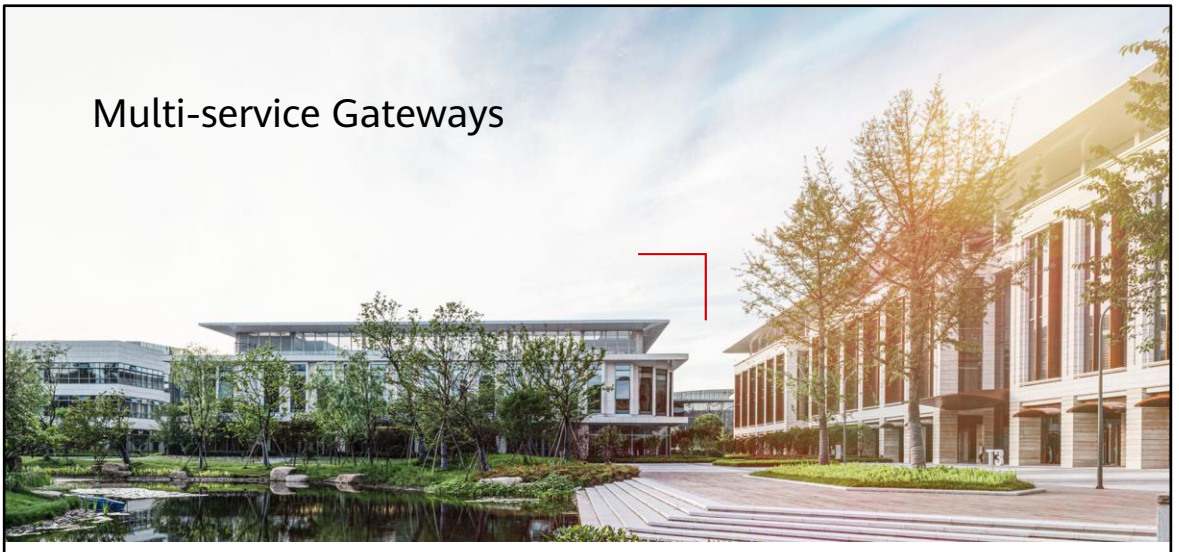
Multi-service Gateways



Foreword

- Next-generation AR routers apply to different industries, network scales, and scenarios.
- AR routers use leading hardware platforms and software architectures. They provide integrated network solutions to enterprise customers with the minimum investment; therefore, they can meet various application requirements of future business expansion and cope with IT industry development.
- This course describes WLAN and security functions of AR routers.

Objectives

- Upon completion of this course, you will be able to:
  - Describe functions and features supported by AR routers.
  - Describe WLAN service features of AR routers.
  - Describe security service features of AR routers.

Contents

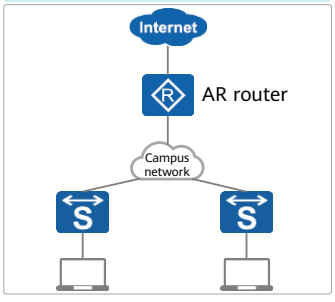
Overview of AR Routers

- AR routers are mainly oriented to enterprise users. As enterprise gateways, AR routers provide all-in-one advantages.
- AR routers provide routing, switching, security, voice, and WLAN functions, reducing initial investment of enterprise users.

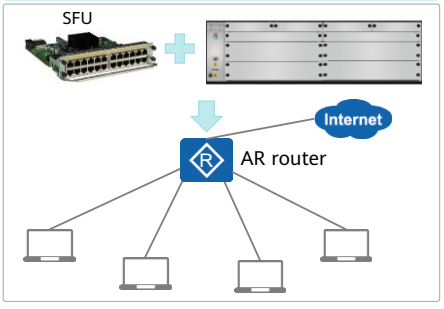
Introduction to Routing and Switching Features

- The AR router can function as the egress router of a medium-sized network. It supports multiple router protocols, MPLS, multicast routing protocols, and WAN interconnection.
- On a small-scale network, an AR router also provides the switching function. For example, after a switching card is installed on an AR router, the AR router can function as a switch and supports multiple Layer 2 technologies such as Virtual Local Area Network (VLAN) and Spanning Tree Protocol (STP).

