1 IEEE 802.1X Commands

Command	Function
aaa authorization ip-auth-mode	Configure the global IP authorization mode.
clear dot1x user	Delete an IEEE 802.1X-authenticated user on the device.
dot1x accounting	Configure an accounting method list.
dot1x acct-update base-on first-time server	Set the accounting update period to that delivered by the server at the first authentication.
dot1x auth-fail max-attempt	Configure the maximum number of consecutive failed authentication attempts.
dot1x auth-fail vlan	Configure the failed VLAN.
dot1x auth-mode	Configure the authentication mode.
dot1x auth-address-table	Configure a list of hosts allowed for authentication.
dot1x auth-with-order	Set the priority of MAB to be higher than that of IEEE 802.1X authentication.
dot1x authentication	Configure an authentication method list.
dot1x auto-req	Enable the active IEEE 802.1X authentication function on the device.
dot1x auto-req packet-num	Configure the maximum number of active authentication request packets that can be sent by the device.
dot1x auto-req req-interval	Configure the interval for the device to send active authentication request packets.
dot1x auto-req user-detect	Enable the function of detecting whether a user is being authenticated during active authentication.
dot1x client-probe enable	Enable online Orion client detection.
dot1x critical	Enable the inaccessible authentication bypass (IAB) function.
dot1x critical recovery action reinitialize	Enable the IAB recovery.
dot1x critical vlan	Configure the IAB VLAN.
dot1x dbg-filter	Configure the debugging of a specific MAC address.

dot1x default-user-limit	Configure the maximum number of users who can be authenticated on an interface.
dot1x default	Restore the default configuration of IEEE 802.1X.
dot1x dynamic-vlan enable	Enable dynamic VLAN redirection on a port.
dot1x guest-vlan	Configure the guest VLAN on a controlled port.
dot1x mab-username upper	Configure usernames used for MAB to use uppercase letters.
dot1x mac-auth-bypass	Enable single-user MAB.
dot1x mac-auth-bypass multi-user	Enable multi-user MAB.
dot1x mac-auth-bypass timeout-activity	Configure the MAB timeout duration.
dot1x mac-auth-bypass violation	Enable the MAB violation function.
dot1x mac-auth-bypass vlan	Configure the MAB VLAN.
dot1x max-req	Configure the maximum retransmission count of Request/Challenge packets.
dot1x multi-account enable	Enable multi-account authentication with one MAC address.
dot1x multi-mab quiet-period	Configure the quiet period after a multi-user MAB failure.
dot1x multi-mab quiet-user fail-times	Configure the number of authentication failures required for user entry aging.
dot1x multi-mab quiet-user authen-num	Configure the rate of initiating authentication using the MAC address in a multi-user MAB quiet user entry.
dot1x multi-mab quiet-user reject-times	Configure the server rejection count for the device to delete a quiet user entry.
dot1x mab-username format	Configure the username format for MAB.
dot1x port-control auto	Enable IEEE 802.1X authentication on a port.
dot1x port-control-mode	Configure the port control mode.
dot1x probe-timer interval	Configure the Orion client detection interval.
dot1x probe-timer alive	Configure the Orion client detection duration.
dot1x private-supplicant-only	Enable the non-Orion client filtering function.
dot1x pseudo source-mac	Configure a virtual MAC address as the source MAC

	address of IEEE 802.1X packets sent by the device.
dot1x redirect	Enable the 2nd-generation Orion Supplicant deployment function.
dot1x reauth-max	Configure the maximum retransmission count of the Request/Identity packets.
dot1x re-authentication	Enable re-authentication.
dot1x stationarity enable	Disable dynamic user migration.
dot1x timeout re-authperiod	Configure the re-authentication interval.
dot1x timeout quiet-period	Configure the quiet period after an authentication failure.
dot1x timeout supp-timeout	Configure the retransmission interval of Request/Challenge packets.
dot1x timeout server-timeout	Configure the server timeout duration.
dot1x timeout tx-period	Configure the retransmission interval of Request/Identity packets.
dot1x user-name compatible	Enable the compatibility with H3C IEEE 802.1X authentication clients and authentication servers.
dot1x valid-ip-acct enable	Enable the function of initiating accounting after a user's IP address is obtained.
dot1x valid-ip-acct timeout	Configure the timeout duration for an authenticated user to obtain an IP address.
dot1x system disable	Disable global IEEE 802.1X features.
show dot1x	Display IEEE 802.1X protocol parameters.
show dot1x auth-address-table	Display the list of hosts allowed for authentication.
show dot1x auto-req	Display active authentication status and parameters.
show dot1x max-req	Display the maximum retransmission count of Request/Challenge packets.
show dot1x port-control	Display information about controlled ports.
show dot1x private-supplicant-only	Display the status of the non-Orion client filtering function.
show dot1x probe-timer	Display the client detection parameters.
show dot1x re-authentication	Display the status of the re-authentication function.
show dot1x reauth-max	Display the maximum retransmission count of

	Request/Identity packets.
show dot1x summary	Display entries of users participating in authentication.
show dot1x timeout quiet-period	Display the quiet period after an authentication failure.
show dot1x timeout re-authperiod	Display the re-authentication interval.
show dot1x timeout server-timeout	Display the server timeout duration.
show dot1x timeout supp-timeout	Display the retransmission interval of Request/Challenge packets.
show dot1x timeout tx-period	Display the retransmission interval of Request/Identity packets.
show dot1x user mac	Display details about a user with a specified MAC address.
show dot1x user name	Display details about a user with a specified username.

1.1 aaa authorization ip-auth-mode

Function

Run the **aaa authorization ip-auth-mode** command to configure the global IP authorization mode.

Run the **no** form of this command to disable this feature.

Global IP authorization is disabled by default.

Syntax

aaa authorization ip-auth-mode { **dhcp-server** | **disable** | **mixed** | **radius-server** | **supplicant** }

no aaa authorization ip-auth-mode

Parameter Description

dhcp-server: Configures the Dynamic Host Configuration Protocol (DHCP) authorization mode, in which IP addresses are assigned via DHCP for binding.

disable: Disables authorization.

mixed: Configures the mixed authorization mode. In the existence of multiple global IP authorization modes, authenticated users select an IP authorization mode based on the sequence of Supplicant authorization, Remote Authentication Dial In User Service (RADIUS) authorization, and DHCP authorization.

radius-server: Configures the RADIUS authorization mode, in which IP addresses are delivered by a RADIUS server for binding.

supplicant: Configures the Supplicant authorization mode, in which Supplicant provides IP addresses for binding.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The Supplicant authorization mode supports only Orion Supplicant.

In RADIUS authorization mode, the server needs to deliver IP addresses through the **framed-ip** attribute.

In DHCP authorization mode, DHCP snooping or DHCP relay needs to be enabled on the device.

You are advised to use the mixed authorization mode in the case of multiple authorization modes.

