Contents

802.1X commands

display dot1x

Use **display dot1x** to display information about 802.1X.

Syntax

display dot1x [**sessions** | **statistics**] [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

sessions: Displays 802.1X session information.

statistics: Displays 802.1X statistics.

interface *interface-type interface-number*: Specifies a port by its type and number.

Usage guidelines

If you do not specify the **sessions** keyword or the **statistics** keyword, this command displays all information about 802.1X, including session information, statistics, and settings.

If you do not specify the **interface** *interface-type interface-number* option, this command displays all global and port-specific 802.1X information.

Examples

Display all information about 802.1X.

```
<Sysname> display dot1x
Global 802.1X parameters:
   802.1X authentication  : Enabled
   CHAP authentication    : Enabled
   Max-tx period          : 30 s
   Handshake period       : 15 s
   Quiet timer            : Disabled
         Quiet period     : 60 s
   Supp timeout           : 30 s
   Server timeout         : 100 s
   Reauth period          : 3600 s
   Max auth requests      : 2
   EAD assistant function : Disabled
       URL                : http://www.dwsoft.com
       Free IP            : 6.6.6.0         255.255.255.0
       EAD timeout        : 30 min
   Domain delimiter       : @
 Online 802.1X wired users    : 1
```

```
GigabitEthernet1/0/1  is link-up
  802.1X authentication      : Enabled
  Handshake                  : Enabled
  Handshake reply            : Disabled
  Handshake security         : Disabled
  Unicast trigger            : Disabled
  Periodic reauth            : Disabled
  Port role                  : Authenticator
  Authorization mode         : Auto
  Port access control        : Port-based
  Multicast trigger          : Enabled
  Mandatory auth domain      : Not configured
  Guest VLAN                 : 3
  Auth-Fail VLAN             : Not configured
  Critical VLAN              : Not configured
  Critical voice VLAN        : Disabled
  Add Guest VLAN delay       : Disabled
  Re-auth server-unreachable : Logoff
  Max online users           : 4294967295
  User IP freezing           : Disabled
  Reauth period              : 0 s
  Send Packets Without Tag   : Disabled
  Max Attempts Fail Number   : 0
  Guest VSI                  : Not configured
  Auth-Fail VSI              : Not configured
  Critical VSI               : Not configured
  Add Guest VSI delay        : Disabled

  EAPOL packets: Tx 3, Rx 3
  Sent EAP Request/Identity packets : 1
       EAP Request/Challenge packets: 1
       EAP Success packets: 1
       EAP Failure packets: 0
  Received EAPOL Start packets : 1
           EAPOL LogOff packets: 1
           EAP Response/Identity packets : 1
           EAP Response/Challenge packets: 1
           Error packets: 0
  Online 802.1X users: 1
         MAC address         Auth state
         0001-0000-0000      Authenticated
```

Table 1 Command output

Field	Description
Global 802.1X parameters	Global 802.1X configuration.
802.1X authentication	Whether 802.1X is enabled globally.
CHAP authentication	Performs EAP termination and uses CHAP to communicate with the

Field	Description
	RADIUS server.
EAP authentication	Relays EAP packets and supports any of the EAP authentication methods to communicate with the RADIUS server.
PAP authentication	Performs EAP termination and uses PAP to communicate with the RADIUS server.
Max-tx period	Username request timeout timer in seconds.
Handshake period	Handshake timer in seconds.
Quiet timer	Status of the quiet timer, enabled or disabled.
Quiet period	Quiet timer in seconds.
Supp timeout	Client timeout timer in seconds.
Server timeout	Server timeout timer in seconds.
Reauth period	Periodic reauthentication timer in seconds.
Max auth requests	Maximum number of attempts for sending an authentication request to a client.
EAD assistant function	Whether EAD assistant is enabled.
URL	Redirect URL for unauthenticated users using a Web browser to access the network.
Free IP	Network segment accessible to unauthenticated users.
EAD timeout	EAD rule timer in minutes.
Domain delimiter	Domain delimiters supported by the device.
Online 802.1X wired users	Number of wired online 802.1X users, including users that have passed 802.1X authentication and users that are performing 802.1X authentication.
GigabitEthernet1/0/1 is link-up	Status of the port. In this example, GigabitEthernet 1/0/1 is up.
802.1X authentication	Whether 802.1X is enabled on the port.
Handshake	Whether the online user handshake feature is enabled on the port.
Handshake reply	Whether the online user handshake reply feature is enabled on the port.
Handshake security	Whether the online user handshake security feature is enabled on the port.
Unicast trigger	Whether the 802.1X unicast trigger is enabled on the port.
Periodic reauth	Whether 802.1X periodic reauthentication is enabled on the port.
Port role	Role of the port. The port functions only as an **Authenticator**.
Authorization mode	Authorization state of the port, which can be Force-Authorized, Auto, or Force-Unauthorized.
Port access control	Access control method of the port: • **MAC-based**—MAC-based access control. • **Port-based**—Port-based access control.
Multicast trigger	Whether the 802.1X multicast trigger feature is enabled.
Mandatory auth domain	Mandatory authentication domain on the port.
Guest VLAN	802.1X guest VLAN configured on the port. If no 802.1X guest VLAN is configured on the port, this field displays

Field	Description
	Not configured.
Auth-Fail VLAN	802.1X Auth-Fail VLAN configured on the port. If no 802.1X Auth-Fail VLAN is configured on the port, this field displays **Not configured**.
Critical VLAN	802.1X critical VLAN configured on the port. If no 802.1X critical VLAN is configured on the port, this field displays **Not configured**.
Critical voice VLAN	Whether the 802.1X critical voice VLAN feature is enabled on the port.
Add Guest VLAN delay	Status and mode of the 802.1X guest VLAN assignment delay feature on a port: • **EAPOL**—EAPOL-triggered 802.1X guest VLAN assignment delay is enabled. • **NewMac**—New MAC-triggered 802.1X guest VLAN assignment delay is enabled. • **ALL**—Both EAPOL-triggered and new MAC-triggered 802.1X guest VLAN assignment delays are enabled. • **Disabled**—802.1X guest VLAN assignment delay is disabled.
Re-auth server-unreachable	Whether to log off online 802.1X users or keep them online when no server is reachable for 802.1X reauthentication.
Max online users	Maximum number of concurrent 802.1X users on the port.
User IP freezing	Whether user IP freezing is enabled on the port.
Reauth period	Periodic reauthentication timer in seconds on the port.
Send Packets Without Tag	Whether to remove the VLAN tags of all 802.1X protocol packets sent out of the port to 802.1X clients.
Max Attempts Fail Number	Maximum number of 802.1X authentication attempts for MAC authenticated users.
Guest VSI	This field is not supported in the current software version. 802.1X guest VSI configured on the port. If no 802.1X guest VSI is configured on the port, this field displays **Not configured**.
Auth-Fail VSI	This field is not supported in the current software version. 802.1X Auth-Fail VSI configured on the port. If no 802.1X Auth-Fail VSI is configured on the port, this field displays **Not configured**.
Critical VSI	This field is not supported in the current software version. 802.1X critical VSI configured on the port. If no 802.1X critical VSI is configured on the port, this field displays **Not configured**.
Add Guest VSI delay	This field is not supported in the current software version. Status and mode of the 802.1X guest VSI assignment delay feature on a port: • **EAPOL only**—EAPOL-triggered 802.1X guest VSI assignment delay is enabled. • **NewMAC only**—New MAC-triggered 802.1X guest VSI assignment delay is enabled. • **EAPOL or NewMAC**—Both EAPOL-triggered and new MAC-triggered 802.1X guest VSI assignment delays are

