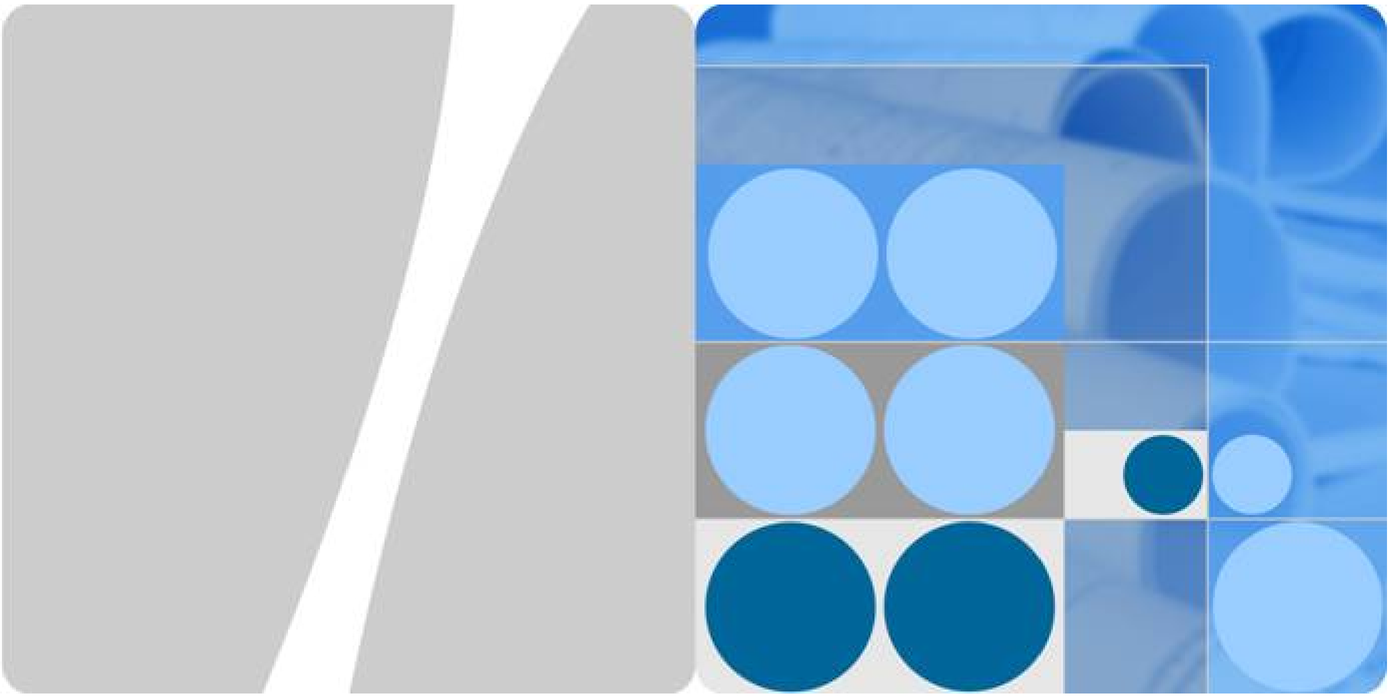


Huawei AR1200-S Series Enterprise Routers

V200R001C01

Product Description

Issue	01
Date	2011-08-15

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Intended Audience

This document describes the positioning, characteristics, networking and application, functions and features, device structure, maintenance and management, system parameters, and component selection guide for the AR.

This document helps you understand the characteristics and features of the AR.

This document is intended for:

- Network planning engineers
- Hardware installation engineers
- Commissioning engineer
- Data configuration engineers
- On-site maintenance engineers
- Network monitoring engineers
- System maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ DANGER	Alerts you to a high risk hazard that could, if not avoided, result in serious injury or death.
⚠ WARNING	Alerts you to a medium or low risk hazard that could, if not avoided, result in moderate or minor injury.
⚠ CAUTION	Alerts you to a potentially hazardous situation that could, if not avoided, result in equipment damage, data loss, performance deterioration, or unanticipated results.
TIP	Provides a tip that may help you solve a problem or save time.

Symbol	Description
📖 NOTE	Provides additional information to emphasize or supplement important points in the main text.

Change History

Updates between document issues are cumulative. Therefore, the latest document issue contains all the updates made in previous issues.

Changes in Issue 01 (2011-08-15)

This issue is the first official release.

Contents

1 Product Position and Characteristics

About This Chapter

1.1 Product Positioning

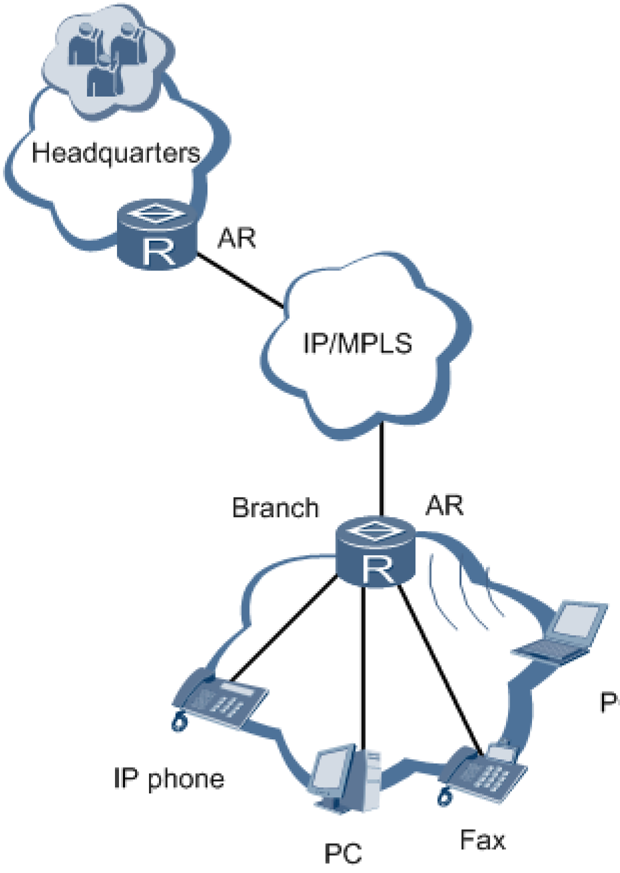
CAUTION

Huawei AR 1200-S series routers are class A products. Customers should take preventative measures as the operating devices may cause radio interference.

