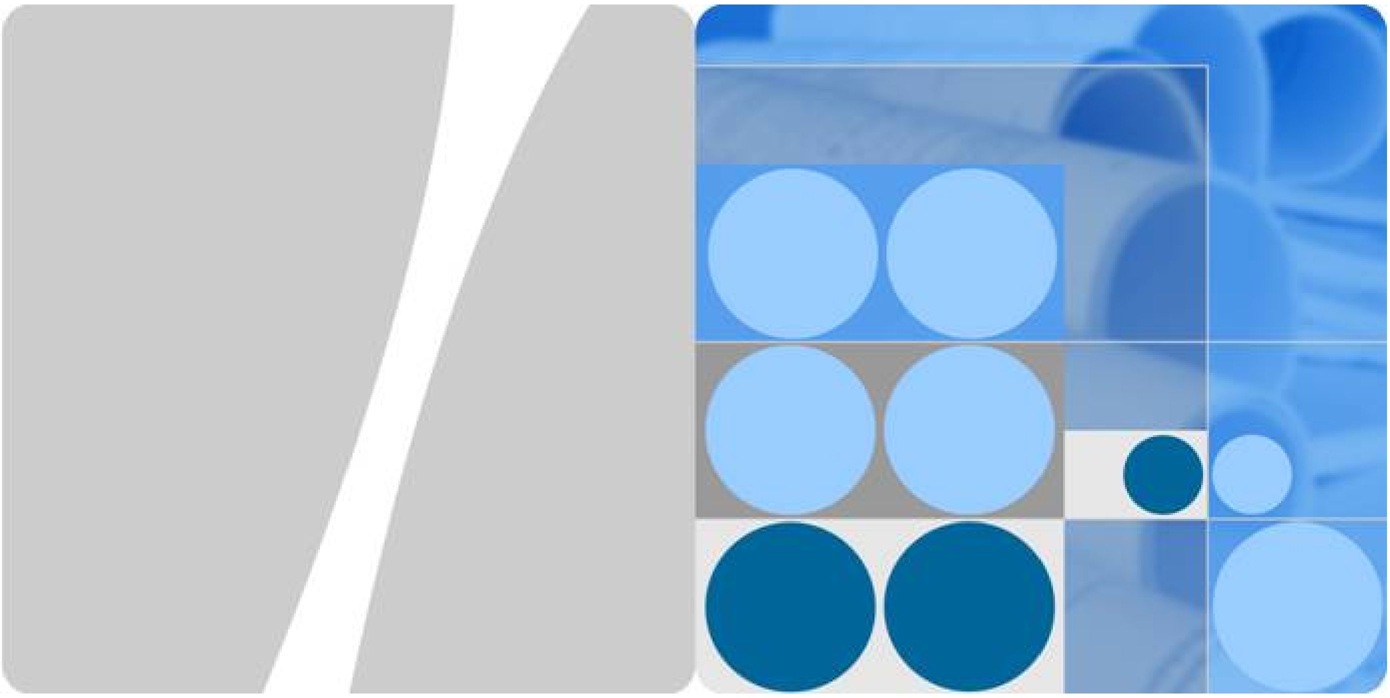


Centralized authentication and local forwarding

Technical White Paper

Issue	**01**
Date	**2012-10-31**

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 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: http://enterprise.huawei.com

About This Document

Change History

Changes between document issues are cumulative. The latest document issue contains all changes made in previous issues.

Changes in Issue 01 (2012-10-31)

Initial commercial release.

Contents

1 Introduction

Definition

Authentication packets from STAs are sent to the AC through tunnels. Service packets are directly forwarded by the gateway, but are not forwarded through tunnels. The AC controls access of all wireless users, reducing occupied bandwidth between the AC and APs.

