Secure VPN Router

AR2050V

Allied Telesis Secure Virtual Private Network (VPN) Routers are the ideal secure gateway for modern businesses. Powerful VPN functionality is combined with comprehensive routing and switching, providing an innovative high performance solution that is easy to use and very secure.

As businesses adapt to faster paced operations, with increasing amounts of data, and the need to access company resources from outside the office, the demand for high performance VPN connectivity becomes more urgent.

The AR2050V features comprehensive security and advanced networking capabilities, meeting the demands of distributed businesses that require multi-site VPNs.

Application-aware firewall

The firewall on the AR2050V inspects every packet passing through it, and uses a built-in application list, so different applications can be managed in line with business security and acceptable use policies. Allied Telesis Secure VPN Routers are the ideal solution for enterprise and branch offices requiring secure online connectivity.

High performance

Harnessing the power of multi-core processors and hardware acceleration engines guarantees high performance, by dramatically increasing throughput and enabling sustained low latency traffic inspection.

Performance	
Firewall throughput	750 Mbps
Concurrent sessions	100,000
New sessions per second	3,600
IPS throughput	200 Mbps
VPN throughput	400 Mbps

Secure Remote VPNs

The AR2050V supports IPSec site-to-site VPN connectivity to connect one or more branch offices to a central office, providing employees company-wide with consistent access to the corporate network.

Remote workers can utilize an SSL VPN connection to encrypt their business data over the Internet, allowing them to utilize all their business resources when working from home, travelling, or otherwise away from the company premises.

Comprehensive routing support

The security features of the AR2050V are complemented by advanced routing and switching capability. Full IPv6 routing and protocol implementation ensures today's networks are fully connectable, both internally and externally with other leading edge equipment. Powerful multicasting features support streaming video and voice traffic in modern converged networks.

High availability

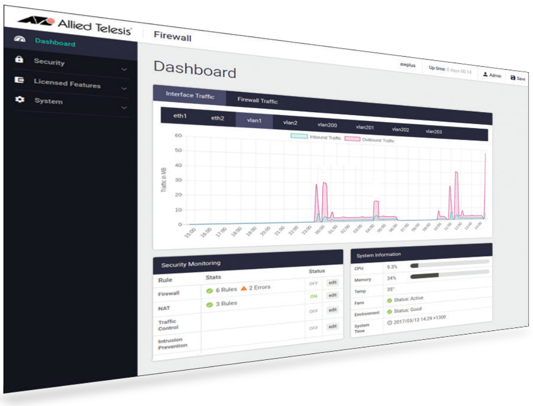
When online connectivity is critical, the AR2050V has a bypass port to allow a link to another device as a passive backup. Automated failover immediately transmits Internet-bound traffic to the backup device, to maximize the availability of external connectivity, and ensure no loss of business productivity.

Easy to manage

The AR2050V runs the advanced AlliedWare Plus™ fully featured operating system, with an industry standard CLI. The Graphical User Interface (GUI) provides a dashboard for monitoring, showing traffic throughput, security status, and application use at a glance. Configuration of security zones, networks and hosts, and rules to limit and manage traffic, provides a consistent approach to policy management.

Wireless LAN management

The AR2050V features Allied Telesis Autonomous Wave Controller (AWC), which is an intelligent, easy-to-use Wireless LAN controller that automatically maintains the optimal wireless coverage. AWC is fully integrated with the GUI for easy setup, management, and monitoring of wireless access points.