Field	Description
	enabled. • **Disabled**—802.1X guest VSI assignment delay is disabled.
EAPOL packets	Number of sent (Tx) and received (Rx) EAPOL packets.
Sent EAP Request/Identity packets	Number of sent EAP-Request/Identity packets.
EAP Request/Challenge packets	Number of sent EAP-Request/MD5-Challenge packets.
EAP Success packets	Number of sent EAP-Success packets.
EAP Failure packets	Number of sent EAP-Failure packets.
Received EAPOL Start packets	Number of received EAPOL-Start packets.
EAPOL LogOff packets	Number of received EAPOL-LogOff packets.
EAP Response/Identity packets	Number of received EAP-Response/Identity packets.
EAP Response/Challenge packets	Number of received EAP-Response/MD5-Challenge packets.
Error packets	Number of received error packets.
Online 802.1X users	Number of online 802.1X users on the port, including users that have passed 802.1X authentication and users that are performing 802.1X authentication.
MAC address	MAC addresses of the online 802.1X users.
Auth state	Authentication status of the online 802.1X users.

display dot1x connection

Use **display dot1x connection** to display information about online 802.1X users.

Syntax

display dot1x connection [**open**] [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-address* | **user-name** *name-string*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

open: Displays information only about 802.1X users that use nonexistent usernames or incorrect passwords for network access in open authentication mode. If you do not specify this keyword, the command displays information about all online 802.1X users.

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays online 802.1X user information for all ports.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays online 802.1X user information for all member devices.

user-mac *mac-address*: Specifies an 802.1X user by MAC address. The *mac-address* argument represents the MAC address of the user, in the form of H-H-H. If you do not specify an 802.1X user, this command displays all online 802.1X user information.

user-name *name-string*: Specifies an 802.1X user by its name. The *name-string* argument represents the username, a case-sensitive string of 1 to 253 characters. If you do not specify an 802.1X user, this command displays all online 802.1X user information.

Examples

Display information about all online 802.1X users.

```
<Sysname> display dot1x connection
Total connections: 1

Slot ID: 1
User MAC address: 0015-e9a6-7cfe
Access interface: GigabitEthernet1/0/1
Username: ias
User access state: Successful
Authentication domain: h3c
IPv4 address: 192.168.1.1
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
Authentication method: CHAP
Initial VLAN: 1
Authorization untagged VLAN: 6
Authorization tagged VLAN list: 1 to 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 29 31 33
                                35 37 40 to 100
Authorization VSI: N/A
Authorization ACL ID: 3001
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: 2 s
Online from: 2013/03/02  13:14:15
Online duration: 0h 2m 15s
```

Table 2 Command output

Field	Description
Total connections	Number of online 802.1X users.
User MAC address	MAC address of the user.
Access interface	Interface through which the user access the device.
User access state	Access state of the user. • **Successful**—The user passes 802.1X authentication and comes online. • **Open**—The user uses a nonexistent username or an incorrect password to come online in open authentication mode.
Authentication domain	ISP domain used for 802.1X authentication.
IPv4 address	IPv4 address of the user. If the device does not get the IPv4 address of the user, this field is not available.
IPv6 address	IPv6 address of the user.

Field	Description
	If the device does not get the IPv6 address of the user, this field is not available.
Authentication method	EAP message handling method: • **CHAP**—Performs EAP termination and uses CHAP to communicate with the RADIUS server. • **EAP**—Relays EAP packets and supports any of the EAP authentication methods to communicate with the RADIUS server. • **PAP**—Performs EAP termination and uses PAP to communicate with the RADIUS server.
Initial VLAN	VLAN to which the user belongs before 802.1X authentication.
Authorization untagged VLAN	Untagged VLAN authorized to the user.
Authorization tagged VLAN list	Tagged VLANs authorized to the user.
Authorization VSI	This field is not supported in the current software version. VSIs authorized to the user.
Authorization ACL ID	ACL authorized to the user. If the ACL authorization fails, this field displays **(Not effective)** after the ACL ID.
Authorization user profile	User profile authorized to the user.
Authorization CAR	This field is not supported in the current software version. Authorization CAR attributes assigned by the server. If no authorization CAR attributes are assigned, this field displays **N/A**.
Authorization URL	Redirect URL authorized to the user.
Termination action	Action attribute assigned by the server to terminate the user session: • **Default**—Logs off the online authenticated 802.1X user when the session timeout timer expires. This attribute does not take effect when 802.1X periodic reauthentication is enabled and the periodic reauthentication timer is shorter than the session timeout timer. • **Radius-request**—Reauthenticates the online user when the session timeout timer expires, regardless of whether the 802.1X periodic reauthentication feature is enabled or not. If the device performs local authentication, this field displays **Default**.
Session timeout period	Session timeout timer assigned by the server.
Online from	Time from which the 802.1X user came online.
Online duration	Online duration of the 802.1X user.

display dot1x mac-address

Use **display dot1x mac-address** to display MAC address information of 802.1X users in 802.1X VLANs of a specific type.

Syntax

display dot1x mac-address { **auth-fail-vlan** | **critical-vlan** | **guest-vlan** } [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

auth-fail-vlan: Specifies the 802.1X Auth-Fail VLAN.

critical-vlan: Specifies the 802.1X critical VLAN.

guest-vlan: Specifies the 802.1X guest VLAN.

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays MAC address information of 802.1X users in the specified 802.1X VLAN on all ports.

Usage guidelines

This command displays rough statistics. It might not fully display the specified information when a large number of 802.1X users perform authentication frequently.

Examples

Display MAC address information of 802.1X users in the 802.1X Auth-Fail VLAN on all ports.

```
<Sysname> display dot1x mac-address auth-fail-vlan
Total MAC addresses: 10
Interface: GigabitEthernet1/0/1        Auth-Fail VLAN: 3    Aging time: N/A
MAC addresses: 8
  0800-2700-9427    0800-2700-2341    0800-2700-2324    0800-2700-2351
  0800-2700-5627    0800-2700-2251    0800-2700-8624    0800-2700-3f51

Interface: GigabitEthernet1/0/2        Auth-Fail VLAN: 5    Aging time: 30 sec
MAC addresses: 2
  0801-2700-9427    0801-2700-2341
```

Table 3 Command output

Field	Description
Total MAC addresses	Total number of MAC addresses in the specified VLAN on the specified port or all ports.
Interface	Access port of 802.1X users.
Type VLAN	VLAN information for 802.1X users. The *Type* argument has the following values: • Auth-Fail VLAN. • Critical VLAN. • Guest VLAN.
Aging time	MAC address aging time in seconds. This field displays **N/A** if the MAC addresses do not age out.
MAC addresses	Number of matching MAC addresses on a port.
xxxx-xxxx-xxxx	MAC address.

