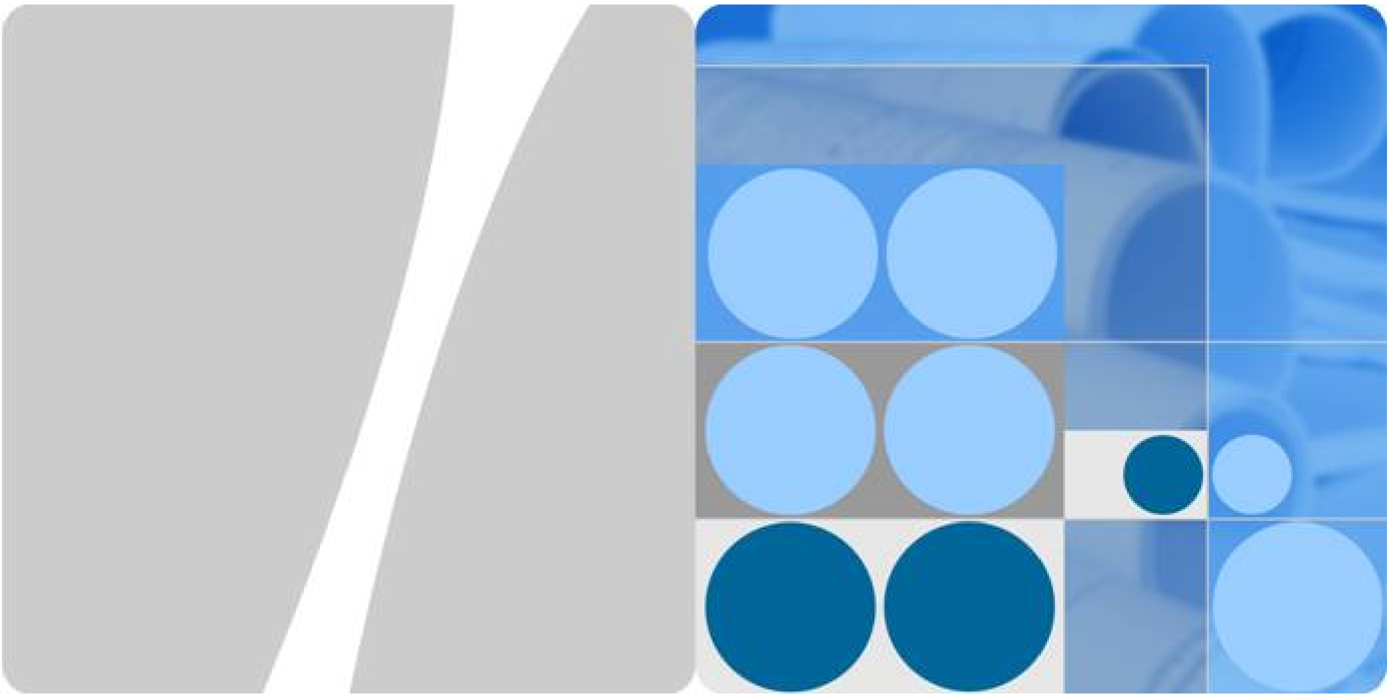


Huawei AR G3 Series Enterprise Routers

V200R002C01

Product Description

Issue 01

Date 2012-04-20

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 (2012-04-20)

This issue is the first official release.

Contents

1 Product Position and Characteristics

About This Chapter

1.1 Product Positioning

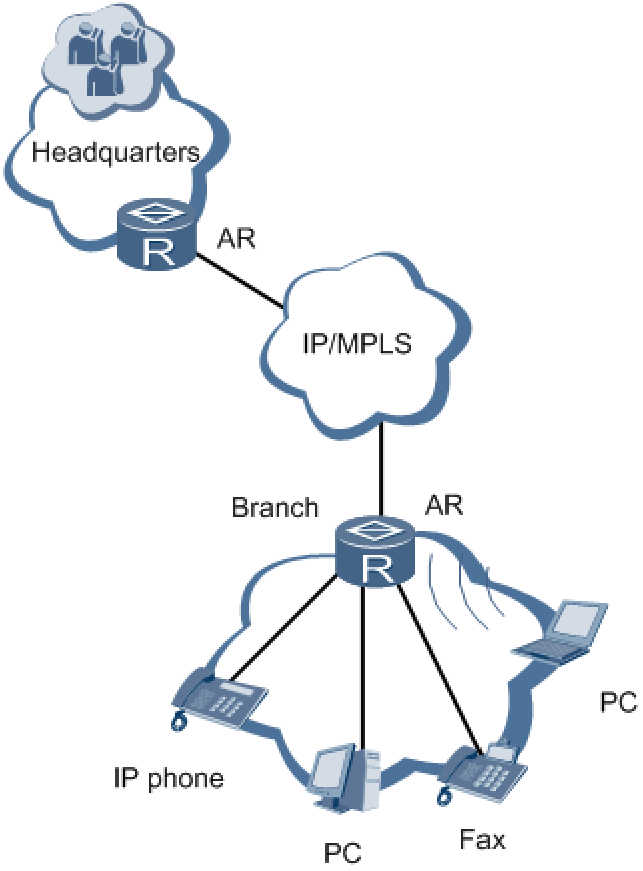
CAUTION

AR G3 Series Enterprise Routers are class A products. Customers should take preventative measures as the operating devices may cause radio interference.

AR series enterprise routers (ARs) include AR150, AR200, AR1200, AR2200, and AR3200. 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. You can select ARs of different specifications as egress gateways based on the user quantity of an enterprise.

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 AR1200&2200&3200 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.
- The AR2200&3200 support redundant power supply units and fans. If one power supply unit or fan is faulty, the AR2200&3200 will still be able to operate.

1.2.2 Service Integration Capability

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

1.2.3 Hardware Extensibility

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

The ARs support flexible slot combination. For example, two SIC slots can be combined into a wide SIC (WSIC) slot, two WSIC slots are combined into an extra SIC (XSIC) slot, and two XSIC slots can be combined into an extended extra SIC (EXSIC) slot. In addition, a SIC card can be installed into a WSIC slot.

NOTE

AR150&200 series do not support subcards.

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.

2 Network Applications

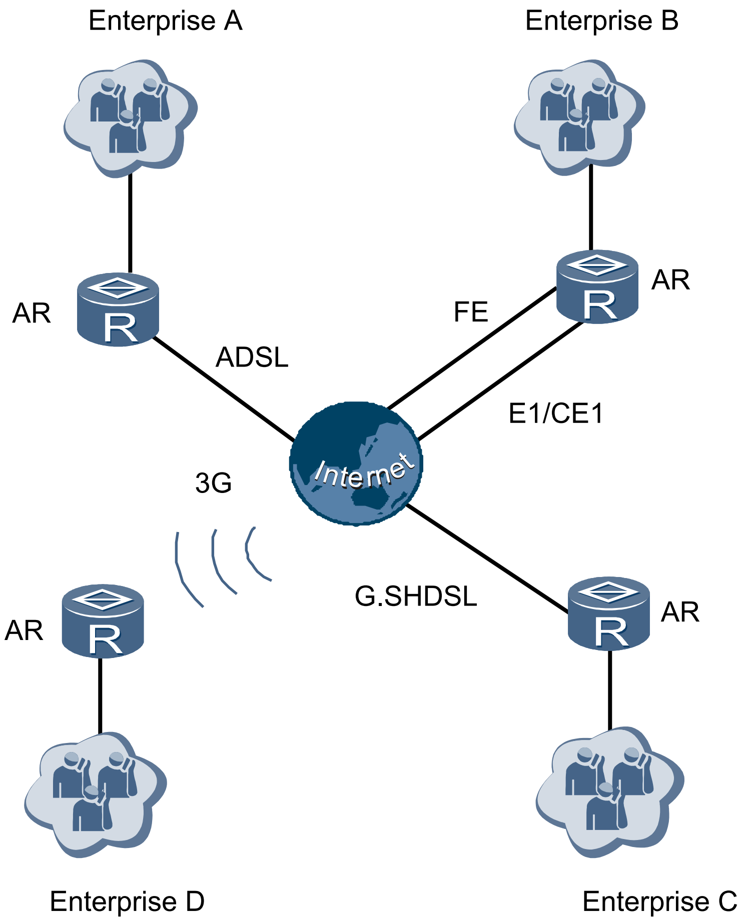
About This Chapter

2.1 WAN 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, VDSL, G.SHDSL, Integrated Services Digital Network (ISDN), CPOS, AS, xPON or SA. The ARs provide dual-uplink to ensure service reliability. The ARs provide the following services for access users:

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 WAN access



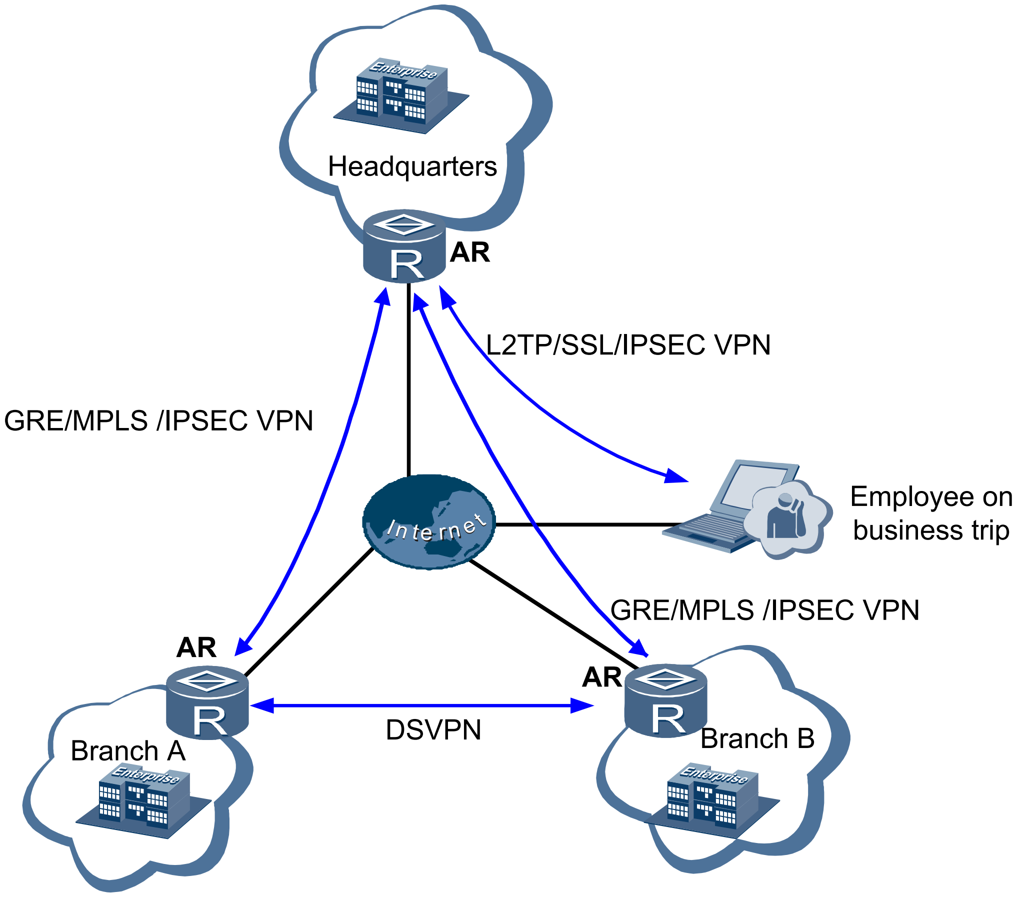
2.2 VPN Access

The headquarters and branches use the ARs establish a VPN and connect to the Internet. The enterprise establishes a VPN and uses GRE, MPLS, 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 AR150&200&1200&2200, so the employees in the branch can access the headquarters network.

The headquarters and branch use GRE VPN, MPLS/BGP IP VPNor IPSec VPN tunnels to establish an intranet. The employees on a business trip set up IPSec VPN , L2TP VPN or SSL VPN tunnels, and access the intranet after passing authentication.