Dashboard

Security Monitoring

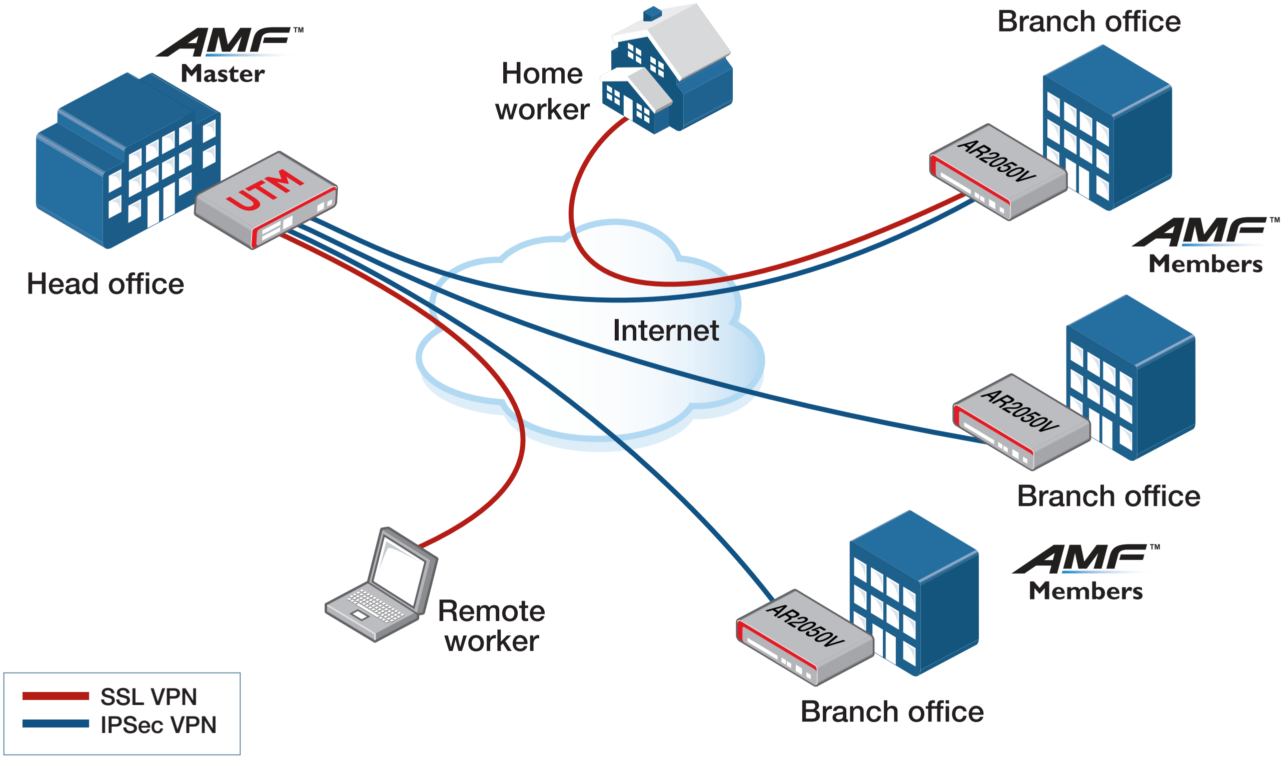
Rule	Stats	Status	
Firewall	6 Rules ⚠ 2 Errors	OFF	edit
NAT	3 Rules	ON	edit
Traffic Control		OFF	edit
Intrusion Prevention		OFF	edit

System Information

CPU	9.3%
Memory	34%
Temp	35°
Fans	Status: Active
Environment	Status: Good
System Time	2017/03/13 14:29 +1300

