Table of Contents

Chapter 1 Configuration of Newly Added 802.1x Features 1-1
1.1 802.1x Client Version Checking Configuration 1-1
1.1.1 Enabling the 802.1x Client Version Checking Function 1-1
1.1.2 Configuring the Maximum Number of Retires to Send Version Checking Request Packets 1-1
1.1.3 Configuring the Version Checking Timer 1-2
1.1.4 802.1x Client Version Checking Configuration Example 1-2
1.2 Guest VLAN Configuration 1-3
1.2.1 Introduction to Guest VLAN 1-3
1.2.2 Prerequisites 1-3
1.2.3 Guest VLAN Configuration 1-4
1.2.4 Guest VLAN Configuration Example 1-5
1.3 802.1x PEAP Configuration 1-5
1.3.1 Configuring 802.1x EAP Authentication 1-6
1.3.2 802.1x PEAP Configuration Example 1-6
1.4 Cooperation of 802.1x authentication and MAC address-based Authentication 1-7
1.5 The 802.1x Trusted MAC Address Synchronization Function 1-7
1.6 802.1x Supplicant System Checking 1-8

Chapter 2 Newly Added 802.1x-Related Commands 2-1
2.1 Newly Added 802.1x-Related Commands 2-1
2.1.1 dot1x authentication-method 2-1
2.1.2 dot1x guest-vlan 2-2
2.1.3 dot1x retry-version-max 2-3
2.1.4 dot1x supp-proxy-check 2-4
2.1.5 dot1x timer ver-period 2-6
2.1.6 dot1x version-check 2-7

Chapter 1 Configuration of Newly Added 802.1x Features

1.1 802.1x Client Version Checking Configuration

With the 802.1x client version checking function enabled on a switch, the switch checks the version and validity of the 802.1x client running on supplicant systems to prevent those that use earlier versions of 802.1x client or illegal clients from logging in. The following are configurations concerning the 802.1x client version checking function.

- Enabling the 802.1x Client Version Checking Function
- Configuring the Maximum Number of Retires to Send Version Checking Request Packets
- Configuring the Version Checking Timer

1.1.1 Enabling the 802.1x Client Version Checking Function

Table 1-1 Enable the 802.1x client version checking function

Operation	Command	Description
Enter system view	**system-view**	—
Enable the 802.1x client version checking function	**dot1x version-check** [**interface** *interface-list*]	Required By default, 802.1x client version checking is disabled.

Note:

- As for the **dot1x version-check** command, if you execute it in system view without specifying the *interface-list* argument, the command applies to all ports. Otherwise, the command applies to the specified ports.
- You can also execute the **dot1x version-check** command in Ethernet port view. In this case, the *interface-list* argument is unnecessary and the command applies to the current port only.

1.1.2 Configuring the Maximum Number of Retires to Send Version Checking Request Packets

After sending a version request packet to a supplicant system, a switch sends another one to the supplicant system if it does not receive the response from the supplicant

system for the period set by the version checking timer. It continues to send version request packets to the supplicant system if it still does not receive the response from the supplicant system. Such a process goes on and on until the maximum number of retries is reached. If the maximum number of retries is reached and the supplicant system still does not respond, the switch ceases checking the client version of the supplicant system and continues the followed authentication procedures.

Table 1-2 Configure the maximum number of retires to send version checking request packets

Operation	Command	Description
Enter system view	**system-view**	—
Configure the maximum number of retires to send version checking request packets	**dot1x retry-version-max** *max-retry-version-value*	Optional By default, the maximum number of retires to send version checking request packets is 3.

1.1.3 Configuring the Version Checking Timer

Table 1-3 Configure the version checking timer

Operation	Command	Description
Enter system view	**system-view**	—
Configure the version checking timer	**dot1x timer ver-period** *ver-period-value*	Optional By default, the version checking timer is set to 30 seconds.

It is recommended that you adopt the default version checking timer setting.