Figure 2-2 VPN access



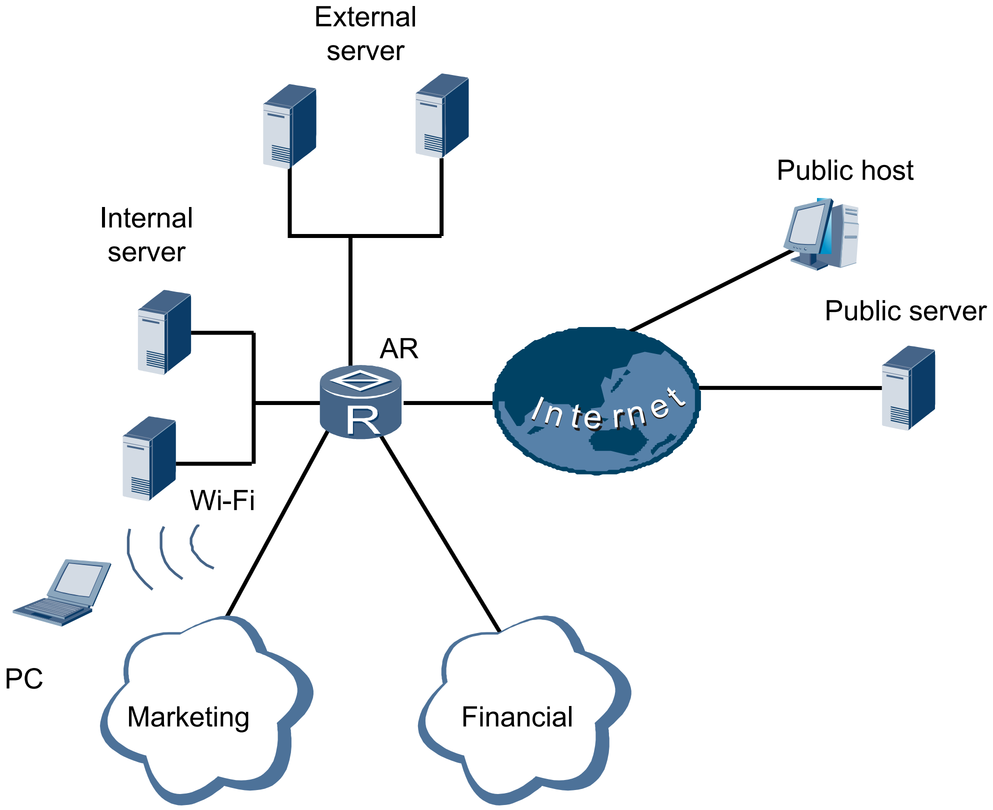
2.3 Enterprise Intranet Security

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 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



2.4 Voice Application

NOTE

- Among the AR200 series routers, only the AR207Vs and AR207V-Ps support the voice features. Among the AR1200 series routers, only the AR1220Vs and AR1220VWs support the voice features. The AR2200 and AR3200 series routers support the transfer of analog to digital signals, as well as digital to analog signals only after a DSP module is installed.
- To provide voice services for POTS users on AR1200, AR2200 ,and AR3200 series routers, 4FXS/1FXO board is required.
- To provide voice services for ISDN users on AR1200, AR2200 ,and AR3200 series routers, 2BST board is required.

An enterprise can build a voice communication system over the IP network, reducing operating expenses (OPEX).

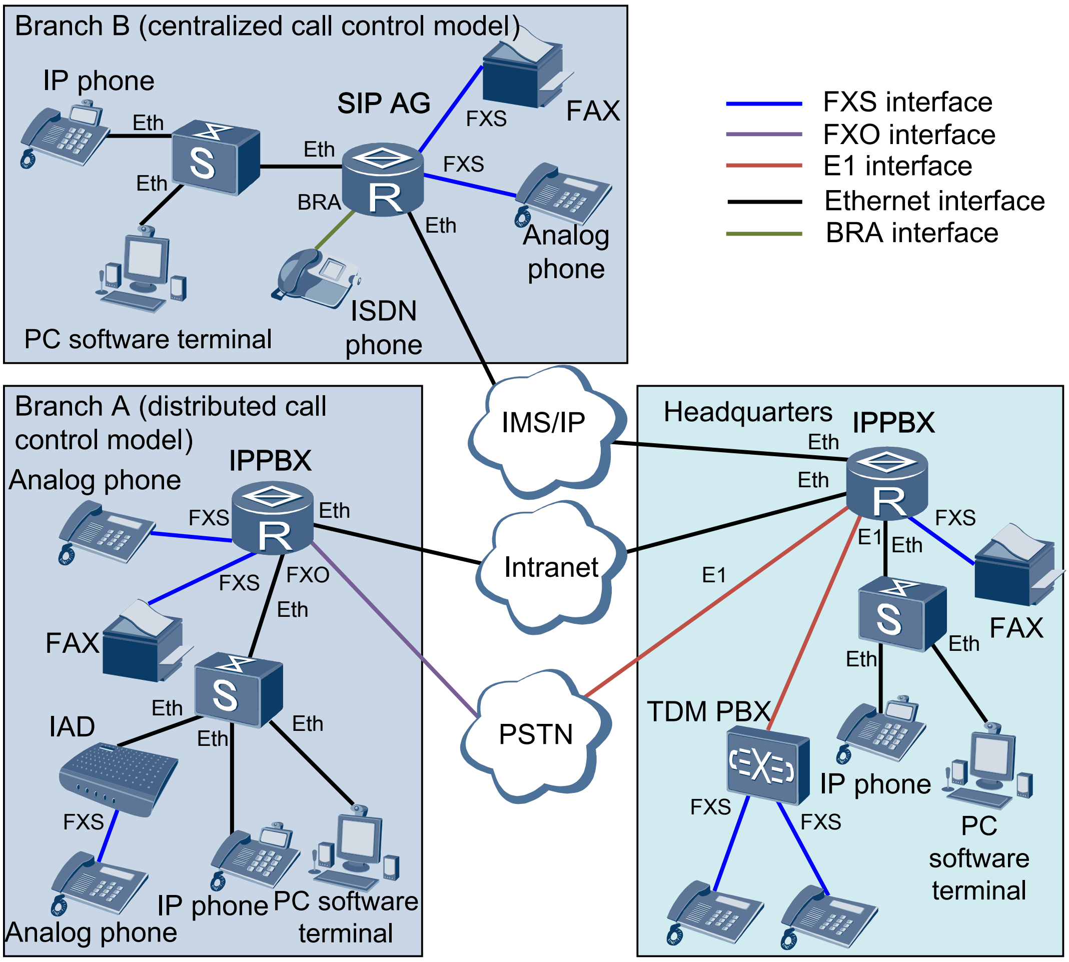
Within the voice communication system, an AR can function as an IP PBX or SIP access gateway (AG). The AR connects to POTS users (analog phones or fax machines) and SIP user equipment (UE) users (IP phones or PC software terminals) through FXS or Ethernet interfaces. The AR connects to the PSTN through FXO or E1interfaces or to the IP network through Ethernet interfaces.

Based on branch locations, the centralized or distributed call control model can be used. If all branches within an enterprise use the same number segment, the centralized call control model is recommended. If an enterprise has many branches that use different number segments, the distributed call control model is recommended.

As shown in **Figure 2-4**, the enterprise headquarters and branch A use different number segments. The ARs working in IP PBX mode are deployed at the enterprise headquarters and branch A as egress routers. Voice users in the enterprise headquarters are registered with the AR in the enterprise headquarters, and voice users in each branch are registered with the AR in the branch. Voice traffic is transmitted between the enterprise headquarters and branches over voice routes. The AR of the enterprise headquarters provides voice routes to branches so that users in different branches can call each other.

Branch B and the enterprise headquarters are connected through the MAN. An AR working in IP PBX mode is deployed at the enterprise headquarters and an AR working in SIP AG mode is deployed at branch B. All voice users at the enterprise headquarters and branches are registered with the AR at the enterprise headquarters. The AR in the enterprise headquarters provides call control services for all users in the enterprise.

Figure 2-4 Voice application

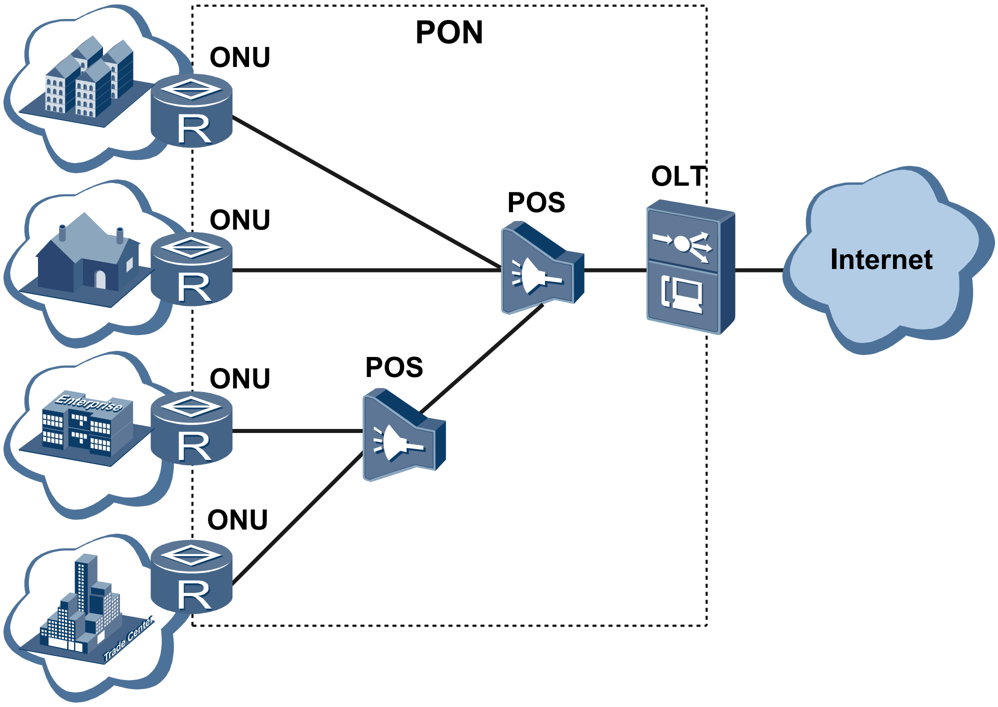


2.5 FTTx

By working with the optical line terminal (OLT), the ARs function as optical network unit (ONU) to provide fiber access to the enterprise. As shown in **Figure 2-5**, the ARs are connected to upstream devices through a passive optical network (PON), and provide fiber-to-the-home, fiber-to-the-building, and fiber-to-the-enterprise services.

The ARs provide the fiber-to-the-x (FTTx) service by connecting to upstream PON devices. This provides higher bandwidth than twisted-pair cable and guarantees the development of future high-speed services.

Figure 2-5 FTTx



3 Product Characteristics

About This Chapter

3.1 Feature List

Table 3-1 Features supported by the AR

Feature	Sub-feature	Description	Difference
LAN	VLAN	VLAN services including basic VLAN, super VLAN, MUX VLAN, voice VLAN, and guest VLAN; dynamic VLAN learning using Generic Attribute Registration Protocol (GVRP)	Only the AR2200 and AR3200 series support MUX VLAN.
	MAC	Dynamic and static MAC address learning; MAC address learning limit, blackhole MAC entries, sticky MAC entries, and anti-MAC flapping	None
	STP	Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP); STP security	None
	Link aggregation	Static link aggregation and Link Aggregation Control Protocol (LACP)-based aggregation	None
	LLDP	Neighboring device discovery	None
	WLAN	Wireless access to LANs	Only the AR1220W and AR1220VW support WLAN features.