Examples

The following example configures the Supplicant authorization mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa authorization ip-auth-mode supplicant
```

Notifications

N/A

Common Errors

IP authorization occupies hardware resources. The considerable number of users in the network and coexistence of multiple security functions may lead to hardware resource insufficiency, which finally causes the failure of users to access the network.

Platform Description

N/A

Related Commands

N/A

1.2 clear dot1x user

Function

Run the **clear dot1x user** command to delete an IEEE 802.1X-authenticated user on the device.

Syntax

clear dot1x user { **all** | **ip** *ipv4-address* | **mac** *mac-address* | **name** *user-name* }

Parameter Description

all: Deletes all IEEE 802.1X-authenticated users.

ip *ipv4-address*: Deletes an IEEE 802.1X-authenticated user with a specific IP address.

mac *mac-address*: Deletes an IEEE 802.1X-authenticated user with a specific MAC address.

name *user-name*: Deletes an IEEE 802.1X-authenticated user with a specific username.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example deletes all IEEE 802.1X-authenticated users from the device.

```
Hostname> enable
Hostname# clear dot1x user all
```

The following example deletes an IEEE 802.1X-authenticated user with the IP address 11.1.1.1.

```
Hostname> enable
Hostname# clear dot1x user ip 11.1.1.1
```

The following example deletes an IEEE 802.1X-authenticated user with the MAC address 0012.3456.789A.

```
Hostname> enable
Hostname# clear dot1x user mac 0012.3456.789A
```

The following example deletes an IEEE 802.1X-authenticated user with the username **dot1x-user**.

```
Hostname> enable
Hostname# clear dot1x user name dot1x-user
```

Notifications

N/A

Platform Description

N/A

1.3 dot1x accounting

Function

Run the **dot1x accounting** command to configure an accounting method list.

Run the **no** form of this command to remove this configuration.

Syntax

dot1x accounting { **default |** *list-name* }

no dot1x accounting

Parameter Description

default: Uses the default accounting method list.

list-name: Name of a specified accounting method list.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Define a method list in AAA before configuring this command.

Examples

The following example configures an accounting method list named **dot1x-acct**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x accounting dot1x-acct
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **aaa accounting network** (AAA)

1.4 dot1x acct-update base-on first-time server

Function

Run the **dot1x acct-update base-on first-time server** command to set the accounting update period to that delivered by the server at the first authentication.

Run the **no** form of this command to remove this configuration.

The accounting update period delivered by the server at the first authentication is not configured as the accounting update period for re-authentication by default.

Syntax

dot1x acct-update base-on first-time server

no dot1x acct-update base-on first-time server

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Some servers do not deliver the accounting update period during user re-authentication, but require that accounting update packets be sent at the accounting update period delivered at the first authentication. In this case, you can configure this command to meet this requirement.

Examples

The following example sets the accounting update period to that delivered by the server at the first authentication.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x acct-update base-on first-time server
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.5 dot1x auth-fail max-attempt

Function

Run the **dot1x auth-fail max-attempt** command to configure the maximum number of consecutive failed authentication attempts.

Run the **no** form of this command to restore the default configuration.

The default maximum number of consecutive failed authentication attempts is **3**.

Syntax

dot1x auth-fail max-attempt *max-attempt-number*

no dot1x auth-fail max-attempt

Parameter Description

max-attempt-number: Maximum number of consecutive failed authentication attempts. The value range is from 1 to 3.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the maximum number of times that a user is consecutively rejected by the authentication server. If the rejection count reaches this number, the port, to which the user is connected, will be added to a failed VLAN and the user is allowed to access network resources in the failed VLAN.

Examples

The following example sets the maximum number of consecutive failed authentication attempts to 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x auth-fail max-attempt 2
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **dot1x auth-fail vlan**

1.6 dot1x auth-fail vlan

Function

Run the **dot1x auth-fail vlan** command to configure the failed VLAN.

Run the **no** form of this command to disable this feature.

The failed VLAN function is disabled by default.

Syntax

dot1x auth-fail vlan *vlan-id*

no dot1x auth-fail vlan

Parameter Description

vlan-id: VLAN, to which users who fail the authentication are to be added. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After the failed VLAN is configured, users who fail the authentication can access network resources only in the failed VLAN.

Examples

The following example sets the failed VLAN to VLAN 30.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x auth-fail vlan 30
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **dot1x auth-fail max-attempt**

1.7 dot1x auth-mode

Function

Run the **dot1x auth-mode** command to configure the authentication mode.

Run the **no** form of this command to restore the default configuration.

The default authentication mode is Extensible Authentication Protocol (EAP) mode.

Syntax

dot1x auth-mode { **chap** | **eap** | **pap** }

no dot1x auth-mode

Parameter Description

chap: Sets the authentication mode to Challenge-Handshake Authentication Protocol (CHAP) mode.

eap: Sets the authentication mode to EAP mode.

pap: Sets the authentication mode to Password Authentication Protocol (PAP) mode.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Select an authentication mode based on whether Orion Supplicant is supported and the authentication mode supported by the authentication server.

Examples

The following example sets the authentication mode to CHAP mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x auth-mode chap
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.8 dot1x auth-address-table

Function

Run the **dot1x auth-address-table** command to configure a list of hosts allowed for authentication.

Run the **no** form of this command to remove this configuration.

Syntax

dot1x auth-address-table address *mac-address* **interface** *interface-type interface-number*

no dot1x auth-address-table address *mac-address* **interface** *interface-type interface-number*

Parameter Description

mac-address: MAC address of an access client allowed for authentication.

interface-type interface-number: Interface type and interface number of the access client.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to allow only clients with specific MAC addresses on a specified port to perform IEEE 802.1X authentication.

Examples

The following example sets the access port of a host allowed for authentication to GigabitEthernet 0/1 and the MAC address to 00d0.f800.0cb2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x auth-address-table address 00d0.f800.0cb2 interface
gigabitEthernet 0/1
```

Notifications

N/A

Platform Description

N/A

1.9 dot1x auth-with-order

Function

Run the **dot1x auth-with-order** command to set the priority of MAB to be higher than that of IEEE 802.1X authentication.

Run the **no** form of this command to restore the default configuration.

The priority of MAB is lower than that of IEEE 802.1X authentication by default.

Syntax

dot1x auth-with-order

no dot1x auth-with-order

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The priority of IEEE 802.1X authentication is higher than that of MAB by default. If IEEE 802.1X authentication is performed after MAB is completed, the IEEE 802.1X authentication result will replace the MAB result. After this function is enabled, MAB has a higher priority and the device performs MAB first. The IEEE 802.1X authentication result cannot replace the MAB result.

Examples

The following example sets the priority of MAB to be higher than that of IEEE 802.1X authentication.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x auth-with-order
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.10 dot1x authentication

Function

Run the **dot1x authentication** command to configure an authentication method list.

Run the **no** form of this command to remove this configuration.

Syntax

dot1x authentication { **default** | *list-name* }

no dot1x authentication

Parameter Description

default: Uses the default authentication method list.

list-name: Name of a specified authentication method list.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Define a method list in AAA before configuring this command.

Examples

The following example configures an authentication method list named **dot1x-authen**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x authentication dot1x-authen
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **aaa authentication dot1x** (AAA)

1.11 dot1x auto-req

Function

Run the **dot1x auto-req** command to enable the active IEEE 802.1X authentication function on the device.

