802-1x Commands

This chapter contains the following sections:

aaa authentication dot1x

To specify which servers are used for authentication when 802.1X authentication is enabled, use the **aaa authentication dot1x** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

aaa authentication dot1x default {**radius** | **none** | {**radius none**}}

no aaa authentication dot1x default

Parameters

- **radius** - Uses the list of all RADIUS servers for authentication
- **none** - Uses no authentication

Default Configuration

RADIUS server.

Command Mode

Global Configuration mode

User Guidelines

You can select either authentication by a RADIUS server, no authentication (**none**), or both methods.

If you require that authentication succeeds even if no RADIUS server response was received, specify **none** as the final method in the command line.

Example

The following example sets the 802.1X authentication mode to RADIUS server authentication. Even if no response was received, authentication succeeds.

```
switchxxxxxx(config)# aaa authentication dot1x default radius none
```

authentication open

To enable open access (monitoring mode) on this port, use the **authentication open** command in Interface Configuration mode. To disable open access on this port, use the **no** form of this command.

Syntax

authentication open

no authentication open

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

Open Access or Monitoring mode allows clients or devices to gain network access before authentication is performed. In the mode the switch performs failure replies received from a Radius server as success.

Example

The following example enables open mode on interface gi1/0/1:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# authentication open
```

clear dot1x statistics

To clear 802.1X statistics, use the **clear dot1x statistics** command in Privileged EXEC mode.

Syntax

clear dot1x statistics [*interface-id*]

Parameters

- ***interface-id***—Specify an Ethernet port ID.

Default Configuration

Statistics on all ports are cleared.

Command Mode

Privileged EXEC mode

User Guidelines

This command clears all the counters displayed in the **show dot1x** and **show dot1x statistics** command.

Example

```
switchxxxxxx# clear dot1x statistics
```

data

To specify web-based page customizing, the **data** command is used in Web-Based Page Customization Configuration mode.

Syntax

data *value*

Parameters

- ***value***—String of hexadecimal digit characters up to 320 characters.

Default Configuration

No user customization.

Command Mode

Web-Based Page Customization Configuration mode

User Guidelines

The command should not be entered or edited manually (unless using copy-paste). It is a part of the configuration file produced by the switch.

A user can only customize the web-based authentication pages by using the WEB interface.

Example 1—The following example shows a partial web-based page customization configuration:

```
switchxxxxxx(config)# dot1x page customization
switchxxxxxx(config-web-page)# data 1feabcde
switchxxxxxx(config-web-page)# data 17645874
switchxxxxxx(config-web-page)# exit
```

Example 2—The following example shows how Web-Based Page customization is displayed when running the **show running-config** command:

```
switchxxxxxx# show running-config
dot1x page customization
data ********
exit
```

description 802.1x

To specify a description for an 802.1X credential structure, use the **description** command in Dot1x credentials configuration mode. To remove the description, use the **no** form of this command.

Syntax

description *text*

no description

Parameters

- ***text***—Text description. The description can be up to 80 characters.

Default Configuration

A description is not specified.

Command Mode

Dot1x credentials configuration mode

User Guidelines

An 802.1X credential structure is necessary when configuring the switch as a supplicant (client). This credentials structure must contain a username and password and may contain a description.

Example

The following example configures an 802.1X credential structure:

```
switchxxxxxx(config)# dot1x credentials site-A
switchxxxxxx(config-dot1x-cred)# username inner-switch
switchxxxxxx(config-dot1x-cred)# password 6f3c576n8
switchxxxxxx(config-dot1x-cred)# description This credentials profile should be used to
connected to site-A
```

dot1x auth-not-req

To enable unauthorized devices access to a VLAN, use the **dot1x auth-not-req** command in Interface (VLAN) Configuration mode. To disable access to a VLAN, use the **no** form of this command.

Syntax

dot1x auth-not-req

no dot1x auth-not-req

Default Configuration

Access is enabled.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

The guest VLAN cannot be configured as unauthorized VLAN.

Example

The following example enables unauthorized devices access to VLAN 5.

