AlliedWare®
Operating System

AlliedWare Layer 3 Fully Featured Operating System

AlliedWare is Allied Telesis' feature-rich first generation operating system. It serves as the foundation for Allied Telesis' original Layer 3 switches and routers. AlliedWare includes the functionality, management capabilities and performance that today's networks demand. As a standards-based implementation, it also assures full interoperability with other major network equipment.

Security

SIF - Stateful Inspection Firewall

Allied Telesis' state-of-the-art Stateful Inspection Firewall delivers the highest level of security possible by providing full application-layer awareness without breaking the client/server model. Stateful Inspection extracts the state-related information required for security decisions from all application layers and maintains this information in dynamic state tables for evaluating subsequent connection attempts. It protects against a wide range of Denial of Service (DoS) attacks including Ping of Death, SYN/FIN flooding, Smurf attacks, port scans, fragment attacks and IP spoofing. E-mail alerts are automatically triggered when such attacks are detected. This provides a solution that is highly secure and offers maximum performance, scalability, and extensibility.

Application Gateways - SMTP Proxy, HTTP Proxy

The mail proxy inspects SMTP sessions as they pass through the firewall. By accepting or rejecting sessions based on source and destination address rules, abuse of e-mail servers is limited. Typical forms of e-mail abuse include receipt of unwanted advertisements, spam, and unauthorized forwarding of mail. The Web proxy inspects and filters outbound HTTP sessions as they pass through the firewall. The proxy can inspect URLs and restrict cookie activity.

Encryption

Advanced Encryption Standard (AES) is an algorithm that replaces the Data Encryption Standard (DES) as the Federal Information Processing Standard for encrypting data.
AES is different from DES and 3DES because it supports a longer key length and uses different routines to encrypt and decrypt data. Encryption algorithms with a long key length are more secure than those with a short key length.

802.1x

The IEEE 802.1x standard manages port-based network access. It provides authentication to devices attached to a LAN port, by initiating a connection or preventing access from that port if authentication fails. Valuable for authenticating and controlling user traffic to a protected network, 802.1x is also effective for dynamically varying encryption keys. 802.1x attaches the Extensible Authentication Protocol (EAP) to both wired and wireless LAN media, and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication.

Routing

IPv6

IPv6 is the next generation of the Internet Protocol (IP). It has primarily been developed to solve the problem of the eventual exhaustion of the IPv4 address space, but also offers other enhancements:

- Addresses are 16 Bytes long in contrast to IPv4's 4 Byte addresses.
- Globally unique addresses with more levels of addressing hierarchy, to reduce the size of routing tables.
- Auto-configuration of addresses by hosts.
- Improved scalability of multicast routing, by adding a 'scope' field to multicast addresses.
- A new type of address, the 'anycast address,' which is used to send a packet to any one of a group of devices.

Standard Features

- **IP** - Internet Protocol
- **TCP** - Transmission Control Protocol
- **NTP** - Network Time Protocol
- **Trigger Facility**
- **Logging Facility**
- **Scripting**
- **Web (HTTP) Server and client**
- **SMTP** - Simple Mail Transfer Protocol
- **TFTP Client** - Trivial File Transfer Protocol
- **CLI** - Command Line Interface
- **DHCP** - Dynamic Host Configuration Protocol
- **SNMPv3** - Simple Network Management Protocol
- **IGMP** - Internet Group Management Protocol
- **Static Routing**
- **RIP v1,v2** - Routing Information Protocol
- **OSPF** - Open Shortest Path First

BGP-4 - Border Gateway Protocol version 4

BGP-4 is an external gateway protocol which allows two routers/switches in different routing domains, known as Autonomous Systems to exchange routing information. This facilitates the forwarding of data across the border of the routing domains. BGP-4 allows routers/switches to learn multiple paths, choose the best path for routing information and install that path in the IP routing table.

