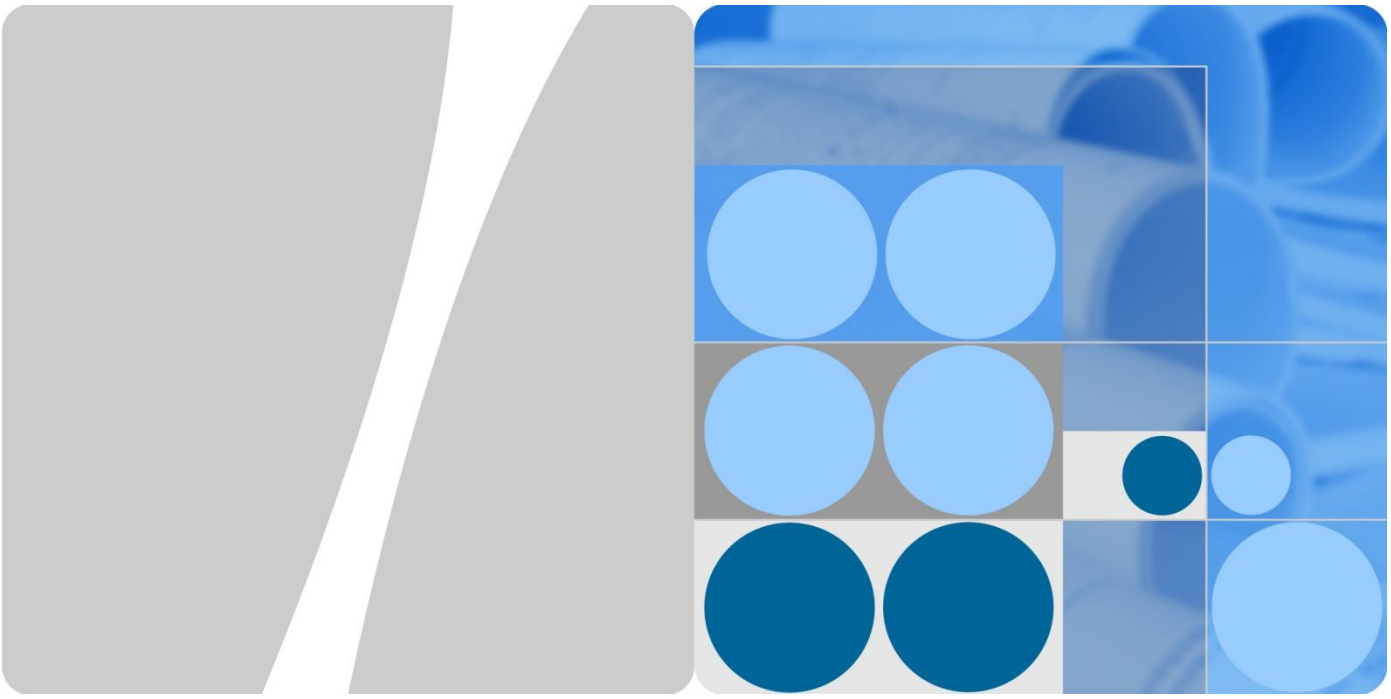


S Series Switches

NAC Technology White Paper

Issue 01

Date 2013-05-25

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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: http://enterprise.huawei.com

Contents

1 Feature Introduction

1.1 NAC Background

With development and increasing applications of network technologies, users have increasing requirements and dependence on their networks. This creates an increase in potential security risks. Network security, which carries more concern than network reliability, switching capability, and QoS, is the most important problem of enterprise users, and the network security facilities are the core in building enterprise networks.

At the past, enterprises were operated in the closed environment and made full control of the information system. At present, enterprises depend on the open and interconnected network environment and the network expands to every corner of the society. While open networks come with the benefits of great convenience, they also make way for threats to enterprise assets. An enterprise intranet may encounter the following problems:

- Unauthorized users access the enterprise intranet.
- Authorized intranet users abuse their rights.
- Terminals do not have patches installed in time.
- Employees install unauthorized software or enable risky services.
- Employees access the websites that are irrelevant to their jobs.
- Employees bypass the firewall to access the Internet.
- Employees do not install the antivirus software.
- Employees forget to set passwords.

Even a small security risk in an enterprise network may endanger the company's reputation, and customers' privacy and intellectual property. In some cases such a risk could potentially strike a fatal blow dealing irreparable damage to the company. According to the statistics from the ISCA, the global loss caused by information security problems reaches the tens of billions of US dollars every year, 60% of which result from internal threats. This has caused internal threats become the primary security concern to enterprises. It can be said to a certain degree that a secure information system has become the basis for enterprise survival in the modern day.

Current network devices use passive and single-point defense modes with no uniform deployment and planning. This prevents security problems from being solved in globally deployed network infrastructure.

- Current security devices cannot effectively protect the network because they are unable to:

  - Assess the security of computers on the network.
  - Prevent authorized user terminals from abusing network resources.
  - Prevent malicious attacks.
- A large number of terminals exist, the system is complex, and employee behavior is not easily managed.
  - There is a lack of effective security monitoring and auditing methods on the enterprise intranet.
  - The system does not adopt effective management and emergency response methods.
  - Employee behavior regarding the disclosure of enterprise information cannot be traced.
  - Employee behavior online cannot be managed and audited.
  - Terminal status cannot be known and updated in real time.

NAC technology serves to ensure the security of network communication services. In the NAC security framework, internal network security is considered from the perspective of user terminal, implementing security control over access users, and guaranteeing end-to-end security.

1.2 NAC Networking

Network Admission Control (NAC) is an end-to-end security access framework. The NAC solution controls network access of user terminals by:

- Integrating network access control with terminal security products
- Combining user ends, access control components, network devices (switches, routers, firewalls, and wireless devices), and third-party software (anti-virus software and patch servers)
- Forcibly implementing security policies for user terminals that access networks
- Strictly controlling network use behaviors of terminal users
- Effectively improving user terminals' proactive defense capabilities
- Providing effective and easy-to-use management tools and methods for network management personnel

NAC is closely associated with users' services. The NAC implementation scheme varies depending on the networking and service. In the scheme, selecting a proper identity authentication method is one of the most important tasks.

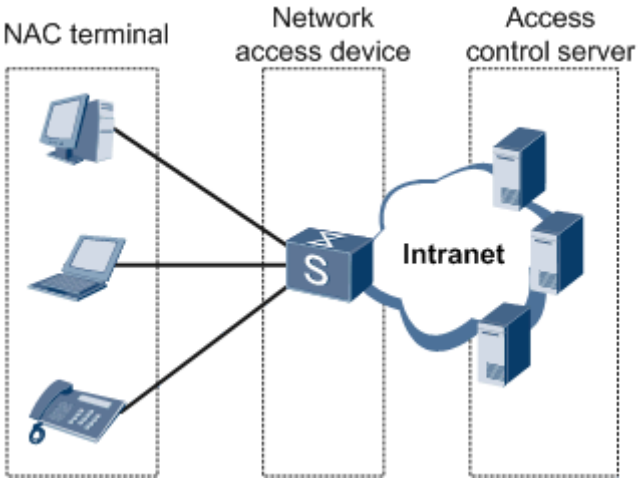
This document describes how network devices implement security control in the NAC solution.

As shown in Figure 1-1 and Figure 1-2, NAC provides an access security solution, which involves the following entities:

- NAC terminal: functions as the NAC client and interacts with network access devices to authenticate access users. If 802.1x authentication is used, users must install client software.
- Network access device (NAD): authenticates and authorizes access users. The NAD usually works with an Authentication, Authorization, and Accounting (AAA) server to prevent unauthorized terminal access, minimize the threats brought by insecure terminals, prevent unauthorized access requests from authorized terminals, and protect core resources.

- Access control server: checks terminal health and manages terminals based on specific policies. It manages user behaviors and checks for rule violations to prevent malicious attacks from terminals.

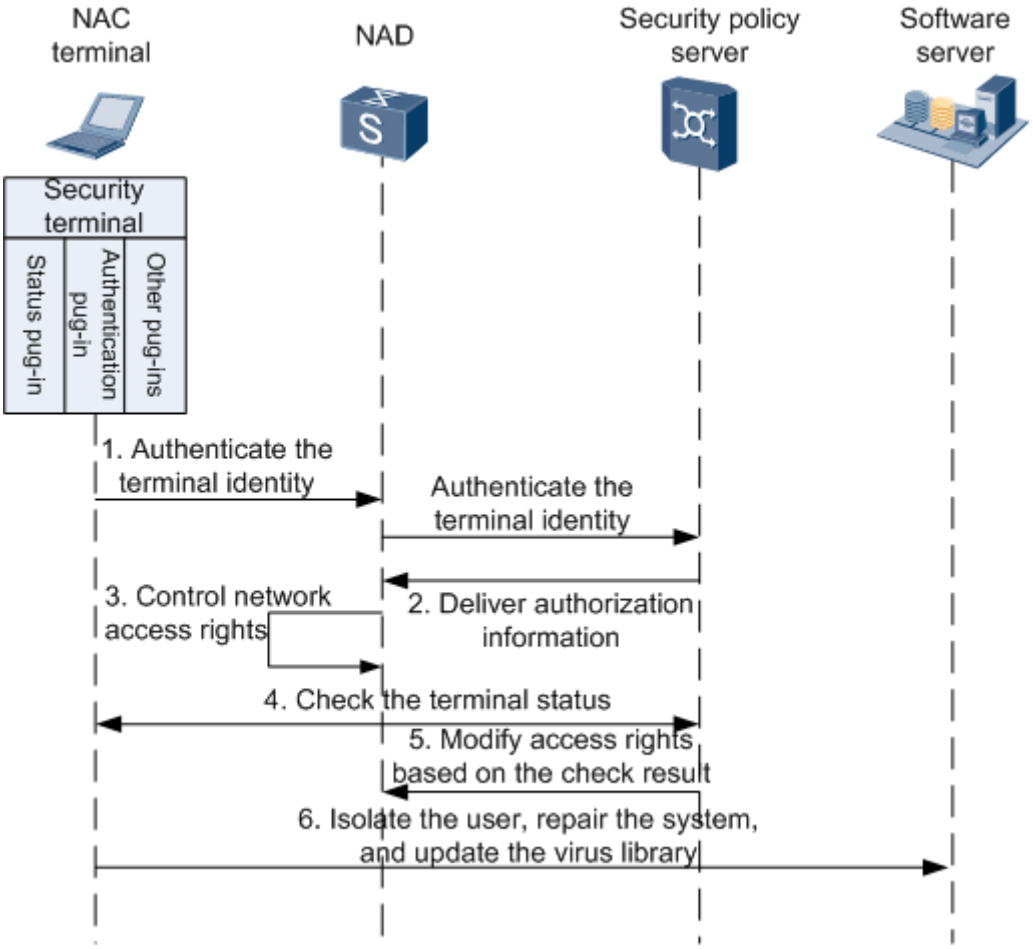
Figure 1-1 Typical NAC networking



1.3 NAC Process

Figure 1-2 shows the NAC process.

Figure 1-2 NAC process



1. The NAD cooperates with a security policy server (for example, the AAA server) to authenticate the NAC terminal when the terminal connects to the network.
2. The security policy server sends the authorization information to the NAD if the terminal has been authenticated. If the authentication fails, the NAD isolates the terminal.
3. Based on the authorization information from the security policy server, the NAD controls the terminal user's network access rights and establishes a communication channel between the terminal and security policy server.
4. The NAC terminal directly exchanges information with the security policy server. The terminal reports its status information, including the virus library, operating system, and patch versions.
5. The security policy server checks the terminal's status information. If the NAC terminal does not comply with the enterprise security standard, the security policy server delivers the authorization information, modifies the terminal's network access rights, and notifies the NAC terminal.
6. Based on the status check result, the NAC terminal can update the virus library, repair the system, or download the client until it complies with the enterprise security standard.

1.4 NAC Advantages

The NAC provides a comprehensive security system to facilitate terminal security management and guarantee network security. The anti-virus function is integrated with network access control to enhance centralized terminal management and improve terminals' proactive defense capabilities. Huawei NAC security solution allows only authorized users and secure terminals to access networks. This solution uses enterprise network products, security products, and Terminal Security Management (TSM). It provides user authentication, security checking, system repair and upgrade, and strengthens enterprises' defense capabilities.

1.4.1 Integrated Terminal Security and Access Control

The NAC ensures that all user terminals connecting to networks comply with the enterprises' anti-virus standards and system patch installation policies. User terminals that do not comply with such policies or fail to be authenticated are isolated with access to only specified network resources. Specific network access rights can be limited for specific users to implement personalized customization and refined control.

1.4.2 Multiple Authentication Modes and Application Scenarios

The NAC supports multiple authentication modes to meet the access requirements of different terminals in different application scenarios. The authentication modes include 802.1x authentication, MAC bypass authentication, MAC address authentication, and Portal authentication. The terminal access control and authorization policies vary depending on the access mode to ensure network security from the perspective of different network layers.

1.4.3 Flexible and Convenient Deployment Modes

- Terminals that do not support 802.1x authentication, such as printers or IP phones, can use the MAC address authentication mode to connect to networks.
- Guests or employees on business can access networks in Portal authentication mode.
- Terminals that do not support the 802.1x client are allowed to access networks without being authenticated by the client.
- The NAC provides fast deployment of the 802.1x client to users without an installation of the 802.1x client, to allow them access to the network in 802.1x authentication mode.

1.4.4 Refined Authorization Control Modes

The NAC solution supports authorization control based on different access modes by:

- Performing authorization control for the port-based 802.1x terminals
- Performing authorization for the MAC address-based terminals
- Isolating the terminals that fail to be authenticated
- Using ACLs or VLANs to perform authorization control for the terminals that can be authenticated

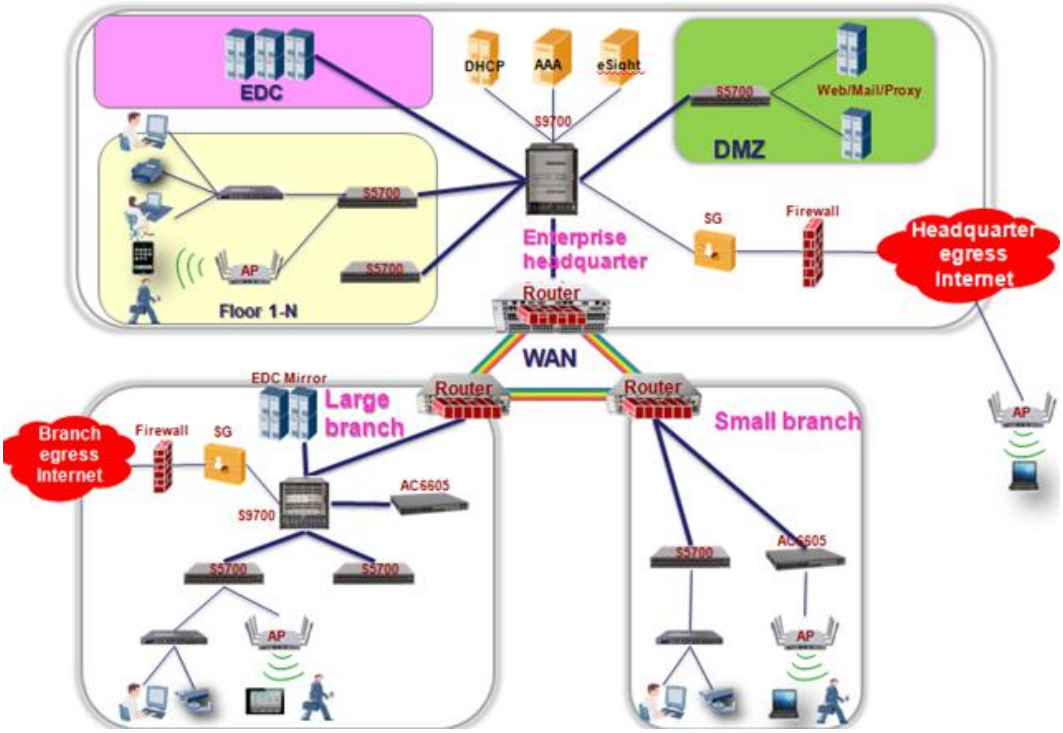
2 Technology Description

2.1 Concepts

Huawei NAC solution provides multiple access control modes including 802.1x authentication, MAC address authentication, and Portal authentication. These access control modes can be flexibly deployed on multiple network devices such as access switches and aggregation switches. The network devices cooperate with the NAC client and server to implement secure and reliable access control for enterprise networks.

Figure 2-1 shows a typical NAC enterprise campus network.