Related commands

dot1x auth-fail vlan

dot1x critical vlan

dot1x guest-vlan

dot1x

Use **dot1x** to enable 802.1X globally or on a port.

Use **undo dot1x** to disable 802.1X globally or on a port.

Syntax

dot1x

undo dot1x

Default

802.1X is neither enabled globally nor enabled for any port.

Views

System view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

For the 802.1X feature to take effect on a port, you must enable the feature both globally and on the port.

Examples

Enable 802.1X globally.

```
<Sysname> system-view
[Sysname] dot1x
```

Enable 802.1X on GigabitEthernet 1/0/1.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x
[Sysname-GigabitEthernet1/0/1] quit
```

Related commands

display dot1x

dot1x access-user log enable

Use **dot1x access-user log enable** to enable logging for 802.1X users.

Use **undo dot1x access-user log enable** to disable logging for 802.1X users.

Syntax

dot1x access-user log enable [**abnormal-logoff** | **failed-login** | **normal-logoff** | **successful-login**] *

undo dot1x access-user log enable [**abnormal-logoff** | **failed-login** | **normal-logoff** | **successful-login**] *

Default

All types of logging for 802.1X users are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

abnormal-logoff: Specifies logs generated for exceptional logoffs of 802.1X users, such as logoffs caused by realtime accounting failures and reauthentication failures.

failed-login: Specifies logs generated for login failures of 802.1X users.

normal-logoff: Specifies logs generated for logoffs requested by 802.1X users.

successful-login: Specifies logs generated for successful logins of 802.1X users.

Usage guidelines

As a best practice, disable this feature to prevent excessive output of logs for 802.1X users.

If you do not specify any parameters, this command enables all types of logging for 802.1X users.

Examples

Enable logging for login failures of 802.1X users.

```
<Sysname> system-view
[Sysname] dot1x access-user log enable failed-login
```

Related commands

info-center source dot1x logfile deny (*Network Management and Monitoring Command Reference*)

dot1x after-mac-auth max-attempt

Use **dot1x after-mac-auth max-attempt** to set the maximum number of 802.1X authentication attempts for MAC authenticated users on a port.

Use **undo dot1x after-mac-auth max-attempt** to restore the default.

Syntax

dot1x after-mac-auth max-attempt *max-attempts*

undo dot1x after-mac-auth max-attempt

Default

The number of 802.1X authentication attempts for MAC authenticated users is not limited on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

max-attempts: Specifies a number in the range of 1 to 50.

Usage guidelines

The device denies 802.1X authentication requests of a MAC authenticated user after the maximum number of 802.1X authentication attempts has been made.

The device will recount the number of 802.1X authentication attempts made by a MAC authenticated user if a user logoff or device reboot event occurs.

Examples

Configure GigabitEthernet 1/0/1 to allow a maximum of 10 802.1X authentication attempts made by a MAC authenticated user.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x after-mac-auth max-attempt 10
```

Related commands

display dot1x

dot1x authentication-method

Use **dot1x authentication-method** to specify an EAP message handling method.

Use **undo dot1x authentication-method** to restore the default.

Syntax

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

undo dot1x authentication-method

Default

The access device performs EAP termination and uses CHAP to communicate with the RADIUS server.

Views

System view

Predefined user roles

network-admin

Parameters

chap: Configures the access device to perform Extensible Authentication Protocol (EAP) termination and use the Challenge Handshake Authentication Protocol (CHAP) to communicate with the RADIUS server.

eap: Configures the access device to relay EAP packets, and supports any of the EAP authentication methods to communicate with the RADIUS server.

pap: Configures the access device to perform EAP termination and use the Password Authentication Protocol (PAP) to communicate with the RADIUS server.

Usage guidelines

The access device terminates or relays EAP packets.

- **In EAP termination mode**—The access device re-encapsulates and sends the authentication data from the client in standard RADIUS packets to the RADIUS server. The device performs either CHAP or PAP authentication with the RADIUS server. In this mode, the RADIUS server supports only MD5-Challenge EAP authentication and the username and password EAP authentication initiated by an iNode client.
  - PAP transports usernames and passwords in plain text. The authentication method applies to scenarios that do not require high security. To use PAP, the client can be an iNode 802.1X client.
  - CHAP transports usernames in plain text and passwords in encrypted form over the network. CHAP is more secure than PAP.

- **In EAP relay mode**—The access device relays EAP messages between the client and the RADIUS server. The EAP relay mode supports multiple EAP authentication methods, such as MD5-Challenge, EAP-TLS, and PEAP. To use this mode, make sure the RADIUS server meets the following requirements:
  - Supports the EAP-Message and Message-Authenticator attributes.
  - Uses the same EAP authentication method as the client.

  If this mode is used, the **user-name-format** command configured in RADIUS scheme view does not take effect. For more information about the **user-name-format** command, see "RADIUS commands."

If RADIUS authentication is used, you must configure the access device to use the same authentication method (PAP, CHAP, or EAP) as the RADIUS server.

Examples

Enable the access device to terminate EAP packets and perform PAP authentication with the RADIUS server.

```
<Sysname> system-view
[Sysname] dot1x authentication-method pap
```

Related commands

display dot1x

dot1x auth-fail eapol

Use **dot1x auth-fail eapol** to enable the device to send an EAP-Success packet to a client when the client user is assigned to the 802.1X Auth-Fail VLAN on a port.

Use **undo dot1x auth-fail eapol** to restore the default.

NOTE:

This command is supported only in Release 6127 and later.

Syntax

dot1x auth-fail eapol

undo dot1x auth-fail eapol

Default

The device sends an EAP-Failure packet to a client when the client user is assigned to the 802.1X Auth-Fail VLAN on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Some 802.1X clients cannot send DHCP requests for IP addresses after they receive EAP-Failure packets. To have these clients obtain IP addresses to access authorized resources after they are assigned to the 802.1X Auth-Fail VLAN, use this feature.