Feature	Sub-feature	Description	Difference
WAN	WAN interface	WAN interfaces: CE1/CT1 PRI interfaces, E1/T1-F interfaces, 3G interfaces, CPOS interfaces, FE/GE interfaces, ADSL interfaces, VDSL interface, G.SHDSL interfaces, ISDN BRI interfaces, synchronous and asynchronous serial interfaces, and PON interfaces	WAN interfaces depend on the device model and the boards installed.
	Interface backup	Various WAN interface backup mechanisms, and association between interface backup and NQA, BFD, and routes	None
	Link layer protocol	Link layer protocols such as Point-to-Point Protocol/ Multilink Protocol (PPP/ MLPPP), 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 FR compression and FR over IP Access of PPPoE IPv4 or IPv6 host and PPPoE dial-up	On the AR150 and AR200, the link layer protocol cannot be FR, MFR, or HDLC.
	Dialing	Dial control center (DCC) function and logical interfaces that transmit the dialing service	None
	PON	EPON and GPON working modes, and connection with an OLT	The AR150 series and AR200 series do not support PON.
	Network bridge	Bridge between Ethernet interfaces and WAN interfaces	None

Feature	Sub-feature	Description	Difference
	3G	3G uplink, allowing access to 3G networks using the DCC function (the AR provides the 3G data card and 3G SIC card)	The AR150 series and AR200 series do not support the 3G data card or 3G SIC card. Only specified 3G models support 3G uplink.
Voice	Line configuration	Foreign exchange station (FXS), foreign exchange office (FXO), VE1, and ISDN line access and configuration	Only the AR207V, AR207V-P, AR1220V, AR1220VW, AR2200 series, and AR3200 series support voice features.
	SIP AG	The upper-layer device such as soft switch performs call control and management. The AR communicates with the soft switch by using the SIP protocol. The AR provides the Branch Exchange for Survivable Telephony (BEST) function.	
	PBX	The AR provides FXS, FXO, VE1, and ISDN interfaces, and supports R2 signaling, H323 signaling, media proxy, multi-party conference, blacklist, and DISA service.	
IP application	ARP	Address resolution for Ethernet	None
	IPv4/IPv6 host	IPv4 and Ipv6 address management, TCP/UDP socket, ICMP, ping and tracert, and UDP helper	None
	DNS	DNS client, DNS proxy, and dynamic DNS (DDNS) client	None
	DHCP	DHCP client(v4/v6), DHCP relay, and DHCP server, and DHCP security	None
	NetStream	Fixed packet sampling and packet statistics collection, with flow output in V5, V8 or V9 format	None

Feature	Sub-feature	Description	Difference
	NAT	NAT, port address translation (PAT), port application mapping (PAM), Easy NAT, and NAT server, providing application layer gateways (ALG) for each application	None
	VRRP	Redundancy backup mechanism for IP services	None
	BFD	Single-hop BFD, multi-hop BFD, BFD for VRRP, and BFD for routing protocols	None
	Network Quality Analysis (NQA)	Detecting the performance of protocols running on the network	None
IP routing	IPv4 and IPv6 Static route	Basic routing functions	None
	RIP and RIPng	Routing protocol	None
	OSPFv2 and OSPFv3	Routing protocol	None
	ISIS and ISISv6	Routing protocol	None
	BGP and BGP4+	Routing protocol	None
	Routing policy	Basic routing functions and intelligent PBR	None
Multicast	IGMP	Basic IGMP functions including IGMP snooping	Only the AR2200 series and AR3200 series support IGMP snooping.
	Multicast routing	Multicast route management, multicast route load balancing, and source-specific multicast (SSM) mapping	None
	PIM (IPv4)	PIM-DM and PIM-SM	None
	MSDP	Inter-domain (PIM-SM domain) multicast routing	None
QoS	MQC	Modular traffic classification	None

Feature	Sub-feature	Description	Difference
	Priority mapping	Mapping between local priorities, 802.1p priorities, DSCP priorities, and EXP priorities	None
	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	None
	Traffic shaping	Traffic shaping based on traffic classifiers, PVCs/ VLANs/DLCIs, and ports, traffic shaping adaptation, and three-level traffic shaping	None
	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, and CBQ	None
	Congestion avoidance	Priority-based weighted random early detection (WRED) and tail drop	None
	HQoS	Hierarchical Quality of Service (HQoS) implements hierarchical scheduling based on queues and differentiates services and users.	None
	Smart Application Control (SAC)	SAC uses the deep packet inspection (DPI) technology to identify packets of dynamic protocols such as HTTP, FTP, and RTP by checking Layer 4 to Layer 7 information in the packets. SAC helps implement refined QoS management.	None
Security	AAA	AAA for administrators and access users, including local, RADIUS, and TACACS AAA	None

Feature	Sub-feature	Description	Difference
	Firewall	DMZ firewall, packet filtering firewall, and stateful firewall; blacklist and whitelist, and attack detection	None
	Traffic suppression	Traffic suppression based on ports	None
	Access security	802.1x authentication, MAC address authentication, MAC address bypass authentication, and direct MAC address authentication based on users and ports; web authentication and guest VLAN for access users	None
	Local attack defense	Device protection measures, including CPU attack defense and attack source tracing.	None
	ARP security	Suppression of ARP packets from the user side and network side, ARP anti-spoofing, ARP gateway attack inspection, and dynamic ARP inspection (DAI)	Only the AR2200 series and AR3200 series support DAI.
	IP security	ICMP anti-attack, URPF, IP source guard and DHCP snooping	Only the AR2200 series and AR3200 series support IP source guard and DHCP snooping.
	PKI	Certificate request, update, and verification	None
	HTTPS	HTTPS server function, ensuring transmission security between users and devices using SSL features such as data encryption and identity verification	None
	ACL	Traffic classification based on physical ports, Layer 2 information, IP protocols, and TCP/UDP ports.	None

Feature	Sub-feature	Description	Difference
VPN	IPSec VPN	Interconnecting headquarters and branches using IKE V1/ V2 IPSec tunnels; hardware-based MD5 and SHA algorithms; AES, DES, and 3DES algorithms	None
	SSL VPN	Virtual gateway, front-door VPN function, and management of SSL VPN users and SSL VPN services	None
	DSVPN	Dynamic setup of a data forwarding channel between hubs	None
	L2TP	Functioning as the LAC or LNS and allowing concurrent user access on multiple channels	None
	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	None
Device management	Information center monitoring	Managing boards, power supply units, fans, and e-labels	None
	Version management	In-service upgrade, rollback, and patch installation	None
	Mirroring	Port- and flow-based mirroring	None
	Remote PoE power supply	LAN-side remote power supply	Only the AR207V-P, AR1220V, AR1220W and AR1220VW support the PoE features.
	Web-based network management system	Internal web management system, providing GUI to manage and maintain devices	None

Feature	Sub-feature	Description	Difference
	Deployment	Automatic deployment using a universal serial bus (USB) flash drive; Auto-Config function for the entire network	None
Network management	SNMP	SNMP agent, fault management (FM), and trap switch control (TSC)	None
	Ping and Tracert	Network connectivity detection	None
	NTP	Time synchronization for traditional IP networks	None
	RMON	Monitoring and traffic statistics for traffic on a network segment	None
	CWMP	CWMP (TR-069) for remotely managing AR devices	None
MPLS	Basic MPLS functions	Static label switched path (LSP) and penultimate hop popping (PHP); MPLS LSP QoS	AR200 series routers do not support MPLS.
	MPLS LDP	MPLS LDP	
	L3VPN	BGP L3VPN	
	MPLS TE	MPLS TE	
	MPLS FRR	LDP FRR, TE FRR, and VPN FRR	

3.2 Key Features

3.2.1 Voice

In addition to broadband services, such as video on demand (VOD) and live data and video, the AR provides high-quality voice service for terminal users.

NOTE

- Among the AR200 series routers, only the AR207Vs and AR207V-Ps support the voice features. Among the AR1200 series routers, only the AR1220Vs and AR1220VWs support the voice features. The AR2200 and AR3200 series routers support the transfer of analog to digital signals, as well as digital to analog signals only after a DSP module is installed.
- To provide voice services for POTS users on AR1200, AR2200 ,and AR3200 series routers, 4FXS/1FXO board is required.
- To provide voice services for ISDN users on AR1200, AR2200 ,and AR3200 series routers, 2BST board is required.

SIP AG

Access gateway (AG) devices provide various access modes and convert various services into a uniform format that can be transmitted. The AG communicates with the soft switch by using the SIP protocol. SIP-based AGs are called SIP AGs.

When an AR functions as the SIP AG, the upper-layer devices such as soft switch control and manage calls. The AR supports the following services.

Table 3-2 Services Supported by a SIP AG

Service Type	Description
Basic voice service	The basic voice service provides call connections, including intra-office calls, local calls, national long-distance calls, international long-distance calls, and transit calls.
Three-party service	The third-party service allows a calling party or called party in a conversation to call a third party without ending the current conversation. Then the calling party or original called party can make a three-party conversation or talk to the other two parties separately.
Call waiting service	If user C calls user A when user A is talking with user B, user A hears a call waiting tone indicating that there is an incoming call.
MWI service	The message waiting indicator (MWI) service allows a user to read unread or leave messages. When the called user is busy, the MWI is on indicating that there are messages.
Malicious call identification (MCID) service	The MCID service allows users to perform certain operations to find the phone number of an attacker that initiates malicious calls.
Call transfer service	The call transfer service allows the called party to transfer an incoming call to a third party by pressing the hookflash so that the calling party establishes a connection with a new called party.
Call conference service	The call conference service allows more than three parties to talk to each other.
Calling line identification presentation (CLIP) service	The CLIP service displays the calling number in onhook state or offhook state (for call waiting). The displayed information includes the phone number, name, date, and time.

Service Type	Description
Calling line identification restriction (CLIR) service	The CLIR service shields the calling number on the terminal of a called party.
Distinctive ringing service	The distinctive ringing service plays different ring tones for incoming calls from different calling parties.
Differentiated ringback tone service	The differentiated ringback tone service plays different ringback tones for different users.
Advice of charge (AoC) service	The AoC service displays the charge rate, fee notification during a call, and total fee of the call.
Polarity reversal charging service	The polarity reversal charging service notifies the accounting terminal of the accounting starting point and stop point using polarity reversal when users are in a conversation or end the conversation.
Polarity reversal pulse charging service	The polarity reversal pulse charging service generates a polarity reversal pulse on an interface to notify the accounting terminal of the accounting starting point and stop point during a conversation or when the conversation ends.
Urgent call process	If the SIP AG detects an urgent call, it inserts an urgent call flag into the SIP message.
Completion of Calls to Busy Subscriber (CCBS) service	The CCBS service enables the SIP AG to monitor the called party status when the called party is busy. When the called party is idle, the SIP AG notifies the calling party so that the calling party can determine whether to make a call to the called party again.
Multiple MSN numbers on a POTS interface	Multiple MSN numbers can be configured on a POTS interface.
Hotline service	● Instant hotline service: After a user picks up a phone, the SIP AG dials the hotline number for the user. ● No dialing within a long time after picking up the phone: If a user does not dial any number within the specified period of time after picking up a phone, the SIP AG dials the hotline number for the user.
Anonymous call service	The anonymous call service disables the called party from viewing information about incoming calls.
BEST	When the primary channel between the branch and headquarters is faulty, enable the Branch Exchange for Survivable Telephony (BEST) function in the branch to implement communication in the branch and between the branch and the headquarters over the PSTN.

PBX

PBXs are widely used in enterprises. They manage incoming and outgoing calls of enterprises. The AR as a PBX supports the following individual and group services.

Table 3-3 Individual Service supported by a PBX

Service Type	Description
Abbreviated dialing	Allows a user to dial an abbreviated code of one or two digits instead of the original called number.
Outgoing call barring	Restricts call-out permissions of some phones. For example, the outgoing call barring service can prevent a phone from making long-distance calls.
Call forwarding	Allows a called user to transfer a call to a specified third party if the called user has activated the call forwarding service and the call meets the call forwarding conditions.
Number barring	Prevents a user from dialing a specified number.
Do-not-disturb	Rejects calls to a user. When other users call a user that has subscribed to the do-not-disturb service, they hear a do-not-disturb tone or busy tone.
Reject anonymous call	Allows a user to reject a call when the calling number is not displayed and plays a voice prompt to the calling user.
Remote office	Allows a user to access the office telephone network from any terminal and use original services such as abbreviated dialing and call transfer.
Secretary	Allows a user to designate another phone number (for example, the secretary's phone number) to process all incoming calls. That is, all incoming calls of the user are transferred to the secretary's phone number first, and only the secretary can call the user directly.
Wake-up service	Allows a phone to ring automatically at the preset time.
Personal ring back tone (RBT)	Uses user-defined music or sound effects to replace the common ringback tone, and plays the music or sound effects to calling users.

Service Type	Description
Selective call rejection	Filters every incoming call against a list of rejected calling numbers created by a user and rejects calls made by numbers on the list.
Selective call acceptance	Filters every incoming call against a list of calling numbers created by a user and accepts calls from only the numbers on the list.

Table 3-4 Group Services supported by a PBX

Service Type	Description
Call interception	Provides a voice prompt when a call fails to be connected. The user can learn about the failure cause and determine whether to redial the called number according to the voice prompt.
Distinctive ringing	Plays different ring tones to users based on the prefix analysis result (local calls, national calls, international calls, and intra-Centrex calls).
Enterprise RBT	Uses music or sound effects made by an enterprise to replace the common ringback tone, and plays the music or sound effects to calling users.
Interactive voice response (IVR)	Provides the automated attendant function and allows enterprises to make their own IVR menus and voice prompts, improving user experience.
Number change	Hides calling numbers or displays the same calling number for all outgoing calls.
Pre-routing number change	Provides various dialing modes and changes the calling number displayed on the called party's phone.
Post-routing number change	Provides various dialing modes and changes the calling number displayed on the called party's phone. A post-routing number change plan can change a called number to a long number to ensure that it complies with the required number format.
PBX line selection	When a calling party dials the access number of a PBX group, the system uses the configured line selection mode to connect the call to a user in the group.

Service Type	Description
Co-group pickup	Allows users in the same group to answer calls for each other on their own phones. For example, when the phone of user A rings, user B in the same group can dial the service access code plus user A's phone number to answer the call.
Simultaneous ringing	When a calling party dials the access number of a simultaneous ringing group, all member phones in the group ring simultaneously, and the called party can answer the call using any ringing phone.
Sequential ringing	When a calling party dials the access number of a sequential ringing group, member phones in the group ring in the configured sequence.
One number link you (ONLY)	When the calling party calls ONLY number of the called party, multiple terminals of the called party ring according to the configured rules, and the called party can select one terminal to answer the incoming call.