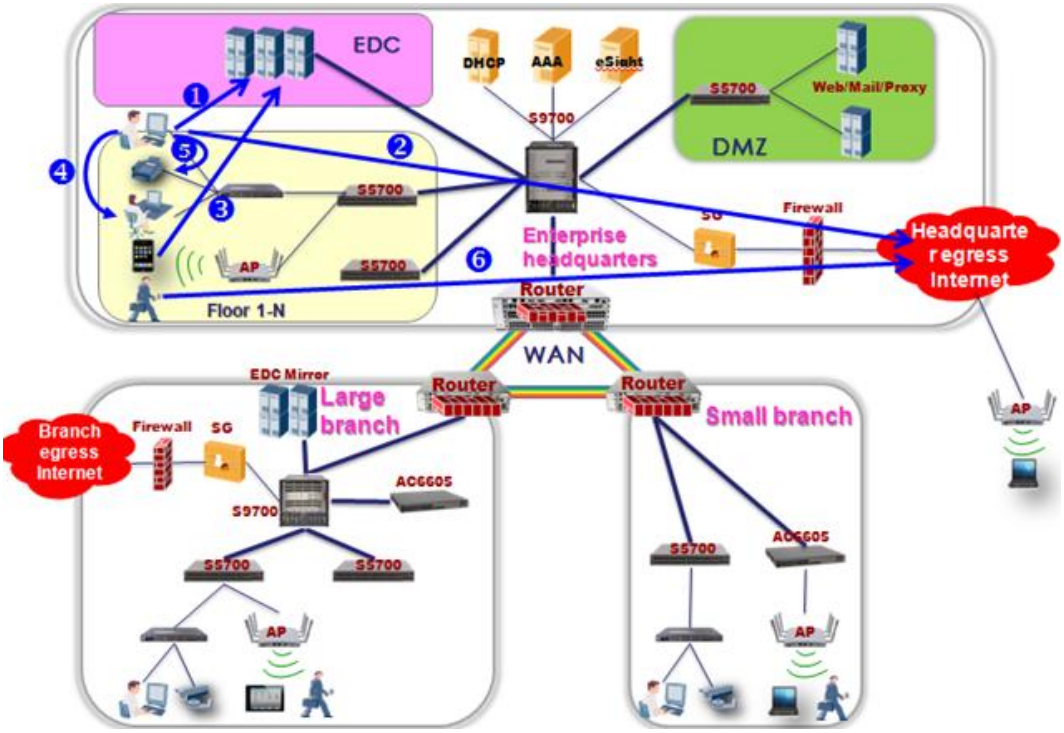
Figure 2-1 NAC enterprise campus network



- Internal access (as shown in Figure 2-2)

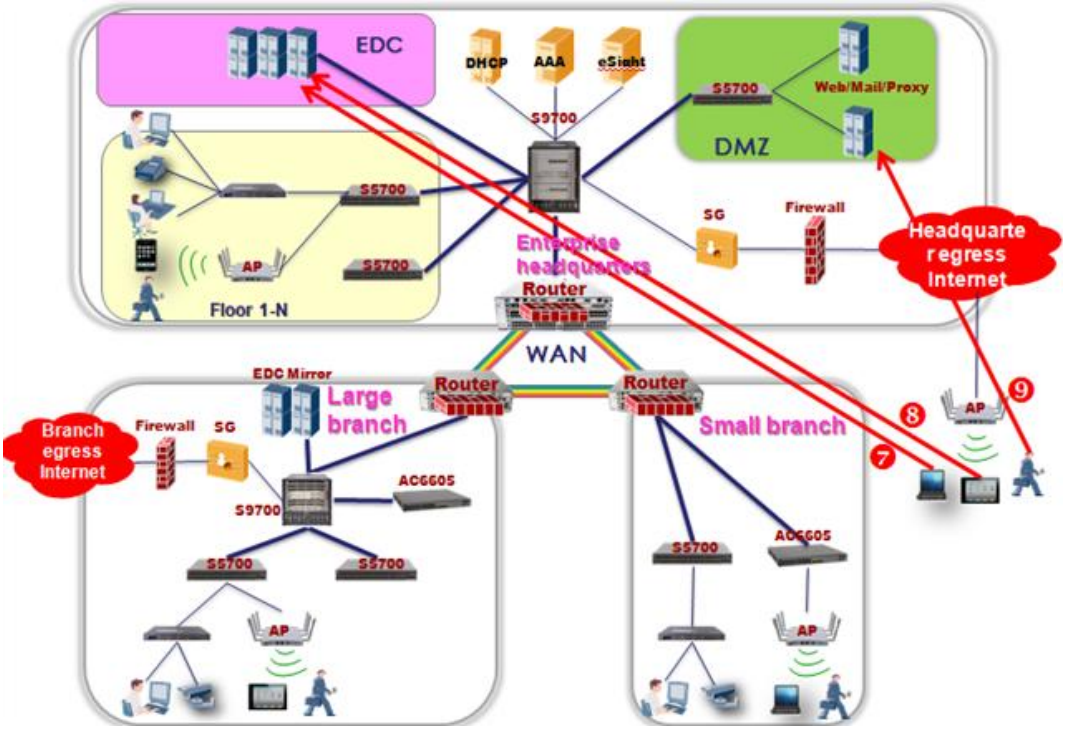
- (1) An employee uses a company terminal to access the campus network in wired or wireless mode and logs in to the Enterprise Data Center (EDC) for routine office work.
- (2) The employee uses the company terminal to access the campus network in wired or wireless mode and accesses the Internet through the SG.
- (3) The employee uses a BYOD device to access the campus network in wired or wireless mode and logs in to the EDC for routine office work.
- (4) The employee communicates with another employee.
- (5) The employee accesses a dumb terminal such as a network printer or video monitoring device.
- (6) A guest uses a BYOD device to access the campus network in wired or wireless mode and accesses the Internet through the SG.

Figure 2-2 Internal access process in an enterprise network



- External access (as shown in Figure 2-3)
  - (7) The employee uses a company terminal to access the enterprise intranet in a secure mode through the Internet and logs in to the EDC for routine office work.
  - (8) The employee uses a BYOD device to access the enterprise intranet in a secure mode through the Internet and logs in to the EDC (or is only allowed to access specified servers) for routine office work.
  - (9) A guest accesses the enterprise's demilitarized zone (DMZ) through the Internet.

Figure 2-3 External access process in an enterprise network



NOTE

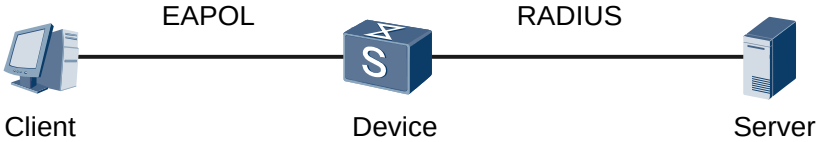
This document describes the NAC functions that are supported by Huawei switches. The process in which wireless users access networks through the NAC is not mentioned.

2.2 802.1x Authentication

2.2.1 802.1x Overview

To solve the security problems of the wireless local area network (LAN), the Institute of Electrical and Electronics Engineers (IEEE) 802 LAN/WAN committee put forward the 802.1x protocol. This protocol has been widely applied in the Ethernet as a common access control mechanism on LAN interfaces to solve problems in terms of authentication and security on the Ethernet. The 802.1x protocol is a port-based network access control protocol. It authenticates user devices and controls based on interfaces connected to user devices, so as to control access to network resources. As shown in Figure 2-4, the 802.1x system has a typical client/server structure and includes three entities: client, device, and server.

Figure 2-4 802.1x authentication system



- Client: an entity on the LAN segment, which is authenticated by the device at the other end of the link. The client is usually a user terminal. A user initiates 802.1x authentication by starting the client software. The client must support Extensible Authentication Protocol over LAN (EAPoL).
- Device: an entity on the LAN segment, which authenticates the connected client. The device is usually a network device that supports the 802.1X protocol and provides an interface (physical or logical) for LAN access of the client.
- Server: an entity that provides the authentication service for the device. The server is usually a Remote Authentication Dial-In User Service (RADIUS) server for implementing authentication, authorization, and accounting (AAA).

2.2.2 802.1x Concepts

- Controlled and uncontrolled interfaces

  The device provides an interface for the client to access the LAN. The interface is classified into two logical interfaces: controlled interface and uncontrolled interface.

  - In authorized mode, the controlled interface transmits service packets in both directions; in unauthorized mode, the controlled interface cannot receive packets from the client.
  - The uncontrolled interface is mainly used to transmit EAPoL frames in both directions to ensure that the client sends and receives authentication packets at any time.

- Authorized and unauthorized states

  The device uses the authentication server to authenticate the client that accesses the LAN and controls the authorized or unauthorized state of the controlled interface according to the authentication result (Accept or Reject).

  The authorization state of the interface can be configured to control whether an access user must be authenticated before accessing network resources. The interface supports the following authorization modes:

  - auto: The interface is initially in unauthorized state and sends and receives only EAPoL packets. Users cannot access network resources. After a user is authenticated, the interface switches to the authorized state and allows the user to access network resources.
  - authorized-force: The interface is always in authorized state and allows users to access network resources without authentication.
  - unauthorized-force: The interface is always in unauthorized state and does not allow users to access network resources. The device does not provide the authentication service for the clients connected to the interface.

- Interface control modes

  The device supports the following interface access control modes:

  - Interface-based: If the first user on the interface can be authenticated, other access users can access the network without being authenticated. However, when the authenticated user goes offline, other users can no longer access the network. This mode applies to group users.
  - MAC address-based: All users on the interface must be authenticated. When any of the users goes offline, other users still maintain access to the network. This mode applies to individual users.

2.2.3 802.1x Authentication Triggering Mode

802.1x authentication can be initiated by:

- Client: sends an EAPOL-Start packet to the device to trigger authentication.
- Device: triggers authentication when the client, such as the built-in 802.1x client of the Windows XP, cannot proactively send an EAPOL-Start packet.

  Two triggering methods are available:

  - Triggered by a DHCP packet: The device triggers 802.1x authentication for a user after receiving a DHCP request packet from the user. The user can specify whether the entire authentication procedure should be adopted.

  NOTE

  The following operations can be performed in a sequence based on the actual scenario:

  - Assign a DHCP address to a wired user.
  - Perform 802.1x authentication.

  - Triggered by a packet with an unknown source MAC address: The device triggers 802.1x authentication after receiving a packet with an unknown MAC address from a new user. If the device does not receive any response from the client within a specified duration, the packet is retransmitted.

2.2.4 802.1x Authentication Modes

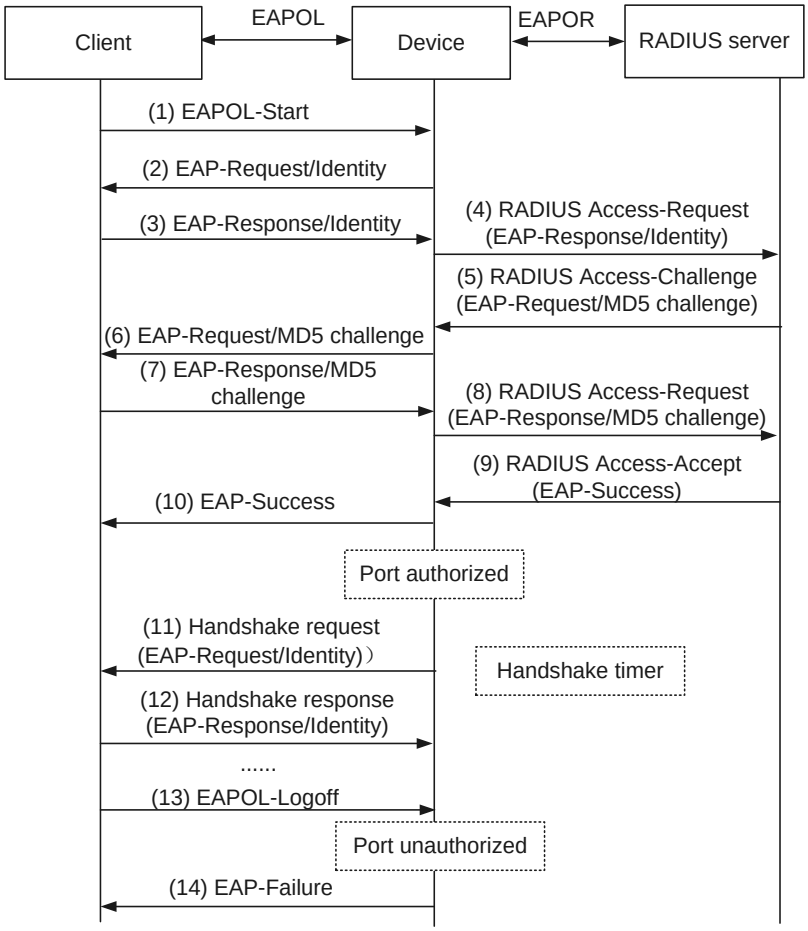
Based on the EAP packet exchange mode between the device and RADIUS server, the following authentication modes are available:

EAP Relay Mode

In EAP relay mode, the device relays EAP packets. The EAP packets are encapsulated in the EAP over RADIUS (EAPOR) format by the device, carried in a RADIUS protocol, and sent to the RADIUS server for authentication. This authentication mode makes device processing simple and supports various EAP authentication methods, such as MD5-Challenge, EAP-TLS, and PEAP. However, the server is required to support corresponding authentication methods.

Figure 2-5 shows the service process in EAP relay mode.

Figure 2-5 Service process in EAP relay mode



1. To access an external network, a user starts the 802.1x client program, enters a registered user name and password, and initiates a connection request. At this time, the client sends an authentication request frame (EAPOL-Start) to the device to start the authentication process.
2. After receiving the authentication request frame, the device sends an identity request frame (EAP-Request/Identity), requiring that the client should send the entered user name.
3. The client sends an identity response frame (EAP-Response/Identity) carrying the user name to the device and selects the authentication domain based on the domain information contained in the user name.
4. The device encapsulates the EAP packet in the response frame sent by the client into a RADIUS packet (RADIUS Access-Request) and sends the RADIUS packet to the authentication server for processing.
5. After receiving the user name forwarded by the device, the RADIUS server searches the user name table in the database for a password corresponding to the user name, encrypts the password with a randomly generated MD5 challenge, and sends the MD5 challenge in a RADIUS Access-Challenge packet to the device.
6. The device forwards the MD5 challenge sent by the RADIUS server to the client.

7. The client uses the password and MD5 challenge obtained to perform MD5 algorithm processing. It then generates an MD5 challenge carried in an EAP-Response/MD5 Challenge packet, and sends the packet to the device.
8. The device encapsulates the EAP-Response/MD5 Challenge packet into a RADIUS packet (RADIUS Access-Request) and sends the RADIUS packet to the RADIUS server.
9. The RADIUS server compares the received encrypted password and the locally encrypted digest information. If they are the same, the RADIUS server considers that the user is authorized and sends a RADIUS Access-Accept packet to the device.
10. After receiving the RADIUS Access-Accept packet, the device sends an EAP-Success frame to the client, changes the interface state to authorized, and allows the user to access the network through the interface. The device creates a complete user table.
11. When the user is online, the device periodically sends handshake packets to the client to monitor the online user.
12. After receiving a handshake packet, the client sends a response packet to the device, indicating that the user is still online. By default, the device disconnects the user if it does not receive any response from the client after sending two consecutive handshake packets. The handshake mechanism allows the device to detect unexpected user disconnections.
13. If the user wants to go offline, the client sends an EAPOL-Logoff frame to the device.
14. The device changes the interface state from authorized to unauthorized and sends an EAP-Failure packet to the client.

EAP Termination Mode

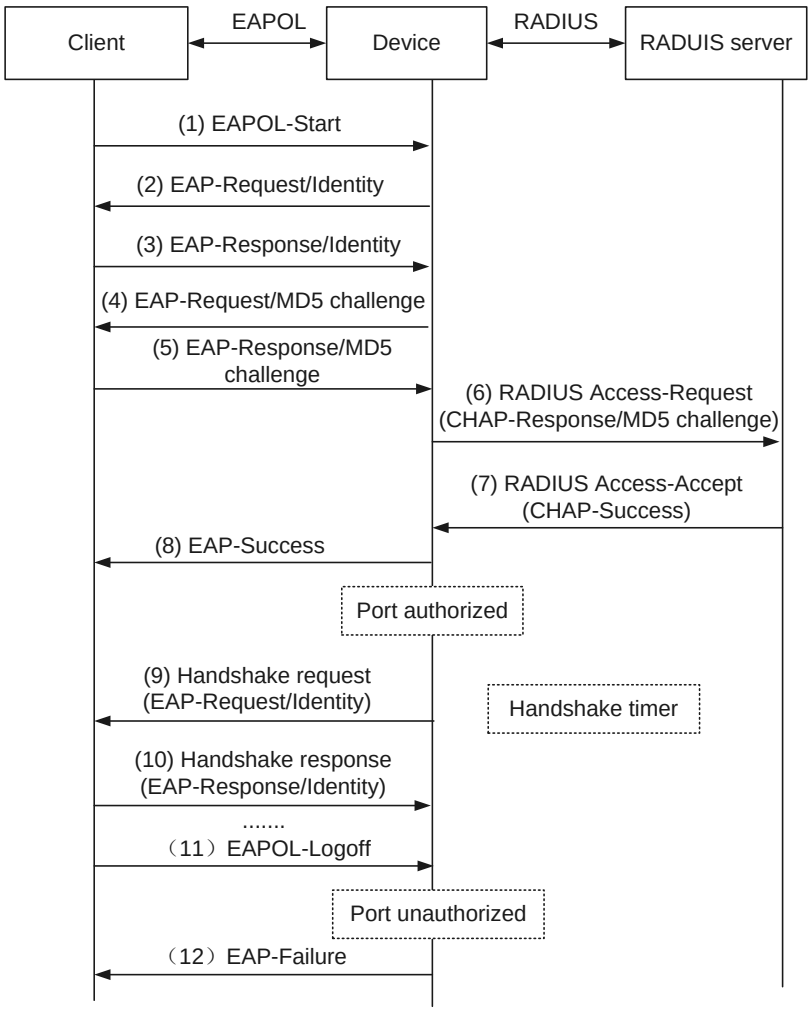
In EAP termination mode, the device terminates the EAP packets. The device encapsulates client authentication information into a standard RADIUS packet and implements authentication with the server using Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP).

- PAP is a two-way handshake authentication protocol. It transmits passwords in plain text format in RADIUS packets.
- CHAP is a three-way handshake authentication protocol. It transmits only the user name but not the password in RADIUS packets. CHAP is more secure and reliable than PAP, making it the better choice for high security.

The advantage of this authentication mode is that all existing RADIUS servers support PAP and CHAP authentication and therefore the server does not require update. However, device processing is complex and only the MD5-Challenge EAP authentication method is supported.

Figure 2-6 shows the service process in EAP termination mode.

Figure 2-6 Service process in EPA termination mode



The difference between the authentication process in EAP termination mode and that in EAP relay mode is that, in EAP termination mode, the device randomly generates an MD5 challenge for encrypting the user password in step 4, and sends the user name, the MD5 challenge, and the password encrypted on the client to the RADIUS server for authentication.

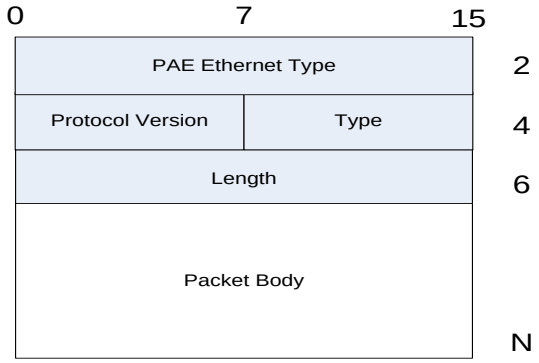
2.2.5 802.1x Packet Format

EAPoL Packet Format

EAPoL is a packet encapsulation format defined by the 802.1x protocol. EAPoL is mainly used to transmit EAP packets between a client and a device to allow EAP packets to be transmitted on the LAN. Figure 2-7 shows the EAPoL packet format.