Examples

Enable the device to send an EAP-Success packet to a client when the client user is assigned to the 802.1X Auth-Fail VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x auth-fail eapol
```

Related commands

dot1x auth-fail vlan

dot1x auth-fail vlan

Use **dot1x auth-fail vlan** to configure an 802.1X Auth-Fail VLAN on a port.

Use **undo dot1x auth-fail vlan** to restore the default.

Syntax

dot1x auth-fail vlan *authfail-vlan-id*

undo dot1x auth-fail vlan

Default

No 802.1X Auth-Fail VLAN exists on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

authfail-vlan-id: Specifies the ID of the 802.1X Auth-Fail VLAN on the port. The value range for the VLAN ID is 1 to 4094. Make sure the VLAN has been created.

Usage guidelines

An 802.1X Auth-Fail VLAN accommodates users that have failed 802.1X authentication for any reason other than unreachable servers. Users in the Auth-Fail VLAN can access a limited set of network resources.

You cannot specify a VLAN as both a super VLAN and an 802.1X Auth-Fail VLAN on a port. For more information about super VLANs, see *Layer 2—LAN Switching Configuration Guide*.

To delete a VLAN that has been configured as an 802.1X Auth-Fail VLAN, you must first use the **undo dot1x auth-fail vlan** command.

Examples

Configure VLAN 100 as the Auth-Fail VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x auth-fail vlan 100
```

Related commands

display dot1x

dot1x critical eapol

Use **dot1x critical eapol** to enable the sending of an EAP-Success packet to a client when the 802.1X client user is assigned to the 802.1X critical VLAN on a port.

Use **undo dot1x critical eapol** to restore the default.

Syntax

dot1x critical eapol

undo dot1x critical eapol

Default

The device sends an EAP-Failure packet to a client when the 802.1X client user is assigned to the 802.1X critical VLAN on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Typically, the device sends EAP-Failure packets to 802.1X clients when the client users are assigned to the 802.1X critical VLAN. Some 802.1X clients, such as Windows built-in 802.1X clients, cannot respond to the EAP-Request/Identity packets of the device if they have received an EAP-Failure packet. As a result, reauthentication fails for these clients when an authentication server is reachable.

This command enables the device to send EAP-Success packets instead of EAP-Failure packets to 802.1X clients when the client users are assigned to the 802.1X critical VLAN. This operation ensures that all 802.1X clients can perform reauthentication.

Examples

Send an EAP-Success packet to a client when the 802.1X client user is assigned to the 802.1X critical VLAN on GigabitEthernet 1/0/1.

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

Related commands

dot1x critical vlan

dot1x critical vlan

Use **dot1x critical vlan** to configure an 802.1X critical VLAN on a port.

Use **undo dot1x critical vlan** to restore the default.

Syntax

dot1x critical vlan *critical-vlan-id*

undo dot1x critical vlan

Default

No 802.1X critical VLAN exists on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

critical-vlan-id: Specifies the ID of the 802.1X critical VLAN on the port. The value range for the VLAN ID is 1 to 4094. Make sure the VLAN has been created.

Usage guidelines

An 802.1X critical VLAN accommodates users that fail 802.1X authentication because all the RADIUS servers in their ISP domains are unreachable. Users in the critical VLAN can access a limited set of network resources depending on the configuration.

You cannot specify a VLAN as both a super VLAN and an 802.1X critical VLAN on a port. For more information about super VLANs, see *Layer 2—LAN Switching Configuration Guide*.

To delete a VLAN that has been configured as an 802.1X critical VLAN, you must first use the **undo dot1x critical vlan** command.

Examples

Specify VLAN 100 as the 802.1X critical VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x critical vlan 100
```

Related commands

display dot1x

dot1x critical-voice-vlan

Use **dot1x critical-voice-vlan** to enable the 802.1X critical voice VLAN feature on a port.

Use **undo dot1x critical-voice-vlan** to disable the 802.1X critical voice VLAN feature on a port.

Syntax

dot1x critical-voice-vlan

undo dot1x critical-voice-vlan

Default

The 802.1X critical voice VLAN feature is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The 802.1X critical voice VLAN on a port accommodates 802.1X voice users that have failed authentication because none of the RADIUS servers in their ISP domain are reachable.

Before you enable the 802.1X critical voice VLAN feature on the port, make sure the following requirements are met:

- The port is configured with the voice VLAN.

  To configure a voice VLAN on a port, use the **voice-vlan enable** command (see *Layer 2—LAN Switching Command Reference*).
- LLDP is enabled both globally and on the port.

The device uses LLDP to identify voice users. For information about LLDP commands, see *Layer 2—LAN Switching Command Reference*.

Examples

Enable the 802.1X critical voice VLAN feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x critical-voice-vlan
```

Related commands

display dot1x

lldp enable (*Layer 2—LAN Switching Command Reference*)

lldp global enable (*Layer 2—LAN Switching Command Reference*)

voice-vlan enable (*Layer 2—LAN Switching Command Reference*)

dot1x domain-delimiter

Use **dot1x domain-delimiter** to specify a set of domain name delimiters supported by the device.

Use **undo dot1x domain-delimiter** to restore the default.

Syntax

dot1x domain-delimiter *string*

undo dot1x domain-delimiter

Default

The device supports only the at sign (@) delimiter for 802.1X users.

Views

System view

Predefined user roles

network-admin

Parameters

string: Specifies a set of 1 to 16 domain name delimiters for 802.1X users. No space is required between delimiters. Available delimiters include the at sign (@), backslash (\), dot (.), and forward slash (/). If you want to use backslash (\) as the domain name delimiter, you must enter the escape character (\) along with the backslash (\) sign.

Usage guidelines

Any character in the configured set can be used as the domain name delimiter for 802.1X authentication users. Usernames that include domain names can use the format of *username*@*domain-name*, *domain-name**username*, *username*.*domain-name*, or *username*/*domain-name*.

The delimiter set you configured overrides the default setting. If the at sign (@) is not included in the delimiter set, the device does not support the 802.1X users that use this sign as the domain name delimiter.

If a username string contains multiple configured delimiters, the device takes the rightmost delimiter in the username string as the domain name delimiter. For example, if you configure the forward slash (/), dot (.), and backslash (\) as delimiters, the domain name delimiter for the username string 121.123/22\@abc is the backslash (\). The username is **@abc** and the domain name is **121.123/22**.

Examples

Specify the at sign (@) and forward slash (/) as domain name delimiters.

```
<Sysname> system-view
[Sysname] dot1x domain-delimiter @/
```

Related commands

display dot1x

dot1x ead-assistant enable

Use **dot1x ead-assistant enable** to enable the EAD assistant feature.

Use **undo dot1x ead-assistant enable** to disable the EAD assistant feature.

Syntax

dot1x ead-assistant enable

undo dot1x ead-assistant enable

Default

The EAD assistant feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The EAD assistant feature enables the access device to redirect the HTTP or HTTPS requests of a user to a URL to download and install EAD client. This feature eliminates the tedious job of the administrator to deploy EAD clients.

For the EAD assistant feature to take effect on a port, you must set the port authorization mode to **auto**.

The feature is mutually exclusive with MAC authentication and port security. You must disable MAC authentication and port security globally before you enable the EAD assistant feature.

To redirect the HTTPS requests of 802.1X users, you must also perform the following tasks:

- Execute the **dot1x ead-assistant url** command.
- Make sure an HTTPS redirect listening port number has been specified.
  - In versions earlier than Release 6127, no HTTPS redirect listening port number is specified by default. You must use the **http-redirect https-port** command to specify an HTTPS redirect listening port.
  - In Release 6127 and later, the device by default listens to port 6654 for HTTPS requests to be redirected. You can use the **http-redirect https-port** command to change the HTTPS redirect listening port.