WAN Load Balancer

The WAN load balancer enables the router to combine bandwidth from multiple WAN connections for increased throughput and redundancy. When a router simultaneously connects to multiple WANs, the WAN load balancer will distribute the traffic based on any one of a number of selectable balancing algorithms. A typical example would be a router that has two Internet connections each exchanging data to remote sites via different Internet providers. In this case an outage limited to one network will not result in a loss of connectivity to these sites.

QoS - Quality of Service

QoS intelligently manages network traffic to allow stable and predictable end-to-end network performance. Comprehensive, low latency QoS features operating at wire-speed provide flow-based traffic management with full classification, prioritization, traffic shaping and min/max bandwidth profiles. AlliedWare's® QoS features are ideal for service providers wanting to ensure maximum availability of premium voice, video, and data services, and at the same time manage customer service level agreements. For enterprise customers, QoS protects productivity by guaranteeing performance of business-critical applications including VoIP services, and helps to restore and maintain responsiveness of enterprise applications in the networked workplace.

Multicasting

PIM - Protocol Independent Multicast

PIM has two modes: Dense Mode (PIM-DM) and Sparse Mode (PIM-SM).

PIM-DM relies on the presence of an existing unicast routing protocol to provide routing table data to build up information for the multicast forwarding database. This process is independent of the mechanisms of the specific unicast routing protocol.

PIM-SM provides efficient communication between members of sparsely distributed groups - the type of groups that are most common in wide-area internetworks. PIM-SM limits multicast traffic so only those network devices interested in receiving traffic for a particular group receive that traffic.

IGMPv2 - Internet Group Management Protocol

IGMP is used between hosts and multicast routers and switches on a single physical network to establish hosts' membership in particular multicast groups. Multicast routers use this information, in conjunction with a multicast routing protocol, to support IP multicast forwarding across the Internet.

Management

GUI and SSL - Graphical User Interface and Secure Sockets Layer

The GUI is a web-based management tool designed for intuitive, easy-to-use device configuration and monitoring. Its purpose is to make complicated tasks simpler and regularly performed tasks quicker. A GUI connection can be secured with the use of the SSL. SSL is a security protocol that provides secure communication by allowing the client to verify the servers identity before either side sends any sensitive information. SSL encrypts data to prevent a third party from interfering with the message.

SSH - Secure Shell

Secure management is increasingly important in modern networks, as easy, effective device management and the need for security are two almost universal requirements. SSH is a secure Telnet type access that provides strong authentication and secure communication over insecure channels. While Telnet sends commands over the network in plaintext, SSH sends them encrypted. With SSH, a client can safely log into another computer over a network, execute commands in a remote machine, or move files from one machine to another.

Scripting

The Scripting facility allows sequences of commands to be stored in a script and replayed at any time so that switches can be easily and quickly configured. This is useful when developing a complex configuration, making the same configuration change to several different devices or security appliances, or introducing a configuration change that must occur at a particular time. Scripts can be activated from the command line, from a trigger, or when users log in.

Triggers

A trigger sets off an ordered sequence of scripts and commands to be executed when a certain event occurs, providing a powerful mechanism for automating the execution of commands in response to certain events. For example, triggers can be configured to collect diagnostic information after a reboot. Each trigger may reference multiple scripts and any script can be used by any trigger.

High Availability

Link Aggregation

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

AlliedWare® supports IEEE standard 802.3ad link aggregation, which can be configured manually, or automated via the use of Link Aggregation Control Protocol (LACP).

LACP automatically detects multiple links between two LACP enabled devices and configures them to use their maximum possible bandwidth by automatically combining the links.

VRRP - Virtual Router Redundancy Protocol

VRRP provides automatic backup in mission-critical environments. This feature enables multiple routers or switches to share a virtual IP address that serves as the default LAN gateway. Should the master fail, the other devices assume the virtual IP address. LAN devices can continue to be configured with a single default gateway address, and because VRRP is a standard Internet protocol, full interoperability with other VRRP-supported products is assured.