Huawei AR 1200-S series routers (ARs) include AR1220-S and AR1220W-S. They are the next-generation routing and gateway devices, which provide the routing, switching, wireless, voice, and security functions.

As shown in **Figure 1-1**, the ARs are located between an enterprise network and a public network, functioning as the only ingress and egress for data transmitted between the two networks. The deployment of various network services over the ARs reduces operation & maintenance (O&M) costs as well as those associated with establishing an enterprise network.

Figure 1-1 ARs on the network



1.2 Product Characteristics

The ARs use leading hardware platforms and software architectures. The ARs provide integrated network solutions to enterprise customers with minimum investment costs; therefore, they can meet the many facets of future business expansion and IT industry developments.

1.2.1 Carrier-Class Reliability

- The AR boards are hot swappable and guarantee carrier-class reliability.
- The ARs are designed to provide quality service and comply with telecommunication standards.
- The ARs protect networks against attacks.
- The ARs support in-service patching so that the system software can be upgraded during system operation.

1.2.2 Service Integration Capability

The AR series routers integrate various services of routers, switches, and wireless devices, including voice, firewall, and VPN.

1.2.3 Hardware Extensibility

The ARs provide the highest port density in industry and flexible service interface card (SIC) slots, allowing enterprise customers to connect to a LAN, WAN, or wireless network. The ARs provide the most economical enterprise network solutions.

The ARs support flexible slot combination methods. For example, 2 SIC slots are combined into a wide SIC (WSIC) slot.

The extensible hardware design allows customers to choose SICs flexibly and to expand network capacity economically.

1.2.4 Remote Maintenance Capability

In addition to one-stop deployment, plug and play capability, and remote commissioning functions, the ARs manage the customer premises equipment (CPE) remotely. The remote maintenance function improves efficiency and greatly reduces maintenance costs.

1.2.5 Surge Protection

The ARs use the Huawei patented surge protection technique. This technique shields the devices against lightning in terrible weather and greatly increases device security.

2 Network Applications

About This Chapter

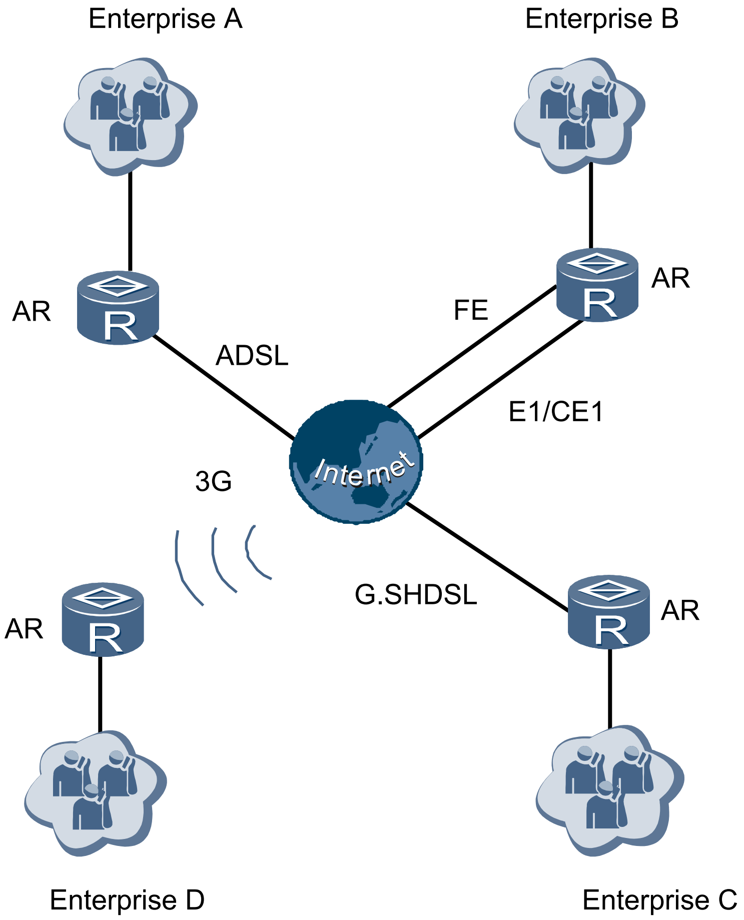
2.1 Network Access

Depending on the network environment provided by carriers, users can access the network by using CE1/CT1, E1/T1-F, 3G, FE/GE, ADSL, G.SHDSL, Integrated Services Digital Network (ISDN), AS or SA. The ARs provide dual-uplink to ensure service reliability. The ARs provide the following services for access users:

- Provides the security, routing, switching, VPN, and wireless services to ensure secure, fast, and reliable data packet forwarding.
- Provides various value-added services, including DHCP, network address translation (NAT), domain name system (DNS), and accounting services.
- Provides security control mechanisms, including controlling access to internal networks and user rights, to ensure the access security on the enterprise intranet and isolate the departments of an enterprise.
- Provides the attack defense function to protect user traffic against attacks from the external and internal networks.
- Guarantees user-specific QoS and service-specific QoS and flexibly allocates bandwidth for services as needed.

As shown in **Figure 2-1**, enterprise A accesses the Internet using ADSL; enterprise B accesses the Internet using FE and CE1 dual-uplink; enterprise C accesses the Internet using G.SHDSL; enterprise D accesses the Internet using 3G.