For details about voice features, see Feature Description - Voice.

3.2.2 WAN

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

The FR compression technologies compress FR packets to save network bandwidth, reduce network load, and improve data forwarding on the FR network. The AR supports FRF.9 (FRF. 9 stac) and FRF.20 (FRF.20 IPHC).

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.

Multilink PPP (MP) is a technique that bundles multiple PPP links together to increase bandwidth. It can be applied to the interfaces that support PPP, such as serial interfaces and low-speed Packet over SDH (POS) interfaces.

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.

ATM

ATM is connection-oriented. Each VC is identified by a Virtual Path Identifier (VPI) and a Virtual Channel Identifier (VCI). One pair of VPI/VCI values is useful only on a link segment between ATM nodes. If a connection is broken, the relevant VPI/VCI values are released.

The Asymmetric Digital Subscriber Line (ADSL) , VDSL and G.Single-pair High Speed Digital Subscriber Line (G.SHDSL) interfaces of the ARs support the Asynchronous Transfer Mode (ATM).

HDLC

The High-level Data Link Control (HDLC) is a typical bit-oriented synchronization data control protocol. It adopts the full-duplex mode and CRC check. Its transmission control function is independent of the processing function, and it features control capabilities and can be flexibly used.

In HDLC, Keepalive packets are used to detect the link status. On the AR, you can set the interval for sending Keepalive packets by setting the polling interval.

ISDN

The ISDN protocol references the Open Systems Interconnection (OSI) model and implements functions of the physical layer, data link layer, and network layer on UNI interfaces.

ISDN physical interfaces are classified into ISDN BRI and ISDN PRI interfaces.When the AR accesses an ISDN network by using an ISDN PRI interface, the AR is directly connected to an ISDN network-side device. When the AR accesses an ISDN network by using an ISDN BRI interface, the AR connects to an NT1 device, and the NT1 device connects to an ISDN network-side device.

For details about WAN features, see Feature Description - WAN.

3.2.3 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 AR supports IPSec VPN and provides high reliability transmission tunnels for users. In addition, the AR uses Generic Routing Encapsulation (GRE) and Layer 2 Tunneling Protocol (L2TP) to support the following VPN services:

- GRE VPN
- IPSec VPN
- BGP/MPLS IP VPN
- SSL VPN
- L2TP VPN
- DSVPN
- GRE over IPSec VPN
- L2TP VPN over IPSec VPN

For details about VPN features, see Feature Description - VPN.

3.2.4 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.

IP Source Guard

Some attacks on networks aim at source IP addresses by accessing and using network resources through spoofing IP addresses, stealing users' information or blocking authorized users from accessing networks.

- The AR2200 and AR3200 series routers support IP source guard. IPSG prevents source address spoof attacks, so attackers cannot access network resources and authorized users' rights are protected.
- Unicast Reverse Path Forwarding (URPF) blocks packets sent from bogus source addresses.

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.

PKI

The public key infrastructure (PKI) is a system that generates public keys and digital certificates, and verifies identities of certificate subjects to ensure information security. PKI issues digital certificates that bind public keys to respective user identities by means of a certificate authority (CA).

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.

For details about security features, see Feature Description - Security.

3.2.5 QoS

Traffic Policing

Traffic policing discards excess traffic 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 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 AR supportstraffic shaping adaptation and level-3 traffic shaping. Three-level shapers include the flow queue shaper, subscriber queue shaper, and port queue shaper.

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 has four default queues and each of other interfaces has eight. LAN-side interfaces support the scheduling modes of priority queuing (PQ), deficit round robin (DRR), weighted round robin (WRR), PQ+DRR, and PQ+WRR. The AR150&200&1200 series routers do not support the DRR mode. 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 affects 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.

For details about QoS features, see Feature Description - QoS.

3.2.6 WLAN

NOTE

Only AR1220W and AR1220VW support WLAN.

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 functions 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

For details about WLAN features, see Feature Description - WLAN.

3.2.7 IPv6

The AR1200 provides the IPv6 host function, which maximizes customers' return on investment (ROI) and prevents repeated investment during network upgrade.

The AR supports the following IPv6 functions:

- IPv6 ND
- IPv6 PMTU
- TCP6, UDP6, RawIP6, Ping IPv6, and Tracert IPv6
- ICMP6 and Socket6
- IPv6 unicast routing protocols: RIPng, OSPFv3, IS-IS, BGP, and IPv6 static route

- TFTP IPv6 client, TFTP IPv6 server, FTP IPv6 client, FTP IPv6 server, Telnet IPv6 client, and Telnet IPv6 server
- SNMP IPv6

For details about IPv6 functions, see Feature Description - IP Service and Feature Description - IP Routing.

4 Device Structure of AR150 and AR200 Series

The following figures show the front view and the rear view of AR150 and AR200 series.

Front view and rear view of AR150 series

Figure 4-1 AR151 front view

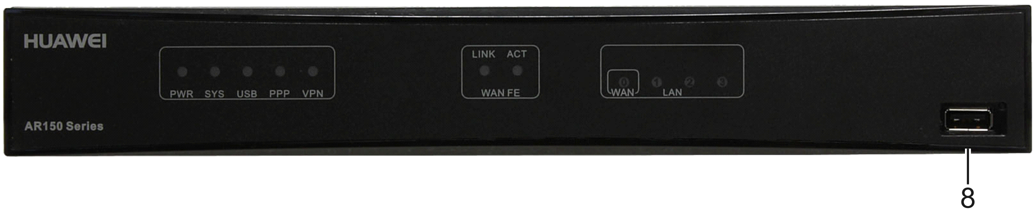


Figure 4-2 AR157 front view

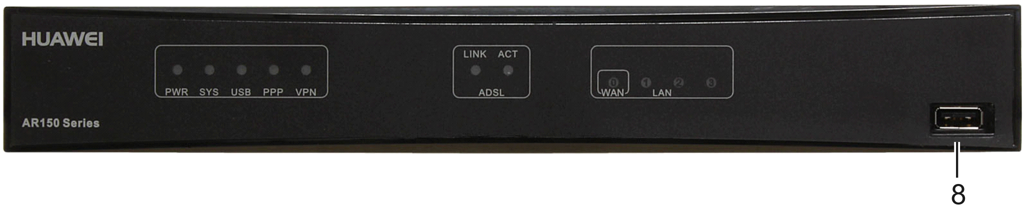


Figure 4-3 AR151 rear view

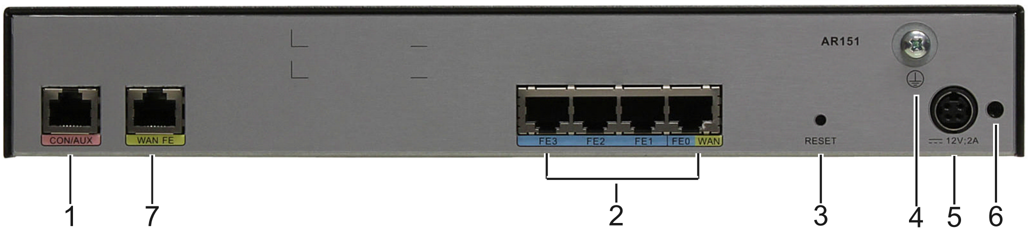
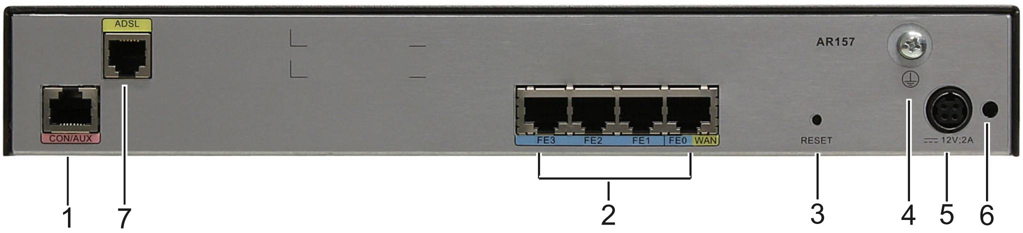


Figure 4-4 AR157 rear view



1. CON/AUX interface	2. Fixed FE interfaces	3. RESET Button	4. Ground screw
5. AC jack	6. Access hole for the power cable	7. WAN-side uplink interface	8. USB interface

NOTE

- The AR150 provides four LAN-side FE interfaces. The FE0 interface can be configured as a WAN-side Layer 3 interface.
- On the AR151, FE interfaces are WAN-side interfaces. On the AR157, ADSL ANNEX A/M interfaces are WAN-side interfaces.