Run the **no** form of this command to disable this feature.

The active IEEE 802.1X authentication function is enabled by default.

Syntax

dot1x auto-req

no dot1x auto-req

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Active authentication refers that the device actively sends a Request/Identity packet, which triggers IEEE 802.1X clients to initiate IEEE 802.1X authentication.

This function must be enabled for MAB deployment.

Some clients use authentication clients embedded in the operating system (OS). They may not initiate authentication immediately after connecting to the network, and users cannot use the network promptly. The

configured active authentication can urge such clients to initiate authentication in a timely manner after they connect to the network.

Do not enable this function when a controlled port is a trunk port and is directly connected to clients. Otherwise, frequent authentication or going offline may occur.

Examples

The following example enables active 802.1X authentication on the device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x auto-req
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.12 dot1x auto-req packet-num

Function

Run the **dot1x auto-req packet-num** command to configure the maximum number of active authentication request packets that can be sent by the device.

Run the **no** form of this command to restore the default configuration.

The device always sends authentication request packets actively by default.

Syntax

dot1x auto-req packet-num *packet-number*

no dot1x auto-req packet-num

Parameter Description

packet-number: Maximum number of active authentication request packets that can be sent. The value range is from 0 to 1000000 and the value **0** indicates that the device sends authentication request packets continuously.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the maximum number of active authentication request packets that can be sent by the device to 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x auto-req packet-num 100
```

Notifications

N/A

Platform Description

N/A

Related Commands

- dot1x auto-req

1.13 dot1x auto-req req-interval

Function

Run the **dot1x auto-req req-interval** command to configure the interval for the device to send active authentication request packets.

Run the **no** form of this command to restore the default configuration.

The default interval for the device to send active authentication request packets is **30** seconds.

Syntax

dot1x auto-req req-interval *req-interval*

no dot1x auto-req req-interval

Parameter Description

req-interval: Interval for sending active authentication request packets, in seconds. The value range is from 10 to 3600.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the interval for the device to send active authentication request packets to 50 seconds.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# dot1x auto-req req-interval 50
```

Notifications

N/A

Platform Description

N/A

Related Commands

- dot1x auto-req

1.14 dot1x auto-req user-detect

Function

Run the **dot1x auto-req user-detect** command to enable the function of detecting whether a user is being authenticated during active authentication.

Run the **no** form of this command to disable this feature.

The function of detecting whether a user is being authenticated during active authentication is enabled by default.

Syntax

dot1x auto-req user-detect

no dot1x auto-req user-detect

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You are advised to enable this function only when one client is connected to a port, to reduce authentication load of the server.

Examples

The following example disables the function of detecting whether a user is being authenticated during active authentication.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no dot1x auto-req user-detect
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.15 dot1x client-probe enable

Function

Run the **dot1x client-probe enable** command to enable online Orion client detection.

Run the **no** form of this command to disable this feature.

Online Orion client detection is disabled by default.

Syntax

dot1x client-probe enable

no dot1x client-probe enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You are advised to enable this function when Orion Supplicant is used.

Examples

The following example enables online Orion client detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x client-probe enable
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.16 dot1x critical

Function

Run the **dot1x critical** command to enable the inaccessible authentication bypass (IAB) function.

Run the **no** form of this command to disable this feature.

IAB is disabled by default.

Syntax

dot1x critical

no dot1x critical

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

IAB is a method provided for new to-be-authenticated users to access the network when all RADIUS servers configured on the device are all unreachable. After a RADIUS server becomes reachable, it verifies the identities of users authorized in the unavailability period of RADIUS servers.

Examples

The following example enables IAB.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x critical
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.17 dot1x critical recovery action reinitialize

Function

Run the **dot1x critical recovery action reinitialize** command to enable the IAB recovery.

Run the **no** form of this command to disable this feature.

IAB recovery is disabled by default.

Syntax

dot1x critical recovery action reinitialize

no dot1x critical recovery action reinitialize

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After this command is configured, if a RADIUS server becomes reachable, it verifies the identities of users authorized by IAB in the unavailability period of RADIUS servers.

Examples

The following example enables IAB recovery.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x critical recovery action
reinitialize
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.18 dot1x critical vlan

Function

Run the **dot1x critical vlan** command to configure the IAB VLAN.

Run the **no** form of this command to disable this feature.

The IAB VLAN function is disabled by default.

Syntax

dot1x critical vlan *vlan-id*

no dot1x critical vlan

Parameter Description

vlan-id: ID of an IAB VLAN. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the IAB VLAN to VLAN 10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x critical vlan 10
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **dot1x critical**

1.19 dot1x dbg-filter

Function

Run the **dot1x dbg-filter** command to configure the debugging of a specific MAC address.

Run the **no** form of this command to remove this configuration.

Debugging information of all authenticated users is printed by default.

Syntax

dot1x dbg-filter *mac-address*

no dot1x dbg-filter *mac-address*

Parameter Description

mac-address: MAC address of a user whose debugging information needs to be output.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When there are a large number of users in the network and a network fault needs to be pinpointed, you can configure the debugging of users with specific MAC addresses, to avoid outputting debugging information of too many irrelevant users.

Examples

The following example debugs the MAC address 00d0.f800.0001.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x dbg-filter 00d0.f800.0001
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.20 dot1x default-user-limit

Function

Run the **dot1x default-user-limit** command to configure the maximum number of users who can be authenticated on an interface.

Run the **no** form of this command to restore the default configuration.

The maximum number of users who can be authenticated on an interface is unlimited.

Syntax

dot1x default-user-limit *limit-number*

no dot1x default-user-limit

Parameter Description

limit-number: Maximum number of users who can be authenticated on an interface. The value range is from 1 to 1000000.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the maximum number of users who can be authenticated on an interface to 10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x default-user-limit 10
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.21 dot1x default

Function

Run the **dot1x default** command to restore the default configuration of IEEE 802.1X.

Syntax

dot1x default

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command can clear existing IEEE 802.1X configurations in one-click mode. Use this command when considerable 802.1X configurations need to be cleared and reconfiguration is needed.

Examples

The following example restores the default configuration of IEEE 802.1X.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x default
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.22 dot1x dynamic-vlan enable

Function

Run the **dot1x dynamic-vlan enable** command to enable dynamic VLAN redirection on a port.

Run the **no** form of this command to disable this feature.

Dynamic VLAN redirection is disabled on a port by default.

Syntax

dot1x dynamic-vlan enable

no dot1x dynamic-vlan enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Configure this command when authenticated users need to be added to the VLAN delivered by the server.

Examples

The following example enables dynamic VLAN redirection on a port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x dynamic-vlan enable
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.23 dot1x guest-vlan

Function

Run the **dot1x guest-vlan** command to configure the guest VLAN on a controlled port.

Run the **no** form of this command to disable this feature.

The guest VLAN function is disabled on a controlled port by default.

Syntax

dot1x guest-vlan *vlan-id*

no dot1x guest-vlan

Parameter Description

vlan-id: Guest VLAN, to which a port needs to be added. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The guest VLAN function is used to provide network access permissions for terminals, on which the IEEE 802.1X client is not installed.