Figure 2-1 Network access



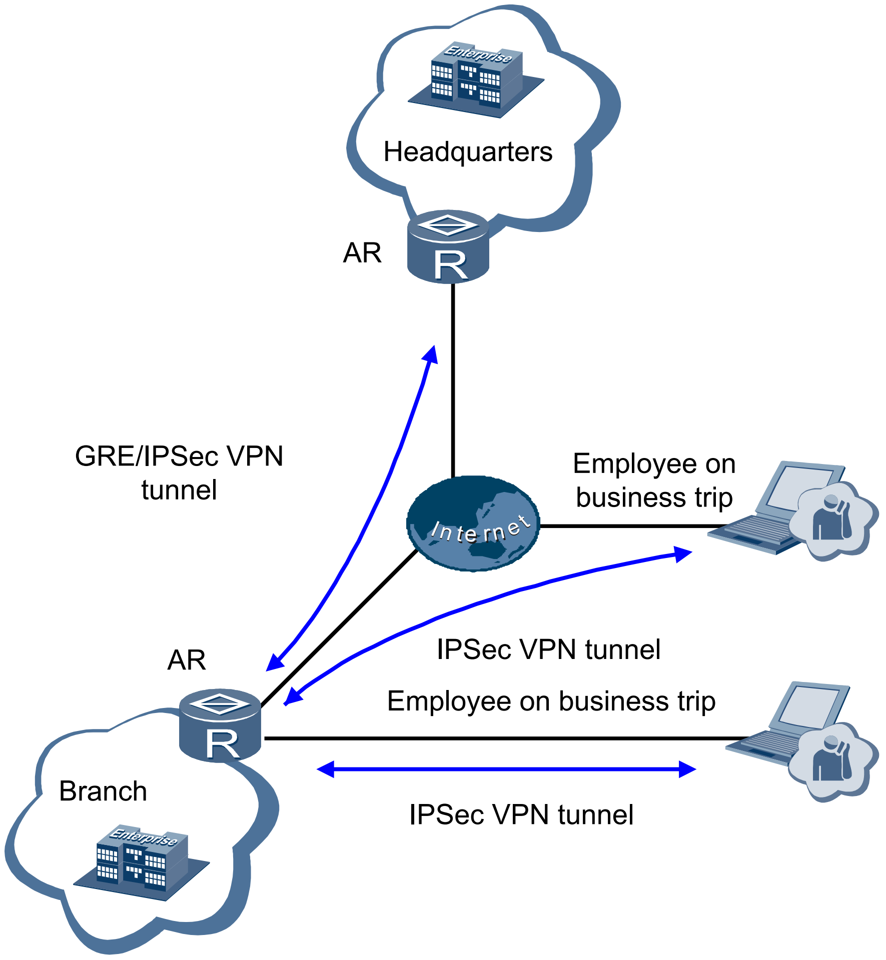
2.2 VPN Access

The headquarters and branches use the ARs establish a VPN and connect to the Internet. The enterprise establishes a VPN and uses GRE, or IPSec VPN to ensure data security. The employees on a business trip use IPSec VPN tunnels to communicate with the headquarters.

As shown in **Figure 2-2**, the headquarters is connected to the Internet by using the AR2200&3200, and provides services for all employees. The LAN of the branch connects to the Internet by using the AR1200-S, so the employees in the branch can access the headquarters network.

The headquarters and branch use GRE VPN, or IPSec VPN tunnels to establish an intranet. The employees on a business trip set up IPSec VPN tunnels, and access the intranet after passing authentication.

Figure 2-2 VPN access



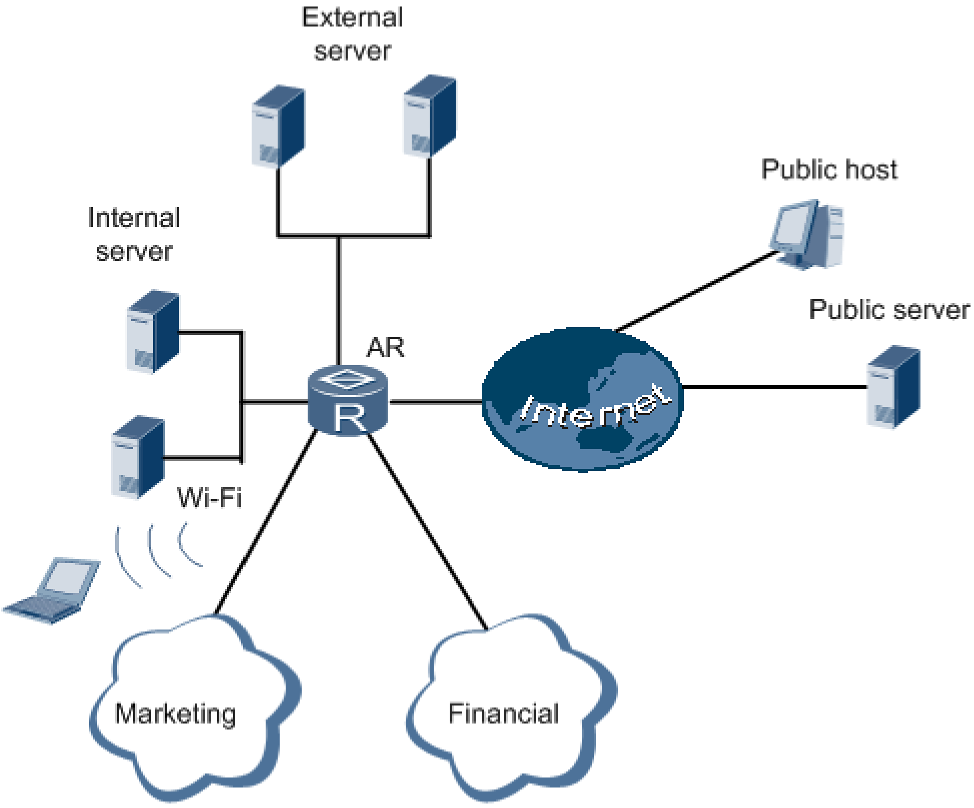
2.3 Enterprise Intranet Security

The ARs, located between the enterprise intranet and the Internet, ensure information security on the entire intranet and intranet LANs.

