AlliedWare Plus™

Fully Featured Layer 3 Switch Operating System

AlliedWare Plus is the next generation operating system from Allied Telesis, providing advanced IPv4 and IPv6 features, superior robustness, and ease of management.

AlliedWare Plus is an industry-leading operating system that delivers more features and robustness by employing a modular approach to software creation. This approach enables Allied Telesis to implement new functionality faster with exceptional quality, which means customers can upgrade their networks with minimal disruption.

The AlliedWare Plus operating system combines superior networking functionality and strong management capabilities with the exceptional performance that today's networks demand. A standards-based implementation, it also assures full interoperability with other major network equipment, and features improved usability for a superior customer experience.

Modularity + Monitoring = Robust Flexibility

AlliedWare Plus features a modular architecture, providing superior reliability. This architecture uses separate software processes, called modules, to handle different functions such as management, routing protocols, and control. Each of these modules can access only its allocated memory, preventing processes from corrupting each other and causing system crashes. Although independent of each other, modules communicate via well-defined interfaces.

Unified network management

AlliedWare Plus can manage large-scale wired and wireless networks on a single platform to reduce complexity and increase administrative consistency. The Allied Telesis Management Framework (AMF) is the key to unifying network management.

It saves time and reduces cost by automating many every day network management tasks.

Management of Allied Telesis TQ Series wireless access points is now possible directly from AlliedWare Plus switches with the Wireless Manager. Provisioning, operation, administration, and maintenance for the entire enterprise wireless infrastructure, can be performed centrally thereby reducing TCO and improving the user experience.

Certified Secure

Allied Ware Plus uses strong cryptographic algorithms with large key sizes to support secure communication and for protection of information. The cryptographic algorithms used in Allied Ware Plus are CAVP* certified.

Easy to use

The AlliedWare Plus operating system incorporates an industry standard Command Line Interface (CLI), facilitating intuitive manageability. Each command is associated with a specific function or task. Many of the commands can be used in scripts, allowing the automation of configuration tasks. Users can also utilize Triggers, which provide a powerful mechanism for automatic and timed management by automating the execution of commands in response to specific events.

The built-in, web-based Graphical User Interface (GUI) is an easy-to-use and powerful management tool. With comprehensive monitoring facilities and the ability to view a virtual chassis as a single entity, the GUI is an essential part of a network management toolkit.

Futureproof

AlliedWare Plus meets the needs of government and enterprise customers seeking to ensure their network investment is protected now and into the future. With a forward thinking product roadmap, a full IPv6 feature set and the imminent release of OpenFlow v1.3, long-term network reliability and investment security is guaranteed with Allied Telesis.

New Features

- AMF Cloud
- Wireless Manager
- Active Fiber Monitoring
- VLAN Mirroring (RSPAN)

* Cryptographic Algorithm Validation Program (CAVP) is administered by the National Institute of Standards and Technology (NIST) in the United States.

Key Features

Allied Telesis Management Framework (AMF)

- Allied Telesis Management Framework (AMF) is a sophisticated suite of management tools that provide a simplified approach to network management. Powerful features like centralized management, auto-backup, auto-upgrade, auto-provisioning and auto-recovery enable plug-and-play networking and zero-touch management.
- The AMF master enables auto-provisioning and auto-upgrade by providing appropriate files to new network members. New network devices can be pre-provisioned making installation easy because no on-site configuration is required.

AMF Controller

- An AMF master can manage networks of up to 120 nodes, which can be located locally or across WAN links. This can be dramatically increased by installing the AMF Controller, which enables multiple AMF Masters to be managed from a single point. With the AMF Controller, a network of over 7,000 devices can be managed, allowing all the time saving, cost reducing benefits of AMF to be multiplied and efficiencies to be increased.

AMF Starter

- With AMF Starter you can try AMF for free, managing up to three nodes from any switch capable of acting as a Master.

AMF Cloud

- AMF Cloud allows the AMF Master and/or Controller to be virtual appliances rather than intergrated into an Allied Telesis switch or firewall. AMF Cloud offers full AMF functionality, with the advantages of cloud-based access and flexibility.