1.1.4 802.1x Client Version Checking Configuration Example

I. Network requirements

- The 802.1x client version checking function is enabled on all ports.
- Configure the maximum number of retires to send version checking request packets to be 6.
- Set the version checking timer to 5 seconds.

II. Configuration procedures

Enter system view.

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

Enable the 802.1x client version checking function on all ports.

```
[Quidway] dot1x version-check
```

Configure the maximum number of retires to send version checking request packets to be 6.

```
[Quidway] dot1x retry-version-max 6
```

Set the version checking timer to 5 seconds.

```
[Quidway] dot1x timer ver-period 5
```

1.2 Guest VLAN Configuration

1.2.1 Introduction to Guest VLAN

The Guest VLAN function enables supplicant systems that are not authenticated to access specific resources and thus perform the corresponding operations, such as obtaining 802.1x client, upgrading client, or obtaining other upgrading programs.

With the Guest VLAN function enabled, supplicant systems that do not have 802.1x client installed can access specific network resources. And those that have 802.1x client installed can upgrade their 802.1x clients without being authenticated.

When the Guest VLAN function is enabled:

- The switch broadcasts active authentication packets to all 802.1x-enabled ports.
- The switch adds the ports that do not return response packets to Guest VLAN When the maximum number of authentication retries is reached.
- Users belonging to the Guest VLAN can access the resources of the Guest VLAN without being authenticated. But they need to be authenticated before accessing external resources.

1.2.2 Prerequisites

- The ports operate in port-based authentication mode.
- The VLAN specified to be the Guest VLAN already exists.

1.2.3 Guest VLAN Configuration

I. Configuring Guest VLAN in system view

Table 1-4 Configure Guest VLAN in system view

Operation	Command	Description
Enter system view	**system-view**	—
Configure Guest VLAN for specified ports	**dot1x guest-vlan** *vlan-id* [**interface** *interface-list*]	Required This operation applies to all ports of the switch if you do not provide the *interface-list* argument. And if you specify the *interface-list* argument, the operation applies to the specified Ethernet ports.

II. Configure Guest VLAN in Ethernet port view

Table 1-5 Configure Guest VLAN in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-num*	—
Configure Guest VLAN for the port	**dot1x guest-vlan** *vlan-id*	Required This operation configures Guest VLAN for the current port only.

Caution:

- The Guest VLAN function is available only when the switch operates in the port-based authentication mode.
- Only one Guest VLAN can be configured for a switch.
- Supplicant systems that are not authenticated, fail to pass the authentication, or are offline belong to Guest VLANs.

1.2.4 Guest VLAN Configuration Example

I. Network requirements

- Create VLAN 2.
- Configure GigabitEthernet1/0/1 port to operate in port-based authentication mode.
- Configure Guest VLAN for GigabitEthernet1/0/1 port.

II. Configuration procedure

Enter system view.

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

Create VLAN 2.

```
[Quidway] vlan 2
```

Enter GigabitEthernet1/0/1 port view.

```
[Quidway] interface GigabitEthernet1/0/1
```

Configure the port to operate in port-based authentication mode.

```
[Quidway-GigabitEthernet1/0/1] dot1x port-method portbased
```

Configure Guest VLAN for the port.

```
[Quidway-GigabitEthernet1/0/1] dot1x guest-vlan 2
```

1.3 802.1x PEAP Configuration

Protected extensible authentication protocol (PEAP) authenticates supplicant systems in a securer way. With PEAP employed, a security channel is created, which is encrypted and is protected using transport level security (TLS) to ensure integrity. And authentication is carried out through a new type of EAP (extensible authentication protocol) negotiation between supplicant systems and authentication servers.

The EAP-TLS mode authenticates supplicant systems by authenticating licenses of both authentication servers and supplicant systems on both sides. In this mode, supplicant systems are authenticated by their licenses only, which are applied for from authentication servers. User name and password are not needed. Before the course of authentication, a supplicant system and the authentication server negotiate with each other by invoking TLS mechanism to obtain the way to encrypt session and then verify the licenses of each other in the way just negotiated.