After the guest VLAN function is configured, if no IEEE 802.1X client is detected on a controlled port, the port is added to the guest VLAN to allow terminals connected to the port to access network resources in the guest VLAN.

After guest VLAN is enabled on a port, do not configure L2 attributes, especially do not manually configure the port VLAN.

Examples

The following example sets the guest VLAN to VLAN 20 on a controlled port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x guest-vlan 20
```

Notifications

N/A

Platform Description

N/A

Related Commands

- dot1x dynamic-vlan enable

1.24 dot1x mab-username upper

Function

Run the **dot1x mab-username upper** command to configure usernames used for MAB to use uppercase letters.

Run the **no** form of this command to restore the default configuration.

Usernames used for MAB use lowercase letters by default.

Syntax

dot1x mab-username upper

no dot1x mab-username upper

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to meet requirements of different servers for username uppercase/lowercase in MAB.

Examples

The following example configures usernames used for MAB to use uppercase letters.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x mab-username upper
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.25 dot1x mac-auth-bypass

Function

Run the **dot1x mac-auth-bypass** command to enable single-user MAB.

Run the **no** form of this command to disable this feature.

Single-user MAB is disabled by default.

Syntax

dot1x mac-auth-bypass

no dot1x mac-auth-bypass

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Single-user MAB applies to the scenario, in which a port has only one dumb terminal attached to it or a port has only one dumb terminal to be authenticated. After successful authentication, other terminals connected to the port can access the network.

Examples

The following example enables single-user MAB.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x mac-auth-bypass
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.26 dot1x mac-auth-bypass multi-user

Function

Run the **dot1x mac-auth-bypass multi-user** command to enable multi-user MAB.

Run the **no** form of this command to disable this feature.

Multi-user MAB is disabled by default.

Syntax

dot1x mac-auth-bypass multi-user

no dot1x mac-auth-bypass multi-user

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Multi-user MAB applies when multiple dumb terminals are connected to one port. Multi-user MAB can be used together with IEEE 802.1X authentication in mixed access scenarios such as the PC+VoIP daisy-chain topology.

Examples

The following example enables multi-user MAB.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x mac-auth-bypass multi-user
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.27 dot1x mac-auth-bypass timeout-activity

Function

Run the **dot1x mac-auth-bypass timeout-activity** command to configure the MAB timeout duration.

Run the **no** form of this command to remove this configuration.

MAB does not time out by default.

Syntax

dot1x mac-auth-bypass timeout-activity *timeout*

no dot1x mac-auth-bypass timeout-activity

Parameter Description

timeout: MAB timeout duration, in seconds. The value range is from 1 to 65535.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You can configure this parameter to restrict the network access duration of dumb terminals.

Examples

The following example sets the MAB timeout duration to 3,600 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x mac-auth-bypass timeout-activity
3600
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.28 dot1x mac-auth-bypass violation

Function

Run the **dot1x mac-auth-bypass violation** command to enable the MAB violation function.

Run the **no** form of this command to disable this feature.

MAB violation is disabled by default.

Syntax

dot1x mac-auth-bypass violation

no dot1x mac-auth-bypass violation

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This function can be configured to restrict one port to have only one dumb terminal. This command applies only to single-user MAB scenarios.

Examples

The following example enables the MAB violation function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x mac-auth-bypass violation
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.29 dot1x mac-auth-bypass vlan

Function

Run the **dot1x mac-auth-bypass vlan** command to configure the MAB VLAN.

Run the **no** form of this command to disable this feature.

The MAB VLAN function is disabled by default.

Syntax

dot1x mac-auth-bypass vlan *vlan-id*

no dot1x mac-auth-bypass vlan *vlan-id*

Parameter Description

vlan-id: ID of a VLAN allowed for MAB. The value is a valid VLAN ID. If you configure multiple VLAN IDs, separate them with commas (,). You can also configure a VLAN ID range, for example, 3-5 indicates VLANs 3, 4, and 5.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is configured to only allow users in a specific VLAN on an interface to perform MAB.

Examples

The following example sets MAB VLANs to VLAN 5 and VLANs 8-20.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x mac-auth-bypass vlan 5, 8-20
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.30 dot1x max-req

Function

Run the **dot1x max-req** command to configure the maximum retransmission count of Request/Challenge packets.

Run the **no** form of this command to restore the default configuration.

The default maximum retransmission count of Request/Challenge packets is **3**.

Syntax

dot1x max-req *max-req-number*

no dot1x max-req

Parameter Description

max-req-number: Maximum retransmission count of Request/Challenge packets. The value range is from 1 to 10.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The default value is recommended.

Examples

The following example sets the maximum retransmission count of Request/Challenge packets to 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x max-req 2
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.31 dot1x multi-account enable

Function

Run the **dot1x multi-account enable** command to enable multi-account authentication with one MAC address.

Run the **no** form of this command to disable this feature.

Multi-account authentication with one MAC address is disabled by default.

Syntax

dot1x multi-account enable

no dot1x multi-account enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to handle account switching during authentication or re-authentication, for example, domain authentication in Windows.

Examples

The following example enables multi-account authentication with one MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x multi-account enable
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.32 dot1x multi-mab quiet-period

Function

Run the **dot1x multi-mab quiet-period** command to configure the quiet period after a multi-user MAB failure.

Run the **no** form of this command to restore the default configuration.

The default quiet period after a multi-user MAB failure is **30** seconds.

Syntax

dot1x multi-mab quiet-period *quiet-period*

no dot1x multi-mab quiet-period

Parameter Description

quiet-period: Quiet period after a multi-user MAB failure, in seconds. The value range is from 0 to 65535 and the value **0** indicates no quiet period.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After multi-user MAB is enabled, illegitimate users connected to an interface may attack the device. Therefore, it is necessary to prevent illegitimate users from frequently initiating authentication, in an effort to reduce the server load. Configure the quiet period after a multi-user MAB failure in global configuration mode. After configuration, if a MAC address fails the authentication, it can re-initiate authentication only after the quiet period elapses. Configure this quiet period as required.

Examples

The following example sets the quiet period after a multi-user MAB failure to 2 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x multi-mab quiet-period 2
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.33 dot1x multi-mab quiet-user fail-times

Function

Run the **dot1x multi-mab quiet-user fail-times** command to configure the number of authentication failures required for user entry aging.

Run the **no** form of this command to restore the default configuration.

The default number of authentication failures required for user entry aging is **60**.

Syntax

dot1x multi-mab quiet-user fail-times [*fail-times*]

no dot1x multi-mab quiet-user fail-times

Parameter Description

fail-times: Number of authentication failures required for user entry aging. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure aging rules for users who fail the authentication.

Examples

The following example sets the number of authentication failures required for user entry aging to 3.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x multi-mab quiet-user fail-times 3
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.34 dot1x multi-mab quiet-user authen-num

Function

Run the **dot1x multi-mab quiet-user authen-num** command to configure the rate of initiating authentication using the MAC address in a multi-user MAB quiet user entry.

Run the **no** form of this command to restore the default configuration.

The default rate of initiating authentication using the MAC address in a multi-user MAB quiet user entry is **50** MAC addresses per second.

Syntax

dot1x multi-mab quiet-user authen-num [*authen-num*]

no dot1x multi-mab quiet-user authen-num

Parameter Description

authen-num: Rate of initiating authentication using the MAC address in a multi-user MAB quiet user entry, in MAC addresses per second. The value range is from 1 to 1000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the rate of initiating authentication using the MAC address in a multi-user MAB quiet user entry to 3 MAC addresses per second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x multi-mab quiet-user authen-num 3
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.35 dot1x multi-mab quiet-user reject-times

Function

Run the **dot1x multi-mab quiet-user reject-times** command to configure the server rejection count for the device to delete a quiet user entry.

Run the **no** form of this command to restore the default configuration.

The default server rejection count for the device to delete a quiet user entry is **1**.

Syntax

dot1x multi-mab quiet-user reject-times [*reject-times*]

no dot1x multi-mab quiet-user reject-times

Parameter Description

reject-times: Server rejection count for the device to delete a quiet user entry.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the device to delete a quiet user entry after the server rejects the user authentication three times.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x multi-mab quiet-user reject-times 3
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.36 dot1x mab-username format

Function

Run the **dot1x mab-username format** command to configure the username format for MAB.

Run the **no** form of this command to remove this configuration.

No username format for MAB is configured by default.

Syntax

dot1x mab-username format [**with-colon** | **with-dot** | **with-hyphen** | **with-3hyphen**]

no dot1x mab-username format

Parameter Description

with-colon: Indicates that the username format is xx:xx:xx:xx:xx:xx.

with-dot: Indicates that the username format is xxxx.xxxx.xxxx.

with-hyphen: Indicates that the username format is xx-xx-xx-xx-xx-xx.

with-3hyphen: Indicates that the username format is xxxx-xxxx-xxxx.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the required username format for MAB is xx-xx-xx-xx-xx-xx, configure **with-hyphen** in this command.

When the required username format for MAB is xxxx.xxxx.xxxx, configure **with-dot** in this command.

When the required username format for MAB is xx:xx:xx:xx:xx:xx, configure **with-colon** in this command.

When the required username format for MAB is xxxx-xxxx-xxxx, configure **with-3hyphen** in this command.

Examples

The following example sets the username format for MAB to **with-hyphen**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x mab-username format with-hyphen
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.37 dot1x port-control auto

Function

Run the **dot1x port-control auto** command to enable IEEE 802.1X authentication on a port.

Run the **no** form of this command to disable this feature.

IEEE 802.1X authentication is disabled on a port by default.

Syntax

dot1x port-control auto

no dot1x port-control auto

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Other IEEE 802.1X commands are meaningful only after this command is configured.

Examples

The following example enables IEEE 802.1X authentication on a port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x port-control auto
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.38 dot1x port-control-mode

Function

Run the **dot1x port-control-mode** command to configure the port control mode.

Run the **no** form of this command to restore the default configuration.

The default port control mode is MAC-based control.

Syntax

dot1x port-control-mode { **mac-based** | **port-based** [**single-host**] }

no dot1x port-control-mode

Parameter Description

mac-based: Sets the port control mode to MAC-based control.

port-based [**single-host**]: Sets the port control mode to port-based control. **single-host** indicates that only one client is allowed on an interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Configure the MAC-based control mode if each user on a controlled port has to pass authentication before making communication.

Configure the port-based control mode if all users on a controlled port can make communication after one of them passes the authentication.

In port-based control mode, this command can be configured only when authenticated users are dynamic users.

Examples

The following example sets the port control mode to port-based control.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# dot1x port-control-mode port-based
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.39 dot1x probe-timer interval

Function

Run the **dot1x probe-timer interval** command to configure the Orion client detection interval.

Run the **no** form of this command to restore the default configuration.

The default client detection interval is **20** seconds.

Syntax

dot1x probe-timer interval *interval*

no dot1x probe-timer interval

Parameter Description

interval: Client detection interval, in seconds. The value range is from 1 to 32767.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The default configuration is recommended.

The interval for sending packets to detect whether Orion clients are online must be smaller than half of the online detection duration.

Examples

The following example sets the Orion client detection interval to 30 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x probe-timer interval 30
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **dot1x probe-timer alive**

1.40 dot1x probe-timer alive

Function

Run the **dot1x probe-timer alive** command to configure the Orion client detection duration.

Run the **no** form of this command to restore the default configuration.

The default Orion client detection duration is **250** seconds.

Syntax

dot1x probe-timer alive *alive-time*

no dot1x probe-timer alive

Parameter Description

alive-time: Orion client detection duration, in seconds. The value range is from 3 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After a client is authenticated and goes online, if the device fails to receive any detection response from the client within the detection duration, the device considers the client offline.

The default configuration is recommended.

The online detection duration must be greater than twice the interval for sending packets to detect whether Orion clients are online.

Examples

The following example sets the Orion client detection duration to 120 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x probe-timer alive 120
```

