Contents

802.1X client commands

display dot1x supplicant

Use **display dot1x supplicant** to display 802.1X client authentication information.

Syntax

display dot1x supplicant [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays 802.1X client authentication information for all interfaces.

Examples

Display 802.1X client authentication information on GigabitEthernet 1/0/1.

```
<Sysname> display dot1x supplicant interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
  Username             : aaa
  EAP method           : PEAP-MSCHAPv2
  Dot1x supplicant     : Enabled
  Anonymous identifier : bbb
  SSL client policy    : policy_1
  FSM state            : Init
  EAPOL-Start packets  : 0
```

Table 1 Command output

Field	Description
Username	802.1X client username.
EAP method	802.1X client EAP authentication method: • MD5. • PEAP-GTC. • PEAP-MSCHAPv2. • TTLS-GTC. • TTLS-MSCHAPv2.
Dot1x supplicant	Status of the 802.1X client feature: • Enabled. • Disabled.
Anonymous identifier	802.1X client anonymous identifier.
SSL client policy	SSL client policy used by the 802.1X client feature.

Field	Description
FSM state	802.1X client authentication state: • **Init**—The authentication process starts. • **Connecting**—The 802.1X client is connecting to the authenticator. • **Authenticating**—The 802.1X client is being authenticated. • **Authenticated**—The 802.1X client has been authenticated. • **Held**—The 802.1X client is waiting for authentication.
EAPOL-Start packets	Number of sent EAPOL-Start packets.

dot1x supplicant anonymous identify

Use **dot1x supplicant anonymous identify** to configure an 802.1X client anonymous identifier.

Use **undo dot1x supplicant anonymous identify** to restore the default.

Syntax

dot1x supplicant anonymous identify *identifier*

undo dot1x supplicant anonymous identify

Default

No 802.1X client anonymous identifier exists.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

identifier: Specifies an 802.1X client anonymous identifier, a case-sensitive string of 1 to 253 characters.

Usage guidelines

At the first authentication phase, packets sent to the authenticator are not encrypted. The use of an 802.1X client anonymous identifier prevents the 802.1X client username from being disclosed at the first phase. The 802.1X client-enabled device sends the anonymous identifier to the authenticator instead of the 802.1X client username. The 802.1X client username will be sent to the authenticator in encrypted packets at the second phase.

If no 802.1X client anonymous identifier is configured, the device sends the 802.1X client username in the first phase.

The configured 802.1X client anonymous identifier takes effect only if one of the following EAP authentication methods is used:

- PEAP-MSCHAPv2.
- PEAP-GTC.
- TTLS-MSCHAPv2.
- TTLS-GTC.

If the MD5-Challenge EAP authentication is used, the configured 802.1X client anonymous identifier does not take effect. The device uses the 802.1X client username at the first authentication phase.

Do not configure the 802.1X client anonymous identifier if the vendor-specific authentication server cannot identify anonymous identifiers.

Examples

Configure the 802.1X client anonymous identifier as **bbb** on a port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant anonymous identify bbb
```

Related commands

display dot1x supplicant

dot1x supplicant enable

dot1x supplicant username

dot1x supplicant eap-method

Use **dot1x supplicant eap-method** to specify an 802.1X client EAP authentication method.

Use **undo dot1x supplicant eap-method** to restore the default.

Syntax

dot1x supplicant eap-method { **md5** | **peap-gtc** | **peap-mschapv2** | **ttls-gtc** | **ttls-mschapv2** }

undo dot1x supplicant eap-method

Default

The MD5-Challenge authentication is used as the 802.1X client EAP authentication method.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

md5: Specifies the MD5-challenge EAP authentication method.

peap-gtc: Specifies the PEAP-GTC EAP authentication method.

peap-mschapv2: Specifies the PEAP-MSCHAPv2 EAP authentication method

ttls-gtc: Specifies the TTLS-GTC EAP authentication method.

ttls-mschapv2: Specifies the TTLS-MSCHAPv2 EAP authentication method.

Usage guidelines

Make sure the specified 802.1X client EAP authentication method is supported by the authentication server.

Examples

Specify PEAP-GTC as the 802.1X client EAP authentication method on a port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant eap-method peap-gtc
```

Related commands

display dot1x supplicant

dot1x supplicant enable

dot1x supplicant enable

Use **dot1x supplicant enable** to enable the 802.1X client feature.

Use **undo dot1x supplicant enable** to disable the 802.1X client feature.

Syntax

dot1x supplicant enable

undo dot1x supplicant enable

Default

The 802.1X client feature is disabled.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Make sure you have configured 802.1X authentication on the authenticator before you use this command.