As the three authentication modes, that is, PEAP, EAP-TLS, and EAP-MD5, are all EAP authentication mode for a switch, you can perform the operations listed in Table 1-6 to specify any one of the three authentication modes. The actual authentication mode adopted depends on the authentication mode configured on the supplicant system.

1.3.1 Configuring 802.1x EAP Authentication

Table 1-6 Configure 802.1x EAP authentication

Operation	Command	Description
Enter system view	**system-view**	—
Configure to authenticate supplicant systems by using EAP	**dot1x authentication-method eap**	Required By default, supplicant systems are authenticated by using CHAP (challenge handshake authentication protocol).
Enter Ethernet port view (supplicant system side)	**interface** *interface-type interface-number*	—
Configure the port to operate in MAC address-based authentication mode	**dot1x port-method macbased**	Optional By default, an Ethernet port operates in MAC address-based authentication mode. When using EAP to authenticate supplicant systems, make sure the related ports operate in MAC address-based authentication mode.

1.3.2 802.1x PEAP Configuration Example

I. Network requirements

- A supplicant system is connected to Ethernet1/0/1 port of a switch.
- Control the accesses to the Internet by authenticating supplicant systems on each port of the switch using PEAP. The ports operate in MAC address-based authentication mode.

II. Network diagram

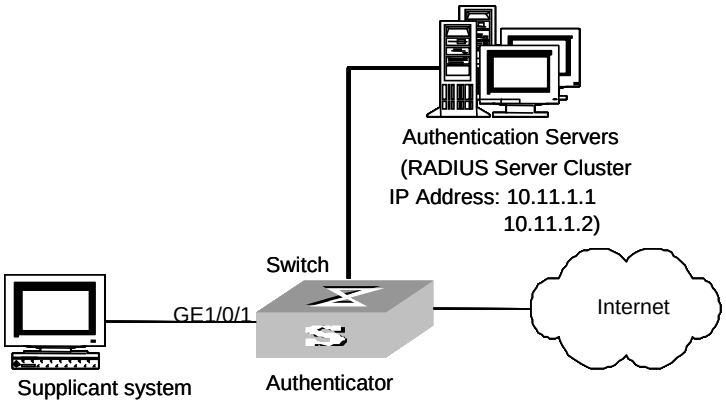

Figure 1-1 Network diagram for 802.1x PEAP configuration

III. Configuration procedure

The following configurations assume that PEAP is selected on 802.1x clients and the RADIUS server to authenticate 802.1x supplicant systems.

Configure the switch.

Enter system view.

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

Enable 802.1x globally.

```
[Quidway] dot1x
```

Enable 802.1x for GigabitEthernet1/0/1 port.

```
[Quidway] dot1x interface GigabitEthernet 1/0/1
```

Configure to use 802.1x PEAP to authenticate supplicant systems.

```
[Quidway] dot1x authentication-method eap
```

Enter GigabitEthernet1/0/1 port view.

```
[Quidway] interface GigabitEthernet 1/0/1
```

Configure the port to operate in MAC address-based authentication mode. (By default, a port operates in MAC address-based authentication mode.)

```
[Quidway] dot1x port-method macbased
```

1.4 Cooperation of 802.1x authentication and MAC address-based Authentication

You can specify to perform both 802.1x authentication and centralized MAC address-based authentication simultaneously on the ports of an S5600 series switch.

1.5 The 802.1x Trusted MAC Address Synchronization Function

Trusted MAC address here refers to the MAC address of a supplicant system that passes 802.1x authentication and MAC address-based authentication. In this case, the MAC address becomes a trusted Mac address. The 802.1x trusted MAC Address synchronization function propagates the trusted MAC addresses in IRF (intelligent resilient framework) if the corresponding supplicant systems pass the authentication performed by IRF-enabled switches.