Notifications

N/A

Platform Description

N/A

Related Commands

- dot1x probe-timer interval

1.41 dot1x private-supplicant-only

Function

Run the **dot1x private-supplicant-only** command to enable the non-Orion client filtering function.

Run the **no** form of this command to disable this feature.

The non-Orion client filtering function is disabled by default.

Syntax

dot1x private-supplicant-only

no dot1x private-supplicant-only

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This function should be configured if Orion Supplicant must be used for authentication.

Examples

The following example enables the non-Orion client filtering function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x private-supplicant-only
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.42 dot1x pseudo source-mac

Function

Run the **dot1x pseudo source-mac** command to configure a virtual MAC address as the source MAC address of IEEE 802.1X packets sent by the device.

Run the **no** form of this command to remove this configuration.

The source MAC address of IEEE 802.1X packets sent by the device is a virtual MAC address by default.

Syntax

dot1x pseudo source-mac

no dot1x pseudo source-mac

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Some Orion Supplicant versions judge whether an access device is a Orion device based on the source MAC addresses of EAP packets, so as to implement Orion private features. If a device works with such Supplicant versions to perform IEEE 802.1X authentication and private features are needed, configure this command on the device.

Examples

The following example configures not to use the virtual MAC address as the source MAC address of IEEE 802.1X packets sent by the device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no dot1x pseudo source-mac
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.43 dot1x redirect

Function

Run the **dot1x redirect** command to enable the 2nd-generation Orion Supplicant deployment function.

Run the **no** form of this command to disable this feature.

The 2nd-generation Orion Supplicant deployment function is disabled by default.

Syntax

dot1x redirect

no dot1x redirect

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The 2nd-generation Orion Supplicant deployment function redirects the browser to a specified resource website so that the Supplicant software can be downloaded.

Redirection parameters need to be configured.

Examples

The following example enables the 2nd-generation Orion Supplicant deployment function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x redirect
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

Related Commands

N/A

1.44 dot1x reauth-max

Function

Run the **dot1x reauth-max** command to configure the maximum retransmission count of the Request/Identity packets.

Run the **no** form of this command to restore the default configuration.

The default maximum retransmission count of Request/Identity packets is **3**.