Usage scenario of routing features

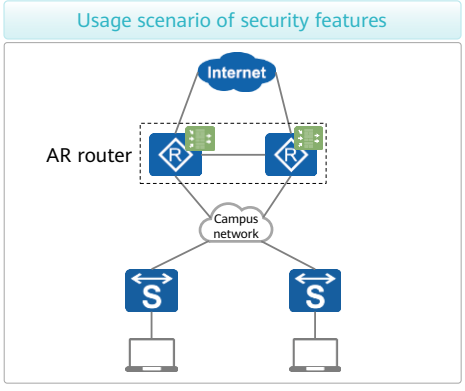


Usage scenario of switching features



Introduction to Security Features

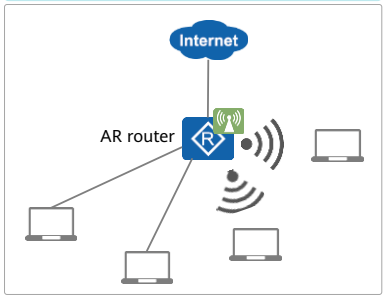
- AR routers provide access security features, such as port security and access authentication. They support network security features, such as firewall, IPS, and URL filtering. In firewall hot standby scenarios, AR routers also support firewall hot standby.



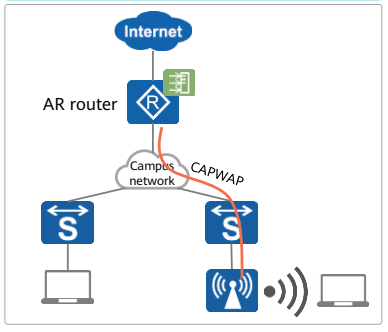
Introduction to WLAN Features

- The AR router supports two working modes: Fat access point (AP) and access controller (AC). The working mode varies according to the usage scenario.
  - An AR router functions as a Fat AP and independently provides WLAN access for stations (STAs).
  - An AR router functions as an AC and provides access to downlink Fit APs. The AR router and Fit APs together provide WLAN access for STAs.

Usage scenario of a Fat AP



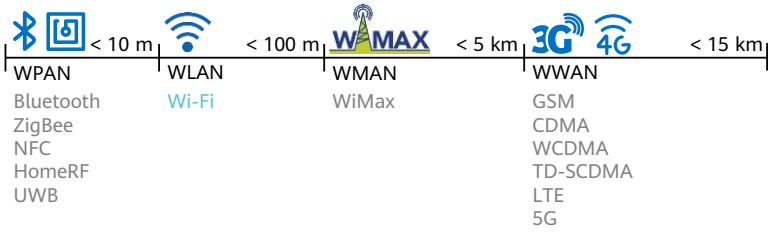
Usage scenario of AC+Fit AP



Contents

Introduction to WLAN Technology

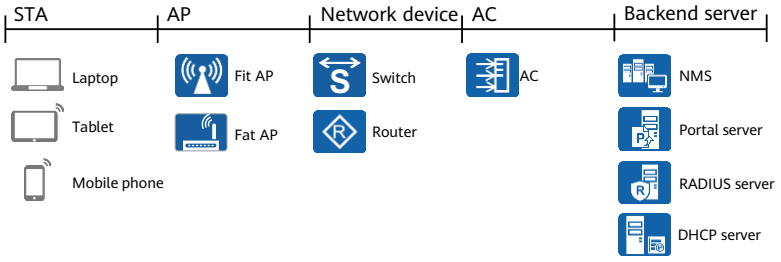
- With rapid development of the Internet, the communication network has developed from the traditional cabling network to the wireless network. As one of the wireless networks, the Wireless Local Area Network (WLAN) meets people's demands of mobile office.
- Wireless networks can be classified into the Wireless Personal Area Network (WPAN), WLAN, Wireless Metro Area Network (WMAN), and Wireless Wide Area Network (WWAN) based on the application scope. WLAN technology is also known as Wi-Fi.