- In an IRF that does not support the 802.1x trusted MAC address synchronization function, an authentication operation is only performed in the unit where the port with the supplicant system attached resides in. And after the supplicant system passes the authentication, its MAC address is not propagated to other units (That is, the MAC address can only be recognized by the unit the supplicant system directly connected to.) This may result in broadcast storms in the fabric.

- In an IRF that supports the 802.1x trusted MAC address synchronization function, the MAC address of an authenticated supplicant system is propagated in all units of the fabric. And when the supplicant system logs off, all the units in the fabric remove the corresponding MAC address. That is, trusted MAC addresses are synchronized in all units whenever supplicant systems join in or leave a fabric.

1.6 802.1x Supplicant System Checking

When accompanied by a CAMS server, an S5600 series switch can check for:

- Supplicant systems logging in through proxies
- Supplicant systems logging in through IE proxies
- Whether or not a supplicant system logs in with more than one network adapters installed in it being active

An S5600 series switch can optionally take the following measures against any of the three cases:

- Disconnecting the supplicant system and sending Trap packets (This can be achieved by using the **dot1x supp-proxy-check logoff** command.)
- Sending Trap packets without disconnecting the supplicant system (This can be achieved by using the **dot1x supp-proxy-check trap** command.)

To achieve this function, following are to meet for 802.1x clients and CAMS.

- The 802.1x clients are capable of detecting multiple network adapters, proxies, and IE proxies.
- CAMS is configured to disable use of multiple network adapters, proxies, or IE proxies.

By default, an 802.1x client allows the use of multiple network adapters, proxies, and IE proxies. If CAMS is configured to disable the use of multiple network adapters, proxies, or IE proxies, it prompts the 802.1x client to disable use of multiple network adapters, proxies, or IE proxies through messages after the supplicant system passes the authentication.

Note:

- This function needs the support of Huawei's 802.1x client.
- As for the proxy detecting function, you need to enable this function on both the 802.1x client and CAMS. You need also to enable client version detecting on the switch (refer to the **dot1x version-check** command for more).

Chapter 2 Newly Added 802.1x-Related Commands

2.1 Newly Added 802.1x-Related Commands

2.1.1 dot1x authentication-method

Syntax

dot1x authentication-method { **chap** | **pap** | **eap** }

undo dot1x authentication-method

View

System view

Parameter

chap: Authenticates supplicant systems using challenge handshake authentication protocol (CHAP). CHAP is a three-way handshake authentication protocol. It has satisfactory security performance and is securer than other authentication modes. With this protocol employed, only usernames are transmitted for supplicant system to be authenticated.

pap: Authenticates supplicant systems using password authentication protocol (PAP). With this protocol employed, passwords are transmitted in plain text.

eap: Authenticates supplicant systems using extensible authentication protocol (EAP). With this protocol employed, authentication information about supplicant systems is sent to authentication servers in the form of EAP packet. To authenticate supplicant systems using PEAP, EAP-TLS, and EAP-MD5, you can specify the **eap** keyword.

Description

Use the **dot1x authentication-method** command to set 802.1x authentication mode.

Use the **undo dot1x authentication-method** command to revert to the default 802.1x authentication mode.

The default 802.1x authentication mode is CHAP.

Related command: **display dot1x**.

Example

Enter system view.

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

Specify to authenticate supplicant systems using EAP.

```
[Quidway] dot1x authentication-method eap
```

2.1.2 dot1x guest-vlan

Syntax

dot1x guest-vlan *vlan-id* [**interface** *interface-list*]

undo dot1x guest-vlan *vlan-id* [**interface** *interface-list*]

View

System view, Ethernet port view

Parameter

vlan-id: VLAN ID to be assigned to the Guest VLAN. This argument ranges from 1 to 4,094 and defaults to 1.

interface-list: List of Ethernet ports for which the Guest VLAN function is to be enabled. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-num*] } *&<1-10>*, where &<1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

Note:

- When being executed in system view, these two commands apply to all ports if you do not provide the *interface-list* argument. If you provide this argument, these two commands apply to the specified ports.
- When being executed in Ethernet port view, these two commands apply to the current port and the *interface-list* argument is not needed.

