

17 802.1X Authentication

[17.1 Why Is 802.1X Authentication Required?](#)

[17.2 Device Roles Defined in 802.1X](#)

[17.3 Port-based Authentication](#)

[17.4 802.1X Information Exchange](#)

[17.5 Configuring 802.1X Authentication](#)

17.1 Why Is 802.1X Authentication Required?

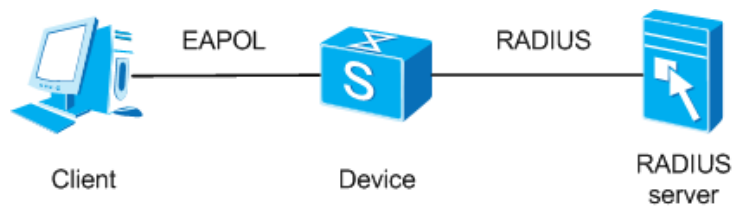
With the popularization of networks, more and more enterprises, campuses, communities, and SOHO users select Ethernet, which is a cost-effective, convenient, and high-bandwidth access mode and one of the most important access modes on the current data communication networks. Users can access network resources from any computer that is connected to a network, which brings severe security risks to the network environment. In addition, the implementation and maintenance of different network services require the underlying Ethernet to provide a necessary security authentication mechanism. How to correctly process user access rights becomes an increasingly prominent problem.

802.1X is used to authenticate and authorize the users connected to a LAN to protect network security. IEEE 802.1X (802.1X for short) is an IEEE standard for port-based network access control (PNAC). It provides an authentication mechanism for user access networks. By authenticating the rights of a user connected to a port, 802.1X can determine which network resources are accessible to the user device connected to the port.

802.1X has complete user authentication and management functions, which can well support the accounting, security, operation, and management requirements of broadband networks.

17.2 Device Roles Defined in 802.1X

Figure 17-1 shows the roles of network devices that use the 802.1X authentication protocol.

Figure 17-1 Device roles defined in 802.1X

- **Client:** A user terminal that seeks to gain access to the network. Based on whether supporting proactive initiation of 802.1X authentication, terminals are classified into common terminals and dumb terminals.
 - a. Common terminals, such as office PCs, can run 802.1X authentication client software. Authentication is triggered after a terminal user enters its user name and password. If the authentication is successful, the terminal accesses the network.
 - b. Dumb terminals, such as network printers and cameras, cannot run 802.1X authentication client software. They cannot access any network by proactively triggering authentication. Instead, they access networks through MAC address bypass (MAB) authentication.
- **Device:** It provides a port for the client to access the LAN and controls the client access rights or scope on the network based on the authentication status of the client. Located between the client and the authentication server, the device requests identity information from the client, encapsulates and decapsulates the Extensible Authentication Protocol (EAP) frame, interacts with the authentication server, and relays the response to the client.
- **Authentication server:** It authenticates the client and notifies the device whether the to-be-authenticated port may access the network, thereby implementing authentication, authorization, and accounting on the user. Generally, the authentication server is a RADIUS server.

After receiving Extensible Authentication Protocol over LAN (EAPOL) frames, the device strips off Ethernet headers and re-encapsulates the remaining EAP frames in RADIUS format (EAPOR) without modifying or checking the EAP frames. Then, the device relays the EAP frames to the authentication server, and the authentication server parses the EAP frames. In the reverse direction, when receiving the frames from the authentication server, the device removes the frame headers and leaves the EAP frames, encapsulates the frames into Ethernet frames, and sends them to the client.

17.3 Port-based Authentication

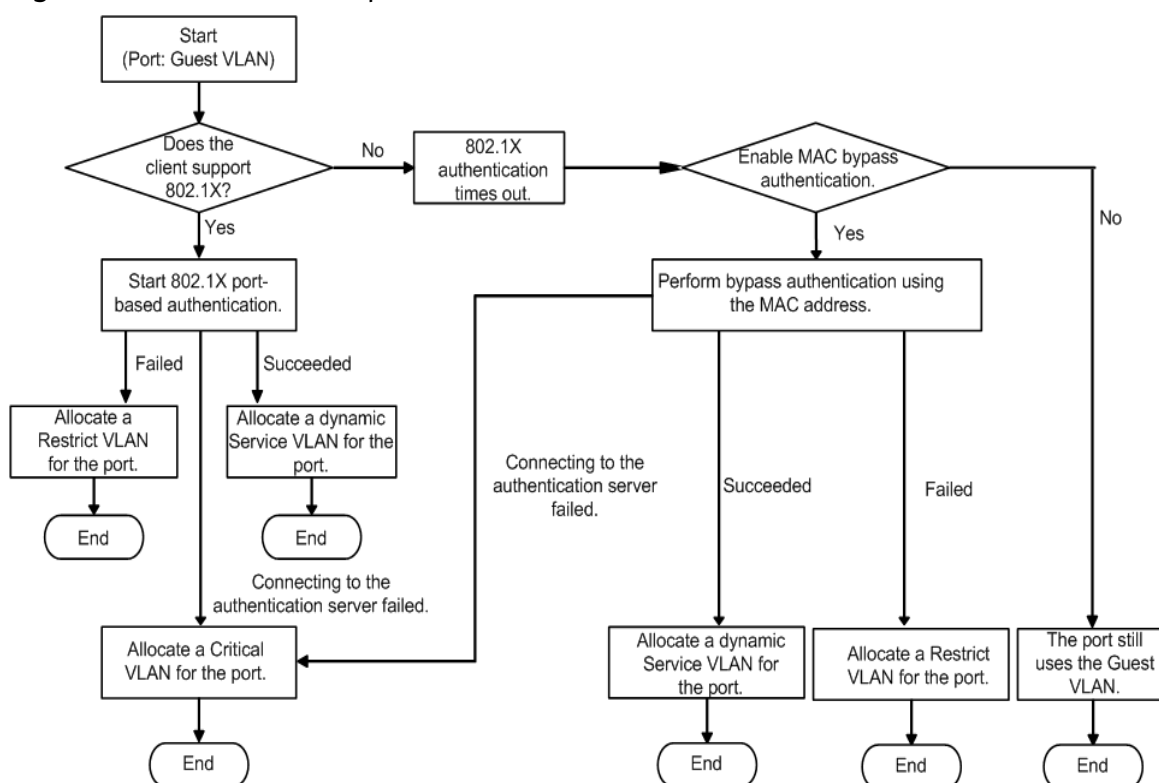
When 802.1X is enabled on a port but authentication is not triggered, all services on the port go through the guest VLAN. For terminals that are not 802.1X-capable, the guest VLAN is used to download 802.1X dial-up software or access restricted web pages. After 802.1 authentication is triggered, the system authenticates the client as follows:

- If the client supports 802.1X client software and the client identity is legitimate, the 802.1X authentication is successful. Then, the client port is assigned a dynamic service VLAN, and the client can access the network.

- If 802.1x authentication times out during EAPOL message exchange and MAC bypass (MAB) authentication is enabled, the device relays the MAC address of the client to the authentication server for authorization. If the MAC address of the client is legitimate, the authorization is successful and a dynamic service VLAN is assigned to the client. Then, the client can access the network.
- If 802.1X authentication of the port times out and the MAC address authentication is not enabled or the authentication fails, the port still uses the guest VLAN to access limited network resources.
- If the authentication server fails to authenticate the client (for example, an incorrect user name or password is entered), all services on this port go through the Restrict VLAN. The Restrict VLAN has similar functions as the guest VLAN. Both allow users to access limited network resources before passing authentication. However, the Restrict VLAN has fewer network resources than the guest VLAN. Therefore, the Restrict VLAN more strictly limits the network resources accessible to unauthenticated users.
- If the authentication server cannot be connected (for example, the network between the device and the authentication server is disconnected or the authentication server is faulty), all services on the port can go through the Critical VLAN, for example, emergency voice call or service assurance.