When EAPoL frames are transmitted at Layer 2, they must have a destination MAC address. If the client and authentication system both do not know the destination, the multicast address 01-80-c2-00-00-03 assigned by the 802.1x protocol is used as the destination MAC address.

Figure 2-7 EAPoL packet format



PAE Ethernet Type: indicates the protocol type. The value is 0x888E.

Protocol Version: indicates the protocol version number supported by the EAPoL frame sender.

Type: indicates the EAPoL data frame type.

Type	Description
EAP-Packet: indicates the authentication information frame used to carry authentication information. The value is 0x00.	This frame is re-encapsulated into the RADIUS protocol on the device, which facilitates the frame in traversing the complex network to the authentication server.
EAPOL-Start: indicates the authentication initiation frame. The value is 0x01.	This frame only exists between the client and device.
EAPOL-Logoff: indicates the logout frame. The value is 0x02.	This frame only exists between the client and device.
EAPOL-Key: indicates the EAPOL-Key frame. The value is 0x03.	This frame is used to exchange dynamic key information. The device uses EAPOL-Key to generate the key required for encrypting data. (This frame is used in wireless access.)
EAPOL-Encapsulated-ASF-Alert: indicates the EAPOL-Encapsulated-ASF-Alert frame. The value is 0x04.	This frame is not supported by the current device.

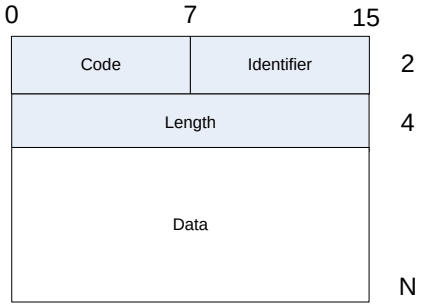
Length: indicates the data length, that is, the length of the Packet Body field. The value is expressed in bytes. If the length is 0, there is no data field.

Packet Body: indicates the data content. It varies depending on the value of Type. If the value of Type is EAP-Packet, EAPOL-Key, or EAPOL-Encapsulated-ASF-Alert, Packet Body has the corresponding value. For other frame types, the value of Packet Body is empty. Only the EAP-Packet type is described in details in this document.

EAP Packet Format

When the Type field in the EAPoL packet format is EAP-Packet, Packet Body is in the EAP packet format, as shown in Figure 2-8.

Figure 2-8 EAP packet format



Code: indicates the type of EAP data packets, which can be Request, Response, Success, and Failure.

Identifier: matches the Request and Response messages.

Length: indicates the length of EAP data packets, including the Code, Identifier, Length, and Data fields. The value is expressed in bytes.

Data: indicates the content of EAP data packets, which is determined by the Code field.

Success and Failure data packets do not have the Data field and their length is 4 bytes.

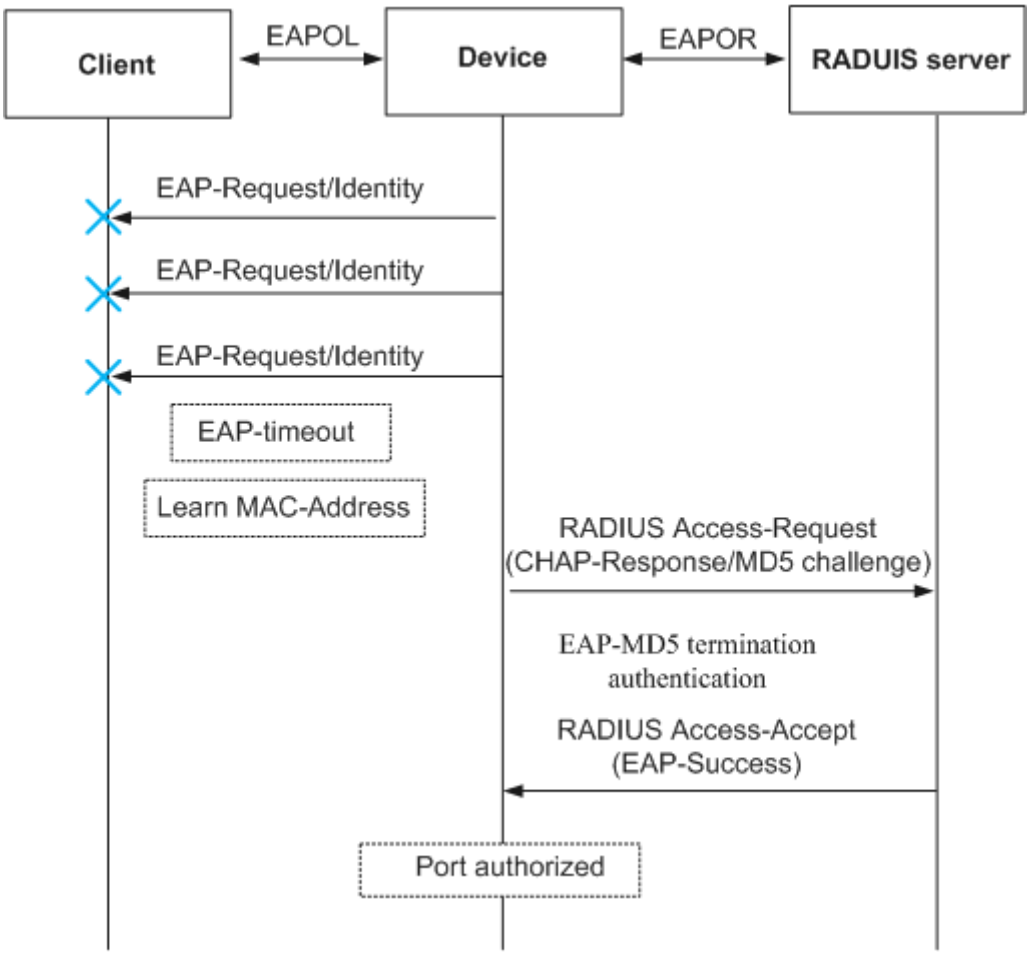
Figure 2-9 shows the format of the Data field in the packets of the Request and Response types. The value of Type indicates an EAP authentication type. The value of Type data is determined by the value of Type. For example, if the value of Type is 1, the value of Type data is Identity, which is used to query the identity of the opposite party. If the value of Type is 4, the value of Type data is MD5-Challenge, which is similar to the PPP CHAP protocol. The type data contains challenge messages.

Figure 2-9 Request/Response packet

2.2.6 MAC Address Bypass Authentication

MAC address bypass authentication enables terminals (for example, printers) that cannot install and use 802.1x client software in the 802.1x authentication system to use their MAC addresses as the user names and passwords for authentication. During the 802.1x authentication process, the device first triggers a user to use 802.1x authentication. If the user does not perform 802.1x authentication after a long time, the user's MAC address is used as the user name and password and sent to the authentication server for authentication. If the device receives no response after sending multiple authentication requests, MAC address bypass authentication is used, as shown in Figure 2-10.

Figure 2-10 MAC address bypass authentication



2.2.7 802.1x Timers

802.1x authentication timers include:

- Handshake timer (handshake-period): starts after a user can be authenticated. The device sends handshake request packets at the intervals specified by handshake-period to regularly check whether a user is online. If the number of sending times is set to *N*, a user is considered offline when the device does not receive response packets from the client *N* consecutive times.
- Quiet timer (quiet-period): The device enters a quiet period set by quiet-period after a user fails to be authenticated. During the quiet period, the device does not process authentication requests from the user.
- Periodical re-authentication timer (reauthenticate-period): If the periodical re-authentication function is enabled on an interface, the device initiates re-authentication for online users on the interface at an interval set by reauthenticate-period.
- Server timeout timer (server-timeout): The device starts this timer after sending a RADIUS Access-Request packet to the authentication server. If the authentication server does not respond within the period set by server-timeout, the device resends the authentication request packet.

- Client timeout timer (client-timeout): The device starts this timer after sending an EAP-Request/MD5-Challenge request packet to the client. If the client does not respond within the period set by client-timeout, the device sends the packet again.
- User name request timeout timer (tx-period): defines two intervals.
  - Interval A: The device starts the timer after sending an EAP-Request/Identity request packet to the client. If the client does not respond within interval A, the device resends the authentication request packet.
  - Interval B: The device multicasts the EAP-Request/Identity request packet at interval B to detect the client that does not proactively send the EAPOL-Start connection request packet for compatibility with such client.

2.2.8 802.1x Authentication Access Control

Access rights of user terminals can be controlled by delivering VLANs or ACLs (or both VLANs and ACLs). Based on different control modes, 802.1x authentication is classified into VLAN-based 802.1x authentication and ACL-based 802.1x authentication.

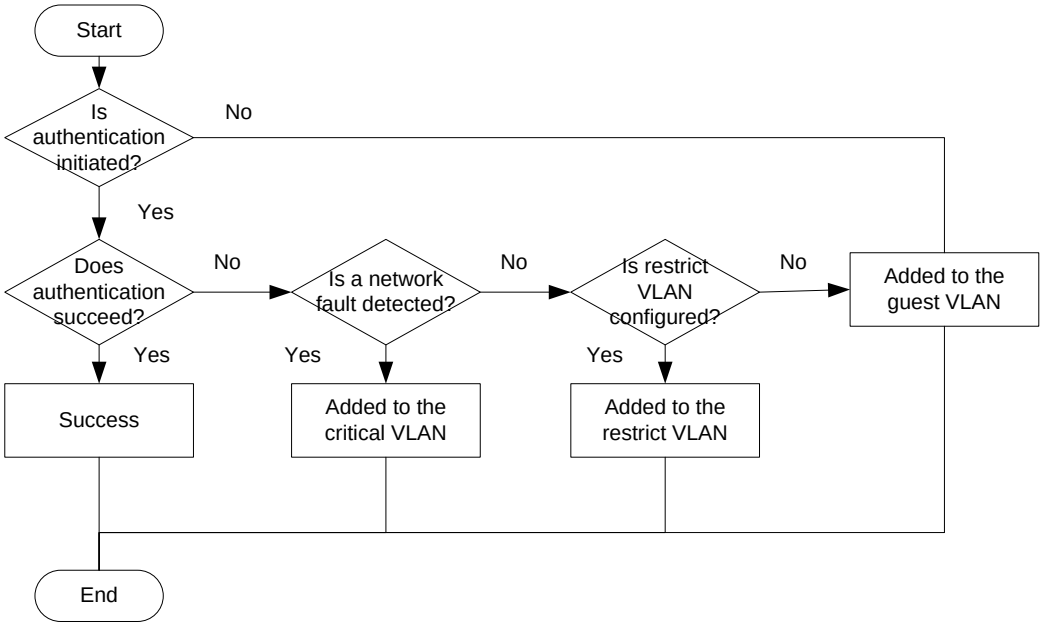
VLAN-based Access Control

VLAN-based authorization is easy to deploy and the maintenance costs are low. This mode applies to scenarios where staff in an office or a department have the same access rights. In this mode, VLANs are switched to modify user rights.

- Before authentication, a user terminal is in the guest VLAN and its access rights are restricted by the guest VLAN.
- If user authentication succeeds and the user terminal is insecure, the user terminal is added to the isolated VLAN and its access rights are restricted by the isolated VLAN.
- If user authentication succeeds and the user terminal is secure, the user terminal is added to the service VLAN and its access rights are restricted by the service VLAN.

Figure 2-11 shows the VLAN judgment process.

Figure 2-11 VLAN judgment process



- Guest VLAN (unknown terminals)

  With the guest VLAN function enabled, when the user does not respond to the 802.1x authentication request (for example, because no client software is installed), the device adds the interface corresponding to the user to the guest VLAN. The user can then access resources in the guest VLAN. In this case, unauthenticated users can obtain client software, upgrade the client, or perform other program upgrade operations.

  If the restrict VLAN is not configured, a user is added to the guest VLAN when the user fails to be authenticated.

- Restrict VLAN (unauthorized users)

  With the restrict VLAN function enabled, when a user fails to be authenticated (for example, because an incorrect user name or password is entered), the device adds the interface corresponding to the user to the restrict VLAN. Similar to the guest VLAN, the restrict VLAN allows users to access limited network resources before authentication. Generally, fewer network resources are deployed in the restrict VLAN than in the guest VLAN; therefore, the restrict VLAN limits unauthorized users' access to network resources more strictly.

- Critical VLAN (unknown network or server)

  With the critical VLAN function enabled, if the authentication server does not respond (for example, because the device and authentication server is disconnected or the authentication server is faulty), the device adds the interface corresponding to the user to the critical VLAN. The user then can access resources in the critical VLAN.

ACL-based Access Control

Dynamic ACL authorization can better control user rights. This authorization mode allows staff within the same department to have different access rights, for example, the department manager has more rights than employees. To control user rights, the server delivers ACLs to switches in either of the following ways:

- Configure ACLs on the server and directly deliver ACLs to switches.

  ACLs configured on the server are easy to maintain, but each user occupies different ACLs, which requires more ACL resources on the access switch.

- Configure ACLs or user groups on the access switch and deliver the ACL numbers or user group names.

  Users with the same access rights share one ACL resource, so fewer ACLs are used on the access switch. However, there are high maintenance costs associated with modifying access rights configured on the access switch.

2.2.9 802.1x-based Fast Deployment

The NAC provides an end-to-end access control scheme to improve the entire network defense capability. In an 802.1x network deployment, if the 802.1x client software is downloaded and upgraded for each access user, the administrator has a large amount of workload when there are a large number of access users. Free IP subnets and redirect-to URLs can be configured for users to implement fast deployment of the 802.1x client.

802.1x-based fast deployment is implemented using the following functions:

- User access limitation: Free IP subnets can be configured to enable users to access the network resources in the subnets before 802.1x authentication succeeds.

- HTTP-based URL redirection: When a terminal user uses a browser to access a network before 802.1x authentication or after an authentication failure, the device redirects the user to a configured URL (client download page).

NOTE
The server that provides the redirect-to URL must be located in the free IP subnet of the user.

2.2.10 User Group Authorization

In an actual NAC network deployment, there are a lot of access users, but user types are limited. User rights are controlled based on user groups. After a user is authenticated, the authentication server delivers a user group for the user. Each user group can be associated with data forwarding and service processing rules to control the network access rights of users in the group.

2.3 MAC Address Authentication

2.3.1 MAC Address Authentication Overview

MAC address authentication controls the network access rights of a user based on the user's interface and MAC address. Client software does not need to be installed. The device starts authenticating a user when detecting the user's MAC address for the first time on the interface where MAC address authentication has been enabled. During the authentication process, the user does not need to enter a user name or password.

2.3.2 MAC Address Authentication Concepts

MAC Address Authentication Types

Based on different user name formats and content that the device uses to authenticate users, user name formats used in MAC authentication can be classified into the following types:

- MAC address: The MAC address of a user is used as the user name and password for authentication.
- Fixed user name: Regardless of users' MAC addresses, all users use a fixed name and password designated on the device for authentication. As multiple users can be authenticated on the same interface, all users requiring MAC address authentication on the interface use the same fixed user name. The server only needs to configure one user account to meet the authentication demands of all users. This applies to a network environment with reliable access clients.

MAC Address Authentication Domains

When the MAC address or the fixed user name without a domain name is used as the user name in MAC address authentication, the user is authenticated in a default domain if the administrator does not configure an authentication domain. In this case, many users are authenticated in the default domain, making the authentication scheme inflexible. An authentication domain for MAC address authentication users can be configured globally or on an interface.

- Globally: The domain is valid for all interfaces.
- On an interface: The domain is valid only for this interface.

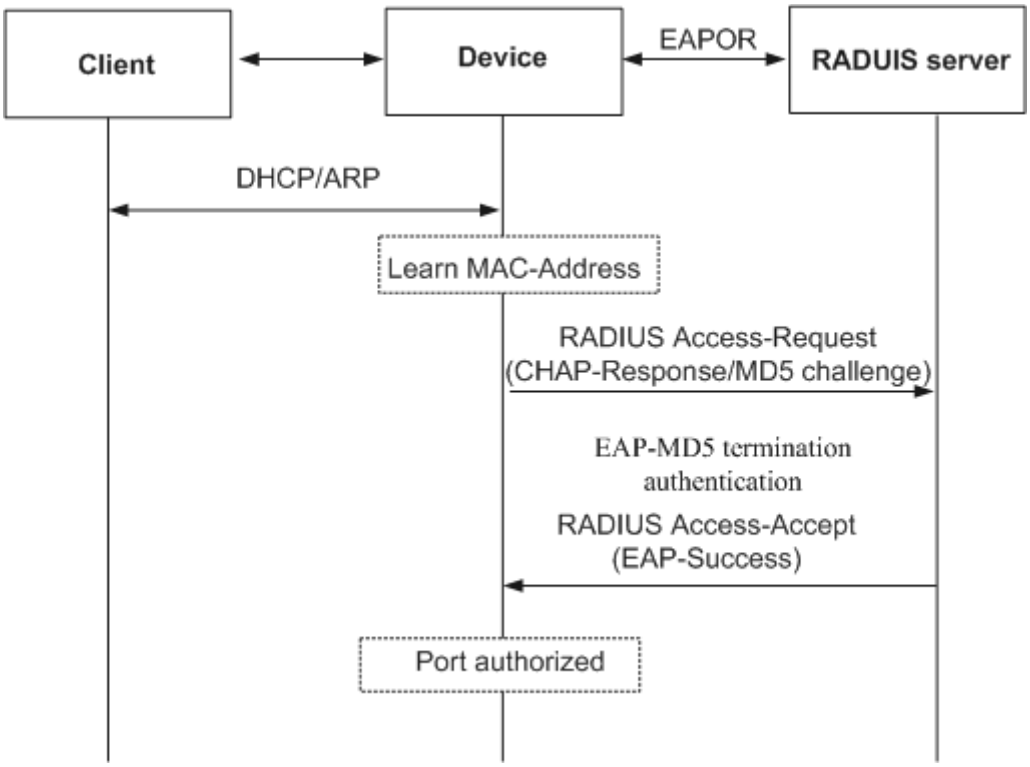
The sequence for selecting an authentication domain is as follows:

Domain specified in the fixed user name > Domain configured on the interface > Domain configured globally > Default domain

2.3.3 MAC Address Authentication Process

Figure 2-12 shows the MAC address authentication process.

Figure 2-12 MAC address authentication process



1. The device triggers MAC address authentication when detecting a DHCP/ARP packet.
2. The device encapsulates the user account (MAC address or fixed user name and password depending on the configuration) into the RADIUS Access-Request packet and sends the packet to the RADIUS server for authentication.
3. The device receives the authentication success packet and changes the interface state to authorized. The user can access the network through the interface.

