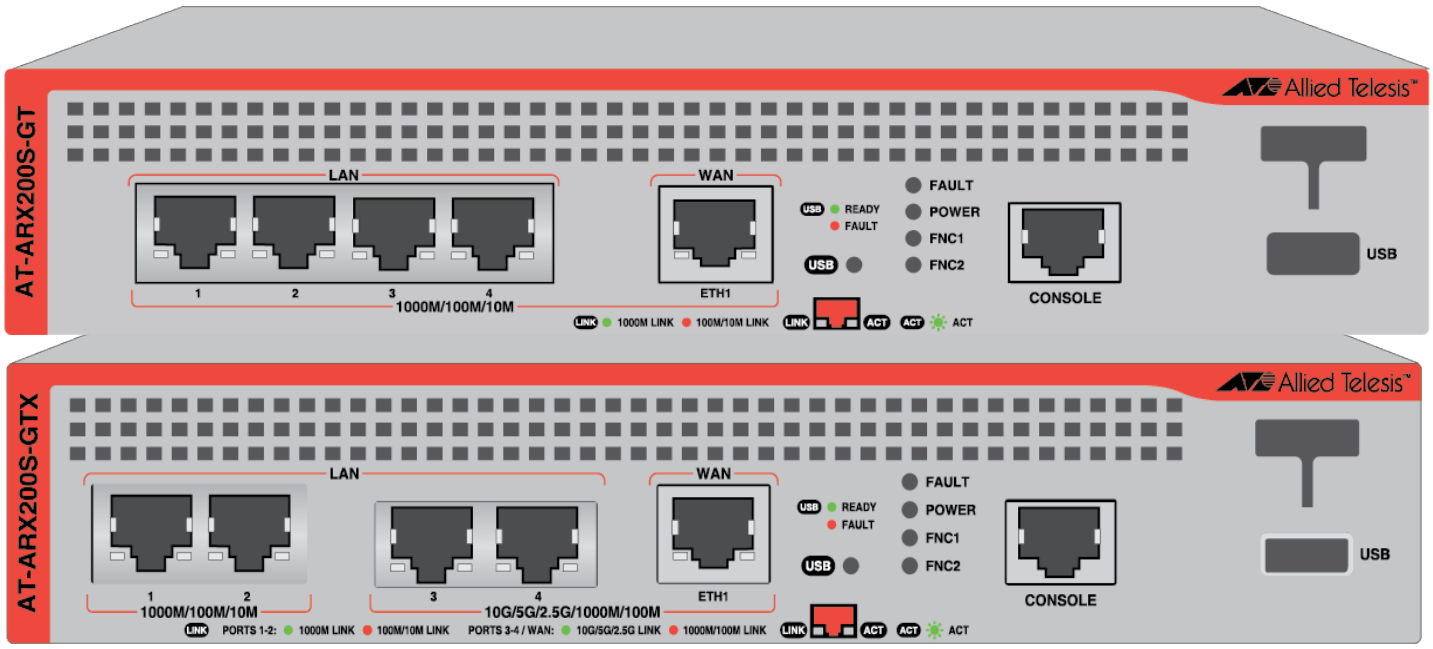
ARX200S Series

1/10G Router Series with Unified Threat Management Firewall, Virtual Private Networking, and Software-Defined WAN

ARX200S-GT

ARX200S-GTX



Installation Guide

613-003198 Rev. B

Electrical Safety Standards, Emissions Standards, and Regulatory Compliances

This product meets the following standards.

U.S. Federal Communications Commission
Radiated Energy Note: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Note: Modifications or changes not expressly approved of by the manufacturer or the FCC, can void your right to operate this equipment.

Industry Canada
This Class A digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Warning: In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Electrical Safety: EN 62368-1 (UL/EN/IEC)

Regulatory compliances for the product are listed here:

Communication (Wired Category)	IEEE 802.3, Overview and Architecture, 2000 IEEE 802.3u, Media Access Control (MAC) Paraeters, Physical Layer, Meium Attachment Units, and Repeater for 100Mbps Operation, Type 100BASE-T 1995. IEEE 802.3ab (1000BASE-T) IEEE 802.3bz (2.5G BASE-T, 5G BASE-T) IEEE 802.3an (10G BASE-T) IEEE 802.3x (flow control) IEEE 802.3az-2010 (Energy Efficient Ethernet)
Safety	EN 62368-1: 2014 ED2 CB IEC 62368-1: 2014 ED2 TUV RH T-mark

EMI (Electro Magnetic Interference)	47 FCC part 15 subpart B, Class A ICES-003 issue 7 EN 55032 2015+A11:2020 Class A CISPR 32: 2015 Class A VCCI 32-1 Class A UKCA RCM AS/NZS CISP32
EMS (Electro Magnetic Susceptibility)	IEC 61000-4-2:2009 IEC 61000-4-3:2020 IEC 61000-4-4:2012 IEC 61000-4-5:2014+A1:2017 IEC 61000-4-6 IEC 61000-4-8:2010 IEC 61000-4-11:2020+AC:2020 IEC 61000-3-2:2019+A1:2021 IEC 61000-3-3:2013+A2:2021 EN 55035
Japan WAN/Security/DSPR	JATE Article 34-8 JATE Article 34-10 JATE Article 34 (LAN 10M/100M/1000M/10G type D)
JGPSSI (Japanese Green Procurement Survey Standardization Initiative)	JIG level A

Contents

Figures

Tables

Preface

This guide contains the hardware installation instructions for the ARX200S Series of firewall routers. The guide contains instructions on how to install the devices on a table, in an equipment rack, or on a wall, and how to verify hardware operations. Also included are introductions to the management interfaces in the AlliedWare Plus management software, as well as the firewall and Unified Threat Management (UTM) features.

The preface contains the following sections:

Note
For support resources, refer to **www.alliedtelesis.com/services**. For hardware installation, configuration, and reference guides, refer to **alliedtelesis.com/library/search**.

Document Conventions

This document has the following conventions:

Note
Notes provide additional information.

Caution
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Warning
Warnings inform you that performing or omitting a specific action may result in bodily injury.

Translated Safety Statements

Important: Safety statements with the ✍ symbol are translated into multiple languages in **Translated Safety Statements** at **alliedtelesis.com/library/search**:

- Übersetzte Sicherheitshinweise (German):
  Wichtig: Sicherheitshinweise mit dem ✍ Symbol werden in **Translated Safety Statements** bei **alliedtelesis.com/library/search** in mehrere Sprachen übersetzt.
- Declaraciones de seguridad traducidas (Spanish):
  Importante: Las declaraciones de seguridad con el símbolo ✍ se traducen a varios idiomas en **Translated Safety Statements** en **alliedtelesis.com/library/search**.
- Consignes de sécurité traduites (French):
  Important: Les déclarations de sécurité avec le symbole ✍ sont traduites en plusieurs langues en **Translated Safety Statements** sur **alliedtelesis.com/library/search**.
- Dichiarazioni di sicurezza tradotte (Italian):
  Importante: Le dichiarazioni di sicurezza con il simbolo ✍ sono tradotte in più lingue in **Translated Safety Statements** su **alliedtelesis.com/library/search**.
- Översatta säkerhetsförklaringar (Swedish):
  Viktig: Säkerhetsföreskrifter med ✍ symbolen översätts till flera språk på **Translated Safety Statements** vid **alliedtelesis.com/library/search**.

Chapter 1
Overview

This chapter contains the following sections:

Front and Rear Panels

Figure 2 identifies the front panel components on the ARX200S-GT Router.

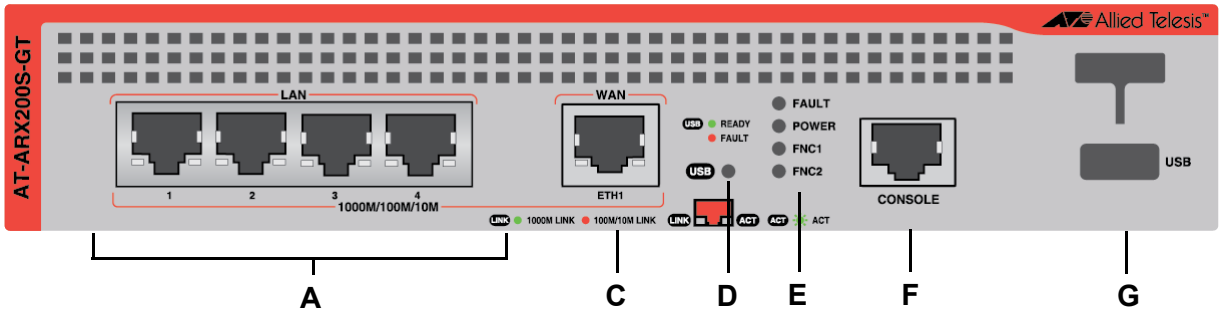


Figure 1. Front Panel Components on the ARX200S-GT Router

Figure 2 identifies the front panel components on theARX200S-GTX Router.

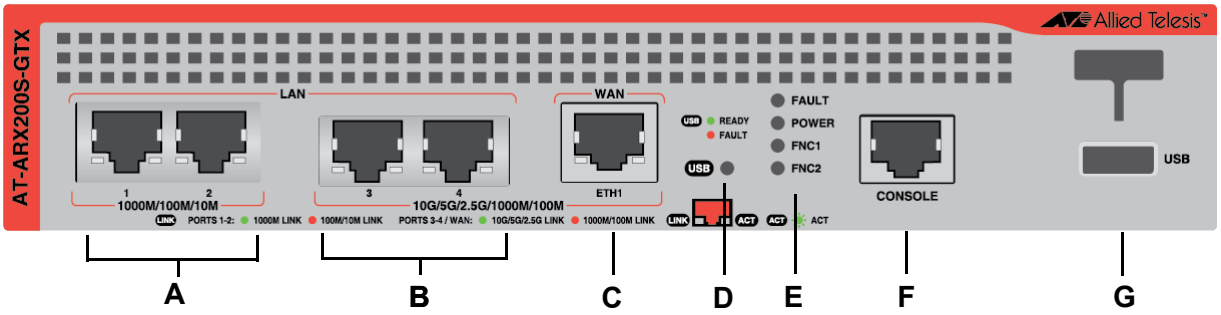


Figure 2. Front Panel Components on the ARX200S-GTX Router

Table 1 describes the front panel components.

Table 1. Front Panel Components on the ARX200S Router Series

Item	Router	Port Number or AW+[1] Identifier	Description
A	ARX200S-GT	Ports 1 to 4	10/100/1000M Copper Ethernet LAN ports with RJ45 connectors. Refer to “10/100/1000M LAN Port LEDs” on page 20.
	ARX200S-GTX	Ports 1 and 2	
B	ARX200S-GTX	Ports 3 and 4	100M/1000M/2.5G/5G/10G Copper Multi-Gigabit Ethernet LAN ports with RJ45 connectors. Refer to “Multi-Gigabit LAN Port LEDs” on page 21.

Table 1. Front Panel Components on the ARX200S Router Series (Continued)

Item	Router	Port Number or AW+[1] Identifier	Description
C	ARX200S-GT	ETH1	10/100/1000M Copper Ethernet WAN ETH1 port with RJ45 connector. Refer to “WAN ETH1 Port” on page 23.
	ARX200S-GTX	ETH1	100M/1000M/2.5G/5G/10G Copper Multi-Gigabit Ethernet WAN ETH1 port with RJ45 connector. Refer to “WAN ETH1 Port” on page 23.
D	ARX200S-GT ARX200S-GTX	-	USB port LED. Refer to “USB Port LED” on page 34.
E	ARX200S-GT ARX200S-GTX	-	System LEDs. Refer to “System LEDs” on page 28.
F	ARX200S-GT ARX200S-GTX	-	RJ45-style Console port for local management. Refer to “Console Port” on page 35 and “Starting a Management Session” on page 91.
G	ARX200S-GT ARX200S-GTX	USB	USB3.0 Type A port for a USB storage device or cellular modem. Refer to “USB Port” on page 31.

1. AlliedWare Plus management software.

Figure 3 illustrates the rear panel of the ARX200S-GT Router.

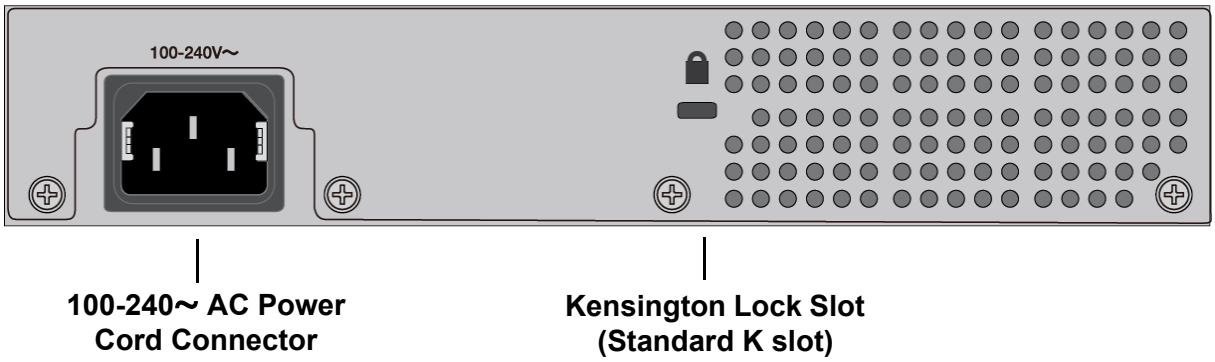


Figure 3. Rear Panel of the ARX200S-GT Router

Note
The ARX200S-GT Router is fanless.

Figure 4 illustrates the rear panel of the ARX200S-GTX Router.

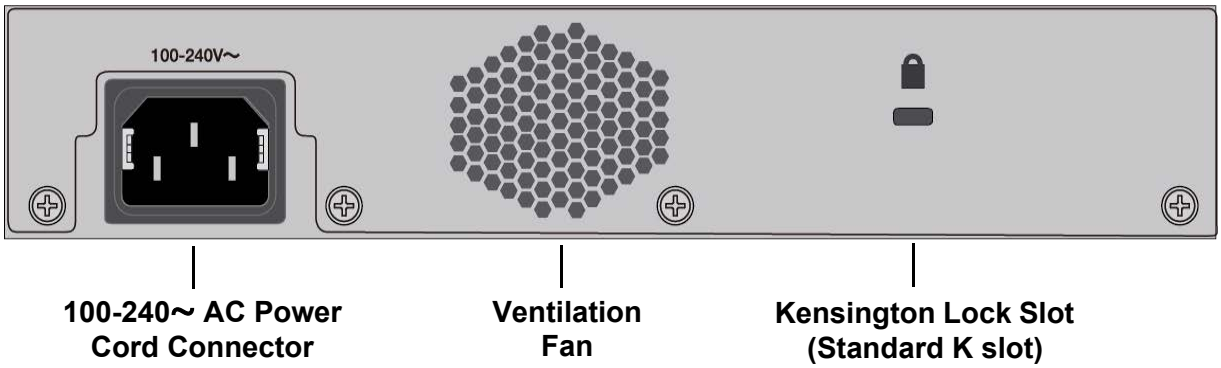


Figure 4. Rear Panel of the ARX200S-GTX Router

Note
The ARX200S-GTX Router has a single fan inside the rear panel. The airflow direction is from front to back.

Copper Ethernet LAN Ports

Ports 1 to 4 on the ARX200S-GT Router and ports 1 and 2 on the ARX200S-GTX Router are 10/100/1000M Copper Ethernet LAN ports with RJ45 connectors. Ports 3 and 4 on the ARX200S-GTX Router are 100M/1000M/2.5G/5G/10G Copper Multi-Gigabit Ethernet LAN ports with RJ45 connectors. The ports are described in the following sections:

- “Port Specifications,” next
- “10/100/1000M LAN Port LEDs” on page 20
- “Multi-Gigabit LAN Port LEDs” on page 21

Port Specifications

Here are common features of all copper LAN ports:

- Standard 8-pin RJ45 connectors
- Speed and activity LEDs
- Maximum copper cable operating distance: 100 meters (328 feet)

Note
For the minimum copper cable requirements, refer to “Cable Requirements” on page 51.

Here are the speeds and corresponding Ethernet standards for LAN ports 1 to 4 on the ARX200S-GT Router and LAN ports 1 and 2 on the ARX200S-GTX Router:

- 10M - IEEE802.3 (10BASE-T)
- 100M - IEEE 802.3u (100BASE-TX)
- 1000M (1G) - IEEE 802.3ab (1000BASE-T)

Here are the speeds and corresponding Ethernet standards for LAN ports 3 and 4 on the ARX200S-GTX Router:

- 100M - IEEE 802.3u (100BASE-TX)
- 1000M (1G) - IEEE 802.3ab (1000BASE-T)
- 2.5G/5G - IEEE 802.3bz (2.5GBASE-T/5GBASE-T)
- 10G - IEEE 802.3an (10GBASE-T)

Here are the default settings for all copper LAN ports:

- Default status: Enabled
- Default speed: Auto-Negotiation
- Default duplex mode: Auto-Negotiation
- MDI/MDIX wiring: Auto-MDI/MDIX

10/100/1000M LAN Port LEDs

The LEDs on the 10/100/1000M Copper Ethernet LAN ports are identified in Figure 5 and described in Table 2.

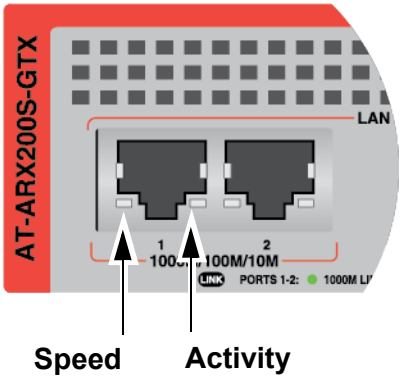


Figure 5. LEDs on the 10/100/1000M Copper Ethernet LAN Ports

Table 2. LEDs on the 10/100/1000M Copper Ethernet LAN Ports

LED	State	Description
Speed (left)	Solid Green	The port has established a link at 1000M to a network device.
	Solid Amber	The port has established a link at 10M or 100M to a network device.
	Off	Causes of this state can include: ❒ The remote device is powered off. Verify that the remote device is powered on. ❒ The port on the router or remote device is disabled. The command for enabling a router port is the NO SHUTDOWN command in the Interface mode. ❒ The copper cable is disconnected at the router or remote device. Verify that the cable is securely connected to the ports on the router and remote device. ❒ The copper cable is faulty. Try replacing the cable. ❒ The MDI/MDIX setting is incorrect. The command for setting the MDI setting on a router port is the POLARITY command in the Interface mode.

Table 2. LEDs on the 10/100/1000M Copper Ethernet LAN Ports

LED	State	Description
Speed (left) (continued)	Off	❒ The router is operating in the eco-friendly mode, with the port LEDs off. To disable the mode and turn on the LEDs, enter the NO ECOFRIEDNLY LED command in the Global Configuration mode.
Activity (right)	Flashing Green	The port is transmitting or receiving packets.
	Off	The port is not transmitting or receiving traffic. Refer to the description of the Speed LED for possible causes.

Multi-Gigabit LAN Port LEDs

The LEDs on the 100M/1000M/2.5G/5G/10G Multi-Gigabit Ethernet LAN ports 3 and 4 on the ARX200S-GTX Router are identified in Figure 6 and described in Table 3 on page 22.

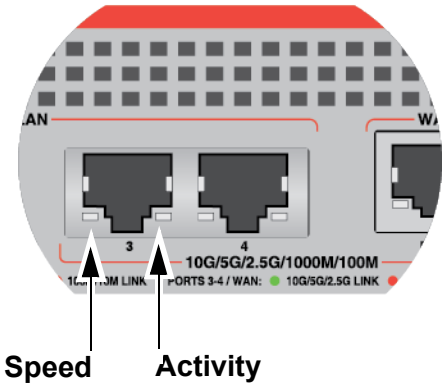


Figure 6. LEDs on the Multi-Gigabit Ethernet LAN Ports 3 and 4 on the ARX200S-GTX Router

Table 3. LEDs on the Multi-Gigabit Ethernet LAN Ports 3 and 4 on the ARX200S-GTX Router

LED	State	Description
Speed (left)	Solid Green	The port has established a link at 2.5G, 5G or 10G to a network device.
	Solid Amber	The port has established a link at 100M or 1000M to a network device.
	Off	The port is not linked to a network device. Refer to the description of the Speed LED in Table 2 on page 20 for possible causes.
Activity (right)	Flashing Green	The port is transmitting or receiving packets.
	Off	The port is not transmitting or receiving traffic. Refer to the description of the Speed LED in Table 2 on page 20 for possible causes.

Note
The pinouts of the Ethernet copper ports are provided in “RJ-45 Copper Port Pinouts” on page 148.

WAN ETH1 Port

The following sections introduce the WAN ETH1 port:

Port Standards

Here are the basic features:

- ❒ Standard 8-pin RJ45 connector
- ❒ Speed and activity LEDs
- ❒ 100 meters (328 feet) maximum operating distance

Here are the available speeds and corresponding Ethernet standards for the WAN ETH1 port on the ARX200S-GT Router:

- ❒ 10M - IEEE 802.3 (10BASE-T)
- ❒ 100M - IEEE 802.3u (100BASE-TX)
- ❒ 1000M - IEEE 802.3ab (1000BASE-T)

Here are the available speeds and corresponding Ethernet standards for the Multi-Gigabit WAN ETH1 port on the ARX200S-GTX Router:

- ❒ 100M - IEEE 802.3u (100BASE-TX)
- ❒ 1000M - IEEE 802.3ab (1000BASE-T)
- ❒ 2.5G/5G - IEEE 802.3bz (2.5GBASE-T/5GBASE-T)
- ❒ 10G - IEEE 802.3an (10GBASE-T)

Here are the default port settings:

- ❒ Speed: Auto-Negotiation
- ❒ Duplex mode: Auto-Negotiation
- ❒ MDI/MDIX wiring: Auto-MDI/MDIX
- ❒ Default routes: none
- ❒ Firewall protection: disabled

Routing Protocols

The WAN ETH1 port supports these IPv4 routing protocols:

- ❒ Static
- ❒ RIPv1/v2
- ❒ OSPF
- ❒ BGP4

The port supports the following IPv6 routing protocols:

- Static
- RIPng
- OSPFv3
- BGP4+

Port Encapsulations

The WAN ETH1 port supports the following encapsulation and IPv4-to-IPv6 transition protocols and techniques:

- IPv4 Point-to-Point Protocol over Ethernet (PPPoE) - Encapsulates Point-to-Point (PPP) packets inside Ethernet packets.
- IPv6 Internet Protocol over Ethernet (IPoE): IPv6 packets are encapsulated according to standard RFC 894, without PPPoE.
- IPv4 over IPv6 tunneling - IPv4 packets are assigned IPv6 headers when tunneled across IPv6 networks.
- Dual Stack Lite (DS-Lite) - IPv4 addresses in packets from hosts are translated by NAT before reaching the public network.
- Mapping of Address and Port with Encapsulation (MAP-E) - Maps IPv4 addresses to IPv6 addresses, and encapsulates IPv4 packets inside IPv6 packets (RFC 2473 IPv6 Tunneling) for transport across IPv6 networks.
- Lightweight 4over6 - An extension of DS-Lite that moves the Network Address and Port Translation (NAPT) function to the client tunnel from the centralized tunnel concentrator.
- IP in IP - Tunneling technique for encapsulating IP packets inside IP packets.

Note
Refer to the product's data sheet on the Allied Telesis website for the complete list of supported encapsulation and transition protocols.

Note
Not all features may be available on the ARX200S-GT Router. Refer to the product's data sheet on the Allied Telesis web site for the list of support features.

Firewall and Unified Threat Management Features

The router supports the following firewall and Unified Threat Management (UTM) features:

- Firewall Control: Defines rules that control the types of traffic that the router allows to enter or exit a trusted network from an untrusted networks, like the Internet.
- Traffic Control: Enables the router to evaluate which packets to retain or discard, as well as the order in which to transmit packets, during periods of heavy traffic.
- Web Control: Defines the types of websites that employees on trusted networks can access on untrusted networks through the router.
- URL Filtering: Permits or blocks access by web users to designated HTTP and HTTPS websites.
- Deep Packet Inspection: Enables the router to examine and categorize traffic according to the applications of the packets.
- IP Reputation: Guards the network from suspect IP addresses of external sources of spam, viruses and other malicious activity.
- Intrusion Prevention System: Protects the network by monitoring inbound and outbound traffic for suspicious or malicious traffic against a known signature database.
- Network Address Translation: Protects the IP addresses on a trusted network by replacing them with one or more shared public IP addresses when packets are transmitted on untrusted networks.
- Policy-based Routing: Controls the routes that packets are to take through a network by designating the next-hop assigned to application packets and traffic flows.
- Software-Defined Wide Area Networks: Enables the router to evaluate the transmission qualities of the WAN and VPN connections and then direct traffic flows over connections best suited to the application types.
- Web Redirect: Redirects ingress HTTP client requests to a specified URL.
- UTM Offload: Offloads the operations of several UTM security services from the router to another physical or virtual device, to improve the router's performance.

Note
Not all features may be available on the ARX200S-GT Router. Refer to the product's data sheet on the Allied Telesis web site for the list of support features.

For basic information, refer to Chapter 8, "Introduction to Firewall and Unified Threat Management Features" on page 115.

Note
Some features come standard with the router, while others require a license or subscription with a third-party provider. Additionally, some features may not be available during the initial release of the product. Refer to the product's data sheet for more information.

Port LEDs

The two LEDs on the WAN ETH1 port are identified in Figure 7 and defined in Table 4.

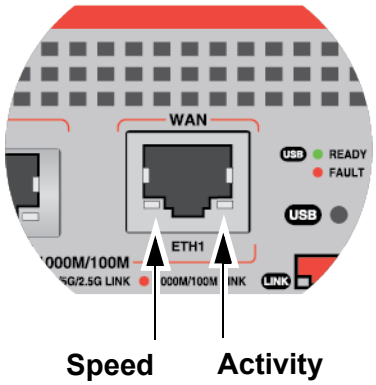


Figure 7. LEDs on the WAN ETH1 Port

Table 4. LEDs on the WAN ETH1 Port

LED	Router	State	Description
Speed (left)	ARX200S-GT	Solid Green	The port is linked at 1000M to a network device.
		Solid Amber	The port is linked at 10M or 100M to a network device.
	ARX200S-GTX	Solid Green	The port is linked at 2.5G, 5G or 10G to a network device.
		Solid Amber	The port is linked at 100M or 1000M to a network device.
	ARX200S-GT ARX200S-GTX	Off	Causes of this state can include: ❒ The remote device is powered off. Verify that the remote device is powered on.