Description

Use the **dot1x guest-vlan** command to enable the Guest VLAN function for specified Ethernet ports.

Use the **undo dot1x guest-vlan** command to disable the Guest VLAN function for specified Ethernet ports.

Caution:

- The Guest VLAN function is available only when the switch operates in the port-based authentication mode.
- Only one Guest VLAN can be configured for a switch.
- Supplicant systems that are not authenticated, fail to pass the authentication, or are offline belong to Guest VLANs.
- Before configuring the Guest VLAN function, make sure the VLAN to be specified as the Guest VLAN already exists.

Example

Enter system view.

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

Create VLAN 2.

```
[Quidway] vlan 2
```

Enter GigabitEthernet1/0/1 port view.

```
[Quidway] interface GigabitEthernet1/0/1
```

Configure the port to operate in the port-based authentication mode.

```
[Quidway-GigabitEthernet1/0/1] dot1x port-method portbased
```

Configure VLAN 2 to be a Guest VLAN.

```
[Quidway-GigabitEthernet1/0/1] dot1x guest-vlan 2
```

2.1.3 dot1x retry-version-max

Syntax

dot1x retry-version-max *max-retry-version-value*

undo dot1x retry-version-max

View

System view

Parameter

max-retry-version-value: Maximum number of retries to send version request packets to an online supplicant system. This argument ranges from 1 to 10 and defaults to 3.

Description

Use the **dot1x retry-version-max** command to set the maximum number of retries for a switch to send version request packets to an online supplicant system.

Use the **undo dot1x retry-version-max** command to revert to the default maximum number of retries.

After sending a version request packet to a supplicant system, a switch sends another one to the supplicant system if it does not receive the response from the supplicant system for the period set by the version checking timer. It continues to send version request packets to the supplicant system if it still does not receive the response from the supplicant system. Such a process goes on and on until the maximum number of retries is reached. If the maximum number of retries is reached and the supplicant system still does not respond, the switch ceases checking the client version of the supplicant system and continues the followed authentication procedures.

These two commands apply to all ports with the version checking function enabled.

Related command: **display dot1x**, **dot1x timer**.

Example

Enter system view.

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

Configure the maximum number of retries for the switch to send version request packets to online supplicant systems to be 6.

```
[Quidway] dot1x retry-version-max 6
```

2.1.4 dot1x supp-proxy-check

Syntax

dot1x supp-proxy-check { **logoff** | **trap** } [**interface** *interface-list*]

undo dot1x supp-proxy-check { **logoff** | **trap** } [**interface** *interface-list*]

View

System view, Ethernet port view

Parameter

logoff: Disconnects a supplicant system if the supplicant system is detected logging in through a proxy or through more than one network adapters.

trap: Sends Trap packets if the supplicant system is detected logging in through a proxy or through more than one network adapters.

interface *interface-list*: Specifies a list of Ethernet ports. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type*

interface-number [**to** *interface-type interface-num*] } *&<1-10>*, where &<1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

Note:

- When being executed in system view, these two commands apply to all ports if you do not provide the *interface-list* argument. If you provide this argument, these two commands apply to the specified ports.
- When being executed in Ethernet port view, these two commands apply to the current port and the *interface-list* argument is not needed.

Description

Use the **dot1x supp-proxy-check** command to enable the supplicant system checking function for specified Ethernet ports.

Use the **undo dot1x supp-proxy-check** command to disable the supplicant system checking function for specified Ethernet ports.

By default, the supplicant system checking function is disabled on an Ethernet port.