- WLAN classification:
  - WPAN
  - WLAN
  - WMAN
  - WWAN

Introduction to WLAN Devices

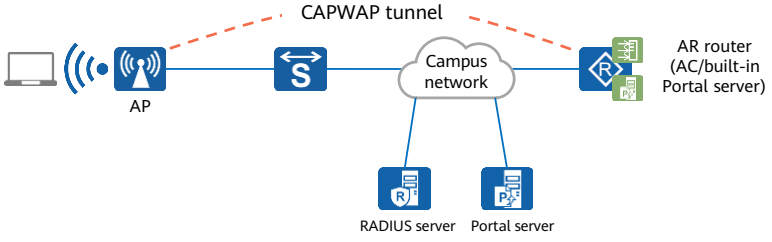
- A WLAN consists of STAs, APs, ACs, network devices, and backend servers.
  - The AP and AC are main devices on the WLAN and are used to control and send wireless signals.
  - Backend servers are used for authentication, IP address distribution, and network monitoring.
  - Network devices are used to forward STA data.
  - The STA is a wireless terminal.



- STA
  - STAs refer to access terminals, including laptops, desktop computers with wireless NICs installed, mobile phones, and PDA.
- AP
  - APs are main devices of the WLAN and key components for wireless technologies. They provide wired connections to upstream devices and wireless access to STAs, bridging the wired and wireless networks.
  - Fat APs are traditional APs. In addition to wireless access, a Fat AP provides security, management, and performance enhancement functions. A Fat AP cannot associate with an AC.
  - Different from traditional Fat APs, Fit APs provide only reliable and high-performance wireless connections. Fit APs must work with ACs.
- AC
  - An AC controls and manages all APs on a WLAN. It can exchange with an authentication server to authenticate WLAN users.

AR Router - NAC

- An AR router provides Wi-Fi access authentication through the built-in network admission control (NAC) feature.
- NAC provides three authentication modes: 802.1X authentication, MAC address authentication, and Portal authentication. NAC needs to be used with the AAA server to implement access authentication.
- An AR router provides 802.1X authentication, MAC address authentication, and Portal authentication. Portal authentication can be implemented by an external or internal Portal server.

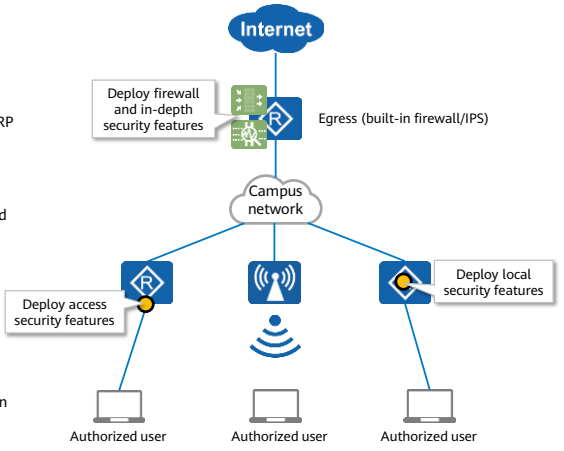


- AAA servers include the RADIUS server, TACACS server, and accounting server.

Contents

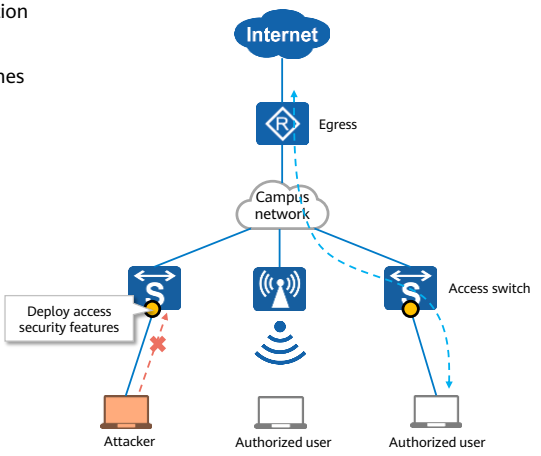
AR Security Features

- All AR series routers support security features.
- AR routers support the following security features:
  - Access security
    - Common access security technologies include NAC, port security, ARP security, traffic suppression, and IP source guard (IPSG).
  - Local security features
    - Common local security technologies include CPU attack defense and attack source tracing.
  - Firewall features
    - Common firewall technologies include packet filtering, stateful firewall, and blacklist and whitelist.
  - In-depth security defense
    - Common in-depth security technologies include intrusion prevention system (IPS) and URL filtering.