Table 4. LEDs on the WAN ETH1 Port (Continued)

LED	Router	State	Description
Speed (left) (continued)	ARX200S-GT ARX200S-GTX	Off	❒ The port on the router or remote device is disabled. The command for enabling a router port is the NO SHUTDOWN command in the Interface mode. ❒ The copper cable is disconnected at the router or remote device. Verify that the cable is securely connected to the ports on the router and remote device. ❒ The copper cable is faulty. Try replacing the cable. ❒ The MDI/MDIX setting is incorrect. The command for setting the MDI setting on a router port is the POLARITY command in the Interface mode. ❒ The router is operating in the eco-friendly mode, with the port LEDs off. To disable the mode and turn on the LEDs, enter the NO ECOFRIEDNLY LED command in the Global Configuration mode.
Activity (right)	ARX200S-GT ARX200S-GTX	Flashing Green	The port is transmitting or receiving packets.
		Off	The port is not transmitting or receiving network traffic. Refer to the Speed LED Description for possible causes.

System LEDs

The system LEDs are shown in Figure 8 and described in Table 5.

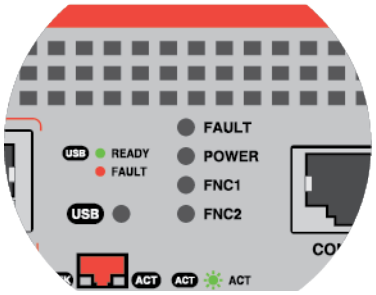


Figure 8. System LEDs

Table 5. System LEDs

LED	State	Description
Fault	1 Red Flash	The ARX200S-GTX Router detects a problem with the internal fan on the rear panel. Use the SHOW SYSTEM ENVIRONMENT command to view the internal temperature and fan status. This applies only to the ARX200S-GTX Router, which has one internal fan. The ARX200S-GT Router is fanless.
	2 Red Flash	The router detects a DC voltage that is either too high or too low on its circuit board. To view the circuit board voltages, use the SHOW SYSTEM ENVIRONMENT command in the User Exec and Privileged Exec modes in the CLI.
	6 Red Flashes	The router is overheating. Use the SHOW SYSTEM ENVIRONMENT command to view the internal temperature and fan status. The maximum ambient temperatures for the routers are 50°C (122°F) for the ARX200S-GT Router and 60°C (140°F) for the ARX200S-GTX Router.
	Off	The router is operating normally or is powered off.

Table 5. System LEDs (Continued)

LED	State	Description
Power	Solid Green	The router is receiving AC power within the approved operating range and is operating normally. Refer to “Power and Environmental Specifications” on page 144.
	Off	The router is not receiving AC power. Possible causes of this condition are: ❒ The AC power cord is disconnected. ❒ The AC power source is powered off. ❒ The AC power source has failed. ❒ The router overheated and shutdown. ❒ The router experienced a hardware or software failure. ❒ The router shutdown from a power surge. ❒ The power supply failed. ❒ The power cord is faulty.
FNC1 and FNC2	Solid Green	The router has activated a trigger in response to an event defined in a script. You can create scripts and triggers to automate the execution of commands in response to specific events. If only one FNC LED is on, the router activated one trigger. If both FNC LEDs are on, the router activated two or more triggers. For instructions, refer to the *Triggers Feature Overview and Configuration Guide* on the Allied Telesis web site.
	Off	The router is not performing any events in its trigger scripts, or no scripts are defined.

eco-friendly Mode

You can toggle the port LEDs on and off with the ECOFRIENDLY LED and NO ECOFRIENDLY LED commands in the Global Configuration mode in the command line interface of the AlliedWare Plus management software. The commands are shown here:

- ECOFRIENDLY LED command - Turns off the LEDs.
- NO ECOFRIENDLY LED command - Turns on the LEDs.

You might turn off the LEDs to conserve electricity when you are not monitoring the device. When the LEDs are turned off, the router is operating in the low power eco-friendly mode. Turning off the port LEDs does not interfere with the network operations of the router.

The AlliedWare Plus management software also has a command that blinks all the port LEDs so that you can quickly identify a specific unit among the devices in an equipment rack. It is the FINDME command. The command works even if the port LEDs are turned off.

Note
Before checking or troubleshooting network connections to the ports on the router, you should always verify that the LEDs are on by issuing the NO ECOFRIENDLY LED command in the Global Configuration mode of the command line interface.

USB Port

The USB port on the front panel of the router supports the following devices:

- ❒ "USB Storage Device," next
- ❒ "USB Cellular Modem" on page 34

For descriptions of the port LED, refer to "USB Port LED" on page 34.

USB Storage Device

The AlliedWare Plus operating system has several commands that allow you to specify a USB storage device in the USB port as a source or destination of a management function. For example, you can copy the router's startup configuration file from its flash memory to a USB storage device to maintain backup copies or transfer its configuration to another router. Table 6 lists examples of management functions and commands that support a USB storage device.

Table 6. Examples of Functions that Use a USB Storage Device

Function	AlliedWare Plus Command
File and Configuration Management	
Configure the router with a configuration file on the USB storage device the next time it boots.	BOOT CONFIG-FILE
Direct the router to a USB storage device for the AlliedWare Plus operating system the next time it boots.	BOOT SYSTEM
Copy files to or from a USB storage device, or create duplicate files on the storage device or to restore files on the router.	COPY
Save debug files on a USB storage device to diagnose and troubleshoot network issues.	COPY DEBUG MOVE DEBUG
Save the running-config file on a USB storage device. The file contains the router's current configuration, including commands not yet saved in the startup-config file.	COPY RUNNING-CONFIG

Table 6. Examples of Functions that Use a USB Storage Device

Function	AlliedWare Plus Command
Save the startup-config file on a USB storage device. The file contains the router's currently saved configuration settings.	COPY STARTUP-CONFIG
Save autoboot.txt files on a USB storage device. The router uses the files to restore a release file and/or configuration file to its file system.	CREATE AUTOBOOT
Save a directory file on a USB storage device. The file contains a list of all the visible files in the router's directory file system.	DIR
Close all open files and stop all management actions on a USB storage device. You should always perform this command before removing a storage device from the drive, to prevent corrupting data files.	UNMOUNT
Logging	
Save syslog messages in a file on a USB storage device.	LOG EXTERNAL
Delete the syslog file on a USB storage device.	CLEAR LOG EXTERNAL
Copy the buffered log onto a USB storage device.	COPY BUFFERED-LOG
Copy the permanent log onto a USB storage device.	COPY PERMANENT-LOG
USB Device	
Display information about a USB device.	SHOW SYSTEM USB
Map a specific USB device to a mode-switch configuration file.	USB MODE-SWITCH

Table 6. Examples of Functions that Use a USB Storage Device

Function	AlliedWare Plus Command
URL Filtering	
Specify a blacklist file on a USB storage device. The file contains a list of URLs to be blocked by URL filtering.	BLACKLIST
Specify a whitelist file on a USB storage device. The file contains a list of URLs to be permitted by URL filtering.	WHITELIST
Local RADIUS Server	
Manage files of local RADIUS server users.	Refer to the “Local RADIUS Server Commands” chapter in *Command Reference: ARX200S UTM Firewall Running AlliedWare Plus.*
Allied Telesis Management Framework (AMF)	
Manage Allied Telesis Management Framework (AMF) files.	Refer to the “Allied Telesis Management Framework (AMF) Commands” chapter in *Command Reference: ARX200S UTM Firewall Running AlliedWare Plus.*
Trigger	
Configure a trigger that the router performs when a USB storage device is inserted in or removed from the USB port.	TYPE USB

Here are the guidelines to using the USB drive with a USB storage device:

- ❒ The USB port is USB v3.0 compatible.
- ❒ The router automatically detects when a storage device is inserted in the USB drive. No command is required.
- ❒ Operating the router with a storage device in the USB drive is optional.

Caution
You should always enter the UNMOUNT USB command in the AlliedWare Plus management software before removing a storage device from the USB port, to avoid corrupting data files.

USB Cellular Modem

The USB port also supports a USB cellular modem. The router can use a cellular modem as a secondary connection to the outside network through a wireless service provider, in the event the WAN ETH1 port loses connection to its service provider. The router supports the following wireless networks:

- 3G: Low speed wireless connection that employs a serial connection between the router and modem.
- 4G/LTE: High speed wireless connection that creates an Ethernet type connection between the router and modem.
- 5G: Higher download speed wireless connection, also with an Ethernet type connection between the router and modem.

In most cases, you will want the router to use the WAN ETH1 port as its primary port for routing traffic outside the trusted network, and reserve the USB cellular modem as a backup port. You control this by setting the priorities of the routes with the administrative distances parameter, which has the range of 1 to 255. The lower the value, the higher a route's priority. By assigning lower administrative distances to the routes on the WAN ETH1 port than those on the USB port, the WAN ETH1 port and its routes will have the higher priorities. As a result, the USB port will act as a redundant connection to the outside network should the connection on the WAN ETH1 port be lost.

For configuration and command instructions, refer to the *USB Cellular Modem Feature Overview and Configuration Guide*. Cellular modems are not available from Allied Telesis. For a list of supported modems, refer to the *3G/4G USB Compatibility* document.

USB Port LED

Table 7 describes the USB port LED.

Table 7. USB Port LED

State	Description
Solid Green	The router detects a device in the USB port and can access it.
Solid Amber	The router cannot access the device in the USB port because of a fault condition. The problem may be with the device. Try replacing the USB device with another device.
Off	The USB port does not have an installed device.

Console Port

You use the Console port with its RJ45 connector to manage the router with the command line interface in the AlliedWare Plus management software. This management is called local management because it is not conducted over a network. Local management sessions typically have to be performed at the physical location of the router. The Console port has these settings:

- Default baud rate: 9600 bps (Range is 9600 to 115200 bps)
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Note
These settings are for a DEC VT100 or ANSI terminal, or an equivalent terminal emulation program.

Local management sessions require a terminal, computer, or laptop with an RS-232 serial port or USB port, and a terminal emulator, such as PuTTy.

Local management sessions also require a management cable. If your computer has an RS-232 port, refer to “RJ-45 Style Serial Console Port Pinouts” on page 149 and “Console Management Cable with DB-9 Female and RJ-45 Connectors” on page 150 for the cable wiring specifications.

If your computer has a USB port, you may purchase a USB-to-Serial converter that is compatible with its operating system. An example is the VT-Kit3 converter from Allied Telesis. It has a USB-A male connector that connects to a USB port on your workstation. Refer to Figure 9.

Figure 9. VT-Kit3 Management Cable

You connect the cable to the Console port on the router with a standard, straight-through Ethernet cable. Refer to Figure 10. The VT-Kit3 management cable with its software are sold separately.

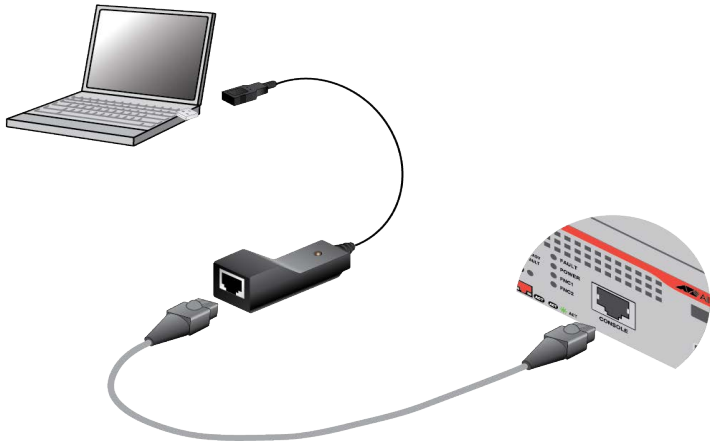


Figure 10. Connecting to the Console Port for Local Management with the VT-Kit3 Management Cable

For instructions on how to start a local management session on the router, refer to “Console Port” on page 92.

Power Supply and Fan Assemblies

The router has one internal power supply. The power supply is not field-replaceable. Refer to “Power and Environmental Specifications” on page 144 for the input voltage ranges.

Warning
The power cord is used as a disconnection device. To de-energize equipment, disconnect the power cord. E3

The router supports the following power savings features:

- The router supports IEEE 802.3az Energy-Efficient Ethernet (EEE). EEE is an energy saving feature that reduces power consumption during periods of no data activity. The router saves electricity by placing the Ethernet circuitry in a special sleep mode when all the ports are inactive. When data activity resumes, the circuitry automatically resumes normal operations.
- The router includes an eco-friendly mode for turning off port LEDs to save power. Refer to “eco-friendly Mode” on page 30.

The ARX200S-GTX Router has one internal fan on the rear panel. The ventilation direction is front-to-back, with the fan drawing air out of the router. The AlliedWare Plus management software issues alerts if it detects problems with the fan. To view fan status, use the SHOW SYSTEM ENVIRONMENT command. The fan assembly is not field-replaceable.

The ARX200S-GT Router is fanless.

Note
Before installing the router, be sure to read and follow the guidelines in “Choosing a Site for the Router” on page 43. The site should provide adequate airflow to prevent the device from overheating. If the device overheats in an environment that does not take into account the guidelines, the warranty of the device might be voided. Consult Allied Telesis when assistance is needed.

Chapter 2

Beginning the Installation

The chapter contains the following sections:

Reviewing Safety Precautions

Review the following safety precautions before beginning the installation procedure.

Note
Safety statements that have the ⁂ symbol are translated into multiple languages in the *Translated Safety Statements* document at **www.alliedtelesis.com/documents/translated-safety-statements**.

Note
Les consignes de sécurité portant le symbole ⁂ sont traduites dans plusieurs langues dans le document *Translated Safety Statements,* disponible à l'adresse **www.alliedtelesis.com/documents/translated-safety-statements**.

Warning
To prevent electric shock, do not remove the cover. No user-serviceable parts inside. This unit contains hazardous voltages and should only be opened by a trained and qualified technician. To avoid the possibility of electric shock, disconnect electric power to the product before connecting or disconnecting the LAN cables. ⁂ E1

Warning
Do not work on equipment or cables during periods of lightning activity. ⁂ E2

Warning
The power cord is used as a disconnection device. To de-energize equipment, disconnect the power cord. ⁂ E3

Warning
Class I Equipment. This equipment must be earthed. The power plug must be connected to a properly wired earth ground socket outlet. An improperly wired socket outlet could place hazardous voltages on accessible metal parts. ⁂ E4

Note
Pluggable Equipment. The socket outlet shall be installed near the equipment and shall be easily accessible. E5

Caution
Air vents must not be blocked and must have free access to the room ambient air for cooling. E6

Warning
Operating Temperature. The maximum ambient temperatures for the routers are 50°C (122°F) for the ARX200S-GT Router and 60°C (140°F) for the ARX200S-GTX Router.

Note
All Countries: Install product in accordance with local and National Electrical Codes. E8

Warning
Only trained and qualified personnel are allowed to install or replace this equipment. E14

Caution
Circuit Overloading: Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern. E21

Caution
Risk of explosion if battery is replaced by an incorrect type. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions. E22

Warning
Mounting of the equipment in the rack should be such that a hazardous condition is not created due to uneven mechanical loading. E25

Note
Use dedicated power circuits or power conditioners to supply reliable electrical power to the device. E27

Caution
The chassis may be heavy and awkward to lift. Allied Telesis recommends that you get assistance when mounting the chassis in an equipment rack. E28

Note
If the device is installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than the room ambient temperature. Therefore, consideration should be given to installing the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature (Tmra). E35

Caution
Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised. E36

Warning
Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuits (e.g., use of power strips). E37

Caution
The unit does not contain serviceable components. Please return damaged units for servicing. E42

Warning
Devices should not be stacked on top of one another on a table or desktop because that could present a personal safety hazard if you need to move or replace devices. E76

Choosing a Site for the Router

Site and enclosure requirements are described in the following sections:

- ❒ “Site Requirements,” next
- ❒ “Enclosure Requirements” on page 44

Note
The ARX200S-GT Router is fanless.

Note
The ARX200S-GTX Router has a single fan on the rear panel. The airflow direction inside the device is from front-to-back.

Site Requirements

Observe these site requirements when planning the installation.

- ❒ You should verify that the temperature range of the installation site is suitable for the device and that there is adequate airflow for ventilation around the unit for cooling. The operating temperature range of the router is provided in “Power and Environmental Specifications” on page 144.
- ❒ If you plan to install the device in an equipment rack, verify that the rack is safely secured so that it will not tip over. Devices in a rack should be installed starting at the bottom, with the heavier devices near the bottom of the rack.
- ❒ If you plan to install the device on a table, verify that the table is level and stable.
- ❒ The power outlet should be located near the device and be easily accessible.
- ❒ The site should allow for easy access to the ports on the front of the device so that you can easily connect and disconnect cables, and view the port and system LEDs.
- ❒ Do not install the device in a wiring or utility box without adequate airflow for cooling. Otherwise, the device might overheat and fail. Refer to “Enclosure Requirements” on page 44.
- ❒ The site should not expose the device to moisture or water.
- ❒ The site should be a dust-free environment.
- ❒ The site should include dedicated power circuits or power conditioners to supply reliable electrical power to the network devices.
- ❒ The site should not expose the copper cabling to sources of electrical noise, such as radio transmitters, broadband amplifiers, power lines, electric motors, and fluorescent fixtures.

- ❒ The ports on the device are suitable for intra-building connections, or where non-exposed cabling is required.
- ❒ Do not place objects on top of the device.

Warning
Devices should not be stacked on top of one another on a table or desktop. That could present a personal safety hazard if you need to move or replace devices. E76

- ❒ Ethernet cables connected to outdoor equipment, such as CCTVs mounted on poles, might be subjected to surges from lightning or power cross events. Properly rated primary protection devices must be installed on the cables before connecting them to the router.
- ❒ The cables should not be exposed to sources of electrical noise, such as radio transmitters, broadband amplifiers, power lines, electric motors, and fluorescent fixtures.

Enclosure Requirements

Observe these guidelines when installing the router in an enclosure:

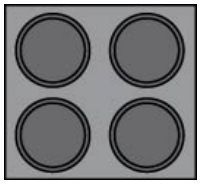
- ❒ Verify that the enclosure has adequate airflow so that the device does not overheat.
- ❒ Select an enclosure that is large enough for the device and all other included equipment.
- ❒ The enclosure size must be determined by considering multiple factors, including the outside ambient temperature, total heat generated by the installed equipment, sealed or unsealed enclosure type, enclosure material, paint color, mounting method (wall, pole, ground, etc.), and sun exposure. The smaller enclosure size you choose, the higher the risk of overheating.

Note
If the product overheats in an enclosure that was selected without taking into account these factors, the warranty of the product might be voided. Consult Allied Telesis when assistance is needed.

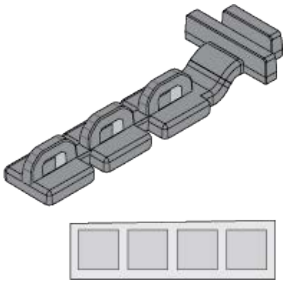
- ❒ The enclosure's BTU/hour rating must be higher than the total BTU/hour values of installed equipment, over the expected operating temperature range. For the operating temperature ratings, refer to Table 18, "ARX200S-GTX Router Environmental Specifications" on page 145.
- ❒ Be sure to review the enclosure's installation guide for rules and restrictions on site requirements, and to follow all guidelines and safety warnings.

Unpacking the ARX200S-GTX Router

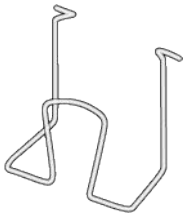
Figure 11 lists the accessory items included in the shipping box with the ARX200S Router Series.



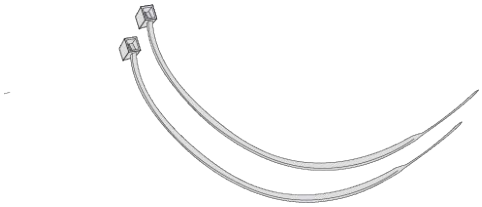
Four bumper feet for tabletop installation



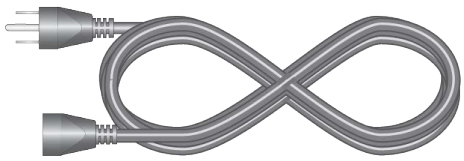
USB device retainer with insulator tape



One AC power cord clip



Two twist ties for the device in the USB drive



One AC power cord

Figure 11. Accessory Items Included with the ARX200S Router Series

The power cord that comes with the product will have one of the AC power connectors in Figure 12. You should verify that the connector on the power cord in the shipping box is correct for your country.

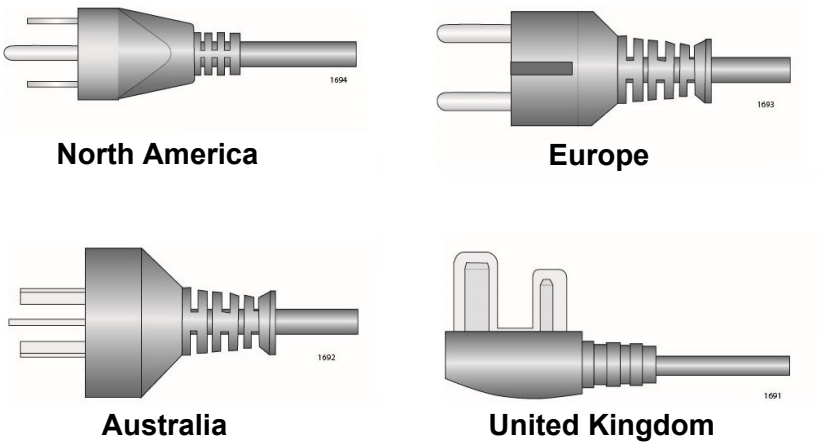


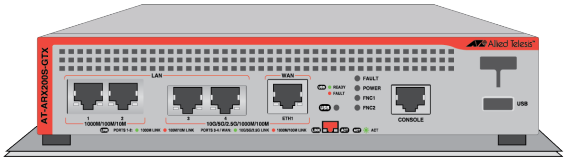
Figure 12. Power Cords

Note
Please retain the original packaging material in the event you need to return the unit to Allied Telesis.

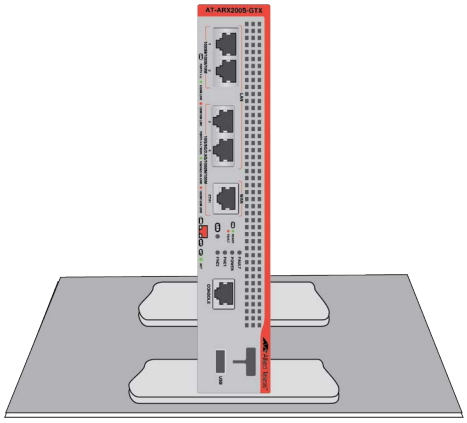
Note
If any item is missing or damaged, contact your Allied Telesis sales representative for assistance.

Installation Options

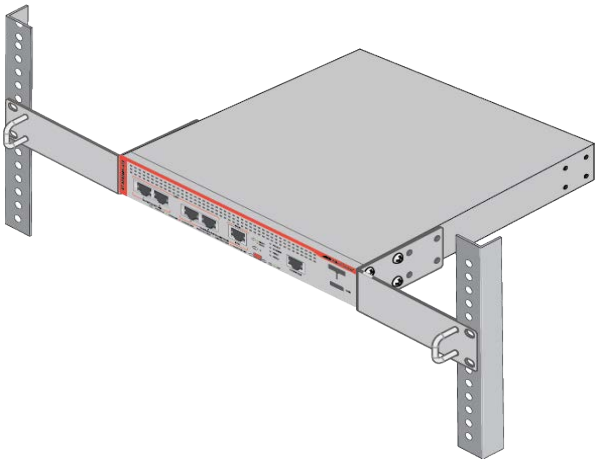
Figure 13 and Figure 14 on page 48 illustrate the installation options for the ARX200S Router Series. The illustrations show the ARX200S-GTX Router. The ARX200S-GT Router has the same installation options.



Installation on a table or desktop with the bumper feet included with router.

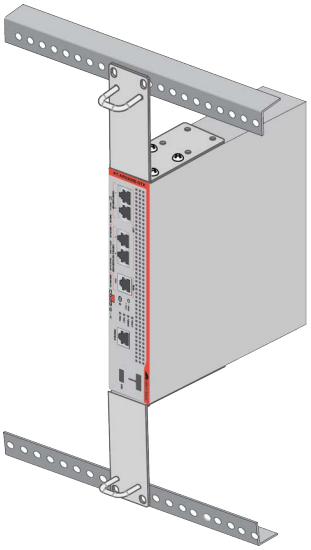


Vertical installation on a table or desktop with the STND-J03 kit. Kit sold separately.

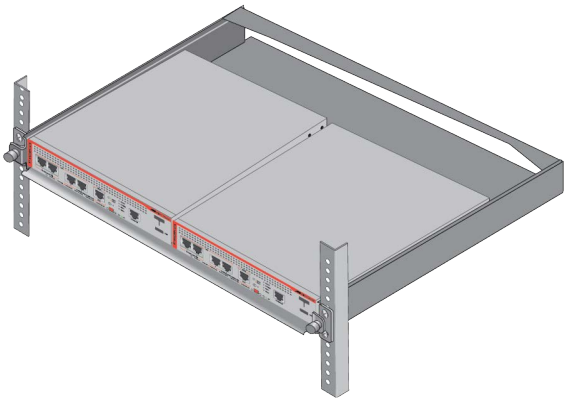


Standard 19-inch horizontal equipment rack with the RKMT-J14 equipment rack brackets kit. Kit sold separately.

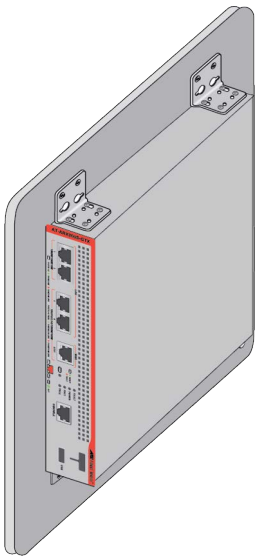
Figure 13. Installation Options for the ARX200S Router Series



Standard 19-inch vertical equipment rack with the RKMT-J14 equipment rack brackets kit. Kit sold separately.



Standard 19-inch horizontal equipment rack with the RKMT-J15 equipment rack tray kit. Kit sold separately.



Vertical wall installation with the BRKT-J24 wall brackets kit. Kit sold separately.

Figure 14. Installation Options for the ARX200S Router Series (Continued)

Hardware Options

The following hardware options for the router are sold separately.

STND-J03 Kit

The STND-J03 kit, shown in Figure 15, lets you install the router vertically on a table or desktop, as illustrated in Figure 13 on page 47. For instructions, refer to “Installing the Router with the STND-J03 Kit” on page 58.