Figure 17-2 shows the system authentication process.

Figure 17-2 Authentication process



 NOTE

The relationship between MAB authentication and port-based 802.1X authentication is as follows: If both port-based 802.1X authentication and MAB authentication are enabled, 802.1X authentication is performed first. If 802.1x authentication times out, MAB authentication is then performed. If 802.1x authentication is disabled but MAB authentication is enabled, MAB authentication is directly performed. Disabling MAB authentication has no impact on 802.1X authentication status.

17.4 802.1X Information Exchange

Authorized/Unauthorized 802.1X Port

Whether the client is authorized to access the network depends on the status of the connected device port. The port is started in the unauthorized state. In this state, all incoming and outgoing traffic except 802.1X protocol packets is not allowed to pass through the port. After the client passes the authentication, the port changes to the authorized state to allow all the traffic from the client.

If a client that does not support 802.1X authentication is connected to an unauthorized 802.1X port, the device requests to authenticate the client. In this case, the client does not respond to the request, the port is still in the unauthorized state, and the client does not have the network access right. The **port dot1x port-control** command and the following keywords can be used to control the port authorization status of the device:

force-authorized: Specifies the forced authorization mode. In this mode, the port always stays in the authorized state and users can access the network through this port without authentication or authorization. The port sends and receives traffic normally without 802.1X client authentication. This configuration has security risks and is not recommended.

force-unauthorized: Specifies the forced unauthorization mode. The port stays in the unauthorized state and users are not allowed to access network resources through this port.

auto: Specifies the automatic identification mode. After 802.1X authentication is enabled, the port is in the unauthorized state and can send and receive only EAPOL packets. If the port receives an EAPOL-start frame, authentication starts. The device requests the identity of the client and starts to relay the authentication message between the client and the authentication server. If the authentication is successful (the client receives an Accept frame from the authentication server), the port status changes to authorized and all frames from the authenticated client are allowed to pass through the port. If the authentication fails, the port remains in the unauthorized state.

802.1X Information Exchange

EAP packets are exchanged between the device and authentication server in EAP relay mode or EAP termination mode. Therefore, 802.1X port-based authentication can be performed in either of the following modes: EAP relay and EAP termination.

EAP Relay

802.1x authentication can be triggered by the client or the device. If the **port dot1x port-control auto** command is used to enable identity authentication on the port, the device sends an EAP-Request/Identity frame to the client when detecting that the link is connected (the link status changes from down to up). After receiving the frame, the client responds with an EAP-response/identity frame.

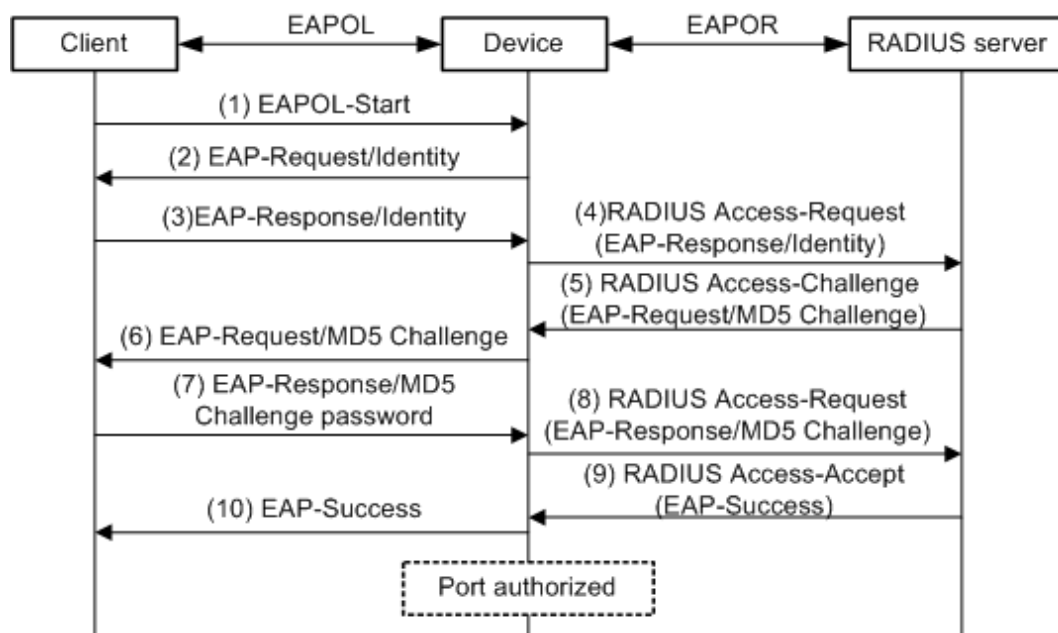
If the client does not receive the EAP-Request/Identity frame from the device during startup, the client can send an EAPOL-start frame to start authentication. This frame can instruct the device to send a request.

When the client provides its identity, the device acts as a mediator to transfer the EAP frame between the client and the authentication server until the authentication succeeds or fails. If the authentication succeeds, the port is authorized. If the authentication fails, it can be performed again. Based on the final authentication result, the port is assigned to a VLAN that provides limited services or the user is not assigned the network access right.

The device relays EAP packets between the client and RADIUS server:

- Re-encapsulates EAPOR packets into EAPOL packets and sends them to the client.
- Re-encapsulates EAPOL packets into EAPOR packets and sends them to the RADIUS server.

Figure 17-3 EAP relay authentication process



(1) When a user accesses the network, the 802.1X client program is automatically started. The client program sends an authentication request frame (EAPOL-start) to the device to start the authentication process.

(2) After receiving the authentication request frame from the client, the device sends an EAP-Request/Identity frame to the client, requesting the client to send the user name.

(3) The client sends the user name to the device through an EAP-Response/Identity frame to respond to the request sent by the device.

(4) The device encapsulates the EAP packets from the client in EAPOR format into a RADIUS Access-Request packet and sends it to the authentication server for processing.

(5)–(9) The authentication server (RADIUS server) verifies the user name and password of the client using a specific method. If the authentication succeeds, the server sends an authentication success packet (RADIUS Access-Accept) to the device.

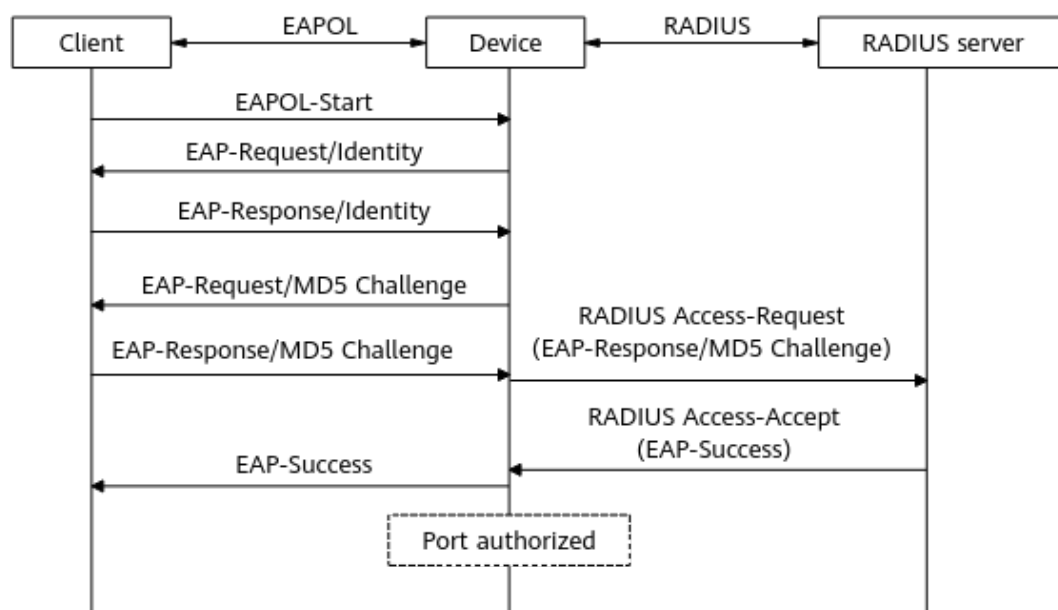
(10) After receiving the RADIUS Access-Accept packet, the device decapsulates it in EAPOR format and sends an EAP-Success packet to the client. Then, the device changes the port to the authorized state and allows the user to access the network through the port.