Purpose

A large-capacity AC is located at the core of a network and connects to branches through the Internet. Centralized authentication and local forwarding implement 802.1X or Portal authentication on Layer 3 networks, and solve the following problems:

1. When an AC connects to an AP over a Layer 3 network and direct forwarding is used, 802.1x or Portal access control points cannot be deployed on the AC and the AC cannot control wireless access users in centralized manner. As a result, air interface control and user access control are separated.
2. When an AC connects to an AP over a Layer 3 network and tunnel forwarding is used, 802.1x or Portal access control points can be deployed on the AC. All data is forwarded through tunnels, and even local forwarding is limited by the bandwidth of the link between the AC and the AP.
3. When an AC connects to an AP over a Layer 3 network and direct forwarding is used, 802.1x or Portal access control points can be deployed on the switch. The management and maintenance costs are high. It is difficult to deploy and manage 802.1x access control points.

Benefits

Centralized authentication and local forwarding implement 802.1X or Portal authentication on Layer 3 networks, and allow the AC to control wireless access users in centralized manner. This facilitates AP deployment and management, reduces the management and maintenance costs, and reduces occupied bandwidth between the AC and APs.

2 Principles

About This Chapter

The following forwarding and authentication modes apply to 802.1X and Portal authentication STAs:

- Local authentication + local forwarding
- Centralized forwarding + centralized authentication
- Local forwarding + centralized authentication

Local Authentication + Local Forwarding Mode

In this mode, authentication control points locate on a switch. Only control packets between the AC and APs are transmitted through the CAPWAP tunnel. STA authentication protocol packets such as 802.1X and Portal authentication packets, and authenticated STA service data are directly forwarded by APs.

Disadvantages:

- EAP packets in 802.1X authentication mode and HTTP packets in Portal authentication mode are Layer 2 authentication packets. This requires that STAs and authentication control points must locate on Layer 2 networks. Generally, authentication control points are deployed on a switch. Authentication control points are deployed separately, leading to high cost and complex maintenance.
- Authentication control points such, for example, the 802.1X authentication control point, are not deployed on the AC in centralized mode. The AC cannot control accessed STAs in centralized mode.
- Security of service data packets and authentication protocol packets cannot be ensured.

Advantages:

- Packets between local STAs are directly forwarded by APs, which saves the upstream bandwidth of APs.
- Service data packets and authentication protocol packets do not need to be encapsulated through the CAPWAP tunnel, which saves the upstream bandwidth of APs.

Centralized Forwarding + Centralized Authentication Mode

In this mode, authentication control points locate on the AC. Control packets between the AC and APs, STA authentication packets such as 802.1X and Portal authentication packets, authenticated STA service data are all transmitted through the CAPWAP tunnel.

Disadvantages:

Access control points such as 802.1X and Portal access points are deployed on the AC. All data are transmitted through the CAPWAP tunnel, even the local forwarding is limited by the bandwidth of the link between the AC and APs.

Advantages:

- Security is ensured.
- The AC can manage the STA access in centralized mode.

Local Forwarding + Centralized Authentication Mode

In this mode, authentication control points locate on the AC. You can configure APs to allow STA authentication packets such as 802.1X and Portal authentication packets to enter the CAPWAP tunnel. Packets are delivered to the AC. The authentication process is complete. Authenticated STA service data is directly transmitted by APs.

Disadvantages:

Compared with the centralized forwarding mode, the security of service data packets is weak.

Advantages:

- The AC can manage the STA access in centralized mode, including STA isolation, rate limiting, and ACL configuration.
- The AC delivers authorization information to APs through the CAPWAP tunnel, which improves the network security.
- Packets between local STAs are directly forwarded by APs, which saves the upstream bandwidth of APs.

To implement 802.1X and Portal authentication at Layer 3 networks which requires high on link bandwidth, use the local forwarding + centralized authentication mode.

2.1 Authentication Mode

2.2 Data Forwarding Mode

2.3 Centralized Authentication and Local Forwarding

2.1 Authentication Mode

2.1.1 802.1X Authentication

802.1x authentication (also called Extensible Authentication Protocol Over Ethernet (EAPOE) authentication) is mainly used for access authentication of local area network (LAN) users.