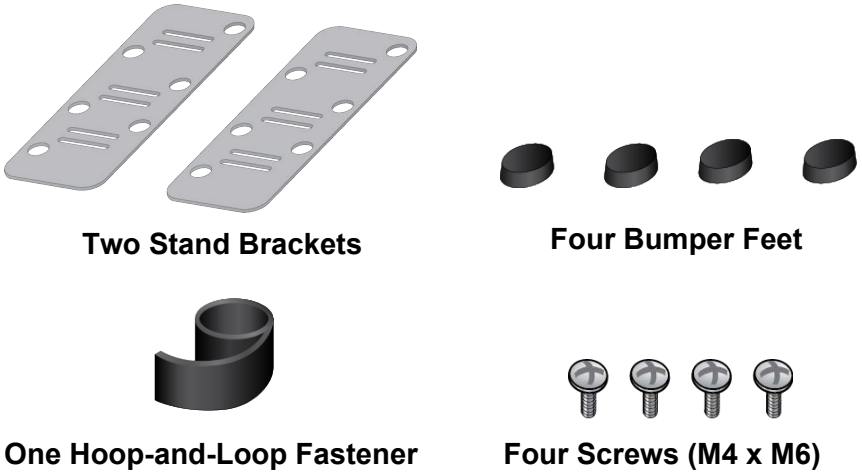


Figure 15. STND-J03 Kit

RKMT-J14 Equipment Rack Brackets Kit

You can install the router horizontally or vertically in a standard 19-inch equipment rack with the RKMT-J14 brackets kit, shown in Figure 16. For instructions, refer to “Installing the Router in an Equipment Rack with the RKMT-J14 Brackets Kit” on page 64.

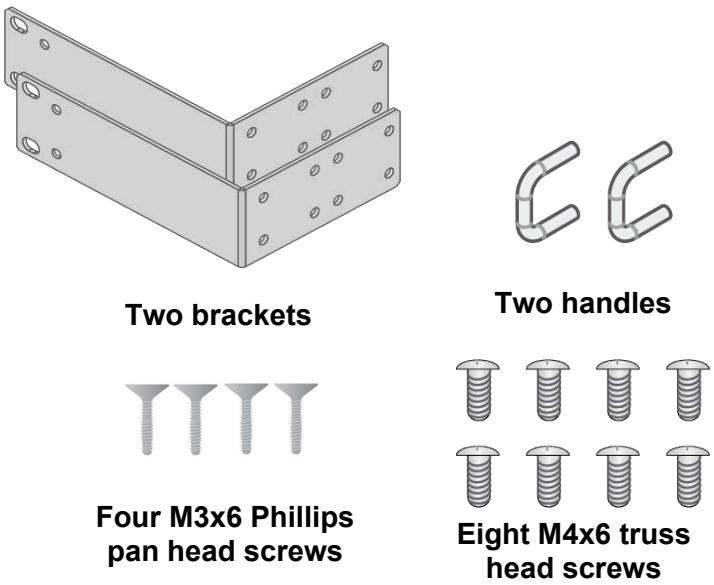


Figure 16. RKMT-J14 Equipment Rack Brackets Kit

RKMT-J15 Equipment Rack Brackets Kit

You can install two routers horizontally side-by-side in a standard 19-inch equipment rack with the RKMT-J15 equipment rack tray. Refer to Figure 17. For instructions, refer to Chapter 4, “Installing the Router in an Equipment Rack with the RKMT-J15 Equipment Rack Tray” on page 69.

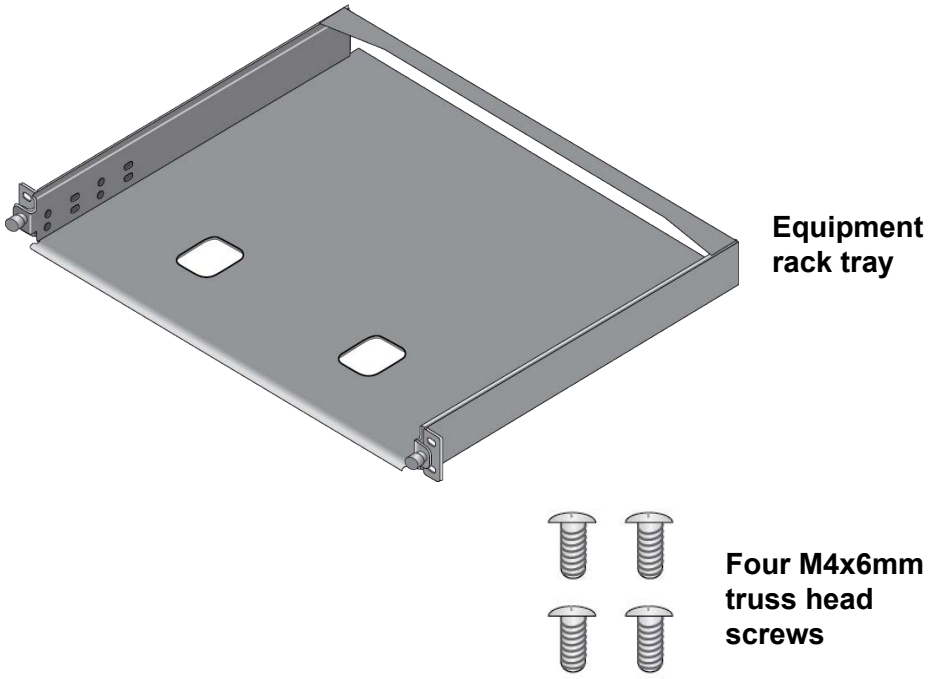


Figure 17. RKMT-J15 Equipment Rack Tray Kit

BRKT-J24 Wall Brackets Kit

Installing the router on a wall requires the BRKT-J24 wall brackets kit, shown in Figure 18. For instructions, refer to Chapter 5, “Installing the Router on a Wall” on page 75.

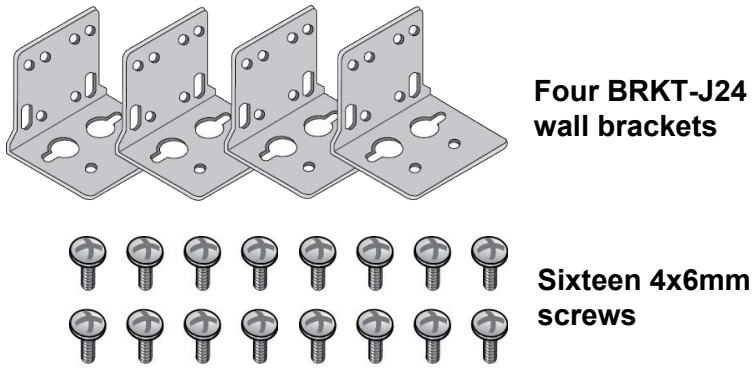


Figure 18. BRKT-J24 Wall Brackets Kit

Cable Requirements

Table 8 lists the minimum copper cable requirements for the following 10M/100M/1000M LAN ports

- LAN ports 1 to 4 and the WAN ETH1 port on the ARX200S-GT Router
- LAN ports 1 and 2 on the ARX200S-GTX Router:

Table 8. 10M/100M/1000M Minimum Cable Requirements

Speed	Minimum Copper Cable Requirements
10M/100M	Standard TIA/EIA 568-compliant Category 5, 100 ohm unshielded cabling, complying with IEEE 802.3u 100Base-TX specifications.
1000M	Standard TIA/EIA 568-A-compliant Category 5 or TIA/EIA 568-B-compliant Enhanced Category 5 (Cat 5e) unshielded cabling.

Table 9 Lists the minimum copper cable requirements for the Multi-Gigabit LAN ports 3 and 4, and the WAN ETH1 port on the ARX200S-GTX Router:

Table 9. Multi-Gigabit Minimum Cable Requirements

Speed	Minimum Copper Cable Requirements
100M	Standard TIA/EIA 568-compliant Category 5, 100 ohm unshielded cabling, complying with IEEE 802.3u 100Base-TX specifications.
1000M/2.5G/ 5G	Standard TIA/EIA 568-A-compliant Category 5 or TIA/EIA 568-B-compliant Enhanced Category 5 (Cat 5e) unshielded cabling.
10G	Standard TIA/EIA 568-C-compliant Category 6a unshielded cabling.

Completing the Worksheet

The following worksheets can assist in planning, installing, and configuring the router. The worksheets in Table 10 and Table 11 on page 53 are for the ARX200S-GT and ARX200S-GTX Routers, respectively. Allied Telesis recommends completing the appropriate worksheet before connecting network devices to the routers. Depending on the network devices, it may be necessary to configure the speed, duplex mode, and MDI/MDIX settings on the router ports as part of the initial installation procedure.

Table 10. ARX200S-GT Router Worksheet

Router		**Network Devices**				
Port	**Speeds**	**Location/ Description**	**IP Address/ MAC Address**	**Port Speed**	**Duplex Mode**	**MDI/ MDIX**
1	10M 100M 1000M					
2						
3						
4						
WAN ETH1		Service provider:				
USB port	USB storage device		NA[1]			
	USB cellular modem	Service provider:	NA			

1. Not applicable.

Table 11. ARX200S-GTX Router Worksheet

Router		Network Devices				
Port	**Speeds**	**Location/ Description**	**IP Address/ MAC Address**	**Port Speed**	**Duplex Mode**	**MDI/ MDIX**
1	10M 100M 1000M					
2						
3	Multi-Gigabit 100M 1000M 2.5G 5G 10G					
4						
WAN ETH1		Service provider:				
USB port	USB storage device		NA[1]			
	USB cellular modem	Service provider:	NA			

1. Not applicable.

To complete the worksheet, do the following:

1. Refer to the documentation of the network devices for their speeds, duplex modes, and MDI/MDIX settings. The Internet service provider can provide you with the specifications of their Internet device.
2. Add network devices to the router ports in the worksheet. Remember that router ports 1 and 2 and ports 3 and 4 support different speeds.
3. Review the following:
   - ❒ The default setting for speed, duplex mode, and MDI/MDIX for all router ports is Auto.

- For router ports that are connected to network devices that also support Auto for the three settings, the router should be able to automatically establish links to those devices.
- For router ports that are connected to network devices that have one or more fixed settings, such as speed or duplex mode, you may need to manually configure their settings before they can establish connections with the devices.

Table 12 is an example of a filled-in worksheet for the ARX200S-GTX Router.

Table 12. Example ARX200S-GTX Router Worksheet

Router		**Network Devices**				
Port	**Speeds**	**Location/ Description**	**IP Address/ MAC Address**	**Port Speed**	**Duplex Mode**	**MDI/ MDIX**
1	10M 100M 1000M	office 102 desktop PC	*xxx.xxx.xxx.xxx* *nn:nn:nn:nn:nn:nn*	auto	auto	auto
2		office 103 document scanner	*xxx.xxx.xxx.xxx* *nn:nn:nn:nn:nn:nn*	Fixed 1000M	Fixed full- duplex	Fixed MDIX
3	Multi- Gigabit 100M 1000M 2.5G 5G 10G	office 103 Data server	*xxx.xxx.xxx.xxx* *nn:nn:nn:nn:nn:nn*	Fixed 5G	Fixed Full	Fixed MDI
4		office 105 10G Unmanaged Ethernet switch (switch port 10)	*nn:nn:nn:nn:nn:nn*	Auto	Auto	Auto
WAN ETH1		Service provider: AAA Internet service provider		Auto	Auto	Auto
USB port	USB storage device		NA			
	USB cellular modem	Service provider: CCC wireless Internet service provider	NA			

Chapter 3

Installing the Router on a Table

The chapter contains the following sections:

Installing the Router with the Bumper Feet

This section contains the procedure for installing the router on a table with the bumper feet included with the product. The following guidelines are in addition to those in “Choosing a Site for the Router” on page 43:

- Do not stack routers on a table.
- Do not install the router upside down on a table.
- Do not install the router vertically on a table without the STND-J03 stand kit.

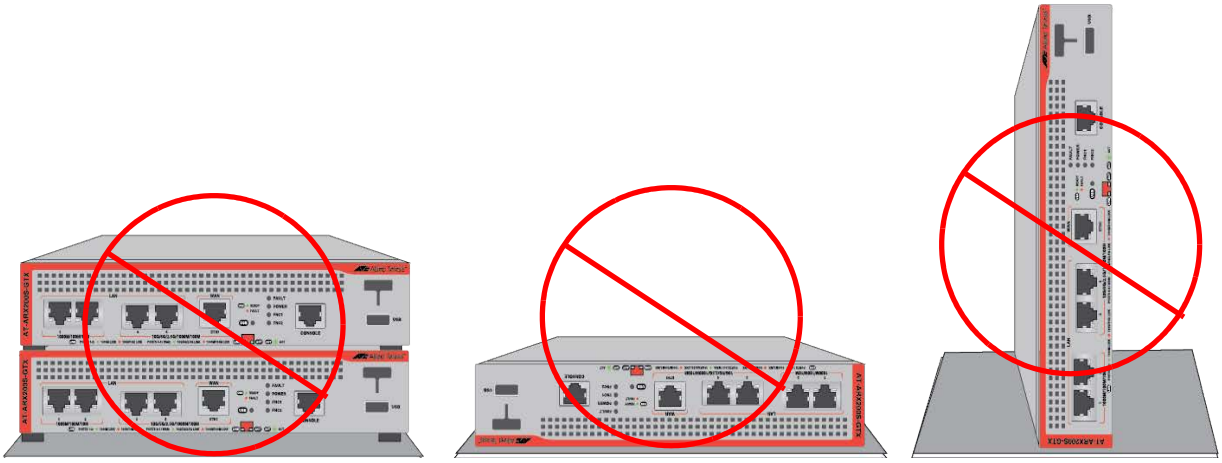


Figure 19. Unsupported Table Installations

Warning
Devices should not be stacked on a table or desktop. They could present a physical safety hazard if you need to move or replace devices. E91

Warning
The device is heavy. Use both hands to lift it. You might injure yourself or damage the device if you drop it. E94

To install the router horizontally on a table with the bumper feet, perform the following procedure:

1. Verify that the selected site is suitable for the unit by reviewing “Reviewing Safety Precautions” on page 40 and “Choosing a Site for the Router” on page 43.

2. Verify that the table is strong enough to support the weight of the router.

3. Verify that the accessory kit came with all the appropriate items. Refer to “Unpacking the ARX200S-GTX Router” on page 45.

4. Lift the router from the shipping box and place it upside down on the table.

5. Attach the four bumper feet to the bottom corners of the device. Refer to Figure 20.

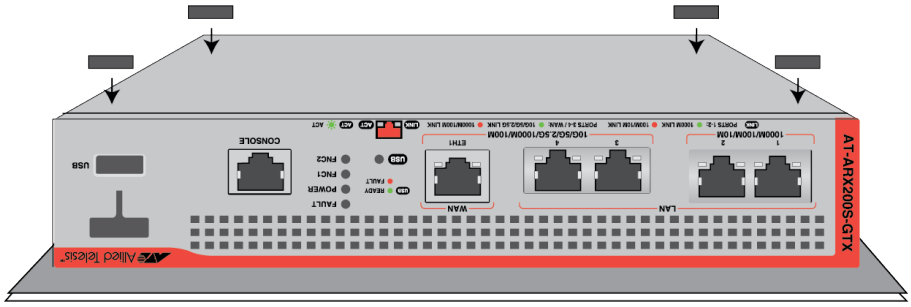


Figure 20. Attaching the Bumper Feet

6. Turn the router over, placing it on the bumper feet.

7. Go to Chapter 6, “Verifying the Hardware Status” on page 87.

Installing the Router with the STND-J03 Kit

You can install the router vertically on a table with the STND-J03 stand kit. The kit is sold separately. The following guidelines are in addition to those in “Choosing a Site for the Router” on page 43:

- The table should be level and secured.
- If you plan to install the router against or by a wall, make sure that the wall is straight and secured.
- The router can be installed upright by itself. Refer to Figure 21.

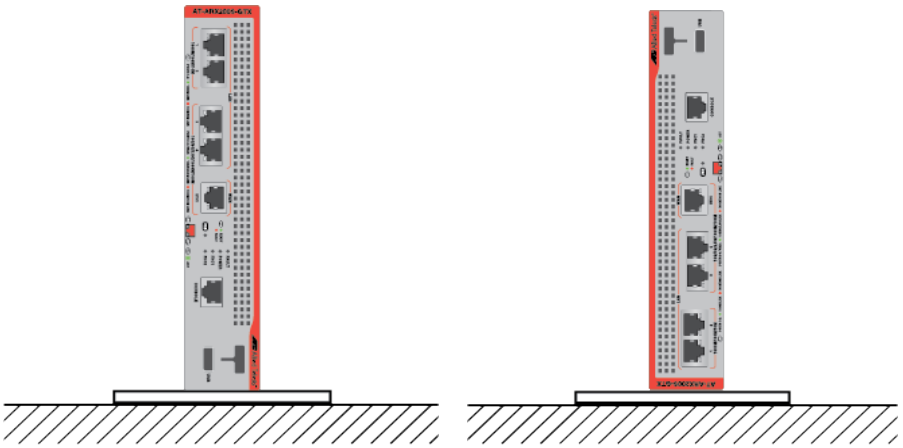


Figure 21. Router Installed Vertically By Itself on a Table

- The router can be installed upright against a wall. Refer to Figure 22.

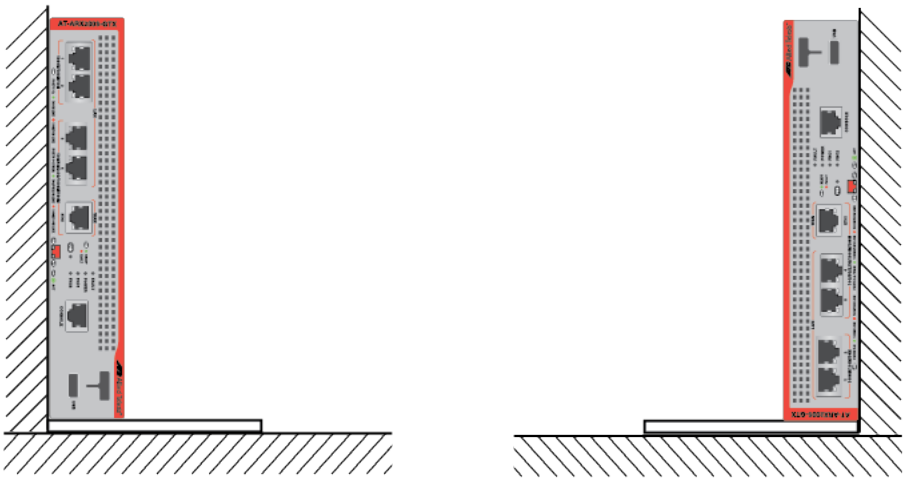


Figure 22. Router Installed Vertically on a Table Against a Wall

Note
When installing the router against a wall, you must place its bottom panel against the wall.

❒ The router can be installed with space between it and the wall. Refer to Figure 23.

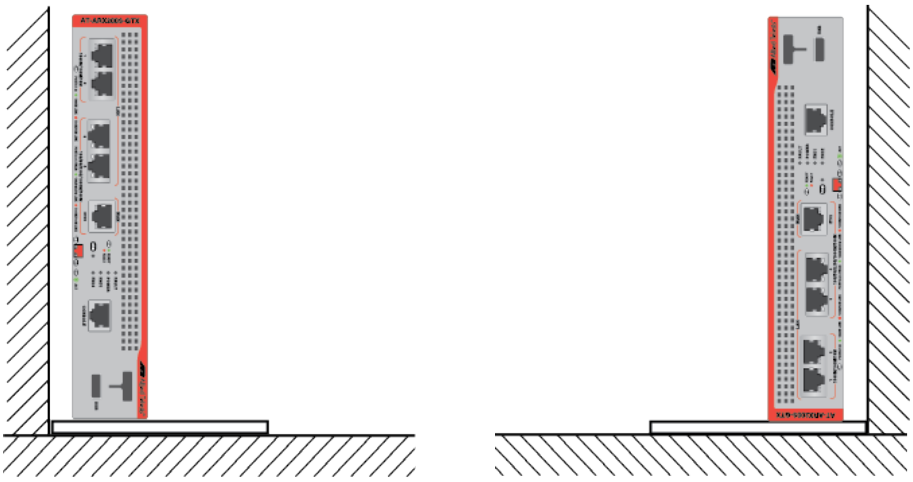


Figure 23. Router Installed Vertically on a Table Near a Wall

The brackets have holes for the different installation orientations. The holes are marked with A, B, and C. Refer to Figure 24 and Figure 25 on page 60.

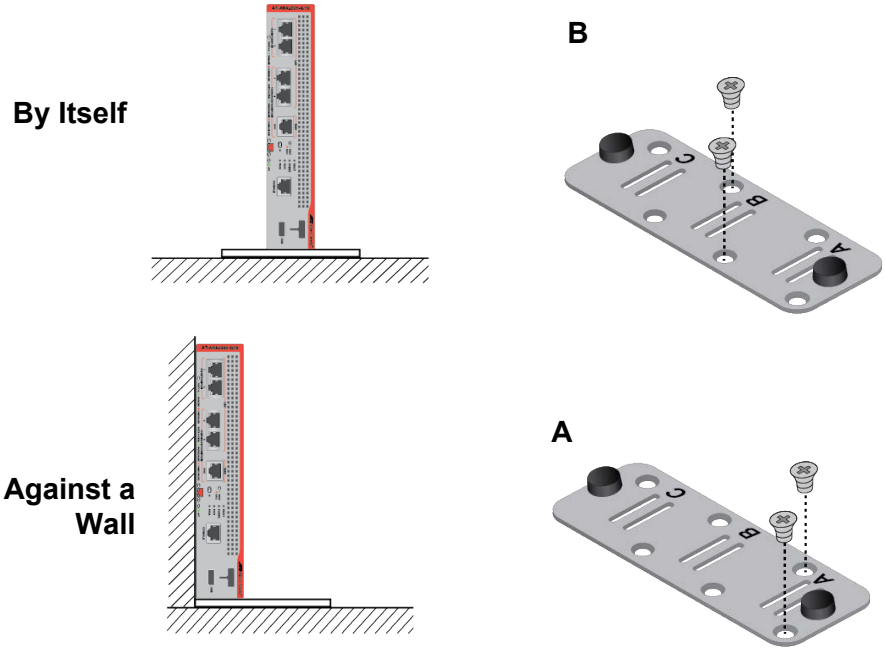


Figure 24. STND-J03 Bracket Holes

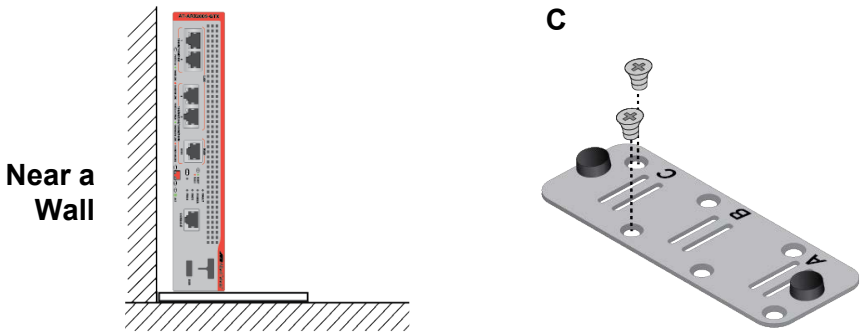


Figure 25. STND-J03 Bracket Holes (Continued)

To install the router on a table with the STND-J03 brackets, perform the following procedure:

1. Verify that the selected site is suitable for the unit by reviewing “Reviewing Safety Precautions” on page 40 and “Choosing a Site for the Router” on page 43.

2. Verify that the table is strong enough to support the weight of the router.

3. Verify that the accessory kit came with all the appropriate items. Refer to “Unpacking the ARX200S-GTX Router” on page 45.

4. Lift the router from the shipping box and place it on the table.

5. Unpack the STND-J03 kit and verify the contents. Refer to Figure 15 on page 49.

6. Attach two bumper feet to the bottom of each bracket. Refer to Figure 26.

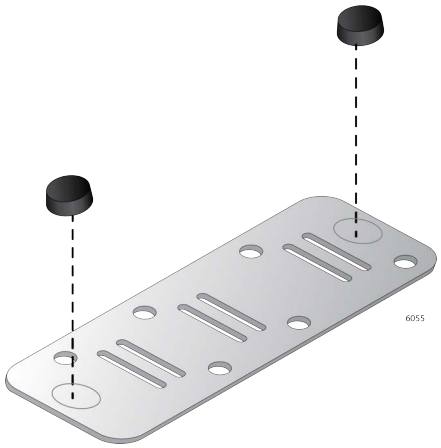


Figure 26. Attaching the Bumper Feet to the STND-J03 Brackets

7. Attach the brackets to one side of the router using the M4 x M6 screws included in the kit. Refer to Figure 27. Be sure to use the bracket holes that correspond to your selected orientation for the router on the table. Refer to Figure 24 on page 59 and Figure 25 on page 60.

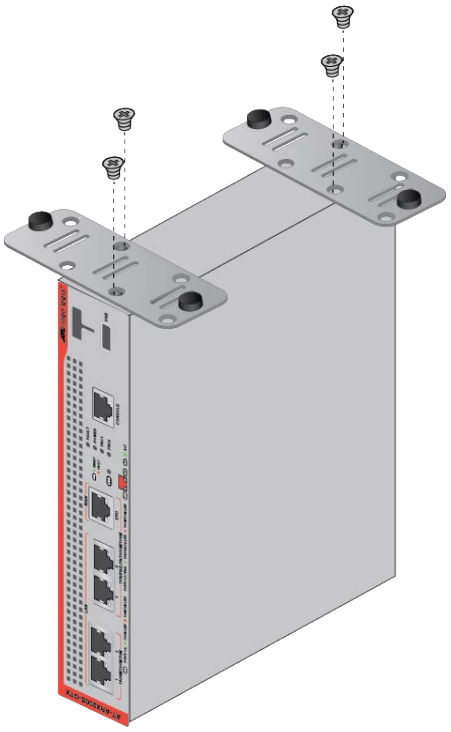


Figure 27. Attaching the STND-J03 Brackets to the Side of the Router

8. Place the router at the selected location.
9. Go to Chapter 6, “Verifying the Hardware Status” on page 87.
10. After cabling the router, you can secure the cables with the hook-and-loop fastener. Refer to Figure 28 on page 62.

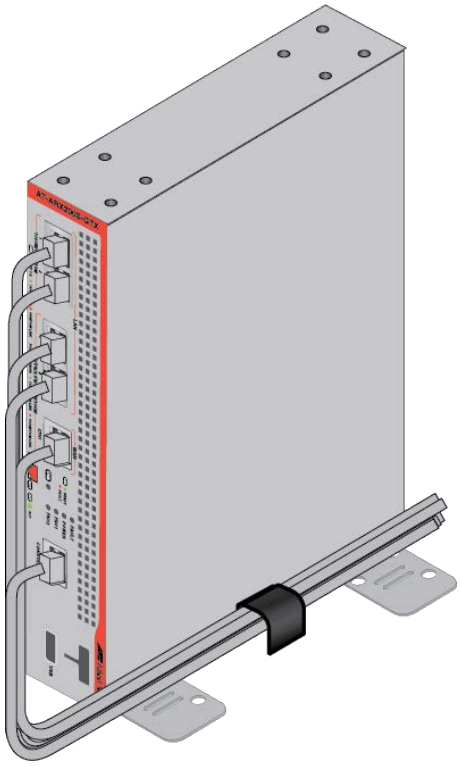


Figure 28. Securing the Router Cables

Chapter 4

Installing the Router in an Equipment Rack

This chapter contains instructions for installing the router in an equipment rack. Here are the procedures:

Installing the Router in an Equipment Rack with the RKMT-J14 Brackets Kit

This section contains the procedure for installing the router in a standard 19-inch equipment rack with the RKMT-J14 brackets kit.