2.3.4 MAC Address Authentication Timers

MAC address authentication timers include:

- Guest VLAN user re-authentication timer (guest-vlan reauthenticate-period): When a user is added to the guest VLAN, the device initiates re-authentication for the user at the interval set by guest-vlan reauthenticate-period. If re-authentication is successful, the user is removed from the guest VLAN.
- Offline detection timer (offline-detect): The device sends a detection packet to check whether a user is online. If the user does not respond within a detection period set by offline-detect, the device considers that the user is offline.

- Quiet timer (quiet-period): The device enters a quiet period set by quiet-period after a user fails to be authenticated. During the quiet period, the device does not process authentication requests from the user.
- Periodical re-authentication timer (reauthenticate-period): If the periodical re-authentication function is enabled on an interface, the device initiates re-authentication for online users on the interface at an interval set by reauthenticate-period.
- Server timeout timer (server-timeout): The device starts this timer after sending a RADIUS Access-Request packet to the authentication server. If the authentication server does not respond within the period set by server-timeout, the device resends the authentication request packet.

2.3.5 Terminal Access Control

Similar to 802.1x-based access control, MAC address authentication supports VLAN- and ACL-based access control. For details, see section 2.2.8 "802.1x Authentication Access Control."

MAC address authentication does not support restrict VLANs because there is no attack of spoofing user names in MAC address authentication. MAC address authentication only supports resource access control of guest VLANs and critical VLANs.

2.3.6 User Group Authorization

In an actual NAC network deployment, there are a lot of access users, but user types are limited. User rights are controlled based on user groups. After a user is authenticated, the authentication server delivers a user group for the user. Each user group can be associated with data forwarding and service processing rules to control the network access rights of users in the group.

2.4 Portal Authentication

2.4.1 Portal Authentication Overview

Portal authentication is also called web authentication. Generally, portal authentication websites are referred to as portal websites. When an unauthenticated user attempts to access the Internet, the device forces the user to log in to a specific site and the user can use services of the site for free. When the user wants to gain access to other information on the Internet, the user must be authenticated on a portal website. The user can actively access a known Portal authentication website and enter a user name and password for authentication, which is referred to as active authentication. If a user attempts to access other external networks through HTTP, the user is forced to access a Portal authentication website to start Portal authentication, which is referred to as forcible authentication.

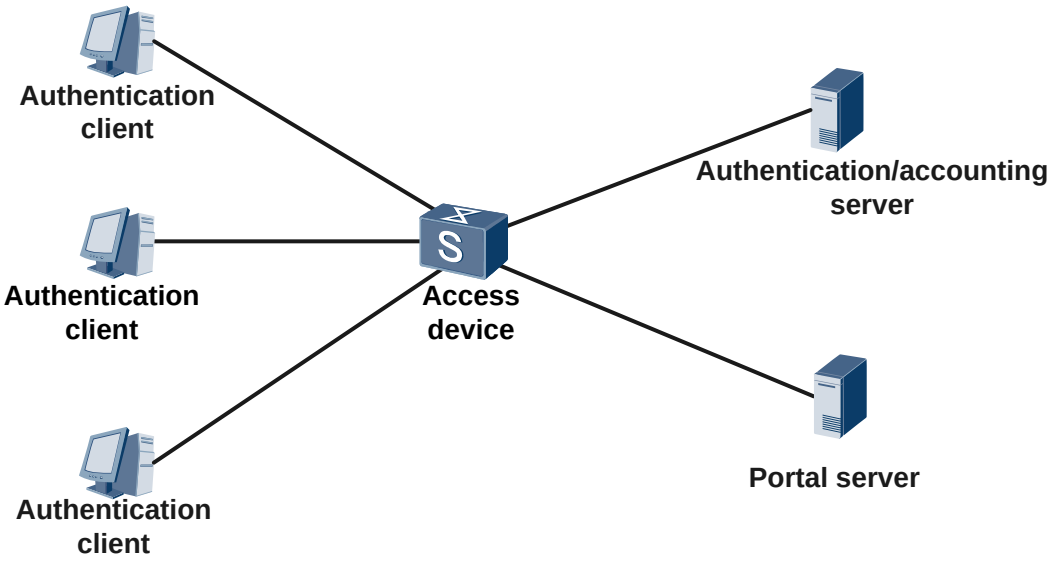
2.4.2 Portal Authentication System Architecture

A Portal server can be independent of an access device (an external Portal server), or integrated into the access device (a built-in Portal server).

Portal Authentication System Using an External Portal Server

As shown in Figure 2-13, typical networking of the Portal authentication system consists of four basic elements: authentication client, access device, Portal server, and authentication/accounting server.

Figure 2-13 Portal authentication system using an external Portal server

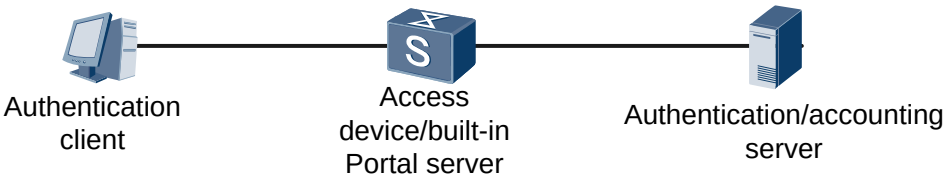


- Authentication client: a client system installed on a user terminal to function as a browser running HTTP/HTTPS protocol or a host running Portal client software.
- Access device: a broadband access device such as a switch or router, which provides the following functions:
  - Before authentication, it redirects all HTTP requests of the users in the authentication network segment to the Portal server.
  - During authentication, it interacts with the Portal server and authentication/accounting server to implement identity authentication/accounting.
  - After the authentication succeeds, it allows the users to access Internet resources authorized by the administrator.
- Portal server: a server system that receives authentication requests from the Portal client. It provides free portal services and an interface based on web authentication, and exchanges authentication information of the authentication client with the access device.
- Authentication/accounting server: interacts with the access device to implement user authentication and accounting.

Portal Authentication System Using a Built-in Portal Server

In the portal authentication system using a built-in Portal server, no external independent Portal server is used, and functions of the Portal server are implemented by the access device. In this case, the Portal authentication system includes only three basic elements: authentication client, access device, and authentication/accounting server, as shown in Figure 2-14.

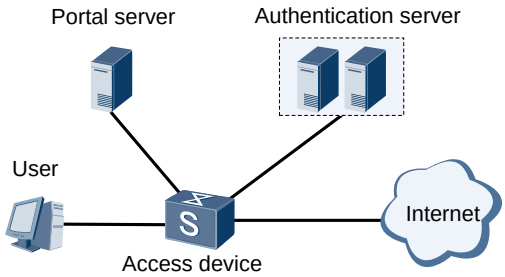
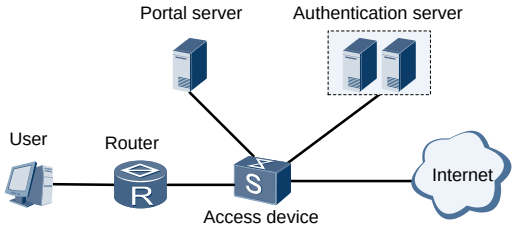
Figure 2-14 Portal authentication system using a built-in Portal server



2.4.3 Portal Authentication Modes

Portal authentication modes can be used on different networks. According to network layers for implementing Portal authentication on the network, Portal authentication is classified into Layer 2 authentication and Layer 3 authentication.

Table 2-1 Comparisons between Layer 2 authentication and Layer 3 authentication

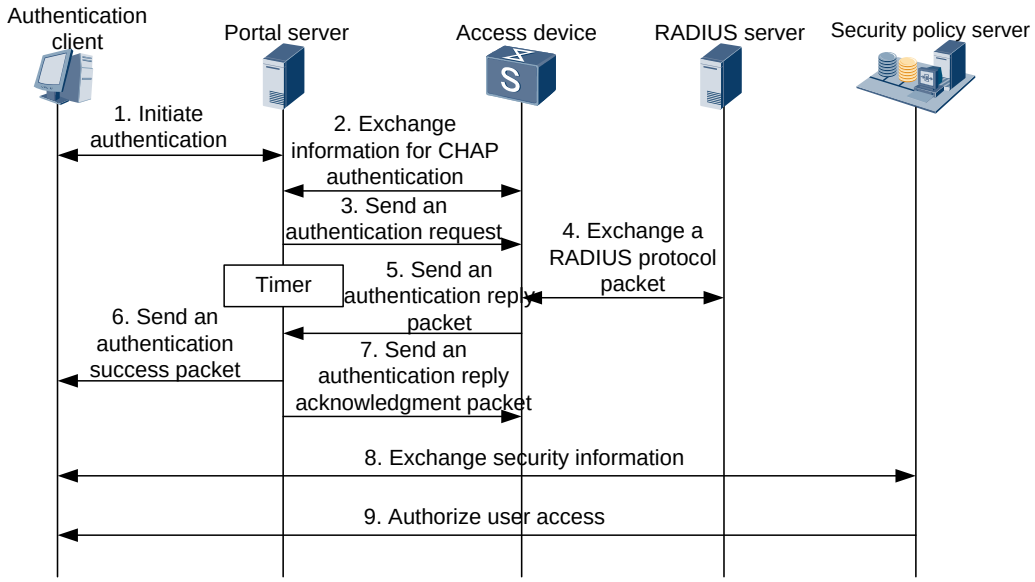
Auth Mode	Typical Network	Description
Layer 2 authentication		The authentication client and access device are either directly connected or have only Layer 2 devices between them. The device can learn users' MAC addresses and identify the users using their MAC addresses and IP addresses. On a network of this configuration, Layer 2 authentication should be used.
Layer 3 authentication		When the device is deployed at the aggregation or core layer, Layer 3 forwarding devices exist between the authentication client and device. The device may not obtain the MAC address of the authentication client. Therefore, an IP address uniquely identifies the user. On a network of this configuration, Layer 3 authentication should be used.

Layer 2 Authentication

The authentication client and access device are either directly connected or have only Layer 2 devices between them. The device can learn users' MAC addresses and identify the users using their MAC addresses and IP addresses. On a network of this configuration, Layer 2 authentication should be used.

Layer 2 authentication provides a simple authentication process with high security. However, users must be in the same network segment with the access device, which makes the networking less flexible. Figure 2-15 shows the packet interaction process when a user goes online in Layer 2 authentication.

Figure 2-15 Layer 2 Portal authentication process



1. A Portal user initiates an authentication request through HTTP. The access device allows the HTTP packet for accessing the Portal server or preset non-authentication network resources to pass through. The access device redirects the HTTP packet for accessing other addresses to the Portal server. The Portal server provides a web page for the user to enter the user name and password for authentication.
2. The Portal server exchanges information with the access device to implement CHAP authentication. If PAP authentication is adopted, the Portal service directly performs step 3 without exchanging information with the access device to implement PAP authentication.
3. The Portal server assembles the user name and password entered by the user into an authentication request packet, sends the packet to the access device, and starts a timer to wait for an authentication reply packet.
4. The access device exchanges a RADIUS protocol packet with the RADIUS server.
5. The access device sends an authentication reply packet to the Portal server.
6. The Portal server sends an authentication success packet to the client.
7. The Portal server sends an authentication reply acknowledgment packet to the access device.
8. The client exchanges security information with the security policy server. The security policy server evaluates the security of the access terminal. Items evaluated include

installing the anti-virus software installation, updating the virus library, installing unauthorized software, and upgrading operating system patches.

9. The security policy server allows the user to access authorized resources based on the user security. The access device uses the authorization information that is stored in the device to control user access.

Steps 8 and 9 constitute the interaction process for the Portal authentication extended function.

Layer 3 Authentication

When the device is deployed at the aggregation or core layer, Layer 3 forwarding devices exist between the authentication client and device. The device may not obtain the MAC address of the authentication client. Therefore, an IP address uniquely identifies the user. On a network of this configuration, Layer 3 authentication should be used. A packet processing procedure of Layer 3 authentication is the same as that of Layer 2 authentication. The networking structure of Layer 3 authentication is flexible, facilitating remote control. However, users can only be identified using their IP addresses, which results in poor security.

2.4.4 Detection and Keepalive Function of Portal Authentication

In an actual Portal authentication network, if communication between the device and Portal server is interrupted due to a network fault or Portal server failure, new Portal authentication users cannot go online and online Portal users cannot go offline normally. This brings great inconvenience to users, and meanwhile may cause inconsistent user information on the Portal server and device, leading to incorrect accounting.

With the Portal detection and keepalive function, even if the network fails or the Portal server cannot work properly, the device still allows users to use the network and have certain network access rights, and reports failures using logs and traps. Meanwhile, the user information synchronization mechanism ensures that the user information on the Portal server is the same as that on the device, preventing incorrect accounting.

2.4.5 User Group Authorization

In an actual NAC network deployment, there are a lot of access users, but user types are limited. User rights are controlled based on user groups. After a user is authenticated, the authentication server delivers a user group for the user. Each user group can be associated with data forwarding and service processing rules to control the network access rights of users in the group.

2.5 Combined Authentication

On a network with diversified clients, different access authentication modes are supported. Some clients (such as printers) support only MAC address authentication. Some hosts support 802.1x authentication because they have 802.1x client software installed. Some hosts require Portal authentication using web browsers.

802.1x authentication, MAC address authentication, and Portal authentication can be uniformly deployed on the user's interface connected to the device, so that users can select the proper authentication mode and access the network successfully.

Combined authentication is configured in either of the following methods:

- Enable any two or all of 802.1x authentication, MAC address authentication, and built-in Portal authentication on a Layer 2 interface.
- Enable MAC address authentication and external Portal authentication on a VLANIF interface.

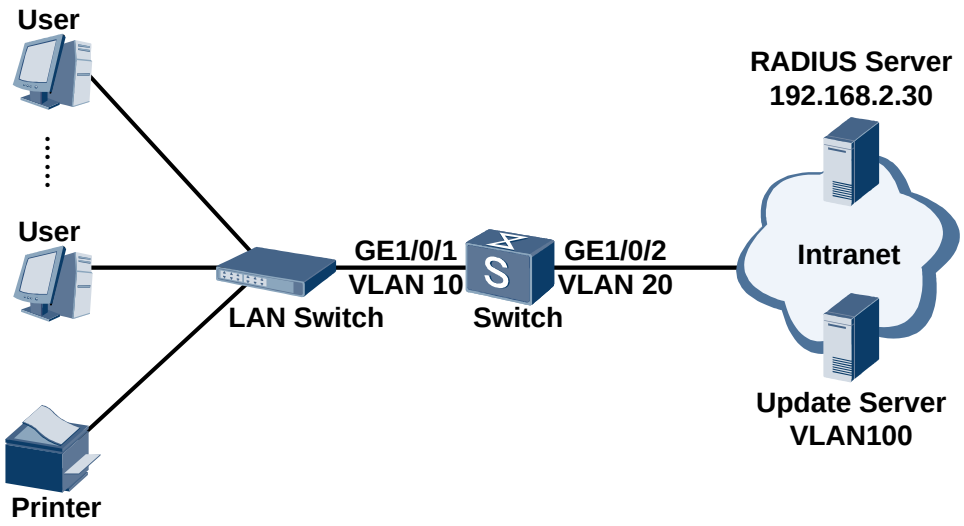
3 Application Scenarios

3.1 Example for Configuring 802.1x Authentication

3.1.1 Networking Requirements

As shown in Figure 3-1, lots of users in a company access the network through GE1/0/1 of the switch (used as an access device). After the network runs for a period of time, user attacks on the company intranet are detected. The administrator must control network access rights of user terminals to ensure network security. The switch allows user terminals to access network resources only after they are authenticated.

Figure 3-1 Networking diagram for configuring 802.1x authentication



3.1.2 Configuration Roadmap

To control the users' network access rights, the administrator can configure 802.1x authentication on the switch after the server with the IP address 192.168.2.30 is configured as the RADIUS server.

The configuration roadmap is as follows:

Step 1 Configure transparent transmission of EAP packets in 802.1x authentication on the LAN switch to ensure that EAP packets can be transparently transmitted to the switch.

Step 2 Create VLANs on the switch and configure the VLANs allowed by the interface to ensure network communication.

Step 3 Create and configure a RADIUS server template, an AAA scheme, and an authentication domain; bind the RADIUS server template and AAA scheme to the authentication domain. This step implements communication between the switch and RADIUS server.

Step 4 Configure 802.1x authentication.

1. Enable 802.1x authentication globally and on the interfaces.
2. Enable MAC address bypass authentication to authenticate the terminals (such as printers) that cannot have 802.1x authentication client software installed.
3. Configure an interface to allow the access of at most 200 802.1x authentication users, preventing excessive concurrent access users.
4. Set the maximum number of times that an authentication request packet is sent to a user to 3, avoiding repeated authentication.
5. Configure VLAN 100 as the guest VLAN so that users can access resources in the guest VLAN without authentication.

NOTE
This example only provides the configurations on the LAN switch and switch. The configurations on the RADIUS server are not provided here.

----End

3.1.3 Procedure

Step 1 Configure transparent transmission of EAP packets in 802.1x authentication on the LAN switch. The S5700 is used as the example of the LAN switch.

Define Layer 2 transparent transmission of EAP packets globally.

```
<LAN Switch> system-view
[LAN Switch] l2protocol-tunnel user-defined-protocol 802.1x protocol-mac
0180-c200-0003 group-mac 0100-0000-0002
```

Enable Layer 2 transparent transmission on the downlink interface connecting the LAN switch to users and the uplink interface connecting the LAN switch to the switch. Assume that GE0/0/1 connects the LAN switch to users. The configurations on GE0/0/1 are the same as those on other interfaces.

```
[LAN Switch] interface gigabitethernet 0/0/1
[LAN Switch-GigabitEthernet0/0/1] l2protocol-tunnel user-defined-protocol 802.1x
enable
[LAN Switch-GigabitEthernet0/0/1] bpdu enable
```

NOTE
Perform this step on the LAN switch and the following steps on the switch.

Step 2 Create VLANs and configure the VLANs allowed by the interface to ensure network communication.