EPSR – Ethernet Protection Switched Rings

Ethernet Protection Switched Rings allow several switches to form a protected ring with sub 50ms failover. This feature is perfect for high performance at the core of enterprise or provider access networks.

MSTP - Multiple Spanning Tree Protocol

MSTP addresses the limitations in the existing spanning tree protocols, Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP). MSTP is similar to RSTP in that it provides loop resolution and rapid convergence. However it also has the significant extra advantage of making it possible to have different forwarding paths for different multiple spanning tree instances. This enables load balancing of network traffic across redundant links.

Networks using multiple VLAN topologies that employ alternative physical links are supported by MSTP. MSTP also supports multiple spanning tree instances on any given link within a network and can group bridges into 'regions' that appear as a single bridge to other devices.

Note: Features available on individual products are dependent on product hardware. For more information go to www.alliedtelesis.com.

AlliedWare® | Operating System

Allied Telesis Product	AR415S	AR44xS	AR450S	AR7x5	AR750S AR750S-DP	AR770S	AT-8600	Rapier 'i'	AT-8800	AT-8948	x900-48FE	AT-9800	AT-9924	AT-9924Ts	x900-24X	AT-SB4000
Software release	54-2.9.1	54-2.9.1	54-2.9.1	52-2.9.1	55-2.9.1	55-2.9.1	sr-2.9.1	86s-2.9.1	86s-2.9.1	89-2.9.1	89-2.9.1	sb-2.9.1	89-2.9.1	3.2.1	3.2.1	sb-2.7.5A
Switching																
Bridging (IEEE 802.1D)	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
VLAN - *Virtual Local Area Network*	✔	✔	✔	–	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
GARP - *Generic Attribution Registration Protocol*	–	–	–	–	–	–	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
High Availability																
STP - *Spanning Tree Protocol*	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
RSTP - *Rapid Spanning Tree Protocol*	–	–	–	–	–	–	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
MSTP (802.1s) - *Multiple Spanning Tree Protocol*	–	–	–	–	–	–	✔	✔	✔	✔	✔	–	✔	✔	✔	–
EPSR - *Ethernet Protected Switched Rings*	–	–	–	–	–	–	–	–	–	✔	✔	–	✔	✔	✔	–
VRRP - *Virtual Router Redundancy Protocol*	✔	✔	✔	✔	✔	✔	✔	✔	✔	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**
Server Load Balancing	**AL3**	**AL3**	**AL3**	**AL3**	**AL3**	**AL3**	–	**AL3**[1]	**AL3**[1]	–	–	**AL3**[1]	–	–	–	–
Security																
802.1x	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
802.1x VLAN Assignment	–	✔	✔	–	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
802.1x MAC Based Authentication	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	–	✔	✔	✔	–
SSL - *Secure Sockets Layer*	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
SSH - *Secure Shell*	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
TACACS+ - *Terminal Access Controller Access System*	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
IPSec - *IP Security*	✔	✔	✔	✔	✔	✔	–	✔	✔	–	–	–	–	–	–	–
ISAKMP - *Internet Security Association Key Management Protocol*	✔	✔	✔	✔	✔	✔	–	✔	✔	–	–	–	–	–	–	–
STT - *Synchronous Tunnelling*	✔	✔	–	✔	✔	✔	–	✔	–	–	–	–	–	–	–	–
TPAD - *Transaction Packet Assembler Disassembler*	✔	✔	✔	✔	✔	✔	–	✔	–	–	–	–	–	–	–	–
PKI - *Public Key Infrastructure*	✔	✔	✔	✔	✔	✔	–	✔	✔	✔	✔	✔	✔	✔	✔	–
Firewall	✔	✔	✔	**Sec**	✔	✔	–	**Sec**	**Sec**	–	–	**Sec**	–	–	–	–
SIP ALG - *Session Initiation Protocol Application Layer Gateway*	✔	✔	✔	✔	✔	✔	–	✔	✔	–	–	✔	–	–	–	–
HTTP Proxy	✔	✔	✔	**Sec**	✔	✔	–	**Sec**	**Sec**	–	–	**Sec**	–	–	–	–