The supplicant system checking function checks for:

- Supplicant systems logging in through proxies
- Supplicant systems logging in through IE proxies
- Whether or not a supplicant system logs in with more than one network adapters installed in it being active

An S5600 series switch can optionally take the following measures against any of the three cases:

- Disconnecting the supplicant system and sending Trap packets (This can be achieved by using the **dot1x supp-proxy-check logoff** command.)
- Sending Trap packets without disconnecting the supplicant system (This can be achieved by using the **dot1x supp-proxy-check trap** command.)

To achieve this function, following are to meet for 802.1x clients and CAMS.

- The 802.1x clients are capable of detecting multiple network adapters, proxies, and IE proxies.
- CAMS is configured to disable use of multiple network adapters, proxies, or IE proxies.

By default, an 802.1x client allows the use of multiple network adapters, proxies, and IE proxies. If CAMS is configured to disable the use of multiple network adapters, proxies, or IE proxies, it prompts the 802.1x client to disable use of multiple network adapters, proxies, or IE proxies through messages after the supplicant system passes the authentication.

Note:

- As for the proxy detecting function, you need to enable this function on both the 802.1x client and CAMS. You need also to enable client version detecting on the switch (refer to the **dot1x version-check** command for more).
- To utilize the supplicant system checking function on a port, you need to enable the function in system view and then in Ethernet port view.

Related command: **display dot1x**.

Example

Enter system view.

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

Configure to disconnect the supplicant systems connected to GigabitEthernet1/0/1 through GigabitEthernet1/0/8 ports if the supplicant systems are detected logging in through proxies.

```
[Quidway] dot1x supp-proxy-check logoff
[Quidway] dot1x supp-proxy-check logoff interface GigabitEthernet 1/0/1 to
GigabitEthernet 1/0/8
```

Configure to send Trap packets if the supplicant systems connected to GigabitEthernet1/0/9 port are detected logging in through proxies.

```
[Quidway] dot1x supp-proxy-check trap
[Quidway] dot1x supp-proxy-check trap interface GigabitEthernet 1/0/9
```

2.1.5 dot1x timer ver-period

Syntax

dot1x timer ver-period *ver-period-value*

undo dot1x timer ver-period

View

System view

Parameter

ver-period-value: Ver-period value in seconds to be set. This argument ranges from 1 to 30 and defaults to 30.

Description

Use the **dot1x timer ver-period** command to set the version checking timer for 802.1x client.

Use the **undo dot1x timer ver-period** command to resume the default value of the version checking timer.

After sending a version request packet to a supplicant system, a switch sends another one to the supplicant system if it does not receive the response from the supplicant system for the period set by the version checking timer.

Normally, the default version checking timer value is recommended.

Related command: **display dot1x**.

Example

Enter system view.

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

Set the version checking timer to 5 seconds.

```
[Quidway] dot1x timer ver-period 5
```

2.1.6 dot1x version-check

Syntax

dot1x version-check [**interface** *interface-list*]

undo dot1x version-check [**interface** *interface-list*]

View

System view, Ethernet port view

Parameter

interface *interface-list*: Specifies a list of Ethernet ports. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-num*] } *&<1-10>*, where &<1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

Description

Use the **dot1x version-check** command to enable 802.1x client version checking for specified Ethernet ports.

Use the **undo dot1x version-check** command to disable 802.1x client version checking for specified Ethernet ports.

By default, 802.1x client version checking is disabled on an Ethernet port.

Note:

- When being executed in system view, these two commands apply to all ports if you do not provide the *interface-list* argument. If you provide this argument, these two commands apply to the specified ports.
- When being executed in Ethernet port view, these two commands apply to the current port and the *interface-list* argument is not needed.

Example

Enter system view.

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

Configure GigabitEthernet1/0/1 port to check the version of the 802.1x client upon receiving authentication packets.

```
[Quidway-GigabitEthernet1/0/1] dot1x version-check
```