FIREWALL ENGINE	
Application-aware	All traffic passing through the firewall is inspected, so different applications can be managed in line with business policies.
DoS attack protection	Protection against Denial of Service (DoS) attacks, which are designed to consume resources and therefore deny users network and application access.
Intrusion Detection and Prevention System (IDS/IPS)	IDS/IPS provides monitoring, analysis and logging of suspicious events that occur on a network. It can also perform a variety of actions to prevent attacks.
URL filtering	Enables HTTP or HTTPS access to particular websites to be allowed (whitelist) or blocked (blacklist) with user-defined lists.
VIRTUAL PRIVATE NETWORKING (VPN)	
IPSec VPN for site-to-site connectivity	High-performance IPSec VPN allows the AR2050V to connect branch offices and other large sites, for secure sharing of business information.
SSL/TLS VPN for secure remote access	Users simply utilize the OpenVPN client on their computer, tablet, or other mobile device for easy access to email, files, and other corporate digital resources when away from the office.
VPN pass-through	Pass-through enables VPN clients to make outbound connections using L2TP, PPTP or IPsec.
Redundant VPN gateway	Primary and secondary VPNs can be configured when using multiple WAN connections, for seamless failover of VPN connectivity to a remote site.
Dynamic routing through VPN tunnels	Dynamic routing over VPN links ensures no loss of connectivity, as traffic is routed through an alternate link in the event of a tunnel failure.
RESILIENCY	
High availability bypass port	The bypass port allows a backup link to be formed to another device, to act as a passive backup. In the event of a power failure, the WAN traffic is immediately transmitted to the backup device for automatic failover of the WAN connection.
VRRP triggers for bypass port failover	The AR2050V supports event-based triggers to automatically change VRRP mastership if a bypass port is activated. This simplifies WAN failover and reduces disruption to other network devices.
QUALITY OF SERVICE (QOS)	
Traffic control	Traffic control allows the amount of bandwidth to be restricted for different traffic classes. RED curves can be defined to predictably drop traffic if congestion occurs.
Bandwidth management	Protect your business-critical traffic by limiting the bandwidth available to non-essential traffic. During peak times, non-essential traffic is limited, allowing critical traffic to flow freely.
NETWORKING	
3G/4G/LTE USB modem	A 3G/4G/LTE USB modem offers an additional secure data connection for critical services, which can automatically switch to a mobile network whenever a primary data connection becomes unavailable.
Layer 2 Tunnelling Protocol (L2TP)	L2TP provides site-to-site connectivity, which can also be protected by IPSec encryption.
IPv6 support	Full support for IPv6 routing, multicasting and security is provided.
DS-Lite	DS (Dual Stack)-Lite supports connecting IPv4 networks over an IPv6 Internet connection.
SD-WAN	Software-Defined Wide Area Networking (SD-WAN) enables users to measure the quality of their WAN links, and send traffic over the best performing connection, as well as send different traffic types to different destinations.
Policy-based routing	Policy-based routing enables traffic forwarding decisions to be based on where the traffic is coming from, rather than where it is going to.
Autonomous Management Framework (AMF)	AMF enables new devices to be pre-provisioned for zero-touch deployment. This simplifies installation, guarantees consistent configuration, and reduces setup time and cost.
AMF backup/recovery	As an AMF member, the AR2050V is automatically backed up, and can be recovered with plug-and-play simplicity.
Flexible deployment options	The AR2050V can be deployed in traditional NAT, Layer 2 Bridge, Wire Mode and Network Tap modes.
VRF-Lite	Virtual Routing and Forwarding (VRF-Lite) allows multiple routing tables. As the routing instances are independant, the same or overlapping IPv4 addresses can be used.

Key solution



Multi-site VPN connectivity

Allied Telesis Secure VPN Routers are the ideal integrated security platform for modern businesses. The powerful combination of VPN connectivity, secure remote access, and routing and switching, provides a single platform to connect and protect corporate data.

This example shows how the AR2050V can provide multi-site connectivity back to a head office. IPSec VPNs to an Allied Telesis Unified Threat Management (UTM) Firewall ensure that all staff have full access to digital resources. SSL VPN access provides secure access for workers when travelling, at home, or otherwise away from the office.