Note
The illustrations show the ARX200S-GTX Router. The procedures are the same for the ARX200S-GT Router.

Required Items for the RKMT-J14 Brackets

This procedure requires the following items:

- One RKMT-J14 equipment rack brackets kit (sold separately)
- Cross-head screwdriver (not provided)
- Four standard equipment rack screws (not provided)

Router Positions in the Equipment Rack

The router has two sets of four screw holes on the left and right sides for attaching the RKMT-J14 brackets. Refer to Figure 29.

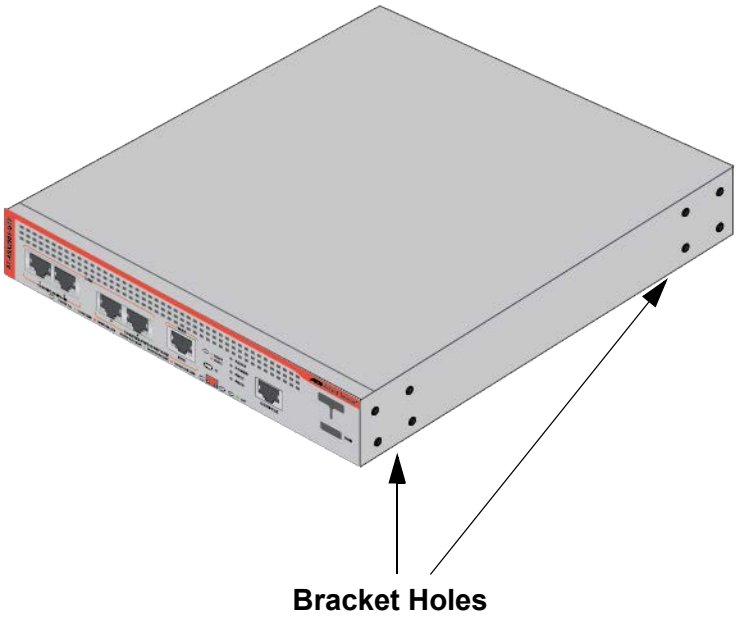


Figure 29. Side Panel Bracket Holes

The brackets also have two sets of four holes. Refer to Figure 30 on page 65.

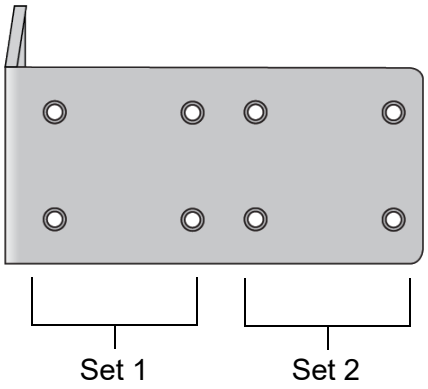


Figure 30. RKMT-J14 Bracket Holes

The different sets of holes on the router and brackets allow you to install the router in a equipment rack in a variety of orientations. You can install it with the front panel flush with, extending in front of, or recessed behind the front of the equipment rack. The illustrations in Figure 31 show the router orientations with the front panel facing the front of the equipment rack.

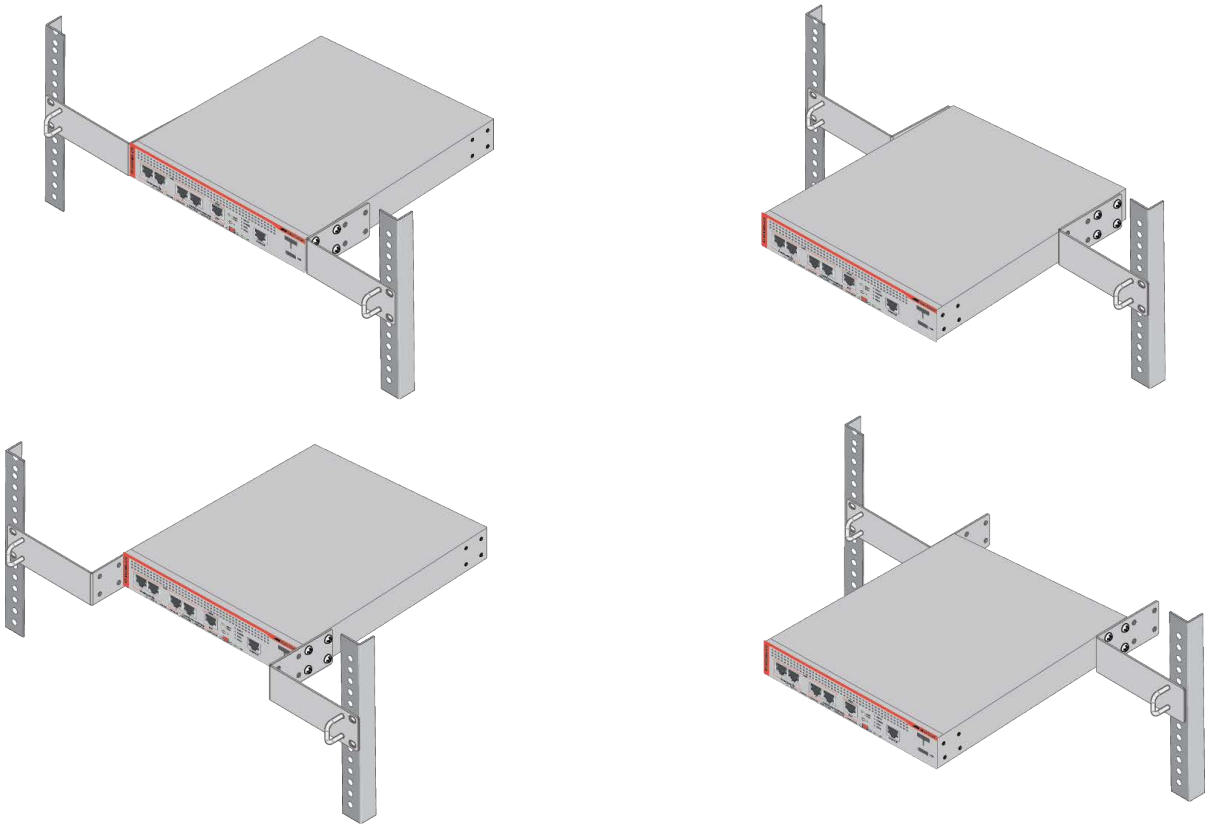


Figure 31. Router Positions in a Horizontal Equipment Rack with the RKMT-J14 Bracket Kit

You can also use the RKMT-J14 bracket kit to install the router in a vertical equipment rack. Refer to Figure 32.

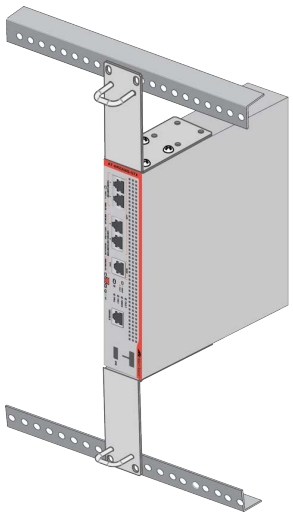


Figure 32. Router in a Vertical Equipment Rack with the RKMT-J14 Bracket Kit

Installing the Router with the RKMT-J14 Brackets

If you have not chosen an orientation for the router in the equipment rack, review “Router Positions in the Equipment Rack” on page 64. Review the installation guidelines in “Choosing a Site for the Router” on page 43 before installing the router.

Caution

The chassis may be heavy and awkward to lift. Allied Telesis recommends asking for assistance when mounting the chassis in an equipment rack. E28

To install the router in a 19-inch equipment rack with the RKMT-J14 brackets kit, perform the following procedure:

1. Verify that the selected site is suitable for the unit by reviewing “Reviewing Safety Precautions” on page 40 and “Choosing a Site for the Router” on page 43.

2. Unpack and verify the contents of the router. Refer to Figure 11 on page 45.

3. Unpack and verify the contents of the RKMT-J14 brackets kit, Refer to Figure 16 on page 49

4. Attach the two handles to the RKMT-J14 brackets with the four M3x6mm screws included in the kit. Attaching the handles is optional. Refer to Figure 33 on page 67.

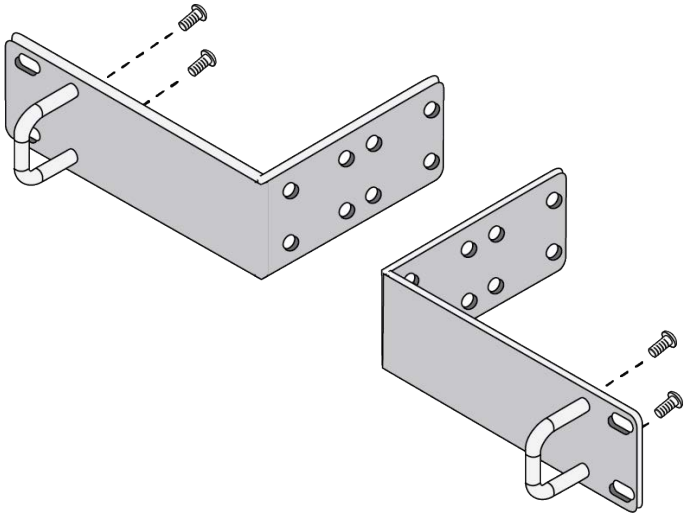


Figure 33. Attaching the Handles to the RKMT-J14 Brackets

5. Place the router on a level, secure surface.

6. Attach the two brackets to the sides of the router in the selected position with the eight M4x6mm screws included in the RKMT-J14 kit. The illustration in Figure 34 shows the brackets being installed so that the front panel of the router will be even with the front of the equipment rack.

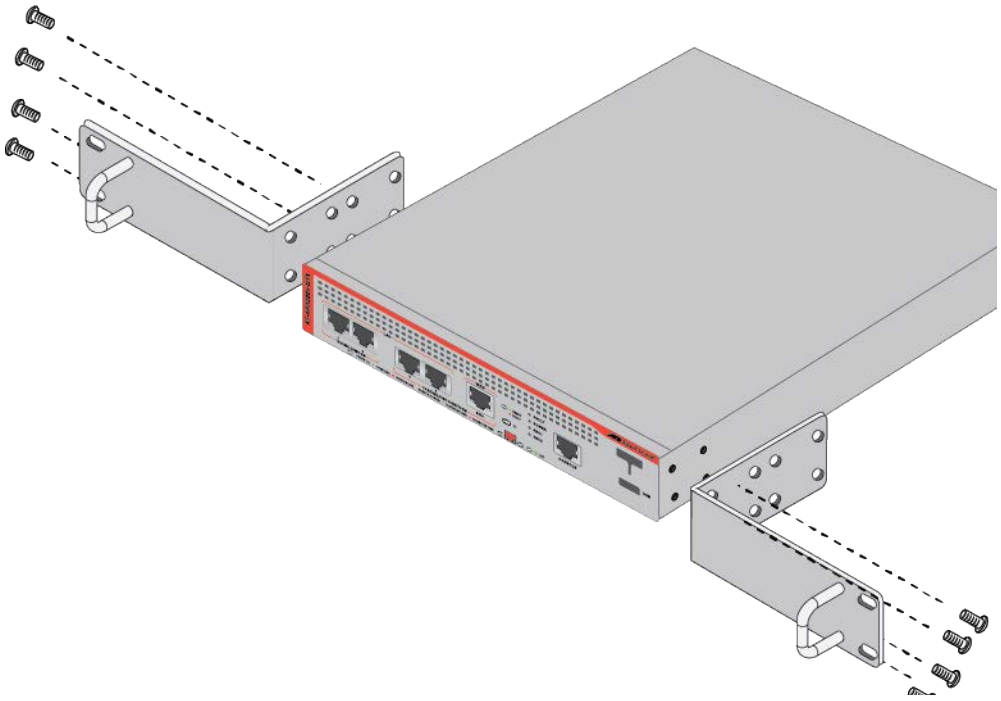


Figure 34. Attaching the RKMT-J14 Brackets to the Router

7. Have another person hold the router in the equipment rack at the selected location while you secure it using four standard equipment rack screws (not provided). Refer to Figure 35.

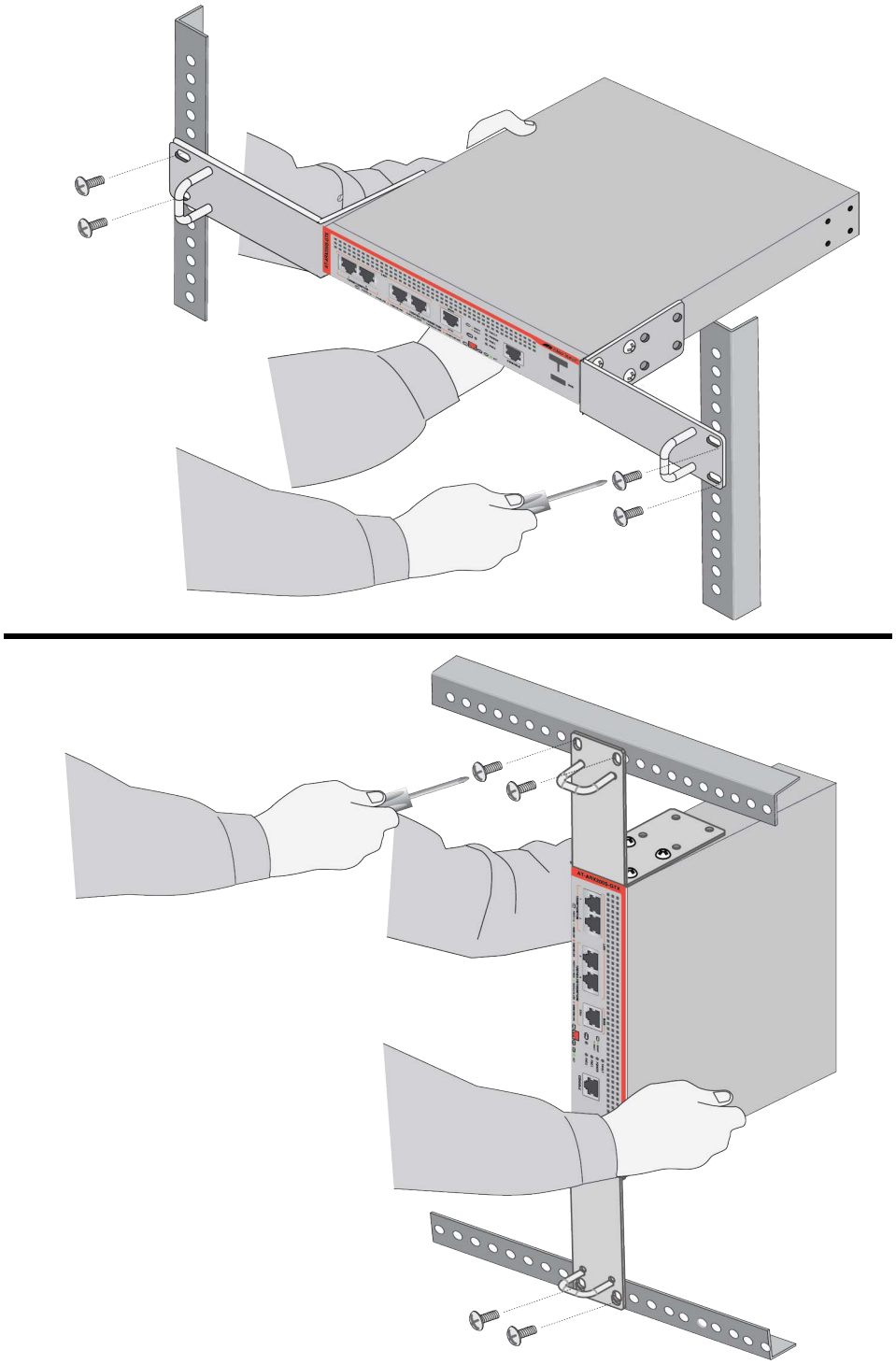


Figure 35. Securing the Router in the Equipment Rack

8. Go to Chapter 6, “Verifying the Hardware Status” on page 87.

Installing the Router in an Equipment Rack with the RKMT-J15 Equipment Rack Tray

This section contains the procedure for installing the router horizontally in a standard 19-inch equipment rack with the RKMT-J15 equipment rack tray.

Note
The illustrations show the ARX200S-GTX Router. The procedures are the same for the ARX200S-GT Router.

Caution
Do not install the RKMT-J15 equipment rack tray vertically in an equipment rack. Refer to Figure 36.

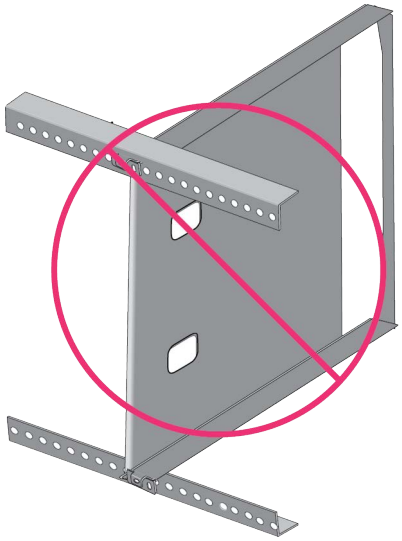


Figure 36. Invalid Vertical installation of the RKMT-J15 Equipment Rack Tray

Here are the required items:

- One RKMT-J15 equipment rack bracket kit (sold separately)
- Four standard equipment rack screws (not provided)
- Cross-head screwdriver (not provided)

To install the router in a 19-inch equipment rack with the RKMT-J15 equipment rack tray, perform the following procedure:

1. Verify that the selected site is suitable for the unit by reviewing “Reviewing Safety Precautions” on page 40 and “Choosing a Site for the Router” on page 43.

2. Unpack and verify the contents of the router. Refer to Figure 11 on page 45.

3. Unpack and verify the contents of the RKMT-J15 equipment rack tray kit. Refer to Figure 17 on page 50.

4. Have another person hold the RKMT-J15 equipment rack tray at the selected location in the equipment rack while you secure it using four standard equipment rack screws (not provided). Refer to Figure 37.

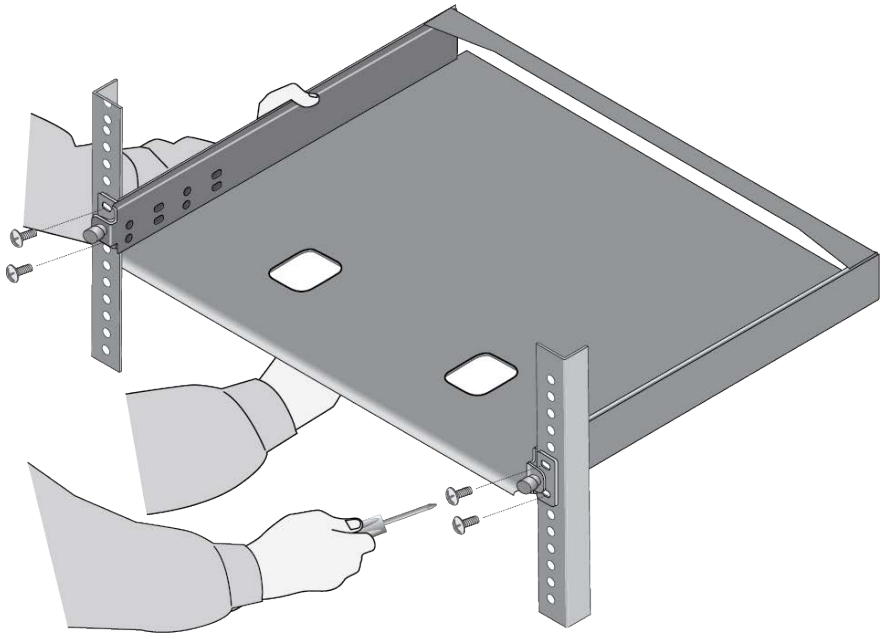


Figure 37. Installing the RKMT-J15 Equipment Rack Tray in an Equipment Rack

5. Loosen the two thumbscrews on the front of the tray. Refer to Figure 38 on page 71.

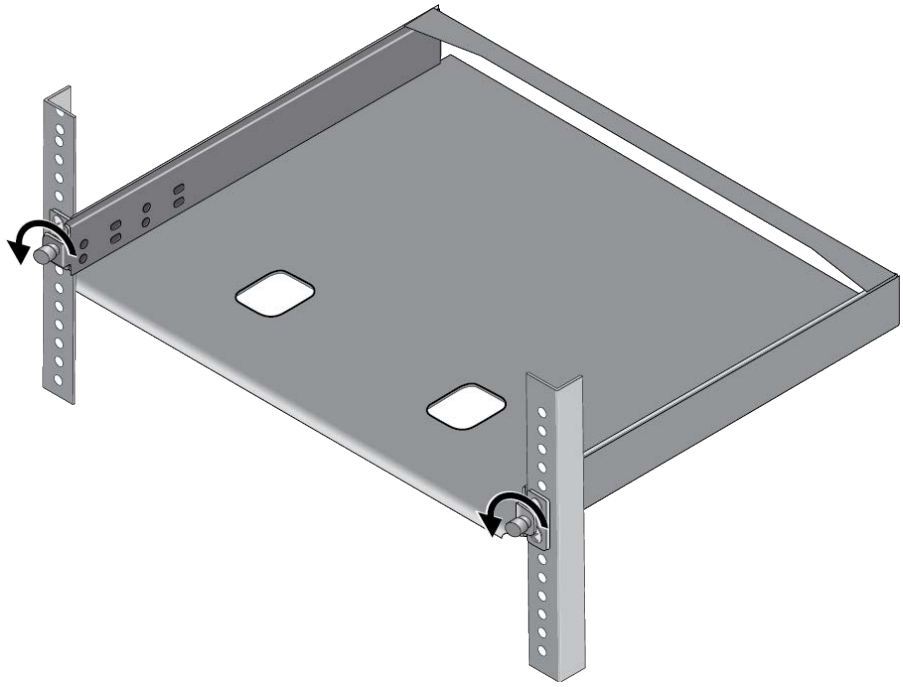


Figure 38. Loosening the Two Thumbscrews on the RKMT-J15 Equipment Rack Tray

6. Slide out the tray. Refer to Figure 39.

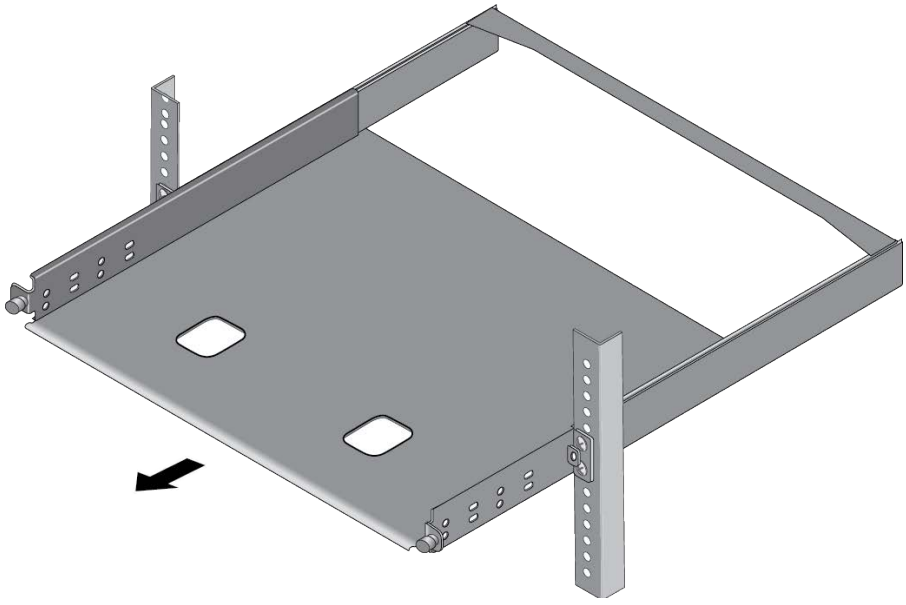


Figure 39. Sliding Out the RKMT-J15 Equipment Rack Tray

Note
Depending on the equipment rack and location, it may be easier to attach the power cord to the router before installing the device in the equipment tray. If so, perform steps 1 to 4 in “Powering On the Router” on page 88 before continuing with the next step.

7. Place the router in the left or right side of the tray, with its front panel facing the front of the tray. Route the power cord out the back of the tray. If you are installing only one router, you may install it on either the left or right side. Refer to Figure 40.