As shown in **Figure 2-3**, an intranet and the Internet are connected by the ARs. The users on the Internet cannot access the intranet. To allow the users on the intranet to access the Internet, configure network address translation (NAT) on the intranet. The financial department and marketing department have individual LANs on the intranet. The ARs utilize a demilitarized zone (DMZ) to protect the server on the external network. In addition, the application specific packet filter (ASPF) firewall can be deployed to protect the intranet.

The ARs provide network access control (NAC) to restrict the access permissions of internal users. This ensures that only authorized users can access the intranet.

Figure 2-3 Enterprise intranet security



3 Product Characteristics

About This Chapter

3.1 Feature List

Table 3-1 Features supported by AR

Feature	Sub-feature	Description
LAN	VLAN	VLAN services including basic VLAN, super VLAN, voice VLAN, and guest VLAN; dynamic VLAN learning using Generic Attribute Registration Protocol (GVRP)
	MAC	Dynamic and static MAC address learning; MAC address learning limit, blackhole MAC entries, sticky MAC entries, and anti-MAC flapping
	STP	Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP); STP security
	Link aggregation	Static link aggregation and Link Aggregation Control Protocol (LACP)-based aggregation
	LLDP	Neighboring device discovery
	WLAN	Wireless access to LANs
WAN	Interface backup	Various WAN interface backup mechanisms
	Link layer protocol	Link layer protocols such as Point-to-Point Protocol/Multilink Protocol (PPP/MP), Frame Relay/Multilink Frame Relay (FR/MFR), High-Level Data Link Control (HDLC), and ATM, and Operation, Administration, and Maintenance (OAM) mechanisms complying with link layer protocols Access of PPPoE host and PPPoE dial-up
	Dialing	Dial control center (DCC) function and logical interfaces that transmit the dialing service
	Network bridge	Bridge between Ethernet interfaces and WAN interfaces
	3G	3G uplink, allowing access to 3G networks using the DCC function
IP application	ARP	Address resolution for Ethernet
	IPv4 host	IPv4 address management, TCP/UDP socket, ICMP, ping and tracert, and UDP helper
	DNS	DNS client, DNS proxy, and dynamic DNS (DDNS) client

Feature	Sub-feature	Description
	DHCP	DHCP client, DHCP relay, and DHCP server, and DHCP security
	NetStream	Fixed packet sampling and packet statistics collection, with flow output in V5, V8 or V9 format
	NAT	NAT, port address translation (PAT), port application mapping (PAM), EASY NAT, and NAT server, providing application layer gateways (ALG) for each application
	VRRP	Redundancy backup mechanism for IP services
	BFD	Single-hop BFD, multi-hop BFD, BFD for VRRP, BFD for routing protocols, BFD for interface backup, and BFD for VRF
	Network Quality Analysis (NQA)	Detecting the performance of protocols running on the network
IP routing	Static route	Basic routing functions
	RIP	Routing protocol
	OSPFv2	Routing protocol
	IS-IS	Routing protocol
	Routing policy	Basic routing functions
Multicast	IGMP	Basic IGMP functions
	Multicast routing	Multicast route management, multicast route load balancing, and source-specific multicast (SSM) mapping
	PIM(IPv4)	PIM-DM and PIM-SM
	MSDP	Inter-domain (PIM-SM domain) multicast routing
QoS	MQC	Modular traffic classification
	Traffic policing	Single-rate-two-bucket and two-rate-two bucket policy based on traffic classifiers, permanent virtual circuits (PVCs)/VLANs/data link connection identifiers (DLCIs), and interfaces
	Traffic shaping	Traffic shaping based on traffic classifiers, PVCs/ VLANs/DLCIs, or ports, and Level-3 HQoS
	Congestion management	Congestion management based on traffic classifiers, PVCs/VLANs/DLCIs, and ports; queue mechanisms including PQ, WRR, DRR, WFQ, PQ+WRR/PQ+DRR/PQ+WFQ, CBQ

Feature	Sub-feature	Description
	Congestion avoidance	Priority-based weighted random early detection (WRED) and tail drop
Security	AAA	AAA for administrators and access users, including local, RADIUS, and TACACS AAA
	Firewall	DMZ firewall, packet filtering firewall, and stateful firewall; blacklist and whitelist, and attack detection
	Traffic suppression	Traffic suppression based on ports
	Access security	802.1x authentication, MAC authentication, MAC bypass authentication, and direct MAC authentication based on users and ports; web authentication and guest VLAN for access users
	Local attack defense	Device protection measures, including CPU attack defense and attack source tracing.
	ARP security	Suppression of ARP packets from the user side and network side, ARP anti-spoofing, ARP-STP association, and ARP gateway attack inspection
	IP security	ICMP anti-attack, URPF
	ACL	Traffic classification based on physical ports, Layer 2 information, IP protocols, and TCP/UDP ports.
VPN	IPSec VPN	Interconnecting headquarters and branches using IKE V1/V2 IPSec tunnels; hardware-based MD5 and SHA algorithms; AES, DES, and 3DES algorithms
	GRE VPN	GRE tunnel for interconnecting the headquarters and branches Used together with IPSec. IPSec cannot protect multicast data, but GRE VPN can protect multicast data
Device management	Information center monitoring	Managing boards, power supply units, fans, and e-labels
	Version management	In-service upgrade, rollback, and patch installation
	Mirroring	Port- and flow-based mirroring
	Remote PoE power supply	LAN-side remote power supply **NOTE** Only the AR1220W-S supports the PoE features.

Feature	Sub-feature	Description
	Deployment	Automatic deployment using a universal serial bus (USB) flash drive; auto-config function for the entire network
Network management	SNMP	SNMP agent, fault management (FM), and trap switch control (TSC)
	Web	Internal web management system, providing GUI to manage and maintain devices
	Ping and Tracert	Network connectivity detection
	NTP	Time synchronization for traditional IP networks
	CWMP	CWMP (TR-069) for remotely managing AR devices

3.2 Key Features

3.2.1 WAN

WAN uses the interfaces such as Ethernet, E1, T1, ADSL, G.SHDSL, 3G, and synchronous/ asynchronous serial interfaces. The physical links on these interfaces can run the FR, PPP, HDLC, and ATM protocols.