Front view and rear view of AR200 series

Figure 4-5 AR201 front view

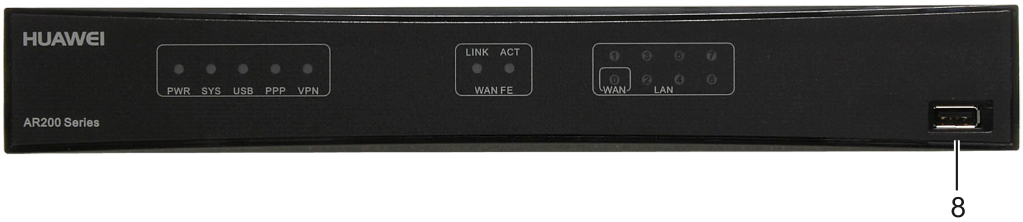


Figure 4-6 AR206 front view

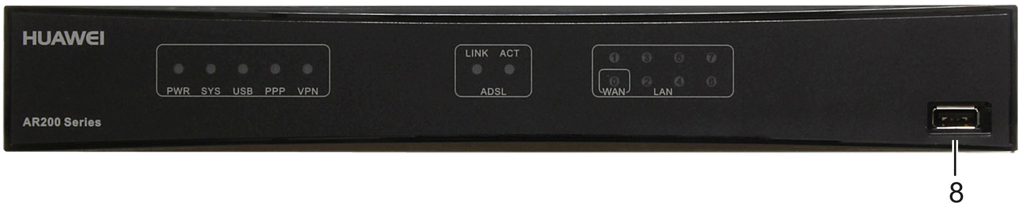


Figure 4-7 AR207 front view

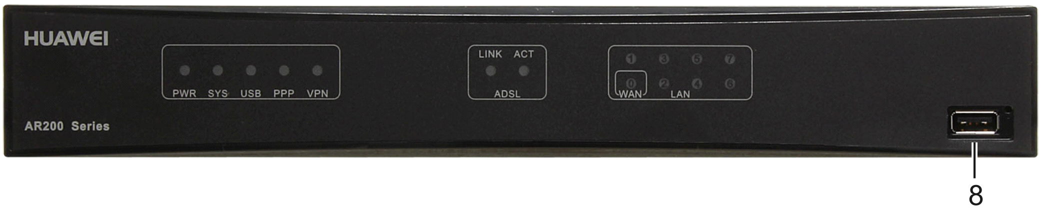


Figure 4-8 AR207V front view

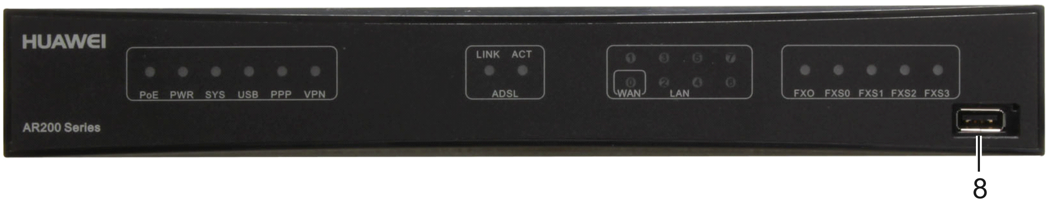


Figure 4-9 AR207V-P front view

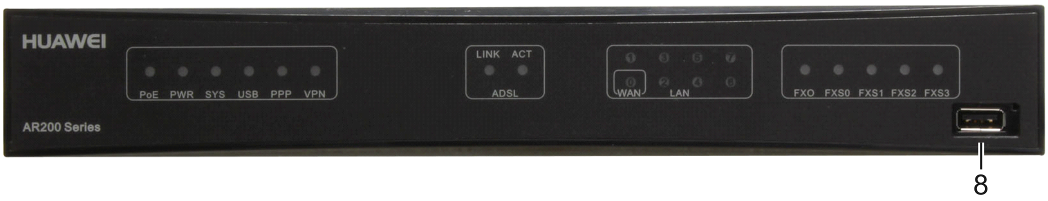


Figure 4-10 AR207G-HSPA+7 front view

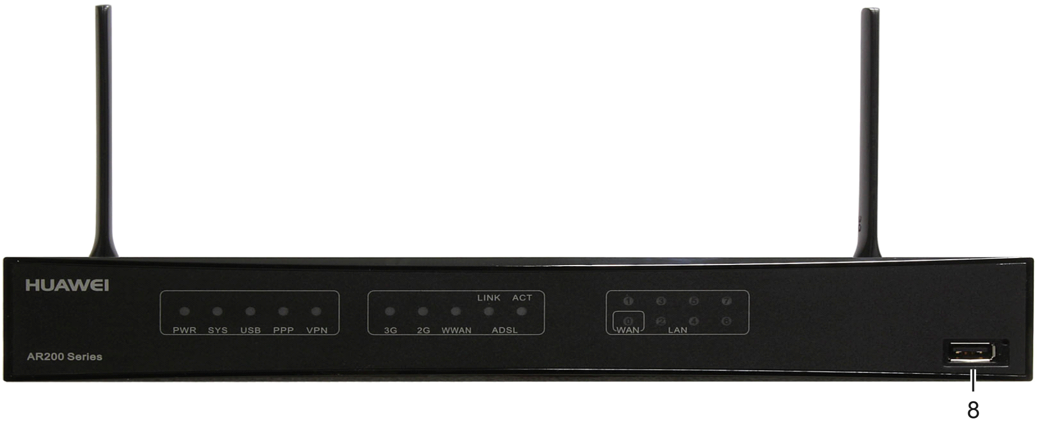


Figure 4-11 AR208E front view

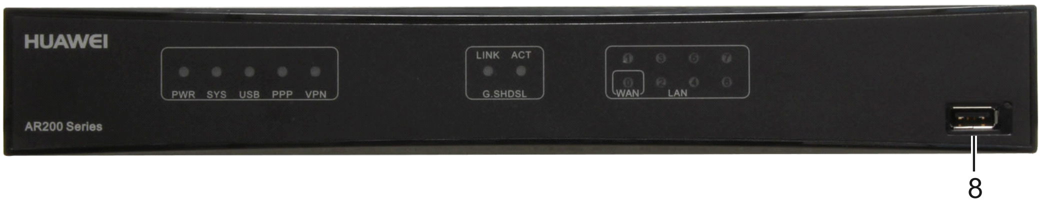


Figure 4-12 AR201 rear view

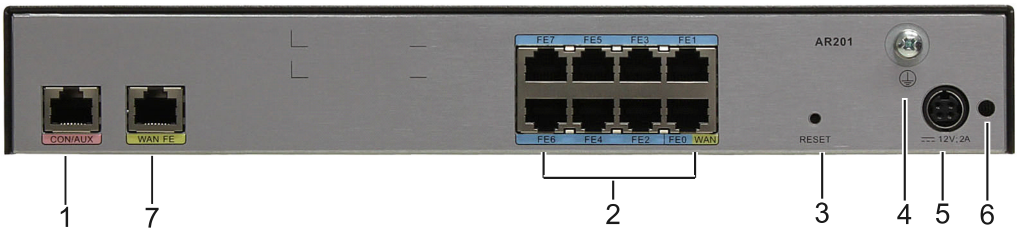


Figure 4-13 AR206 rear view

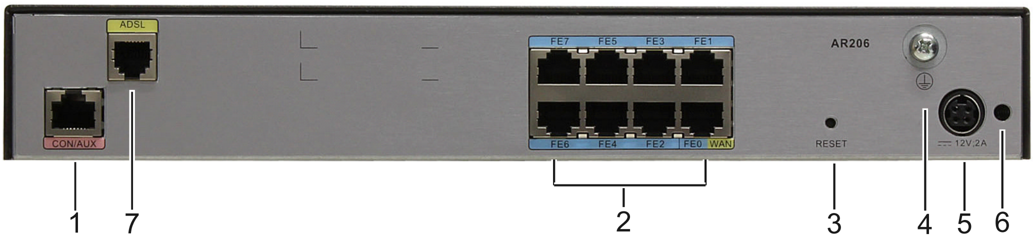


Figure 4-14 AR207 rear view

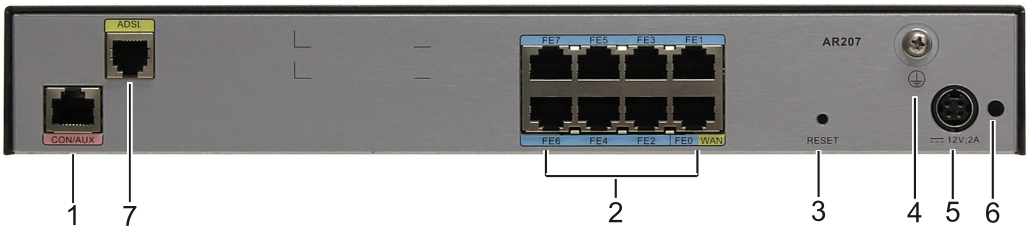


Figure 4-15 AR207V rear view

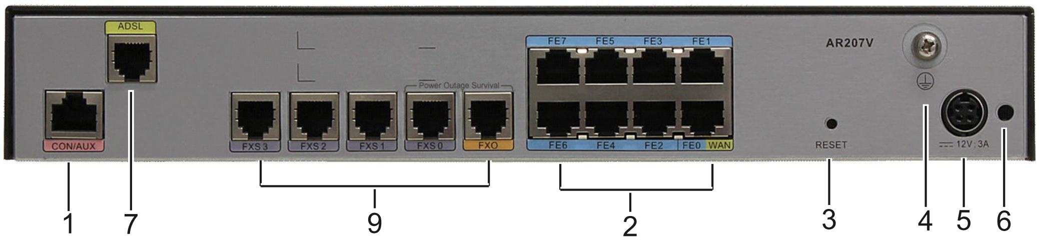


Figure 4-16 AR207V-P rear view

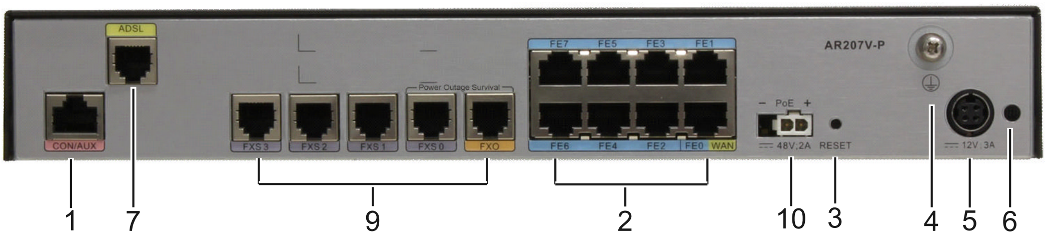


Figure 4-17 AR207G-HSPA+7 rear view

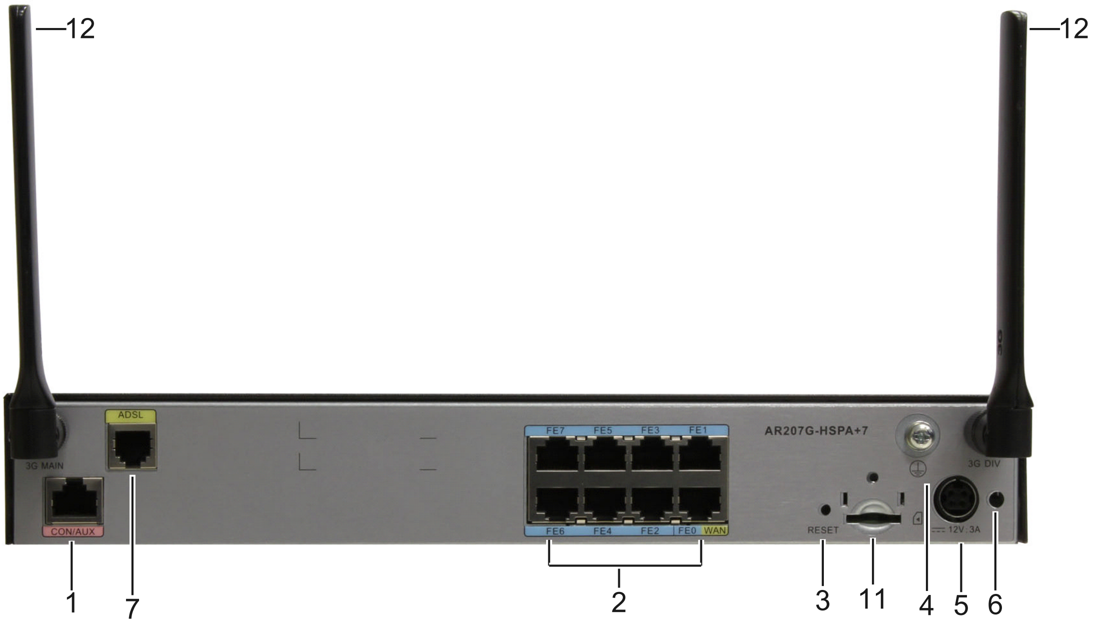
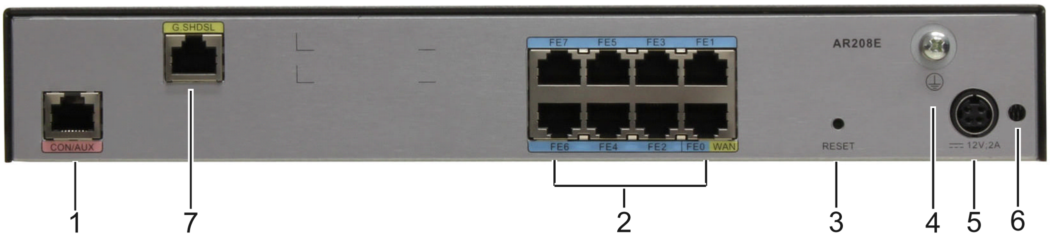


Figure 4-18 AR208E rear view



1. CON/AUX interface	2. Fixed FE interfaces	3. RESET Button	4. Ground screw
5. AC jack	6. Access hole for the power cable	7. WAN-side uplink interface	8. USB interface
9. 4FXO/1FXS interfaces	10. PoE port	11. SIM card slot	12. 3G antenna

NOTE

- The AR200 provides eight LAN-side FE interfaces. The FE0 interface can be configured as a WAN-side Layer 3 interface.
- On the AR201, WAN-side interface is FE interface . On the AR206, WAN-side interface is ADSL ANNEX B interface. On the AR207, AR207V, AR207V-P, and AR207G-HSPA+7, WAN-side interface is ADSL ANNEX A/M interfaces. On the AR208E, WAN-side interface is 4-channel G.SHDSL interface.

5 Device Structure of AR1200, AR2200 and AR3200 Series

Appearance

Figure 5-1 and Figure 5-2 show the front view of AR1200 series.

NOTE

AR1220 has two models: AC model and DC model. The two models are identical in the front panels, but different in the power supply units at the rear of the chassis.

Figure 5-1 AR1220/AR1220V/AR1220L front view

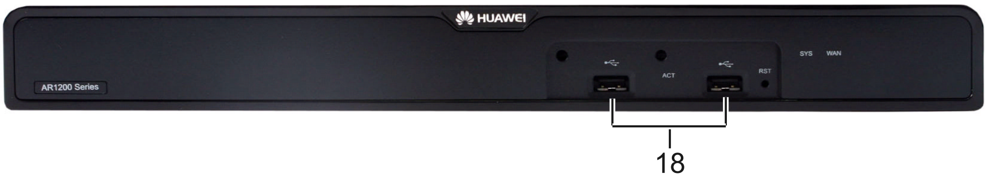


Figure 5-2 AR1220W/AR1220VW front view

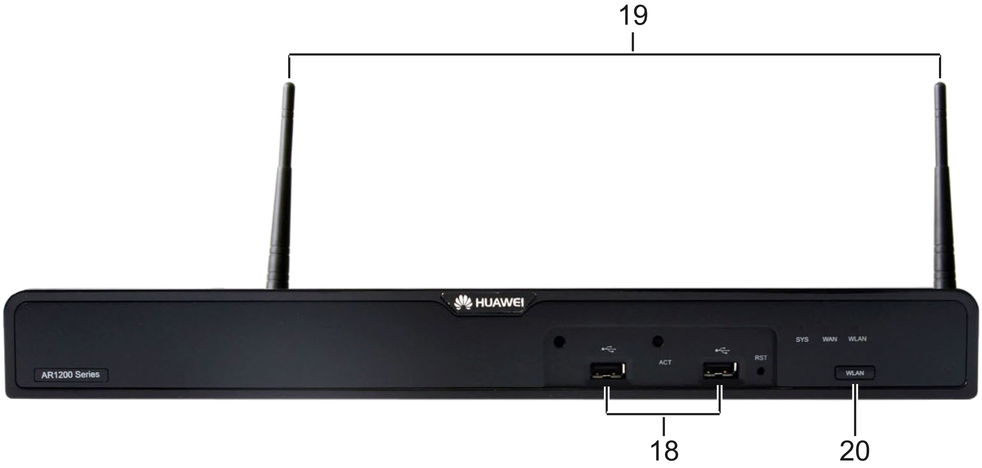


Figure 5-3, Figure 5-5, Figure 5-6, Figure 5-7, and Figure 5-8 show rear views of AR1200 series.