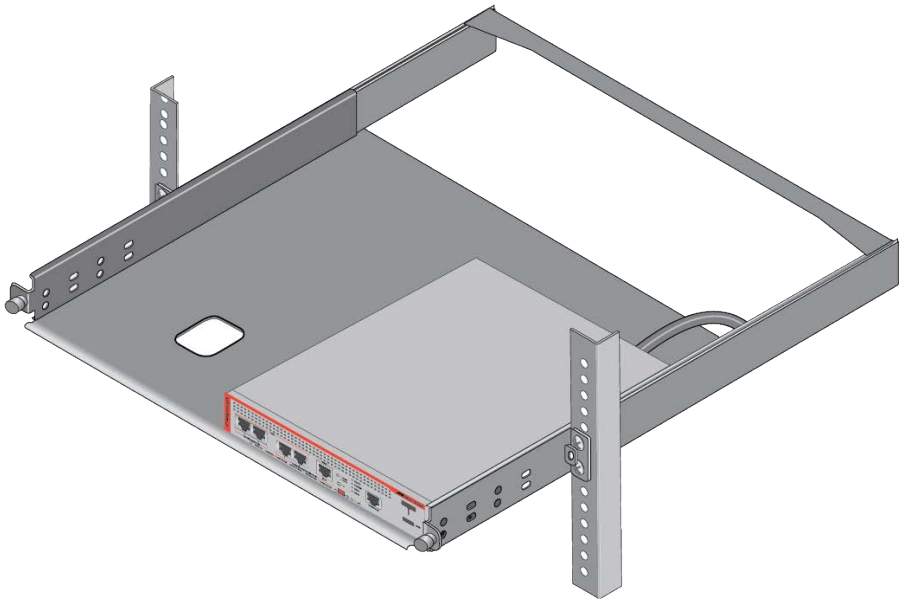


Figure 40. Placing the Router in the RKMT-J15 Equipment Rack Tray

8. Secure the router in the tray with two M4x6mm screws included with the tray. Refer to Figure 41 on page 73.

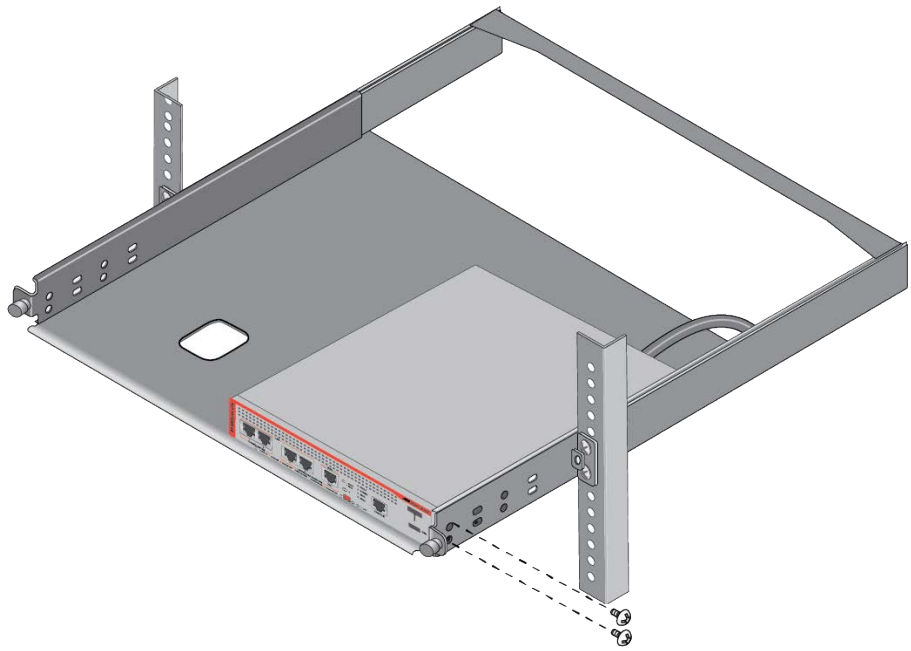


Figure 41. Securing the Router to the RKMT-J15 Equipment Rack Tray

9. To install a second router in the tray, repeat steps 7 and 8.
10. Slide in the tray. Refer to Figure 42.

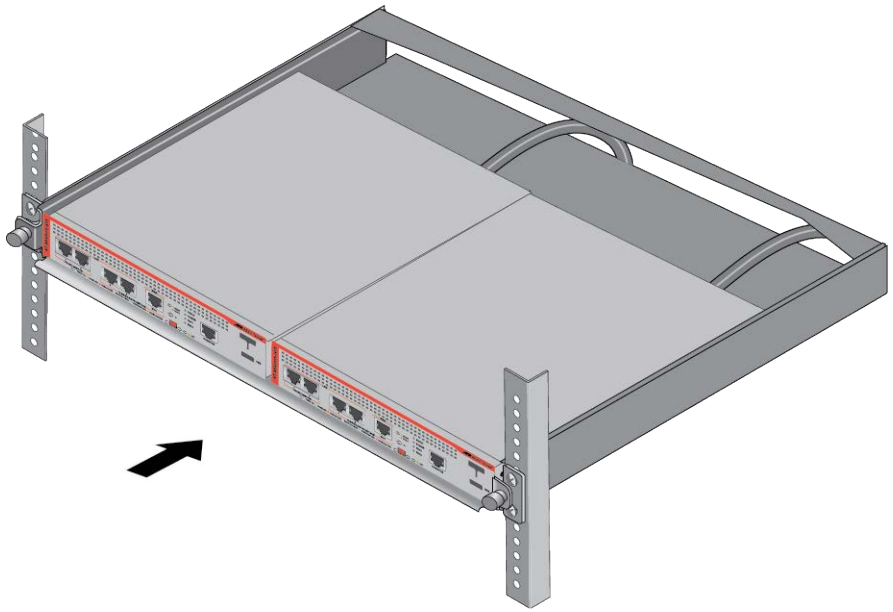


Figure 42. Sliding in the RKMT-J15 Equipment Rack Tray

11. Tighten the two thumbscrews to secure the tray to the bracket. Refer to Figure 43.

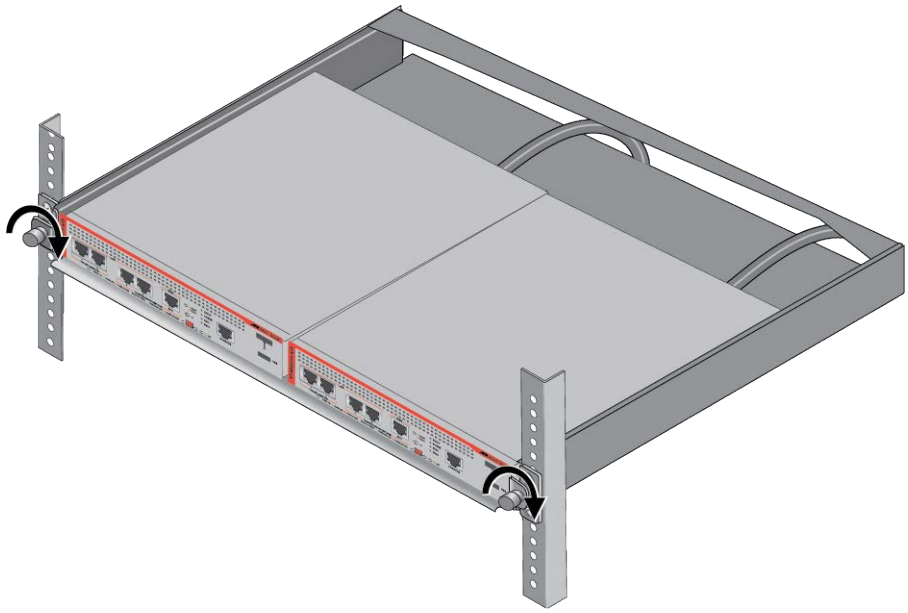


Figure 43. Tightening the Two Thumbscrews on the RKMT-J15 Equipment Rack Tray

12. Go to Chapter 6, “Verifying the Hardware Status” on page 87.

Chapter 5

Installing the Router on a Wall

This chapter contains instructions for installing the ARX200S Router Series on a wall with the AT-BRKT-J24 wall brackets kit. The chapter contains the following sections:

Installation Guidelines

Wall installations of the ARX200S Router Series require the AT-BRKT-J24 brackets kit. The kit is sold separately. Refer to Figure 18 on page 50. You can install the router on a wall with the front panel facing up, left or right, as shown in Figure 44.

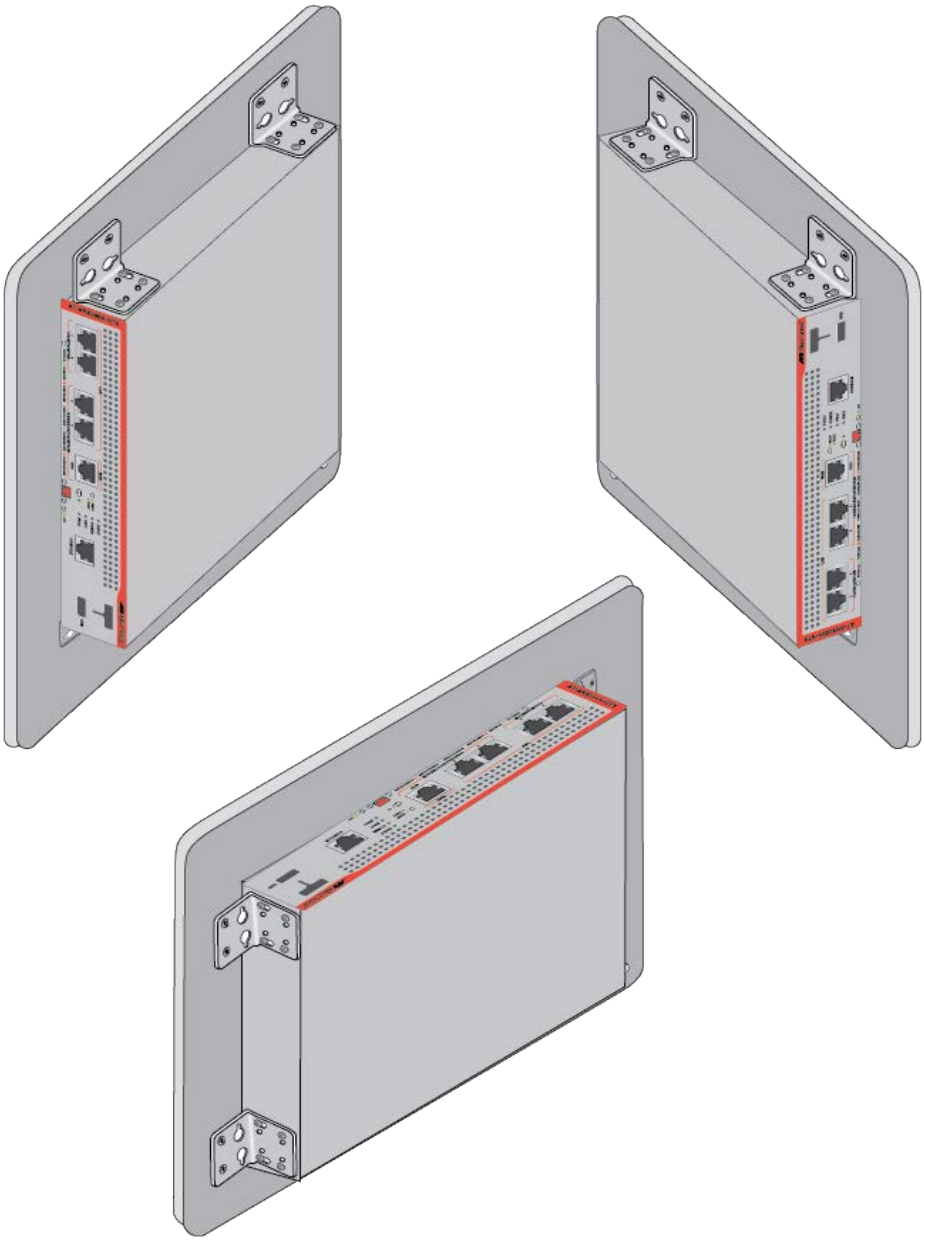


Figure 44. ARX200S Router Series on a Wall with the AT-BRKT-J24 Brackets Kit

Do not install the router with the front panel facing down. Refer to Figure 45.

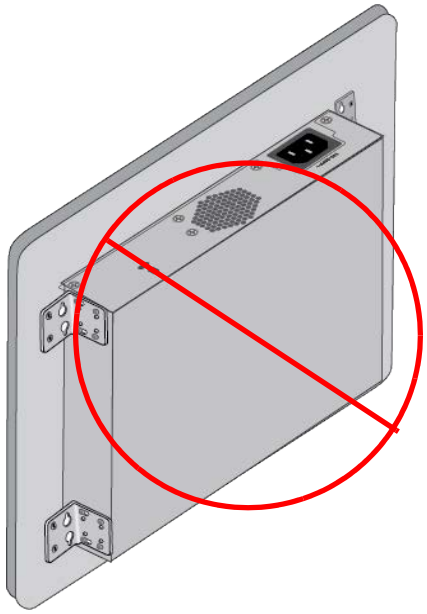


Figure 45. Unsupported Wall Installation with the Front Facing Down

Here are the guidelines to installing the router on a wall:

- You may install the router on a wooden or concrete wall.
- If you are installing the router on a wall with wooden studs, you should install it on a plywood base. For more information, refer to “Plywood Base for a Wall with Wooden Studs” on page 79.
- You should not install the router on Sheetrock or similar material. Sheetrock might not be strong enough to safely support the device.

Warning
The device is heavy. Ask for assistance before moving or lifting it to avoid injuring yourself or damaging the equipment. E94

Warning
The device should be installed on a wall by a qualified building contractor. Serious injury to yourself or others or damage to the equipment may result if it is improperly fastened to the wall. E105

Here are the required tools and material for installing the router on a wall:

- One AT-BRKT-J24 wall brackets kit (sold separately).
- Four wall anchors and screws (not provided) The diameter of the screw holes in the brackets is 5mm.
- Cross-head screwdriver (not provided).

- ❒ Stud finder for a wooden wall to identify the middle of wall studs and hot electrical wiring (not provided).
- ❒ Drill and 1/4-inch carbide drill bit for a concrete wall (not provided).
- ❒ Plywood base if you are installing the router on a wall with wooden studs (not provided.) Refer to “Plywood Base for a Wall with Wooden Studs” on page 79 for illustrations.
- ❒ Four screws to attach the plywood base to the wall (not provided).

Note
The illustrations in the following procedures show the ARX200S-GTX Router. The procedures are the same for the ARX200S-GT Router.

Installing the ARX200S-GTX Router on a Wooden Wall

This section contains the procedures for installing the router on a wooden wall.

Plywood Base for a Wall with Wooden Studs

When installing the router on a wall that has wooden studs, Allied Telesis recommends installing the device on a plywood base. (A plywood base is not required for concrete walls.) Refer to Figure 46.

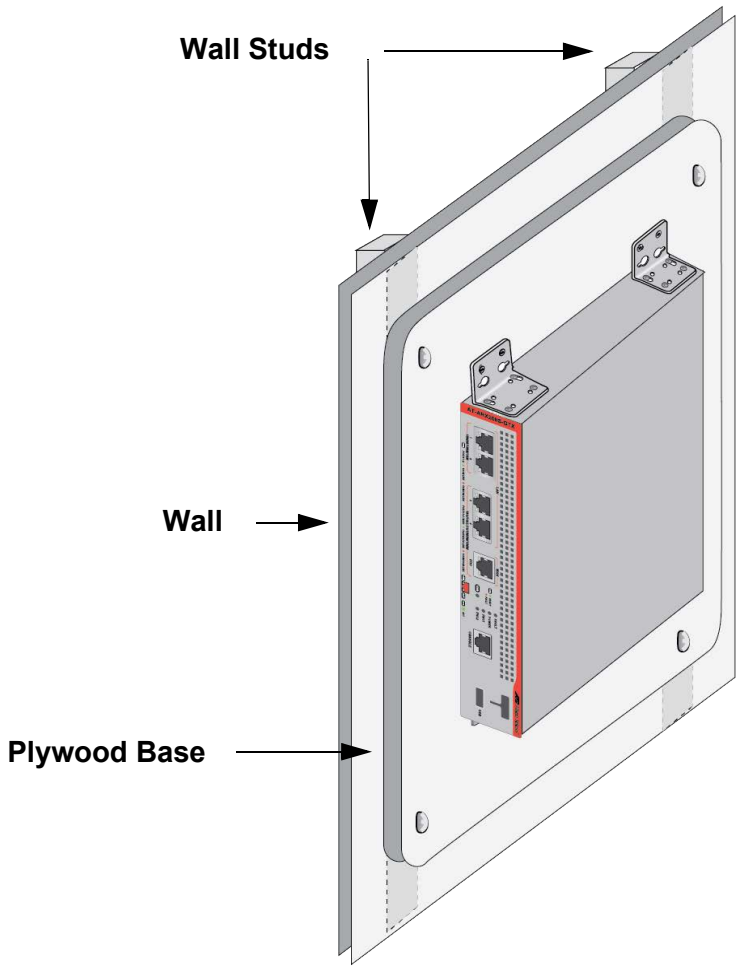


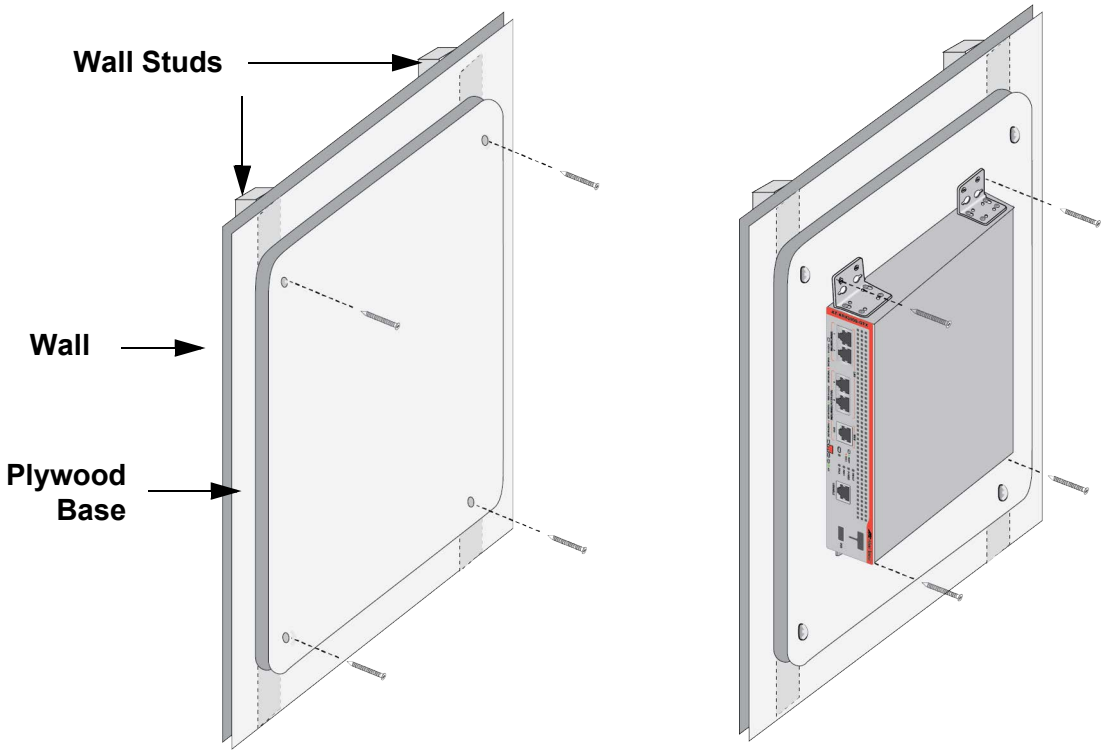
Figure 46. ARX200S-GTX Router on a Wooden Wall with a Plywood Base

The plywood base should be mounted on two studs in the wall. The recommended minimum dimensions of a plywood base for the ARX200S-GTX Router are listed here:

- Width: 55.9 centimeters (22 inches)
- Height: 50 centimeters (20 inches)
- Thickness: 2.5 centimeters (1 inch)

The dimensions assume the wall studs are 41 centimeters (16 inches) apart. You might need to adjust the width of the base if the distance between the studs in your wall is different than the industry standard.

You should install the plywood base on the wall and then install the router on the base. Refer to Figure 47.



Step 1: Install the plywood base on the wall.

Step 2: Install the router on the plywood base.

Figure 47. Steps to Installing the ARX200S-GTX Router on a Plywood Base

Consult a qualified building contractor for installation instructions for the plywood base. The installation guidelines are listed here:

- ❒ Use a stud finder to identify the middle of studs and hot electrical wiring in the wall.
- ❒ Attach the base to two wall studs with a minimum of four screws.
- ❒ The selected wall location for the base should provide sufficient space from other devices or walls so that you can access the front and back panels, and for adequate airflow for ventilation.

Installing the Router on a Plywood Base

This procedure assumes that the plywood base for the router is already installed on the wall. Review "Reviewing Safety Precautions" on page 40 and "Choosing a Site for the Router" on page 43 before performing this procedure. This procedure requires a minimum of two people.

Warning
The device is heavy. Always ask for assistance before moving or lifting it to avoid injuring yourself or damaging the equipment. E94

Warning
The device should be installed on the wall by a qualified building contractor. Serious injury to yourself or others or damage to the equipment may result if it is improperly fastened to the wall. E105

To install the router on the plywood base, perform the following procedure:

1. Verify that the selected site is suitable for the unit by reviewing "Reviewing Safety Precautions" on page 40 and "Choosing a Site for the Router" on page 43.

2. Unpack the router and place it on a table.

   Note
   If the bumper feet are attached to the bottom on the router, remove them before continuing.

3. Unpack the AT-BRKT-J24 wall brackets kit and verify the contents. Refer to Figure 18 on page 50.

4. Attach the four AT-BRKT-J24 wall brackets to the sides of the router, with the sixteen M4x6mm screws in the brackets kit. Refer to Figure 48 on page 82.

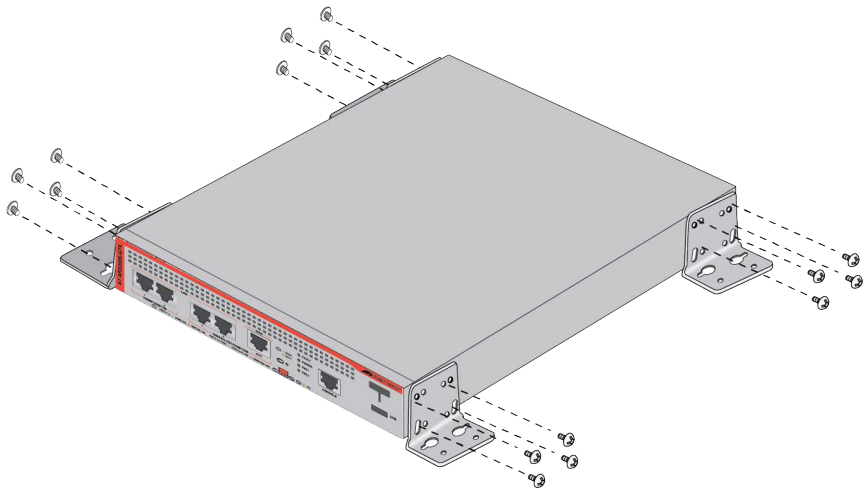


Figure 48. Attaching the AT-BRKT-J24 Wall Brackets to the ARX200S Router Series

5. Have another person hold the router on the plywood base on the wall while you secure it with four screws. (Wall screws not supplied.) Follow these guidelines when positioning the router on the wall:

   - ❒ You can install the router with the front panel facing up, left, or right, Figure 49 on page 83 shows the router with the faceplate on the left.

   Note
   Do not install the router with the front panel facing down.

   - ❒ Leave sufficient space from other devices or walls so that you can access the front and back panels, and for adequate air ventilation.

6. Go to Chapter 6, “Verifying the Hardware Status” on page 87.

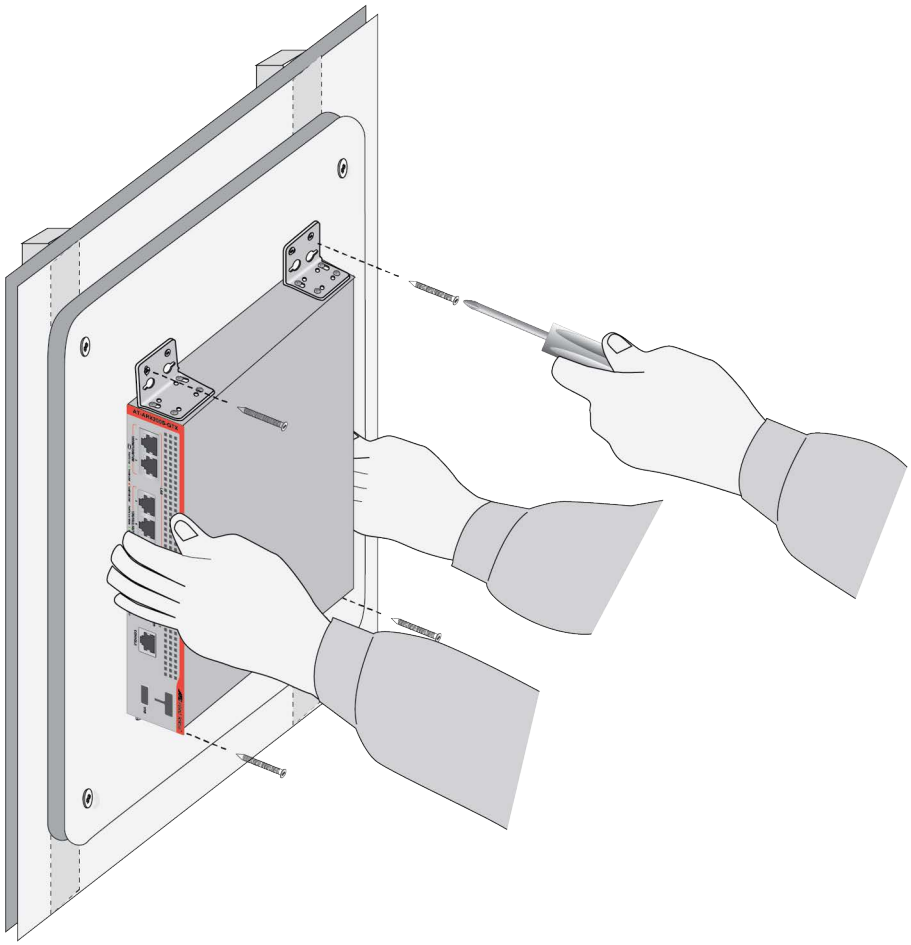


Figure 49. Installing the ARX200S Router Series on a Plywood Base

Installing the ARX200S Router Series on a Concrete Wall

This section contains the installation instructions for the ARX200S Router Series on a concrete wall with the AT-BRKT-J24 wall brackets kit. Review “Installation Guidelines” on page 76 before performing the procedure: This procedure requires a minimum of two people.

Warning
The device is heavy. Always ask for assistance before moving or lifting it to avoid injuring yourself or damaging the equipment.
E94

Warning
The device should be installed on the wall by a qualified building contractor. Serious injury to yourself or others or damage to the equipment may result if it is improperly fastened to the wall.
E105

To install the router on a concrete wall, perform the following procedure:

1. Verify that the selected site is suitable for the unit by reviewing “Reviewing Safety Precautions” on page 40 and “Choosing a Site for the Router” on page 43.

2. Place the router on a table.

   Note
   If the bumper feet are attached to the bottom on the router, remove them before continuing.

3. Unpack the AT-BRKT-J24 wall brackets kit and verify the contents. Refer to Figure 18 on page 50.

4. Install the four AT-BRKT-J24 wall brackets to the sides of the router with the sixteen M4x6mm screws included with the brackets. Refer to Figure 48 on page 82.

5. Have another person hold the router on the concrete wall at the selected location for the device while you use a pencil or pen to mark the wall with the locations of the four screw holes in the four brackets (one screw per bracket). Follow these guidelines when positioning the router on the wall:

   - You can install the router with the front panel facing up, left, or right, Figure 50 on page 85 shows the router with the faceplate on the left.

Note
Do not install the router with the front panel facing down.

- Leave sufficient space from other devices or walls so that you can access the front and back panels, and for adequate air ventilation.