```
switchxxxxxx(config)# interface vlan 5
switchxxxxxx(config-if)# dot1x auth-not-req
```

dot1x authentication

To enable authentication methods on a port, use the **dot1x authentication** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x authentication [**802.1x**] [**mac**] [**web**]

no dot1x authentication

Parameters

- **802.1x**—Enables authentication based on 802.1X (802.1X-based authentication).
- **mac**—Enables authentication based on the station's MAC address (MAC-Based authentication).
- **web**—Enables WEB-Based authentication.

Default Configuration

802.1X-Based authentication is enabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

Static MAC addresses cannot be authorized by the MAC-based method.

It is not recommended to change a dynamic MAC address to a static one or delete it if the MAC address was authorized by the MAC-based authentication:

1. If a dynamic MAC address authenticated by MAC-based authentication is changed to a static one, it will not be manually re-authenticated.
2. Removing a dynamic MAC address authenticated by the MAC-based authentication causes its re-authentication.

802.1x enabled on a port associated with a port channel has the following limitations:

- Only the 802.1X-based authentication is supported.
- Only the multi-host (legacy 802.1x mode) mode is supported.

Example

The following example enables authentication based on 802.1x and the station’s MAC address on port gi1/0/1:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x authentication 802.1x mac
```

dot1x credentials

To define the name of an 802.1X credential structure and enter the Dot1x credentials configuration mode, use the **dot1x credentials** command in Global Configuration mode. To remove the credential structure, use the **no** form of this command.

Syntax

dot1x credentials *name*

no dot1x credentials *name*

Parameters

- ***name***—The credential structure name up to 32 characters.

Default Configuration

A credentials structure is not specified

Command Mode

Global Configuration mode

User Guidelines

Use the **dot1x credentials** command to start configuration of credential structure. The credential structure contains the parameters of supplicant (client) and it is used during the 802.1X supplicant enabling on interface.

The credential configuration takes a place only after exit from the credential context.

Changing configuration of used credential causes supplicant logoff and logon.

The switch supports up to 24 credentials.

Use the **no dot1x credentials** command, to delete a credential. A used credential cannot be deleted.

Example

The following example configures an 802.1X credential structure:

```
switchxxxxxx(config)# dot1x credentials site-A
switchxxxxxx(config-dot1x-cred)# username inner-switch
switchxxxxxx(config-dot1x-cred)# password agrcx5642
switchxxxxxx(config-dot1x-cred)# description This credentials profile should be used to
connected to site-A
```

dot1x eap-max-retrans

To set the EAP maximum number retransmissions, use the **dot1x eap-max-retrans** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x eap-max-retrans *count*

no dot1x eap-max-retrans

Parameters

- ***count***—Specifies the maximum number of times that the EAP Server (EAP Authenticator) retransmits an EAP request when no response from a EAP client (EAP Peer) was received. (Range: 1–10).

Default Configuration

The default maximum number of attempts is 2.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The parameter is used by the 802.1x Supplicant.

Example

The following example sets the EAP maximum number retransmissions to 6:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x eap-max-retrans 6
```

dot1x guest-vlan

To define a guest VLAN, use the **dot1x guest-vlan** mode command in Interface (VLAN) Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x guest-vlan

no dot1x guest-vlan

Default Configuration

No VLAN is defined as a guest VLAN.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

A device can have only one global guest VLAN.

The guest VLAN must be a static VLAN and it cannot be removed.

An unauthorized VLAN cannot be configured as guest VLAN.

Example

The following example defines VLAN 2 as a guest VLAN.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# dot1x guest-vlan
```

dot1x guest-vlan enable

To enable unauthorized users on the access interface to the guest VLAN, use the **dot1x guest-vlan enable** command in Interface Configuration mode. To disable access, use the **no** form of this command.

Syntax

dot1x guest-vlan enable

no dot1x guest-vlan enable

Default Configuration

The default configuration is disabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The guest VLAN and the WEB-Based authentication cannot be configured on a port at the same time.

This command cannot be configured if the monitoring VLAN is enabled on the interface.

If the port does not belong to the guest VLAN it is added to the guest VLAN as an egress untagged port.

If the authentication mode is single-host or multi-host, the value of PVID is set to the guest VLAN_ID.

If the authentication mode is multi-sessions mode, the PVID is not changed and all untagged traffic and tagged traffic not belonging to the unauthenticated VLANs from unauthorized hosts are mapped to the guest VLAN.

If 802.1X is disabled, the port static configuration is reset.