EAP Termination

The device terminates the EAP authentication process:

- Encapsulates the client's authentication information in received EAP packets into standard RADIUS packets.
- Communicates with the RADIUS server using the Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) for access authentication.

Figure 17-4 EAP termination authentication process



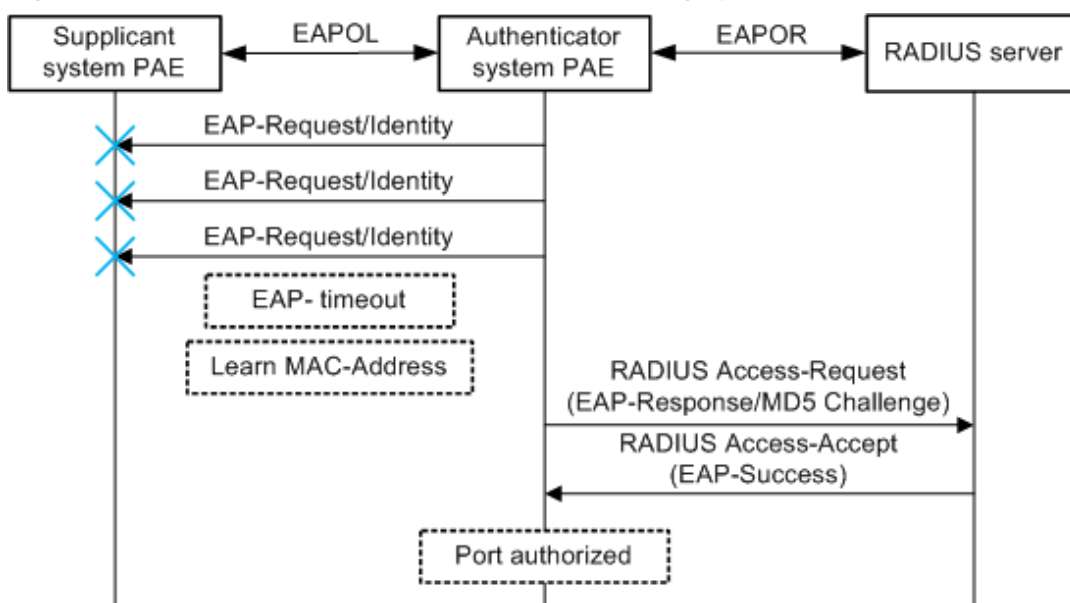
The difference between the 802.1X authentication process in EAP termination mode and that in EAP relay mode is as follows: In EAP termination mode, the device randomly generates an MD5-Challenge value for user password encryption, and then sends the user name, random MD5-Challenge value, and password encrypted on the client to the RADIUS server for authentication.

MAC Bypass (MAB) Authentication

If MAB authentication is enabled and 802.1X authentication times out during EAPOL message exchange, the device can authorize the client when detecting

Ethernet packets from the client. The device uses the MAC address of the client as its identifier, adds the MAC address to the RADIUS-Access/Request frame, and sends the frame to the RADIUS server. After the server sends a RADIUS-Access/Accept frame (authorization success) to the device, the port is authorized. If the MAB authorization fails and the guest VLAN is specified, the device assigns the port to the guest VLAN. If the device detects an EAPOL packet when waiting for an Ethernet packet, the device stops MAB authorization and starts 802.1X authentication. The detailed process is shown in [Figure 17-5](#). In the figure, PAE refers to the port access entity, that is, the device for authentication and authorization.

Figure 17-5 MAB authentication information exchange process



Re-authentication and Forcing Users to go Offline

If an administrator modifies the access rights and authorization parameters (such as the dynamic service VLAN) of an online user, re-authentication is required for the user.

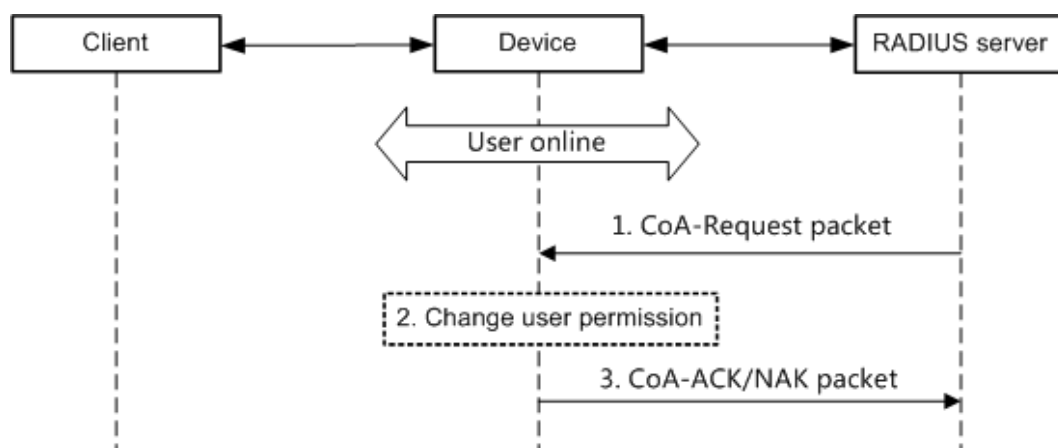
After the re-authentication function is configured for online 802.1X users, the device sends the saved authentication parameters of an online user to the authentication server for re-authentication (when a user goes online, the device saves the user authentication information). If the authentication information of the user on the authentication server remains unchanged, the user keeps online. If the authentication information has been changed, the user is logged out and needs to be re-authenticated.

RADIUS CoA

Change of Authorization (CoA) allows the administrator to modify the rights of online users or re-authenticate the users through RADIUS after they are successfully authenticated. [Figure 17-6](#) shows the CoA packet exchange process.

Table 17-1 RADIUS CoA packets

Packet Name	Description
CoA-Request	Indicates a dynamic authorization request packet. When the administrator needs to modify the rights of an online user (for example, the administrator does not want the user to access a website), the RADIUS server can send a dynamic authorization request packet to the RADIUS client to enable the client to modify the rights of the online user.
CoA-ACK	Indicates a dynamic authorization accept packet. If the RADIUS client successfully modifies the user rights, the RADIUS client sends a dynamic authorization accept packet to the RADIUS server.
CoA-NAK	Indicates a dynamic authorization reject packet. If the RADIUS client fails to modify the user rights, the RADIUS client sends a dynamic authorization reject packet to the RADIUS server.

