; and support from sound warranty terms and quality services. Allied Telesis connects the IP world efficiently thanks to affordable and highly reliable network solutions. For more information see: www.alliedtelesis.com

Service and Support

Allied Telesis provides value-added support services for its customers under its Net.CoverSM programs. For more information on Net.CoverSM support programs available in your area, contact your Allied Telesis sales representative or visit our website: www.alliedtelesis.com

Ordering Information

AT-AR450S-xx
Order number: 990-11847-xx (Not RoHS compliant)
Where xx = 10 for U.S. power cord
20 for no power cord
30 for U.K. power cord
40 for Australia power cord
50 for Europe power cord

Software upgrade options

AT-AR400 – ADVL3UPGRD
AR400 series advanced layer 3 upgrade
- IPv6
- BGP4
- Load balancing

Order number: 980-10021-00

AT-FL-15
WAN load balancer (feature license)
Order number: 980-000038

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

 617-00510-00 RevK