Example

The following example enables unauthorized users on gi1/0/1 to access the guest VLAN.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x guest-vlan enable
```

dot1x guest-vlan timeout

To set the time delay between enabling 802.1X (or port up) and adding a port to the guest VLAN, use the **dot1x guest-vlan timeout** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x guest-vlan timeout *timeout*

no dot1x guest-vlan timeout

Parameters

- ***timeout***—Specifies the time delay in seconds between enabling 802.1X (or port up) and adding the port to the guest VLAN. (Range: 30–180).

Default Configuration

The guest VLAN is applied immediately.

Command Mode

Global Configuration mode

User Guidelines

This command is relevant if the guest VLAN is enabled on the port. Configuring the timeout adds a delay from enabling 802.1X (or port up) to the time the device adds the port to the guest VLAN.

Example

The following example sets the delay between enabling 802.1X and adding a port to a guest VLAN to 60 seconds.

```
switchxxxxxx(config)# dot1x guest-vlan timeout 60
```

dot1x host-mode

To allow a single host (client) or multiple hosts on an IEEE 802.1X-authorized port, use the **dot1x host-mode** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x host-mode {multi-host | **single-host** | **multi-sessions**}

Parameters

- **multi-host**—Enable multiple-hosts mode.
- **single-host**—Enable single-hosts mode.
- **multi-sessions**—Enable multiple-sessions mode.

Default Configuration

Default mode is multi-host.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

Single-Host Mode

The single-host mode manages the authentication status of the port: the port is authorized if there is an authorized host. In this mode, only a single host can be authorized on the port.

When a port is unauthorized and the guest VLAN is enabled, untagged traffic is remapped to the guest VLAN. Tagged traffic is dropped unless the VLAN tag is the guest VLAN or the unauthenticated VLANs. If guest VLAN is not enabled on the port, only tagged traffic belonging to the unauthenticated VLANs is bridged.

When a port is authorized, untagged and tagged traffic from the authorized host is bridged based on the static vlan membership configured at the port. Traffic from other hosts is dropped.

A user can specify that untagged traffic from the authorized host will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process. In this case, tagged traffic is dropped unless the VLAN tag is the RADIUS-assigned VLAN or the unauthenticated VLANs.

The switch removes from FDB all MAC addresses learned on a port when its authentication status is changed from authorized to unauthorized.

Multi-Host Mode

The multi-host mode manages the authentication status of the port: the port is authorized after at least one host is authorized.

When a port is unauthorized and the guest VLAN is enabled, untagged traffic is remapped to the guest VLAN. Tagged traffic is dropped unless the VLAN tag is the guest VLAN or the unauthenticated VLANs. If guest VLAN is not enabled on the port, only tagged traffic belonging to the unauthenticated VLANs is bridged.

When a port is authorized, untagged and tagged traffic from all hosts connected to the port is bridged based on the static vlan membership configured at the port.

A user can specify that untagged traffic from the authorized port will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process. In this case, tagged traffic is dropped unless the VLAN tag is the RADIUS assigned VLAN or the unauthenticated VLANs.

The switch removes from FDB all MAC addresses learned on a port when its authentication status is changed from authorized to unauthorized.

Multi-Sessions Mode

Unlike the single-host and multi-host modes (port-based modes) the multi-sessions mode manages the authentication status for each host connected to the port (session-based mode). If the multi-sessions mode is configured on a port the port does have any authentication status. Any number of hosts can be authorized on the port. The command can limit the maximum number of authorized hosts allowed on the port.

Each authorized client requires a TCAM rule. If there is no available space in the TCAM, the authentication is rejected.

When using the **dot1x host-mode** command to change the port mode to **single-host** or **multi-host** when authentication is enabled, the port state is set to unauthorized.

If the **dot1x host-mode** command changes the port mode to **multi-session** when authentication is enabled, the state of all attached hosts is set to unauthorized.

To change the port mode to single-host or multi-host, set the port (**dot1x port-control**) to force-unauthorized, change the port mode to single-host or multi-host, and set the port to authorization auto.

Tagged traffic belonging to the unauthenticated VLANs is always bridged regardless if a host is authorized or not.

When the guest VLAN is enabled, untagged and tagged traffic from unauthorized hosts not belonging to the unauthenticated VLANs is bridged via the guest VLAN.

Traffic from an authorized hosts is bridged in accordance with the port static configuration. A user can specify that untagged and tagged traffic from the authorized host not belonging to the unauthenticated VLANs will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process.

The switch does not remove from FDB the host MAC address learned on the port when its authentication status is changed from authorized to unauthorized. The MAC address will be removed after the aging timeout expires.

802.1x enabled on a port associated with a port channel has the following limitations:

- Only the 802.1X-based authentication is supported.
- Only the multi-host (legacy 802.1x mode) mode is supported.

Example

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x host-mode multi-host
```

dot1x mac-auth

To specify a type (EAP or Radius), and MAC based username format, that MAC-Based authentication will use, use the **dot1x mac-auth** command in Global Configuration mode. To reset the default configuration, use the **no** form of the command.