For more information about configuring the HTTPS redirect listening port number, see configuring HTTP redirect in *Layer 3—IP Services Configuration Guide*.

Examples

Enable the EAD assistant feature.

```
<Sysname> system-view
[Sysname] dot1x ead-assistant enable
```

Related commands

display dot1x

dot1x ead-assistant free-ip

dot1x ead-assistant url

http-redirect https-port (*Layer 3—IP Services Command Reference*)

dot1x ead-assistant free-ip

Use **dot1x ead-assistant free-ip** to configure a free IP.

Use **undo dot1x ead-assistant free-ip** to remove the specified or all free IP addresses.

Syntax

dot1x ead-assistant free-ip *ip-address* { *mask-address* | *mask-length* }

undo dot1x ead-assistant free-ip { *ip-address* { *mask-address* | *mask-length* } | **all** }

Default

No free IPs exist. Users cannot access any segments before they pass 802.1X authentication.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies a freely accessible IP address segment, also called a free IP.

mask: Specifies an IP address mask.

mask-length: Specifies IP address mask length in the range of 1 to 32.

all: Removes all free IP addresses.

Usage guidelines

With EAD assistant enabled on the device, unauthenticated 802.1X users can access the network resources in the free IP segments before they pass 802.1X authentication.

Execute this command multiple times to configure multiple free IPs.

Examples

Configure 192.168.1.1/16 as a free IP.

```
<Sysname> system-view
[Sysname] dot1x ead-assistant free-ip 192.168.1.1 255.255.0.0
```

Related commands

display dot1x

dot1x ead-assistant enable

dot1x ead-assistant url

dot1x ead-assistant url

Use **dot1x ead-assistant url** to configure a redirect URL for EAD assistant.

Use **undo dot1x ead-assistant url** to restore the default.

Syntax

dot1x ead-assistant url *url-string*

undo dot1x ead-assistant url

Default

No redirect URL exists for EAD assistant.

Views

System view

Predefined user roles

network-admin

Parameters

url-string: Specifies the redirect URL, a case-sensitive string of 1 to 256 characters in the format http://*string* or https://*string*. If the specified URL does not start with http:// or https://, the URL is considered to start with http:// by default.

Usage guidelines

When an unauthenticated user uses a Web browser to access any network other than the free IP, the device redirects the HTTP or HTTPS requests of the user to the redirect URL.

The redirect URL must be on the free IP subnet.

If you execute this command multiple times, the most recent configuration takes effect.

In versions earlier than Release 6127, no HTTPS redirect listening port number is specified by default. You must use the **http-redirect https-port** command to specify an HTTPS redirect listening port. In Release 6127 and later, the device by default listens to port 6654 for HTTPS requests to be redirected. You can use the **http-redirect https-port** command to change the HTTPS redirect listening port.

For more information about configuring the HTTPS redirect listening port number, see configuring HTTP redirect in *Layer 3—IP Services Configuration Guide*.

Examples

Configure the redirect URL as http://test.com.

```
<Sysname> system-view
[Sysname] dot1x ead-assistant url http://test.com
```

Related commands

display dot1x

dot1x ead-assistant enable

dot1x ead-assistant free-ip

http-redirect https-port (*Layer 3—IP Services Command Reference*)

dot1x eapol untag

Use **dot1x eapol untag** to enable the device to remove the VLAN tags of all 802.1X protocol packets sent out of a port to 802.1X clients.

Use **undo dot1x eapol untag** to restore the default.

Syntax

dot1x eapol untag

undo dot1x eapol untag

Default

Whether the device removes the VLAN tags of all 802.1X protocol packets sent out of a port to 802.1X clients depends on the configuration in the VLAN module.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command operates on a hybrid port to have it send 802.1X protocol packets with their VLAN tags removed, regardless of whether the port is a tagged or untagged member of a VLAN.

Use this command if the 802.1X-enabled hybrid port is a tagged member of its PVID and the attached 802.1X clients cannot recognize VLAN-tagged 802.1X protocol packets.

This command removes the VLAN tags of all 802.1X protocol packets sent out of the port to 802.1X clients. Do not use this command if VLAN-aware 802.1X clients are attached to the port.

Examples

Enable the device to remove the VLAN tags of all 802.1X protocol packets sent out of GigabitEthernet 1/0/1 to 802.1X clients.

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

Related commands

display dot1x

dot1x guest-vlan

Use **dot1x guest-vlan** to configure an 802.1X guest VLAN on a port.

Use **undo dot1x guest-vlan** to restore the default.

Syntax

dot1x guest-vlan *guest-vlan-id*

undo dot1x guest-vlan

Default

No 802.1X guest VLAN exists on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

guest-vlan-id: Specifies the ID of the 802.1X guest VLAN. The value range for the VLAN ID is 1 to 4094. Make sure the VLAN has been created.

Usage guidelines

An 802.1X guest VLAN accommodates users that have not performed 802.1X authentication. In the guest VLAN, users can access a limited set of network resources, such as a software server, to download anti-virus software and system patches.

You cannot specify a VLAN as both a super VLAN and an 802.1X guest VLAN on a port. For more information about super VLANs, see *Layer 2—LAN Switching Configuration Guide*.

To delete a VLAN that has been configured as a guest VLAN, you must use the **undo dot1x guest-vlan** command first.

Examples

Specify VLAN 100 as the 802.1X guest VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x guest-vlan 100
```

Related commands

display dot1x

dot1x guest-vlan-delay

Use **dot1x guest-vlan-delay** to enable 802.1X guest VLAN assignment delay on a port.

Use **undo dot1x guest-vlan-delay** to disable the specified 802.1X guest VLAN assignment delay on a port.

Syntax

dot1x guest-vlan-delay { **eapol** | **new-mac** }

undo dot1x guest-vlan-delay [**eapol** | **new-mac**]

Default

802.1X guest VLAN assignment delay is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

eapol: Specifies EAPOL-triggered 802.1X guest VLAN assignment delay. This keyword takes effect if 802.1X authentication is triggered by EAPOL-Start packets.

new-mac: Specifies new MAC-triggered 802.1X guest VLAN assignment delay. This keyword takes effect if 802.1X authentication is triggered by packets from unknown MAC addresses.

Usage guidelines

This command enables the device to delay assigning an 802.1X-enabled port to the 802.1X guest VLAN when 802.1X authentication is triggered on the port.

To use this feature, the 802.1X-enabled port must perform MAC-based access control.

When 802.1X authentication is triggered on a port, the device performs the following operations:

1. Sends a unicast EAP-Request/Identity packet to the MAC address that triggers the authentication.

2. Retransmits the packet if no response has been received within the username request timeout interval set by using the **dot1x timer tx-period** command.
3. Assigns the port to the 802.1X guest VLAN after the maximum number of request attempts set by using the **dot1x retry** command is reached.

If you use the **undo** command without any keyword, the command disables both EAPOL-triggered and new MAC-triggered 802.1X guest VLAN assignment delay on a port.

Examples

Enable EAPOL-triggered 802.1X guest VLAN assignment delay on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x guest-vlan-delay eapol
```

Related commands

display dot1x

dot1x guest-vlan

dot1x retry

dot1x timer tx-period

dot1x handshake

Use **dot1x handshake** to enable the online user handshake feature.