Syntax

dot1x reauth-max *reauth-max-number*

no dot1x reauth-max

Parameter Description

reauth-max-number: Maximum retransmission count of Request/Identity packets. The value range is from 1 to 10.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The default value is recommended.

Examples

The following example sets the maximum retransmission count of Request/Identity packets to 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x reauth-max 2
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.45 dot1x re-authentication

Function

Run the **dot1x re-authentication** command to enable re-authentication.

Run the **no** form of this command to disable this feature.

The re-authentication function is disabled by default.

Syntax

dot1x re-authentication

no dot1x re-authentication

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Re-authentication brings great burden to the server. You are advised to disable this function in an environment with a large number of users.

Examples

The following example enables the re-authentication function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x re-authentication
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.46 dot1x stationarity enable

Function

Run the **dot1x stationarity enable** command to disable dynamic user migration.

Run the **no** form of this command to restore the default configuration.

Dynamic user migration is enabled by default.

Syntax

dot1x stationarity enable

no dot1x stationarity enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is configured, dynamic users are not allowed to migrate to other ports in port-based control mode.

Examples

The following example disables dynamic user migration.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x stationarity enable
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.47 dot1x timeout re-authperiod

Function

Run the **dot1x timeout re-authperiod** command to configure the re-authentication interval.

Run the **no** form of this command to restore the default configuration.

The default re-authentication interval is **3600** seconds.

Syntax

dot1x timeout re-authperiod *interval*

no dot1x timeout re-authperiod

Parameter Description

interval: Re-authentication interval, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The default value is recommended.

Examples

The following example sets the re-authentication interval to 2,400 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x timeout re-authperiod 2400
```

Notifications

N/A

Platform Description

N/A

Related Commands

- **dot1x re-authentication**

1.48 dot1x timeout quiet-period

Function

Run the **dot1x timeout quiet-period** command to configure the quiet period after an authentication failure.

Run the **no** form of this command to restore the default configuration.

The default quiet period after an authentication failure is **10** seconds.

Syntax

dot1x timeout quiet-period *quiet-period*

no dot1x timeout quiet-period

Parameter Description

quiet-period: Quiet period after an authentication failure, in seconds. The value range is from 0 to 65535 and the value **0** indicates no quiet period.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The default value is recommended.

Examples

The following example sets the quiet period after an authentication failure to 60 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x timeout quiet-period 60
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.49 dot1x timeout supp-timeout

Function

Run the **dot1x timeout supp-timeout** command to configure the retransmission interval of Request/Challenge packets.

Run the **no** form of this command to restore the default configuration.

The default retransmission interval of Request/Challenge packets is **3** seconds.

Syntax

dot1x timeout supp-timeout *interval*

no dot1x timeout supp-timeout

Parameter Description

interval: Retransmission interval of Request/Challenge packets, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The default value is recommended.

Examples

The following example sets the retransmission interval of Request/Challenge packets to 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x timeout supp-timeout 10
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.50 dot1x timeout server-timeout

Function

Run the **dot1x timeout server-timeout** command to configure the server timeout duration.

Run the **no** form of this command to restore the default configuration.

The default server timeout duration is **5** seconds.

Syntax

dot1x timeout server-timeout *server-timeout*

no dot1x timeout server-timeout

Parameter Description

server-timeout: Server timeout time, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The server timeout duration of IEEE 802.1X must be greater than that of RADIUS.

The server timeout duration of IEEE 802.1X is smaller than that of RADIUS by default. Set the server timeout duration of RADIUS to a smaller value in actual application.

Examples

The following example sets the server timeout duration to 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x timeout server-timeout 10
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.51 dot1x timeout tx-period

Function

Run the **dot1x timeout tx-period** command to configure the retransmission interval of Request/Identity packets.

Run the **no** form of this command to restore the default configuration.

The default retransmission interval of Request/Identity packets is **3** seconds.

Syntax

dot1x timeout tx-period *interval*

no dot1x timeout tx-period

Parameter Description

interval: Retransmission interval of Request/Identity packets, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The default value is recommended.

Examples

The following example sets the retransmission interval of Request/Identity packets to 5 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x timeout tx-period 5
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.52 dot1x user-name compatible

Function

Run the **dot1x user-name compatible** command to enable the compatibility with H3C IEEE 802.1X authentication clients and authentication servers.

Run the **no** form of this command to disable this feature.

The compatibility with H3C 802.1X authentication clients and authentication servers is disabled by default.

Syntax

dot1x user-name compatible

no dot1x user-name compatible

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Configure this command when H3C authentication clients and authentication servers are used for IEEE 802.1X authentication.

Configure this command when H3C authentication servers are used for MAB.

Examples

The following example enables the compatibility with H3C IEEE 802.1X authentication clients and authentication servers.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x user-name compatible
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.53 dot1x valid-ip-acct enable

Function

Run the **dot1x valid-ip-acct enable** command to enable the function of initiating accounting after a user's IP address is obtained.

Run the **no** form of this command to disable this feature.

The function of initiating accounting after a user's IP address is obtained is disabled by default.

Syntax

dot1x valid-ip-acct enable

no dot1x valid-ip-acct enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is configured, clients do not initiate accounting immediately after passing authentication, but wait until they obtain IP addresses.

Configure this function when a server requires that accounting packets carry user IP addresses.

Examples

The following example enables the function of initiating accounting after a user's IP address is obtained.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x valid-ip-acct enable
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.54 dot1x valid-ip-acct timeout

Function

Run the **dot1x valid-ip-acct timeout** command to configure the timeout duration for an authenticated user to obtain an IP address.

Run the **no** form of this command to restore the default configuration.

The default timeout duration for an authenticated user to obtain an IP address is **5** minutes.

Syntax

dot1x valid-ip-acct timeout *timeout*

no dot1x valid-ip-acct timeout

Parameter Description

timeout: Allowed timeout duration for an authenticated user to obtain an IP address, in minutes. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the function of initiating accounting after a user's IP address is obtained, is enabled, a client may not initiate accounting within a long period of time due to the failure to obtain an IP address. For this, you can configure a timeout duration as required.

Examples

The following example sets the timeout duration for an authenticated user to obtain an IP address to 10 minutes.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# dot1x valid-ip-acct timeout 10
```

Notifications

N/A

Platform Description

N/A

Related Commands

- dot1x valid-ip-acct enable

1.55 dot1x system disable

Function

Run the **dot1x system disable** command to disable global IEEE 802.1X features.

Run the **no** form of this command to restore the default configuration.

Global IEEE 802.1X features are enabled by default.

Syntax

dot1x system disable

no dot1x system disable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Disable global IEEE 802.1X features when servers are unavailable. After global IEEE 802.1X features are disabled, users can access the Internet without authentication and authenticated users will be brought offline.

If global IEEE 802.1X features are enabled after server recovery, users on the controlled ports need to be authenticated before accessing the Internet.

Examples

The following example disables global IEEE 802.1X features.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# dot1x system disable
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.56 show dot1x

Function

Run the **show dot1x** command to display IEEE 802.1X protocol parameters.