Virtual Routing and Forwarding (VRF Lite)

- VRF Lite provides Layer 3 network virtualization by dividing a single router into multiple independent virtual routing domains. With independent routing domains, IP addresses can overlap without causing conflict, allowing multiple customers to have their own secure virtual network within the same physical infrastructure.

VCStack™ (Virtual Chassis Stacking)

- VCStack makes networking simple. It allows multiple switches to be connected together via high speed stacking links. This aggregates the switches, which then appear as a single switch, or 'virtual chassis'. The virtual chassis can be configured and managed via a single serial console or IP address, which provides greater ease of management in comparison to an arrangement of individually managed switches, and often eliminates the need to configure protocols like VRRP and Spanning Tree.

Long-distance Stacking

- Long-distance stacking allows a VCStack to be created over longer distances, perfect for a distributed network environment.

VCStack Plus™

- Two SwitchBlade x8100 chassis can be stacked together into a single virtual unit using VCStack Plus. The stacking link uses the 10 Gigabit front panel ports on the CFC960 control cards, which provides a massive 160 Gigabits of stacking bandwidth. VCStack Plus provides a highly available system where network resources and distribution switches are connected across the units for ultimate resiliency. Management is simplified as the two chassis operate as a single virtual unit.

In-Service Software Upgrade (ISSU)

- ISSU (also called "hitless firmware upgrade") allows firmware to be updated without causing any network disruption from a device reboot. This enables essential maintenance to be performed when it is required rather than having to schedule a network outage or tolerate any loss of service. ISSU is supported on dual controller systems and can be used in conjunction with VCStack Plus, making it ideal for high availability applications.

Link Aggregation

- Link aggregation 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.

VCStack and Link Aggregation

- Link aggregation can be used across members of a stack to protect against link and device failures. This provides a resilient network solution that is easier to implement and administer than traditional redundant core networks. A VCStack solution in combination with link aggregation also achieves load balancing, as the stacked devices share the network traffic.

MEF Certified

- Switching products running AlliedWare Plus have been certified by the Metro Ethernet Forum (MEF) certification program, which tests products for conformance to the strict requirements of Carrier Ethernet. Specifically, these products are certified for compliance to MEF 9 and MEF 14 Ethernet services tests.

sFlow

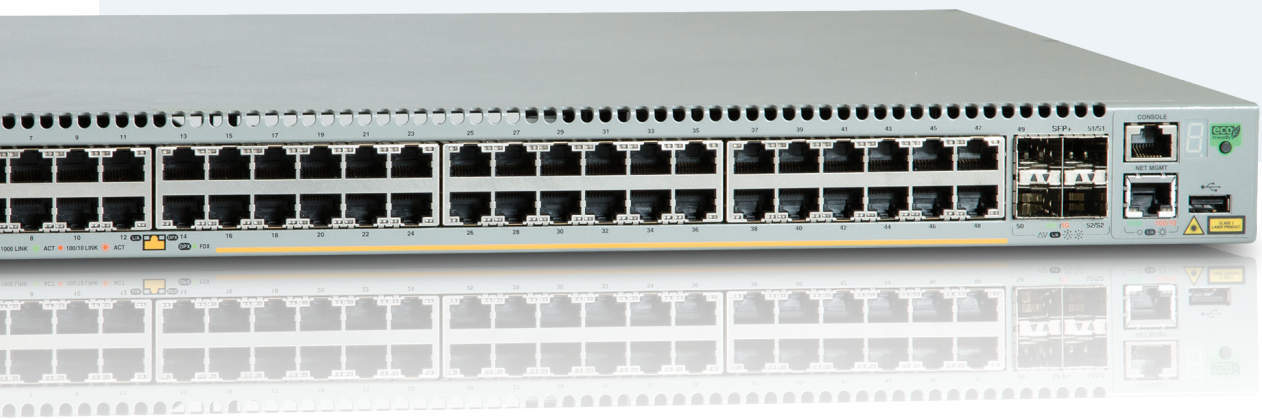
- sFlow is an industry-standard technology for monitoring high-speed switched networks. It gives complete visibility into network use, enabling performance optimization, usage accounting/billing, and defense against security threats. Sampled packets sent to a collector ensure it always has a real-time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

AlliedWare Plus Licensing Unlocks New Features

- With AlliedWare Plus, a single license password or "key" is all that is necessary to unlock additional feature bundles that ship with the switches. This single key enables the bundled features on all hardware of that particular product type.