The Institute of Electrical and Electronics Engineers (IEEE) 802.1x standard, 802.1x in brief, is an interface-based network access control protocol. Interface-based network access control is the authentication and control implemented for access devices on an interface of a LAN access control device. User devices connected to the interface can access the resources on the LAN only after passing authentication.

The 802.1x protocol is concerned about only the status of an access interface. When an authorized user accesses an interface using an account and password, the interface is enabled; when an unauthorized user accesses an interface or no users access an interface, the interface is disabled. The authentication result is based on the change in the interface status but is not involved with the IP address negotiation and assignment that need to be considered in common authentication technologies. 802.1x authentication is the most simplified implementation solution among various authentication technologies.

802.1x supports interface-based authentication and MAC-based authentication.

- Interface-based authentication: When interface-based authentication is used, all other access users can use network resources and do not need to be authenticated, as long as the first user on an interface passes authentication. After the first user goes offline, other users cannot use network resources.
- MAC-based authentication: When MAC-based authentication is used, all access users on an interface must be independently authenticated.

802.1x supports the following authentication modes:

- Extensible Authentication Protocol (EAP) termination authentication: The AC terminates EAP packets from users, parses user names and passwords, encrypts the passwords, and then sends them to the AAA server for authentication. EAP termination authentication includes Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).
- EAP relay authentication: The AC encapsulates authentication information about 802.1x users and EAP packets to in the attribute fields in RADIUS packets or HWTACACS packets and sends them to the AAA server.

EAP is not an authentication mechanism but a common architecture. EAP is used to transmit actual authentication protocols. The advantage of EAP is that when a new authentication protocol is developed, the basic EAP mechanism does not need to be changed. Currently, there are more than 20 types of EAP protocols.

EAP packets are Layer 2 authentication packets. When Layer 3 networking is used between an AP and an AC and direct forwarding is configured on the AP, EAP packets cannot be forwarded at Layer 3, resulting in an authentication failure. After the function that forwards EAP packets over tunnels is enabled, the AP forwards EAP packets over tunnels to the AC, implementing authentication packet exchange with the AC.

2.1.2 Portal Authentication

Web authentication is also called Portal authentication. When a user opens a browser for the first time and enters any web site address, the user is redirected to the authentication page of the Portal server and can access network resources only after being authenticated.

The Portal protocol is used to exchange messages between a Portal authentication server and other devices. It uses the client/server model and uses the User Datagram Protocol (UDP) as the transmission protocol. In Portal authentication, the Portal authentication server and the AC communicate with each other through the portal protocol. In this case, the AC functions as the client. When obtaining the user name and password entered by the user on the authentication page, the Portal authentication server transfers them to the AC through the portal protocol.

Portal authentication is classified into direct authentication and Layer 3 authentication.

Direct Authentication

A user's PC is connected to the access device directly or through a Layer 2 device. The access device can learn the PC's MAC address and identifies the user based on IP address and MAC address.

Direct authentication is simple, secure, and easy to implement. However, the networking is not flexible because the PC must be connected to the access device directly or through a Layer 2 device.

Layer 3 Authentication

At the aggregation or core layer, the device connects to an authentication client through a Layer 3 device. The device may not obtain the client's MAC address; therefore, it must use the IP address to identify the client. Layer 3 authentication is required.

The packet interaction process in Layer 3 authentication is the same as the packet interaction process in direct authentication except that the networking of Layer 3 authentication is more flexible and easy to control remotely. However, in Layer 3 authentication, the device identifies users only by using IP addresses, so this authentication mode is not secure.

HTTP packets are Layer 2 authentication packets. When Layer 3 networking is used between an AP and an AC and direct forwarding is configured on the AP, HTTP packets cannot be forwarded at Layer 3, resulting in an authentication failure. After the function that forwards HTTP packets over tunnels is enabled, the AP forwards HTTP packets over tunnels to the AC, implementing authentication packet exchange with the AC.

2.2 Data Forwarding Mode

On a WLAN, control packets and data packets are transmitted in direct forwarding mode (also called local forwarding) and Control and Provisioning of Wireless Access Points (CAPWAP) tunnel forwarding mode (also called centralized forwarding).