Figure 5-3 AR1220 rear view

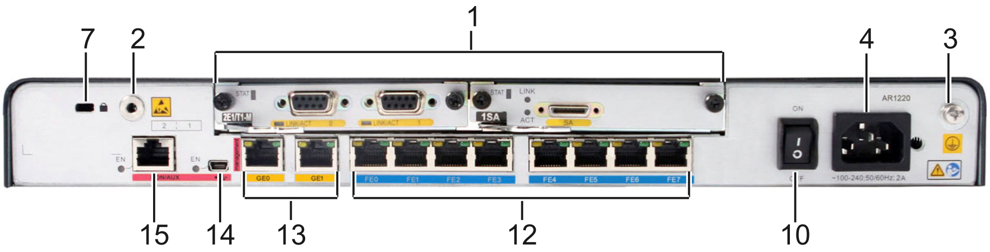


Figure 5-4 AR1220-D rear view

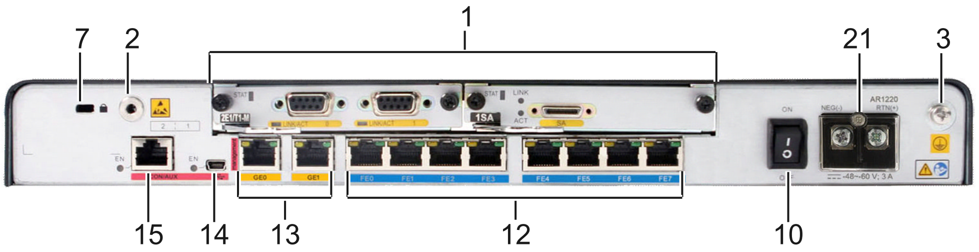


Figure 5-5 AR1220V rear view

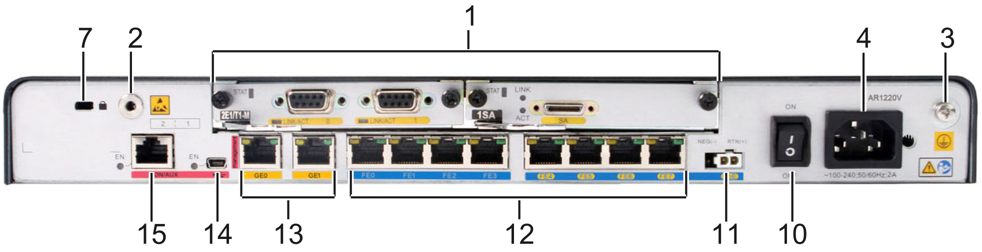


Figure 5-6 AR1220W rear view

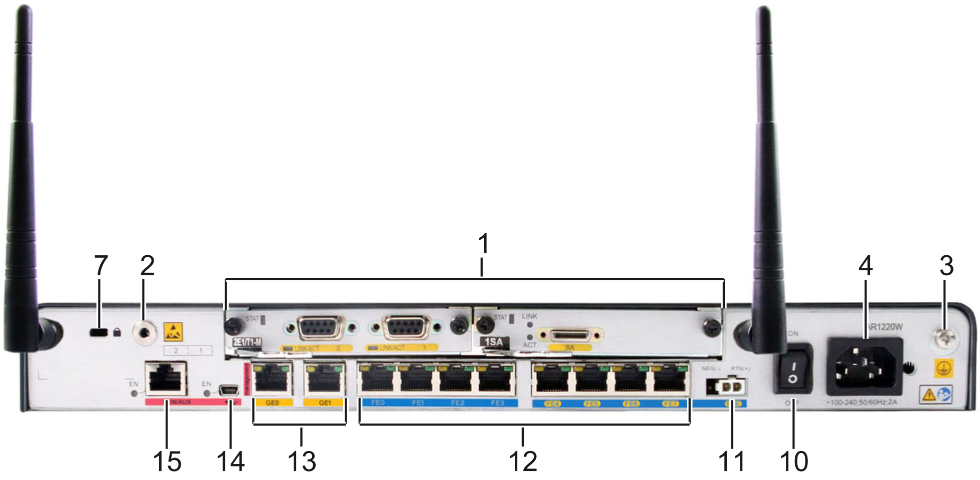


Figure 5-7 AR1220VW rear view

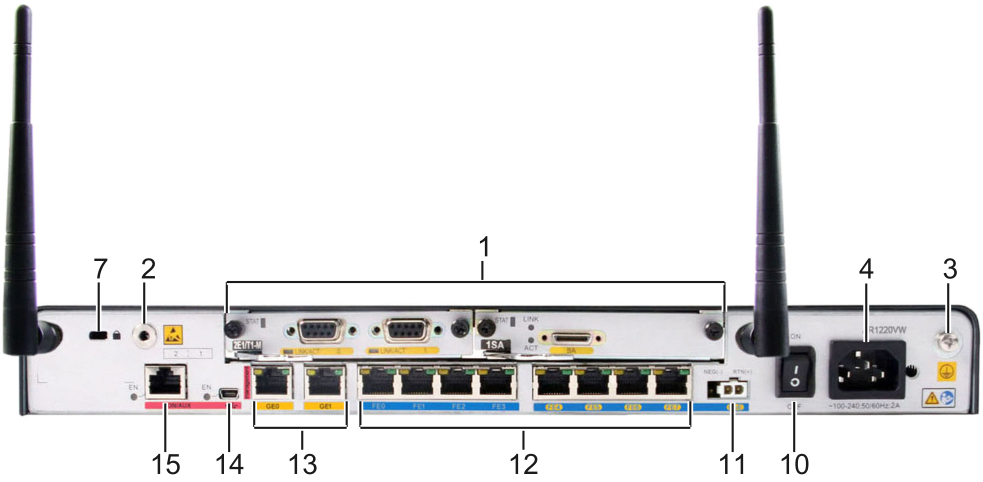
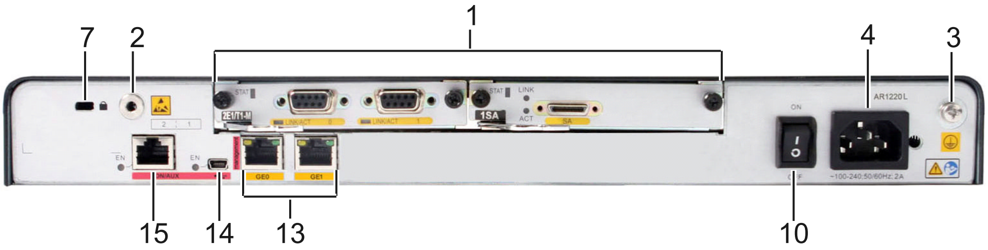


Figure 5-8 AR1220L rear view



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
19. Antenna	20. WLAN switch button		

Figure 5-9 and Figure 5-10 show front views of AR2200 series.

Figure 5-9 AR2220 front view

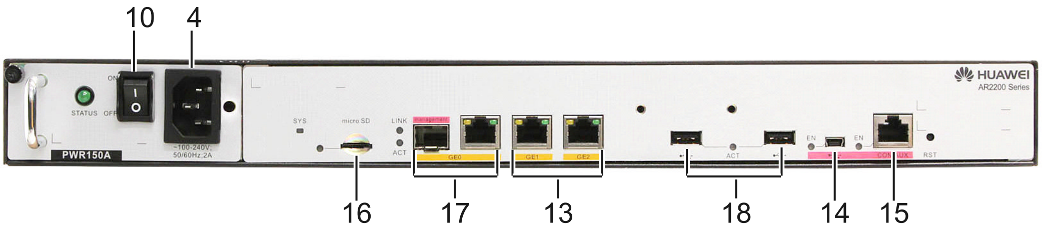


Figure 5-10 AR2240 front view

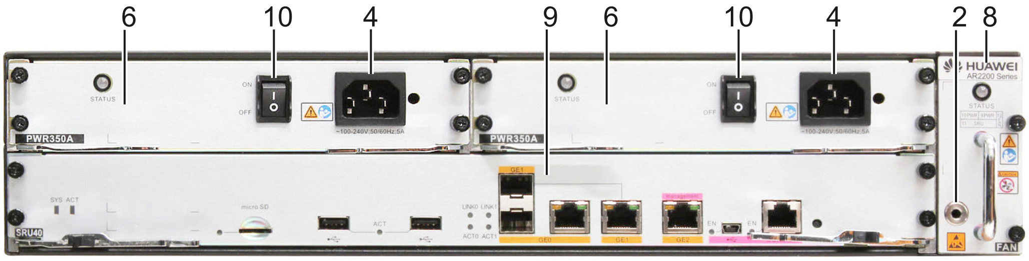


Figure 5-11 and Figure 5-12 show rear views of AR2200 series.

Figure 5-11 AR2220 rear view

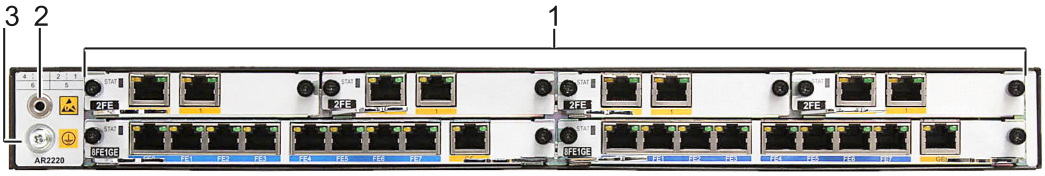
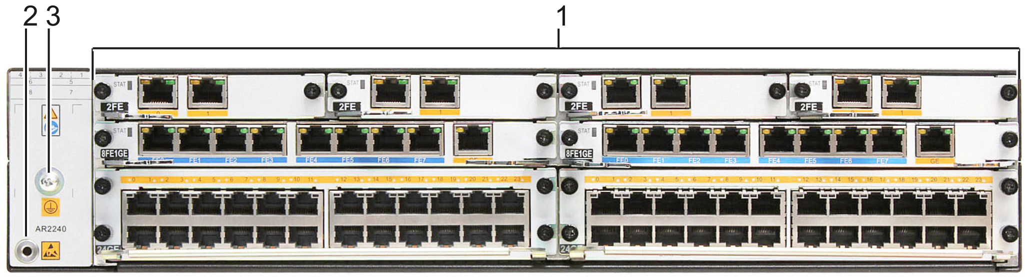


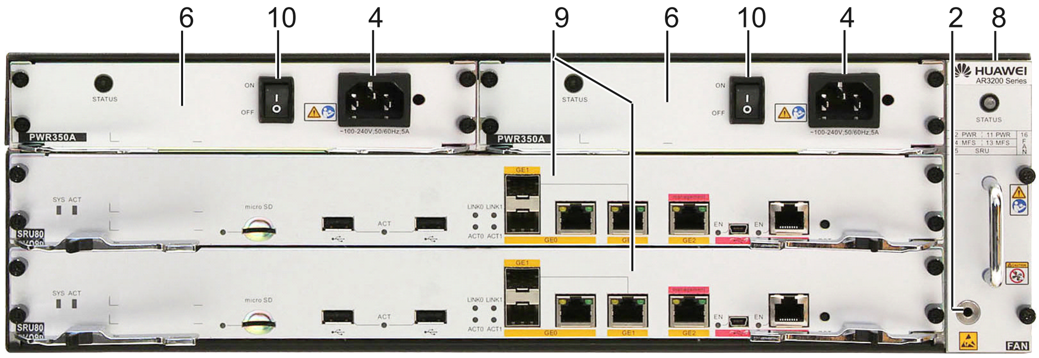
Figure 5-12 AR2240 rear view



1. Pluggable card	2. ESD jack	3. Ground screw	4. AC jack
6. Pluggable AC power supply unit	8. Pluggable fan module	9. SRU	10. AC power switch
13. Two Fixed GE interfaces on the panel	14. Mini USB interface	15. CON/AUX interface	16. Micro SD card interface
17. GE optical/ electrical Combo interface	18. USB interfaces		

Figure 5-13 shows the front view of AR3260.