Figure 17-6 CoA packet exchange process

1. The RADIUS server sends a CoA-Request packet to the device based on the service information, requesting the device to modify the user authorization information. The packet may include authorization information such as an ACL rule.
2. After receiving the CoA-Request packet, the device matches the packet with user information on the device to identify the user. If the matching is successful, the authorization information of the user is modified. If the matching fails, the original authorization information of the user is retained.

The device replies with a CoA-ACK or CoA-NAK packet.

- If the change is successful, the device returns a CoA-ACK packet to the RADIUS server.
- If the change fails, the device returns a CoA-NAK packet to the RADIUS server.

The following table lists the Huawei extended RADIUS attributes involved in this feature.

Table 17-2 Huawei extended RADIUS attributes involved in RADIUS CoA

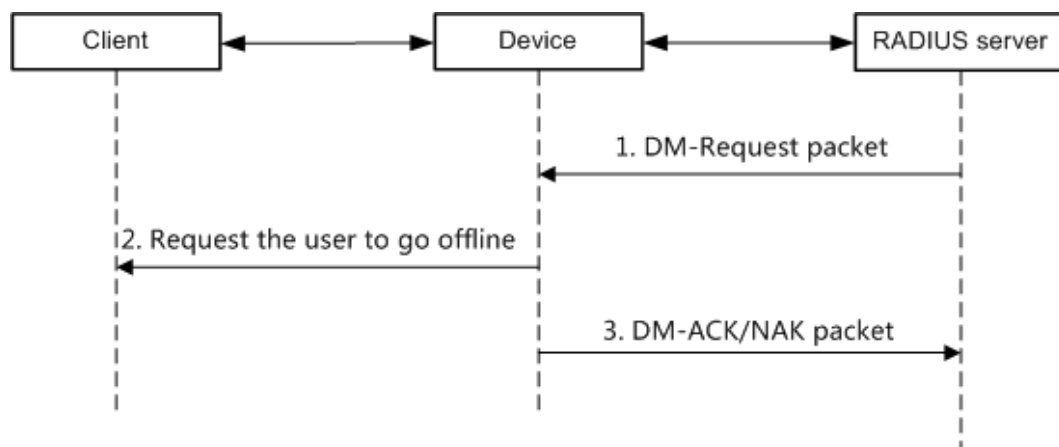
Attribute ID	Attribute Name	Attribute Type	Description
26-238	HW-Ext-Specific	string	User extension attribute. • user-command: The value can be 1, 2, or 3. – 1: Re-authenticates a user. In this case, you need to set this attribute as user-command=1 on the authentication server. NOTE If user-command is set to 1, other authorization attributes are not supported. – 2: The authentication port is intermittently disconnected. In this case, you need to set this attribute as user-command=2 on the authentication server. – 3: The authentication port is disabled. In this case, you need to set this attribute as user-command=3 on the authentication server. NOTE • You can run the display ont port state portid ontid eth-port all command to query the status of an ONU port. • After the authentication port is disabled, you can run the ont port attribute portid ontid eth ont-portid operational-state switch command to restore the port to the normal state.

RADIUS DM

A Disconnect Message (DM) is sent by a RADIUS server to force a user to go offline. [Figure 17-7](#) shows the DM packet exchange process.

Table 17-3 RADIUS DM packets

Packet Name	Description
DM-Request	Indicates a user logout request packet. To log out an online user, the administrator can configure the RADIUS server to send a user offline request packet to the RADIUS client. The RADIUS client then terminates the user connection.
DM-ACK	Indicates a user logout request accept packet. After terminating the user connection, the RADIUS client sends a user logout request accept packet to the RADIUS server.
DM-NAK	Indicates a user logout request reject packet. If the RADIUS client fails to disconnect the user, the RADIUS client sends a user logout request reject packet to the RADIUS server.

Figure 17-7 DM packet exchange process

1. After the administrator forces a user to go offline on the RADIUS server, the RADIUS server sends a DM-Request packet to the device to request the user to go offline.
2. After receiving the DM-Request packet, the device matches the packet with user information on the device to identify the user. If the matching is successful, the device instructs the user to go offline. If the matching fails, the user remains online.
3. The device replies with a DM-ACK or DM-NAK packet.
 - If the user goes offline successfully, the device sends a DM-ACK packet to the RADIUS server.
 - If the user does not go offline, the device sends a DM-NAK packet to the RADIUS server.

Compared with user online authorization or active user offline processes, the CoA/DM request packet is sent by the server, and the CoA/DM response packet is sent by the device in CoA/DM scenarios. If the operation is successful, the device replies with an ACK packet. If the operation fails, the device replies with a NAK packet.

Active RADIUS Server Detection

The reachability and availability of the RADIUS server are the basic conditions for user access authentication. If the authentication server cannot be connected (for example, the network between the device and the authentication server is disconnected or the authentication server is faulty), the RADIUS server cannot authenticate or authorize users. To solve this problem, the device supports the escape function when the RADIUS server is down. That is, all services on a port can access resources in a critical VLAN, for example, in emergency voice call or service assurance scenarios. However, the escape function can be enabled only after the device sets the RADIUS server status to Down. If the status of the RADIUS server is not set to Down and the device cannot communicate with the RADIUS server, users cannot obtain authorization from the server or escape, and cannot access network resources for a long time. Therefore, the device must detect the RADIUS server status in a timely manner so that users can immediately obtain the escape right when the RADIUS server is down. After the RADIUS server goes up, users exit the escape mode and are re-authenticated.

Server Down/Up State Transition

By default, the server is in the Up state. It is marked Down when the detection function is enabled and a new user who initiates an authentication request does not receive any response from the server.

If either the primary or secondary server is down, the device starts to detect the server status at the configured detection interval by sending RADIUS probe packets to the server. After the server returns a response packet, the server status changes to Up and the detection stops.

If both the primary and secondary servers are down, the device does not forward authentication request packets initiated by a user to the server. Instead, the device directly terminates the authentication process and allocates a critical VLAN to the user to enable the escape function. After either of the primary or secondary server goes up, the device sends user authentication request packets to the server to start the authentication process.

ACL

Access control list (ACL) is a widely used tool for filtering network traffic. An ACL can identify specific traffic on the network based on the source IP address, destination IP address, protocol type, and source and destination ports in packets, and then process the traffic accordingly.

On the ONU, different ACLs can be configured to filter different types of users, and then implement different access control policies for the users.

Pre-auth ACL

When a user client connects to the network but does not initiate 802.1X authentication, a pre-auth ACL can be configured to filter user packets that meet certain conditions (such as the specified destination IP address and destination MAC address) so that the user can connect to the specified network, for example, logging in to a website. To use a pre-auth ACL, the system administrator needs to pre-configure ACL rules on the ONU.

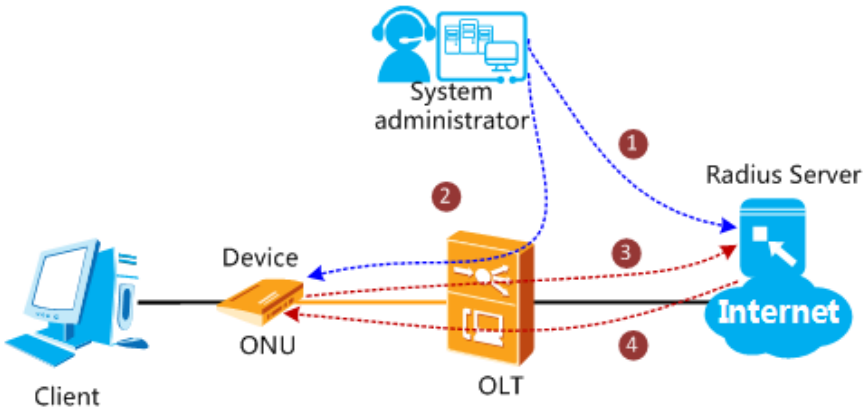
The pre-auth ACL takes effect only in the period from the time when the user fails to be authenticated, the time when the RADIUS server is unreachable, and the

time when the user initiates authentication to the time when the authentication succeeds.