Access Security Features

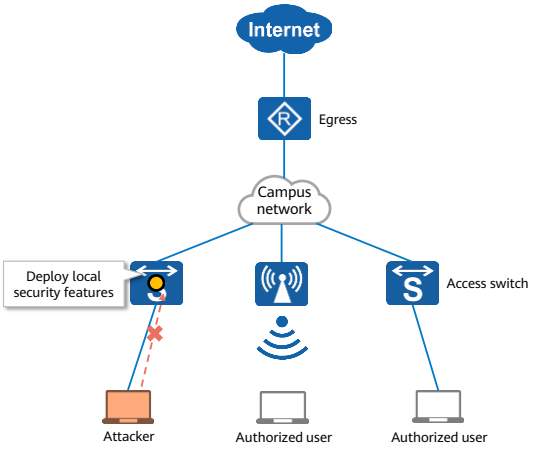
- The network has become an important tool for information exchange. The cyber security issue needs to be resolved urgently with the wide use of network. The access switches that play an important role on the network are prone to hackers' attacks.
- Access security involves the following:
  - Confidentiality
  - Integrity
  - Availability
- Common access security technologies are as follows:
  - NAC, port security, ARP security, traffic suppression, and IPSG



- Confidentiality: When a switch stores, handles, and transmits data, the data will not be leaked to unauthorized users, entities, or procedures. Information can only be accessed by authorized users.
- Integrity: Data cannot be modified without permission. Information stored or transmitted by switches is free from corruption or loss caused by accidental or malicious deletion, modification, falsification, disordering, relocation, or insertion.
- Availability: The given functions of a switch can be executed under the specified conditions and at the specified time or time period when the required external resources are ensured. Services are always available and meet carrier-class QoS requirements.

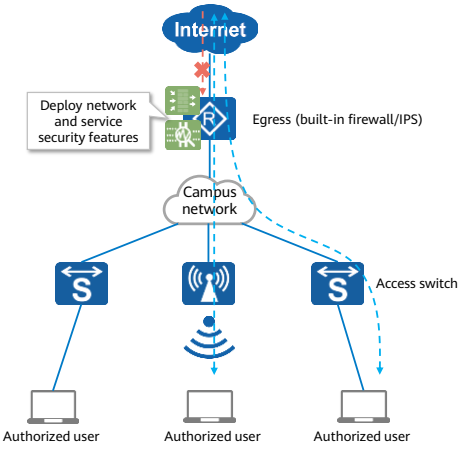
Introduction to Local Security Features

- Device CPUs need to process a large number of packets including valid packets and malicious attack packets on a network.
- To ensure that the CPU can properly process and respond to normal services, the device provides the local attack defense function.
- Common local security technologies are as follows:
  - CPU attack defense and attack source tracing



Introduction to Firewall and In-Depth Security Defense Features

- Access security features are used to protect the internal network and focus more on validity of access devices or users.
- Firewall and in-depth security defense features focus more on validity of traffic between the intranet and extranet and validity of services carried over the traffic.
- Common firewall and in-depth security defense technologies are as follows:
  - Firewall and connection control technology
  - IPS
  - URL filtering
  - Attack defense



Quiz

1. (True or false) AR routers can be used as Fat APs or Fit APs.

   A. True

   B. False

2. (True or false) AR routers can be used as firewalls, but do not support firewall hot standby.

   A. True

   B. False

- 1. B
- 2. B

Summary

- AR routers provide routing, switching, security, voice, and WLAN functions.
  - Routing and switching functions: It has similar functions of a Huawei switch.
  - Security functions: It provides similar functions of a firewall, such as IPS and URL filtering.
  - WLAN function: It can be used as a Fat AP or an AC.
  - Voice capability: It can be used as an IP PBX or SIP AG.