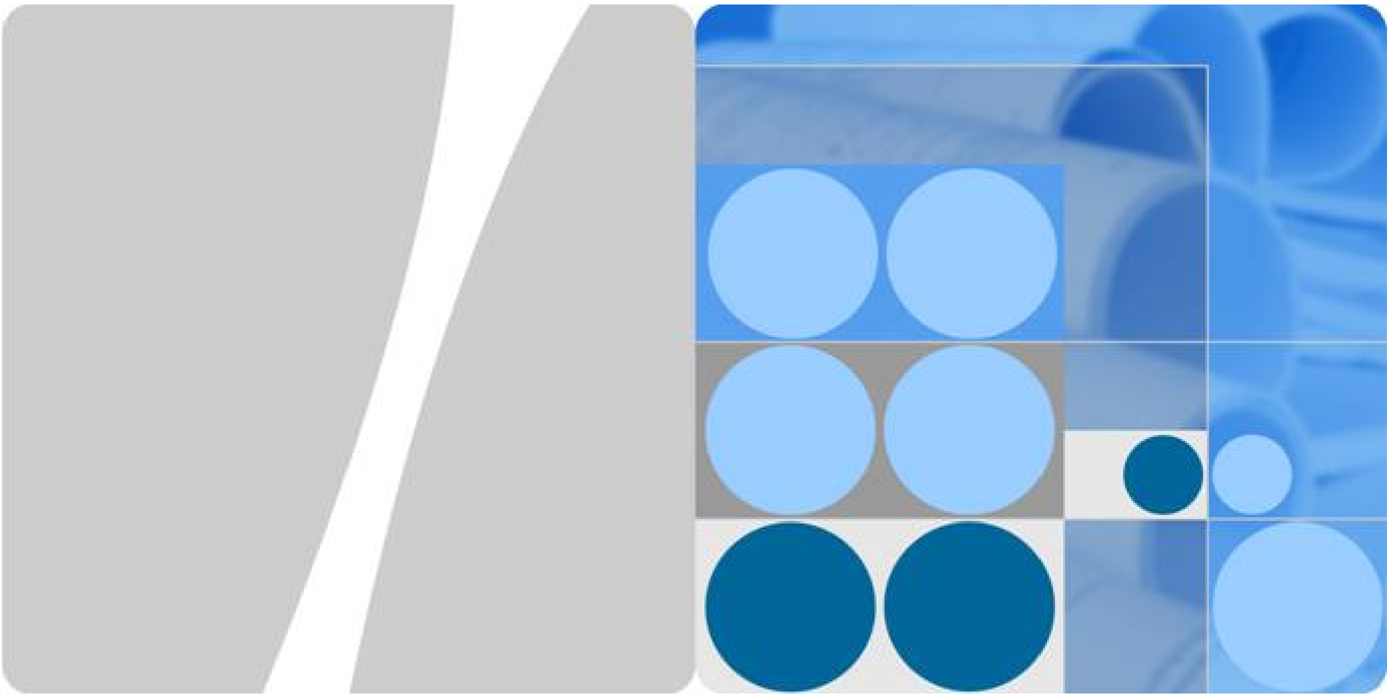


NetEngine AR

Product Description

Issue	**01**
Date	**2020-03-20**

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2020. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

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 a 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: https://e.huawei.com

About This Document

Intended Audience

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	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
⚠ CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.

Symbol	Description
🕮 NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Security Conventions

- Password setting
  - When configuring a password, the cipher text is recommended. To ensure device security, change the password periodically.
  - When you configure a password in plain text that starts and ends with %@%@, @%@%, %#%#, or %^%# (the password can be decrypted by the device), the password is displayed in the same manner as the configured one in the configuration file. Do not use this setting.
  - When you configure a password in cipher text, different features cannot use the same cipher-text password. For example, the cipher-text password set for the AAA feature cannot be used for other features.
- Encryption algorithm

  Currently, the device uses the following encryption algorithms: 3DES, AES, RSA, SHA1, SHA2, and MD5. 3DES, RSA and AES are reversible, while SHA1, SHA2, and MD5 are irreversible. The encryption algorithms DES, 3DES, RSA (RSA-1024 or lower), MD5 (in digital signature scenarios and password encryption), and SHA1 (in digital signature scenarios) have a low security, which may bring security risks. If protocols allowed, using more secure encryption algorithms, such as AES, RSA (RSA-2048 or higher), SHA2, and HMAC-SHA2, is recommended. The encryption algorithm depends on actual networking. The irreversible encryption algorithm must be used for the administrator password, SHA2 is recommended.
- Personal data

  Some personal data (such as MAC or IP addresses of terminals) may be obtained or used during operation or fault location of your purchased products, services, features, so you have an obligation to make privacy policies and take measures according to the applicable law of the country to protect personal data.
- The terms mirrored port, port mirroring, traffic mirroring, and mirroring in this manual are mentioned only to describe the product's function of communication error or failure detection, and do not involve collection or processing of any personal information or communication data of users.