Dynamic ACL

After a user passes 802.1X authentication, the RADIUS server sends a RADIUS packet carrying dynamic ACL information to the network access server (NAS) and applies the ACL rule to the user, as shown in [Figure 17-8](#).

Figure 17-8 Dynamic ACL process



- 1 The system administrator configures the name of the dynamic ACL rule that takes effect after user authentication on the RADIUS server.
- 2 The system administrator configures a dynamic ACL rule on the ONU through the OLT.
- 3 The ONU initiates 802.1X authentication to the RADIUS server.
- 4 The RADIUS server sends the authentication result and dynamic ACL rule name to the ONU, and the ONU enables the specified dynamic ACL rule to take effect.

The dynamic ACL name is carried in the RADIUS standard attribute field Filter-ID, as shown in [Table 17-4](#). In addition, specific rules need to be configured on the device.

Table 17-4 Standard RADIUS attributes involved in dynamic ACL

Attribute ID	Attribute Name	Attribute Type	Description
11	Filter-ID	string	Indicates the name of an IPv4 ACL for a user.

Download ACL

Download ACL is another type of ACL on the RADIUS server. You can configure download ACL rules in plaintext. It also applies to users who are successfully authenticated.

The configuration information of a download ACL is carried by Huawei extended RADIUS attributes, as listed in [Table 17-5](#).

Table 17-5 Huawei extended RADIUS attributes involved in the download ACL feature

Attribute ID	Attribute Name	Attribute Type	Description
26-82	HW-Data-Filter	string	The RADIUS server uses this attribute to deliver ACL rules to users. NOTE - A RADIUS packet can carry multiple No. 26–82 attributes. Currently, each attribute can carry only one ACL rule. - You can run the display access-user user-id user-id command to check whether this attribute takes effect. If the command output displays Dynamic ACL desc (Effective), this attribute takes effect. If Dynamic ACL desc (Ineffective) is displayed, the attribute does not take effect. New attribute format (fields in square brackets are optional) Format: \$number permit/deny [<i>protocol</i>] [<i>direction ip-address</i> [<i>port</i>]] The fields are described as follows: \$: indicates the start character of each ACL rule. number: specifies the last 3 digits of an ACL rule number. The value ranges from 0 to 999. The first 2 digits of an ACL rule number are fixed to 10. For example, if an ACL rule number is 12, the actual ACL rule number is 10012. permit/deny: indicates the ACL action. permit indicates that access is permitted, and deny indicates that access is denied. protocol: specifies the protocol type. The value can be tcp or udp. direction: indicates the IP address type. The value can be dst or src. dst indicates the destination IP address, and src indicates the source IP address. ip-address: specifies an IP address. The value can be any or x.x.x.x/xx. x.x.x.x indicates an IP address in dotted decimal notation and xx indicates the mask in decimal notation. The IP address and mask are separated by a slash (/). port: indicates a port number. Currently, only one port is supported. Example:

Attribute ID	Attribute Name	Attribute Type	Description
			• \$1 permit dst 10.0.239.192/26 • \$2 permit udp src any 8080 • \$5 deny Old Attribute Format acl <i>number</i> key1 <i>key-value1</i>... keyN <i>key-valueN</i> permit/deny The fields are described as follows: • acl: indicates that ACL rules are delivered. • <i>number</i>: specifies the number of an ACL rule. The value ranges from 10000 to 10999. • keyM <i>key-valueM</i> (1≤M≤N): indicates the keyword and value of an ACL rule. The keyword can be: – dest-ip <i>ip-address</i>: specifies the destination IP address. The value is in dotted decimal notation. When the destination IP address is 0.0.0.0, this parameter does not need to be configured. – dest-ipmask <i>mask</i>: specifies the destination IP address mask. For NAC users, the value is an integer ranging from 0 to 32. For VM users, the value is in dotted decimal notation. If the IP address mask is 0, you do not need to set this parameter. – tcp-srcport <i>port</i>: specifies the source TCP start port number. The value ranges from 0 to 65535. – tcp-srcport-end <i>port</i>: specifies the source TCP end port number. The value ranges from 0 to 65535 and must be greater than the start port number. – tcp-dstport <i>port</i>: specifies the destination TCP start port number. The value ranges from 0 to 65535. – tcp-dstport-end <i>port</i>: specifies the destination TCP end port number. The value ranges from 0 to 65535 and must be greater than the start port number. – udp-srcport <i>port</i>: specifies the source UDP start port number. The value ranges from 0 to 65535.

Attribute ID	Attribute Name	Attribute Type	Description
			– udp-srcport-end <i>port</i>: specifies the source UDP end port number. The value ranges from 0 to 65535 and must be greater than the start port number. – udp-dstport <i>port</i>: specifies the destination UDP start port number. The value ranges from 0 to 65535. – udp-dstport-end <i>port</i>: specifies the destination UDP end port number. The value ranges from 0 to 65535 and must be greater than the start port number. • permit/deny: indicates the ACL action. permit indicates that access is permitted, and deny indicates that access is denied. NOTE • It is recommended that the standard RADIUS attribute Filter-Id be used to deliver ACLs. • A maximum of 64 ACL rules can be delivered to a single user. If too many ACL rules are delivered, the number of online users and the access rate will be affected. It is recommended that no more than 16 ACL rules be delivered to a single user. • When the direct forwarding mode is used, ACL rules cannot be delivered through this attribute to wireless users. Instead, ACL rules can be delivered through standard RADIUS attribute 11. • All keywords are case insensitive. All keywords and (or) key values are separated by spaces. The sequence of keywords can be flexible. The permit and deny keywords can be placed after <i>number</i> or at the end of the statement. Example: • acl 10005 deny • acl 10006 tcp-dstport 5080 permit • acl 10007 dest-ip 10.11.11.2 dest-ipmask 32 permit • acl 10008 dest-ip 10.11.11.3 dest-ipmask 32 udp-dstport 5070 permit • acl 10009 dest-ip 11.1

Automatic Logout After Idle Time Expires

When the idle time of a user exceeds the specified time, the user is automatically logged out. You can configure the standard RADIUS attribute field Idle-Timeout on the server to implement this function.

Table 17-6 Standard RADIUS attributes

Attribute ID	Attribute Name	Attribute Type	Description
28	Idle-Timeout	integer	Indicates the maximum idle time of a user before a session ends, that is, the idle logout time of the user, in seconds.

17.5 Configuring 802.1X Authentication

This section describes how to configure 802.1X authentication.