IETF established a CAPWAP workgroup in 2005 to standardize the tunneling protocol used between APs and ACs and to define the mechanism that APs use to discover ACs.

CAPWAP packets include control packets and data packets, which are sent using different UDP ports. Control packets are forwarded by a control tunnel and data packets are forwarded by a data tunnel.

CAPWAP provides heartbeat detection and DTLS encryption, which ensures security of CAPWAP tunnels. As defined in CAPWAP, DTLS encryption is mandatory for the control tunnel and optional for the data tunnel.

In CAPWAP tunnel forwarding, packets are transmitted from an AP to an AC over a CAPWAP tunnel, and then are forwarded to the upper-layer network. This improves packet forwarding security.

Local Forwarding

In local forwarding, packets from an AP are forwarded to the upper-layer network by the AC directly, without using the CAPWAP tunnel. This improves packet forwarding efficiency.

In local forwarding, the AP sends original packets without any change on the packets.

Usage Instructions

Control packets must be transmitted between an AP and an AC using a CAPWAP tunnel. Data packets can be forwarded using a CAPWAP tunnel or forwarded directly.

To forward data packets using a CAPWAP tunnel, run the following commands:

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] service-set name ChinaNet
[Quidway-wlan-service-set-ChinaNet] forward-mode tunnel
```

To directly forward data packets, run the following commands:

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] service-set name ChinaNet
[Quidway-wlan-service-set-ChinaNet] forward-mode direct-forward
```

Tunnel forwarding has the following advantages:

- Service VLANs do not need to be configured for the WLAN service on the network devices between APs and ACs. This simplifies network configuration and reduces configuration errors.
- CAPWAP-encapsulated packets are encrypted using the Datagram Transport Layer Security (DTLS) protocol, enhancing security of WLAN service packets.
- WLAN service packets are sent to an AC through CAPWAP tunnels and forwarded by the AC in a centralized manner. All WLAN service packets pass through the AC so that WLAN packet rate limiting, monitoring, analysis, and filtering can be performed on the AC.

Direct forwarding has the following advantages:

- WLANs can be deployed flexibly based on network environments.
- WLAN service packets are not sent to the AC, so the load on the AC is low.

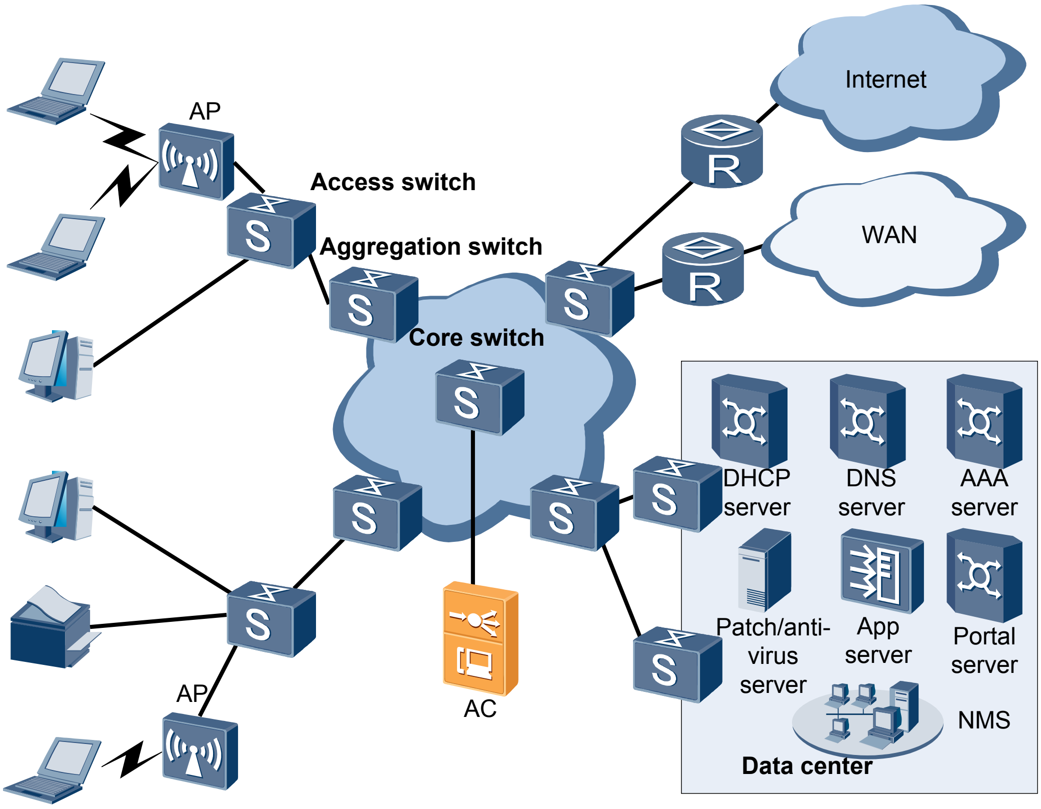
When an AC is connected in branched mode (an Ethernet port functions as both the service access port and uplink port), data packets do not pass the AC if direct forwarding is used; data packets pass the AC if CAPWAP tunnel forwarding is used.