802.1x, RADIUS Authentication and Dynamic VLAN Assignment

- 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 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, certificates, and public key authentication.
- 802.1x uses the RADIUS (Remote Authentication Dial In User Service) protocol to transfer authentication and configuration information between the switch and a shared RADIUS authentication server, which manages a user database and provides information to the client.
- Dynamic VLAN assignment allows an 802.1x supplicant to be placed into a specific VLAN, based on information returned from the RADIUS server during authentication. This limits a supplicant's network access to a specific VLAN, and prevents supplicants from connecting to VLANs for which they are not authorized.



Access Control Lists (ACLs)

- AlliedWare Plus delivers industry-standard access control functionality through Access Control Lists (ACLs). ACLs filter network traffic to control whether packets are forwarded or blocked at the port interface. The switch examines each packet to determine whether to forward or drop the packet, based on criteria that is specified within the ACL, such as source and destination MAC or IP address, IP protocol, or TCP/UDP port. This provides a powerful network security mechanism to select the types of traffic to be analyzed, forwarded, or influenced in some way, for example, to restrict routing updates or provide traffic flow control.

Bridge Protocol Data Unit (BPDU) Protection

- BPDU protection adds extra security to the Spanning Tree Protocol (STP). It protects the spanning tree configuration by preventing malicious DoS attacks caused by spoofed BPDUs.
- BPDU Protection is designed to be enabled on ports that should not receive BPDUs. These are edge ports connected to end user devices that do not run spanning tree. If a spoofed BPDU packet is received on a protected port, the BPDU Protection feature disables the port and alerts the network manager.

EPSRings™ (Ethernet Protection Switched Ring)

- EPSRing and 10 Gigabit Ethernet allow several switches to form high-speed protected rings, capable of recovery within as little as 50ms. This feature is perfect for high performance and high availability in enterprise networks.
- SuperLoop Prevention (SLP) enables a link between two EPSR nodes to be in separate EPSR domains, improving redundancy and network fault resiliency.

Control Plane Prioritization (CPP)

- The Control Plane Prioritization (CPP) feature allows priorities to be allocated to packet types, to ensure minimum interruption to the flow of control information through the network.
- CPP stops the control plane from being flooded by traffic in the event of a network storm or Denial of Service (DoS) attack. This ensures maximal performance and prevents network outages.

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 allows the traffic rate that creates a broadcast storm to be defined. The action the device should take when it detects a storm, such as disabling the port from the VLAN or shutting the port down, can also be configured.
- 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 specified when the device will discard each of the different packet types.

Loop Protection

- AlliedWare Plus provides two forms of Loop Protection, Thrash Limiting and Loop Detection.
- 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.
- Loop Detection works in conjunction with Thrash Limiting. 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 sends special Loop Detection Frame (LDF) packets that the switch listens for. If an LDF packet is received, then the switch can be configured to either disable the port, disable the link, or send an SNMP trap.

Policy-Based Quality of Service (QoS)

- Comprehensive, low latency QoS features operating at wirespeed provide flow-based traffic management with full classification, prioritization, traffic shaping and min/max bandwidth profiles.
- Our 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 (SLAs).
- For enterprise customers, QoS features protect productivity by guaranteeing performance of business-critical applications (including VoIP services), and help to restore and maintain the responsiveness of enterprise applications in the workplace.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP - MED)

- LLDP-MED extends LLDP's basic network endpoint discovery and management functions. LLDP-MED allows for media end-point specific messages, providing detailed information on power requirements, network policy, location discovery (for emergency call services) and inventory. LLDP-MED is an important feature for simplifying VoIP, security camera and WLAN deployments.