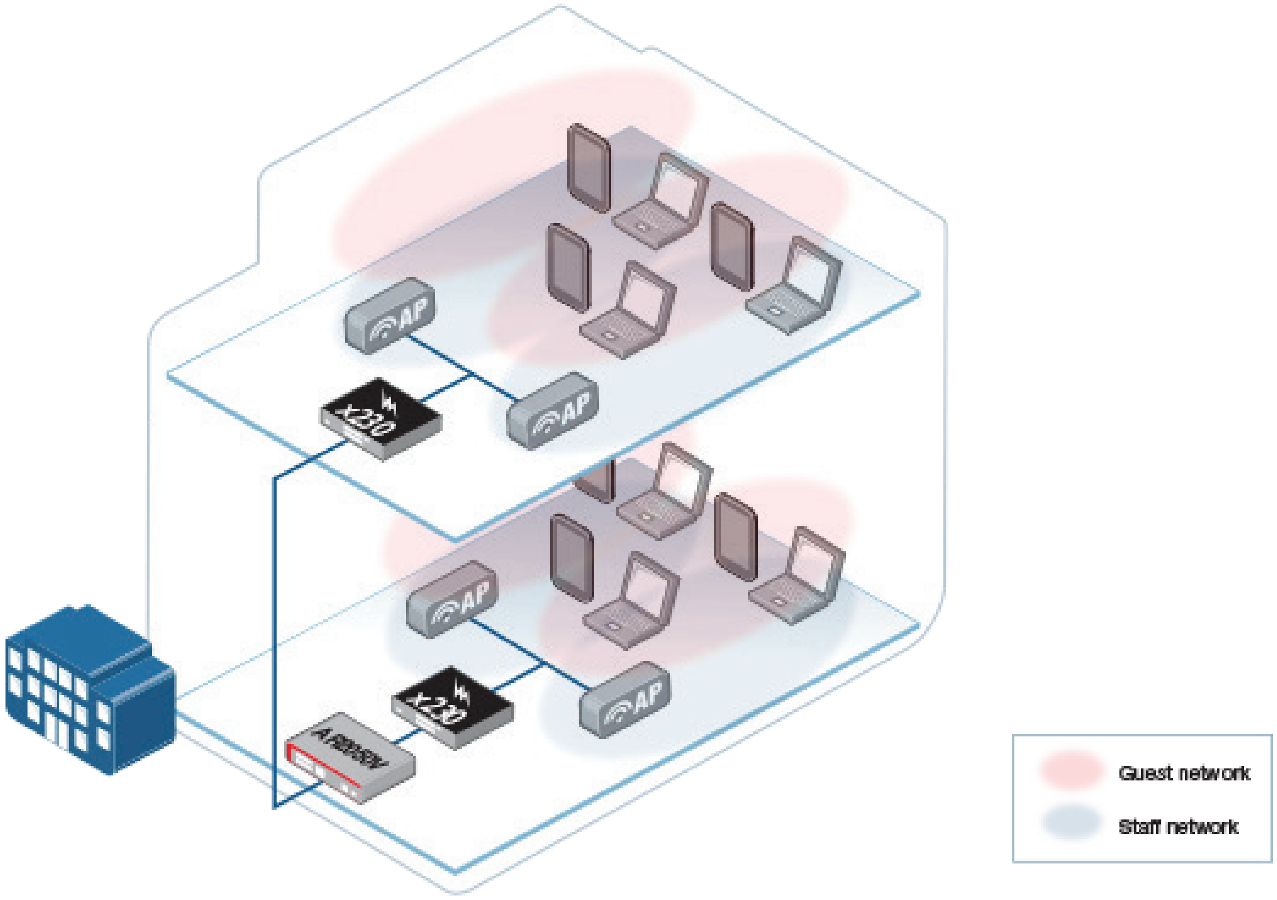
Automated network management

In addition to protecting and connecting modern networks, the AR2050V is fully supported by AMF.

Autonomous Management Framework (AMF) is a sophisticated suite of management tools that automate and simplify many day-to-day network administration tasks. Powerful features like centralized management, auto-backup, auto-upgrade, auto-provisioning and auto-recovery ensure streamlined networking. Growing the network can be accomplished with plug-and-play simplicity, and network node recovery is fully zero-touch.

As part of an AMF network, along with all of the network switches, the UTM Firewall and VPN Routers are automatically backed up, ensuring seamless recovery if required.