Use **undo dot1x handshake** to disable the online user handshake feature.

Syntax

dot1x handshake

undo dot1x handshake

Default

The online user handshake feature is enabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The online user handshake feature enables the device to periodically send EAP-Request/Identity packets to the client for verifying the connectivity status of online 802.1X users. The device sets a user to the offline state if it does not receive an EAP-Response/Identity packet from the user after making the maximum attempts within the handshake period. To set the handshake timer, use the **dot1x timer handshake-period** command. To set the maximum handshake attempts, use the **dot1x retry** command.

Examples

Enable the online user handshake feature on GigabitEthernet 1/0/1.

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

Related commands

display dot1x

dot1x timer handshake-period

dot1x retry

dot1x handshake reply enable

Use **dot1x handshake reply enable** to enable the 802.1X online user handshake reply feature.

Use **undo dot1x handshake reply enable** to disable the 802.1X online user handshake reply feature.

Syntax

dot1x handshake reply enable

undo dot1x handshake reply enable

Default

The 802.1X online user handshake reply feature is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to reply to 802.1X clients' EAP-Response/Identity packets with EAP-Success packets during the online handshake process.

Use this command only if 802.1X clients will go offline without receiving EAP-Success packets from the device.

Examples

Enable the 802.1X online user handshake reply feature on GigabitEthernet 1/0/1.

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

Related commands

dot1x handshake

dot1x handshake secure

Use **dot1x handshake secure** to enable the online user handshake security feature.

Use **undo dot1x handshake secure** to disable the online user handshake security feature.

Syntax

dot1x handshake secure

undo dot1x handshake secure

Default

The online user handshake security feature is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The online user handshake security feature enables the device to prevent users from using illegal client software.

The feature is implemented based on the online user handshake feature. To bring the security function into effect, make sure the online user handshake feature is enabled.

The online user handshake security feature takes effect only on the network where the iNode client and IMC server are used.

Examples

Enable the online user handshake security feature on GigabitEthernet 1/0/1.

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

Related commands

display dot1x

dot1x handshake

dot1x mac-binding

Use **dot1x mac-binding** to add an 802.1X MAC address binding entry.

Use **undo dot1x mac-binding** to delete the specified 802.1X MAC address binding entries.

Syntax

dot1x mac-binding *mac-address*

undo dot1x mac-binding { *mac-address* | **all** }

Default

No 802.1X MAC address binding entries exist on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in the format of H-H-H, excluding broadcast, multicast, and all-zero MAC addresses.

all: Specifies all MAC addresses that are bound to a port.

Usage guidelines

This command takes effect only when the 802.1X MAC address binding feature takes effect.

802.1X MAC address binding entries, both manually added and automatically generated, never age out. They can survive a user logoff or a device reboot. To delete an entry, you must use the **undo**

dot1x mac-binding *mac-address* command. An 802.1X MAC address binding entry cannot be deleted when the user in the entry is online.

After the number of 802.1X MAC address binding entries reaches the upper limit of concurrent 802.1X users (set by using the **dot1x max-user** command), the following restrictions exist:

- Users not in the binding entries will fail authentication even after users in the binding entries go offline.
- New 802.1X MAC address binding entries are not allowed.

Examples

Add an 802.1X MAC address binding entry on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x mac-binding 000a-eb29-75f1
```

Related commands

dot1x

dot1x mac-binding enable

dot1x port-method

dot1x mac-binding enable

Use **dot1x mac-binding enable** to enable the 802.1X MAC address binding feature.

Use **undo dot1x mac-binding enable** to disable the 802.1X MAC address binding feature.

Syntax

dot1x mac-binding enable

undo dot1x mac-binding enable

Default

The 802.1X MAC address binding feature is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only on a port that performs MAC-based access control.

The 802.1X MAC address binding feature automatically binds MAC addresses of authenticated 802.1X users to the users' access port and generates 802.1X MAC address binding entries.

802.1X MAC address binding entries, both automatically generated and manually added, never age out. They can survive a user logoff or a device reboot. To delete an entry, you must use the **undo dot1x mac-binding** *mac-address* command. An 802.1X MAC address binding entry cannot be deleted when the user in the entry is online.

After the number of 802.1X MAC address binding entries reaches the upper limit of concurrent 802.1X users (set by using the **dot1x max-user** command), the following restrictions exist:

- Users not in the binding entries will fail authentication even after users in the binding entries go offline.
- New 802.1X MAC address binding entries are not allowed.

Examples

Enable 802.1X MAC address binding on GigabitEthernet 1/0/1.

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

Related commands

dot1x

dot1x mac-binding

dot1x port-method

dot1x mandatory-domain

Use **dot1x mandatory-domain** to specify a mandatory 802.1X authentication domain on a port.

Use **undo dot1x mandatory-domain** to restore the default.

Syntax

dot1x mandatory-domain *domain-name*

undo dot1x mandatory-domain

Default

No mandatory 802.1X authentication domain is specified on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the ISP domain name, a case-insensitive string of 1 to 255 characters.

Usage guidelines

When the system authenticates an 802.1X user trying to access a port, it selects an authentication domain in the following order:

1. Mandatory domain.
2. ISP domain specified in the username.
3. Default ISP domain.

Examples

Specify **my-domain** as the mandatory authentication domain for 802.1X users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x mandatory-domain my-domain
```

Related commands

display dot1x

dot1x max-user

Use **dot1x max-user** to set the maximum number of concurrent 802.1X users on a port.

Use **undo dot1x max-user** to restore the default.

Syntax

dot1x max-user *max-number*

undo dot1x max-user

Default

A port allows a maximum of 4294967295 concurrent 802.1X users.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of concurrent 802.1X users on a port. The value range is 1 to 4294967295.

Usage guidelines

Set the maximum number of concurrent 802.1X users on a port to prevent the system resources from being overused. When the maximum number is reached, the port denies subsequent 802.1X users.