#Create VLAN 10 and VLAN 20.

```
<Quidway> system-view
```

```
[Quidway] vlan batch 10 20
```

On the switch, configure GE1/0/1 connecting to users as a trunk interface and add GE1/0/1 to VLAN 10.

```
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] port link-type trunk
[Quidway-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[Quidway-GigabitEthernet1/0/1] quit
```

NOTE

Configure the interface type and VLANs based on the site requirements. In this example, users are added to VLAN 10.

On the switch, configure GE1/0/2 connecting to the uplink network as an access interface and add GE1/0/2 to VLAN 20.

```
[Quidway] interface gigabitethernet 1/0/2
[Quidway-GigabitEthernet1/0/2] port link-type access
[Quidway-GigabitEthernet1/0/2] port default vlan 20
[Quidway-GigabitEthernet1/0/2] quit
```

Create VLANIF10 and VLANIF20 and assign IP addresses to the VLANIF interfaces so that user terminals, Switch, and internal devices on the enterprise network can set up routes. In this example, the IP address of VLANIF10 is 192.168.1.20/24 and the IP address of VLANIF20 is 192.168.2.29/24.

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 192.168.1.20 24
[Quidway-Vlanif10] quit
[Quidway] interface vlanif 20
[Quidway-Vlanif20] ip address 192.168.2.29 24
[Quidway-Vlanif20] quit
```

Step 3 Create and configure a RADIUS server template, an AAA scheme, and an authentication domain.

Create and configure a RADIUS server template **rd1**.

```
[Quidway] radius-server template rd1
[Quidway-radius-rd1] radius-server authentication 192.168.2.30 1812
[Quidway-radius-rd1] radius-server shared-key cipher hello
[Quidway-radius-rd1] radius-server retransmit 2
[Quidway-radius-rd1] quit
```

Create an AAA scheme **abc** and set the authentication mode to RADIUS.

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme abc
[Quidway-aaa-authen-abc] authentication-mode radius
[Quidway-aaa-authen-abc] quit
```

Create an authentication domain **isp1**, and bind the AAA scheme **abc** and RADIUS server template **rd1** to the domain **isp1**.

```
[Quidway-aaa] domain isp1
[Quidway-aaa-domain-isp1] authentication-scheme abc
[Quidway-aaa-domain-isp1] radius-server rd1
[Quidway-aaa-domain-isp1] quit
[Quidway-aaa] quit
```

Configure the global default domain **isp1**. During access authentication, enter a user name in the format *user*@isp1 to perform AAA authentication in the domain **isp1**. If the user name does not contain the domain name or the contained domain name does not exist, the user is authenticated in the default domain.

```
[Quidway] domain isp1
```

Step 4 Configure 802.1x authentication.

Enable 802.1x authentication globally and on an interface.

```
[Quidway] dot1x enable
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] dot1x enable
```

Configure MAC address bypass authentication.

```
[Quidway-GigabitEthernet1/0/1] dot1x mac-bypass
```

Set the maximum number of concurrent access users for 802.1x authentication to 200 on an interface.

```
[Quidway-GigabitEthernet1/0/1] dot1x max-user 200
[Quidway-GigabitEthernet1/0/1] quit
```

Set the maximum number of times that an authentication request packet is sent to the user to 3.

```
[Quidway] dot1x retry 3
```

Configure VLAN 100 as the guest VLAN.

```
[Quidway] authentication guest-vlan 100 interface GigabitEthernet 1/0/1
```

Step 5 Check the 802.1x configuration.

```
<Quidway> display dot1x interface gigabitethernet 1/0/1
 GigabitEthernet1/0/1 status: UP  802.1x protocol is Enabled[mac-bypass]
  Port control type is Auto
  Authentication method is MAC-based
  Reauthentication is disabled
  Maximum users: 200
  Current users: 0
  There is no fast deploy user on the interface.
  Guest VLAN is not effective
  Critical VLAN is disabled
  Restrict VLAN is disabled

  Authentication Success: 0         Failure : 0
  EAPOL Packets: TX     : 0         RX      : 0
  Sent     EAPOL Request/Identity Packets   : 0
           EAPOL Request/Challenge Packets  : 0
           Multicast Trigger Packets        : 0
           EAPOL Success Packets            : 0
           EAPOL Failure Packets            : 0
  Received  EAPOL Start Packets             : 0
           EAPOL Logoff Packets             : 0
           EAPOL Response/Identity Packets  : 0
           EAPOL Response/Challenge Packets : 0
```

----End

3.1.4 Configuration Files

Configuration file of the LAN switch

```
#
l2protocol-tunnel user-defined-protocol 802.1x protocol-mac 0180-c200-0003 group-mac
0100-0000-0002
#
interface GigabitEthernet0/0/1
 l2protocol-tunnel user-defined-protocol 802.1x enable
```

Configuration file of the switch

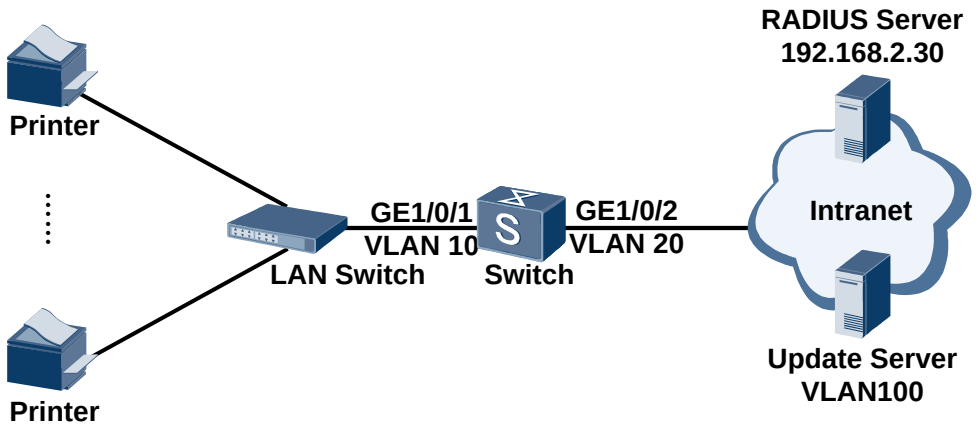
```
#
vlan batch 10 20 100
#
domain isp1
#
dot1x enable
dot1x retry 3
#
radius-server template rd1
 radius-server shared-key cipher %$%$lrWRXXUmJ/5W\uBqID/6EULC%$%$
 radius-server authentication 192.168.2.30 1812
 radius-server retransmit 2
#
aaa
 authentication-scheme abc
  authentication-mode radius
 domain isp1
  authentication-scheme abc
  radius-server rd1
#
interface Vlanif10
 ip address 192.168.1.20 255.255.255.0
#
interface Vlanif20
 ip address 192.168.2.29 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 dot1x mac-bypass
 dot1x max-user 200
 authentication guest-vlan 100
#
interface GigabitEthernet1/0/2
 port link-type access
 port default vlan 20
#
return
```

3.2 Example for Configuring MAC Address Authentication

3.2.1 Networking Requirements

As shown in Figure 3-2, lots of printers in a company access the network through GE1/0/1 of the switch (used as an access device). After the network runs for a period of time, the administrator controls the network access rights of the printers to improve network security. The switch allows the printers to access network resources only after they are authenticated.

Figure 3-2 Networking diagram for configuring MAC address authentication



3.2.2 Configuration Roadmap

The configuration roadmap is as follows:

Step 1 Create VLANs on the switch and configure the VLANs allowed by the interface to ensure network communication.

Step 2 Create and configure a RADIUS server template, an AAA scheme, and an authentication domain; bind the RADIUS server template and AAA scheme to the authentication domain. This step implements communication between the switch and RADIUS server.

Step 3 Configure MAC address authentication.

1. Enable MAC address authentication globally and on the interfaces.
2. Set the maximum number of MAC address authentication users allowed to access an interface to 100, preventing excessive concurrent access users.
3. Configure VLAN 100 as the guest VLAN so that users can access resources in the guest VLAN without authentication.

NOTE
This example only provides the configurations on the switch. The configurations on the LAN switch and RADIUS server are not provided here.

----End

3.2.3 Procedure

Step 1 Create VLANs and configure the VLANs allowed by the interface to ensure network communication.

#Create VLAN 10 and VLAN 20.

```
<Quidway> system-view
[Quidway] vlan batch 10 20
```

On the switch, configure GE1/0/1 connecting to users as a trunk interface and add GE1/0/1 to VLAN 10.

```
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] port link-type trunk
[Quidway-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[Quidway-GigabitEthernet1/0/1] quit
```

NOTE

Configure the interface type and VLANs based on the site requirements. In this example, users are added to VLAN 10.

On the switch, configure GE1/0/2 connecting to the uplink network as an access interface and add GE1/0/2 to VLAN 20.

```
[Quidway] interface gigabitethernet 1/0/2
[Quidway-GigabitEthernet1/0/2] port link-type access
[Quidway-GigabitEthernet1/0/2] port default vlan 20
[Quidway-GigabitEthernet1/0/2] quit
```

Create VLANIF10 and VLANIF20 and assign IP addresses to the VLANIF interfaces so that user terminals, Switch, and internal devices on the enterprise network can set up routes. In this example, the IP address of VLANIF10 is 192.168.1.20/24 and the IP address of VLANIF20 is 192.168.2.29/24.

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 192.168.1.20 24
[Quidway-Vlanif10] quit
[Quidway] interface vlanif 20
[Quidway-Vlanif20] ip address 192.168.2.29 24
[Quidway-Vlanif20] quit
```

Step 2 Create and configure a RADIUS server template, an AAA scheme, and an authentication domain.

Create and configure a RADIUS server template **rd1**.

```
[Quidway] radius-server template rd1
[Quidway-radius-rd1] radius-server authentication 192.168.2.30 1812
[Quidway-radius-rd1] radius-server shared-key cipher hello
[Quidway-radius-rd1] radius-server retransmit 2
[Quidway-radius-rd1] quit
```

Create an AAA scheme **abc** and set the authentication mode to RADIUS.

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme abc
[Quidway-aaa-authen-abc] authentication-mode radius
[Quidway-aaa-authen-abc] quit
```

Create an authentication domain **isp1**, and bind the AAA scheme **abc** and RADIUS server template **rd1** to the domain **isp1**.

```
[Quidway-aaa] domain isp1
[Quidway-aaa-domain-isp1] authentication-scheme abc
[Quidway-aaa-domain-isp1] radius-server rd1
[Quidway-aaa-domain-isp1] quit
[Quidway-aaa] quit
```

Configure the global default domain **isp1**. During access authentication, enter a user name in the format *user*@isp1 to perform AAA authentication in the domain **isp1**. If the user name does not contain the domain name or the contained domain name does not exist, the user is authenticated in the default domain.

```
[Quidway] domain isp1
```

Step 3 Configure MAC address authentication.

Enable MAC address authentication globally and on the interface.

```
[Quidway] mac-authen
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] mac-authen
```

#Set the maximum number of concurrent MAC authentication access users to 100 on the interface.

```
[Huawei-Ethernet1/0/1] mac-authen max-user 100
[Huawei-Ethernet1/0/1] quit
```

Configure VLAN 100 as the guest VLAN for MAC address authentication.

```
[Quidway] authentication guest-vlan 100 interface gigabitethernet 1/0/1
```

Step 4 Run the **display mac-authen interface** command to check the configuration of MAC address authentication.

```
[Quidway] display mac-authen interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 state: UP.  MAC address authentication is enabled
  Maximum users: 100
  Current users: 0
  Authentication Success: 0, Failure: 0
  Guest VLAN 100 is not effective
  Critical VLAN is disabled
```

----End

3.2.4 Configuration Files

Configuration file of the switch

```
#
vlan batch 10 20 100
#
domain isp1
#
mac-authen
#
radius-server template rd1
```

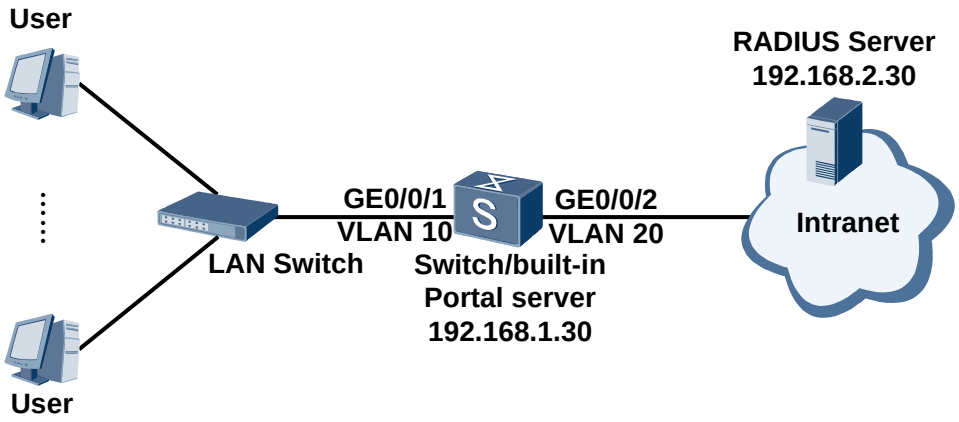
```
 radius-server shared-key cipher %$%$lrWRXXUmJ/5W\uBqID/6EULC%$%$
 radius-server authentication 192.168.2.30 1812
 radius-server retransmit 2
#
aaa
 authentication-scheme abc
  authentication-mode radius
 domain isp1
  authentication-scheme abc
  radius-server rd1
#
interface Vlanif10
 ip address 192.168.1.20 255.255.255.0
#
interface Vlanif20
 ip address 192.168.2.29 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 authentication guest-vlan 100
 mac-authen
 mac-authen max-user 100
#
interface GigabitEthernet1/0/2
 port link-type access
 port default vlan 20
#
return
```

3.3 Example for Configuring Built-in Portal Authentication

3.3.1 Networking Requirements

As shown in Figure 3-3, lots of users in a company access the network through GE0/0/1 of the switch (used as an access device). After the network runs for a period of time, attacks are detected. The administrator must control network access rights of user terminals to ensure network security. The switch allows user terminals to access network resources only after they are authenticated.

Figure 3-3 Networking diagram for configuring built-in Portal authentication



3.3.2 Configuration Roadmap

To control the users' network access rights, the administrator can configure Portal authentication on the switch after the server with the IP address 192.168.2.30 is configured as the RADIUS server. Due to limited device resources, the administrator uses the built-in Portal server and configures the IP address 192.168.1.30 of a loopback interface on the switch as the IP address of the built-in Portal server.

The configuration roadmap is as follows:

Step 1 Create VLANs on the switch and configure the VLANs allowed by the interface to ensure network communication.

Step 2 Create and configure a RADIUS server template, an AAA scheme, and an authentication domain; bind the RADIUS server template and AAA scheme to the authentication domain. This step implements communication between the switch and RADIUS server.

Step 3 Configure built-in Portal authentication.

1. Configure the IP address of the built-in Portal server so that the switch can exchange information with the built-in Portal server.
2. Enable Portal authentication to authenticate access users.

NOTE

Only the S5700EI, S5700HI, S5710HI, and S5710EI support the built-in Portal authentication function.

This example only provides the configurations on the switch. The configurations on the LAN switch and RADIUS server are not provided here.

----End

3.3.3 Procedure

Step 1 Create VLANs and configure the VLANs allowed by the interface to ensure network communication.

#Create VLAN 10 and VLAN 20.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10 20
```

On the switch, configure GE0/0/1 connecting to users as a trunk interface and add GE0/0/1 to VLAN 10.

```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[HUAWEI-GigabitEthernet0/0/1] quit
```

NOTE

Configure the interface type and VLANs based on the site requirements. In this example, users are added to VLAN 10.

On the switch, configure GE0/0/2 connecting to the uplink network as an access interface and add GE0/0/2 to VLAN 20.

```
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] port link-type access
[HUAWEI-GigabitEthernet0/0/2] port default vlan 20
[HUAWEI-GigabitEthernet0/0/2] quit
```

Create VLANIF10 and VLANIF20 and assign IP addresses to the VLANIF interfaces so that user terminals, Switch, and internal devices on the enterprise network can set up routes. In this example, the IP address of VLANIF10 is 192.168.1.20/24 and the IP address of VLANIF20 is 192.168.2.29/24.

```
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ip address 192.168.1.20 24
[HUAWEI-Vlanif10] quit
[HUAWEI] interface vlanif 20
[HUAWEI-Vlanif20] ip address 192.168.2.29 24
[HUAWEI-Vlanif20] quit
```

Step 2 Create and configure a RADIUS server template, an AAA scheme, and an authentication domain.

Create and configure a RADIUS server template **rd1**.

```
[HUAWEI] radius-server template rd1
[HUAWEI-radius-rd1] radius-server authentication 192.168.2.30 1812
[HUAWEI-radius-rd1] radius-server shared-key cipher hello
[HUAWEI-radius-rd1] radius-server retransmit 2
[HUAWEI-radius-rd1] quit
```

Create an AAA scheme **abc** and set the authentication mode to RADIUS.

```
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme abc
[HUAWEI-aaa-authen-abc] authentication-mode radius
[HUAWEI-aaa-authen-abc] quit
```

Create an authentication domain **isp1**, and bind the AAA scheme **abc** and RADIUS server template **rd1** to the domain **isp1**.

```
[HUAWEI-aaa] domain isp1
[HUAWEI-aaa-domain-isp1] authentication-scheme abc
[HUAWEI-aaa-domain-isp1] radius-server rd1
[HUAWEI-aaa-domain-isp1] quit
[HUAWEI-aaa] quit
```

Configure the global default domain **isp1**. During access authentication, enter a user name in the format *user*@isp1 to perform AAA authentication in the domain **isp1**. If the user name does not contain the domain name or the contained domain name does not exist, the user is authenticated in the default domain.

```
[HUAWEI] domain isp1
```

Step 3 Configure built-in Portal authentication.

Create a loopback interface and configure an IP address for the loopback interface.

```
[HUAWEI] interface LoopBack 10
[HUAWEI-LoopBack10] ip address 192.168.1.30 32
[HUAWEI-LoopBack10] quit
```

Configure the IP address for the built-in Portal server.

```
[HUAWEI] portal local-server ip 192.168.1.30
```

Configure the SSL policy loaded on the built-in Portal authentication page.

```
[HUAWEI] ssl policy huawei
[HUAWEI -ssl-policy-huawei] certificate load pem-cert cert_rsa_cert.pem key-pair rsa
key-file cert_rsa_key.pem auth-code cipher 123456@abc
[HUAWEI -ssl-policy-huawei] quit
```

NOTE

Before loading a certificate for the SSL policy, ensure that the certificate file and key pair file have been stored on the device; otherwise, certificate loading will fail.

Enable built-in Portal authentication.