Declaration

- This manual is only a reference for you to configure your devices. The contents in the manual, such as web pages, command line syntax, and command outputs, are based on the device conditions in the lab. The manual provides instructions for general scenarios, but do not cover all usage scenarios of all product models. The contents in the manual may be different from your actual device situations due to the differences in software versions, models, and configuration files. The manual will not list every possible difference. You should configure your devices according to actual situations.

- The specifications provided in this manual are tested in lab environment (for example, the tested device has been installed with a certain type of boards or only one protocol is run on the device). Results may differ from the listed specifications when you attempt to obtain the maximum values with multiple functions enabled on the device.
- In this document, public IP addresses may be used in feature introduction and configuration examples and are for reference only unless otherwise specified.
- In this document, NetEngine access routers include AR600&AR1600&AR6000&AR6000-S Series.

Change History

Changes between document issues are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Changes in Issue 01 (2020-03-20)

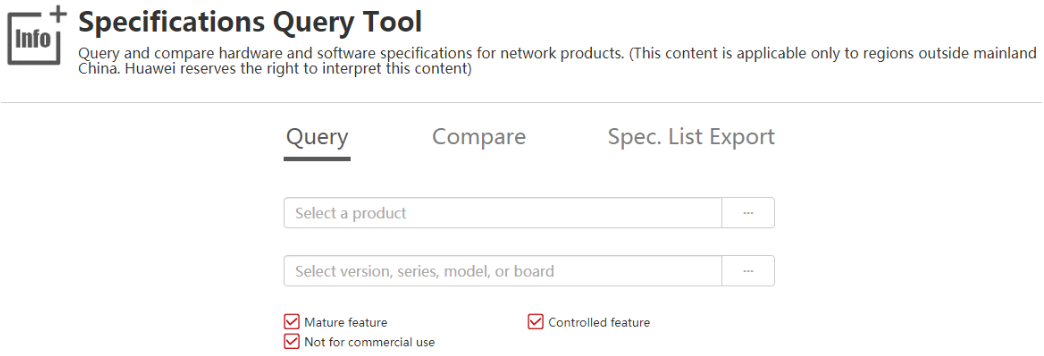
Initial commercial release.

Contents

1 Using the Specifications Query Tool to Query Product Specifications

Figure1 shows the interface of the **Specifications Query Tool**. You can use this tool to query and compare hardware and software specifications for network products, information can be quickly retrieved based on conditions such as product, version, model, and board, or keywords.

Figure 1-1 Web page of the Specifications Query Tool



Specifications Query Tool

Query and compare hardware and software specifications for network products. (This content is applicable only to regions outside mainland China. Huawei reserves the right to interpret this content)

Select a product ···

Select version, series, model, or board ···

☑ Mature feature ☑ Controlled feature

☑ Not for commercial use

2 Product Characteristics

Huawei's NetEngine AR series routers (AR for short) are the next-generation routing and gateway devices, which provide the SD-WAN, routing, switching, VPN, security, voice, and MPLS functions. AR include AR600, AR6000, and AR6000-S series routers.

Carrier-Class Reliability

- The ARs provide hot swappable interface cards, standby SRU, power module, fan module, and optical module, ensuring 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 ARs support redundant power supply units. If one power supply unit is faulty, the device will still be able to operate.
- The ARs provide dual SRUs in redundancy mode. When a fault occurs on the control, forwarding, or switching plane, services can be smoothly switched to the standby SRU.

Service Integration Capability

The ARs integrate various services of routers, switches, and wireless devices, including voice, firewall, WLAN, 3G/LTE, and VPN.

Hardware Extensibility

The ARs provide the highest port density in the industry and flexible slot combination, 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 SIC slots and one WSIC slot below can be combined into one XSIC slot by removing guide rails, and two multiple-function slots (MFSs) can be combined into an SRU slots by removing the guide rail between them.