Syntax

dot1x mac-auth {**eap** | **radius**} [**username groupsize** {**1**|**2**|**4**|**12**} **separator** {**-** | **:** |**.**} [**lowercase** | **uppercase**]]

no dot1x mac-auth

Parameters

- **eap**—Specifies that the EAP MD5-Challenge authentication is used.
- **radius**—Specifies that only Radius (without EAP) authentication with the Service-Type attribute equals to Call-Check(10) is used.
- **username**—Specifies the format of the username. If the keyword is not configured the format without separator with the lower case is applied.

username groupsize 12 separator - lowercase

- **groupsize**—Specifies the numbers of ASCII characters between delimiters.
- **separator**—Specifies the delimiter.
- **lowercase**—Specifies that the username is coded in the lower case. The argument is applied if the case argument is not configured.
- **uppercase**—Specifies that the username is coded in the upper case.

Default Configuration

EAP MD5-Challenge Authentication

Command Mode

Global Configuration mode

User Guidelines

The switch supports the following two types of MAC-Based authentication with the host MAC address as user name and password :

- EAP MD5-Challenge authentication.
- Pure Radius authentication with the Service-Type attribute equals to Call-Check(10) and with username and password in the ASCII format.

Use the **eap** keyword, to specify the EAP MD5-Challenge authentication type.

Use the **radius** keyword, to specify the pure Radius authentication type. The pure Radius authentication uses the following Radius attributes:

- User-Name: Host MAC address
- Password
- Service-Type: Call-Check(10)
- Frame-MTU
- Called-Station-Id: MAC address of the switch
- Calling-Station-Id: MAC address of the host
- Message-Authentication
- NAS-Port-Type: Ethernet(15)
- NAS-Port: ifIndex of the port where the host is connected to
- NAS-Port-Id: full CLI name of the port where the host is connected to (for example: GigabitEthernet2/0/2)
- NAS-IP-Address: IP address of the switch

Use the **username** keyword, to specify the format of the Username attributes. The following table gives examples of the Username coding for MAC address 08002b8619de:

Table 1: Examples of Username coding

Size	Separator	Username
1	-	0-8-0-0-2-b-8-6-1-9-d-e
2	:	08:00:2b:86:19:de
4	.	0800.2b86.19de
12	N/A	08002b8619de

Changing of the username format or the authentication type (EAP or Radius) causes reauthentication.

Example 1. The following example specifies that MAC-Based authentication will use the pure Radius authentication and specifies the attributes to use in username based on the station's MAC address:

switchxxxxxx(config)# dot1x mac-auth radius username groupsize 2 separator : uppercase

Example 2. The following example specifies that MAC-Based authentication will use the EAP MD5-Challenge authentication. The username format will be set to format without separator ,with lower case:

```
switchxxxxxx(config)# dot1x mac-auth eap
```

dot1x mac-auth password

To specify a global password for MAC-Based authentication, use the **dot1x mac-auth password** command in Global Configuration mode. To remove the password, use the **no** form of this command.

Syntax

encrypted dot1x mac-auth password *encrypted-password*

dot1x mac-auth password *password*

no dot1x mac-auth password

Parameters

- ***encrypted-password***—The password in encrypted format.
- ***password***—The password up to 32 characters.

Default Configuration

Username.

Command Mode

Global Configuration mode

User Guidelines

Use the command, to specify a password that will be used for MAC-Based authentication instead of the host MAC address.

Changing of the password or its format causes reauthentication.

Example

The following example configures a global password for MAC-Based authentication:

```
switchxxxxxx(config)# dot1x mac-auth password 87b$#9hv5*
```

dot1x max-hosts

To configure the maximum number of authorized hosts allowed on the interface, use the **dot1x max-hosts** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x max-hosts *count*

no dot1x max-hosts

Parameters

- ***count***—Specifies the maximum number of authorized hosts allowed on the interface. May be any 32 bits positive number.

Default Configuration

No limitation.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

By default, the number of authorized hosts allowed on an interface is not limited. To limit the number of authorized hosts allowed on an interface, use the **dot1x max-hosts** command.