Examples

Set the maximum number of concurrent 802.1X users to 32 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x max-user 32
```

Related commands

display dot1x

dot1x multicast-trigger

Use **dot1x multicast-trigger** to enable the 802.1X multicast trigger feature.

Use **undo dot1x multicast-trigger** to disable the 802.1X multicast trigger feature.

Syntax

dot1x multicast-trigger

undo dot1x multicast-trigger

Default

The 802.1X multicast trigger feature is enabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The multicast trigger feature enables the device to act as the initiator. The device periodically multicasts EAP-Request/Identity packets out of a port to detect 802.1X clients and trigger authentication. You can use the **dot1x timer tx-period** command to set the interval for sending multicast EAP-Request/Identity packets.

Examples

Enable the multicast trigger feature on GigabitEthernet 1/0/1.

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

Related commands

display dot1x

dot1x timer tx-period

dot1x unicast-trigger

dot1x port-control

Use **dot1x port-control** to set the authorization state for the port.

Use **undo dot1x port-control** to restore the default.

Syntax

dot1x port-control { **authorized-force** | **auto** | **unauthorized-force** }

undo dot1x port-control

Default

The default port authorization state is **auto**.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

authorized-force: Places the port in authorized state, enabling users on the port to access the network without authentication.

auto: Places the port initially in unauthorized state to allow only EAPOL packets to pass, and places the port in authorized state after a user passes authentication. You can use this option in most scenarios.

unauthorized-force: Places the port in unauthorized state, denying any access requests from users on the port.

Usage guidelines

You can use this command to set the port authorization state to determine whether a client is granted access to the network.

Examples

Set the authorization state of GigabitEthernet 1/0/1 to **unauthorized-force**.

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

```
[Sysname-GigabitEthernet1/0/1] dot1x port-control unauthorized-force
```

Related commands

display dot1x

dot1x port-method

Use **dot1x port-method** to specify an access control method for the port.

Use **undo dot1x port-method** to restore the default.

Syntax

dot1x port-method { **macbased** | **portbased** }

undo dot1x port-method

Default

MAC-based access control applies.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

macbased: Uses MAC-based access control on the port to separately authenticate each user attempting to access the network. Using this method, when an authenticated user logs off, no other online users are affected.

portbased: Uses port-based access control on the port. Using this method, once an 802.1X user passes authentication on the port, any subsequent user can access the network through the port without authentication. When the authenticated user logs off, all other users are logged off.

Examples

Configure GigabitEthernet 1/0/1 to implement port-based access control.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x port-method portbased
```

Related commands

display dot1x

dot1x quiet-period

Use **dot1x quiet-period** to enable the quiet timer.

Use **undo dot1x quiet-period** to disable the quiet timer.

Syntax

dot1x quiet-period

undo dot1x quiet-period

Default

The quiet timer is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When a client fails 802.1X authentication, the device must wait a period of time before it can process authentication requests from the client. You can use the **dot1x timer quiet-period** command to set the quiet timer.

Examples

Enable the quiet timer and set the quiet timer to 100 seconds.

```
<Sysname> system-view
[Sysname] dot1x quiet-period
[Sysname] dot1x timer quiet-period 100
```

Related commands

display dot1x

dot1x timer

dot1x re-authenticate

Use **dot1x re-authenticate** to enable the 802.1X periodic reauthentication feature.

Use **undo dot1x re-authenticate** to disable the 802.1X periodic reauthentication feature.

Syntax

dot1x re-authenticate

undo dot1x re-authenticate

Default

The 802.1X periodic reauthentication feature is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Periodic reauthentication enables the access device to periodically authenticate online 802.1X users on a port. This feature tracks the connection status of online users and updates the authorization attributes assigned by the server, such as the ACL and VLAN.

You can use the **dot1x timer reauth-period** command to configure the interval for reauthentication.

Examples

Enable the 802.1X periodic reauthentication feature on GigabitEthernet 1/0/1, and set the periodic reauthentication interval to 1800 seconds.

```
<Sysname> system-view
[Sysname] dot1x timer reauth-period 1800
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dot1x re-authenticate
```

Related commands

display dot1x

dot1x timer

dot1x re-authenticate manual

Use **dot1x re-authenticate manual** to manually reauthenticate all online 802.1X users on a port.

Syntax

dot1x re-authenticate manual

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

After this command is executed, this device reauthenticates all online 802.1X users on a port. The command takes effect regardless of the server-assigned reauthentication attribute and the periodic reauthentication feature.

Examples

Manually reauthenticate all online 802.1X users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x re-authenticate manual
```

Related commands

dot1x re-authenticate

dot1x re-authenticate server-unreachable keep-online

Use **dot1x re-authenticate server-unreachable keep-online** to enable the keep-online feature on a port.

Use **undo dot1x re-authenticate server-unreachable** to restore the default.

Syntax

dot1x re-authenticate server-unreachable keep-online

undo dot1x re-authenticate server-unreachable

Default

The keep-online feature is disabled on a port. The device logs off online 802.1X authenticated users if no server is reachable for 802.1X reauthentication.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This feature keeps authenticated 802.1X users online when no server is reachable for 802.1X reauthentication.

Examples

Enable the keep-online feature on GigabitEthernet 1/0/1 for 802.1X reauthentication.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x re-authenticate server-unreachable keep-online
```

Related commands

display dot1x

dot1x re-authenticate

dot1x retry

Use **dot1x retry** to set the maximum number of attempts for sending an authentication request to a client.

Use **undo dot1x retry** to restore the default.

Syntax

dot1x retry *retries*

undo dot1x retry

Default

A maximum of two attempts are made to send an authentication request to a client.

Views

System view

Predefined user roles

network-admin

Parameters

retries: Specifies the maximum number of attempts for sending an authentication request to a client. The value range is 1 to 10.

Usage guidelines

The access device retransmits an authentication request to a client in any of the following situations:

- The device does not receive any responses from the client within the username request timeout interval. The timer is set by using the **dot1x timer tx-period** *tx-period-value* command for the EAP-Request/Identity packet.
- The device does not receive any responses from the client within the client timeout interval. The timer is set by using the **dot1x timer supp-timeout** *supp-timeout-value* command for the EAP-Request/MD5-Challenge packet.

The access device stops retransmitting the request, if it has made the maximum number of request transmission attempts but still received no response.

Examples

Set the maximum number of attempts to 9 for sending an authentication request to a client.

```
<Sysname> system-view
[Sysname] dot1x retry 9
```

Related commands

display dot1x

dot1x timer

dot1x timer

Use **dot1x timer** to set an 802.1X timer.

Use **undo dot1x timer** to restore the default of an 802.1X timer.

Syntax

dot1x timer { **ead-timeout** *ead-timeout-value* | **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **reauth-period** *reauth-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* }

undo dot1x timer { **ead-timeout** | **handshake-period** | **quiet-period** | **reauth-period** | **server-timeout** | **supp-timeout** | **tx-period** }

Default

The following 802.1X timers apply:

- EAD rule timer: 30 minutes.
- Handshake timer: 15 seconds.
- Quiet timer: 60 seconds.
- Periodic reauthentication timer: 3600 seconds.
- Server timeout timer: 100 seconds.
- Client timeout timer: 30 seconds.
- Username request timeout timer: 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

ead-timeout *ead-timeout-value*: Sets the EAD rule timer in minutes. The value range for the *ead-timeout-value* argument is 1 to 1440.

handshake-period *handshake-period-value*: Sets the handshake timer in seconds. The value range for the *handshake-period-value* argument is 5 to 1024.

quiet-period *quiet-period-value*: Sets the quiet timer in seconds. The value range for the *quiet-period-value* argument is 10 to 120.

reauth-period *reauth-period-value*: Sets the periodic reauthentication timer in seconds. The value range for the *reauth-period-value* argument is 60 to 7200.

server-timeout *server-timeout-value*: Sets the server timeout timer in seconds. The value range for the *server-timeout-value* argument is 100 to 300.

supp-timeout *supp-timeout-value*: Sets the client timeout timer in seconds. The value range for the *supp-timeout-value* argument is 1 to 120.

tx-period *tx-period-value*: Sets the username request timeout timer in seconds. The value range for the *tx-period-value* argument is 1 to 120.