Examples

Enable the 802.1X client feature on a port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant enable
```

Related commands

display dot1x supplicant

dot1x supplicant mac-address

Use **dot1x supplicant mac-address** to configure an 802.1X client MAC address used for 802.1X client authentication.

Use **undo dot1x supplicant mac-address** to restore the default.

Syntax

dot1x supplicant mac-address *mac-address*

undo dot1x supplicant mac-address

Default

An Ethernet interface uses the interface's MAC address for 802.1X client authentication. If the interface's MAC address is unavailable, the interface uses the device's MAC address for 802.1X client authentication.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in the format of H-H-H, excluding multicast, all-zero, and all-F MAC addresses. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

Usage guidelines

When the device acts as an 802.1X client, each interface requires a unique MAC address to pass 802.1X client authentication.

You can use either of the following methods to configure a unique MAC address for each 802.1X client-enabled interface:

- Execute the **mac-address** command in Ethernet interface view.
- Execute the **dot1x supplicant mac-address** command.

Examples

Configure the 802.1X client MAC address for 802.1X client authentication as 0001-0001-0001.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant mac-address 1-1-1
```

dot1x supplicant password

Use **dot1x supplicant password** to set an 802.1X client password.

Use **undo dot1x supplicant password** to restore the default.

Syntax

dot1x supplicant password { **cipher** | **simple** } *string*

undo dot1x supplicant password

Default

No 802.1X client password exists.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 127 characters. Its encrypted form is a case-sensitive string of 1 to 201 characters.

Examples

Set the 802.1X client password to **123456** in plaintext form on a port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dot1x supplicant password simple 123456
```

Related commands

display dot1x supplicant

dot1x supplicant enable

dot1x supplicant ssl-client-policy

Use **dot1x supplicant ssl-client-policy** to specify an SSL client policy for an 802.1X client-enabled device.

Use **undo dot1x supplicant ssl-client-policy** to restore the default.

Syntax

dot1x supplicant ssl-client-policy *policy-name*

undo dot1x supplicant ssl-client-policy *policy-name*

Default

An 802.1X client-enabled device uses the default SSL client policy.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies an SSL client policy by its name, a case-insensitive string of 1 to 31 characters. Make sure the specified SSL client policy already exists.

Usage guidelines

If the PEAP-MSCHAPv2, PEAP-GTC, TTLS-MSCHAPv2, or TTLS-GTC authentication is used, the 802.1X client authentication process is as follows:

- **The first phase**—The device acts as an SSL client to negotiate with the SSL server.

  The SSL client uses the SSL parameters specified in the specified SSL client policy to establish a connection to the SSL server for negotiation. The SSL parameters include a PKI domain, supported cipher suites, and the SSL version. For information about SSL client policies, see *Security Configuration Guide*.
- **The second phase**—The device uses the negotiated result to encrypt and transmit the interchanged authentication packets.

If the MD5-Challenge authentication is used, the device does not use an SSL client policy during the authentication process.

Examples

#Specify SSL client policy **policy_1** to be used by an 802.1X client-enabled device on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant ssl-client-policy policy_1
```

Related commands

display dot1x supplicant

dot1x supplicant enable

ssl client-policy

dot1x supplicant transmit-mode

Use **dot1x supplicant transmit-mode** to specify a mode used by 802.1X client authentication for sending EAP-Response and EAPOL-Logoff packets.

Use undo dot1x supplicant transmit-mode to restore the default.

Syntax

dot1x supplicant transmit-mode { **multicast** | **unicast** }

undo dot1x supplicant transmit-mode

Default

802.1X client authentication uses unicast mode to send EAP-Response and EAPOL-Logoff packets.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

multicast: Specifies multicast mode for sending EAP-Response and EAPOL-Logoff packets, of which the destination addresses are multicast MAC address 01-80-C2-00-00-03.

unicast: Specifies unicast mode for sending EAP-Response and EAPOL-Logoff packets.

Usage guidelines

When the device acts as an 802.1X client, use the multicast mode to avoid 802.1X authentication failures if the NAS device does not support receiving unicast EAP-Response or EAPOL-Logoff packets.

Examples

Configure 802.1X client authentication to use multicast mode for sending EAP-Response and EAPOL-Logoff packets on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant transmit-mode multicast
```

dot1x supplicant username

Use **dot1x supplicant username** to configure an 802.1X client username.

Use **undo dot1x supplicant username** to restore the default.

Syntax

dot1x supplicant username *username*

undo dot1x supplicant username

Default

No 802.1X client username exists.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

username: Specifies the 802.1X client username, a case-sensitive string of 1 to 253 characters.

Usage guidelines

802.1X client usernames can include domain names. The supported domain name delimiters include the at sign (@), backslash (\), dot (.), and forward slash (/). Usernames that include domain names can use the format of *username*@*domain-name*, *domain-name**username*, *username*.*domain-name*, or *username*/*domain-name*.

If you want to use backslash (\) as the domain name delimiter, you must enter the escape character (\) along with the backslash (\) sign.

If a username string includes multiple configured delimiters, the device takes the rightmost delimiter in the username string as the domain name delimiter. For more information about the domain name delimiters, see the **dot1x domain-delimiter** command.

Examples

Configure the 802.1X client username as **aaa** on a port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant username aaa
```

Related commands

display dot1x supplicant

dot1x domain-delimiter

dot1x supplicant enable