2.3 Centralized Authentication and Local Forwarding

Actual Application

Figure 2-1 shows the centralized AC solution on a large and medium campus network. In **Figure 2-1**, the AC connects to only a core device.

Figure 2-1 Centralized AC solution on a large and medium campus network



A large number of APs exist on large and medium campus networks. Generally, the AC and APs are connected across a Layer 3 network. If the CAPWAP tunnel forwarding mode is used, all data packets and control packets from APs are forwarded to the AC over a CAPWAP tunnel. The packet transmission rate is lowered due to limited CAPWAP tunnel bandwidth. Therefore, local forwarding mode is widely used to allow only the control packets to be forwarded to the AC.

When local forwarding is used and an AC connects to APs over a Layer 3 network, Extensible Authentication Protocol (EAP) packets used in 802.1x authentication and HTTP packets in Portal authentication are Layer 2 packets and cannot be forwarded at Layer 3. Therefore, 802.1x or Portal access control points cannot be deployed on the AC, and the AC cannot control wireless access users in a centralized manner. As a result, air interface control and user access control are separated. If 802.1x or Portal access control points are deployed on a switch, the management and maintenance costs are high and APs are difficult to deploy and manage.

Centralized authentication and local forwarding are introduced to address these problems. Portal or 802.1x authentication packets are encapsulated into a CAPWAP tunnel and forwarded to the AC.

To configure 802.1x authentication packets to be forwarded over tunnels, run the following commands:

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] service-set name huawei
[Quidway-wlan-service-set-huawei] tunnel-forward protocol dot1x
```

To configure Portal authentication packets to be forwarded over tunnels, run the following commands:

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] service-set name huawei
[Quidway-wlan-service-set-huawei] tunnel-forward protocol http
```

Basic Process

Figure 2-2 shows the networking diagram of centralized authentication and local forwarding. Authentication points of all STAs are on the AC. STAs connect to the network after passing 802.1x authentication. Data packets from STAs are directly processed by the AC and not forwarded by the AC.