Remote Maintenance Capability

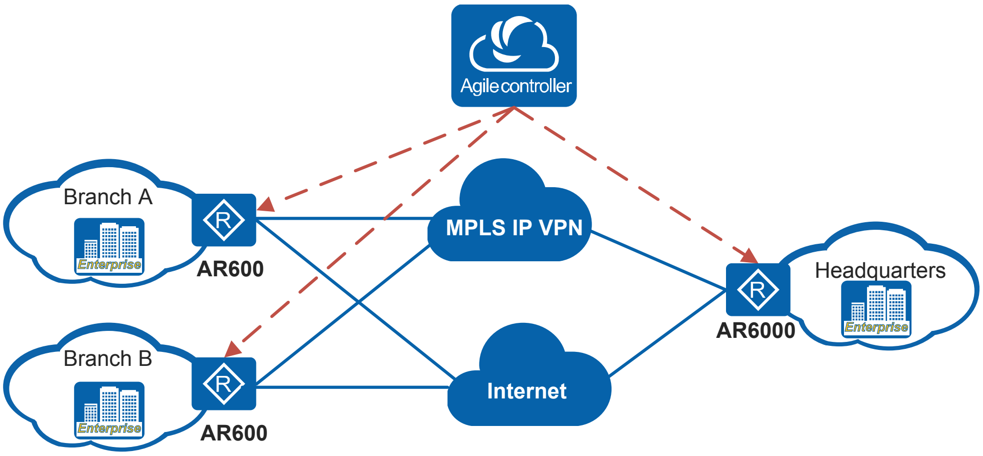
In addition to one-stop deployment, plug and play capability, and remote commissioning functions, the ARs manage the customer premises equipment (CPE) remotely. The remote maintenance function improves efficiency and greatly reduces maintenance costs.

3 Usage Scenarios

3.1 Interconnection Between Branches in the SD-WAN Solution

As shown in **Figure1**, In the SD-WAN solution, the AR600&AR6000 functions as the edge or aggregation gateway and supports multiple types of physical links, such as MPLS leased line, Internet, and LTE. The AR600&AR6000 integrates various SD-WAN features, supports hybrid link access, and provides visualized and controllable services. This reduces WAN interconnection costs and improves O&M efficiency.

Figure 3-1 Interconnection between branches in the SD-WAN solution



3.2 WAN Access

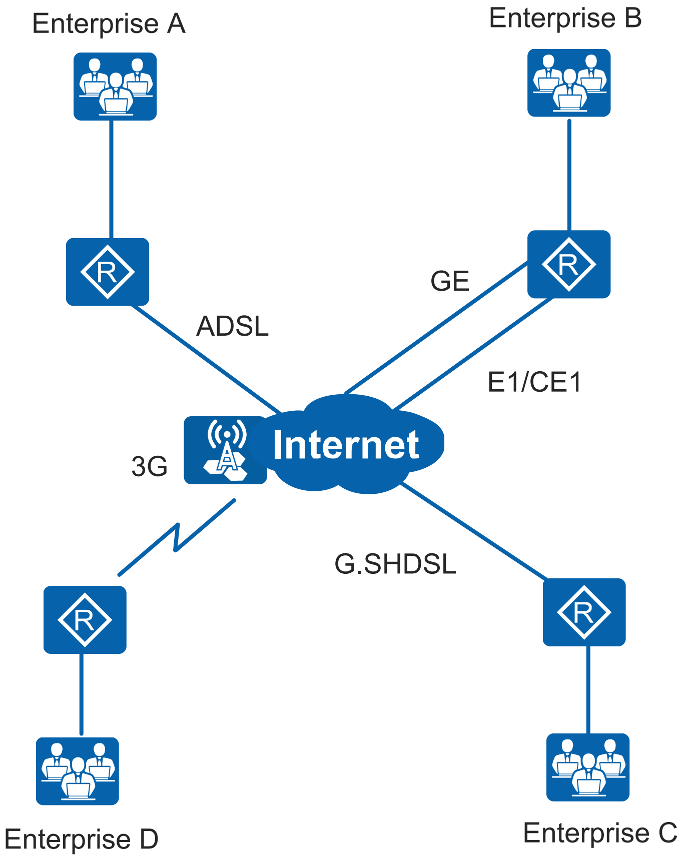
Depending on the network environment provided by carriers, users can access the network by using interfaces including GE interfaces, synchronous/asynchronous serial interface, Async interface, CE1/CT1 PRI interfaces, E1-F interfaces, T1-F interfaces, 3G/LTE cellular interfaces, Integrated Services Digital Network BRI interfaces, PoS interfaces, CPoS interfaces, ADSL interfaces, VDSL interfaces, G.SHDSL interfaces, E1-IMA interfaces, CE3 interfaces, E&M interfaces, and xPON interfaces. The router provides dual uplinks to implement interface backup and ensure service reliability.