Frame Relay

Working at the data link layer of the Open System Interconnection (OSI) model, Frame Relay (FR) uses simple methods to transmit and exchange data. On a frame relay (FR) network, virtual circuits connect two FR devices. A physical line on the FR network provides multiple VCs. A VC defines an FR channel by using the data link connection identifier (DLCI), and detects and maintains the VC status by using the local management interface (LMI).

Multilink frame relay (MFR) is a cost-effective solution provided for FR users. MFR (FRF.16) implements the multilink frame relay function on the user-to-network interfaces (UNIs).

PPP

The point-to-point protocol (PPP) is used at the data link layer of the OSI model as well as at the link layer of TCP/IP. PPP transmits data from one point to another through synchronous links and asynchronous links that support full duplex.

PPP provides a complete authentication mechanism. To set up a PPP connection, users must pass authentication, ensuring a secured connection.

PPPoE

A Point-to-Point Protocol over Ethernet (PPPoE) network consists of an Ethernet containing many hosts. It accesses the Internet through a remote access device.

An AR can create a PPP session with the remote end by using PPPoE, and implement access control and accounting.

An AR can function as the PPPoE server to connect to different types of PPPoE clients on the Ethernet or function as a dial-up PPPoE client.

ADSL

An Asymmetric Digital Subscriber Line (ADSL) implements high-speed data transmission over twisted-pair copper wire by using idle high frequency ranges through a regular telephone line, but with a different modulation method. With an uplink band from 26 kHz to 138 kHz, ADSL can provide transmission rates up to 640 kbit/s; with a downlink band from 138 kHz to 1.104 MHz, ADSL can provide up to an 8 Mbit/s transmission rate.

The current ADSL technology can provide faster transmission rates by improving the modulation rate, coding gain, the initialization state machine, by reducing the frame head overhead, and by using enhanced signal processing methods. ADSL2 can provide up to a 1024 kbit/s uplink transmission rate and a 12 Mbit/s downlink transmission rate. By expanding the downlink band from 1.104 MHz to 2.208 MHz, the latest ADLS technology, ADSL2+, provides a 24 Mbit/s downlink rate.

The transmission distance and line quality affect the ADSL transmission rate. If the transmission distance is long and the line quality is poor, the transmission rate will be low; if the transmission distance is short and line quality is high, the transmission rate is high. When setting up a link, ADSL automatically adjusts transmission rates based on line conditions such as distance and noise.

The ARs transmit the LAN-side service to the wide area network by using ADSL lines.

G.SHDSL

G.Single-pair high-speed Digital Subscriber Line (G.SHDSL) implements high-speed data transmission over twisted-pair copper wire by using idle high frequency ranges on regular telephone line, but with different modulation methods. G.SHDSL provides transmission rates up to 2.312 Mbit/s. The transmission distance and line quality affect the G.SHDSL transmission rate. If the transmission distance is long and the line quality is poor, the transmission rate will be low; if the transmission distance is short and the line quality is high, the transmission rate is high. When setting up a link, G.SHDSL automatically adjusts transmission rates based on line conditions such as distance and noise. G.SHDSL is a rate/distance-adaptive DSL technology. Different from ADSL, G.SHDSL does not require a splitter.

The ARs transmit the LAN-side service to the wide area network by using SHDSL lines.

3G

The first generation (1G) uses an analog system and the second generation (2G), such as GSM and TDMA, uses digital systems. The Third Generation (3G) integrates wireless communication and the Internet. The 3G technology can process pictures, music, video, and provide various information services such as web page browsing, call conferences, and E-commerce.

The ARs support WCDMA wireless interface standards. Users on a LAN can access the WAN using 3G cards.

3.2.2 VPN

The ARs provide an IP security (IPSec) mechanism to ensure high quality, interoperable, and cryptology-based security for communication processes. The two parties in communication can encrypt data and authenticate the data source at the IP layer to ensure the confidentiality and integrity of the data and prevent replay on the network.

IPSec implements these functions by using two security protocols: Authentication Header (AH) protocol and Encapsulating Security Payload (ESP). Internet Key Exchange (IKE) provides the automatic key negotiation, SA establishment, and SA maintenance functions to simplify IPSec use and management.

The ARs support IPSec VPN and provide high reliability transmission tunnels for users. In addition, the ARs use Generic Routing Encapsulation (GRE) to support the following VPN services:

- GRE VPN
- IPSec VPN
- GRE over IPSec VPN

3.2.3 Security

ACL

An access control list (ACL) defines a series of filtering rules based on certain policy, the ACL permits or forbids the passage of data packets.

The ARs can use ACL rules to filter packets.

Firewall

- ACL-based packet filtering

  ACL-based packet filtering is used to analyze the information of the packets to be forwarded, including source/destination IP addresses, source/destination port numbers, and IP protocol numbers. The ARs compare the packet information with the ACL rules and determine whether to forward or discard the packets.

  In addition, the ARs can filter the fragmented IP packets to prevent the non-initial fragment attack.

- ASPF

  Application Specific Packet Filter (ASPF) filters packets of the application layer based on packet status. ASPF, used for security policies, detects the session information of the application layer protocol packets, which attempt to pass the AR and prevent the unsatisfied packets.

- Attack defense

  With the attack defense feature, the ARs can detect various network attacks and protect the internal network against attacks.

  Network attacks are classified into three types: DoS attacks, scanning and snooping attacks, and malformed packet attacks.

  - DoS attack

    The DoS attack is an attack to a system by using a large number of data packets. This prevents the system from receiving requests from authorized users or suspends the host. DoS attacks include SYN Flood attacks and Fraggle attacks. DoS attacks are different from other attacks because DoS attackers do not search for the ingress of a network, but prevent authorized users from accessing resources or routers.