```
[HUAWEI] portal local-server https ssl-policy huawei
[HUAWEI] portal local-server enable interface gigabitethernet 0/0/1
```

Step 4 Check the parameters of the configured built-in Portal server.

```
<HUAWEI> display portal local-server
Portal local-server config:
  server status            : enable
  server ip                : 192.168.1.30
  authentication method    : chap
  protocol                 : https
  https ssl-policy         : huawei
```

----End

3.3.4 Configuration Files

Configuration file of the switch

```
#
vlan batch 10 20
#
domain isp1
#
portal local-server ip 192.168.1.30
portal local-server https ssl-policy huawei
#
radius-server template rd1
```

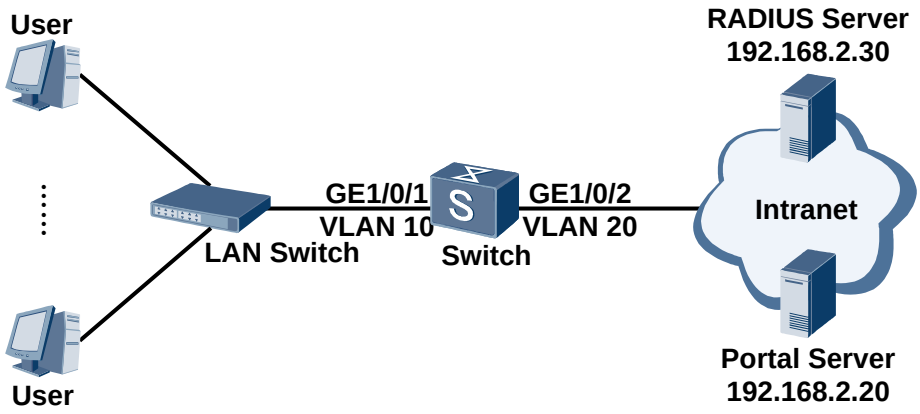
```
 radius-server shared-key cipher %$%$lrWRXXUmJ/5W\uBqID/6EULC%$%$
 radius-server authentication 192.168.2.30 1812
 radius-server retransmit 2
#
aaa
 authentication-scheme abc
  authentication-mode radius
 domain isp1
  authentication-scheme abc
  radius-server rd1
#
interface Vlanif10
 ip address 192.168.1.20 255.255.255.0
#
interface Vlanif20
 ip address 192.168.2.29 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 portal local-server enable
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 20
#
interface LoopBack10
 ip address 192.168.1.30 255.255.255.255
#
ssl policy huawei
 certificate load pem-cert cert_rsa_cert.pem key-pair rsa key-file cert_rsa_key.pem
auth-code cipher %$%$UR;Q$+r`=!1TvU,0.H,S!9"<%$%$
#
return
```

3.4 Example for Configuring External Portal Authentication

3.4.1 Networking Requirements

As shown in Figure 3-4, lots of users in a company access the network through GE1/0/1 of the switch (used as an access device). After the network runs for a period of time, attacks are detected. The administrator must control network access rights of user terminals to ensure network security. The switch allows user terminals to access network resources only after they are authenticated.

Figure 3-4 Networking diagram for configuring external Portal authentication



3.4.2 Configuration Roadmap

To control the users' network access rights, the administrator can configure Portal authentication on the switch after the server with the IP address 192.168.2.30 is used as the RADIUS server, and configure the IP address 192.168.2.20 as the IP address of the Portal server.

The configuration roadmap is as follows:

Step 1 Create VLANs on the switch and configure the VLANs allowed by the interface to ensure network communication.

Step 2 Create and configure a RADIUS server template, an AAA scheme, and an authentication domain; bind the RADIUS server template and AAA scheme to the authentication domain. This step implements communication between the switch and RADIUS server.

Step 3 Configure Portal Authentication.

1. Create and configure a Portal server template to ensure information exchange between the device and Portal server.
2. Enable Portal authentication to authenticate access users.
3. Configure a shared key that the device uses to exchange information with the Portal server to improve communication security.
4. Configure the maximum number of concurrent Portal authentication users to prevent excess concurrent users.
5. Configure the offline detection interval for Portal authentication users to ensure that the device deletes information about offline users in real time.
6. Configure the detection and keepalive function of Portal authentication so that users can still access networks when the Portal server is faulty.

NOTE

This example only provides the configurations on the switch. The configurations on the LAN switch and RADIUS server are not provided here.

----End

3.4.3 Procedure

Step 1 Create VLANs and configure the VLANs allowed by the interface to ensure network communication.

#Create VLAN 10 and VLAN 20.

```
<Quidway> system-view
[Quidway] vlan batch 10 20
```

On the switch, configure GE1/0/1 connecting to users as a trunk interface and add GE1/0/1 to VLAN 10.

```
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] port link-type trunk
[Quidway-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[Quidway-GigabitEthernet1/0/1] quit
```

NOTE

Configure the interface type and VLANs based on the site requirements. In this example, users are added to VLAN 10.

On the switch, configure GE1/0/2 connecting to the uplink network as an access interface and add GE1/0/2 to VLAN 20.

```
[Quidway] interface gigabitethernet 1/0/2
[Quidway-GigabitEthernet1/0/2] port link-type access
[Quidway-GigabitEthernet1/0/2] port default vlan 20
[Quidway-GigabitEthernet1/0/2] quit
```

Create VLANIF10 and VLANIF20 and assign IP addresses to the VLANIF interfaces so that user terminals, Switch, and internal devices on the enterprise network can set up routes. In this example, the IP address of VLANIF10 is 192.168.1.20/24 and the IP address of VLANIF20 is 192.168.2.29/24.

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 192.168.1.20 24
[Quidway-Vlanif10] quit
[Quidway] interface vlanif 20
[Quidway-Vlanif20] ip address 192.168.2.29 24
[Quidway-Vlanif20] quit
```

Step 2 Create and configure a RADIUS server template, an AAA scheme, and an authentication domain.

Create and configure a RADIUS server template **rd1**.

```
[Quidway] radius-server template rd1
[Quidway-radius-rd1] radius-server authentication 192.168.2.30 1812
[Quidway-radius-rd1] radius-server shared-key cipher hello
[Quidway-radius-rd1] radius-server retransmit 2
[Quidway-radius-rd1] quit
```

Create an AAA scheme **abc** and set the authentication mode to RADIUS.

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme abc
[Quidway-aaa-authen-abc] authentication-mode radius
[Quidway-aaa-authen-abc] quit
```

Create an authentication domain **isp1**, and bind the AAA scheme **abc** and RADIUS server template **rd1** to the domain **isp1**.

```
[Quidway-aaa] domain isp1
[Quidway-aaa-domain-isp1] authentication-scheme abc
[Quidway-aaa-domain-isp1] radius-server rd1
[Quidway-aaa-domain-isp1] quit
[Quidway-aaa] quit
```

Configure the global default domain **isp1**. During access authentication, enter a user name in the format *user*@isp1 to perform AAA authentication in the domain **isp1**. If the user name does not contain the domain name or the contained domain name does not exist, the user is authenticated in the default domain.

```
[Quidway] domain isp1
```

Step 3 Configure Portal authentication.

Create and configure a Portal server template **abc**.

```
[Quidway] web-auth-server abc
[Quidway-web-auth-server-abc] server-ip 192.168.2.20
[Quidway-web-auth-server-abc] quit
```

Enable Portal Authentication.

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] web-auth-server abc direct
[Quidway-Vlanif10] quit
```

Set the shared key that the device uses to exchange information with the Portal server to 12345 in cipher text.

```
[Quidway] web-auth-server abc
[Quidway-web-auth-server-abc] shared-key cipher 12345
[Quidway-web-auth-server-abc] quit
```

Set the maximum number of concurrent Portal authentication users to 100.

```
[Quidway] portal max-user 100
```

Set the offline detection interval for Portal authentication users to 500s.

```
[Quidway] portal timer offline-detect 500
```

Configure the detection and keepalive function of Portal authentication.

```
[Quidway] web-auth-server abc
[Quidway-web-auth-server-abc] server-detect action log
[Quidway-web-auth-server-abc] user-sync
[Quidway-web-auth-server-abc] quit
[Quidway] quit
```

Step 4 Verify the configuration.

Run the **display portal** command to check the Portal parameters that are set in the system view.

```
<Quidway> display portal
 Portal timer offline-detect length:500
 Portal max-user number:100
```

```
 Vlanif10 protocol status: up, web-auth-server layer2(direct)
```

Run the **display portal interface** command to check the Portal parameters that are set in the VLANIF interface view.

```
<Quidway> display portal interface vlanif 10

 Vlanif10 protocol status: up, web-auth-server layer2(direct)
```

Run the **display web-auth-server configuration** command to check the configuration of the Portal server.

```
<Quidway> display web-auth-server configuration
  Listening port        : 2000
  Portal                : version 1, version 2
  Include reply message : enabled
  ------------------------------------------------------------------------
  Web-auth-server Name : abc
  IP-address           : 192.168.3.20
  Shared-key           : %$%$qqZ$ZM:$i&]T9sF7KE~Xi%yp%$%$
  Source-IP            : -
  Port / PortFlag      : 50100 / NO
  URL                  :
  Redirection          : Enable
  Sync                 : Enable
  Sync Seconds         : 300
  Sync Max-times       : 3
  Detect               : Enable
  Detect Seconds       : 60
  Detect Max-times     : 3
  Detect Critical-num  : 0
  Detect Action        : log
  Bound Vlanif         : 10

  ------------------------------------------------------------------------
  1 Web authentication server(s) in total
```

----End

3.4.4 Configuration Files

Configuration file of the switch

```
#
vlan batch 10 20
#
domain isp1
#
portal max-user 100
portal timer offline-detect 500
#
web-auth-server abc
 server-ip 192.168.2.20
 port 50100
 shared-key cipher %$%$9|vQ3(`Js#[:m\+~xK:W7cZQ%$%$
 server-detect interval 60 max-times 3 critical-num 0 action log
 user-sync
```

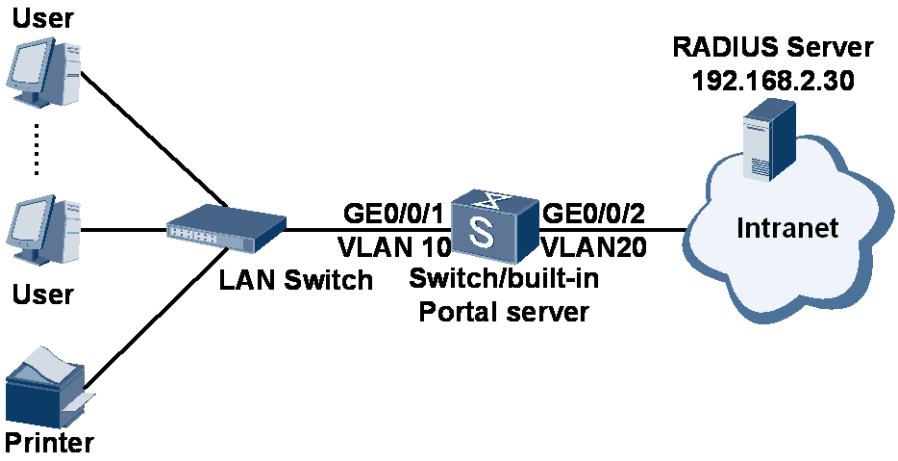
```
#
radius-server template rd1
 radius-server shared-key cipher %$%$lrWRXXUmJ/5W\uBqID/6EULC%$%$
 radius-server authentication 192.168.2.30 1812
 radius-server retransmit 2
#
aaa
 authentication-scheme abc
  authentication-mode radius
 domain isp1
  authentication-scheme abc
  radius-server rd1
#
interface Vlanif10
 ip address 192.168.1.20 255.255.255.0
 web-auth-server abc direct
#
interface Vlanif20
 ip address 192.168.2.29 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet1/0/2
 port link-type access
 port default vlan 20
#
return
```

3.5 Example for Configuring Combined Authentication Based on Layer 2 Physical Interfaces

3.5.1 Networking Requirements

As shown in Figure 3-5, lots of users in a company access the network through GE0/0/1 of the switch (used as an access device). To effectively manage the users accessing the network, the company requires that only authenticated users can access the network. In addition, as access users use various types of terminals, the administrator needs to configure combined authentication to control user access.

Figure 3-5 Networking diagram for configuring combined authentication



3.5.2 Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and configure the VLANs allowed by the interface to ensure network communication.
2. Create and configure a RADIUS server template, an AAA scheme, and an authentication domain; bind the RADIUS server template and AAA scheme to the authentication domain. This step implements communication between the switch and RADIUS server.
3. Configure built-in Portal authentication so that user terminals can access networks in Portal authentication mode.
4. Configure 802.1x authentication so that user terminals can access networks in 802.1x authentication mode.
5. Configure MAC address authentication so that user terminals can access networks in MAC address authentication mode.

NOTE

Only the S5700EI, S5700HI, S5710HI, and S5710EI support the Portal authentication function.

This example only provides the configurations on the switch. The configurations on the LAN switch and RADIUS server are not provided here.

3.5.3 Procedure

Step 1 Create VLANs and configure the VLANs allowed by the interface to ensure network communication.

#Create VLAN 10 and VLAN 20.

```
<Quidway> system-view
[Quidway] vlan batch 10 20
```

Step 2 # On the switch, configure GE0/0/1 connecting to users as a trunk interface and add GE0/0/1 to VLAN 10.

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type trunk
[Quidway-GigabitEthernet0/0/1] port trunk allow-pass vlan 10 20
```

```
[Quidway-GigabitEthernet0/0/1] quit
```

NOTE

Configure the interface type and VLANs based on the site requirements. In this example, users are added to VLAN 10.

On the switch, configure GE0/0/2 connecting to the uplink network as an access interface and add GE0/0/2 to VLAN 20.

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type access
[Quidway-GigabitEthernet0/0/2] port default vlan 20
[Quidway-GigabitEthernet0/0/2] quit
```

Create VLANIF10 and VLANIF20 and assign IP addresses to the VLANIF interfaces so that user terminals, Switch, and internal devices on the enterprise network can set up routes. In this example, the IP address of VLANIF10 is 192.168.1.20/24 and the IP address of VLANIF20 is 192.168.2.29/24.

```
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ip address 192.168.1.20 24
[HUAWEI-Vlanif10] quit
[HUAWEI] interface vlanif 20
[HUAWEI-Vlanif20] ip address 192.168.2.29 24
[HUAWEI-Vlanif20] quit
```

Step 3 Create and configure a RADIUS server template, an AAA scheme, and an authentication domain.

Create and configure a RADIUS server template **rd1**.

```
[Quidway] radius-server template rd1
[Quidway-radius-rd1] radius-server authentication 192.168.2.30 1812
[Quidway-radius-rd1] radius-server shared-key cipher hello
[Quidway-radius-rd1] radius-server retransmit 2
[Quidway-radius-rd1] quit
```

Create an AAA scheme **abc** and set the authentication mode to RADIUS.

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme abc
[Quidway-aaa-authen-abc] authentication-mode radius
[Quidway-aaa-authen-abc] quit
```

Create an authentication domain **isp1**, and bind the AAA scheme **abc** and RADIUS server template **rd1** to the domain **isp1**.

```
[Quidway-aaa] domain isp1
[Quidway-aaa-domain-isp1] authentication-scheme abc
[Quidway-aaa-domain-isp1] radius-server rd1
[Quidway-aaa-domain-isp1] quit
[Quidway-aaa] quit
```

Configure the global default domain **isp1**. During access authentication, enter a user name in the format *user*@isp1 to perform AAA authentication in the domain **isp1**. If the user name does not contain the domain name or the contained domain name does not exist, the user is authenticated in the default domain.

```
[Quidway] domain isp1
```

Step 4 Configure built-in Portal authentication.

Create a loopback interface and configure an IP address for the loopback interface.

```
[HUAWEI] interface loopback 10
[HUAWEI-LoopBack10] ip address 192.168.1.30 32
[HUAWEI-LoopBack10] quit
```

Configure the IP address for the built-in Portal server.

```
[HUAWEI] portal local-server ip 192.168.1.30
```

Configure the SSL policy loaded on the built-in Portal authentication page.

```
[HUAWEI] ssl policy huawei
[HUAWEI-ssl-policy-huawei] certificate load pem-cert cert_rsa_cert.pem key-pair rsa
key-file cert_rsa_key.pem auth-code cipher 123456@abc
[HUAWEI-ssl-policy-huawei] quit
```

NOTE

Before loading a certificate for the SSL policy, ensure that the certificate file and key pair file have been stored on the device; otherwise, certificate loading will fail.

Enable built-in Portal authentication.

```
[HUAWEI] portal local-server https ssl-policy huawei
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] portal local-server enable
[HUAWEI-GigabitEthernet0/0/1] quit
```

Step 5 Configure 802.1x authentication.

Enable the 802.1x authentication globally.

```
[HUAWEI] dot1x enable
```

Enable 802.1x authentication on the interface.

```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x enable
[HUAWEI-GigabitEthernet0/0/1] quit
```

Step 6 Configure MAC address authentication.

Enable MAC address authentication globally.

```
[HUAWEI] mac-authen
```

Enable MAC address authentication on the interface.

```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-authen
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] quit
```

Step 7 Verify the configuration.

Check the parameters of the configured built-in Portal server.

```
<HUAWEI> display portal local-server
 Portal local-server config:
  server status           : enable
  server ip               : 192.168.1.30
  authentication method   : chap
```

```
 protocol               : https
 https ssl-policy       : huawei
```

Check the 802.1x configuration.

```
<HUAWEI> display dot1x
 Global 802.1x is Enabled
 Authentication method is CHAP
 Max users: 1024
 Current users: 0
 DHCP-trigger is Disabled
 Handshake is Disabled
 Quiet function is Enabled
 Parameter set:Handshake Period   15s   Reauthen Period   3600s
             Client Timeout       30s   Server Timeout     30s
             Quiet Period          60s   Quiet-times        1
 dot1x URL: Not configed.
 Free-ip configuration(IP/mask): Not configed.