This command is relevant only for multi-session mode.

Example

The following example limits the maximum number of authorized hosts on Ethernet port gi1/0/1 to 6:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x max-hosts 6
```

dot1x max-login-attempts

To set the maximum number of allowed login attempts, use the **dot1x max-login-attempts** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x max-login-attempts *count*

no dot1x max-login-attempts

Parameters

- ***count***—Specifies the maximum number of allowed login attempts. A value of 0 means an infinite numbers of attempts. The valid range is 3-10.

Default Configuration

Unlimited.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

By default, the switch does not limit the number of failed login attempts. To specify the number of allowed fail login attempts, use this command.

The command is applied only to the Web-based authentication.

Example

The following example sets maximum number of allowed login attempts to 5:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x max-login-attempts 5
```

dot1x max-req

To set the maximum number of times that the device sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client before restarting the authentication process, use the **dot1x max-req** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x max-req *count*

no dot1x max-req

Parameters

- ***count***—Specifies the maximum number of times that the device sends an EAP request/identity frame before restarting the authentication process. (Range: 1–10).

Default Configuration

The default maximum number of attempts is 2.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example

The following example sets the maximum number of times that the device sends an EAP request/identity frame to 6.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x max-req 6
```

dot1x page customization

To enter Web-Based Page Customization Configuration mode, use the **dot1x page customization** command in Global Configuration mode.

Syntax

dot1x page customization

Default Configuration

No user customization.

Command Mode

Global Configuration mode

User Guidelines

The command should not be entered or edited manually (unless when using copy-paste). It is a part of the configuration file produced by the switch.

A user must customize the web-based authentication pages by using the browser Interface.

Example

The following example shows part of a web-based page customization configuration:

```
switchxxxxxx(config)# dot1x page customization
switchxxxxxx(config-web-page)# data 1feabcde
switchxxxxxx(config-web-page)# data 17645874
switchxxxxxx(config-web-page)# exit
```

dot1x port-control

To enable manual control of the port authorization state, use the **dot1x port-control** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x port-control {auto | **force-authorized** | **force-unauthorized**} [**time-range** *time-range-name*]

no dot1x port-control

Parameters

- **auto**—Enables 802.1X authentication on the port and causes it to transition to the authorized or unauthorized state, based on the 802.1X authentication exchange between the device and the client.

Note All ingress and egress traffic will be dropped.

- **force-authorized**—Disables 802.1X authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port sends and receives traffic without 802.1X-based client authentication.
- **force-unauthorized**—Denies all access through this port by forcing it to transition to the unauthorized state and ignoring all attempts by the client to authenticate. The device cannot provide authentication services to the client through this port.
- **time-range** *time-range-name*—Specifies a time range. When the Time Range is not in effect, the port state is Unauthorized. (Range: 1-32 characters).

Default Configuration

The port is in the force-authorized state.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

802.1X authentication cannot be enabled on an interface if port security feature is already enabled on the same interface.

The switch removes all MAC addresses learned on a port when its authorization control is changed from **force-authorized** to another.

Note It is recommended to disable spanning tree or to enable spanning-tree PortFast mode on 802.1X edge ports in **auto** state that are connected to end stations, in order to proceed to the forwarding state immediately after successful authentication.

Example

The following example sets 802.1X authentication on gi1/0/1 to auto mode.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x port-control auto
```

dot1x radius-attributes vlan

To enable RADIUS-based VLAN assignment, use the **dot1x radius-attributes vlan** command in Interface Configuration mode. To disable RADIUS-based VLAN assignment, use the **no** form of this command.

Syntax

dot1x radius-attributes vlan [**reject** | **static**]

no dot1x radius-attributes vlan

Parameters

- **reject**—If the RADIUS server authorized the supplicant, but did not provide a supplicant VLAN the supplicant is rejected. If the parameter is omitted, this option is applied by default.
- **static**—If the RADIUS server authorized the supplicant, but did not provide a supplicant VLAN, the supplicant is accepted.

Default Configuration

reject

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

If RADIUS provides invalid VLAN information, the authentication is rejected.

If a RADIUS server assigns a client with a non-existing VLAN, the switch creates the VLAN. The VLAN is removed when it is no longer being used.

If RADIUS provides valid VLAN information and the port does not belong to the VLAN received from RADIUS, it is added to the VLAN as an egress untagged port. When the last authorized client assigned to the VLAN becomes unauthorized or 802.1x is disabled on the port, the port is excluded from the VLAN.