Syntax

show dot1x

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays IEEE 802.1X protocol parameters.

```
Hostname> enable
Hostname# show dot1x
802.1X basic information:
  802.1X Status ......................... enable
  Authentication Mode ................... eap
  Authorization mode .................... disable
  Total User Number ..................... 0 (exclude dynamic user)
  Authenticated User Number ............. 0 (exclude dynamic user)
  Dynamic User Number ................... 0
  Re-authentication ..................... disable
  Re-authentication Period .............. 3600 seconds
  Re-authentication max ................. 3 times
  Quiet Period .......................... 10 seconds
  Tx Period ............................. 30 seconds
  Supplicant Timeout .................... 3 seconds
  Server Timeout ........................ 5 seconds
  Maximum Request ....................... 3 times
  Client Online Probe ................... disable
```

```
Eapol Tag ............................ enable
802.1x redirect ...................... disable
Private supplicant only ............... disable
```

Table 1-1Output Fields of the show dot1x Command

Field	Description
802.1X Status	Whether the IEEE 802.1X function is enabled
Authentication Mode	Authorization mode
Total User Number	Total number of authenticated users and users being authenticated
Authed User Number	Number of authenticated users
Dynamic User Number	Number of dynamic users in port mode
Re-authentication	Status of the re-authentication function
Re-authentication Period	Re-authentication period
Re-authentication max	Maximum number of re-authentication times
Quiet Period	Quiet period after an authentication failure
Tx Period	Retransmission interval of Request/Identity packets
Supplicant Timeout	Retransmission interval of Request/Challenge packets
Server Timeout	Server timeout duration
Maximum Request	Maximum request count
Client Online Probe	Status of online client detection
Eapol Tag	Whether EAPOL packets carry tags
802.1x redirect	Status of the 2nd-generation Orion Supplicant deployment function
Private supplicant only	Status of private client detection

Notifications

N/A

Platform Description

N/A

1.57 show dot1x auth-address-table

Function

Run the **show dot1x auth-address-table** command to display the list of hosts allowed for authentication.

Syntax

show dot1x auth-address-table [**address** *mac-address*] [**interface** *interface-type interface-number*]

Parameter Description

address *mac-address*: Specifies the MAC address of a client.

interface *interface-type interface-number*: Specifies the interface type and interface number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the list of hosts allowed for authentication.

```
Hostname> enable
Hostname# show dot1x auth-address-table
Interface        Address
---------------- -------------------
Gi0/1            00d0.f800.0c0e
Gi0/2            001a.c800.0102
Hostname# show dot1x auth-address-table interface fastEthernet 0/1
Interface        Address
---------------- -------------------
Gi0/1            00d0.f800.0c0e
Hostname# show dot1x auth-address-table address 00d0.f8.00.0c0e
Interface        Address
---------------- -------------------
Gi0/1            00d0.f800.0c0e
```

Table 1-1Output Fields of the show dot1x auth-address-table Command

Field	Description
Interface	Port
Address	MAC address of a host allowed for authentication

Notifications

N/A

Platform Description

N/A

1.58 show dot1x auto-req

Function

Run the **show dot1x auto-req** command to display active authentication status and parameters.

Syntax

show dot1x auto-req

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the active authentication status and parameters.

```
Hostname> enable
Hostname# show dot1x auto-req
Auto-Req: Enabled
User-Detect : Enabled
Packet-Num  : 0
Req-Interval: 30 Seconds
```

Table 1-1Output Fields of the show dot1x auto-req Command

Field	Description
Auto-Req	Status of the active authentication function
User-Detect	Status of the user detection function
Packet-Num	Number of active authentication request packets
Req-Interval	Transmission interval of active authentication packets

Notifications

N/A

Platform Description

N/A

1.59 show dot1x max-req

Function

Run the **show dot1x max-req** command to display the maximum retransmission count of Request/Challenge packets.

Syntax

show dot1x max-req

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the maximum retransmission count of Request/Challenge packets.

```
Hostname> enable
Hostname# show dot1x max-req
Max-Req: 3 Times
```

Table 1-1 Output Fields of the show dot1x max-req Command

Field	Description
Max-Req	Maximum retransmission count of Request/Challenge packets

Notifications

N/A

Platform Description

N/A

1.60 show dot1x port-control

Function

Run the **show dot1x port-control** command to display information about controlled ports.

Syntax

show dot1x port-control [**interface** *interface-type interface-numbe*r]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and interface number. Information about all controlled ports is displayed by default.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information about controlled ports.

```
Hostname> enable
Hostname# show dot1x port-control
Interface      Mode       Dynamic-User Static-User Max-User  Authened MAB
-------------- ---------- ------------ ----------- --------- -------- ---------
Gi0/5     mac-based  0            0           unlimited no       disable
```

Table 1-1Output Fields of show dot1x port-control Command

Field	Description
Interface	Name of a controlled port
Mode	Port mode
Dynamic-User	Number of dynamic users on the port
Static-User	Number of static users on the port
Max-User	Maximum number of users supported by the port
Authened	Whether the port passes authentication
MAB	Status of MAB configured on the port

Notifications

N/A

Platform Description

N/A

1.61 show dot1x private-supplicant-only

Function

Run the **show dot1x private-supplicant-only** command to display the status of the non-Orion client filtering function.

Syntax

show dot1x private-supplicant-only

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the status of the non-Orion client filtering function.

```
Hostname> enable
Hostname# show dot1x private-supplicant-only
private-supplicant-only: Disabled
```

Table 1-1 Output Fields of the show dot1x private-supplicant-only Command

Field	Description
private-supplicant-only	Status of the non-Orion client filtering function

Notifications

N/A

Platform Description

N/A

1.62 show dot1x probe-timer

Function

Run the **show dot1x probe-timer** command to display the client detection parameters.

Syntax

show dot1x probe-timer

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays client detection parameters.

```
Hostname> enable
Hostname# show dot1x probe-timer
Hello Interval    : 20
Hello Alive       : 60
```

Table 1-1Output Fields of the show dot1x probe-timer Command

Field	Description
Hello Interval	Detection interval
Hello Alive	Detection duration

Notifications

N/A

Platform Description

N/A

1.63 show dot1x re-authentication

Function

Run the **show dot1x re-authentication** command to display the status of the re-authentication function.

Syntax

show dot1x re-authentication

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the status of the re-authentication function.

```
Hostname> enable
Hostname# show dot1x re-authentication
Reauth-Enabled: Disabled
```

Table 1-1 Output Fields of the show dot1x re-authentication Command

Field	Description
Reauth-Enabled	Status of the re-authentication function

Notifications

N/A

Platform Description

N/A

1.64 show dot1x reauth-max

Function

Run the **show dot1x reauth-max** Command to display the maximum retransmission count of Request/Identity packets.

Syntax

show dot1x reauth-max

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the maximum retransmission count of Request/Identity packets.

```
Hostname> enable
Hostname# show dot1x reauth-max
Reauth-Max: 3 Times
```

Table 1-1Output Fields of the show dot1x reauth-max Command

Field	Description
Reauth-Max	Maximum retransmission count of Request/Identity packets

Notifications

N/A

Platform Description

N/A

1.65 show dot1x summary

Function

Run the **show dot1x summary** command to display entries of users participating in authentication.