17.5.1 ONU Functioning as the 802.1x Authentication Device

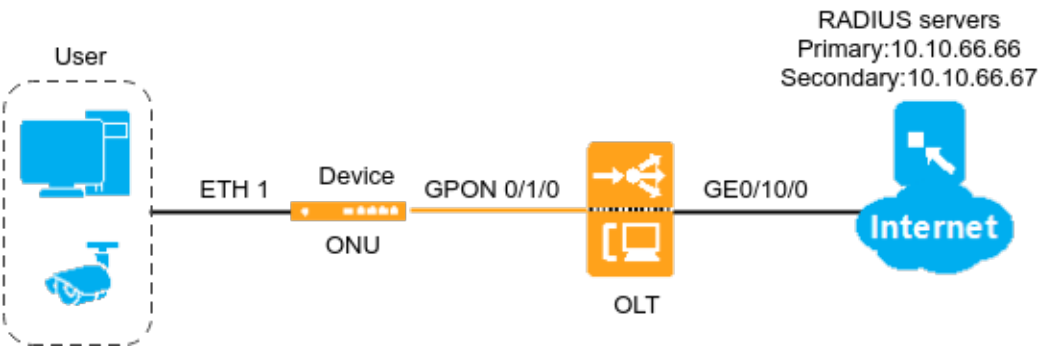
The ONU functions as the 802.1X authentication device. 802.1x authentication configurations are delivered to the ONU through the OLT.

Prerequisites

- The OLT has been connected to a Layer 3 switch.
- The ONU is online and can be managed by the OLT.
- The remote RADIUS server has been deployed, and the network connection is normal.

Figure 17-9 shows the networking diagram for RADIUS authentication.

Figure 17-9 Networking diagram for RADIUS authentication



Data Planning

Configuration Item	Value
Networking data	PON port ID: 0/1/0 Upstream port: 0/10/0 ONU ID: 0 ONU IP: 10.10.10.20

Configuration Item	Value
802.1X authentication	Port authentication mode: auto Authentication method: EAP ONU port authentication granularity: MAC address authentication NOTE Port-based authentication and MAC address-based authentication are applicable to the following scenarios: • In MAC-based authentication mode, every 802.1X user accessing an interface must be authenticated. If a user goes offline, other authenticated users can still access the network. This authentication mode applies to scattered users. • In port-based authentication mode, other 802.1X users can use network resources without being authenticated as long as one user on the interface is successfully authenticated. However, if the authenticated user goes offline, other users cannot use network resources. This authentication mode applies to group users. • By default, the port-based authentication mode is used.
VLAN planning	• VLAN ID of the management WAN port: 11 • Guest VLAN, SVLAN: 10; CVLAN: 10 • Restrict VLAN, SVLAN: 20; CVLAN: 20 • Critical VLAN, SVLAN: 30; CVLAN: 30 • Dynamic Service VLAN, SVLAN: 40; CVLAN: 40 NOTE The preceding VLANs must be mapped to GEM ports in the line profile and service profile during network planning.
RADIUS server	• Primary authentication server: IP address: 10.10.66.66; Port number: 1812 • Secondary authentication server: IP address: 10.10.66.67; Port number: 1812 • Shared primary key: 0123456789123456 • Shared secondary key: 0123456789123456 • The IP address and shared key of the charging and authorization servers are the same as those of the authentication server.

Procedure

Step 1 Create and configure the dot1x (802.1X) profile.

Set the ONU port authentication mode to MAC-based authentication, enable dot1x authentication, set the port authentication mode to auto, set the

authentication method to EAP, and configure the related VLAN. If ONU port 1 connects to a terminal that does not support 802.1X, MAB authentication needs to be enabled.

NOTE

The ONU port authentication granularity can be set to MAC address authentication only when the ONU supports the MAC address authentication granularity. Otherwise, the ONU configuration fails.

```
huawei(config)#ont dot1x-profile profile-id 1
huawei(config-dot1x-profile-1)#port dot1x eth 1 enable
huawei(config-dot1x-profile-1)#port dot1x authentication-method eth 1 eap
huawei(config-dot1x-profile-1)#port dot1x port-control eth 1 auto
huawei(config-dot1x-profile-1)#port dot1x port-method eth 1 mac
huawei(config-dot1x-profile-1)#port dot1x guest-vlan eth 1 10
huawei(config-dot1x-profile-1)#port dot1x restrict-vlan eth 1 20
huawei(config-dot1x-profile-1)#port dot1x critical-vlan eth 1 30
huawei(config-dot1x-profile-1)#port mac-bypass eth 1 enable
huawei(config-dot1x-profile-1)#quit
```

Step 2 Configure a WAN profile.

```
huawei(config)#ont wan-profile profile-id 9 profile-name wan_prof_hwtest
huawei(config-wan-profile-9)#connection-type route
huawei(config-wan-profile-9)#quit
```

Step 3 Configure the IP address of the ONU and the IP interface index of the Internet service, and bind the WAN profile.

Set the static IP address of the ONU to 10.10.10.20 and the IP interface index of the Internet service to 0.

```
huawei(config)#gpon ont home-gateway config-method omci
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 0 ip-index 0 static ip-address 10.10.10.20 mask
255.255.255.0 vlan 11 gateway 10.10.10.10
huawei(config-if-gpon-0/1)#ont internet-config 0 0 ip-index 0
huawei(config-if-gpon-0/1)#ont wan-config 0 0 ip-index 0 profile-id 9
huawei(config-if-gpon-0/1)#quit
```

Step 4 Configure the RADIUS server IP address and authentication domain.

Configure the RADIUS server 10.10.66.66 as the primary authentication server, the RADIUS server 10.10.66.67 as the secondary authentication server, and configure the primary and secondary shared keys as 0123456789123456. Set the authentication timeout interval to 20s and the maximum number of retries to 3. RADIUS authentication servers work in primary/secondary mode.

```
huawei(config-dot1x-profile-1)#radius-server authentication 10.10.66.66 1812
huawei(config-dot1x-profile-1)#radius-server shared-key 0123456789123456
huawei(config-dot1x-profile-1)#radius-server authentication 10.10.66.67 1812 secondary
huawei(config-dot1x-profile-1)#radius-server shared-key 0123456789123456 secondary
huawei(config-dot1x-profile-1)#radius-server user-name domain-included
huawei(config-dot1x-profile-1)#radius-server accounting 10.10.66.66 1813
huawei(config-dot1x-profile-1)#radius-server accounting 10.10.66.67 1813 secondary
huawei(config-dot1x-profile-1)#radius-server accounting shared-key 0123456789123456
huawei(config-dot1x-profile-1)#radius-server accounting shared-key 0123456789123456 secondary
huawei(config-dot1x-profile-1)#radius-server authorization 10.10.66.66 shared-key 0123456789123456
huawei(config-dot1x-profile-1)#radius-server authorization 10.10.66.67 shared-key 0123456789123456
huawei(config-dot1x-profile-1)#radius-server timeout 20
huawei(config-dot1x-profile-1)#radius-server retransmit 3
huawei(config-dot1x-profile-1)#radius-server authentication mode backup
huawei(config-dot1x-profile-1)#quit
```

Step 5 Configure service flows for 802.1X authentication.

- Add a service flow to the RADIUS server. Set SVLAN and CVLAN to 11.
huawei(config)#vlan 11 smart
huawei(config)#port vlan 11 0/10 0
huawei(config)#service-port vlan 11 gpon 0/1/0 ont 0 gempport 0 multi-service user-vlan 11
- Add a service flow to the Guest network. Set SVLAN and CVLAN to 10.
huawei(config)#vlan 10 smart
huawei(config)#port vlan 10 0/10 0
huawei(config)#service-port vlan 10 gpon 0/1/0 ont 0 gempport 0 multi-service user-vlan 10
- Add a service flow to the Restrict network. Set SVLAN and CVLAN to 20.
huawei(config)#vlan 20 smart
huawei(config)#port vlan 20 0/10 0
huawei(config)#service-port vlan 20 gpon 0/1/0 ont 0 gempport 0 multi-service user-vlan 20
- Add a service flow to the Critical network. Set SVLAN and CVLAN to 30.
huawei(config)#vlan 30 smart
huawei(config)#port vlan 30 0/10 0
huawei(config)#service-port vlan 30 gpon 0/1/0 ont 0 gempport 0 multi-service user-vlan 30
- Add a service flow to the Dynamic Service network. Set SVLAN and CVLAN to 40.
huawei(config)#vlan 40 smart
huawei(config)#port vlan 40 0/10 0
huawei(config)#service-port vlan 40 gpon 0/1/0 ont 0 gempport 0 multi-service user-vlan 40
huawei(config)#save

Step 6 (Optional) Configure the Pre-auth ACL function of the ONU port.