  - Scanning and snooping attack

The scanning and snooping attack is to identify the existing systems on a network by using ping scanning (including ICMP and TCP scanning), and then find out potential targets. By using TCP scanning, attackers can identify the operating system and the monitored services. By scanning and snooping, an attacker can know the service type and security vulnerability of the system and prepare for further intrusion to the system.

- Malformed packet attack

  The malformed packet attack is to send malformed packets to the system. If such an attack occurs, the system breaks down when processing the malformed IP packets. Malformed packet attacks include Ping of Death and Teardrop.

ARP Security

There are various ARP attacks on networks, including attacks targeting hosts and gateways, address spoofing attacks and violent attacks, virus attacks, and malicious software attacks.

The ARs ensure ARP security by discarding untrusted ARP packets, suppressing ARP packets by using timestamps, discarding invalid ARP packets, and performing dynamic CAR on the packets sent to the CPU. In addition to preventing ARP protocol attacks, the ARs also prevent ARP-based network scanning attacks.

Local Attack Defense

The Internet technology and size develop quickly and various network applications emerge. Many enterprises try to boost their own development by using their networks. They are concerned about how to protect confidential data and resources in an open network environment. Some unconscious operations may attack network devices and degrade device performance or even cause device failure.

A large number of packets including valid packets and malicious attack packets on a network must be processed by devices' CPUs. The malicious attack packets affect services and may even cause a system breakdown. In addition, excessive normal packets can also lead to high CPU usage, which degrades the CPUs' performance and interrupts services. Therefore, protecting the CPU is a necessary and important factor for processing services and system response.

The local attack defense and source tracing functions protect the ARs against attacks. When an attack occurs, these functions ensure non-stop service transmission and minimize the impact of the attack on network services.

AAA

The ARs support Authentication, Authorization, and Accounting (AAA).

- Authentication

  Verifies users' identities.

- Authorization

  Grants different rights for different users to restrict the services that can be used by users.

- Accounting

  Records information about network service usage of users, including service type, start time, and traffic volume.

3.2.4 QoS

Traffic Policing

Traffic policing discards excess traffic in order to limit the traffic within a specified range and to protect network resources as well as the carriers' interests.

The ARs use committed access rate (CAR) to perform traffic policing. They support dual-rate-three-color markers and precise bandwidth management.

Traffic Shaping

When the rate of an interface on a downstream device is slower than the that of an interface on an upstream device or burst traffic occurs, traffic congestion may occur on the downstream device interface. Traffic shaping can be configured on the interface of an upstream device so that outgoing traffic is sent at even rates and congestion is avoided.

The ARs support traffic shaping based on queues, sub-interfaces, and main interfaces.

Congestion Management

If a network transmitting both delay-sensitive and delay-insensitive services is congested intermittently, congestion management is required. However, if a network is always congested, bandwidth needs to be increased. Congestion management sends packet flows by using queuing and scheduling.

An interface on AR has four or eight default queues for outgoing packets. a fixed FE interface on AR1220-S has four default queues and each of other interfaces has eight. LAN-side interfaces support the scheduling modes of priority queuing (PQ), weighted round robin (WRR), and PQ +WRR. WAN-side interfaces support the scheduling modes of PQ, WFQ, PQ+WFQ, and class-based WFQ (CBQ). Each scheduling algorithm schedules specific types of traffic, and affect bandwidth allocation, delay, and jitter.

Congestion Avoidance

Congestion avoidance is a flow control mechanism. A system configured with congestion avoidance monitors network resource usage such as queues and memory buffers. When congestion occurs or aggravates, the system discards packets.

The ARs support tail drop and WRED.

- Tail drop

  When the queue length reaches the upper limit, the excess packets (buffered at the queue tail) are discarded.

- WRED

  WRED sets the upper and lower drop thresholds and the maximum drop probability for each queue. When the queue length is smaller than the lower threshold, no packets are discarded. When the length of the queue exceeds the upper threshold, all packets are discarded. When the queue length is between the lower threshold and the upper threshold, incoming packets are discarded randomly. The drop probability cannot be greater than the maximum drop probability.

  The ARs use the WRED based on queue profiles or traffic policies.

3.2.5 WLAN

NOTE

Only AR1220W-S supports.

A wireless local area network (WLAN) connects two or more computers or devices and enables the devices to communicate by using the wireless telecommunication technology. WLAN uses the wireless technology to implement fast Ethernet access. The primary advantage of WLAN is that terminals, such as computers, can access a network through a wireless medium rather than a physical cable. This facilitates network construction and allows users to move around without interrupting communication. WLAN is more flexible than traditional wired access.

WLAN is widely used in public areas such as on campuses, business centers, and airports. The WLAN uses cables at the backbone layer, and users access the WLAN through one or more wireless access points (WAPs) using radio waves. The transmission distance of a WAP is tens of meters.

IEEE 802.11 is widely used by WLANs. The AR function as fat APs to provide the following WLAN functions:

- WLAN user management
  - Dot1X access authentication
  - MAC address authentication
  - Pre-share-key (PSK) authentication
  - EAPOL-Key negotiation
  - User access control
  - AAA for WLAN users
- Radio frequency (RF) management
  - Country code
  - RF type
  - Setting radio transmission rate
  - Setting radio transmission power
  - Setting radio working channels
  - Monitoring and eliminating radio interference
  - Configurable wireless MAC layer parameters
  - Configuring and querying radio attributes
  - Collecting and querying performance statistics of radio frequency interfaces
- WLAN security
  - WEP Open-System link authentication and encryption
  - WEP Share-Key link authentication and encryption
  - WPA PSK authentication and encryption
  - WPA Dot1X authentication and encryption
  - WPA2 PSK authentication and encryption
  - WPA2 Dot1X authentication and encryption
  - WAPI authentication and encryption

  - TKIP/CCMP encryption
  - HMAC-MD5 algorithm
  - User blacklist and whitelist
- WLAN QoS
  - WMM (802.11e)
  - Mapping wireless-side priority to the wired-side priority
  - Bandwidth limit based on users
  - Bandwidth limit based on SSIDs

4 Device Structure

Appearance

Figure 4-1 and Figure 4-2 show the front view of AR1200-S series.