GigabitEthernet0/0/1 status: UP  802.1x protocol is Enabled
 Port control type is Auto
 Authentication method is MAC-based
 Reauthentication is disabled
 Maximum users: 256
 Current users: 0
 Guest VLAN 1000 is not effective
 Critical VLAN is disabled
 Restrict VLAN is disabled

 Authentication Success: 0        Failure: 0
 EAPOL Packets: TX     : 0        RX     : 0
 Sent     EAPOL Request/Identity Packets  : 0
          EAPOL Request/Challenge Packets : 0
          Multicast Trigger Packets       : 0
          EAPOL Success Packets           : 0
          EAPOL Failure Packets           : 0
 Received  EAPOL Start Packets            : 0
          EAPOL Logoff Packets            : 0
          EAPOL Response/Identity Packets  : 0
          EAPOL Response/Challenge Packets : 0
```

Check configurations of MAC address authentication.

```
<HUAWEI> display mac-authen
 MAC address authentication is Enabled.
 Username format: use MAC address without-hyphen as username
 Quiet period is 60s
 Offline detect period is 300s
 Server response timeout value is 30s
 Reauthenticate period is 1800s
 Guest user reauthenticate period is 60s
 Maximum users: 1024
 Current users: 0
 Global domain is not configured

GigabitEthernet0/0/1 state: UP.  MAC address authentication is enabled
 Maximum users: 256
```

```
  Current users: 0
  Authentication Success: 0, Failure: 0
  Guest VLAN is disabled
  Critical VLAN is disabled
  Restrict VLAN is disabled
```

----End

3.5.4 Configuration Files

Configuration file of the switch

```
#
vlan batch 10 20
#
domain isp1
#
dot1x enable
mac-authen
#
portal local-server ip 192.168.1.30
portal local-server https ssl-policy huawei
#
radius-server template rd1
 radius-server shared-key cipher %$%$lrWRXXUmJ/5W\uBqID/6EULC%$%$
 radius-server authentication 192.168.2.30 1812
 radius-server retransmit 2
#
aaa
 authentication-scheme abc
  authentication-mode radius
 domain isp1
  authentication-scheme abc
  radius-server rd1
#
interface Vlanif10
 ip address 192.168.1.20 255.255.255.0
#
interface Vlanif20
 ip address 192.168.2.29 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 portal local-server enable
 dot1x enable
 mac-authen
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 20
#
interface LoopBack10
 ip address 192.168.1.30 255.255.255.255
#
```

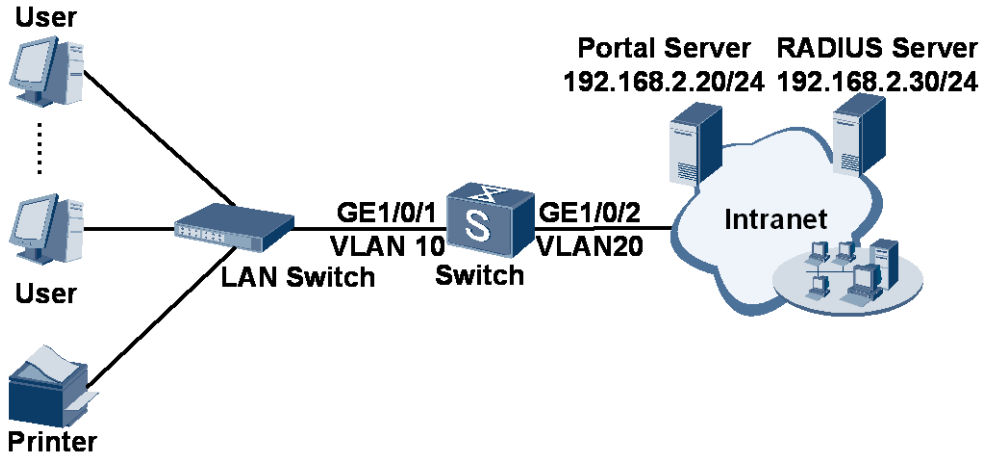
```
ssl policy huawei
 certificate load pem-cert cert_rsa_cert.pem key-pair rsa key-file cert_rsa_key.pem
auth-code cipher %$%$UR;Q$+r`=!1TvU,0.H,S!9"<%$%$
#
return
```

3.6 Example for Configuring Combined Authentication on Based on VLANIF Interfaces

3.6.1 Networking Requirements

As shown in Figure 3-6, lots of users in a company access the network through GE1/0/1 of the switch (used as an access device). To effectively manage the users accessing the network, the company requires that only authenticated users can access the network. As access users use various types of terminals and some terminals do not have authentication clients installed, the administrator needs to configure combined authentication based on VLANIF interfaces to control user access.

Figure 3-6 Networking diagram for configuring combined authentication



3.6.2 Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and configure the VLANs allowed by the interface to ensure network communication.
2. Create and configure a RADIUS server template, an AAA scheme, and an authentication domain; bind the RADIUS server template and AAA scheme to the authentication domain. This step implements communication between the switch and RADIUS server.
3. Configure MAC address authentication on VLANIF interfaces.
4. Configure Portal authentication.

NOTE

This example only provides the configurations on the switch. The configurations on the LAN switch and RADIUS server are not provided here.

3.6.3 Procedure

Step 1 Create VLANs and configure the VLANs allowed by the interface to ensure network communication.

#Create VLAN 10 and VLAN 20.

```
<Quidway> system-view
[Quidway] vlan batch 10 20
```

On the switch, configure GE1/0/1 connecting to users as a trunk interface and add GE1/0/1 to VLAN 10 and VLAN 20.

```
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] port link-type trunk
[Quidway-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[Quidway-GigabitEthernet1/0/1] quit
```

NOTE

Configure the interface type and VLANs based on the site requirements. In this example, users are added to VLAN 10.

On the switch, configure GE1/0/2 connecting to the uplink network as an access interface and add GE1/0/2 to VLAN 20.

```
[Quidway] interface gigabitethernet 1/0/2
[Quidway-GigabitEthernet1/0/2] port link-type access
[Quidway-GigabitEthernet1/0/2] port default vlan 20
[Quidway-GigabitEthernet1/0/2] quit
```

Create VLANIF10 and VLANIF20 and assign IP addresses to the VLANIF interfaces so that user terminals, Switch, and internal devices on the enterprise network can set up routes. In this example, the IP address of VLANIF10 is 192.168.1.20/24 and the IP address of VLANIF20 is 192.168.2.29/24.

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 192.168.1.20 24
[Quidway-Vlanif10] quit
[Quidway] interface vlanif 20
[Quidway-Vlanif20] ip address 192.168.2.29 24
[Quidway-Vlanif20] quit
```

Step 2 Create and configure a RADIUS server template, an AAA scheme, and an authentication domain.

Create and configure a RADIUS server template **rd1**.

```
[Quidway] radius-server template rd1
[Quidway-radius-rd1] radius-server authentication 192.168.2.30 1812
[Quidway-radius-rd1] radius-server shared-key cipher hello
[Quidway-radius-rd1] radius-server retransmit 2
[Quidway-radius-rd1] quit
```

Create an AAA scheme **abc** and set the authentication mode to RADIUS.

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme abc
[Quidway-aaa-authen-abc] authentication-mode radius
[Quidway-aaa-authen-abc] quit
```

Create an authentication domain **isp1**, and bind the AAA scheme **abc** and RADIUS server template **rd1** to the domain **isp1**.

```
[Quidway-aaa] domain isp1
[Quidway-aaa-domain-isp1] authentication-scheme abc
[Quidway-aaa-domain-isp1] radius-server rd1
[Quidway-aaa-domain-isp1] quit
[Quidway-aaa] quit
```

Configure the global default domain **isp1**. During access authentication, enter a user name in the format *user*@isp1 to perform AAA authentication in the domain **isp1**. If the user name does not contain the domain name or the contained domain name does not exist, the user is authenticated in the default domain.

```
[Quidway] domain isp1
```

Step 3 Configure MAC address authentication.

Enable MAC address authentication globally and on VLANIF interfaces.

```
[Quidway] mac-authen
[Quidway] interface vlanif 10
[Quidway-Vlanif10] mac-authen
```

Configure the authentication domain for MAC address authentication on VLANIF interfaces.

```
[Quidway-Vlanif10] mac-authen domain isp1
```

Configure MAC address re-authentication on VLANIF interfaces.

```
[Quidway-Vlanif10] mac-authen reauthenticate
[Quidway-Vlanif10] quit
```

Step 4 Configure Portal authentication.

Create and configure a Portal server template **abc**.

```
[Quidway] web-auth-server abc
[Quidway-web-auth-server-abc] server-ip 192.168.2.20
[Quidway-web-auth-server-abc] quit
```

Enable Portal authentication.

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] web-auth-server abc direct
[Quidway-Vlanif10] quit
```

Set the shared key that the device uses to exchange information with the Portal server to 12345 in cipher text.

```
[Quidway] web-auth-server abc
[Quidway-web-auth-server-abc] shared-key cipher 12345
[Quidway-web-auth-server-abc] quit
```

Set the maximum number of concurrent Portal authentication users to 100.

```
[Quidway] portal max-user 100
```

Set the offline detection interval for Portal authentication users to 500s.

```
[Quidway] portal timer offline-detect 500
```

Configure the detection and keepalive function of Portal authentication.

```
[Quidway] web-auth-server abc
[Quidway-web-auth-server-abc] server-detect action log
[Quidway-web-auth-server-abc] user-sync
[Quidway-web-auth-server-abc] quit
[Quidway] quit
```

Step 5 Verify the configuration.

Check configurations of MAC address authentication.

```
<Quidway> display mac-authen
  MAC address authentication is Enabled.
  Username format: use MAC address without-hyphen as username
  Quiet period is 60s
  Authentication fail times before quiet is 1
  Offline detect period is 300s
  Eth-trunk offline detect period is 7200s
  Server response timeout value is 30s
  Reauthenticate period is 1800s
  Guest user reauthenticate period is 60s
  Maximum users: 1024
  Current users: 0
  Global domain is none

 Vlanif10 state: UP.  MAC address authentication is disabled
  Reauthentication is enabled
  Reauthen Period: 1800s
  Current users: 0
  Current domain is isp1
  Authentication Success: 0, Failure: 0
```

Run the **display portal** command to check the Portal parameters that are set in the system view.

```
<Quidway> display portal
 Portal timer offline-detect length:500
 Portal timer eth-trunk offline-detect length:7200
 Portal max-user number:100
 Quiet function is Disabled
 Parameter set: Quiet Period     60s   Quiet-times        3

  Vlanif10 protocol status: down, web-auth-server layer2(direct)
```

Run the **display web-auth-server configuration** command to check the configuration of the Portal server.

```
<Quidway> display web-auth-server configuration
  Listening port       : 2000
  Portal               : version 1, version 2
  Include reply message : enabled
  ------------------------------------------------------------------------
  Web-auth-server Name : abc
  IP-address           : 192.168.3.20
  Shared-key           : %@%@CzDI4gECB>#5fI+Avcj!WI:e%@%@
```

```
  Source-IP           : -
  Port / PortFlag     : 50100 / NO
  URL                 :
  URL Template        :
  Redirection         : Enable
  Sync                : Enable
  Sync Seconds        : 300
  Sync Max-times      : 3
  Detect              : Enable
  Detect Seconds      : 60
  Detect Max-times    : 3
  Detect Critical-num : 0
  Detect Action       : log
  Bound Vlanif        : 10

  ------------------------------------------------------------------------------
  1 Web authentication server(s) in total
```

----End

3.6.4 Configuration Files

Configuration file of the switch

```
#
vlan batch 10 20
#
domain isp1
#
mac-authen
#
radius-server template rd1
 radius-server shared-key cipher %$%$lrWRXXUmJ/5W\uBqID/6EULC%$%$
 radius-server authentication 192.168.2.30 1812
 radius-server retransmit 2
#
web-auth-server abc
 server-ip 192.168.2.20
 port 50100
 shared-key cipher %@%@CzDI4gECB>#5fI+Avcj!WI:e%@%@
 server-detect interval 60 max-times 3 critical-num 0 action log
 user-sync
#
aaa
 authentication-scheme abc
  authentication-mode radius
 domain isp1
  authentication-scheme abc
  radius-server rd1
#
interface Vlanif10
ip address 192.168.1.20 255.255.255.0
 web-auth-server abc direct
 mac-authen
 mac-authen domain isp1
```

```
#
interface Vlanif20
 ip address 192.168.2.29 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet1/0/2
 port link-type access
 port default vlan 20
#
portal max-user 100
portal timer offline-detect 500
#
return
```

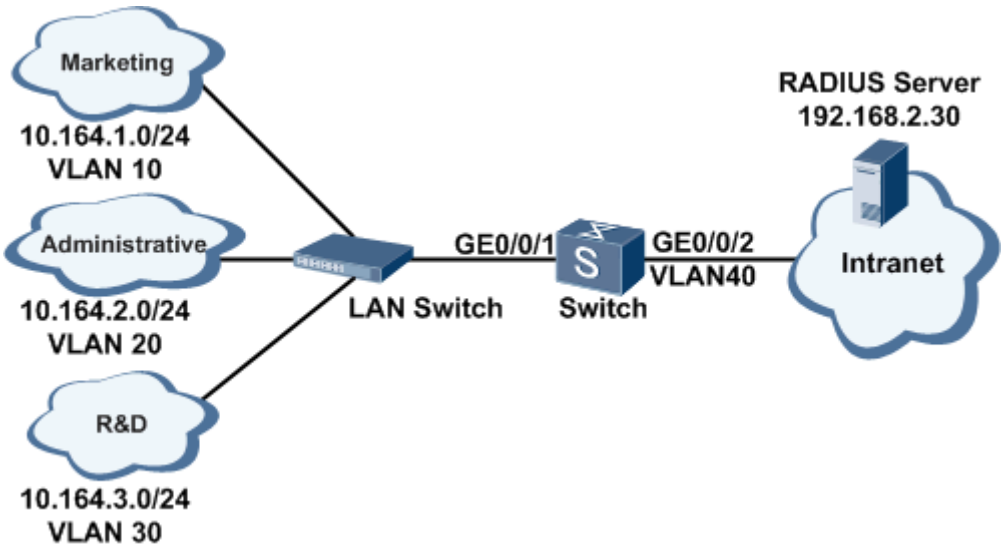
3.7 Example for Configuring User Group

3.7.1 Networking Requirements

As shown in Figure 3-7, lots of users in a company access the network through GE1/0/1 of the switch (used as an access device). To effectively manage the users accessing the network, the company requires that only authenticated users can access the network. In addition, users of different departments have limited network access rights:

- Marketing personnel can only access the network segment 172.16.104.0/24.
- Administrative personnel can only access the network segment 172.16.105.0/24.
- R&D personnel can only access the network segment 172.16.106.0/24.

Figure 3-7 User group configuration network



3.7.2 Configuration Roadmap

The configuration roadmap is as follows:

Step 1 Create VLANs and configure the VLANs allowed by the interface to ensure network communication.

Step 2 Create and configure a RADIUS server template, an AAA scheme, and an authentication domain; bind the RADIUS server template and AAA scheme to the authentication domain. This step implements communication between the switch and RADIUS server.

Step 3 Configure user groups to differentially manage the users' network access rights.

1. Create ACLs.
2. Create user groups and bind them to ACLs.
3. Enable the user group function.

Step 4 Configure 802.1x authentication to ensure that only authenticated users can access network resources.

1. Enable 802.1x authentication globally and on the interfaces.
2. Enable MAC address bypass authentication to authenticate the terminals (such as printers) that cannot have 802.1x authentication client software installed.

NOTE

This example only provides the configurations on the switch. The configurations on the LAN switch and RADIUS server are not provided here.

----End

3.7.3 Procedure

Step 1 Create VLANs and configure the VLANs allowed by the interface to ensure network communication.

Create VLAN 10, VLAN 20, VLAN 30, and VLAN 40.

```
<Quidway> system-view
[Quidway] vlan batch 10 20 30 40
```

On the switch, configure GE1/0/1 connecting to users as a trunk interface and add GE1/0/1 to VLAN 10, VLAN 20, and VLAN 30.

```
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] port link-type trunk
[Quidway-GigabitEthernet1/0/1] port trunk allow-pass vlan 10 20 30
[Quidway-GigabitEthernet1/0/1] quit
```

On the switch, configure GE1/0/2 connecting to the RADIUS server as an access interface and add GE1/0/2 to VLAN 40.

```
[Quidway] interface gigabitethernet 1/0/2
[Quidway-GigabitEthernet1/0/2] port link-type access
[Quidway-GigabitEthernet1/0/2] port default vlan 40
[Quidway-GigabitEthernet1/0/2] quit
```

Create VLANIF 40 and assign the IP address 192.168.2.29/24 to VLANIF 40.

```
[Quidway] interface vlanif 40
[Quidway-Vlanif40] ip address 192.168.2.29 24
[Quidway-Vlanif40] quit
```

Step 2 Create and configure a RADIUS server template, an AAA scheme, and an authentication domain.

Create and configure a RADIUS server template **rd1**.

```
[Quidway] radius-server template rd1
[Quidway-radius-rd1] radius-server authentication 192.168.2.30 1812
[Quidway-radius-rd1] radius-server shared-key cipher hello
[Quidway-radius-rd1] radius-server retransmit 2
[Quidway-radius-rd1] quit
```

Create an AAA scheme **abc** and set the authentication mode to RADIUS.

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme abc
[Quidway-aaa-authen-abc] authentication-mode radius
[Quidway-aaa-authen-abc] quit
```

Create the authentication domains **abc11**, **abc22**, and **abc33**, and bind the AAA scheme **abc** and RADIUS server template **rd1** to the authentication domains.

```
[Quidway-aaa] domain abc11
[Quidway-aaa-domain-abc11] authentication-scheme abc
[Quidway-aaa-domain-abc11] radius-server rd1
[Quidway-aaa-domain-abc11] quit
[Quidway-aaa] domain abc22
[Quidway-aaa-domain-abc22] authentication-scheme abc
[Quidway-aaa-domain-abc22] radius-server rd1
[Quidway-aaa-domain-abc22] quit
[Quidway-aaa] domain abc33
[Quidway-aaa-domain-abc33] authentication-scheme abc
[Quidway-aaa-domain-abc33] radius-server rd1
[Quidway-aaa-domain-abc33] quit
[Quidway-aaa] quit
```

Step 3 Configure the user group function.

Create ACLs.