Figure 2-2 Networking diagram of centralized authentication and local forwarding

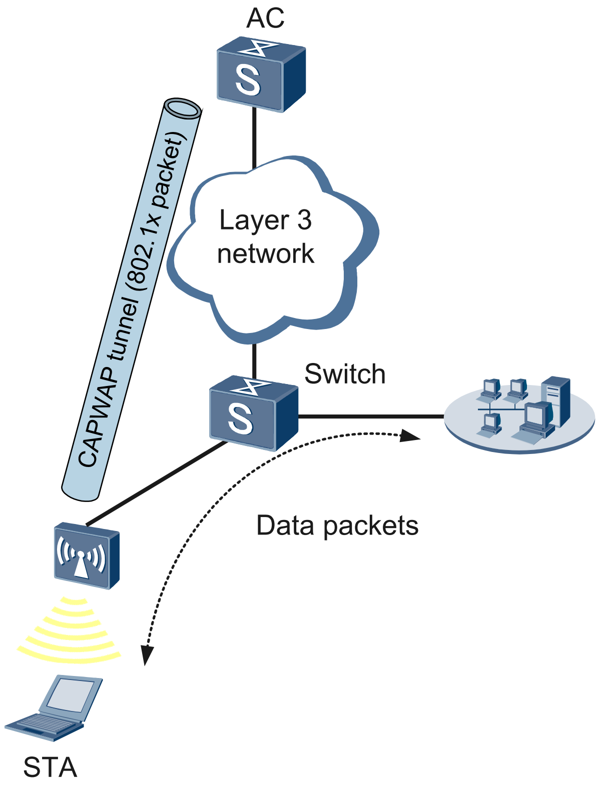
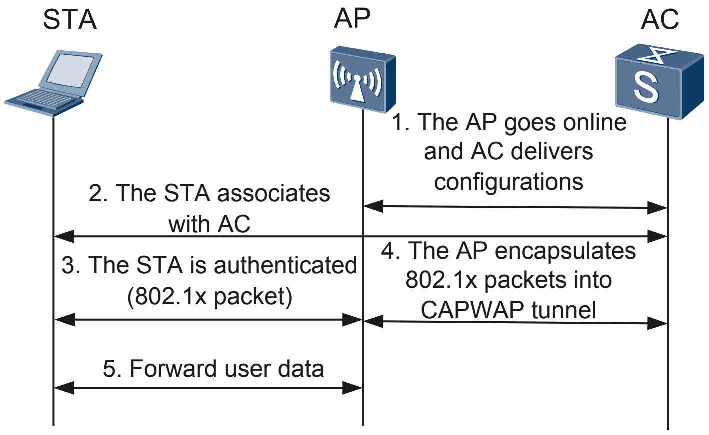


Figure 2-3 shows the process of centralized authentication and local forwarding.

Figure 2-3 Process of centralized authentication and local forwarding


STA
AP
AC
1. The AP goes online and AC delivers configurations
2. The STA associates with AC
3. The STA is authenticated (802.1x packet)
4. The AP encapsulates 802.1x packets into CAPWAP tunnel
5. Forward user data

The process of centralized authentication and local forwarding is as follows:

1. The AP sends a broadcast or unicast packet to discover the AC. The AC delivers the data forwarding mode and 802.1x packet forwarding mode to the AP.
2. The STA associates with the AC.
3. The STA sends an 802.1x packet to the AP to trigger authentication.
4. After receiving the 802.1x packet, the AP encapsulates the 802.1x packet into the CAPWAP tunnel and forwards it to the AC. The AC decapsulates the packet, and authenticates the STA or forwards the packet. The 802.1x packet that the AC returns to the STA is also encapsulated into the CAPWAP tunnel.
5. The STA can forward data after being authenticated. The AP forwards the data in the mode delivered by the AC. In local forwarding, the AP does not need to encapsulate user data into the CAPWAP tunnel.