Voice VLAN

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

Power over Ethernet Plus (PoE+)

- With PoE, a separate power connection to media end points such as IP phones and wireless access points is not necessary. PoE+ provides even greater flexibility, as it is capable of connecting devices that require more power (up to 30 Watts), for example tilt and zoom security cameras.

Dynamic Host Configuration Protocol (DHCPv6)

- DHCPv6 is used to dynamically assign IPv6 addresses to hosts from a central location. Acting as DHCPv6 client enables the switch to receive an IPv6 address, and acting as server enables the switch to dynamically allocate IPv6 addresses to hosts. The DHCPv6 server and client both support the Prefix Delegation feature, which allocates a whole IPv6 subnet to a DHCP client. The client, in turn, can allocate addresses from this subnet to the hosts that are connected to it.

Virtual Router Redundancy Protocol (VRRPv3)

- VRRPv3 is a protocol for providing device redundancy, by connecting redundant WAN gateway routers or server access switches in an IPv6 network. It allows a backup router or switch to automatically take over if the primary (master) router or switch fails.

Find Me

- In busy server rooms consisting 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.

Wireless Manager

- The Allied Telesis Wireless Manager has been designed specifically to meet the requirements of enterprise organizations and addresses key concerns about mobility, security, and TCO. The Wireless Manager is embedded within the operating system of the switch so no separate server is required. It is able to control a number of Allied Telesis TQ Series wireless access points and can centralize the provisioning, operation, administration, and maintenance for the entire enterprise wireless infrastructure.

Active Fiber Monitoring

- Active Fiber Monitoring detects tamping on optical links by regularly checking received optical power. This provides increased security by ensuring the integrity of short- and long-haul fiber links.

VLAN Mirroring (RSPAN)

- VLAN mirroring allows traffic from a port on a remote switch to be analysed locally. Traffic being transmitted or received on the port is duplicated and sent across the network on a special VLAN.