Figure 5-13 AR3260 front view

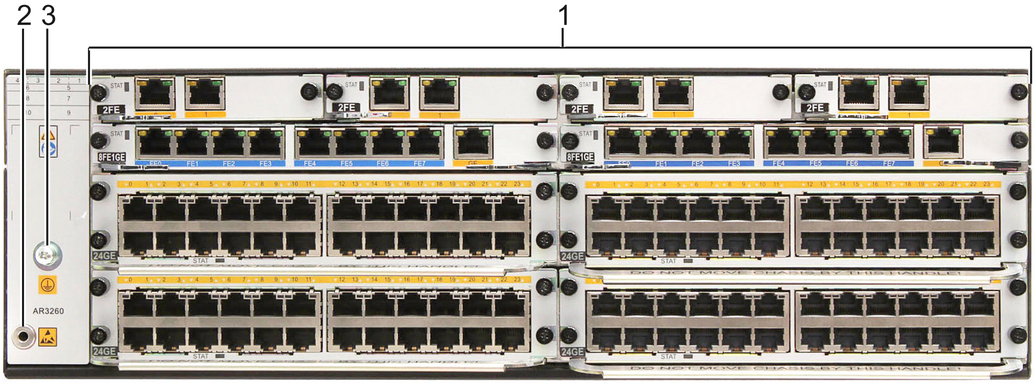


NOTE

The AR3260 supports only one SRU, which can be installed in slot 15. It will support double SRUs in later versions.

Figure 5-14 shows the rear view of AR.

Figure 5-14 AR3260 rear view



1. Pluggable card	2. ESD jack	3. Ground screw	4. AC jack
6. Pluggable AC power supply unit	8. Pluggable fan module	9. SRU	10. AC power switch

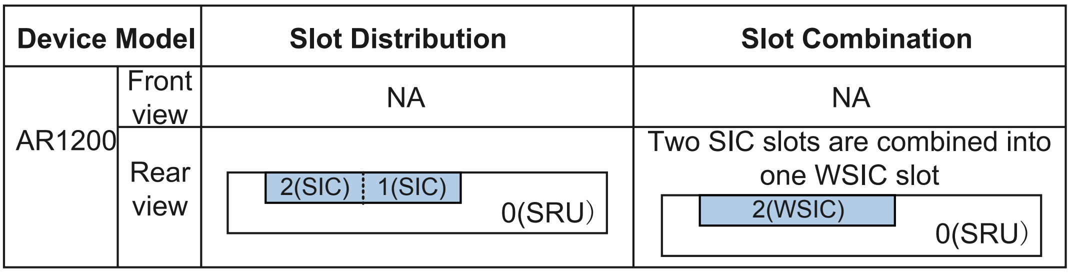
Slot distribution

Figure 5-15, Figure 5-16 and Figure 5-17 show slot distribution on AR.

NOTE

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

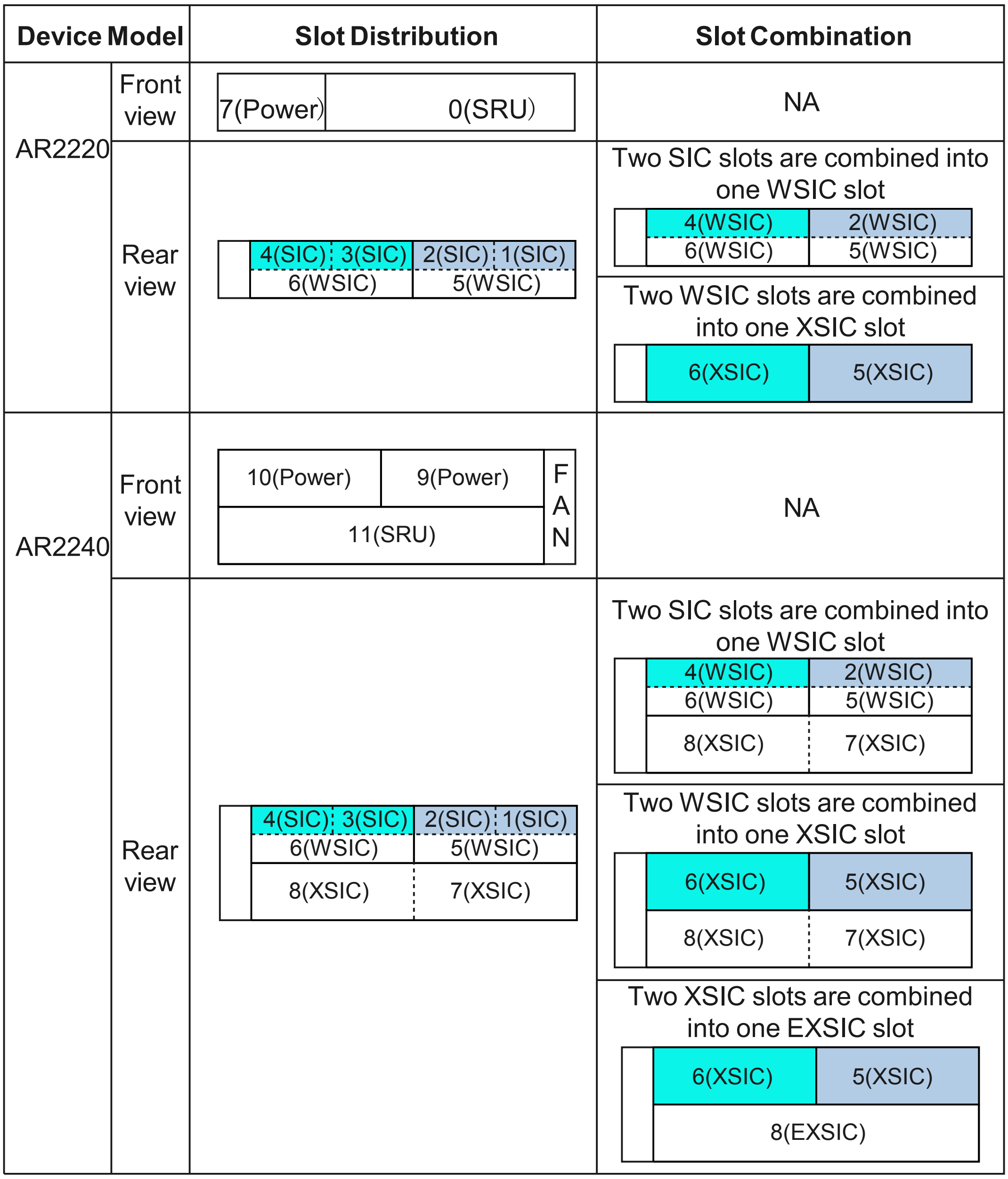
Figure 5-15 Slot distribution on AR1200



Device Model		Slot Distribution	Slot Combination
AR1200	Front view	NA	NA

	Rear view	2(SIC) 1(SIC)
		0(SRU)
			Two SIC slots are combined into one WSIC slot
			2(WSIC)
			0(SRU)

Figure 5-16 Slot distribution on AR2200



Device Model		Slot Distribution	Slot Combination
AR2220	Front view	7(Power) 0(SRU)	NA

	Rear view	4(SIC) 3(SIC) 2(SIC) 1(SIC)
		6(WSIC) 5(WSIC)
			Two SIC slots are combined into one WSIC slot
			4(WSIC) 2(WSIC)
			6(WSIC) 5(WSIC)

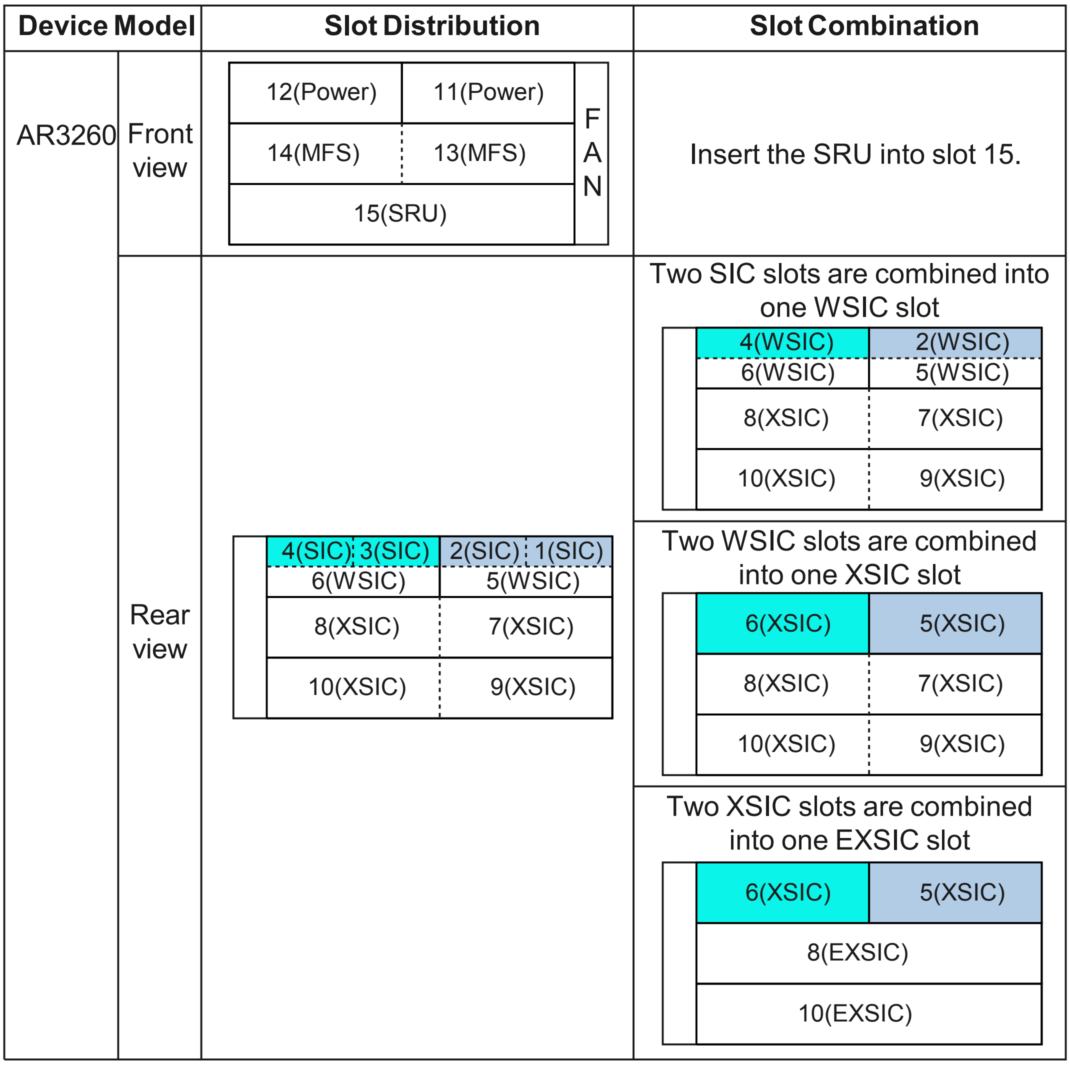
			Two WSIC slots are combined into one XSIC slot 6(XSIC) 5(XSIC)
AR2240	Front view	10(Power) 9(Power) FAN 11(SRU)	NA

	Rear view	4(SIC) 3(SIC) 2(SIC) 1(SIC)
		6(WSIC) 5(WSIC)
		8(XSIC) 7(XSIC)
			Two SIC slots are combined into one WSIC slot
			4(WSIC) 2(WSIC)
			6(WSIC) 5(WSIC)
			8(XSIC) 7(XSIC)

			Two WSIC slots are combined into one XSIC slot
			6(XSIC) 5(XSIC)
			8(XSIC) 7(XSIC)

			Two XSIC slots are combined into one EXSIC slot
			6(XSIC) 5(XSIC)
			8(EXSIC)

Figure 5-17 Slot distribution on AR3200



As shown in **Figure 5-15**, **Figure 5-16** and **Figure 5-17**, the slots of AR can be combined.

- AR1200 Series
  - Slot 1 and slot 2 are combined into new slot 2.
- AR2220
  - Slot 1 and slot 2 are combined into new slot 2.
  - Slot 3 and slot 4 are combined into new slot 4.
  - New slot 2 and slot 5 are combined into new slot 5.
  - New slot 4 and slot 6 are combined into new slot 6.
- AR2240
  - Slot 1 and slot 2 are combined into new slot 2.
  - Slot 3 and slot 4 are combined into new slot 4.
  - New slot 2 and slot 5 are combined into new slot 5.

  - New slot 4 and slot 6 are combined into new slot 6.
  - Slot 7 and slot 8 are combined into new slot 8.
- AR3260
  - Slot 1 and slot 2 are combined into new slot 2.
  - Slot 3 and slot 4 are combined into new slot 4.
  - New slot 2 and slot 5 are combined into new slot 5.
  - New slot 4 and slot 6 are combined into new slot 6.
  - Slot 7 and slot 8 are combined into new slot 8.
  - Slot 9 and slot 10 are combined into new slot 10.
  - Slots 13 and 14 are multiple function slots. They can be combined into new slot 14, which is reserved for the slave main control board.

6 Maintenance and Management

About This Chapter

6.1 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).

6.1.1 Web-based Network Management System

The ARs support the web-based network management system, which provides GUI for device configuration and management.

Users can use the web-based system to manage network devices on the GUI. A junior engineer can use the GUI easily.