3 Applications

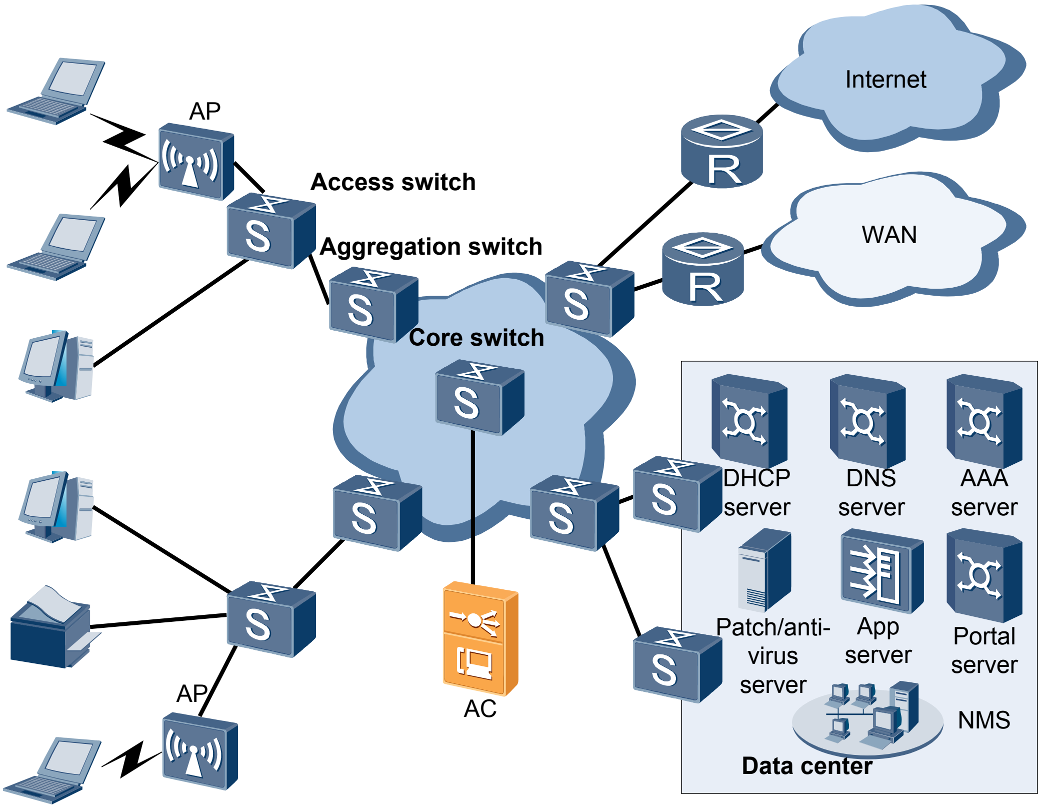
About This Chapter

3.1 Applications of Centralized Authentication and Local Forwarding

Actual Application

Figure 3-1 shows the centralized AC solution on a large and medium campus network. The AC connects to APs over a Layer 3 network. APs are connected to the core switch through access switches and aggregation switches, and then connected to the Internet, wide area network (WAN), and servers. A large number of STAs are connected to APs, and 802.1X or Portal authentication is used. Network administrators want to manage APs on the AC conveniently without affecting the network speed.

Figure 3-1 Centralized AC solution on a large and medium campus network



Configuration Analysis

- Use centralized authentication and local forwarding to implement AP centralized management on the AC without affecting the network speed when there are a large number of STAs on the network.
- Configure 802.1x or Hypertext Transfer Protocol (HTTP) authentication packets to be forwarded over tunnels.

- Configure a service IP address pool on the aggregation switch and a management IP address pool on the AC wireless side. Assign IP addresses for STAs and APs.

The configuration roadmap is as follows:

1. Configure the access switch, aggregation switch, core switch, and AC so that APs can communicate with the AC.
    - Connect the access switch to ports of APs and configure the access switch to tag AP management packets with the management VLAN ID. No configuration is required for APs.
    - Configure the access switch and AC to communicate in the service VLAN and management VLAN.
    - Configure the aggregation switch or core switch to be the Dynamic Host Configuration Protocol (DHCP) server for STAs. Configure the gateway address for STAs on the aggregation switch or core switch. The gateway address cannot be configured on the AC wireless side.
    - Configure the AC to be the DHCP server of APs. APs apply to the AC wireless side for IP addresses using DHCP relay. The gateway of APs can be configured on the switch.
    - Configure the wired side and wireless side on the AC to communicate with each other.
2. Configure the WLAN service on the AC wireless side.
    - Configure the AC ID, carrier ID, country code, and source interface.
    - Configure the AP address pool.
    - Configure the AP authentication mode, configure APs to go online, and add APs to the specified region.
    - Configure WLAN-ESS interfaces.
    - Configure a radio profile and bind the radio profile to a radio.
    - Configure security profiles, traffic profiles, and service sets. Set data forwarding mode to direct forwarding. Enable EAP packets to be forwarded over tunnels.
3. Deliver services to APs.
    - Configure VAPs and deliver configuration to the APs.