NOTE

WAN interfaces depend on the device model and the boards installed.

As shown in **Figure1**, enterprise A accesses the Internet using ADSL; enterprise B accesses the Internet using GE and E1/CE1 dual-uplink (E1/CE1 link functions as the backup link of the GE link); enterprise C accesses the Internet using G.SHDSL; enterprise D accesses the Internet using 3G. This setting achieves WAN interconnection.

Figure 3-2 WAN access

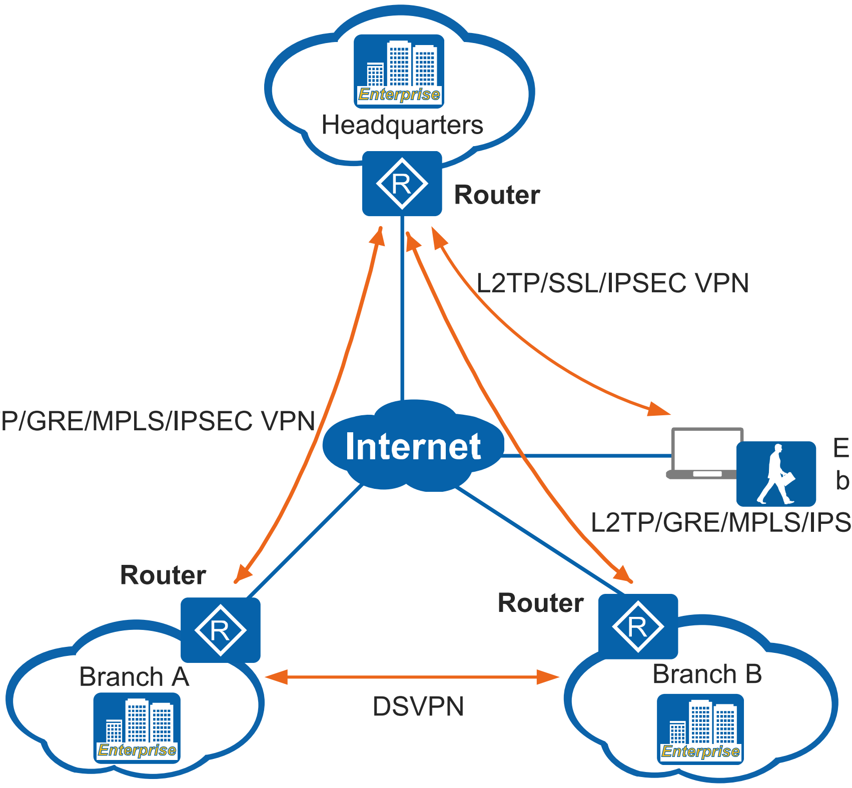


3.3 VPN Access

The headquarters and branches use the Router to connect to the Internet, establish a VPN, and use VPN tunnels to secure data.

As shown in **Figure1**, the headquarters is connected to the Internet through the Router. LANs of branches connect to the Internet through the Router. The headquarters and branches use L2TP/GRE/MPLS/IPSec VPN tunnels, and the headquarters and traveling employees use L2TP/SSL/IPSec VPN tunnels to secure data. After branches and headquarters establish VPN tunnels, branches can communicate with each other through the headquarters. You can also deploy DSVPN to dynamically establish tunnels between branches. This method improves forwarding performance and efficiency, and reduces resource usage of the headquarters.