Key Solution



Autonomous Wireless LAN solution

Allied Telesis AWC offers solutions for two of the most common problems with Wireless LANs: initial setup complexity and on-going performance degradation. Initial WLAN set-up usually requires a site survey to achieve the best coverage; and performance of WLANs can often change over time as external sources of radio interference reduce coverage and bandwidth. These issues can be time-consuming to identify and resolve.

AWC features an intelligent process that automatically re-calibrates the signal strength and radio channel of each Access Point (AP) for optimal WLAN performance. This re-calibration is performed daily based on measurements taken from each AP to compensate for interference such as unscreened electrical equipment, changes to office layout, or neighbouring wireless networks.

When AWC is combined with the security features of the AR2050V, it becomes an ideal solution for branch offices and small businesses to both protect and manage the office network. AWC is an essential tool for busy network administrators to save time and money when deploying and managing WLANs.

Up to 5 TQ or MWS Series wireless APs can be managed using the built-in AWC functionality.

Note: For larger Wireless networks, Allied Telesis AR4050S UTM Firewall can manage a further 20 APs (25 max) with a feature license.

Features

Firewall

- Multi zone firewall with a built-in application list
- Application Layer Gateway (ALG) for FTP, SIP and H.323
- Bandwidth limiting control
- Firewall session limiting per user
- Bridging between LAN and WAN interfaces
- Intrusion Detection and Prevention System (IDS/IPS)
- User-defined URL blacklists and whitelists (block or allow HTTP and HTTPS access to specific Websites)
- DoS and DDoS attack detection and protection
- Maximum and guaranteed bandwidth control
- Static NAT (port forwarding), double NAT and subnet-based NAT
- Masquerading (outbound NAT)
- Enhanced NAT (static and dynamic)
- Security for IPv6 traffic

Networking

- Routing mode / bridging mode / mixed mode
- Static unicast and multicast routing for IPv4 and IPv6
- DS-Lite for connecting IPv4 networks over IPv6
- Dynamic routing (RIP, OSPF and BGP) for IPv4 and IPv6
- Flow-based Equal Cost Multi Path (ECMP) routing
- Dynamic multicasting support by IGMP and PIM
- Route maps and route redistribution (OSPF, BGP, RIP)
- Virtual Routing and Forwarding (VRF-Lite)
- Traffic control for bandwidth shaping and congestion avoidance
- Policy-based routing
- SD-WAN: performance measure and load balance WAN links
- PPPoE client with PADT support
- DHCP client, relay and server for IPv4 and IPv6
- Dynamic DNS client
- IPv4 and IPv6 dual stack
- Device management over IPv6 networks with SNMPv6, Telnetv6 and SSHv6
- Logging to IPv6 hosts with Syslog v6

Management

- Allied Telesis Autonomous Management Framework (AMF) enables powerful centralized management and zero-touch device installation and recovery
- Web-based GUI for device configuration and easy monitoring
- Industry-standard CLI with context-sensitive help
- Role-based administration with multiple CLI security levels
- Built-in text editor and powerful CLI scripting engine
- Comprehensive SNMPv2c/v3 support for standards-based device management
- Event-based triggers allow user-defined scripts to be executed upon selected system events
- Comprehensive logging to local memory and syslog
- Console management port on the front panel for ease of access
- USB interface allows software release files, configurations and other files to be stored for backup and distribution to other devices

Resiliency

- Policy-based storm protection
- Link Aggregation Control Protocol (LACP) on LAN ports
- Spanning Tree Protocol (STP, RSTP) with root guard
- Virtual Router Redundancy Protocol (VRRPv2/v3)

Diagnostic Tools

- Automatic link flap detection and port shutdown
- Optical Digital Diagnostic Monitoring (DDM)
- Ping polling for IPv4 and IPv6
- Port mirroring
- TraceRoute for IPv4 and IPv6

Authentication

- RADIUS authentication and accounting
- TACACS+ Authentication, Accounting and Authorization (AAA)
- Local or server-based RADIUS user database
- RADIUS group selection per VLAN or port
- Strong password security and encryption