If the authentication mode is single-host or multi-host, the value of PVID is set to the VLAN_ID.

If an authorized port in the single-host or multi-host mode changes its status to unauthorized, the port static configuration is reset.

If the authentication mode is multi-sessions mode, the PVID is not changed and all untagged traffic and tagged traffic not belonging to the unauthenticated VLANs are mapped to the VLAN using TCAM.

If the last authorized host assigned to a VLAN received from RADIUS connected to a port in the multi-sessions mode changes its status to unauthorized, the port is removed from the VLAN if it is not in the static configuration.

See the User Guidelines of the **dot1x host-mode** command for more information.

If 802.1X is disabled the port static configuration is reset.

If the **reject** keyword is configured and the RADIUS server authorizes the host but the RADIUS accept message does not assign a VLAN to the supplicant, authentication is rejected.

If the **static** keyword is configured and the RADIUS server authorizes the host then even though the RADIUS accept message does not assign a VLAN to the supplicant, authentication is accepted and the traffic from the host is bridged in accordance with port static configuration.

If this command is used when there are authorized ports/hosts, it takes effect at subsequent authentications. To manually re-authenticate, use the **dot1x re-authenticate** command.

Example 1. This example enables user-based VLAN assignment. If the RADIUS server authorized the supplicant, but did not provide a supplicant VLAN, the supplicant is rejected.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x radius-attributes vlan
switchxxxxxx(config-if)# exit
```

Example 2. This example enables user-based VLAN assignment. If the RADIUS server authorized the supplicant but did not provide a supplicant VLAN, the supplicant is accepted and the static VLAN configurations is used.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x radius-attributes static
switchxxxxxx(config-if)# exit
```

dot1x re-authenticate

To initiate manually re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port, use the **dot1x re-authenticate** command in Privileged EXEC mode.

Syntax

dot1x re-authenticate [*interface-id*]

Parameters

- ***interface-id***—Specifies an Ethernet port or OOB port.

Default Configuration

If no port is specified, command is applied to all ports.

Command Mode

Privileged EXEC mode

Example

The following command manually initiates re-authentication of 802.1X-enabled gi1/0/1:

```
switchxxxxxx# dot1x re-authenticate gi1/0/1
```

dot1x reauthentication

To enable periodic re-authentication of the client, use the **dot1x reauthentication** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x reauthentication

no dot1x reauthentication

Default Configuration

Periodic re-authentication is disabled.

Command Mode

Interface (Ethernet, OOB) Configuration mode

Example

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x reauthentication
```

dot1x supplicant

To enable the dot1x supplicant role for a given interface, use the **dot1x supplicant** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x supplicant *name*

no dot1x supplicant

Parameters

- ***name***—The name of the credential structure applied on the interface.

Default Configuration

The supplicant role is disabled.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

Use the **dot1x supplicant** command to enable the dot1x supplicant on a given interface. When the supplicant is enabled on an interface the interface becomes an unauthorized. When the 802.1X authentication successes the interface state is changed to authorized.

If the *name* argument specifies an undefined or not fully defined (password or username is not configured) 802.1X credential structure, the command is rejected.

Authenticator and Supplicant cannot be enabled together on the same interface.

The command cannot be configured a few times on the same port. To replace the configured credential, use the **no** form of the command before configuration a new credential.

Unlike unauthorized authenticator interface an unauthorized supplicant interface does not limit any traffic passed through.

The following events start the 802.1X supplicant authentication on a port:

- The **dot1x supplicant** command enables the supplicant on the port in the UP status.
- The status of the port is changed to UP and the supplicant is enabled on the port.
- The EAP Identifier Request message is received on the port and the supplicant is enabled on the port.

Example

The following example configures an 802.1X supplicant on port gi1/0/1:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x supplicant upstream-port
```

dot1x supplicant traps authentication failure

To enable sending traps when an 802.1X supplicant authentication fails, use the **dot1x supplicant traps authentication failure** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x supplicant traps authentication failure

no dot1x supplicant traps authentication failure

Default Configuration

Traps are disabled.

Command Mode

Global Configuration mode

User Guidelines

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

Example

The following example enables sending traps when an 802.1X supplicant authentication failed:

```
switchxxxxxx(config)# dot1x supplicant traps authentication failure
```

dot1x supplicant traps authentication success

To enable sending traps when an 802.1X supplicant authentication is succeeded, use the **dot1x supplicant traps authentication success** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x supplicant traps authentication success

no dot1x supplicant traps authentication success

Default Configuration

Traps are disabled.