SMTP Proxy	✔	✔	✔	**Sec**	✔	✔	–	**Sec**	**Sec**	–	–	**Sec**	–	–	–	–
DHCP Snooping/Filtering/Option 82	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	–	✔	–	–	–
QoS / Performance Tuning																
QoS - *Quality of Service*	–	–	–	–	–	–	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Software QoS	✔	✔	✔	✔	✔	✔	–	✔	✔	–	–	–	–	–	–	–
General Packet Classifier	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
RSVP - *Resource Reservation Protocol*	✔	✔	✔	✔	✔	✔	–	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**
Layer 2 Transport																
PPP - *Point-to-Point Protocol*	✔	✔	✔	✔	✔	✔	–	✔	✔	✔	✔	✔	✔	–	–	✔
L2TP - *Layer 2 Tunnelling Protocol*	✔	✔	✔	✔	✔	✔	–	✔	✔	✔	✔	✔	✔	–	–	✔
Frame Relay	✔	✔	–	✔	✔	✔	–	✔	–	–	–	–	–	–	–	–
ISDN - *Integrated Services Digital Network*	✔	✔	–	✔	✔	✔	–	✔	–	–	–	–	–	–	–	–
X.25	✔	✔	–	✔	✔	✔	–	✔	–	–	–	–	–	–	–	–
TDM - *Time Division Multiplexing*	✔	✔	–	✔	✔	✔	–	✔	–	–	–	–	–	–	–	–
ACC - Asynchronous Call Control	✔	✔	✔	✔	✔	✔	–	✔	✔	–	–	–	–	–	–	–
ATM/xDSL	–	✔	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Network Manageability																
CLI - *Command Line Interface*	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
GUI - *Graphical User Intface*	✔	✔	✔	✔	✔	–	✔	✔	✔	–	–	✔	✔	✔	✔	✔
HTTP Server	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
HTTP Client	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
TFTP Client - *Trivial File Transfer Protocol*	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
SNMP - *Simple Network Management Protocol*	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Trigger Facility	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Test Facility	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Scripting	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Terminal Server	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	–	–	✔
DHCP - *Dynamic Host Configuration Protocol*	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Management Stacking	–	–	–	–	–	–	**STK**	**STK**	**STK**	**STK**	**STK**	–	**STK**	**STK**	**STK**	–
WAN Load Balancing	**WAN**	**WAN**	**WAN**	–	✔	✔	–	–	–	–	–	–	–	–	–	–
NTP - *Network Time Protocol*	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Routing																
IPv6	**AL3**	**AL3**	**AL3**	**AL3**	**AL3**	**AL3**	–	**AL3**	**AL3**	**AL3**	**AL3**	**AL3**	**AL3**	**AL3**	**AL3**	–
OSPFv2 - *Open Shortest Path First*	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
GRE - *Generic Routing Encapsulation*	✔	✔	✔	✔	✔	✔	–	✔	✔	✔	✔	✔	–	–	–	✔
BGP-4 - *Border Gateway Protocol version 4*	**AL3**	**AL3**	**AL3**	**AL3**	**AL3**	**AL3**	–	**AL3**	**AL3**	**AL3**	**AL3**	**AL3**	**AL3**	**AL3**	**AL3**	**BGP**
Novell IPX	✔	✔	✔	✔	✔	✔	–	**FL3**	**FL3**	–	–	✔	–	–	–	✔
NAT/NAT-T - *Network Address Translation/NAT-Traversal*	✔	✔	✔	✔	✔	✔	–	**Sec**	**Sec**	–	–	–	–	–	–	–
Multicasting																
IGMP - *Internet Group Management Protocol*	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
IGMP Proxy	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	–	✔	✔	✔	–
DVMRP - *Distance Vector Multicast Routing Protocol*	✔	✔	✔	✔	✔	✔	–	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**
PIM-SM - *Protocol Independent Multicast Sparse Mode*	✔	✔	✔	✔	✔	✔	**FL**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**
PIM-DM - *Protocol Independent Multicast Dense Mode*	✔	✔	✔	✔	✔	✔	**FL**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**	**FL3**
RIPv1/v2	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Telephony																
VoIP - *Voice over Internet Protocol*	✔	✔	–	✔	–	–	–	✔	–	–	–	–	–	–	–	–