- Configure the pre-auth ACL for ONU port 1 to allow the user packets with the destination IP address 10.10.100.1 to pass through.
huawei(config)#ont acl-profile profile-id 1
huawei(config-acl-profile-1)#acl add acl-id 1 acl-name acl-preauth
huawei(config-acl-profile-1)#rule add acl-id 1 rule-id 0 priority 1 permit
huawei(config-acl-profile-1)#rule add acl-id 1 rule-id 1 priority 1 deny
huawei(config-acl-profile-1)#conditon add acl-id 1 rule-id 0 condition-id 0 validation-operator equal field dst-ipv4-address 10.10.100.1
huawei(config-acl-profile-1)commit
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont acl-config 0 0 profile-id 1
huawei(config-if-gpon-0/1)#quit
huawei(config)#ont dot1x-profile profile-id 1
huawei(config-dot1x-profile-1)#port dot1x acl-id eth 1 1
huawei(config-dot1x-profile-1)#quit

Step 7 (Optional) Configure the dynamic ACL function for ONU users.

- Configure a dynamic ACL for the ONU to allow user packets with destination MAC address 00e0-fc00-0033 to pass through.
huawei(config)#ont acl-profile profile-id 1
huawei(config-acl-profile-1)#acl add acl-id 2 acl-name acl-dynamic.in
huawei(config-acl-profile-1)#rule add acl-id 2 rule-id 0 priority 1 permit
huawei(config-acl-profile-1)#conditon add acl-id 2 rule-id 0 condition-id 0 validation-operator equal field dst-mac-address 00e0-fc00-0033
huawei(config-acl-profile-1)commit
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont acl-config 0 0 profile-id 1
huawei(config-if-gpon-0/1)#quit

Step 8 (Optional) Configure the ONU to automatically detect the RADIUS server.

Use the specified user name and password to detect the RADIUS authentication server at an interval of 30 seconds.

```
huawei(config)#ont dot1x-profile profile-id 1
huawei(config-dot1x-profile-1)radius-server auto-detect username user@2020 password
huawei(config-dot1x-profile-1)radius-server auto-detect interval 30
huawei(config-dot1x-profile-1)quit
```

Step 9 Bind the ONU to the dot1x profile.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont dot1x-config 0 0 profile-id 1
huawei(config-if-gpon-0/1)#quit
```

----End

Result

After the ONU is configured, it can be used as an access point for 802.1X authentication. A connected terminal can access the LAN by using the user name and password, or by using the MAC address.

17.5.2 OLT Functioning as the 802.1X Authentication Device (Configured on the CLI).

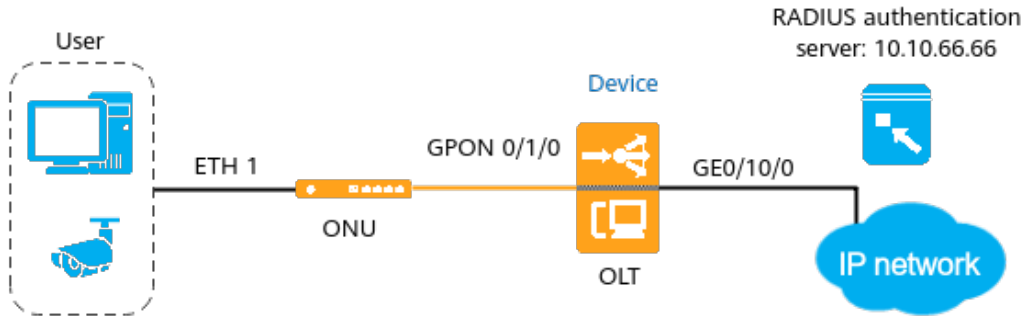
As the 802.1X authentication device, an OLT authenticates clients and controls the network access rights or scope of the clients.

Prerequisites

The remote RADIUS server has been deployed, and the network connection is normal.

Figure 17-10 shows the networking diagram for RADIUS authentication.

Figure 17-10 Networking diagram for RADIUS authentication



Data Planning

Configuration Item	Value
Networking data	PON port: 0/1/0 Upstream port: 0/10/0 ONU ID: 0
802.1X authentication	Service flow ID: 1 Service VLAN ID for MAC address-based 802.1X authentication: 20 Enabling MAC bypass authentication
VLAN planning	User side VLAN: 100

Configuration Item	Value
RADIUS server	- Authentication server IP address: 10.10.66.66; port number: 1812 - Shared key: 0123456789123456

Procedure

Step 1 Configure a GPON ONU profile. The line profile is configured with the 802.1p priority mapping and the service profile is configured with the transparent transmission mode. In this way, packets of all VLANs on ONUs can pass through, and service flows can be dynamically created when the RADIUS server issues any dynamic VLAN.

1. Configure a DBA profile.

Run the **display dba-profile** command to query existing DBA profiles in the system. If existing DBA profiles in the system do not meet the requirement, run the **dba-profile add** command to create a DBA profile.

Add a DBA profile with service profile ID 10 and type 4.

```
huawei(config)#dba-profile add profile-id 10 type4 max 1024000
```

2. Configure an ONU line profile.

Add GPON ONU line profile 10 and bind T-CONT 1 to DBA profile 10. In this way, the T-CONT provides flexible DBA solutions based on different configurations in the DBA profile.

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 1 dba-profile-id 10
```

Use GEM port 0 to carry services and bind the GEM port to a T-CONT.

```
huawei(config-gpon-lineprofile-10)#gem add 0 eth tcont 1
```

Set the mapping mode between GEM ports and the ONU-side services to 802.1p priority mapping.

```
huawei(config-gpon-lineprofile-10)#mapping-mode priority
huawei(config-gpon-lineprofile-10)#gem mapping 0 0 priority 0
huawei(config-gpon-lineprofile-10)#gem mapping 0 1 priority 1
huawei(config-gpon-lineprofile-10)#gem mapping 0 2 priority 2
huawei(config-gpon-lineprofile-10)#gem mapping 0 3 priority 3
huawei(config-gpon-lineprofile-10)#gem mapping 0 4 priority 4
huawei(config-gpon-lineprofile-10)#gem mapping 0 5 priority 5
huawei(config-gpon-lineprofile-10)#gem mapping 0 6 priority 6
huawei(config-gpon-lineprofile-10)#gem mapping 0 7 priority 7
```

After the configuration is completed, run the **commit** command to make the configured parameters take effect.

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

3. Configure an ONU service profile.

Set the profile ID to 100. Set the maximum number of auto-adaptive ETH ports on an ONU to 8 in the ONU service profile. The port capability set profile of an ONU must be the same as the actual capability set of the ONU. Set the packet forwarding mode of a port to TAG transparent transmission. In this mode, the port does not process the packets and keeps the VLAN tag unchanged.

```
huawei(config)#ont-srvprofile gpon profile-id 10
huawei(config-gpon-srvprofile-10)#ont-port eth adaptive 8
```

```
huawei(config-gpon-srvprofile-10)#port vlan eth 1 transparent
huawei(config-gpon-srvprofile-10)#port vlan eth 2 transparent
huawei(config-gpon-srvprofile-10)#port vlan eth 3 transparent
huawei(config-gpon-srvprofile-10)#port vlan eth 4 transparent
huawei(config-gpon-srvprofile-10)#port vlan eth 5 transparent
huawei(config-gpon-srvprofile-10)#port vlan eth 6 transparent
huawei(config-gpon-srvprofile-10)#port vlan eth 7 transparent
huawei(config-gpon-srvprofile-10)#port vlan eth 8 transparent
huawei(config-gpon-srvprofile-10)#commit
huawei(config-gpon-srvprofile-10)#quit
```

Step 2 Add an ONU to the OLT.