Feature Licenses for AlliedWare Plus 5.4.6-1

Product	License Bundles			Standalone Licenses
	Advanced L3	IPv6 Pack	Premium	
CentreCOM GS900MX Series	-	-	-	**AT-FL-GS9X-UDLD** ■ UniDirectional Link Detection
CentreCOM XS900MX Seriess	-	-	-	**AT-FL-XS9X-UDLD** ■ UniDirectional Link Detection
x210 Series	-	-	-	**AT-FL-x210-UDLD** ■ UniDirectional Link Detection
x230 Series	-	-	-	**AT-FL-x230-QinQ** ■ VLAN double tagging (QinQ) **AT-FL-x230-OPEN** ■ OpenFlow v1.3 **AT-FL-x230-UDLD** ■ UniDirectional Link Detection
x310 Series	-	-	**AT-FL-x310-01** ■ RIP (64 routes) ■ OSPF (64 routes) ■ PIMv4-SM, DM and SSM ■ EPSR master ■ RIPng (64 routes) ■ OSPFv3 (64 routes) ■ PIMv6-SM and SSM ■ UDLD ■ VRRP	**AT-FL-x310-OPEN** ■ OpenFlow v1.3
IX5-28GPX	-	-	-	**AT-FL-IX5-EPSR** ■ EPSR master ■ UDLD
x510 Series	-	-	**AT-FL-x510-01** ■ RIP (256 routes) ■ OSPF (256 routes) ■ PIMv4-SM, DM, SSM ■ EPSR master ■ VLAN Q-in-Q ■ RIPng (256 routes) ■ OSPFv3 (256 routes) ■ UDLD ■ MLDv1 and v2 ■ PIMv6-SM, SSM	**AT-FL-x510-AM20-1YR** **AT-FL-x510-AM20-5YR** ■ AMF master (20 nodes) **AT-FL-x510-OPEN** ■ OpenFlow v1.3 **AT-FL-x510L-10G** ■ 10G upgrade license
x610 Series	**AT-FL-x610-01** ■ OSPF[1] (10,000 routes) ■ BGP4 (5,000 routes) ■ PIMv4-SM, DM, SSM ■ UDLD ■ VLAN Q-in-Q ■ VRF lite (64 domains)	**AT-FL-x610-02** ■ RIPng (1,000 routes) ■ OSPFv3 (5,000 routes) ■ BGP4+ for IPv6 (5,000 routes) ■ PIMv6-SM, SSM ■ MLDv1 and v2	-	**AT-FL-RAD-FULL** ■ RADIUS-Full[2] **AT-FL-x610-AM20-1YR** **AT-FL-x610-AM20-5YR** ■ AMF master (20 nodes)
x900 Series **AlliedWare Plus 5.4.4**	**AT-FL-x900-01** ■ OSPF[1] (10,000 routes) ■ BGP4 (5,000 routes) ■ PIMv4-SM, DM, SSM ■ VLAN Q-in-Q ■ VRF lite (64 domains)	**AT-FL-x900-02** ■ RIPng (1,000 routes) ■ OSPFv3 (8,000 routes) ■ BGP4+ for IPv6 (5,000 routes) ■ PIMv6-SM ■ MLDv1 and v2	-	**AT-FL-RAD-FULL** ■ RADIUS-Full[2]
x930 Series	-	-	**AT-FL-x930-01** ■ OSPF (10,000 routes) ■ BGP4 (5,000 routes) ■ PIMv4-SM, DM, SSM ■ VLAN Q-in-Q ■ RIPng (5,000 routes) ■ OSPFv3 (8,000 routes) ■ BGP4+ for IPv6 (5,000 routes) ■ MLDv1 and v2 ■ UDLD ■ PIMv6-SM, SSM ■ VRF lite (64 domains) ■ RADIUS-Full	**AT-FL-x930-WM20** ■ Wireless Manager (20 APs) **AT-FL-x930-WM40** ■ Wireless Manager (40 APs) **AT-FL-x930-AM40[3]** ■ AMF master (40 nodes) **AT-FL-x930-AM80[3]** ■ AMF master (80 nodes) **AT-FL-x930-AM120[3]** ■ AMF master (120 nodes) **AT-FL-x930-OPEN** ■ OpenFlow v1.3

[1] 64 OSPF routes are included for free in the base firmware
[2] RADIUS-Full increases the local RADIUS database limits to 1,000 NAS devices and 5,000 users
[3] AMF licenses are available for 1 year or 5 years