✔ = Feature is available in the Standard AlliedWare release of this product
Sec = Feature is available with the Security feature license for this product
STK = Feature is available with the AT-AR-STACKING license for this product
BGP = Feature is available with the AT-SB4000BGP-150 feature license (restricted to 150 routes)

– = Feature is not available
FL3 = Feature is available with the Full L3 feature license for this product
FL = AT-8600PIM feature (PIM-SM, PIM-DM)

AL3 = Feature is available with the Advanced L3 feature license for this product
WAN = Feature is available with the AT-FL-15 license for this product
AL3[1] = Feature requires AL3 and Sec License to be installedr

Note: *This table does not provide a complete AlliedWare® feature list. For more information about individual products go to www.alliedtelesis.com.*

Feature licenses - Routers

Product	Full Layer 3: RSVP PIM DM PIM SM DVMRP VRRP	Advanced L3: IPv6 BGP-4 Load balancing (server)	Security: Firewall SMTP Proxy HTTP Proxy	Security: Concurrent Sessions *(18B), *(18C)	Encryption: 3DES	Encryption: AES	Concurrent VPN Sessions: *(19B), *(19C) *(19D), *(19E)	WAN Load Balancer
AT-AR410(S)	Included	AT-AR400-ADVL3UPGRD	AT-AR400sSecPk[1]	N/A	AT-AR-3DES[2]	N/A	N/A	N/A
Order number		980-10021-00	980-10027-00		980-10000-01			
AT-AR415S	Included	AT-AR400-ADVL3UPGRD	Included	AT-FL-18B, 18C	Included	Included	AT-FL-19B, 19C, 19D, 19E	AT-FL-15
Order number		980-10021-00		980-000046, 47			980-000094, 95, 96, 97	980-000038
AT-AR440S/AR441S	Included	AT-AR400-ADVL3UPGRD	Included	N/A	Included[4]	Included[4]	N/A	AT-FL-15[5]
Order number		980-10021-00						980-000038
AT-AR442S	Included	AT-AR400-ADVL3UPGRD	Included	AT-FL-18C,	Included[4]	Included[4]	N/A	AT-FL-15[5]
Order number		980-10021-00		980-000047				980-000038
AT-AR450S	Included	AT-AR400-ADVL3UPGRD	Included	N/A	AT-AR-3DES	AT-AR-AES	N/A	AT-FL-15
Order number		980-10021-00			980-10000-01	980-10036-00		980-000038
AT-AR725/AR745	Included	AT-AR700-ADVL3UPGRD	AT-AR700sSecPk	N/A	AT-AR-3DES[3]	N/A	N/A	N/A
Order number		980-10022-00	980-10028-00		980-10000-01			
AT-AR750S/AR750S-DP	Included	AT-AR700-ADVL3UPGRD	Included	N/A	Included[4]	Included[4]	N/A	Included
Order number		980-10022-00						
AT-AR770S	Included	AT-AR700-ADVL3UPGRD	Included	N/A	Included[4]	Included[4]	N/A	Included
Order number		980-10022-00						

Concurrent Firewall Sessions
*(18B)=4000 Concurrent F/W Sessions
*(18C)=8000 Concurrent F/W Sessions

Concurrent VPN Sessions
*(19B)=5 Concurrent VPN Sessions
*(19C)=10 Concurrent VPN Sessions
*(19D)=25 Concurrent VPN Sessions
*(19E)=50 Concurrent VPN Sessions