Figure 3-3 VPN access



3.4 Application of Enterprise Intranet Security

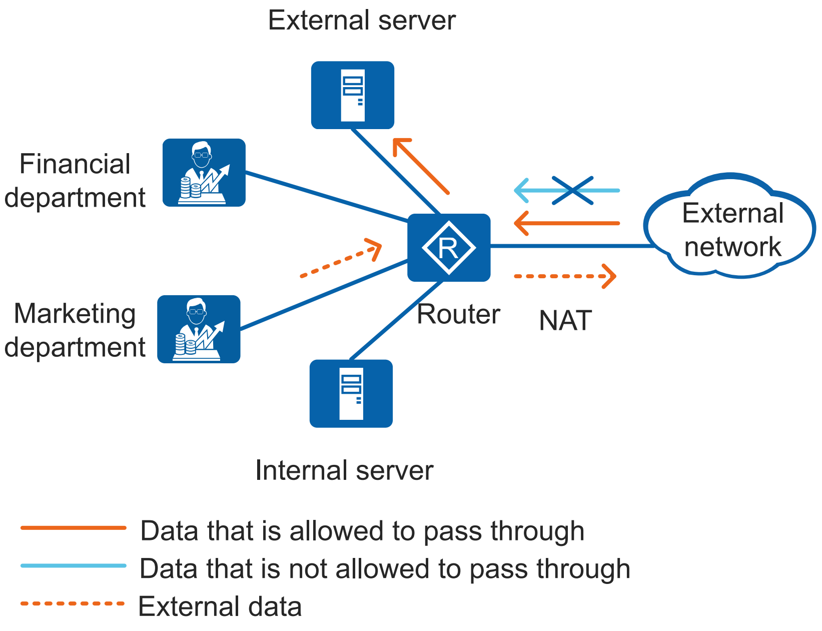
The router located between the enterprise intranet and external networks, ensures information security on the entire intranet and intranet LANs.

As shown in **Figure1**, the enterprise intranet is connected to the external network through the Router. The router can prevent external users from accessing the enterprise intranet. For example, external users can access the enterprise external server but cannot access the enterprise internal server. The financial department and marketing department have individual LANs on the intranet. To allow the users on the intranet to access the external network, configure network address translation (NAT) on the intranet.

The router ensures information security on the enterprise intranet in the following modes:

- Enabling packet filtering or stateful firewall on the Router to isolate the enterprise intranet from external networks. This prevents unauthorized external users from accessing the intranet.
- The router provides network access control (NAC) to restrict the access permissions of internal users. This ensures that only authorized users can access the intranet.
- IPS defends against attacks, provides secure environments for enterprise networks, and accurately manages network resources.

Figure 3-4 Application of enterprise intranet security



3.5 Voice Application

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

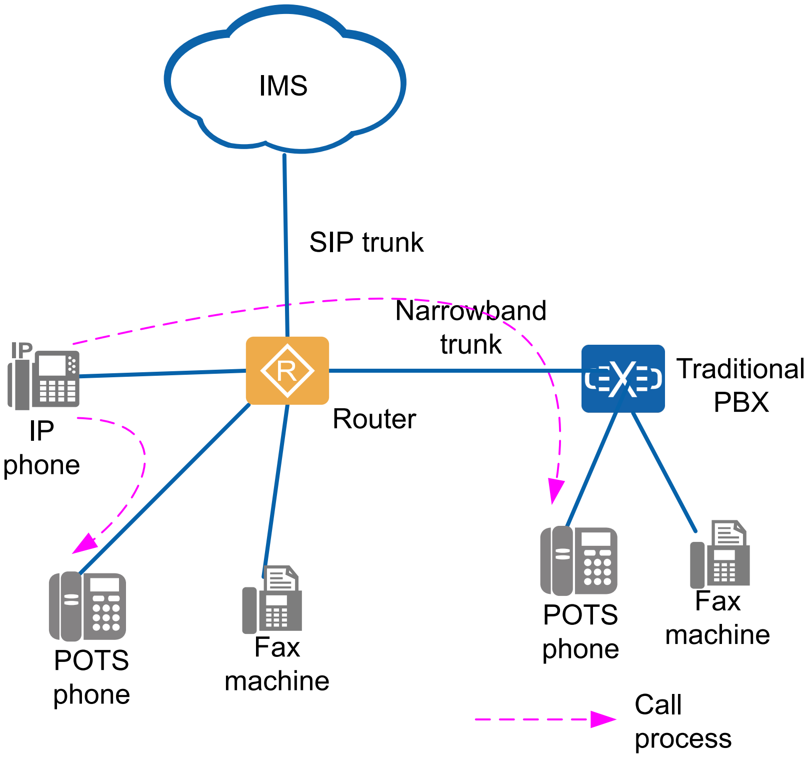
The AR can function as the private branch exchange (PBX) or access gateway (AG) to meet different service requirements.