Syntax

show dot1x summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can check user entries to figure out the current phase of a client (for example, being authenticated, authenticated, or quiet).

Examples

The following example displays entries of users participating in authentication.

```
Hostname> enable
Hostname# show dot1x summary
ID        Username                        MAC            Interface VLAN Auth-State
Backend-state Port-Status User-Type Time
--------- ------------------------------ -------------- --------- ----
--------------- ------------- ----------- --------- -----------------
```

Table 1-1Output Fields of the show dot1x summary Command

Field	Description
ID	ID obtained from AAA (You can run the **show aaa user all** command to check the ID.)
User	Username
MAC	MAC address of a client participating in authentication
Interface	Port, to which the client participating in authentication is connected
VLAN	ID of the VLAN, to which the client participating in authentication belongs
INNER-VLAN	ID of the inner VLAN, to which the client participating in authentication belongs. The device that supports dual tags of users participating in authentication supports this field.
Auth-State	Status of the authentication state machine
Backend-State	Status of the backend authentication state machine
Port-State	Port authentication status
User-Type	Authentication type
Time	Online duration

Notifications

N/A

Platform Description

N/A

Related Commands

- **show aaa user** (AAA)

1.66 show dot1x timeout quiet-period

Function

Run the **show dot1x timeout quiet-period** command to display the quiet period after an authentication failure.

Syntax

show dot1x timeout quiet-period

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the quiet period after an authentication failure.

```
Hostname> enable
Hostname# show dot1x timeout quiet-period
Quiet-Period: 10 Seconds
```

Table 1-1Output Fields of the show dot1x timeout quiet-period Command

Field	Description
Quiet-Period	Quiet period after an authentication failure

Notifications

N/A

Platform Description

N/A

1.67 show dot1x timeout re-authperiod

Function

Run the **show dot1x timeout re-authperiod** command to display the re-authentication interval.

Syntax

show dot1x timeout re-authperiod

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the re-authentication interval.

```
Hostname> enable
Hostname# show dot1x timeout re-authperiod
Reauth-Period: 3600 Seconds
```

Table 1-1Output Fields of the show dot1x timeout re-authperiod Command

Field	Description
Reauth-Period	Re-authentication interval

Notifications

N/A

Platform Description

N/A

1.68 show dot1x timeout server-timeout

Function

Run the **show dot1x timeout server-timeout** command to display the server timeout duration.

Syntax

show dot1x timeout server-timeout

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the server timeout duration.

```
Hostname> enable
Hostname# show dot1x timeout server-timeout
Server-Timeout: 5 Seconds
```

Table 1-1 Output Fields of the show dot1x timeout server-timeout Command

Field	Description
Server-Period	Server timeout duration

Notifications

N/A

Platform Description

N/A

1.69 show dot1x timeout supp-timeout

Function

Run the **show dot1x timeout supp-timeout** command to display the retransmission interval of Request/Challenge packets.

Syntax

show dot1x timeout supp-timeout

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the retransmission interval of Request/Challenge packets.

```
Hostname> enable
```

```
Hostname# show dot1x timeout supp-timeout
Supp-Timeout: 3 Seconds
```

Table 1-1Output Fields of the show dot1x timeout supp-timeout Command

Field	Description
Supp-Timeout	Retransmission interval of Request/Challenge packets

Notifications

N/A

Platform Description

N/A

1.70 show dot1x timeout tx-period

Function

Run the **show dot1x timeout tx-period** command to display the retransmission interval of Request/Identity packets.

Syntax

show dot1x timeout tx-period

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays retransmission interval of Request/Identity packets.

```
Hostname> enable
Hostname# show dot1x timeout tx-period
Tx-Period: 30 Seconds
```

Table 1-1Output Fields of the show dot1x timeout tx-period Command

Field	Description
Tx-Period	Retransmission interval of Request/Identity packets

Notifications

N/A

Platform Description

N/A

1.71 show dot1x user mac

Function

Run the **show dot1x user mac** command to display details about a user with a specified MAC address.

Syntax

show dot1x user mac *mac-address*

Parameter Description

mac-address: MAC address of a user. After this parameter is specified, details about the user are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

You can run the **show dot1x summary** command to obtain the user MAC address from the user summary.

Examples

The following example displays details about a user with the MAC address 0023.aeaa.4286.

```
Hostname> enable
Hostname# show dot1x user mac 0023.aeaa.4286
User name: ts-user
User id: 16777225
Type: static
Mac address is 0023.aeaa.4286
Vlan id is 2
Inner-VLAN id 5
Access from port Gi0/5
Time online: 0days 0h 0m17s
User ip address is 192.168.3.21
Max user number on this port is 0
```

```
Authorization session time is 1000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name ts-user_6_0_0 :
```

Table 1-1Output Fields of the show dot1x user mac Command

Field	Description
User name	Username
User id	User ID
Type	User type
Mac address	MAC address of a user
Vlan id	User VLAN ID
Inner-VLAN id	ID of the inner VLAN, to which the client participating in authentication belongs. The device that supports dual tags of users participating in authentication supports this field.
Access from port	User port
Time online	Online duration
User ip address	IP address of a user
Max user number on this port	Maximum number of users supported by the port
Authorization session time	Authorization time of the user
Supplicant is private	Whether the user client is a Orion client
Start accounting	Whether accounting is started for the user
Permit proxy user	Whether the user is allowed to act as a proxy
Permit dial user	Whether the user is allowed to perform dialup
IP privilege	IP privilege level of the user
user acl-name	ACL delivered to the user

Notifications

N/A

Platform Description

N/A

1.72 show dot1x user name

Function

Run the **show dot1x user name** command to display details about a user with a specified username.

Syntax

show dot1x user name *user-name*

Parameter Description

user-name: Username. After this parameter is specified, details about a user with the username are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

After running the **show dot1x summary** command to display the user summary, you can run this command to display details about a user.

Examples

The following example displays details about a user with the username **ts-user**.

```
Hostname> enable
Hostname# show dot1x user name ts-user
User name: ts-user
User id: 16777225
Type: static
Mac address is 0023.aeaa.4286
Vlan id is 2
Inner-VLAN id 5Access from port Gi0/5
Time online: 0days 0h 0m17s
User ip address is 192.168.3.21
Max user number on this port is 0
Authorization session time is 1000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name ts-user_6_0_0 :
```

Table 1-1Output Fields of the show dot1x user name Command

Field	Description
User name	Username
User id	User ID
Type	User type
Mac address	MAC address of a user
Vlan id	User VLAN ID
Inner-VLAN id	ID of the inner VLAN, to which the client participating in authentication belongs. The device that supports dual tags of users participating in authentication supports this field.
Access from port	User port
Time online	Online duration
User ip address	IP address of a user
Max user number on this port	Maximum number of users supported by the port
Authorization session time	Authorization time of the user
Supplicant is private	Whether the user client is a Orion client
Start accounting	Whether accounting is started for the user
Permit proxy user	Whether the user is allowed to act as a proxy
Permit dial user	Whether the user is allowed to perform dialup
IP privilege	IP privilege level of the user
user acl-name	ACL delivered to the user

Notifications

N/A

Platform Description

N/A