[1] Applies to AT-AR410 only, included with the AT-AR410S
[2] The AT-AR011i ECMAC encryption card and 3DES license is required for hardware compression on the AT-AR410. The AT-AR011i ECMAC encryption card is already included in the AT-AR410S.
[3] AT-AR061 hardware encryption required.
[4] Included as standard in units manufactured from July 2006. A feature license is required on units made before this date:
- AT-AR-AES 980-10036-00
- AT-AR-AES/3DES 980-10037-00
- AT-AR-3DES 980-10000-01

[5] Available in AlliedWare® Operating System version 2.9.1-08 or later

Feature licenses - Switches

Product	Full Layer 3: RSVP PIM DIM PIM SM DVMRP VRRP	Advanced L3: IPv6 BGP-4 Load balancing (server)	Security: Firewall SMTP Proxy HTTP Proxy	3DES	VLAN Double Tagging	BGP-4 (restricted to 150 routes)
AT-8600	AT-8600PIM[4]	N/A	N/A	N/A	N/A	N/A
Order number	980-000099					
Rapier 'i' / Rapier	AT-AR-RPFL3UPGRD[9]	AT-RPADVL3UPGRD	AT-RPSecPk-00	AT-AR-3DES	N/A	N/A
Order number	980-10002-00	980-10024-00	980-10030-00	980-10000-00		
AT-8800	AT-AR-RPFL3UPGRD[9]	AT-RPADVL3UPGRD	AT-RPSecPk-00	AT-AR-3DES	N/A	N/A
Order number	980-10002-00	980-10024-00	980-10030-00	980-10000-00		
AT-8948	AT-AR-8900FL3UPGRD	AT-AR-8900ADVL3UPGRD	N/A	AT-AR-3DES	AT-AR-VLANTAG	N/A
Order number	980-10038-00	980-10039-00		980-10000-00	980-10041-00	
AT-9800	AT-AR-9800FL3UPGRD[5]	AT-9800ADVL3UPGRD	AT-9800SecPk-00	N/A	N/A	N/A
Order number	980-10033-00	980-10025-00	980-10031-00			
AT-9924	AT-9900FL3UPGRD[6]	AT-9900ADVL3UPGRD[7]	N/A	AT-AR-3DES[8]	AT-AR-VLANTAG	N/A
Order number	980-000001-00	980-000009-00		980-10000-00	980-10041-00	
AT-9924Ts	AT-9900FL3UPGRD[6]	AT-9900ADVL3UPGRD[7]	N/A	AT-AR-3DES[8]	AT-AR-VLANTAG	N/A
Order number	980-000001-00	980-000009-00		980-10000-00	980-10041-00	
AT-SB4000	AT-AR-SBFL3UPGRD	N/A	N/A	N/A	N/A	AT-SB4000BGP-150
Order number	980-10013-00					980-000125-00
x900-24X	AT-9900FL3UPGRD[6]	AT-9900ADVL3UPGRD[7]	N/A	AT-AR-3DES[8]	AT-AR-VLANTAG	N/A
Order number	980-000001-00	980-000009-00		980-10000-00	980-10041-00	
x900-48FE	AT-AR-8900FL3UPGRD	AT-AR-8900ADVL3UPGRD	N/A	AT-AR-3DES	AT-AR-VLANTAG	N/A
Order number	980-10038-00	980-10039-00		980-10000-00	980-10041-00	

[4] AT-8600 PIM-DM & PIM-SM feature license only
[5] Included in North American products as part of their base configuration. Free registration required in other regions.
[6] Full Layer 3 upgrade does not include IPX Routing.
[7] Advanced Layer 3 upgrade does not include Load Balancing.
[8] For SSL
[9] Rapier i / Rapier / AT-8800 Full layer 3 excludes VRRP. VRRP is included in the standard AlliedWare® release for these products.

USA Headquarters | 19800 North Creek Parkway | Suite 100 | 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

 617-00476-00 Rev. ZA