AR Used as the PBX

A PBX can connect to the Public Switched Telephone Network (PSTN). A traditional PBX is a voice program control switch of an enterprise and provides exchange between phones inside an enterprise or between an enterprise and the PSTN. It implements unified management of incoming and outgoing calls, and integrates functions of phones, fax machines, and modems. As communication technologies develop, the traditional PBX lacks of support for integration with computer telecommunication and VoIP technologies, and openness and standardization. In addition, the communication cost is high. IP PBXs are used to prevent the preceding problems. They integrate voice communication into enterprise data networks so that an integrated voice and data network is established to connect offices and employees around the world.

The AR can function as an IP PBX or a traditional PBX. It can also function as the integrated voice platform to provide specialized voice services.

Figure 3-5 AR used as the PBX



The AR is the core switching gateway that integrates functions such as number management, service control, and media conversion. It provides open interfaces to connect to traditional PBXs and access gateways to allow flexible networking.

The device supports the following trunks:

- SIP (SIP IP, SIP PRA, SIP AT0)

- PRA
- QSIG
- R2
- AT0
- BRA
- H.323

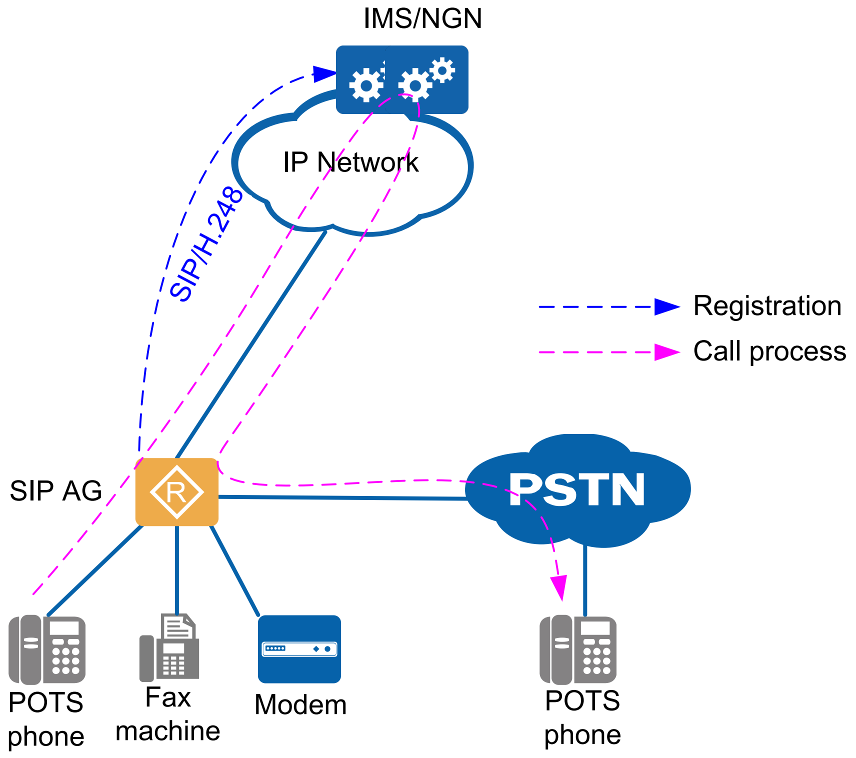
AR Used as the AG

An AG connects the PSTN to the IP multimedia system (IMS). It can implement conversion between analog and digital signals.

The traditional PSTN uses line switching technology and exclusive lines, and faces problems such as low resource use efficiency and high costs of inter-area communication. As VoIP develops, the IP bearer network solves the preceding problems. The traditional PSTN has been developing for many years and there are many existing devices on the traditional PSTN. Replacing the traditional PSTN with the IP network requires a high cost. Using IP-based AGs can implement integration of the traditional PSTN and data network and smooth evolution of network reconstruction.

The AR can function as the AG and use SIP to connect to the IMS or NGN through the IP bearer network or use H.248 to connect to the MGC. The AGs in the preceding two scenarios are called SIP AG and H.248 AG, respectively.