Feature Licenses for AlliedWare Plus 5.4.6-1

Product	License Bundles			Standalone Licenses
	Advanced L3	IPv6 Pack	Premium	
DC2552XS/L3	-		**AT-FL-DC2552XS-01** ■ OSPF (10,000 routes) ■ BGP4 (5,000 routes) ■ PIMv4-SM, DM, SSM ■ VLAN Q-in-Q ■ RIPng (5,000 routes) ■ OSPFv3 (8,000 routes) ■ UDLD ■ BGP4+ for IPv6 (5,000 routes) ■ MLDv1 and v2 ■ PIMv6-SM, SSM ■ VRF lite (64 domains) ■ RADIUS-Full	**AT-FL-DC2552-AM40**[3] ■ AMF master (40 nodes) **AT-FL-DC2552-AM80**[3] ■ AMF master (80 nodes) **AT-FL-DC2552-AM120**[3] ■ AMF master (120 nodes) **AT-FL-DC25-OPEN** ■ OpenFlow v1.3
SwitchBlade x908	**AT-FL-SBX9-01** ■ OSPF[1] (10,000 routes) ■ BGP4 (5,000 routes) ■ PIMv4-SM, DM, SSM ■ UDLD ■ VLAN Q-in-Q ■ VRF lite (64 domains)	**AT-FL-SBX9-02** ■ RIPng (1,000 routes) ■ OSPFv3 (8,000 routes) ■ BGP4+ for IPv6 (5,000 routes) ■ PIMv6-SM, SSM ■ MLDv1 and v2	-	**AT-FL-SBX9-AM40**[3] ■ AMF master (40 nodes) **AT-FL-SBX9-WM20** ■ Wireless Manager (20 APs) **AT-FL-RAD-FULL** ■ RADIUS-Full[2]
SwitchBlade x8100 Series with CFC400 controller card	-	-	**AT-FL-CFC400-01** ■ OSPF[1] (5,000 routes) ■ BGP4 (5,000 routes) ■ PIMv4-SM, DM, SSM ■ VLAN Q-in-Q ■ RIPng (1,000 routes) ■ UDLD ■ OSPFv3 (1,000 routes) ■ BGP4+ for IPv6 (1,000 routes) ■ MLDv1 & v2 ■ PIMv6-SM, SSM ■ RADIUS-Full[2]	**AT-FL-CF4-AM40**[3] ■ AMF master (40 nodes) **AT-FL-CF4-AM80**[3] ■ AMF master (80 nodes)
SwitchBlade x8100 Series with CFC960 controller card	-	-	**AT-FL-CFC960-01** ■ OSPF[1] (5,000 routes) ■ BGP4 (5,000 routes) ■ PIMv4-SM, DM, SSM ■ VLAN Q-in-Q ■ RIPng (1,000 routes) ■ UDLD ■ OSPFv3 (1,000 routes) ■ BGP4+ for IPv6 (1,000 routes) ■ MLDv1 & v2 ■ PIMv6-SM, SSM ■ RADIUS-Full[2] ■ VRF lite (64 domains)	**AT-FL-CF9-VCSPL** ■ VCStack Plus **AT-FL-CF9-AM80**[3] ■ AMF master (80 nodes) **AT-FL-CF9-AM120**[3] ■ AMF master (120 nodes) **AT-FL-CF9-AC10**[3] ■ AMF Controller (10 areas) **AT-FL-CF9-AC30**[3] ■ AMF Controller (30 areas) **AT-FL-CF9-AC60**[3] ■ AMF Controller (60 areas) **AT-FL-CF9-WM40** ■ Wireless Manager (40 APs) **AT-FL-CF9-WM80** ■ Wireless Manager (80 APs) **AT-FL-CF9-WM120** ■ Wireless Manager (120 APs)

[1] 64 OSPF routes are included for free in the base firmware
[2] RADIUS-Full increases the local RADIUS database limits to 1,000 NAS devices and 5,000 users
[3] AMF licenses are available for 1 year or 5 years

Feature Licenses for AlliedWare Plus 5.4.6-1

Industrial Product	License Bundles	
	Layer 2 Premium	Layer 3 Premium
IE300 Series	**AT-FL-IE3-L2-01** ■ EPSR master ■ ITU-T G.8032 ■ VLAN Q-in-Q ■ UDLD	**AT-FL-IE3-L3-01** ■ RIP (64 routes) ■ OSPF (64 routes) ■ PIMv4-SM, DM and SSM ■ RIPng (64 routes) ■ OSPFv3 (64 routes) ■ PIMv6-SM and SSM ■ VRRP
IE510-28GSX-80		**AT-FL-IE5-L3-01** ■ RIP (256 routes) ■ OSPF (256 routes) ■ PIMv4-SM, DM and SSM ■ EPSR master ■ VLAN Q-in-Q ■ RIPng (256 routes) ■ OSPFv3 (256 routes) ■ PIMv6-SM and SSM ■ MLDv1 and v2

About Allied Telesis

For nearly 30 years, Allied Telesis has been delivering reliable, intelligent connectivity for everything from enterprise organizations to complex, critical infrastructure projects around the globe.

In a world moving toward Smart Cities and the Internet of Things, networks must evolve rapidly to meet new challenges. Allied Telesis smart technologies, such as Allied Telesis Management Framework™ (AMF) and Enterprise SDN, ensure that network evolution can keep pace, and deliver efficient and secure solutions for people, organizations, and “things”—both now and into the future.

Allied Telesis is recognized for innovating the way in which services and applications are delivered and managed, resulting in increased value and lower operating costs.

Visit us online at **alliedtelesis**.com

Allied Telesis NETWORK SMARTER

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

alliedtelesis.com

617-00475-00 Rev ZE