Command Mode

Global Configuration mode

User Guidelines

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

Example

The following example enables sending traps when an 802.1X supplicant authentication is succeeded:

```
switchxxxxxx(config)# dot1x supplicant traps authentication success
```

dot1x system-auth-control

To enable 802.1X globally, use the **dot1x system-auth-control** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x system-auth-control

no dot1x system-auth-control

Default Configuration

Disabled.

Command Mode

Global Configuration mode

Example

The following example enables 802.1X globally.

```
switchxxxxxx(config)# dot1x system-auth-control
```

dot1x timeout eap-timeout

To set the EAP timeout, use the **dot1x timeout eap-timeout** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x timeout eap-timeout *seconds*

no dot1x timeout eap-timeout

Parameters

- ***seconds***—Specifies the time interval in seconds during which the EAP Server (EAP Authenticator) waits for a response from the EAP client (EAP Peer) before the request retransmission. (Range: 1–65535 seconds).

Default Configuration

The default timeout period is 30 seconds.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The parameter is used by the 802.1x Supplicant.

Example

The following example sets the EAP timeout to 45 seconds.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout eap-timeout 45
```

dot1x timeout quiet-period

To set the time interval that the device remains in a quiet state following a failed authentication exchange, use the **dot1x timeout quiet-period** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

Parameters

- ***seconds***—Specifies the time interval in seconds that the device remains in a quiet state following a failed authentication exchange with a client. (Range: 10–65535 seconds).

Default Configuration

The default quiet period is 60 seconds.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

During the quiet period, the device does not accept or initiate authentication requests.

The default value of this command should only be changed to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

To provide faster response time to the user, a smaller number than the default value should be entered.

For 802.1x and MAC-based authentication, the number of failed logins is 1.

For WEB-based authentication, the quiet period is applied after a number of failed attempts.

For 802.1x-based and MAC-based authentication methods, the quiet period is applied after each failed attempt.

Example

The following example sets the time interval that the device remains in the quiet state following a failed authentication exchange to 120 seconds.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout quiet-period 120
```

dot1x timeout reauth-period

To set the number of seconds between re-authentication attempts, use the **dot1x timeout reauth-period** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x timeout reauth-period seconds

no dot1x timeout reauth-period

Parameters

- **reauth-period** seconds—Number of seconds between re-authentication attempts. (Range: 300-4294967295).

Default Configuration

3600

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

The command is only applied to the 802.1x authentication method.

Example

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout reauth-period 5000
```

dot1x timeout server-timeout

To set the time interval during which the device waits for a response from the authentication server, use the **dot1x timeout server-timeout** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

Parameters

- **server-timeout** *seconds*—Specifies the time interval in seconds during which the device waits for a response from the authentication server. (Range: 1–65535 seconds).

Default Configuration

The default timeout period is 30 seconds.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

The actual timeout period can be determined by comparing the value specified by this command to the result of multiplying the number of retries specified by the radius-server retransmit command by the timeout period specified by the radius-server transmit command, and selecting the lower of the two values.

Example

The following example sets the time interval between retransmission of packets to the authentication server to 3600 seconds.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout server-timeout 3600
```

dot1x timeout silence-period

To set the authentication silence time, use the **dot1x timeout silence-period** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x timeout silence-period *seconds*

no dot1x timeout silence-period

Parameters

- ***seconds***—Specifies the silence interval in seconds. The valid range is 60 - 65535.

Default Configuration

The silence period is not limited.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The silence time is the number of seconds that if an authorized client does not send traffic during this period, the client is changed to unauthorized.

If an authorized client does not send traffic during the silence period specified by the command, the state of the client is changed to unauthorized.

The command is only applied to WEB-based authentication.