Figure 3-6 AR used as the AG

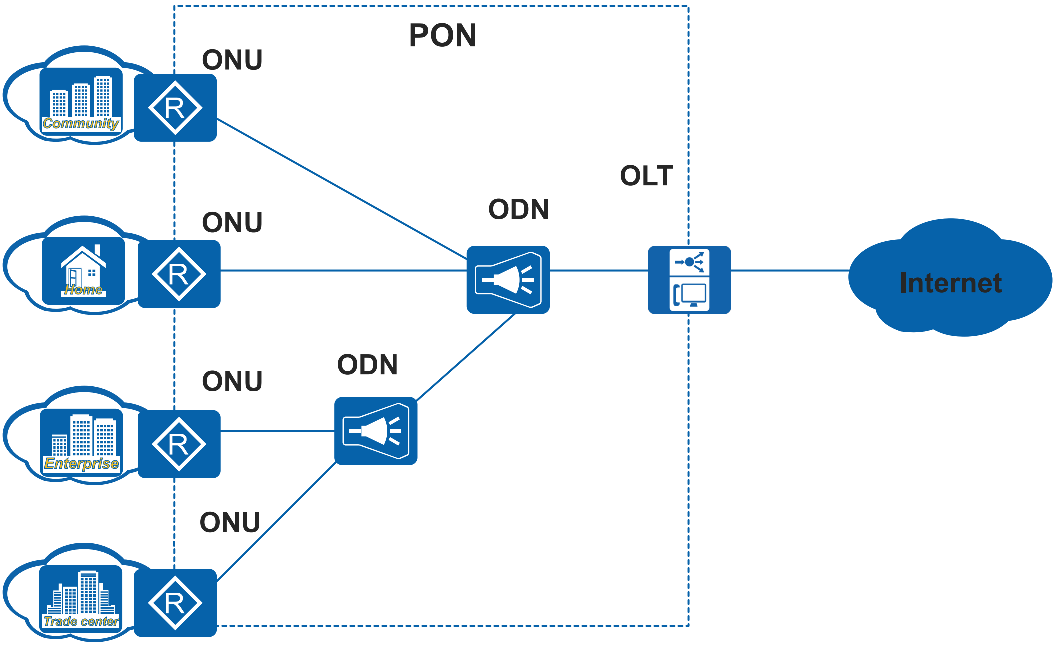


3.6 FTTx

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 **Figure1**, 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 3-7 FTTx

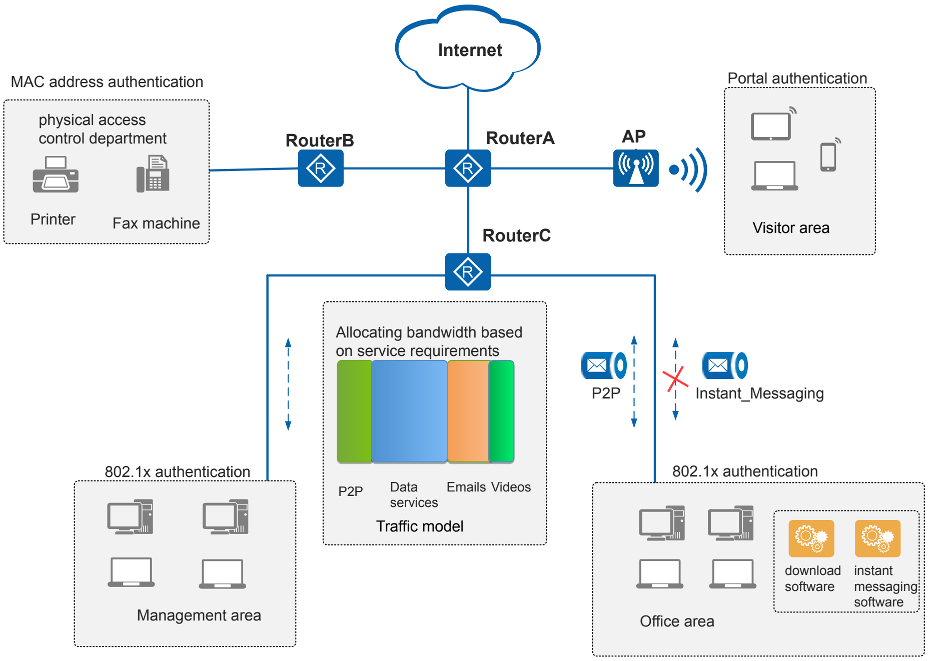


3.7 Online Behavior Management

With the emergence of new applications and behavior on networks, enterprise network administrators need to standardize online behavior of users in complex network environment. Router supports online behavior management, including various access authentication and application control methods, to prevent unauthorized users from accessing the network and prevent employees from performing non-work-related operations. This function improves bandwidth use efficiency.