Connect an ONU to a GPON port of the OLT using a fiber. Services can be configured only after an ONU is successfully added to the OLT. Set the native VLAN of the port as the authentication VLAN.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont add 0 0 sn-auth 1234567891234560 omci ont-lineprofile-id 10 ont-
srvprofile-id 10
huawei(config-if-gpon-0/1)#ont port native-vlan 0 0 eth 1 vlan 100
```

Step 3 Create an S-VLAN and add an upstream port to it.

```
huawei(config)#vlan 100 smart
huawei(config)#port vlan 100 0/10 0
```

Step 4 Create service flows for 802.1X authentication.

```
huawei(config)#service-port 1 vlan 100 gpon 0/1/0 ont 0 gempport 0 multi-service user-vlan 100 tag-
transform translate
```

Step 5 Configure the RADIUS protocol.

Set the IP address of the RADIUS server to 10.10.66.66 and set the shared key to 0123456789123456.

Configure a RADIUS server profile named far1 for 802.1X authentication.

```
huawei(config)#radius-server template far1
huawei(config-radius-far1)#radius-server shared-key-cipher 0123456789123456
huawei(config-radius-far1)#radius-server authentication 10.10.66.66 1812
huawei(config-radius-far1)#quit
```

Configure the RADIUS server profile named default for MAC bypass authentication, in which the MAC bypass authentication packet does not contain a domain name.

```
huawei(config)#radius-server template default
huawei(config-radius-default)#radius-server shared-key-cipher 0123456789123456
huawei(config-radius-default)#radius-server authentication 10.10.66.66 1812
huawei(config-radius-default)#undo radius-server user-name domain-included
huawei(config-radius-default)#quit
```

Configure the interface of the server source IP address for the OLT to communicate with the server.

```
huawei(config)#radius-server source-interface vlanif 999
```

Step 6 Configure the authentication scheme.

- Configure an 802.1X authentication scheme far1 and use RADIUS to authenticate users.

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme far1
huawei(config-aaa-authen-far1)#authentication-mode radius
huawei(config-aaa-authen-far1)#quit
```

- Create a domain named **far1** and bind the created authentication scheme and RADIUS server profile to the domain.

 NOTE

A domain is a group of users of the same type. Generally, in a user name in the format of `userid@domain-name`, *domain-name* following @ is the domain name, and *userid* is the user name used for identity authentication.

```
huawei(config-aaa)#domain far1
huawei(config-aaa-domain-far1)#authentication-scheme far1
huawei(config-aaa-domain-far1)#radius-server far1
```

- Configure a MAC bypass authentication scheme named **default** and use RADIUS to authenticate users.

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme default
huawei(config-aaa-authen-default)#authentication-mode radius
huawei(config-aaa-authen-default)#quit
```

- Create a domain named **default** and bind the created authentication scheme and RADIUS server profile to the domain.

```
huawei(config-aaa)#domain default
huawei(config-aaa-domain-default)#authentication-scheme default
huawei(config-aaa-domain-default)#radius-server default
```

Step 7 Configure service port-based 802.1X authentication.

Enable the 802.1X global switch. Enable 802.1X authentication, MAC bypass authentication, and DHCP-triggered authentication on service port 1.

```
huawei(config)#dot1x enable
huawei(config)#dot1x service-port 1
huawei(config)#dot1x mac-bypass enable
huawei(config)#dot1x mac-bypass service-port 1
huawei(config)#dot1x dhcp-trigger enable
```

Step 8 Configure MAC address-based 802.1X authentication.

Enable the 802.1X global switch. Enable 802.1X authentication and DHCP-triggered authentication on service port 1.

 NOTE

- The service VLAN ID for 802.1X authentication must be different from the guest VLAN ID. Otherwise, dynamic service port creation fails.
- If a service VLAN is configured for 802.1X authentication and the RADIUS authentication server delivers another service VLAN, the service VLAN delivered by the RADIUS authentication server is preferentially used.

```
huawei(config)#dot1x enable
huawei(config)#dot1x service-port auth-method 1 mac-based
huawei(config)#dot1x service-port 1
huawei(config)#dot1x service-vlan 20
huawei(config)#dot1x dhcp-trigger enable
```

----End

Operation Result

After the OLT is configured, it can be used as an access point for 802.1X authentication. A connected terminal can access the LAN by using the user name and password, or by using the MAC address.

17.5.3 Core Switch Functioning as the 802.1X Authentication Device

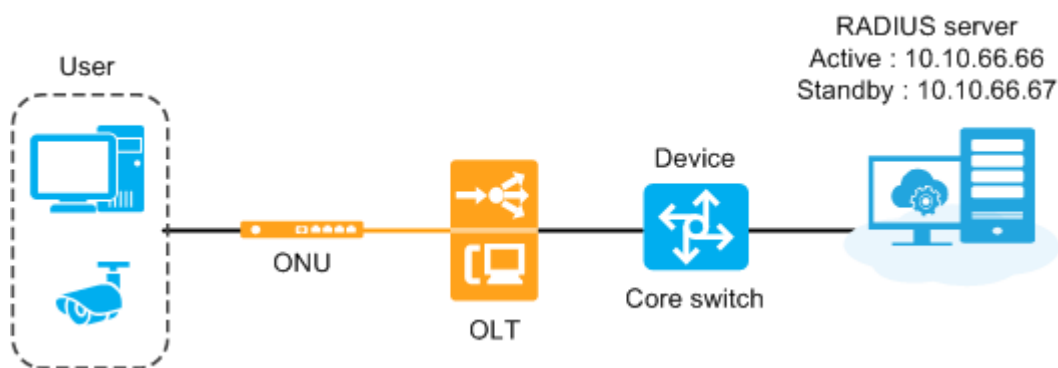
The core switch functions as the 802.1X authentication device, and the transparent transmission function is configured on the OLT for 802.1x protocol packets.

Prerequisites

- The ONU/OLT is online and in the normal state.
- The ONU has been configured to transparently transmit EAPOL and BPDU packets.

Figure 17-11 shows the networking diagram for RADIUS authentication.

Figure 17-11 Networking diagram for RADIUS authentication



Procedure

- Configure EAPOL packets to be transparently transmitted on the OLT.

```
huawei(config)#protocol permit-forwarding eapol enable
```

- Configure BPDU packets to be transparently transmitted on the OLT.

```
huawei(config)#vlan service-profile profile-id 10
huawei(config-vlan-srvprof-10)#bpdu tunnel enable
huawei(config-vlan-srvprof-10)#commit
huawei(config-vlan-srvprof-10)#quit
huawei(config)#vlan bind service-profile 11 profile-id 10
```

Operation Result

After the configuration is completed, 802.1x protocol packets can be transparently transmitted to the core switch, and the core switch then implements 802.1X authentication.

Configuration Script

```
protocol permit-forwarding eapol enable
vlan service-profile profile-id 10
bpdu tunnel enable
commit
quit
vlan bind service-profile 11 profile-id 10
```