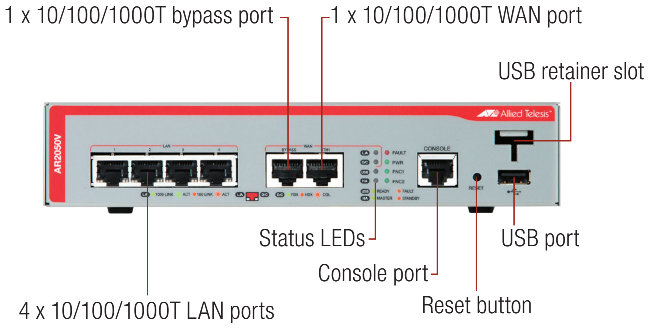
VPN Tunneling

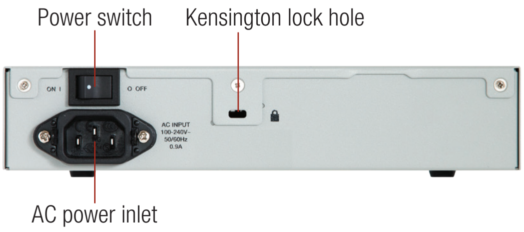
- Diffie-Hellman key exchange
- Secure encryption algorithms: AES and 3DES
- Secure authentication: SHA-1, SHA-256, SHA-512
- IKEv2 key management
- IPsec Dead Peer Detection (DPD)
- IPsec NAT traversal
- IPsec VPN for site-to-site connectivity
- VPN pass-through
- Dynamic routing through VPN tunnels (RIP, OSPF, BGP)
- Generic Routing Encapsulation (GRE) over IPv6
- Redundant VPN gateway
- SSL/TLS VPN for secure remote access

Wireless Controller AWC

- Allied Telesis AWC is an intelligent WLAN controller that automatically maintains optimal wireless coverage
- Manage up to five access points (APs)
- Rogue AP detection for increased WLAN security
- WEP/WPA personal or WPA enterprise, pre-shared key (WEP/WPA personal), RADIUS server (WPA enterprise)
- Wireless networks can have separate SSIDs, VLANs, security settings, etc.
- APs can belong to multiple networks each with different wireless settings, and can broadcast multiple SSIDs (Virtual AP)
- APs can be defined individually or in bulk using a common profile.
- AP radio settings can be configured automatically (default) or manually
- AP functions such as updating firmware, executing AWC calculations and applying calculation results can be run automatically based on a user-defined schedule
- AWC supports Allied Telesis TQ and MWS Series wireless access points

AR2050V SECURE VPN ROUTER





Specifications

	AR2050V
Processor & memory	
Security processor	800MHz dual-core
Memory (RAM)	512MB
Memory (Flash)	4GB
Security features	
Firewall	Application-aware packet inspection firewall
Application proxies	FTP, TFTP, SIP
Threat protection	DoS attacks, fragmented & malformed packets, blended threats & more
Tunneling & encryption	
IPsec site-to-site VPN tunnels	50
SSL VPN users	100
Encrypted VPN	IPsec, SHA-1, SHA-256, IKEv2, SSL/TLS VPN
Encryption	3DES, AES-128, AES-192, AES-256
Key exchange	Diffie-Hellman groups 2, 5, 14, 15, 16, 18
Dynamic routed VPN	RIP, OSPF, BGP, RIPng, OSPFv3, BGP4+
Point to point	Static PPP, L2TPv2 virtual tunnels, L2TPv3 Ethernet pseudo-wires
Encapsulation	GRE for IPv4 and IPv6
Management & authentication	
Logging & notifications	Syslog & Syslog v6, SNMPv2 & v3
User interfaces	Scriptable industry-standard CLI, Web-based GUI
Secure management	SSHv1/v2, strong passwords
Management tools	Allied Telesis Autonomous Management Framework™ (AMF) Autonomous Wave Control for wireless LAN APs (AWC) Vista Manager EX
User authentication	RADIUS, TACACS+, internal user database, Web authentication
Command authorization	TACACS+ AAA (Authentication, Accounting and Authorization)
Networking	
Routing (IPv4)	Static, Dynamic (BGP4, OSPF, RIPv1/v2), source-based routing, policy-based routing, VRF-Lite, SD-WAN
Routing (IPv6)	Static, Dynamic (BGP4+, OSPFv3, RIPng), policy-based routing, SD-WAN
Multicasting	IGMPv1/v2/v3, PIM-SM, PIM-DM, PIM-SSM, PIMv6
Resiliency	STP, RSTP
High availability	VRRP, VRRPv3, hardware controlled bypass port
Traffic control	8 priority queues, DiffServ, HTB scheduling, RED curves
IP address management	Static v4/v6, DHCP v4/v6 (server, relay, client), PPPoE
NAT	Static, IPsec traversal, Dynamic NAPT
Link aggregation	802.3ad static and dynamic (LACP)
VLANs	802.1Q tagging
Reliability features	
	Modular AlliedWare Plus operating system Full environmental monitoring of PSU, fan, temperature and internal voltages. SNMP traps alert network managers in case of any failure Variable fan speed control