Figure 4-1 AR1220-S front view

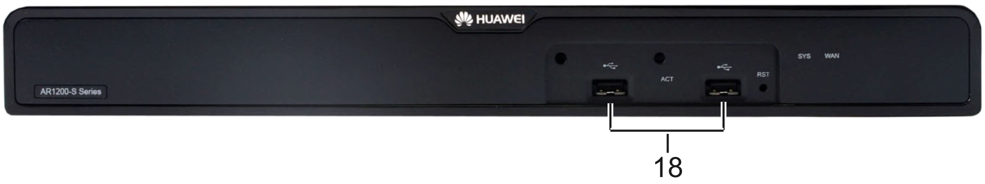


Figure 4-2 AR1220W-S front view

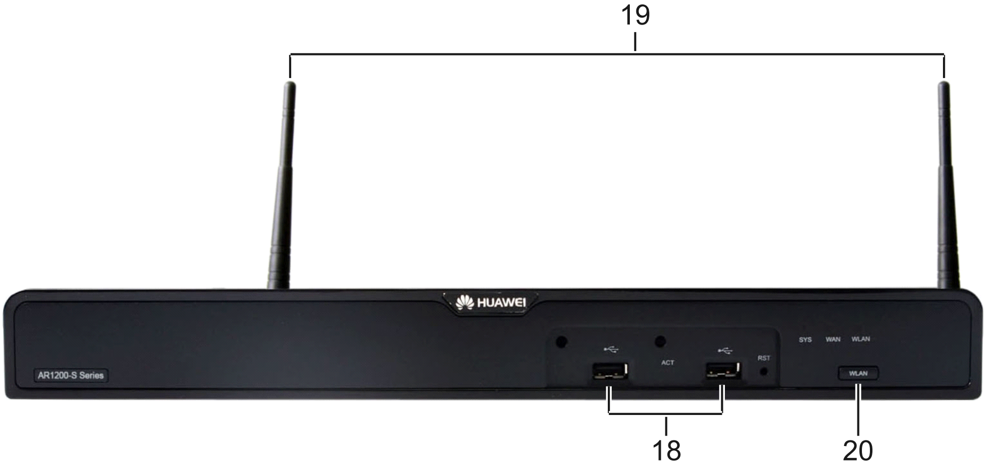


Figure 4-3 and Figure 4-4 show rear views of AR1200-S series.

Figure 4-3 AR1220-S rear view

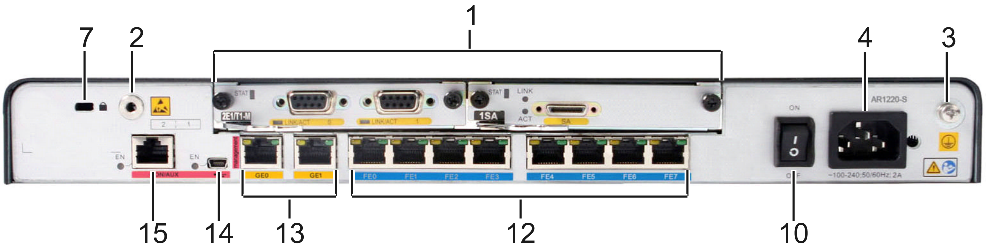
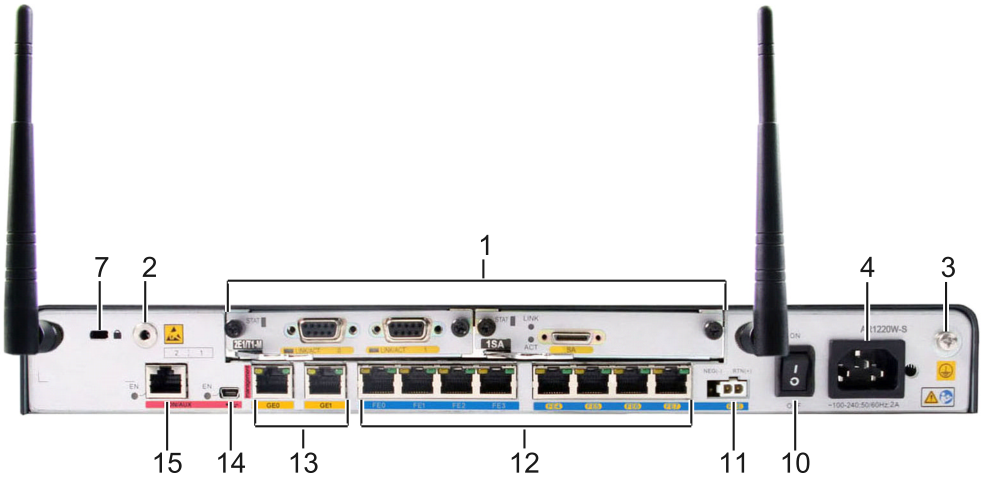


Figure 4-4 AR1220W-S rear view



1. Pluggable card	2. ESD jack	3. Ground screw	4. AC jack
7. Security lock	10. AC power switch	11. PoE port	12. Fixed 8FE interface on the panel
13. Two Fixed GE interfaces on the panel	14. Mini USB interface	15. CON/AUX interface	18. USB interface

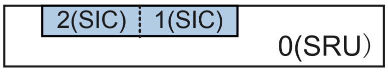
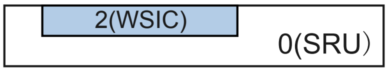
Slot distribution

Figure 4-5 shows slot distribution on AR1200-S series.

NOTE

After two slots are combined into one, the slot ID is the larger one between the original two slots.

Figure 4-5 Slot distribution on AR1200-S series

Device Model		Slot Distribution	Slot Combination
AR1200-S	Front view	NA	NA
	Rear view		Two SIC slots are combined into one WSIC slot

As shown in **Figure 4-5**, slot 1 and slot 2 are combined into new slot 2.