In **Figure1**, an enterprise network is connected to the Internet through Router A, which functions as the gateway. The physical access control department is connected to Router A through Router B, the office and management areas are connected to Router A through Router C, and the guest area is connected to Router A through APs. To ensure security of the enterprise intranet, user access needs to be controlled. Only the users who are successfully authenticated can access authorized network resources. To standardize online behavior and improve work efficiency, the instant messaging software and download software such as BT and eDonkey_eMule must be forbidden in the office area. In addition, bandwidth needs to be properly allocated to different services to ensure the key services. When congestion occurs, the management area needs higher bandwidth.

Figure 3-8 Online behavior management



User Access and Authentication

To protect security of the entire enterprise network, router integrates terminal security and access control and takes the check, isolation, security hardening, and audit measures. These measures improve the proactive protection capability of terminals.

The router provides different authentication methods for different scenarios:

- 802.1x: based on port and MAC address. This method is applicable to new networks that have high-density users and information confidentiality requirement.
- MAC address: based on MAC address of users. This method is applicable to dumb terminals such as printers and fax machine.
- Portal: through portal authentication website. This method is applicable to networks with scattered, moving users.

router provides authentication for the following users:

- Authenticates static users based on user IP address.
- Assigns priorities and VLAN IDs to user groups so that users in different groups have different priorities and network access rights.

For details about the preceding functions, see NAC Configuration.

Application-based Management

To prevent employees from accessing non-work-related websites, the network administrator needs to control the applications used by online employees. The router supports Smart Application Control (SAC), which intelligent classifies applications and enforces policies to different application categories. For example, SAC can prohibit the non-work-related applications such as QQ to standardize user online behavior and improve work efficiency. For details about SAC, see SAC Configuration.

Bandwidth Management

To improve network use efficiency, enterprise administrators need to allocate different bandwidth to different service flows, for example, sufficient bandwidth for key services and restricted bandwidth for common services.

router supports multi-dimension bandwidth management:

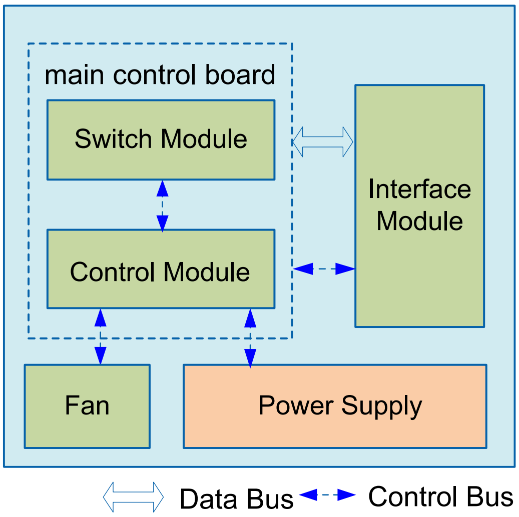
- Based on interface: control inbound and outbound traffic rate on an interface.
- Based on service type: restrict bandwidth for a certain type of service.
- Based on IP address: restrict bandwidth for a certain IP address.
- Based on user group: restrict bandwidth for the user group matching certain conditions.
- Based on multi-level queue: restrict bandwidth for a certain type of service and user.

For details about bandwidth management, see Traffic Policing and Traffic Shaping Configurations, Bandwidth Management Configuration, and Configuring HQoS.

4 Hardware Information

Figure1 shows the logical structure of hardware modules in the router. Hardware modules of the router refer to the Service and Router Unit (SRU), power supply, fan, and card.

Figure 4-1 Logical structure of hardware modules



SRU

The SRU integrates the switching module and control module and provides the following functions:

- Processes protocol packets.
- Manages the system and monitors the system performance according to instructions of the user, and reports the device running status to the user.
- Monitors and maintains the switching module and control module.

Power Supply

The power supply powers the router. For details about power supply configurations for the router, see the Power Supplies section in the *Hardware Description*.

Fan Module

The fan module dissipates heat for the router. Cold air flows into the router from the left side and is exhausted from the right side, taking away heat generated by the router. This ensures that the router works in the operating temperature range.

For details about fan modules in different models, see "Heat dissipation" under Chassis in the *Hardware Description*.

Card

The router supports multiple types of service cards, these cards improve networking flexibility and meet customers' requirements for cost-effective and personalized solutions.

For details, see Cards in the *Hardware Description*.

5 Performance Specifications

The features mentioned in the "Product Characteristics", and "Usage Scenarios" sections are not supported on all models.

For the features and specifications supported by different product models, download their brochures or specification lists from **Huawei official website**. (If your account is unauthorized, contact Huawei local office.)