	AR2050V
Hardware characteristics	
Input power	90 to 260V AC (auto-ranging), 47 to 63Hz
Max power consumption	14W
LAN ports	4 x 10/100/1000T RJ-45
WAN ports	1 x 10/100/1000T RJ-45
High Availability bypass ports	1 x 10/100/1000T RJ-45
Other ports	1 x USB, 1 x RJ-45 console
Product dimensions (H x W x D)	42.5mm (1.67 in) x 210mm (8.26 in) x 220mm (8.66 in)
Packaged dimensions (H x W x D)	112 mm (4.41 in) x 254 mm (10.00 in) x 360 mm (14.17 in)
Product weight	1.8 kg (4.0 lb) unpackaged, 2.5 kg (5.51 lb) packaged
Environmental specifications	
Operating temperature range	0°C to 45°C (32°F to 113°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 80% non-condensing
Storage relative humidity range	5% to 95% non-condensing
Operating altitude	2,000 meters maximum (6,600 ft)
Regulations and compliances	
EMC	EN55022 class A, FCC class A, VCCI class A
Immunity	EN55024, EN61000-3-levels 2 (Harmonics), and 3 (Flicker)
Safety Standards	UL60950-1, CAN/CSA-C22.2 No. 60950-1-03, EN60950-1, EN60825-1, AS/NZS 60950.1
Safety Certifications	UL, cUL, TuV
Reduction of Hazardous Substances (RoHS)	EU RoHS6 compliant, China RoHS compliant
IPv6 Ready	Phase 2 (Gold) Logo
Country of origin	
	China

Ordering information

AT-AR2050V-xx

1 x GE WAN and 4 x 10/100/1000 LAN

AT-RKMT-J15

Rack mount kit to install two devices side by side in a 19-inch equipment rack

AT-RKMT-J14

Rack mount kit to install one device in a 19-inch equipment rack

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
51 for encryption not enabled

3G/4G USB Modems

For a list of supported USB modems visit alliedtelesis.com

Related Products

AT-MWS600AP (Version 2.2.3)

Wireless Access Point with IEEE 802.11ac dual-band radio and embedded antennas

AT-MWS1750AP (Version 2.2.3)

Wireless Access Point with IEEE 802.11ac wave1 dual-band radio and embedded antennas

AT-MWS2533AP (Version 2.2.1, 2.2.3)

Wireless Access Point with IEEE 802.11ac wave2 dual-band radio and embedded antennas

AT-TQ4600-xx (Version 4.0.5)

Enterprise-Class Wireless Access Point with IEEE 802.11ac dual-band radio and embedded antenna

AT-TQ4400e-xx (Version 4.0.5)

Enterprise-Class Outdoor Wireless Access Point with IEEE 802.11ac dual-band radio