5 Maintenance and Management

About This Chapter

5.1 Various Maintenance Methods

The ARs support various local and remote maintenance methods:

- Local maintenance using the console interface
- Local or remote maintenance using Telnet
- Secure shell (SSH) maintenance: guarantees security and provides authentication for login users on an insecure network, and defends against various attacks, including IP address spoofing, plain text password interception, and denial of service (DoS).

5.1.1 CWMP

The CPE WAN Management Protocol (CWMP) is drafted by the Digital Subscriber's Line (DSL) forum. It is also called TR-069 standard. CWMP standardizes the communication between customer premises equipment (CPE) and auto-configuration server (ACS).

There are a lot of user devices separated on the access network. They are difficult to manage and maintain. The ARs are the CPE deployed at the user network side. The ACS uses CWMP to remotely manage the CPE. This reduces maintenance cost and improves troubleshooting efficiency.

5.1.2 Remote Deployment and Maintenance Using USB

The software engineers do not need to commission devices onsite during deployment. After installing the device, hardware engineers will insert the USB disk into the USB interface on the device and power on the device. After being started, the device automatically connects to the network and upgrades software.

The deployment process is simplified and deployment costs are reduced by using the USB disk on the AR.

5.1.3 SNMP-based Maintenance

The ARs support the Simple Network Management Protocol (SNMP) v1/v2c/v3 and the Client/Server model. The ARs can be managed by the network management system (NMS), such as iManager U2000.

5.2 Fault Location

5.2.1 Device Fault Location

The ARs support the following functions to locate device faults:

- Black box

  If an AR restarts or stops working because of an error, it records the error information to locate the fault.
- Log

  After detecting a service error or recovery event, the AR logs the event and sends the information to the background server.

- Fast information collection

  A system administrator can use only one command to collect device fault information.

- Device monitoring

  The AR can monitor all the key indexes and components such as voltage, temperature, fan, and power supply unit. In addition, the AR can send a trap if an error occurs.

5.2.2 Service Fault Location

The ARs support the following functions to locate service faults:

- Locating Ethernet interface faults

  The ARs support interface status display, line tests, and loopback tests on interfaces. The ARs test packet sending and receiving on interfaces and collect packet statistics, assisting administrators to locate network faults and Ethernet interface connection faults.

- Network-side interface faults

  The ARs support WAN interface tests, which collect traffic statistics and event statistics on WAN interfaces and perform tests such as ATM, OAM, and interface loopback.

- Port mirroring

  The ARs support packet mirroring on Ethernet interfaces, mirroring of packets from a network-side interface to a user-side Ethernet interface, and mirroring of protocol packets sent to the CPU.

- Connection fault

  The ARs test connections and display connection status on network-side interfaces, and collect connection statistics.

6 System Parameters

About This Chapter

6.1 System Configuration

Table 6-1 System configuration

Model	Processor	Memory	Flash Memory
AR1220-S	Dual-core, 500 MHz	512 MB	256 MB
AR1220W-S	Dual-core, 500 MHz	512 MB	256 MB

6.2 Physical Specifications

Table 6-2 Physical specifications

Item		Description
Dimensions (width x depth x height)		● Without rack-mounting ear AR1220-S, AR1220W-S: 390.0 mm x 220.0 mm x 44.5 mm ● With rack-mounting ear AR1220-S, AR1220W-S: 482.6 mm x 220.0 mm x 44.5 mm
Maximum power consumption (empty chassis)		AR1220-S, AR1220W-S: 33.3W
Weight	Full configuration	AR1220-S, AR1220W-S: 3.60 kg
	Empty chassis	AR1220-S, AR1220W-S: 2.90 kg
AC input voltage	Rated voltage	100 V AC to 240 V AC
	Voltage range	85 V AC to 264 V AC
Working temperature		0°C to 40°C
Relative humidity		5%RH to 90%RH
Altitude	Long-term altitude	Lower than 4000 m
	Storage altitude	Lower than 4000 m

7 Component Selection Guide

About This Chapter

7.1 Router Purchase List

Table 7-1 Purchase list of AR1220-S and AR1220W-S

Component	Typical Configuration	Remarks
AR1220-S	Basic configuration of AR1220-S, including assembly chassis, basic software package, and documentation package	Mandatory
AR1220W-S	Basic Configuration of AR1220W-S, including AR1220W-S Chassis,802.11b/g/n AP ETSI Complian,with Basic Software and Document	Mandatory
PoE power supply unit	100 W PoE power supply adapter module	Optional. Only the AR1220W-S supports PoE power supply.

7.2 Board Purchase List

Table 7-2 Board purchase list

Silkscreen	Board Name	Description
8FE1GE	WMF9TTA	9-port 8FE/1GE L2/L3 Ethernet interface card
1GEC	SEG1CA	1-port GE combo WAN interface card
2FE	SEF2TA	2-port FE WAN interface card
1E1/T1-M	SDME1A	1-port channelized E1/PRI/VE1; MFT: multiflex trunk
1E1/T1-F	SDE11A	1-port unchannelized E1/unstructure E1/ fractional E1, 120 ohm WAN interface card
2E1/T1-F	SDE12A	2-port unchannelized E1/unstructure E1/ fractional E1, 120 ohm WAN interface card
2E1/T1-M	SDME2A	2-port channelized E1/PRI/VE1; MFT: multiflex trunk
1SA	SDSA1A	1-port sync serial WAN interface card
2SA	SDSA2A	2-Port Sync/Async Serial WAN Interface Card
8AS	WDAS8A	8-Port Async Serial WAN Interface Card
1BST	SDS1XA	1-port ISDN S/T WAN interface card

Silkscreen	Board Name	Description
1ADSL-A/M	SLA1XA	1-port ADSL2+ annex A/M WAN interface card
1ADSL-B	SLB1XA	1-port ADSL2+ annex B WAN interface card
4G.SHDSL	SLS1XA	4-pair G.SHDSL WAN interface card