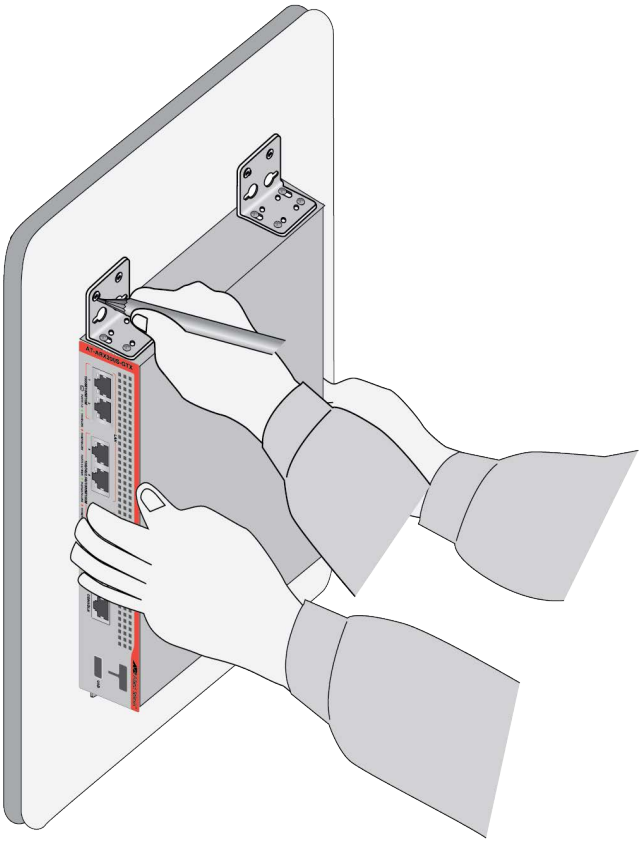


Figure 50. Marking the Locations of the BRKT-J24 Bracket Holes on a Concrete Wall

6. Place the router on a table or desk.
7. Use a drill and 1/4” carbide drill bit to pre-drill the holes you marked in step 5. Review the following guidelines:
   - Prior to drilling, set the drill to hammer and rotation mode. The modes break up the concrete and clean out the hole.
   - Allied Telesis recommends cleaning out the holes with a brush or compressed air.
8. Insert wall anchors in the four holes. (Wall anchors not supplied.)

9. Have another person hold the router at the selected location while you secure it to the wall with four screws. (Wall screws not supplied.) Refer to Figure 51.

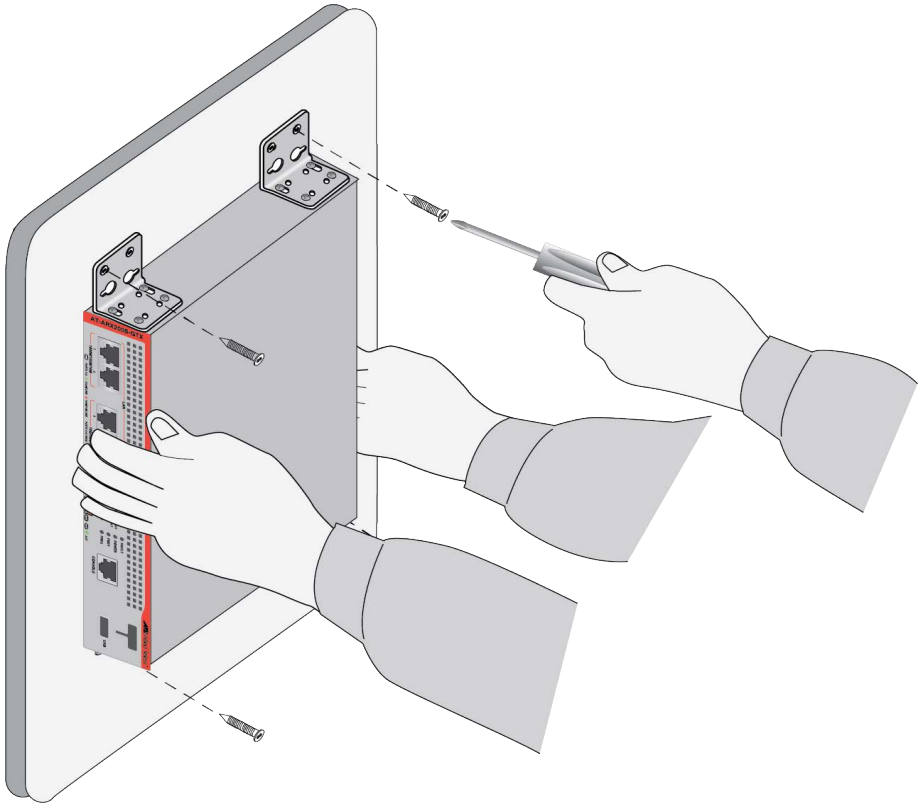


Figure 51. Securing the ARX200S-GTX Router on a Concrete Wall

10. Go to Chapter 6, “Verifying the Hardware Status” on page 87.

Chapter 6

Verifying the Hardware Status

The procedures in this chapter explain how to start a management session with the command line and web browser interfaces in the AlliedWare Plus management software on the ARX200S Router Series. There are also instructions for verifying the status of the hardware, cabling the ports, and more. This chapter contains the following procedures:

Powering On the Router

For the AC power specifications of the router, refer to “Power and Environmental Specifications” on page 144.

Warning
Power cord is used as a disconnection device. To de-energize equipment, disconnect the power cord. E3

Note
Pluggable Equipment. The socket outlet shall be installed near the equipment and shall be easily accessible. E5

Caution
You should connect the AC power cord to the router before connecting it to the AC power source. E141

To power on the router, perform the following procedure:

1. Install the power cord retaining clip on the AC power connector on the rear panel of the router. Refer to Figure 52.

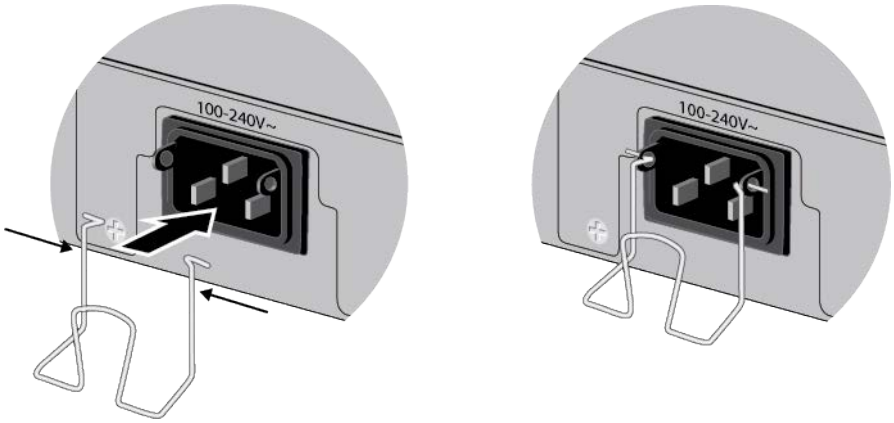


Figure 52. Installing the Power Cord Retaining Clip

2. Raise the retaining clip and connect the AC power cord to the AC power connector. Refer to Figure 53 on page 89.

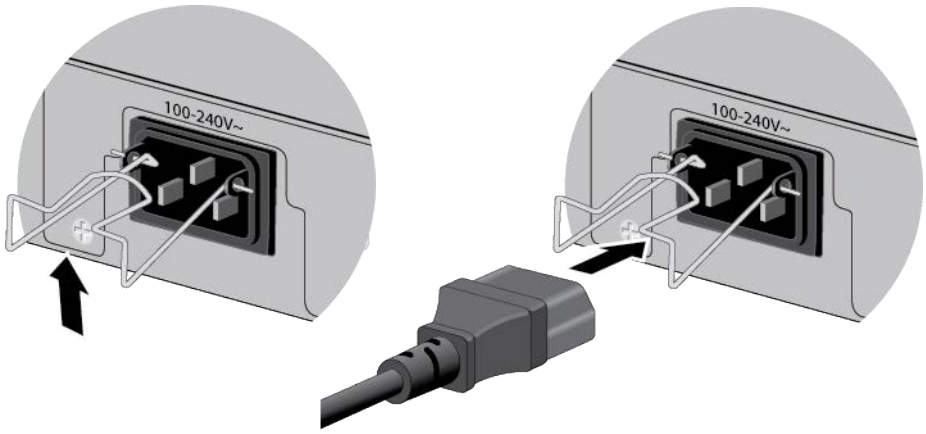


Figure 53. Connecting the AC Power Cord

3. Lower the power cord retaining clip to secure the power cord to the router. Refer to Figure 54.

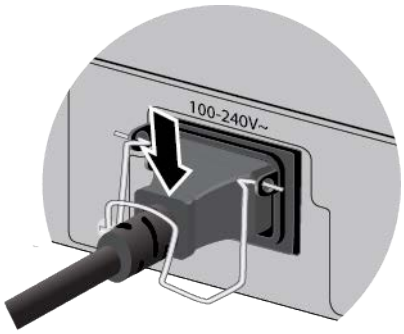


Figure 54. Lowering the Power Cord Retaining Clip

4. Connect the power cord to an appropriate AC power source. Refer to Figure 55.

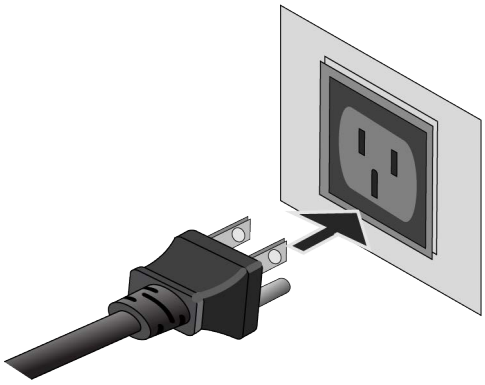


Figure 55. Connecting the Power Cord to an AC Power Source

Note
The illustration shows a North American power cord. Your power cord may be different.

5. Wait several minutes for the router to start the AlliedWare Plus management software.
6. Go to “Starting a Management Session” on page 91.

Starting a Management Session

The following sections contain the procedures for starting the first management session on the router:

- ❒ “Console Port” on page 92
- ❒ “DHCP or DHCPv6 Server” on page 93
- ❒ “Default IPv4 Address” on page 95

Here are factory default settings that relate to the first management session:

- ❒ Console port: enabled
- ❒ LAN ports 1 to 4: enabled
- ❒ WAN ETH1 port: enabled
- ❒ DHCP and DHCPv6 clients: enabled
- ❒ VLAN1 default IP address without a DHCP server: 169.168.1.1 (255.255.0.0)
- ❒ SSH server: enabled (See Note below)
- ❒ Telnet server: disabled
- ❒ Web server: enabled
- ❒ VLAN membership: port-based VLAN1
- ❒ Configuration file: none

Review the following guidelines:

- ❒ The Console port cannot be disabled.
- ❒ The router is shipped from the factory without a configuration file. It creates the file the first time you save its parameter settings. The configuration file contains parameter settings that have been changed from their default values. It does not include parameter settings at their default values.
- ❒ Management sessions do not interfere with the network operations of the router.

Note
When you save the router’s configuration for the first time, the default settings for SSH changes from enabled to disabled, and Telnet from disabled to enabled. Unless you change their settings manually, you will need to use Telnet instead of SSH to manage the router with the CLI after the router saves its first configuration file and after the next reboot.

The router supports the following web browsers:

- Google Chrome™
- Mozilla Firefox™
- Microsoft Edge or Internet Explorer 11™
- Apple Safari™

Console Port

This section explains how to start a local management session with the command line interface (CLI) through the Console port on the router. Here are the guidelines:

- Local management sessions require a terminal, computer, or laptop with an RS-232 serial port or USB port, and a terminal emulator, such as PuTTy.
- Local management sessions also require a management cable. If your computer has a USB port, you may need to purchase a USB-to-Serial converter that is compatible with its operating system. An example is the VT-Kit3 converter from Allied Telesis. Refer to Figure 9 on page 35.
- If your computer has an RS-232 port, refer to “RJ-45 Style Serial Console Port Pinouts” on page 149 and “Console Management Cable with DB-9 Female and RJ-45 Connectors” on page 150 for the cable wiring specifications.
- You do not specify the router’s IP address to start local management sessions.
- The Console port supports the command line interface. It does not support web browser management or SNMP.

To start a local management session with the command line interface, perform the following procedure:

1. Connect your workstation to the Console port on the router:
   - If your workstation has a USB connector, use a USB-to-Serial converter, such as the VT-Kit3 from Allied Telesis. Refer to Figure 9 on page 35 and Figure 10 on page 36. The kit and driver are sold separately.
   - If your workstation has a DB-9 female connector, refer to “RJ-45 Style Serial Console Port Pinouts” on page 149 and “Console Management Cable with DB-9 Female and RJ-45 Connectors” on page 150 for the cable specifications.
2. Power on the router and wait several minutes for it to start the AlliedWare Plus management software. Refer to “Powering On the Router” on page 88.

3. Configure your VT-100 terminal or terminal emulation program as follows:

   - ❒ Baud rate: 9600 bps (The baud rate of the Console port is adjustable from 1200 to 115200 bps. The default is 9600 bps.)
   - ❒ Data bits: 8
   - ❒ Parity: None
   - ❒ Stop bits: 1
   - ❒ Flow control: None

   Note
   The port settings are for a DEC VT100 or ANSI terminal, or an equivalent terminal emulator program.

4. Press Enter. You are prompted for the name and password of the manager account.

5. Enter the default user name “manager” and password “friend” (without the quotes).

   Note
   User names and passwords are case sensitive.

   The router starts the local management session and displays the CLI prompt for the User Exec mode:

   ```
   awplus>
   ```

6. Go to “Verifying the Hardware Status” on page 96.

DHCP or DHCPv6 Server

This section contains the procedure for starting the first management session with the router on a network that has a DHCP or DHCPv6 server. To start the management session, perform the following procedure:

1. Enter the MAC address of the router in your DHCP or DHCPv6 server so that the server assigns an address to the router when you power it on. (The MAC address on the label on the bottom panel is assigned to the WAN ETH1 port.) Refer to your DHCP server’s documentation for instructions.

2. Connect one LAN port (ports 1 to 4) on the router to your network. For cable specifications, refer to “Cable Requirements” on page 51,

3. Power on the router and wait several minutes for it to start the AlliedWare Plus management software and obtain its IPv4 or IPv6 address from the DHCP server on your network.

4. On your management workstation, enter the router's assigned IP address from the DHCP server in an SSH client or the URL field of the browser.

   Note
   If this is not the first management session and the SSH and Telnet settings have not been set, it may be necessary to use Telnet instead of SSH to manage the router. Refer to the Note in "Starting a Management Session" on page 91.

5. Press Enter. You are prompted for the name and password of the manager account.

6. Enter the default user name "manager" and password "friend" (without the quotes).

   Note
   User names and passwords are case sensitive.

   If you are starting an SSH or a Telnet management session, the router displays the CLI prompt for the User Exec mode:

   ```
   awplus>
   ```

   If you are starting a web browser session, the router displays the Dashboard in your browser window, with the main navigation bar on the left side. Refer to Figure 56.

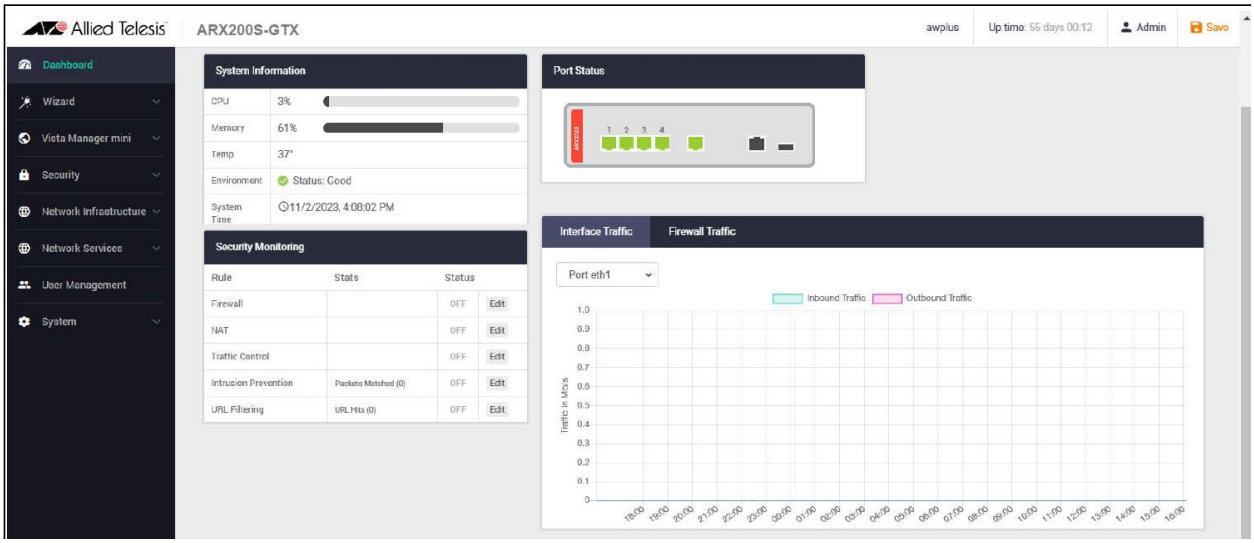


Figure 56. Graphical User Interface

7. Go to "Verifying the Hardware Status" on page 96.

Default IPv4 Address

The router comes with the default IPv4 address 192.168.1.1 and subnet mask 255.255.0.0. If your network does not have a DHCP or DHCPv6 server, you can still initially manage the router over the network using its default IPv4 address, as explained in the following procedure. To start the session, perform the following procedure:

1. Change the IP address of your workstation to 192.168.1.*n*/24 (255.255.0.0), where *n* is any number from 2 to 254.
2. Connect the Ethernet port on your workstation to one of the LAN ports on the router.
3. Power on the router and wait several minutes for it to start the AlliedWare Plus management software.
4. Do one of the following:
   - ❒ To manage the router with the web browser management windows, start your web browser on your management workstation and enter the IP address 192.168.1.1, the router's default IP address for VLAN1, in the URL field.
   - ❒ To manage the router with the CLI, start your SSH client and enter the IP address 192.168.1.1 in the client.

   Note
   If this is not the first management session and the SSH and Telnet servers have not been set, you might need to use Telnet instead of SSH to manage the router with the CLI. Refer to the Note in "Starting a Management Session" on page 91.
5. Press Enter.
6. When prompted, enter the default user name "manager" and password "friend" (without the quotes).

   Note
   User names and passwords are case sensitive.

   For a web browser session, the router displays the Dashboard in your browser window, with the main navigation bar on the left-hand side. Refer to Figure 56 on page 94.

   For an SSH or Telnet management session, the router displays the CLI prompt for the User Exec mode:

   ```
   awplus>
   ```
7. Go to "Verifying the Hardware Status" on page 96.

Verifying the Hardware Status

After powering on the router and waiting several minutes for it to start the AlliedWare Plus management software, perform the following procedure to verify the hardware status:

1. Start a local or remote command line or web browser management session on the router. Refer to “Starting a Management Session” on page 91.

   Note
   If you started a command line management session, go to step 3.

2. From the main navigation bar on the left side of the web browser window, select **System** - **CLI** to display the command line window.

3. Enter the SHOW SYSTEM ENVIRONMENT command in the User Exec or Privileged Exec mode of the management software.

4. Check the Status column. The status of all hardware components should be “OK”.

5. To continue using SSH to manage the router in future management sessions, enter these commands to enable the SSH server and disable the Telnet server:

   ```
   awplus> enable
   awplus# configure terminal
   awplus(config)# service ssh
   awplus(config)# no service telnet
   ```

6. To save your changes, enter the WRITE FILE or COPY RUNNING-ONFIG STARTUP-CONFIG in the Privileged Exec mode.

   Note
   If this is the first management session, the router creates a configuration file to store your changes.

7. Go to “Cabling the Copper Ports 1 to 4” on page 97 or “Completing the Hardware Installation” on page 99.

Cabling the Copper Ports 1 to 4

Here are the guidelines to cabling the copper ports:

- The ports have 8-pin RJ45 connectors.
- The cables should not exceed 100 meters (328 feet). Refer to “Cable Requirements” on page 51.
- The connectors on the cables should fit snugly into the ports, and the tabs should lock the connectors into place.
- The default status for the copper ports is enabled.
- The default setting for speed, duplex mode and MDI/MDIX is auto-negotiation.

Here are guidelines for setting port speed:

- The default setting for port speed is Auto-Negotiation. This setting is appropriate for ports connected to network devices that also support Auto-Negotiation.
- For ports connected to network devices that have fixed speeds, you should set their speeds manually with the SPEED command in the CLI of the AlliedWare Plus management software. This example sets the speed on port 2 to 100M:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# speed 100
```

Here are guidelines for setting port duplex mode:

- The default setting for duplex mode on ports is auto-negotiate. This setting is appropriate for ports connected to network devices that also support auto-negotiate for duplex mode.
- For ports connected to network devices that do not support auto-negotiate for duplex mode, you should set their duplex modes manually with the DUPLEX command. This example sets the duplex mode on port 3 to full:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# duplex full
```

Here are guidelines for setting MDI/MDIX on ports:

- The default MDI/MDI-X wiring configuration is automatic detection. This setting is appropriate for router ports that are connected to network devices that also support auto-MDI/MDI-X.

- For ports connected to network devices that do not support auto-MDI/MDIX, you should set the wiring configuration manually with the POLARITY command. The correct MDI/MDI-X setting for a router port with a fixed wiring configuration depends on the setting of the network device and whether the router and network device are connected with straight-through or crossover cable. If the devices are connected with straight-through copper cable, the wiring configurations of the ports on the router and network device must be opposite each other, such that one port uses MDI and the other MDI-X. If the devices are connected with a crossover copper cable, the wiring configurations of the ports on the router and network device must be the same. This example sets the MDI/MDIX setting on port 1 on the router to MDI:

  ```
  awplus> enable
  awplus# configure terminal
  awplus(config)# interface port1.0.4
  awplus(config-if)# polarity mdi
  ```

Completing the Hardware Installation

This section contains the following instructions:

- “Installing a USB Device,” next
- “Securing the Router with a Kensington Lock” on page 102
- “Registering the Product” on page 102

Installing a USB Device

The USB port on the front panel of the router supports these devices:

- USB storage device for storing or transferring router files. Refer to “USB Storage Device” on page 31.
- USB cellular modem for connecting the router to a cellular service provider. Refer to “USB Cellular Modem” on page 34.

Note
The router does not require a USB device for network operations. For background information, refer to “USB Port” on page 31.

Caution
You should always enter the UNMOUNT USB command in the Privileged Exec mode of the AlliedWare Plus management software before removing a USB storage device from the USB port, to avoid damaging files.

To install a USB device and secure it with the retainer and twist ties included with the router, perform the following procedure:

1. Insert the USB device in the USB port. Refer to Figure 57.

Figure 57. Installing a USB Device

2. You can cut one or two sections from the USB retainer to shorten it to make it more compatible with the USB device. Refer to Figure 58.

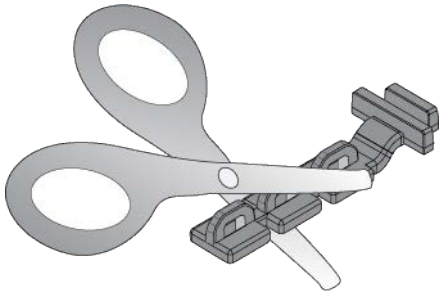


Figure 58. Shortening the USB Retainer

3. Affix one or more insulator tapes to the bottom pads of the USB retainer. Refer to Figure 59.

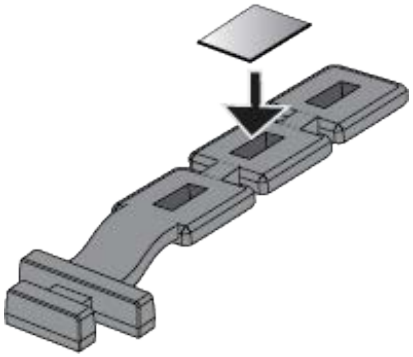


Figure 59. Affixing an Insulator Pad to the USB Retainer

4. Install the USB retainer in the slot above the USB device. Refer to Figure 60.

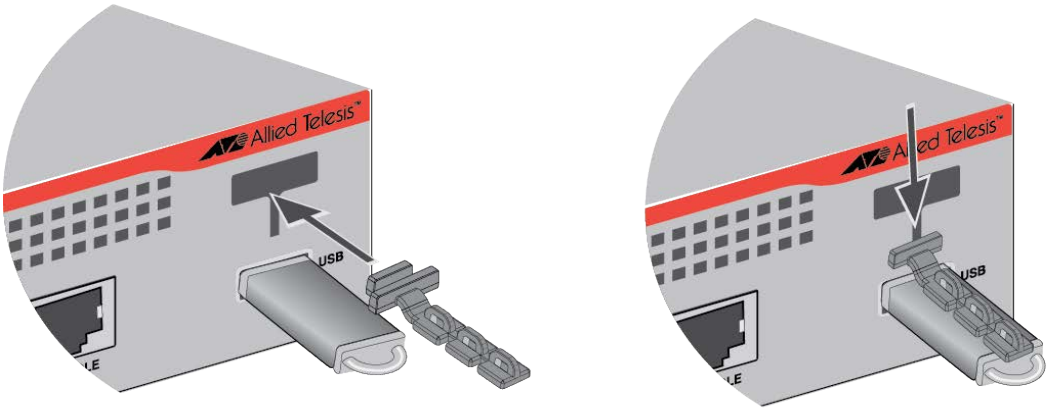


Figure 60. Installing the USB Retainer

5. To secure the device with twist ties, wrap a tie around the device and insert the end into the hole on the retainer and twist tie lock. Refer to Figure 61.

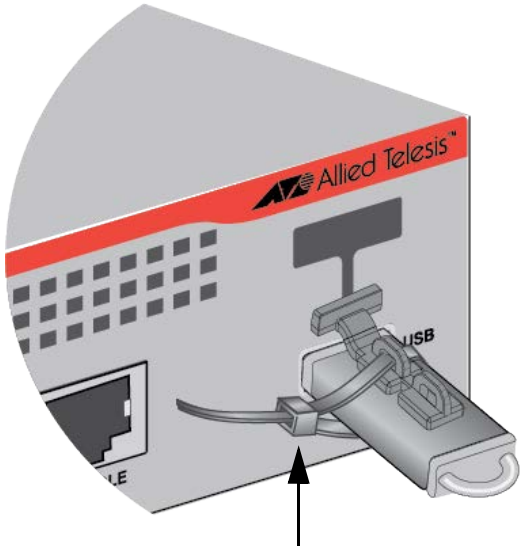


Figure 61. Securing the USB Device with a Twist Tie

6. Tighten the twist tie and cut off the excess. Refer to Figure 62.

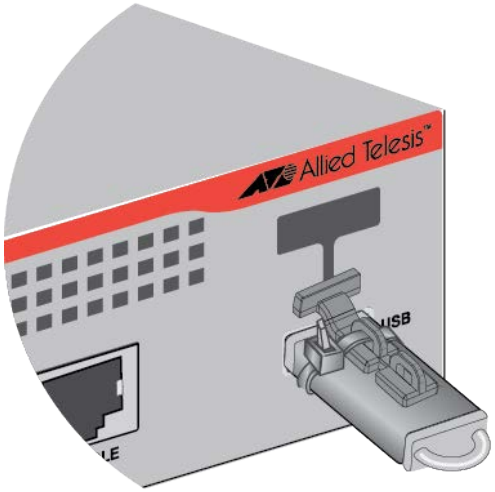


Figure 62. Securing the USB Device with One Twist Tie

7. Repeat with the second twist tie. Refer to Figure 63 on page 102.

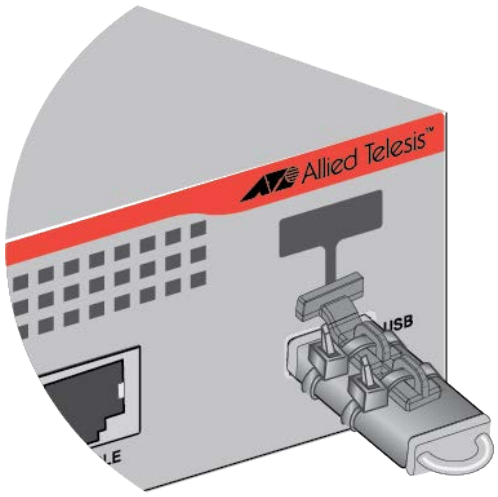


Figure 63. Securing the USB Device with Two Twist Ties

Securing the Router with a Kensington Lock

The router has a port for a Kensington lock (Standard K size) on the rear panel for physically securing the device at the installation site. Refer to Figure 64.