```
[Quidway] acl 3001
[Quidway-acl-adv-3001] rule permit ip source 10.164.1.0 0.0.0.255 destination
172.16.104.0 0.0.0.255
[Quidway-acl-adv-3001] rule deny ip source 10.164.1.0 0.0.0.255 destination any
[Quidway-acl-adv-3001] quit
[Quidway] acl 3002
[Quidway-acl-adv-3002] rule permit ip source 10.164.2.0 0.0.0.255 destination
172.16.105.0 0.0.0.255
[Quidway-acl-adv-3002] rule deny ip source 10.164.2.0 0.0.0.255 destination any
[Quidway-acl-adv-3002] quit
[Quidway] acl 3003
[Quidway-acl-adv-3003] rule permit ip source 10.164.3.0 0.0.0.255 destination
172.16.106.0 0.0.0.255
[Quidway-acl-adv-3002] rule deny ip source 10.164.3.0 0.0.0.255 destination any
[Quidway-acl-adv-3003] quit
```

Create user groups and bind them to ACLs. Allocate marketing personnel to the user group **abc1**, administrative personnel to the user group **abc2**, and R&D personnel to the user group **abc3**.

```
[Quidway] user-group abc1
[Quidway-user-group-abc1] acl-id 3001
[Quidway-user-group-abc1] quit
[Quidway] user-group abc2
[Quidway-user-group-abc2] acl-id 3002
[Quidway-user-group-abc2] quit
[Quidway] user-group abc3
[Quidway-user-group-abc3] acl-id 3003
[Quidway-user-group-abc3] quit
# Enable the user group function.
[Quidway] user-group abc1 enable
[Quidway] user-group abc2 enable
[Quidway] user-group abc3 enable
```

Bind the user groups to the authentication domains. The marketing personnel are authenticated in the authentication domain **abc11**, administrative personnel in the authentication domain **abc22**, and R&D personnel in the authentication domain **abc33**.

```
[Quidway] aaa
[Quidway-aaa] domain abc11
[Quidway-domain-abc11] user-group abc1
[Quidway-domain-abc11] quit
[Quidway-aaa] domain abc22
[Quidway-domain-abc22] user-group abc2
[Quidway-domain-abc22] quit
[Quidway-aaa] domain abc33
[Quidway-domain-abc33] user-group abc3
[Quidway-domain-abc33] quit
[Quidway-aaa] quit
```

Step 4 Configure 802.1x authentication.

Enable 802.1x authentication globally and on an interface.

```
[Quidway] dot1x enable
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] dot1x enable
```

Configure MAC address bypass authentication.

```
[Quidway-GigabitEthernet1/0/1] dot1x mac-bypass
[Quidway-GigabitEthernet1/0/1] quit
[Quidway] quit
```

Step 5 Verify the configuration.

Run the **display user-group** command in any view to check brief information about all user groups.

```
<Quidway> display user-group
 ------------------------------------------------------------------------------
 ID   Group name                 Rule-num GID     User-num  Status
 ------------------------------------------------------------------------------
 0    abc1                       2       1       0        enabled
 1    abc2                       2       2       0        enabled
```

```
 2    abc3                       2       3       0       enabled
 ------------------------------------------------------------------------------
 Total 3
```

Run the **display user-group***group-name* command in any view to check details about a specified user group. The user group **abc1** is used as an example here.

```
<Quidway> display user-group abc1
  User group ID          : 0
  Group name             : abc1
  ACL ID                 : 3001
  ACL rule number        : 2
  GID                    : 1
  User-num               : 0
  VLAN                   :
  Remark dscp            :
  Remark 8021p           :
  Status                 : enabled
```

Run the **display domain name***domain-name* command in any view to check configuration information about an AAA domain. The authentication domain **abc11** is used as an example here.

```
<Quidway> display domain name abc11

  Domain-name                  : abc11
  Domain-state                 : Active
  Authentication-scheme-name   : abc
  Accounting-scheme-name       : default
  Authorization-scheme-name    : -
  Service-scheme-name          : -
  RADIUS-server-template       : rd1
  HWTACACS-server-template     : -
  User-group                   : abc1
```

Check the 802.1x configuration.

```
<Quidway> display dot1x
  Global 802.1x is Enabled
  Authentication method is CHAP
  Max users: 1024
  Current users: 0
  DHCP-trigger is Disabled
  Handshake is Disabled
  Quiet function is Disabled
  Parameter set:Handshake Period   60s   Reauthen Period   3600s
              Client Timeout     30s   Server Timeout     30s
              Quiet Period       60s   Quiet-times        3
              Eth-Trunk Handshake Period   45s
  dot1x URL: Not configed.
  Free-ip configuration(IP/mask): Not configed.

 GigabitEthernet1/0/1 status: UP  802.1x protocol is Enabled[mac-bypass]
  Port control type is Auto
  Authentication method is MAC-based
  Reauthentication is disabled
  Maximum users: 2048
```

```
  Current users: 0
  Guest VLAN is disabled
  Critical VLAN is disabled
  Restrict VLAN is disabled

  Authentication Success: 0        Failure: 0
  EAPOL Packets: TX    : 0        RX    : 0
  Sent     EAPOL Request/Identity Packets  : 0
           EAPOL Request/Challenge Packets : 0
           Multicast Trigger Packets       : 0
           EAPOL Success Packets           : 0
           EAPOL Failure Packets           : 0
  Received  EAPOL Start Packets            : 0
           EAPOL Logoff Packets             : 0
           EAPOL Response/Identity Packets : 0
           EAPOL Response/Challenge Packets: 0
```

When an administrative user A (user name **userA@abc22**) accesses the network, the switch authenticates the user in the authentication domain **abc22** after receiving the authentication request. The authentication domain **abc22** is bound to the user group **abc2**, so user A is granted the network access rights of the user group **abc2**. After accessing the network, user A can only access network resources in the network segment 172.16.105.0/24. The same rule applies to R&D and marketing personnel: R&D personnel can only access 172.16.106.0/24 and marketing personnel can only access 172.16.104.0/24.

----End

3.7.4 Configuration Files

Configuration file of the switch

```
#
vlan batch 10 20 30 40
#
dot1x enable
#
radius-server template rd1
 radius-server shared-key cipher %$%$lrWRXXUmJ/5W\uBqID/6EULC%$%$
 radius-server authentication 192.168.2.30 1812
 radius-server retransmit 2
#
acl number 3001
 rule 5 permit ip source 10.164.1.0 0.0.0.255 destination 172.16.104.0 0.0.0.255
 rule 10 deny ip source 10.164.1.0 0.0.0.255
#
acl number 3002
 rule 5 permit ip source 10.164.2.0 0.0.0.255 destination 172.16.105.0 0.0.0.255
 rule 10 deny ip source 10.164.2.0 0.0.0.255
#
acl number 3003
 rule 5 permit ip source 10.164.3.0 0.0.0.255 destination 172.16.106.0 0.0.0.255
 rule 10 deny ip source 10.164.3.0 0.0.0.255
#
aaa
 authentication-scheme abc
```

```
 authentication-mode radius
domain abc11
 authentication-scheme abc
 radius-server rd1
 user-group abc1
domain abc22
 authentication-scheme abc
 radius-server rd1
 user-group abc2
domain abc33
 authentication-scheme abc
 radius-server rd1
 user-group abc3
#
interface Vlanif40
 ip address 192.168.2.29 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 20 30
 dot1x mac-bypass
#
interface GigabitEthernet1/0/2
 port link-type access
 port default vlan 40
#
user-group abc1
 acl-id 3001
user-group abc1 enable
#
user-group abc2
 acl-id 3002
user-group abc2 enable
#
user-group abc3
 acl-id 3003
user-group abc3 enable
#
return
```

4 Troubleshooting

4.1 802.1x Authentication Fails

Possible Causes

This fault is commonly caused by one of the following:

- Some parameters are set incorrectly or not set, such as the 802.1x authentication parameters, AAA authentication domain, authentication server template, and authentication server.
- The user name or password entered by the user is incorrect.
- The number of online users reaches the maximum.

Procedure

Step 1 Check whether 802.1x authentication is enabled on the device.

Run the **display dot1x** command to check whether 802.1x authentication is enabled globally or on the interfaces. If the command output does not contain **Global 802.1x is Enabled** or **802.1x protocol is Enabled**, 802.1x authentication is disabled. Run the **dot1x enable** command to enable 802.1x authentication.

Step 2 Check the configuration of 802.1x authentication.

Run the **display dot1x** command to check whether the 802.1x authentication configuration complies with the following requirements:

- The authentication method on the device must be the same as that on the authentication server.
- EAP authentication and local authentication cannot be configured simultaneously. To check the AAA configuration, go to step 3.
- If the authentication method for 802.1x users is PAP, check whether the authentication client supports PAP authentication. If the client does not support PAP authentication, change the authentication method to CHAP or EAP.

  You can run the **dot1x authentication-method** command to configure the 802.1x authentication method.

Step 3 Check whether AAA is correctly configured.

- Check whether the user name contains the domain name.

  - If no, the user is authenticated in the default domain. Check the authentication template bound to the default domain.
  - If yes, the user should be authenticated in the specified domain. However, if the domain name is not found, the authentication fails. Check the authentication template bound to the specified domain.
- Check whether the authentication scheme applied to the user domain on the device is correct.
  - If RADIUS or HWTACACS authentication is configured for the user domain, check whether the user name and password are created on the authentication server and whether dynamic authorization information is configured on the server. If no, create the user name and password and configure dynamic authorization information on the authentication server.
  - If local authentication is configured for the user domain, run the **display local-user** command to check whether the local user name and password are created. If no, create the user name and password.
  - If the authentication scheme is none, go to step 4.
- Run the **display accounting-scheme** command to check the accounting scheme. If the accounting scheme is configured but the authentication server does not support accounting, the user cannot go online. To allow the user to go online, cancel the accounting configuration in the user domain or run the **accounting start-fail online** command in the accounting scheme view to keep the user online after the accounting fails.

Step 4 Check whether the user name and password entered by the user are correct.

If RADIUS authentication is configured and the authentication method is CHAP or PAP, run the **test-aaa** command to check whether the user name and password can pass the RADIUS authentication.

- If the authentication fails, check the configuration on the RADIUS server and the RADIUS configuration on the device. For details, see the RADIUS troubleshooting procedure.
- If the authentication succeeds, check the option settings on the client or capture packets on the network adapter of the client to check whether the client sends authentication packets correctly.

If the user name and password are correct, go to step 5.

Step 5 Run the **display dot1x interface** *interface-type interface-number* command on the device to check whether the number of concurrent online 802.1x users reaches the maximum.

When the number of users connected to the interface reaches the maximum, the device does not trigger authentication for the subsequent access users. You can run the **dot1x max-user** command to increase the maximum number of 802.1x users allowed by the interface.

----End

4.2 MAC Address Authentication Fails

Possible Causes

This fault is commonly caused by one of the following:

- Some parameters are set incorrectly or not set, such as the MAC address authentication parameters, AAA authentication domain, authentication server template, and authentication server.
- The number of online users reaches the maximum.

Procedure

Step 1 Check whether MAC address authentication is enabled on the device.

Run the **display mac-authen** command to check whether MAC address authentication is enabled globally or on the interfaces. If the command output does not contain **MAC address authentication is Enabled**, MAC address authentication is disabled. Run the **mac-authen** command to enable MAC address authentication.

Step 2 Check the configuration of the user name for MAC address authentication.

Run the **display mac-authen** command to check the current configuration of the user name for MAC address authentication

MAC address authentication supports two user name formats: fixed user name and MAC address.

- If the MAC address is used as the user name, the device sends the MAC address of the user terminal as the user name and password to the authentication server. The authentication domain is configured using the **mac-authen domain** command. If this command is not executed, the default domain is used as the authentication domain.
- When the fixed user name contains a domain name, this domain is used as the authentication domain. If the fixed user name does not contain a domain name, the default domain is used as the authentication domain.

Check the authentication server template and AAA scheme bound to the authentication domain. Go to step 3.

Step 3 Check whether AAA is correctly configured.

Check whether the authentication server template bound to the domain is correct, and whether the IP address and interface of the authentication server are configured correctly in the template. Check whether the user name format and shared key specified in the template are the same as those on the authentication server.

- Check whether the authentication scheme applied to the user domain on the device is correct.
  - If RADIUS or HWTACACS authentication is configured for the user domain, check whether the user name and password are created on the authentication server and whether dynamic authorization information is configured on the server. If no, create the user name and password and configure dynamic authorization information on the authentication server.
  - If local authentication is configured for the user domain, run the **display local-user** command to check whether the local user name and password are created. If no, run the **local-user** command to create the local user name and password.
  - If the authentication scheme is none, go to step 4.
- Run the **display accounting-scheme** command to check the accounting scheme. If the accounting scheme is configured but the authentication server does not support accounting, the user cannot go online. To allow the user to go online, cancel the accounting configuration in the user domain or run the **accounting start-fail online**

command in the accounting scheme view to keep the user online after the accounting fails.

Step 4 Run the **display mac-authen interface** *interface-type interface-number* command on the device to check whether the number of concurrent online MAC address authentication users reaches the maximum.

When the number of users connected to the interface reaches the maximum, the device does not trigger authentication for the subsequent access users. You can run the **mac-authen max-user** command to increase the maximum number of MAC address authentication users allowed by the interface.

----End

4.3 Portal Authentication Fails

Possible Causes

This fault is commonly caused by one of the following:

- Some parameters are set incorrectly or not set, such as the Portal authentication parameters, AAA authentication domain, authentication server template, and authentication server.
- The Portal authentication server is unreachable or unavailable.
- The user name or password entered by the user is incorrect.

Procedure

Step 1 Run the **ping** command to check whether the link between the device and the Portal authentication server and the link between the device and the RADIUS or HWTACACS authentication server work properly.

- If the ping operation fails on any link, rectify the fault on the link.
- If the ping operations succeed, go to step 2.

Step 2 Check whether Portal authentication is configured correctly on the device.

Run the **display web-auth-server configuration** command to check whether the Portal authentication server is configured. If the Portal authentication server is not configured, run the **web-auth-server** *server-name* command in the system view to create the web authentication server name. Run the **server-ip** *ip-address* and **url** commands in the web-auth-server view to configure the IP address and URL for the web authentication server.

You can configure the server port and shared key in the web-auth-server view. Ensure that the server port and shared key configured in the web-auth-server view are the same as those on the server.

- Run the **display this** command in the VLANIF interface view to check whether the Portal server is bound to the VLANIF interface. If the Portal server is not bound to the VLANIF interface, run the **web-auth-server** *server-name*{direct | layer3} command in the interface view.
- Run the **display web-auth-server configuration** command to check whether the listening port is the same as that on the Portal server. To check the Portal server, go to step 3.

Step 3 Check whether the Portal authentication server is correctly configured.

- Check whether the device is in the authenticated device list.
- Check whether the listening port that the Portal server uses to exchange Portal packets with the device is the same as that configured on the device.

Ensure that the device is in the authenticated device list and the listening port configured on the Portal server is the same as that on the device.

Step 4 Check whether AAA is correctly configured.

Check whether the authentication server template bound to the domain is correct, and whether the IP address and interface of the authentication server are configured correctly in the template. Check whether the user name format and shared key specified in the template are the same as those on the authentication server.

- Check whether the authentication scheme applied to the user domain on the device is correct.
  - If RADIUS or HWTACACS authentication is configured for the user domain, check whether the user name and password are created on the authentication server and whether dynamic authorization information is configured on the server. If no, create the user name and password and configure dynamic authorization information on the authentication server.
  - If local authentication is configured for the user domain, run the **display local-user** command to check whether the local user name and password are created. If no, run the **local-user** command to create the local user name and password.
- Run the **display accounting-scheme** command to check the accounting scheme. If the accounting scheme is configured but the authentication server does not support accounting, the user cannot go online. To allow the user to go online, cancel the accounting configuration in the user domain or run the **accounting start-fail online** command in the accounting scheme view to keep the user online after the accounting fails.

5 FAQ

5.1 802.1x Authentication

What Is the Difference Between 802.1x and DOT1X?

They have the same function and just are called different names.

How Can the Switch Connect to the RADIUS Server When I Configure 802.1x Authentication?

When you configure 802.1x authentication, run the **dot1x enable** command to enable 802.1x authentication globally and on an interface. In addition, ensure that the switch and the RADIUS server can communicate at Layer 3.

Can Layer 3 Functions Be Enabled in the Dynamic VLAN and Guest VLAN Used in 802.1x Authentication?

In versions earlier than V100R006, Layer 3 functions cannot be enabled in the dynamic VLAN and guest VLAN used in 802.1x authentication. In V100R006 and later versions, Layer 3 functions can be enabled in the dynamic VLAN and guest VLAN.

Why Does a Client Go Offline 10 Seconds After It Passes 802.1x Authentication on the Switch?

If handshake with online 802.1x users is enabled on the switch, the switch sends handshake packets to a client after the client is authenticated. If the client sends no handshake packet to the switch, the switch forces the client offline.

The client goes offline 10 seconds after it is authenticated. This may be caused by a handshake failure. In this case, run the **undo dot1x handshake** command in the system view to disable the handshake function.

Why 802.1x or MAC Address Authentication Does Not Take Effect After the dot1x enable or mac-authen Command Is run Globally or on an Interface and Displayed in the Configuration File?

If ACL resources are used up, the **dot1x enable** or **mac-authen** command run globally or on an interface does not take effect.

5.2 Portal Authentication

Can Portal Authentication Be Configured on an Eth-Trunk and Is the Shared Key Necessary in Portal Authentication?

In V100R006 and later versions, Portal authentication cannot be configured on an Eth-Trunk.

In V100R006 and later versions, the shared key must be configured on the switch and Portal authentication server during Portal authentication.

Does the Portal Server IP Address Need to Be Added to the Portal Free Rule When I Bind the Portal Authentication Server to a VLANIF Interface?

When you bind the Portal authentication server to a VLANIF interface, the Portal authentication server IP address needs to be added to the Portal free rule in the versions earlier than V100R005. In V100R005 and later versions, the Portal authentication server IP address does not need to be added to the Portal free rule.

A Glossary

Acronym and Abbreviation	Full Name
NAC	Network Admission Control
NAD	Network Access Device
ACS	Access Control Server
AAA	Authentication, Authorization, and Accounting
EDC	Enterprise Data Center
RADIUS	Remote Authentication Dial-In User Service
TLS	Transport Layer Security
PEAP	Protected Extensible Authentication Protocol
EAP	Extensible Authentication Protocol
PAP	Password Authentication Protocol
CHAP	Challenge Handshake Authentication Protocol