Usage guidelines

In most cases, the default settings are sufficient. You can edit the timers, depending on the network conditions.

- In a low-speed network, increase the client timeout timer.
- In a vulnerable network, set the quiet timer to a high value.
- In a high-performance network with quick authentication response, set the quiet timer to a low value.
- In a network with authentication servers of different performance, adjust the server timeout timer.

The network device uses the following 802.1X timers:

- **EAD rule timer (`ead-timeout`)**—Sets the lifetime of each EAD rule. When the timer expires or the user passes authentication, the rule is removed. If users fail to download the EAD client or fail to pass authentication within the timer interval, they must reconnect to the network to access the free IP.
- **Handshake timer (`handshake-period`)**—Sets the interval at which the access device sends client handshake requests to check the online status of a client that has passed authentication. If the device does not receive a response after sending the maximum number of handshake requests, it considers that the client has logged off.
- **Quiet timer (`quiet-period`)**—Starts when a client fails authentication. The access device must wait the time period before it can process the authentication attempts from the client.
- **Periodic reauthentication timer (`reauth-period`)**—Sets the interval at which the network device periodically reauthenticates online 802.1X users. To enable 802.1X periodic reauthentication on a port, use the **`dot1x re-authenticate`** command.
- **Server timeout timer (`server-timeout`)**—Starts when the access device sends a RADIUS Access-Request packet to the authentication server. If no response is received when this timer expires, the 802.1X authentication fails.

  To avoid forced logoffs before the server timeout timer expires, set the server timeout timer to a value that is lower than or equal to the product of the following values:

  - The maximum number of RADIUS packet transmission attempts set by using the **`retry`** command in RADIUS scheme view.
  - The RADIUS server response timeout timer set by using the **`timer response-timeout`** command in RADIUS scheme view.

  For information about setting the maximum number of RADIUS packet transmission attempts and the RADIUS server response timeout timer, see AAA in *Security Configuration Guide*.
- **Client timeout timer (`supp-timeout`)**—Starts when the access device sends an EAP-Request/MD5-Challenge packet to a client. If no response is received when this timer expires, the access device retransmits the request to the client.
- **Username request timeout timer (`tx-period`)**—Starts when the device sends an EAP-Request/Identity packet to a client in response to an authentication request. If the device does not receive a response before this timer expires, it retransmits the request. The timer also sets the interval at which the network device sends multicast EAP-Request/Identity packets to detect clients that cannot actively request authentication.

The change to the periodic reauthentication timer applies to the users that have been online only after the old timer expires. Other timer changes take effect immediately on the device.

Examples

Set the server timeout timer to 150 seconds.

```
<Sysname> system-view
[Sysname] dot1x timer server-timeout 150
```

Related commands

display dot1x

retry

timer response-timeout (RADIUS scheme view)

dot1x timer reauth-period

Use **dot1x timer reauth-period** to set the 802.1X periodic reauthentication timer on a port.

Use **undo dot1x timer reauth-period** to restore the default.

Syntax

dot1x timer reauth-period *reauth-period-value*

undo dot1x timer reauth-period

Default

No 802.1X periodic reauthentication timer is configured on a port. The port uses the global 802.1X periodic reauthentication timer.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

reauth-period-value: Sets the 802.1X periodic reauthentication timer in seconds. The value range for the *reauth-period-value* argument is 60 to 7200.

Usage guidelines

The device reauthenticates online 802.1X users on a port at the specified periodic reauthentication interval when the port is enabled with periodic reauthentication. To enable periodic reauthentication on a port, use the **dot1x re-authenticate** command.

A change to the periodic reauthentication timer applies to online users only after the old timer expires.

The device selects a periodic reauthentication timer for 802.1X reauthentication in the following order:

1. Server-assigned reauthentication timer.
2. Port-specific reauthentication timer.
3. Global reauthentication timer.
4. Default reauthentication timer.

Examples

Set the 802.1X periodic reauthentication timer to 60 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x timer reauth-period 60
```

Related commands

dot1x timer

dot1x unicast-trigger

Use **dot1x unicast-trigger** to enable the 802.1X unicast trigger feature.

Use **undo dot1x unicast-trigger** to disable the 802.1X unicast trigger feature.

Syntax

dot1x unicast-trigger

undo dot1x unicast-trigger

Default

The 802.1X unicast trigger feature is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The unicast trigger feature enables the access device to initiate 802.1X authentication when the device receives a data frame from an unknown source MAC address. The device sends a unicast EAP-Request/Identity packet to the unknown source MAC address. It will retransmit the packet if it does not receive any responses within a period of time (set by using the **dot1x timer tx-period** command). This process continues until the maximum number of request attempts (set by using the **dot1x retry** command) is reached.

Examples

Enable the unicast trigger feature on GigabitEthernet 1/0/1.

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

Related commands

display dot1x

dot1x multicast-trigger

dot1x retry

dot1x timer

dot1x user-ip freeze

Use **dot1x user-ip freeze** to enable 802.1X user IP freezing.

Use **undo dot1x user-ip freeze** to disable 802.1X user IP freezing.

Syntax

dot1x user-ip freeze

undo dot1x user-ip freeze

Default

802.1X user IP freezing is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command prevents 802.1X-generated IPSG bindings from being updated because of user IP changes. For information about IP source guard commands, see "IP source guard commands."

Examples

Enable 802.1X user IP freezing on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x user-ip freeze
```

reset dot1x guest-vlan

Use **reset dot1x guest-vlan** to remove users from the 802.1X guest VLAN on a port.

Syntax

reset dot1x guest-vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

mac-address *mac-address*: Specifies the MAC address of an 802.1X user in the guest VLAN. If you do not specify this option, the command removes all 802.1X users from the 802.1X guest VLAN on the port.

Examples

Remove the 802.1X user with MAC address 1-1-1 from the 802.1X guest VLAN on GigabitEthernet 1/0/1.

```
<Sysname> reset dot1x guest-vlan interface gigabitethernet 1/0/1 mac-address 1-1-1
```

Related commands

dot1x guest-vlan

reset dot1x statistics

Use **reset dot1x statistics** to clear 802.1X statistics.

Syntax

reset dot1x statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command clears 802.1X statistics on all ports.

Examples

Clear 802.1X statistics on GigabitEthernet 1/0/1.

```
<Sysname> reset dot1x statistics interface gigabitethernet 1/0/1
```

Related commands

display dot1x