Figure 64. Kensington Lock Port (Standard K Size)

Refer to the instructions included with the Kensington lock for installation directions.

Note
Kensington locks are not available from Allied Telesis.

Registering the Product

To register the product with Allied Telesis, go to the **Net.Cover Registration** web page and complete the on-line registration form.

Note
You can view the serial number and MAC address of the product with the SHOW SYSTEM SERIALNUMBER and SHOW SYSTEM MAC commands in the User Exec or Privileged EXEC mode of the AlliedWare Plus management software. The MAC address is assigned to the WAN ETH1 port.

Chapter 7

Management Interfaces

This chapter contains introductions to the three management interfaces in the AlliedWare Plus management software and three tools to assist in managing your networks. The sections in the chapter include:

Note
Not all features may be supported on the product or available in the initial release. Refer to the product’s data sheet for further information.

Introduction

The router comes with the AlliedWare Plus management software pre-installed and with the following management interfaces:

- Command line interface (CLI). The industry-standard commands in this interface allow you to configure all the features and functions of the router, everything from switching, routing and firewall, to Unified Threat Management, TQ wireless access points, and more. You cannot disable the CLI. Refer to “Command Line Interface (CLI)” on page 106.
- Graphical user interface (GUI): The windows in this interface allow you to view device and traffic status, display system and environmental information, configure TQ wireless access points, and more. There is also a window for entering CLI commands so that you can enter commands without exiting the windows interface. The default setting for the GUI is enabled. Refer to “Graphical User Interface (GUI)” on page 107.
- SNMP: The router supports SNMPv1, v2c, and v3. The AlliedWare Plus management software supports a number of standard and enterprise SNMP Management Information Bases (MIBs), and device specific MIB objects, as well. The default setting for the SNMP servers on the routers is disabled. Refer to “Simple Network Management Protocol” on page 109.

You can manage the router as a standalone device by accessing the interfaces, as follows:

- Local CLI management is accessed through the Console port on the front panel of the device. You do not identify the IP address of the router to perform local management sessions.
- Remote CLI is accessed over your network with an SSH or Telnet client.
- Remote GUI is accessed over your network with an HTTP or HTTPS web browser.
- Remote SNMP is accessed over your network with a Network Management Station and the router’s MIBs.

The router saves it settings in a configuration file in memory. The file contains only those router settings that have been changed from their default values. You can create backup copies of the file as well as transfer the file to replacement units or to assign similar settings to multiple routers.

Note
The router does not come with a configuration file. It automatically creates the file the first time you save its settings with the WRITE FILE or COPY RUNNING-CONFIG command in the Privileged Exec mode in the CLI, or from the GUI.

Accessing the CLI or GUI to manage the router involves logging in to the management software with a username and password. The default credentials are:

- Username: manager
- Password: friend

Usernames and passwords are case-sensitive. The procedure for logging on the router is provided in “Starting a Management Session” on page 91.

Note
To protect the router from unauthorized access, Allied Telesis recommends changing the default username and password with the USERNAME and ENABLE PASSWORD commands in the Global Configuration mode in the CLI during your first management session.

Allied Telesis may periodically release updates to the AlliedWare Plus management software and make them available on the company’s website for download. To view the version number of the AlliedWare Plus management software on the router, enter the SHOW SYSTEM command in the User Exec or Privileged Exec mode in the CLI.

The three management interfaces are reviewed in the following sections:

- “Command Line Interface (CLI)” on page 106
- “Graphical User Interface (GUI)” on page 107
- “Simple Network Management Protocol” on page 109

This chapter also summarizes the following management tools for the router:

- “Autonomous Management Framework (AMF) Plus” on page 110
- “Vista Manager EX” on page 112
- “Vista Manager mini with Autonomous Wave Control (AWC)” on page 113

Note
Refer to the product’s data sheet for information on whether the tools come standard with the product or are sold separately.

Command Line Interface (CLI)

The AlliedWare Plus management software, the router's operating software, has an industry standard command line interface (CLI) with commands for monitoring and configuring all routing, firewall, and WAN functions. You can access the command line interface as follows:

- Locally through the Console port on the front panel of the router. You do not specify the router's IP address when starting a management session through the Console port.
- Remotely with a Secure Shell (SSH) or a Telnet utility.
- Remotely with the command line window in the UTM firewall web interface.

For further information, refer to the following documents on the Allied Telesis website:

- *Getting Started with the AlliedWare Plus Command Line Interface*
- *Command Reference: ARX200S UTM Firewall Running AlliedWare Plus*

Note
The default settings for the SSH and Telnet clients when the router is powered on for the first time are enabled and disabled, respectively. However, when the router creates its first configuration file, their settings in the file are reversed, with SSH disabled and Telnet enabled. Unless you manually change their settings, that will be their settings the next time you reboot or power cycle the router. For instructions, refer to "Verifying the Hardware Status" on page 96.

Graphical User Interface (GUI)

The AlliedWare Plus management software has a graphical user interface for monitoring the router. You can access it with a web browser over the network through the copper Ethernet ports, the WAN ETH1 port, or a USB cellular modem, with either HTTP or HTTPS. Refer to Figure 65.

Note
The GUI is not available through the Console port.

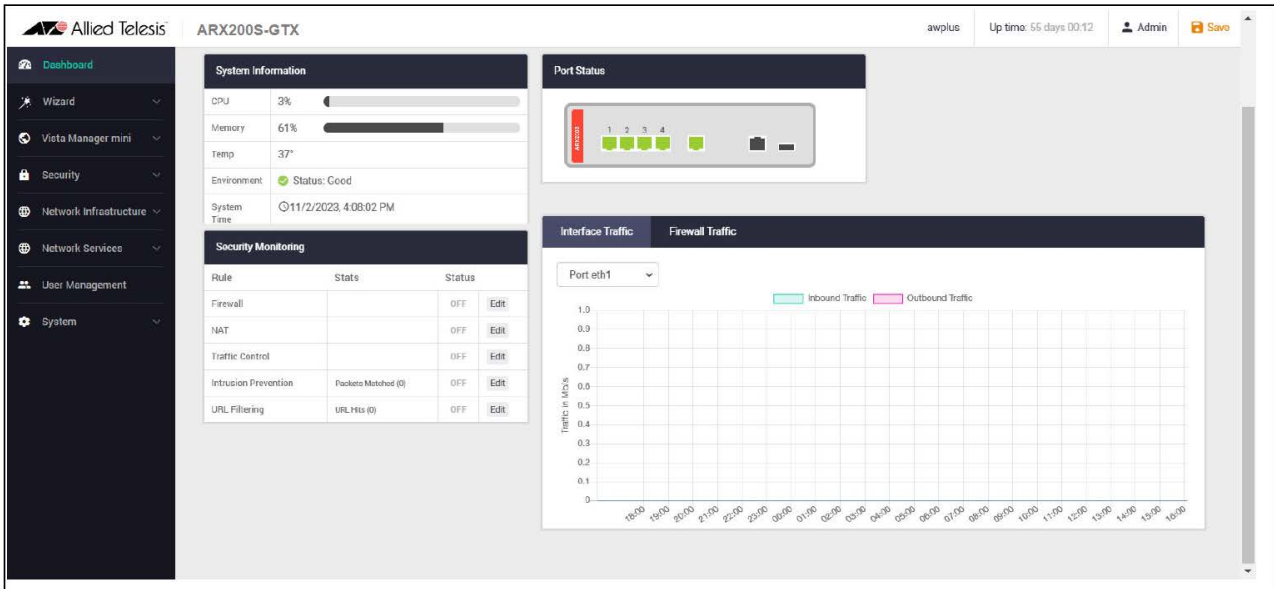


Figure 65. Graphical User Interface

Here are several functions available to you from the GUI:

- View status information in the Dashboard of the devices, interface and firewall traffic, and system and environmental information.
- View router and firewall status and traffic statistics.
- Display maps in Vista Manager mini showing the connections of the AlliedWare Plus wired devices This requires AMF Plus.
- Configure Allied Telesis TQ wireless access points with Autonomous Wave Controller in Vista Manager mini.
- View configuration files stored on network devices.
- Download new versions of the AlliedWare Plus management software to network devices.
- View and add new licenses to devices.
- Display security and threat protections status.

The GUI also has a window for entering CLI commands so that you can perform CLI commands without having to exit the GUI.

The GUI supports the following web browsers:

- Google Chrome™
- Mozilla Firefox™
- Microsoft Edge
- Internet Explorer™ 11 or later
- Apple Safari™

For further information, refer to the following documents:

- *Getting Started with the Device GUI on VPN Routers*
- *Getting Started with the Device GUI on UTM Firewalls*
- *User Guide: Wireless Management (AWC) with Vista Manager mini*
- *Vista Manager mini Technical Documents*

Simple Network Management Protocol

The ARX200S-GTX Router supports SNMP, with the following guidelines:

- The routers support SNMPv1, SNMPv2cv, and SNMPv3.
- SNMP is supported on the copper and WAN ETH1 ports. It is not supported on the Console port.
- The routers do not have default SNMPv1 or SNMPv2c communities.
- The Allied Telesis MIBs are available on the *Software Downloads* web site. The MIBs define objects specific to Allied Telesis products that are not supported by pubic MIBs. The MIB objects reside in the private(4) subtree, with the object identifier “alliedTelesis” {enterprise 207} OID 1.3.6.1.4.1.207.
- The routers have separate IPv4 and IPv6 SNMP agents that you can enable or disable independently. The default setting for the agents is enabled.
- The VLAN on the router where SNMP is conducted must have an IPv4 or IPv6 address. The router comes with the default VLAN “VLAN1”, with the default IP address 192.168.1.1 (255.255.0.0). All copper and WAN ETH1 ports are members of the default VLAN.
- The routers use UDP as the transport protocol, with UDP port 162 for SNMP trap messages and UDP port 161 for all other messages.
- If you are using SNMPv1 or SNMPv2c, Allied Telesis recommends creating complex community names and assigning access lists (standard numbered) with the IP addresses of authorized management stations to the community names. This is to protect the device from unauthorized access.
- You can configure the SNMP agents from the CLI or GUI.

For further information, refer to the following documents:

- *Simple Network Management Protocol (SNMP) Feature Overview and Configuration Guide*
- *Device Discovery and Monitoring using SNMP Feature Overview and Configuration Guide*
- *Support for Allied Telesis Enterprise MIBs in AlliedWare Plus Technical Guide*

Autonomous Management Framework (AMF) Plus

Autonomous Management Framework (AMF) Plus provides tools for simplifying and automating routine management tasks on the router. By designating an Allied Telesis device as the master of an AMF Plus network, you add these management functions to your network:

- Rather than having to configure network devices individually, you can group them together and manage them with the unified command line interface in AMF Plus. You define the groups by creating working-sets, which can contain one node, a subset of nodes, or all the nodes in an AMF Plus network.
- Managing network devices often means having to log in to each individually. But with the remote login feature, logging on routers designated as the master node allows you to connect to and perform commands on other AMF Plus nodes in the master node's area.
- AMF Plus master nodes can automatically backup the configuration files of their member nodes, including boot configurations, firmware, licenses, and user scripts. If an AWF Plus member node needs to be replaced, the AMF Plus master node can automatically recognize and configure the replacement unit by sending it the appropriate configuration file.
- AMF Plus master nodes can automatically distribute new AlliedWare Plus updates to the member nodes in their networks and monitor the status of the update processes.
- The master of an AMF Plus network can also backup the configuration files of TQ wireless access points. If a TQ device fails, you can instruct the master to download the appropriate configuration file to the replacement unit.

When AMF Plus is combined with Vista Manager mini, the latter application can display topology maps of the connections between AlliedWare Plus devices, including switches, routers, and TQ wireless access points.

Note the following guidelines:

- You can designate the ARX200S-GTX Router as the master or member node of an AMF Plus network. You cannot designate it as a controller node.
- As the master node, the ARX200S-GTX Router can manage up to ten AMF Plus nodes.

AMF Plus is managed with the command line interface in the AlliedWare Plus management software. For reference information, refer to the following documents:

- *AMF Plus Feature Overview and Configuration Guide*
- *How to Configure an AR-series Router as a Secure VPN Gateway and an AMF Node*
- *Getting Started with the AlliedWare Plus Command Line Interface*
- *Command Reference: ARX200S UTM Firewall Running AlliedWare Plus*

Vista Manager EX

Vista Manager EX is a graphical network monitoring and management tool for Allied Telesis AMF networks. It automatically creates a topology map of an AMF network of switches, routers, and wireless access points. It facilitates management of network devices from a dashboard that gives you a central overview of your network. From the dashboard you can monitor up-to-date network status and take action to resolve network problems. Vista Manager EX consists of the following tools and components:

- Dashboard - Displays network details and a network map of all devices connected in each area.
- Asset Management - Displays a complete list of all devices in your network and allows you to search for specific devices.
- Network Map: Displays a graphical topology map of your AMF network, from which you can view device information and perform basic management functions.
- Events - Displays a list of colored coded events.
- Network Services - Allows you to monitor the status of active network services and configure monitoring tasks.
- Allied Intent-based Orchestrator / AMF Plus - Provides network optimization, automation, management, and visualization. Also offers automation of branch security and WAN ETH1 bandwidth management.
- SD-WAN - Allows you to set performance metrics for applications, and load-balance traffic for improved network performance.
- User Management - Allows you to add, change, or delete Vista Manager EX users.
- System Management - Displays various system details such as the current version, serial number, and license information. It also allows you to manage the system configuration, such as SMTP settings;

For reference information, refer to the following documents:

- *Vista Manager EX User Guide*
- *Vista Manager EX Installation Guide*
- *Vista Manager EX Technical Documents*

Vista Manager mini with Autonomous Wave Control (AWC)

If your plans include managing AlliedWare Plus wired devices with AMF Plus or your network has TQ series wireless access points, then Vista Manager mini with AWC can be a valuable management tool for your wired and wireless networks. As shown in Figure 66, Vista Manager mini is integrated into the main menu in the router's GUI.

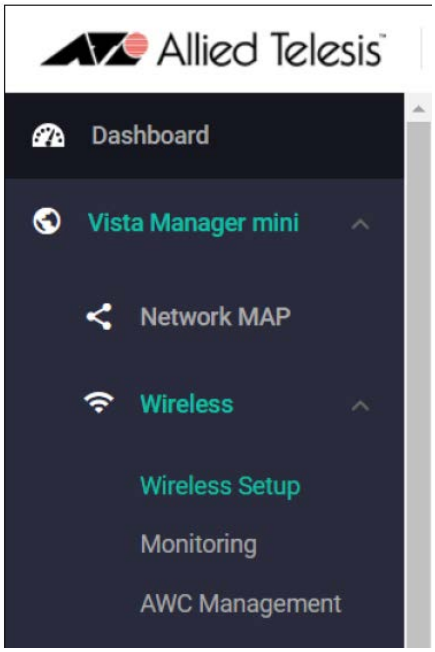


Figure 66. Vista Manager mini in the Router's GUI

When you select Network MAP, Vista Manager mini builds a network topology map with information from AMF Plus. The map includes wired AlliedWare Plus devices, including switches and routers, as well as TQ wireless access points. Here are some of the management functions available to you from the map:

- View the connections between devices.
- View device status information.
- View details on individual devices, such as model names, IP addresses, and MAC addresses.
- View heat maps of the wireless coverage of TQ access points.
- Add a background image and change node icons.

Selections under the Wireless menu option let you configure and manage TQ wireless access points from the GUI, either manually or automatically. AWC has an Auto Setup feature that determines the locations and signal strengths of the access points, and automatically configures their wireless outputs and channel selections to minimize coverage gaps and reduce interference.

The AWC on the router supports up to five TQ wireless access points. You can purchase a license to add support for ten additional TQ access points. The maximum number of access points the AWC can support is fifteen.

Note
The ARX200S-GTX Router does not support channel blankets (AWC-CB) and smart connect (AWC-SC).

Note
You can use AWC without AMF Plus. However, without the device information from AMF Plus, the topology map in Vista Manager mini will show all TQ wireless access points as directly connected to the router, including those indirectly connected through other network devices.

For reference information, refer to the following documents:

- *Vista Manager mini Technical Documents*
- *Wireless Management (AWC) with Vista Manager mini User Guide*

Chapter 8

Introduction to Firewall and Unified Threat Management Features

This chapter provides a brief introduction to the firewall and Unified Threat Management (UTM) features on the router. For a complete list of features, refer to the product's data sheet and the *Command Reference: ARX200S UTM Firewall Running AlliedWare Plus.* The chapter contains the following sections:

Note
Not all features may be supported on the product or available in the initial release. Refer to the product's data sheet for further information.

Firewalls

Firewalls are often the foundation of network defenses. They consist of definable rules that control the types of traffic permitted between trusted and untrusted networks, and between devices within networks. The rules are flexible. They can block entire categories of traffic from an entire network or allow specific applications into parts of your network and block them in others.

Firewalls have three definable building blocks called entities. To the entities you add rules and deploy tools that control the types of traffic and applications that can crossover to or enter other entities. The entities are:

- Zones - This entity represents the highest level in firewall hierarchies. A common practice is to define different zones for your internal trusted networks, external untrusted networks, such as the Internet, and any internal devices that need to be accessed from outside your network, such as web servers. Any rules or tools added to a zone apply to all the entities contained within it.
- Networks - This entity defines the logical groupings of functionally related devices that constitute internal or external networks. Examples might include company departments or functions, such as Sales, Engineering, and Customer Support.
- Hosts - This entity represents individual network devices, such as workstations, printers, and servers, within networks. As with the other entries, you can deploy rules that define which internal networks or other hosts they can access or be accessed by, and so define their available network resources. For instance, you can define rules for a workstation entity to control which servers or other internal networks it can access.

The three entities allow you to organize the task of adding and managing the rules and tools that control the traffic flows and the applications to which they belong. Rules that are to apply equally to multiple networks can be applied to a zone entity rather than to the individual networks themselves. Similarly, rules that should apply equally to all the nodes within a network can be applied to the corresponding network entity, rather than the individual nodes themselves. Finally, host entities give the greatest granularity of control by allowing for the assignment of rules to individual devices, when necessary.

To the entities you apply rules. One example is firewall rules. These rules filter traffic for specific applications, permitting or denying traffic between entities. For example, a company might block social media platforms company-wide, or permit access by a specific department, while blocking it from all other departments. The zone, network, and host entities allow for that flexibility,

Firewall rules have several primary elements. The first is the action, which defines what the router does when it encounters traffic matching a rule. The actions are listed here:

- Permit - Permits the specified traffic connection.
- Deny - Blocks the specified traffic connection without notifying the source node.
- Reject - Blocks the connection and attempts to notify the source to properly close the connection, when possible.
- Log - Enters an entry in the log each time a connection matches the rule, with no effect on connections. Traffic connections continue to be compared against subsequent rules.

Other important elements of firewall rules are the source and destination entities of the traffic. They specify where traffic is coming from as well as where is it going to, in terms of zone, network, and node entities, as described earlier.

The target applications to which rules apply are another important part of firewall rules. There are several ways to define applications:

- You can use the default applications that come with the firewall and are available as soon as you activate the feature.
- You can add applications yourself by defining their properties, such as protocol ICMP-type, ICMP-code, and source and destination ports.
- You can activate Deep Packet Inspection (DPI) to add its built-in list of applications. Refer to “Deep Packet Inspection” on page 122.
- Finally, you can expand DPI by subscribing to the third-party Procera and its extensive up-to-date application library.

You can also apply rules to entities to control the bandwidth the router allocates to applications. These are referred to as traffic control rules. For example, you might permit music streaming sites into your network, but limit their bandwidth to ensure that the router gives your company’s business traffic the higher priority on the Internet connection. Refer to “Traffic Control” on page 119.

Preventing the private IP addresses of your company’s devices from ending up on the Internet is also a category of firewall rules. The router prevents this by replacing the source addresses of traffic leaving your company’s network with a shared public network address for routing through the Internet. Consequently, the public Internet does not see the private IP address on your network. These are referred to as Network Address Translation (NAT) rules. Of course, when ingress traffic arrives from the Internet, the router replaces the shared public network address in the ingress traffic with the corresponding private IP addresses. Refer to “Network Address Translation (NAT)” on page 126.

For further information, refer to the following documents:

- *Getting Started with the Device GUI on UTM Firewall*
- *Firewall and Network Address Translation (NAT) Feature Overview and Configuration Guide*
- *Traffic Control Feature Overview and Configuration Guide*
- *Getting Started with the AlliedWare Plus Command Line Interface*
- *Command Reference: ARX200S UTM Firewall Running AlliedWare Plus*

Traffic Control

Periods of heavy network activity can result in congestion in the router's egress interfaces. These events may cause the router to discard packets in oversubscribed egress queues, which may adversely affect network quality and performance. Traffic Control, also referred to as Quality of Service (QoS), can mitigate these occurrences by enabling the router to evaluate which packets to retain or discard, as well as the order in which to transmit packets from its queues and interfaces.

Classes and policies in Traffic Control define the traffic flows and actions taken by the router. Some of the definable functions include:

- Traffic flows: Identifying traffic flows is an important part of Traffic Control. Some flows are likely to be more time-sensitive than others, and thus require a higher priority than other traffic. Identifying traffic flows for this solution is the same as for other router solutions, such as Policy-base Routing and Firewall Control. Applications can be added manually with the Application mode in the CLI, or automatically with DPI. Refer to "Deep Packet Inspection" on page 122.
- Priority levels: Assigned to classes and, in turn, to egress queues, priority levels typically reflect the time-sensitive characteristics of traffic flows. Traffic flows of high priorities are given preferential treatment for transmission over flows with lower priorities.
- Scheduling policies: Specifies the order in which the router transmits packets from egress queues. Choices are Strict Priority, Weighted Round Robin, and Hierarchical Token Bucket.
- Setting the DSCP values in egress packets. Conveys to downstream devices information about the priority assigned by the router to traffic flows.
- Setting the number and size of egress queues on interfaces. Virtual egress queues are added to interfaces as you assign traffic classifications rules.
- Setting bandwidth limiting and burst control for Strict Priority and Hierarchical Token Bucket. Weighted Round Robin does not support bandwidth limiting.
- Virtual bandwidth: This sets limits of the total bandwidths that the router permits interfaces to transmit.

For further information, refer to the following documents:

- *Traffic Control Feature Overview and Configuration Guide*
- *Application Awareness Feature Overview and Configuration Guide*
- *Command Reference: ARX200S UTM Firewall Running AlliedWare Plus*

Web Control

Web Control allows network administrators to control the types of websites that employees on trusted networks can access on untrusted networks, through the router. Websites are grouped into categories, with each category consisting of a set of rules that determine whether users can access its sites. Users who attempt to access websites belonging to prohibited categories are blocked and instead receive notification messages.

Web Control uses a third-party website categorizer. There are approximately 100 categories, and web sites can belong to more that one category. The categories and their lists of websites are updated regularly. When the router receives an HTTP request from a user, it sends the embedded URL of the website to the website classifier engine to determine the category of the site. After receiving back the category, it examines the corresponding rules of the category and either blocks or permits access to the website, in accordance with the rules.

Once the router has processed an HTTP request, it caches the request so that it can respond to further requests to the same website without having to query the classifier engine. This reduces processing time and enables the router to respond in real-time.

You may create a limited number of customized categories that supersede the standard categories. You might use this feature to identify individual websites that you want to permit access to even when they belong to standard categories that are blocked. You can also create zones in which you can specify IP addresses of employees who can access specific websites that are blocked to other employees.

For reference information, refer to the following documents:

- *UTM Firewall Overview*
- *Advanced Network Protection Feature Overview and Configuration Guide*
- *Command Reference: ARX200S UTM Firewall Running AlliedWare Plus*

URL Filtering

URL Filtering is similar to Web Control in that you use it to permit or block access by web users to designated HTTP and HTTPS websites, in the following three ways:

- Create a built-in whitelist of up to 1000 URLs of approved websites.
- Create a built-in blacklist of up to 1000 URLs of websites to be blocked.
- Subscribe to an advanced blacklist from a third-party subscription service.

You can use the three methods simultaneously.

HTTP and HTTPS requests from users are first compared against the whitelist, if present. The router permits access to URLs in the whitelist, even for sites also included in a blacklist.

The primary difference between Web Control and URL Filtering is that the former provides a greater level of control over web site access. The web sites are grouped into categories to which you assign rules. You can also configure Web Control such that the router permits specified users to access websites while blocking others. In comparison, URL Filtering enforces the same rules of allowing or denying access to web sites to all users.

The default setting of URL Filtering is disabled.

Note
The built-in URL Filtering whitelist and blacklist do not require a license. However, the advanced URL Filtering blacklist does require a software bundle license. Refer to the product's data sheet for license information.

For reference information, refer to the following documents:

- *URL Filtering Feature Overview and Configuration Guide*
- *UTM Firewall Overview*
- *Advanced Network Protection Feature Overview and Configuration Guide*
- *Command Reference: ARX200S UTM Firewall Running AlliedWare Plus*

Deep Packet Inspection

Deep Packet Inspection (DPI) allows the router to examine and categorize traffic according to the applications of the packets themselves. DPI works by looking at the relationships between packets and matching them to a database or libraries of predefined application signatures. Examples of application categories include social networking, instant messaging, and file sharing. The router has the following database options:

- Built-in database: This limited database comes with the AlliedWare Plus management software and becomes available as soon as you enable DPI on the router.
- Subscription libraries: This is a subscription service provided by the third-party Procera. Its application and category databases are maintained and updated daily.

Note
The built-in database does not require a license. However, the subscription for the DPI libraries from Procera does require a software bundle license. Refer to the product's data sheet for license information.