6.1.2 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.

6.1.3 Remote Deployment and Maintenance Using USB

As the network expands, more and more network devices are used and software commissioning costs increase. USB-based deployment does not require software commissioning, which reduces deployment costs.

Before using a USB flash drive to configure an AR, store software package and configuration files on the USB flash drive. Software engineers do not need to commission devices onsite. After installing the AR, hardware engineers will insert the USB flash drive into the USB interface on the AR and power on the AR. After being started, the AR automatically loads and upgrades the software.

6.1.4 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.

6.2 Fault Location

6.2.1 Device Fault Location

The ARs support the following functions to locate device faults:

- 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 **display diagnostic-information** 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.

6.2.2 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 and traffic 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.

- Voice signal fault

  The ARs record the entire signal interaction process and test signal online. In addition, the ARs test the quality of VoIP services and locate dialing and service faults.

7 System Parameters

About This Chapter

7.1 System Configuration

Table 7-1 System configuration

Model	Processor	Memory	Flash Memory	Micro SD Card (built-in)
AR151	Dual-core, 533 MHz	512 MB	512 MB	0
AR157	Dual-core, 533 MHz	512 MB	512 MB	0
AR201	Dual-core, 533 MHz	512 MB	512 MB	0
AR206	Dual-core, 533 MHz	512 MB	512 MB	0
AR207	Dual-core, 533 MHz	512 MB	512 MB	0
AR207V	Dual-core, 533 MHz	512 MB	512 MB	0
AR207V-P	Dual-core, 533 MHz	512 MB	512 MB	0
AR207G-HSPA+7	Dual-core, 500 MHz	512M	512M	0
AR208	Dual-core, 533 MHz	512 MB	512 MB	0
AR1220	Dual-core, 500 MHz	512 MB	256 MB	0
AR1220V	Dual-core, 500 MHz	512 MB	256 MB	0
AR1220W	Dual-core, 500 MHz	512 MB	256 MB	0
AR1220VW	Dual-core, 500 MHz	512 MB	256 MB	0
AR1220L	Dual-core, 500 MHz	512M	256M	0
AR2220	4-core 600 MHz	2 GB	16 MB	2 GB
AR2240	8-core 600 MHz	2 GB	16 MB	2 GB
AR3260	12-core 750 MHz	2 GB	16 MB	2 GB

7.2 Physical Specifications

Table 7-2 Physical specifications

Item	Description
Dimensions (H x W x D)	● Without rack-mounting ear – AR150 series: 44 mm x 300 mm x 216.4 mm (1.73in. x 11.81in. x 8.52in.) – AR200 series: 44 mm x 300 mm x 216.4 mm (1.73in. x 11.81in. x 8.52in.) – AR1200 series: 44.5mm x 390.0 mm x 220.0 mm (1.75in. x 15.35in. x 8.66in.) – AR2220: 44.5mm x 442.0 mm x 420.0 mm (1.75 in. x 17.4 in. x 16.54 in.) – AR2240: 88.1 mm x 442.0 mm x 470.0 mm (3.47 in. x 17.4 in. x 18.5 in.) – AR3260: 130.5 mm x 442.0 mm x 470.0 mm (5.14 in. x 17.4 in. x 18.5 in.) ● With rack-mounting ear – AR150 series: 44 mm x 482.6 mm x 216.4 mm (1.73in. x 19in. x 8.52in.) – AR200 series: (1.73in. x 19in. x 8.52in.) – AR1200 series: 44.5 mm x 482.6 mm x 220.0 mm (1.75 in. x 19 in. x 8.66 in.) – AR2220: 44.5 mm x 482.6 mm x 420.0 mm (1.75 in. x 19 in. x 16.54 in.) – AR2240: 88.1 mm x 482.6 mm x 470.0 mm (3.47 in. x 19 in. x 18.5 in.) – AR3260: 130.5 mm x 482.6 mm x 470.0 mm (5.14 in. x 19 in. x 18.5 in.)

Item		Description
Maximum power consumption (empty chassis)		● AR151: 11.6W ● AR157: 15.2W ● AR201: 12.3W ● AR206: 16W ● AR207: 16W ● AR207V: 22.8W ● AR207V-P: 23.5W ● AR208E: 14.6W ● AR207G-HSPA+7: 16.6W ● AR1200 series: 33.3 W ● AR2220: 65.1W ● AR2240: 114.9W ● AR3260: 163.2W
Weight	Full configuration	● AR150 and AR200 series: 2.20kg ● AR1200 series: 3.60 kg (7.94 lb) ● AR2220: 8.45 kg (18.63 lb) ● AR2240: 19.30 kg (42.56 lb) ● AR3260: 25.65 kg (56.56 lb)
	Empty chassis	● AR150 and AR200 series: 2.20kg ● AR1200 series: 2.90 kg (6.39 lb) ● AR2220: 4.95 kg (10.91 lb) ● AR2240: 8.85 kg (19.51 lb) ● AR3260: 11.00 kg (24.26 lb)
DC input voltage (AR2200 and AR3200 Series)	Rated voltage	-48 V DC to -60 V DC
	Voltage range	-38.4 V DC to -72 V DC
DC input voltage (AR150 and AR200 Series)	Rated voltage	12V DC
AC input voltage	Rated voltage	100 V AC to 240 V AC
	Voltage range	AR1200/AR2200/AR3200 series: 85 V AC to 264 V AC AR150/AR200 Series: 90 V AC to 264 V AC
Operating temperature		0 °C to 40 °C (0 °F to 104 °F)
Relative humidity		5% RH to 90% RH

Item		Description
Altitude	Long-term altitude	- AR1200/AR2200/AR3200 series: Lower than 4000 m (13123.2 ft.) - AR150/AR200 series: Lower than 3000 m (9842.4 ft.)
	Storage altitude	Lower than 4000 m (13123.2 ft.)

8 Component Selection Guide

About This Chapter

8.1 Router Purchase List

Table 8-1 Purchase list of AR150 series

Component	Typical Configuration	Remarks
AR151	Basic configuration of the AR151, including the AR151 assembly chassis, and basic software package	Mandatory
AR157	Basic configuration of the AR157, including the AR207 assembly chassis, and basic software package	Mandatory

Table 8-2 Purchase list of AR200 series

Component	Typical Configuration	Remarks
AR201	Basic configuration of the AR201, including the AR201 assembly chassis, and basic software package	Mandatory
AR206	Basic configuration of the AR206, including the AR206 assembly chassis, and basic software package	Mandatory
AR207	Basic configuration of the AR207, including the AR207 assembly chassis, and basic software package	Mandatory
AR207V	Basic configuration of the AR207V, including the AR207L assembly chassis, and basic software package	Mandatory
AR207V-P	Basic configuration of the AR207V-P, including the AR207V-P assembly chassis, 100 W PoE power supply adapter module, and basic software package	Mandatory
AR208E	Basic configuration of the AR208E, including the AR208E assembly chassis, and basic software package	Mandatory
AR207G-HSPA+7	Basic configuration of the AR207G-HSPA+7, including the AR207G-HSPA+7 assembly chassis, and basic software package	Mandatory
3G extended antenna	Omni antenna	Optional **NOTE** Only the AR207G-HSPA+7 can be configured with the Omni antenna.

Table 8-3 Purchase list of AR1200 series

Component	Typical Configuration	Remarks
AR1220	● Basic configuration of AR1220, including AR1220 assembly chassis, 60 W AC power supply unit in an open rack, and basic software package ● Basic configuration of AR1220-D, including AR1220 assembly chassis, 54 W DC power supply unit in an open rack, and basic software package	Mandatory
AR1220V	AR1220 with the voice function, including AR1220 assembly chassis, 32-channel digital signal processor (DSP), and basic software package	Mandatory
AR1220W	AR1220 with the WLAN functions, including AR1220 assembly chassis, 802.11b/g/n AP, and basic software package	Mandatory
AR1220VW	AR1220 with the voice and WLAN functions, including AR1220 assembly chassis, 16-channel DSP, 802.11b/g/n AP, and basic software package	Mandatory
AR1220L	Basic configuration of AR1220L, including AR1220L assembly chassis and basic software package	Mandatory
PoE power supply unit	100 W PoE power supply adapter module	Optional **NOTE** Only applied to AR1220V, AR1220VW, and AR1220W.

Table 8-4 Purchase list of AR2220

Component	Typical Configuration	Remarks
AR2220	Basic configuration of AR2220 with AC power, including AR2220 assembly chassis, 150 W AC power supply, and basic software package Basic configuration of AR2220 with DC power, including AR2220 assembly chassis, 150 W DC power supply, and basic software package	Mandatory
DSP module	16/32/64/128-channel voice DSP module	Optional

Table 8-5 Purchase list of AR2240

Component	Typical Configuration	Remarks
AR2240	● Basic configuration of AR2240 with standard main control board and AC power supply, including AR2240 assembly chassis, 350 W AC power supply, standard main control board, and basic software package ● Basic configuration of AR2240 with standard main control board and DC power supply, including AR2240 assembly chassis, 350 W DC power supply, standard main control board, and basic software package ● Basic configuration of AR2240 with enhanced main control board and AC power supply, including AR2240 assembly chassis, 350 W AC power supply, enhanced main control board, and basic software package ● Basic configuration of AR2240 with enhanced main control board and DC power supply, including AR2240 assembly chassis, 350 W DC power supply, standard main control board, and basic software package	Mandatory
Fan	AR2240 Fan module	Mandatory
AC power supply unit	350 W AC power supply unit	Optional. By default, a router has one AC power supply unit. To perform load balancing, two AC power supply units can be installed.
DC power supply unit	350 W DC power supply unit	Optional. By default, a DC router has one DC power supply unit. To perform load balancing, two DC power supply units can be installed.
DSP module	16/32/64/128-channel voice DSP module	Optional

Table 8-6 Purchase list of AR3260

Component	Typical Configuration	Remarks
AR3260	● Basic configuration of AR3260 with enhanced main control board and AC power supply, including AR3260 assembly chassis, 350 W AC power supply, enhanced main control board, and basic software package ● Basic configuration of AR3260 with standard main control board and AC power supply, including AR3260 assembly chassis, 350 W AC power supply, standard main control board, and basic software package ● Basic configuration of AR3260 with standard main control board and DC power supply, including AR3260 assembly chassis, 350 W DC power supply, standard main control board, and basic software package ● Basic configuration of AR3260 with enhanced main control board and DC power supply, including AR3260 assembly chassis, 350 W DC power supply, enhanced main control board, and basic software package	Mandatory
Fan	AR3260 fan module	Mandatory
AC power supply unit	350 W AC power supply unit	Optional. By default, an AC router has one AC power supply unit. To perform load balancing, two AC power supply units can be installed.
DC power supply unit	350 W DC power supply unit	Optional. By default, a DC router has one DC power supply unit. To perform load balancing, two DC power supply units can be installed.
DSP module	16/32/64/128-channel voice DSP module	Optional

8.2 Board Purchase List

NOTE

An AR150 router or AR200 router has no slot; therefore, you do not need to purchase the following boards for the AR200.

Table 8-7 Board purchase list

Silkscreen	Description
8FE1GE	9-port 8FE/1GE L2/L3 Ethernet interface card
24GE	24-port GE L2/L3 Ethernet interface card
1GEC	1-port GE combo WAN interface card
2FE	2-port FE WAN interface card
4GEW-T	4-port GE optical port WAN interface card
4GEW-S	4-port GE electrical port WAN interface card
1E1/T1-M	1-port channelized E1/PRI/VE1; MFT: Multiflex Trunk
1E1/T1-F	1-port unchannelized E1/unstructure E1/fractional E1,120 ohm WAN interface card
2E1/T1-F	2-port unchannelized E1/unstructure E1/fractional E1,120 ohm WAN interface card
2E1/T1-M	2-port channelized E1/PRI/VE1; MFT: Multiflex Trunk, including SIC and WSIC
1SA	1-port sync/async serial WAN interface card
2SA	2-port sync/async serial WAN interface card
8AS	8-port async serial WAN interface card, including WSIC and XSIC
1BST	1-port ISDN S/T WAN interface card
2BST	2-port ISDN S/T voice interface card, including SIC and WSIC
4FXS1FXO	5-port 4FXS/1FXO voice interface card
1ADSL-A/M	1-port ADSL2+ annex A/M WAN interface card
1ADSL-B	1-port ADSL2+ annex B WAN interface card
VDSL	1-port VDSL2 over POTS WAN interface card
4G.SHDSL	4-pair G.SHDSL WAN interface card

Silkscreen	Description
1CPOS-155M	1-Port Channelized Packet over SDH/Sonet interface card **NOTE** The AR1200 does not support 1CPOS-155M.
1PON	1-port-xPON WAN interface card
3G-HSPA+7	3G WAN interface card
-	16/32/64/128-channel DSP module