DPI is not used by itself. Instead, you use it in combination with other router solutions to create rules that control the router's response to specified application packets and traffic flows identified by DPI. Here are UTM solutions that use DPI:

- Firewall Control: Determines which application connections the router permits or rejects. Refer to "Firewalls" on page 116.
- Traffic Control: Controls how the router handles application packets and flows during periods of interface congestion caused by heavy traffic. Refer to "Traffic Control" on page 119.
- Web Control: Blocks individuals on the private, trusted network from accessing designated web sites on external networks, such as the Internet. Refer to "Web Control" on page 120.

You can also use DPI with these router solutions:

- Network Address Translation: Replaces the IP addresses in application packets from devices on your private, trusted network with a public address for the Internet. Refer to "Network Address Translation (NAT)" on page 126.
- Policy-based Routing: Assigns the next-hop to application packets. This solution lets you control the network paths that application packets take to reach their destinations. Refer to "Policy-based Routing (PBR)" on page 128.

- SD-WAN: Enables the router to evaluate the transmission qualities of the WAN and VPN connections over Internet Service Provider (ISP) networks, and direct traffic flows over connections best suit to their requirements. Refer to “Software-Defined Wide Area Network (SD-WAN)” on page 129.
- Web Redirect: Redirects ingress HTTP client requests to a specified URL, on either a periodic or permanent basis. Refer to “Web Redirect” on page 131.

DPI is managed with the command line interface. Its default setting is disabled. For further information, refer to the following documents:

- *UTM Firewall Overview*
- *Application Awareness Feature Overview and Configuration Guide*
- *Advanced Network Protection Feature Overview and Configuration Guide*
- *Command Reference: ARX200S UTM Firewall Running AlliedWare Plus*

IP Reputation

IP Reputation is designed to guard networks against external sources of spam, viruses and other malicious activity. It maintains lists of suspect IP addresses that are grouped into categories. The addresses are assigned scores that are compared against thresholds that determine the actions taken by the router when encountering packets with suspect IP addresses. The router discards ingress packets whose source or destination IP addresses meet the specified thresholds and scores.

IP Reputation is a subscription service. The lists, categories, and scores of suspect IP addresses are provided by a third-party and automatically updated regularly. This ensures that the router protects a network against the latest in external threats. The protection is also configurable. You can create a whitelist of approved IP addresses that would otherwise be blocked by IP Reputation. Examples could be IP addresses of sites that you deem no longer pose reasonable threats to your network, but are labeled as suspect in IP Reputation.

IP Reputation is managed with the command line interface in the AlliedWare Plus management software. The default setting for IP Reputation on the router is disabled.

Refer to the product's data sheet for license information.

For reference information, refer to the following documents:

- *UTM Firewall Overview*
- *Advanced Network Protection Feature Overview and Configuration Guide*
- *Command Reference: ARX200S UTM Firewall Running AlliedWare Plus*

Intrusion Prevention System

The Intrusion Prevention System (IPS) on the router monitors inbound and outbound traffic for suspicious or malicious traffic in real-time by comparing threats against a known signature database. IPS has the following two levels:

- Built-in IPS: This level of support consists of a set of built-in categories in the AlliedWare Plus management software of possible suspect traffic. It has several hundred categorized rules, providing protection against many known common threats, such as invalid checksums, gre-decoder event anomalies, and HTTP anomalies. This level of protection comes standard with the AlliedWare Plus management software on the router and does not require a subscription license.
- Advanced IPS: This is a subscription service from the third-party vendor Proofpoint and their ET Pro Ruleset. Updated daily, it can detect a much wider range of malicious attacks, such as malware delivery, distributed denial-of-service (DDOS) attacks, and protocol and application anomalies. Associated threats are analyzed and categorized, producing a rule-set consisting of tens of thousands of rules. Advanced IPS requires the optional AT-FL-ARX2-UTM-02-2023 bundle pack license. Built-in IPS and Advanced IPS can be used simultaneously.

The default setting for IPS on the router is disabled. This feature is managed with the command line interface in the AlliedWare Plus management software:

For reference information, refer to the following documents:

- *UTM Firewall Overview*
- *Advanced Network Protection Feature Overview and Configuration Guide*
- *Command Reference: ARX200S UTM Firewall Running AlliedWare Plus*

Network Address Translation (NAT)

If your company's private, trusted network is connected to a public network, as most are these days, you should protect the IP addresses of your devices by restricting them only to the trusted network. Packets leaving your network to a public network, such as the Internet, should have their IP addresses replaced with one or more shared public IP addresses. This is the function of NAT.

When NAT is enabled and configured, the router acts as an IP address agent between the devices on your trusted network and a public network. When the router receives packets from devices on the trusted network that are intended for the public network, it replaces the IP addresses with a valid, public address. Of course, NAT also works in reverse. When packets arrive from a public network intended for devices on your trusted network, the router replaces the shared public address in the packets with the appropriate private addresses.

To configure NAT you create rules that specify the types of IP address replacements that the router should perform. There are three types of rules:

- Masquerading rule: This rule instructs the router to use one public IP address for multiple devices on the trusted network. To make the different packet flows identifiable, they are given unique protocol source port numbers (TCP or UDP).
- Port Forwarding: This rule configures the router to forward packets from remote devices on a public network to specific devices or services on your network, such as web servers.
- Netmap rules: This rule configures the router to translate only the subnet portions of IP addresses of the devices on the trusted network, and not the host portion.

When you create NAT rules, you may identify applications with DPI. You can define the applications yourself with the Application mode in the CLI, or with DPI, which adds the applications to the router automatically. Refer to "Deep Packet Inspection" on page 122.

For further information, refer to these documents:

- *Firewall and Network Address Translation (NAT) Feature Overview and Configuration Guide*
- *Getting Started with the Device GUI on UTM Firewalls*
- *Advanced Network Protection Feature Overview and Configuration Guide*
- *Application Awareness Feature Overview and Configuration Guide*

- *How to Configure an AR-series Router as a Secure VPN Gateway and an AMF Node*
- *OpenVPN Feature Overview and Configuration Guide*
- *Command Reference: ARX200S UTM Firewall Running AlliedWare Plus*

Policy-based Routing (PBR)

Policy-based routing (PBR) lets you designate the next-hop that the router assigns to specific application packets and traffic flows. This solution lets you control the routes that packets are to take through your network. You might use this feature to improve network performance by directing time-sensitive traffic, such as voice or video packets, to high quality or dedicated transmission paths, or to improve network resiliency by designating secondary paths for traffic flows when primary paths are down.

Here are some of the feature's configurable parameters:

- You identify the applications with DPI. Refer to "Deep Packet Inspection" on page 122.
- You can enter the next-hop of a route by the device's IP address or the egress interface on the router. The latter is useful when the route is over a tunnel or PPP link, where the next-hop is not relevant or unknown.
- You can specify whether the route of a traffic flow is to be reevaluated if there is an update to the application in DPI.
- You can also log debugging messages to troubleshoot any problems.

You can combine PBR with other router features to enforce more control over traffic routing decisions. For instance, you might use triggers to control the days and times when specified traffic flows are to use designated routes, or with Link Health Monitoring probes in SD-WAN to test link quality.

The router supports both IPv4 and IPv6 routes.

Note
Network packets directed to the router itself, such as management packets, are not affected by PBR.

For further information, refer to the following documents:

- *Policy-based Routing Feature Overview and Configuration Guide*
- *Route Selection Feature Overview and Configuration Guide*
- *Internet Protocol (IP) Addressing and Protocol Feature Overview and Configuration Guide*
- *Command Reference: ARX200S UTM Firewall Running AlliedWare Plus*

Software-Defined Wide Area Network (SD-WAN)

Software-Defined Wide Area Network (SD-WAN) improves the performance of a network by enabling the router to evaluate the transmission qualities of the WAN and VPN connections over Internet Service Provider (ISP) networks. The router can then dynamically direct traffic flows over connections best suited to the application types. For instance, you can configure SD-WAN so that the router directs traffic from time-sensitive applications, such as voice and video, over VPN connections on ISP networks with the highest transmission quality, and nonsensitive traffic, such as bulk file transfers, to lesser quality links. Should the performance of a VPN link fall below the requirements of its application traffic, the router can dynamically redirect the traffic to another VPN connection that does meet the traffic's requirements.

SD-WAN requires a minimum of two Internet connections from different ISPs between sites, such as between branch offices and a central office. The router tests the Internet connections by transmitting probes that test for jitter, latency, packet-loss, and consecutive probe loss. You can configure the probes to match your network environment and application requirements, Examples of adjustable probe parameters include the probe type (i.e., ICMP or HTTP), the transmission interval, and IP version (i.e., IPv4 or IPv6).

After testing the connections, the router matches the application traffic flows to the connections according to acceptable performance metrics. The metrics that define what is acceptable for VPN performance are detailed in profiles, which specify how much jitter, latency, packet loss, and consecutive probe loss are acceptable for different traffic flows.

The router identifies traffic applications with DPI. As explained in "Deep Packet Inspection" on page 122, this tool categorizes traffic based on the corresponding applications of the packets, such as social networking, instant messaging, and file sharing. DPI identifies applications by looking at the relationships between packets and matching them to a database of predefined application signatures.

After identifying a traffic flow with DPI, the router can select the VPN connection and ISP that best matches the flow's performance requirements. It then directs the packets of the traffic flow to the designated connection.

Allied Telesis SD-WAN supports both IPv4 and IPv6 traffic flows.

SD-WAN is configured with the command line interface. For further information, refer to the following documents:

- *What is SD-WAN*
- *Lifting the Lid - Explaining SD-WAN*

- *Software Defined WAN (SD-WAN) Feature Overview and Configuration Guide*
- *Command Reference: ARX200S UTM Firewall Running AlliedWare Plus*

Web Redirect

This feature allows you to configure the router to redirect ingress HTTP client requests to a specified URL, on a periodic or constant basis. When you enable the feature you can exclude specified client requests from being redirected. With the EXCLUDE APP command in the Web Redirect Configuration mode, you can exclude HTTP client requests from specified applications. For further information, refer to the *Web Redirect Feature Overview and Configuration Guide*.

UTM Offload

The UTM Offload feature lets you offload the operations of several UTM security services from the router to another physical or virtual device. This can improve the router's performance by freeing up memory and CPU resources for other routing functions. Here are the UTM firewall services you can offload from the router to a secondary device:

- URL Filtering
- IP Reputation
- Intrusion Protection System

The router automatically manages the secondary device by functioning as a Pre-Boot Execution Environment (PXE) server. It boots, configures, and manages the secondary device, and then configures itself to send network traffic to the secondary device for processing. However, even though the firewall services are running on the secondary device, they will appear to be running directly on the router.

Here are several basic guidelines:

- The UTM Offload feature and the licenses for the offloaded UTM firewall service are installed on the router, not the secondary device.
- A second set of licenses for the secondary device is not required.

Here are the requirements for the secondary device:

- It must have a serial port.
- Its connection to the router must be direct, without any intermediary devices, such as switches or media converters, between the two devices.
- The interface must be configured with IPv4. UTM Offload does not support IPv6.
- The Ethernet connection on the secondary device must support a maximum transmission unit (MTU) of 1588 or higher.
- The secondary device must support PXE.
- The secondary device must be configured to boot from the router. This is usually accomplished by enabling PXE boot in the BIOS settings.

For further information, refer to the following documents:

- *United Threat Management (UTM) Offload Feature Overview and Configuration Guide*

- *Advanced Network Protection Feature Overview and Configuration Guide*

Note
Allied Telesis does not recommend activating both UTM Offload and Web Control on the router. The results may be unpredictable.

Chapter 9
Troubleshooting

This chapter contains suggestions on troubleshooting problems with the router.

> **Note**
> For further assistance, contact Allied Telesis Technical Support at **www.alliedtelesis.com/services-support**.

Problem 1: The Ethernet LAN and WAN ETH1 ports are connected to active network devices, but the port LEDs are off.

Solutions: The router might be operating in the low power eco-friendly LED mode. To turn on the LEDs, enter the NO ECOFRIENDLY LED command in the Global Configuration mode in the command line interface of the AlliedWare Plus management software, as shown here. The default mode for the eco-friendly LED mode is off:

```
awplus> enable
awplus# configure terminal
awplus(config)# no ecofriendly led
```

Problem 2: An Ethernet LAN port or the WAN ETH1 port is connected to an active network device, but the link and activity LEDs are off, indicating the router and network device have not established a link.

> **Note**
> Copper ports may require up to five to ten seconds to establish links to network devices.

Solutions: Try the following:

- The RJ45 connectors on the copper cable might not be securely connected to the ports on the router and network device. Check that the cable connectors are securely connected to the ports.
- Connect another network device to the port with a different cable. If the port is able to establish a link, then the problem is with the cable or the other network device.

- The copper cable might be too long or the wrong category. Verify that the cable does not exceed 100 meters (328 feet) and that it is the correct category by referring to “Cable Requirements” on page 51.
- The router may have blocked the port because the spanning tree protocol detected a loop in the network topology. The default setting for RSTP on the router is enabled on all ports. To view the spanning tree status on the ports, use the SHOW SPANNING-TREE command in the User Exec or Privileged Exec mode. This example displays the spanning tree status of LAN port 2:

  ```
  awplus> enable
  awplus# show spanning-tree interface port1.0.2
  ```

- If the network device has a port speed of 10M, 100M or 1000M, the copper ports on the router and network device might be set to the same MDI/MDIX wiring setting. Note the following:

  - MDI/MDIX is not applicable to speeds above 1000M.
  - The ports on the router and network device must have different wiring settings, with one device set to MDI and the other to MDIX.

  The MDI/MDIX setting is controlled with the POLARITY command in the Interface Configuration mode. The default setting is auto-detection. Review the documentation included with the network device for its MDI/MDIX setting on its network port. If it has a fixed setting, try manually setting the router port to the opposite setting. For example, if the network device on LAN port 2 of the router has a fixed setting of MDIX at 100M, you would enter these commands to set the router’s port to MDI:

  ```
  awplus> enable
  awplus# configure terminal
  awplus(config)# interface port1.0.2
  awplus(config-if)# speed 100
  awplus(config-if)# polarity mdi
  ```

- The port may have been manually shutdown. To view the status of a port, use the SHOW INTERFACE command in the User Exec or Privileged Exec mode. This example displays the status of LAN port 4:

  ```
  awplus> show interface port1.0.4
  ```

  To bring up a port that is shutdown, use the NO SHUTDOWN command in the INTERFACE mode. The following example brings up LAN port 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no shutdown
```

Problem 3: The connection between a router port and a network device is slow or intermittent.

Solutions: Try the following:

- The RJ45 connectors on the copper cable might not be securely connected to the ports on the router and network device. Check that the connectors are securely connected to the ports.
- The copper cable may be faulty. Try replacing the cable.
- The network device may be experiencing a problem. Try replacing the device.
- The network device might be connected to a router port that does not support its speed. Review the following:
  - ARX200S-GT Router - Ethernet LAN ports 1 to 4 and the WAN ETH1 port support speeds of 10/100/1000M.
  - ARX200S-GTX Router - Ethernet LAN ports 1 to 2 support speeds of 10/100/1000M.
  - ARX200S-GTX Router - Ethernet LAN ports 3 and 4 and the WAN ETH1 port support Multi-Gigabit 100M/1000M/2.5G/5G/10G.

  For further information, refer to “Front and Rear Panels” on page 16.
- If the network device supports only one speed, a speed mismatch may have occurred if the router port is using Auto-Negotiation, the default setting. It may be necessary to set the speed manually on the router port with the SPEED command in the Interface Configuration mode. For example, if the network device connected to LAN port 2 on the router has a fixed speed of 1000M, the commands to configure the LAN port to the fixed speed 1000M would be:

  ```
  awplus> enable
  awplus# configure terminal
  awplus(config)# interface port1.0.2
  awplus(config-if)# speed 1000
  ```

  or:

  ```
  awplus(config-if)# speed auto 1000
  ```

- A duplex mode mismatch between a network device and a router port can result in reduced performance. Supported duplex mode settings on the router ports are auto, half, or full duplex. As an example, a duplex mode mismatch can occur if a network device that has a fixed duplex mode of full duplex is connected to a router port operating in auto or half duplex mode.

  The command for setting the duplex mode is the DUPLEX command in the Interface Configuration mode. The default setting is auto-negotiation. Review the network device's documentation for its duplex mode setting. If the device supports only half or full duplex, try manually setting the duplex mode on the router's port to the same setting. For example, if the network device on LAN port 3 on the router has a fixed duplex mode setting of full duplex, you would enter the following commands to set the LAN port to full duplex:

  ```
  awplus> enable
  awplus# configure terminal
  awplus(config)# interface port1.0.3
  awplus(config-if)# duplex full
  ```

- Examine the physical route of the copper cable to determine if it comes in close proximity to electromagnetic devices, such as factory equipment or lighting fixtures. Electromagnetic emissions may interfere with the transmission of network traffic over copper cables. If necessary, reroute the copper cable away from electromagnetic devices.

Problem 4: Remote SSH management sessions stopped working after the router was rebooted or power cycled.

Solution: The default settings for the SSH and Telnet clients when the router is powered on for the first time are enabled and disabled, respectively. However, when the router saves its first configuration file, their settings in the file are reversed, with SSH disabled and Telnet enabled. Unless you manually change their settings, that will be their settings the next time you reboot or power cycle the router.

To continue using SSH instead of Telnet to manage the router in subsequent management sessions, enter these command to enable the SSH server and disable the Telnet server:

```
awplus> enable
awplus# configure terminal
awplus(config)# service ssh
awplus(config)# no service telnet
```

Problem 5: The router functions intermittently.

Solutions: Try the following:

- The AC power source might be faulty. Try connecting the router to a different power source.
- The AC power source might be fluctuating above or below the approved operating range for the router. Use the SHOW SYSTEM ENVIRONMENT command in the User Exec or Privileged Exec mode to verify that the input voltage from the power source is stable and within the approved operating range:

  ```
  awplus# show system environment
  ```

- There may be a problem with one or more of the voltages on the circuit board. Use the SHOW SYSTEM ENVIRONMENT command to view their status.
- The router may be overheating. Verify that the location of the router allows for adequate airflow. Also confirm the status of the internal fan with the SHOW SYSTEM ENVIRONMENT command in the User Exec or Privileged Exec mode.
- The AC power cord might not be securely connected to the router or the AC power source. Verify that the power cord is securely connected to the AC connector on the rear panel of the router and the AC power source.
- The power cord might be faulty. Try replacing it.

Problem 6: The router shuts down.

Solutions: Try the following:

- The AC power cord might be disconnected. Verify that the power cord is securely connected to the AC connector on the rear panel of the router and the AC power source.
- The AC power source might be powered off or have failed. Verify that the AC power source is powered on or try connecting the router to a different AC power source.
- The router may have overheated. Verify that the location of the router allows for adequate airflow. Review the guidelines in “Choosing a Site for the Router” on page 43.
- For the ARX200S-GTX Router, when the router is powered on again, view the operational status of its internal fan by entering the SHOW SYSTEM ENVIRONMENT command in the User Exec or Privileged Exec mode in the command line interface.
- The router experienced a hardware or software failure.
- The router shutdown from a power surge.

- The power supply may have failed.
- The power cord might be faulty. Try replacing it.

Appendix A
Technical Specifications

This appendix contains the following sections:

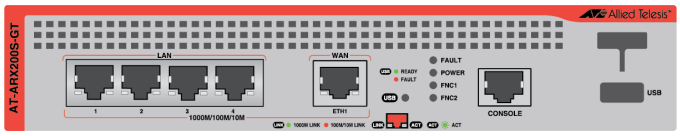
Physical Specifications

Table 13 lists the hardware specifications of the ARX200S-GT Router.

Table 13. ARX200S-GT Router Hardware Specifications

Router Dimensions (W x D x H)	210 x 220 x 42.5 mm (8.27 x 8.66 x 1.67 in.)
Router Weight	1.322 kg (2.91 lb.)
Router Weight with Shipping Box	1.974 kg (4.35 lb)
Recommended Minimum Ventilation on All Sides	10 cm (4.0 in)

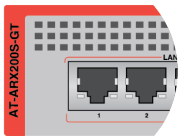
Width



210 mm (8.27 in.)

Height

42.5 mm (1.67 in.)



Depth

220 mm (8.66 in.)

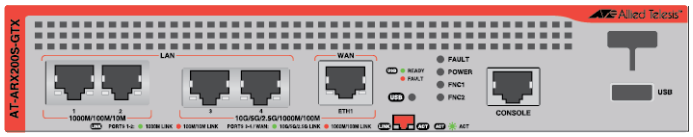
Figure 67. ARX200S-GT Router Dimensions

Table 14 lists the hardware specifications of the ARX200S-GTX Router.

Table 14. ARX200S-GTX Router Hardware Specifications

Router Dimensions (W x D x H)	210 x 220 x 42.5 mm (8.27 x 8.66 x 1.67 in.)
Router Weight	1.33 kg (2.93 lb.)
Router Weight with Shipping Box	2.2 kg (4.9 lb)
Recommended Minimum Ventilation on All Sides	10 cm (4.0 in)

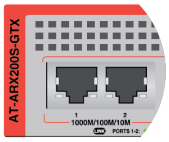
Width



210 mm (8.27 in.)

Height

42.5 mm (1.67 in.)



Depth

220 mm (8.66 in.)

Figure 68. ARX200S-GTX Router Dimensions

Power and Environmental Specifications

Table 15 lists the power specifications of the ARX200S-GT Router.

Table 15. ARX200S-GT Router Power Specifications

Input Voltage	100-240 VAC~, 2.5A maximum, 50/60 Hz
Maximum Power Consumption	20.7 watts
Heat Dissipation	70.59 BTU/hr

Table 16 lists the power specifications of the ARX200S-GTX Router.

Table 16. ARX200S-GTX Router Power Specifications

Input Voltage	100-240 VAC~, 2.5A maximum, 50/60 Hz
Maximum Power Consumption	39.2 watts
Heat Dissipation	133.75 BTU/hr

Note
The input voltage, current, and frequency can be found on the ratings label on the bottom panel of the routers.

Table 18 lists the environmental specifications of the ARX200S-GT Router.

Table 17. ARX200S-GT Router Environmental Specifications

Operating Temperature Range	0°C to 50°C (32°F to 122°F)
Storage Temperature	-25°C to 70°C (-13°F to 158°F)
Operating Humidity	5% to 90% noncondensing
Storage Humidity	5% to 95% noncondensing
Maximum Operating Altitude	3,000 m (9,842 ft)
Maximum Nonoperating Altitude	4,000 m (13,100 ft)

Table 18 lists the environmental specifications of the ARX200S-GTX Router.

Table 18. ARX200S-GTX Router Environmental Specifications

Operating Temperature Range	0°C to 60°C (32°F to 140°F)
Storage Temperature	-25°C to 70°C (-13°F to 158°F)
Operating Humidity	5% to 90% noncondensing
Storage Humidity	5% to 95% noncondensing
Maximum Operating Altitude	3,000 m (9,842 ft)
Maximum Nonoperating Altitude	4,000 m (13,100 ft)

Certifications

Table 19 lists the product certificates.

Table 19. Product Certifications

Additional Certificates	CISPR Class A (Comité International Spécial des Perturbations Radioélectriques) Compliant with European and China RoHS standards
Australia/New Zealand	RCM (Regulatory Compliance Mark)
Common Criteria	NIAP (National Information Assurance Partnership)
European Economic Area (EEA)	CE (Conformité Européenne) WEEE (Waste Electrical and Electronic Equipment) RoHS (EU 1025/863) (Restriction of Hazardous Substances)
European Standards (EN)	EMC (Immunity): EN 55024, EN 55035 EN 55032 Class A, EN 61000-3-2, EN 61000-3-3 Electrical Safety: EN 62368-1 (UL/EN/IEC)
India	TEC (Telecommunications Engineering Center)
Japan	VCCI Class A (Voluntary Control Council for Interference)

Table 19. Product Certifications (Continued)

North America	FCC Class A UL62368-1 $_{C}UL_{US}$
United Kingdom	UKCA (UK Conformity Assessment)

RJ-45 Copper Port Pinouts

Figure 69 illustrates the pin layout of the RJ-45 copper ports.

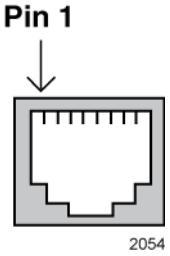


Figure 69. Pin Layout for the RJ-45 Copper Ports (Front View)

Table 20 lists the pin signals for the copper LAN and WAN ports.

Table 20. Pin Signals for Copper LAN and WAN Ports

Pin	10M/100M MDI	10M/100M MDI-X	1G/2.5G/5G/10G[1]
1	TX+	RX+	Bi-directional pair A+
2	TX-	RX-	Bi-directional pair A-
3	RX+	TX+	Bi-directional pair B+
4	Not used	Not used	Bi-directional pair C+
5	Not used	Not used	Bi-directional pair C-
6	RX-	TX-	Bi-directional pair B-
7	Not used	Not used	Bi-directional pair D+
8	Not used	Not used	Bi-directional pair D-

1. Ports 3 and 4 and the WAN port on the ARX200S-GTX Router only.

RJ-45 Style Serial Console Port Pinouts

Table 21 lists the pin signals of the RJ-45 style serial Console port.

Table 21. RJ-45 Style Serial Console Port Pin Signals

Pin	Signal
1	Unused
2	Unused
3	Transmit Data
4	Signal Ground
5	Signal Ground
6	Receive Data
7	Unused
8	Unused

Console Management Cable with DB-9 Female and RJ-45 Connectors

Figure 70 and Table 22 show the pin-outs for DB-9 female and RJ-45 connectors for a management cable for RS-232 serial management sessions on the Console port on the router.

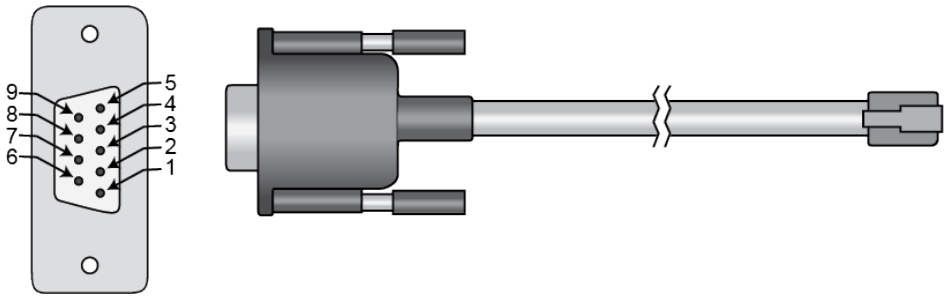


Figure 70. Console Port Management Cable with DB-9 Female and RJ-45 Connectors

Table 22. Pin-outs of Console Port Management Cable with DB-9 Female and RJ-45 Connectors

DB-9 Female Connector Pins	RJ-45 Connector Pins
1	4
2	3
3	6
4	7
5	5
6	2
7	8
8	1
9	NC