Example

The following example sets the authentication silence time to 100 seconds:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout silence-period 100
```

dot1x timeout supp-timeout

To set the time interval during which the device waits for a response to an Extensible Authentication Protocol (EAP) request frame from the client before resending the request, use the **dot1x timeout supp-timeout** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

Parameters

- **supp-timeout** *seconds*—Specifies the time interval in seconds during which the device waits for a response to an EAP request frame from the client before resending the request. (Range: 1–65535 seconds).

Default Configuration

The default timeout period is 30 seconds.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The command is only applied to the 802.1x authentication method.

Example

The following example sets the time interval during which the device waits for a response to an EAP request frame from the client before resending the request to 3600 seconds.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout supp-timeout 3600
```

dot1x timeout supplicant-held-period

To set the time period during which the supplicant waits before restarting authentication after receiving the FAIL response from the Radius server, use the **dot1x timeout supplicant-held-period** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command

Syntax

dot1x timeout supplicant-held-period *seconds*

no dot1x timeout supplicant-held-period

Parameters

- ***seconds***—Specifies the time period during which the supplicant waits before restarting authentication after receiving the FAIL response from the Radius server. (Range: 1–65535 seconds).

Default Configuration

The default timeout period is 60 seconds.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example

The following example sets the time period during which the supplicant waits before restarting authentication after receiving the FAIL response from the Radius server to 70 seconds.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout supplicant-held-period 70
```

dot1x timeout tx-period

To set the time interval during which the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the client before resending the request, use the **dot1x timeout tx-period** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

Parameters

- ***seconds***—Specifies the time interval in seconds during which the device waits for a response to an EAP-request/identity frame from the client before resending the request. (Range: 30–65535 seconds).

Default Configuration

The default timeout period is 30 seconds.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The command is only applied to the 802.1x authentication method.

Example

The following command sets the time interval during which the device waits for a response to an EAP request/identity frame to 60 seconds.

```
switchxxxxxx(config)# interface gi1/0/1:
switchxxxxxx(config-if)# dot1x timeout tx-period 60
```

dot1x traps authentication failure

To enable sending traps when an 802.1X authentication method failed, use the **dot1x traps authentication failure** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x traps authentication failure {[**802.1x**] [**mac**] [**web**]}

no dot1x traps authentication failure

Parameters

- **802.1x**—Enables traps for 802.1X-based authentication.
- **mac**—Enables traps for MAC-based authentication.
- **web**—Enables traps for WEB-based authentication.

Default Configuration

All traps are disabled.

Command Mode

Global Configuration mode

User Guidelines

Any combination of the keywords are allowed. At least one keyword must be configured.

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

Example

The following example enables sending traps when a MAC address fails to be authorized by the 802.1X mac-authentication access control.

```
switchxxxxxx(config)# dot1x traps authentication failure 802.1x
```

dot1x traps authentication quiet

To enable sending traps when a host state is set to the quiet state after failing the maximum sequential attempts of login, use the **dot1x traps authentication quiet** command in Global Configuration mode. To disable the traps, use the **no** form of this command.

Syntax

dot1x traps authentication quiet

no dot1x traps authentication quiet

Default Configuration

Quiet traps are disabled.

Command Mode

Global Configuration mode

User Guidelines

The traps are sent after the client is set to the quiet state after the maximum sequential attempts of login.

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

Example

The following example enables sending traps when a host is set in the quiet state:

```
switchxxxxxx(config)# dot1x traps authentication quiet
```

dot1x traps authentication success

To enable sending traps when a host is successfully authorized by an 802.1X authentication method, use the **dot1x traps authentication success** command in Global Configuration mode. To disable the traps, use the **no** form of this command.

Syntax

dot1x traps authentication success {[**802.1x**] [**mac**] [**web**]}

no dot1x traps authentication success

Parameters

- **802.1x**—Enables traps for 802.1X-based authentication.
- **mac**—Enables traps for MAC-based authentication.
- **web**—Enables traps for WEB-based authentication.

Default Configuration

Success traps are disabled.

Command Mode

Global Configuration mode

User Guidelines

Any combination of the keywords are allowed. At least one keyword must be configured.

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

Example

The following example enables sending traps when a MAC address is successfully authorized by the 802.1X MAC-authentication access control.

```
switchxxxxxx(config)# dot1x traps authentication success mac
```

dot1x unlock client

To unlock a locked (in the quiet period) client, use the **dot1x unlock client** command in Privileged EXEC mode.

Syntax

dot1x unlock client *interface-id mac-address*

Parameters

- ***interface-id***—Interface ID where the client is connected to.
- ***mac-address***—Client MAC address.

Default Configuration

The client is locked until the silence interval is over.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to unlock a client that was locked after the maximum allowed authentication failed attempts and to end the quiet period. If the client is not in the quiet period, the command has no affect.

Example

```
switchxxxxxx# dot1x unlock client gi1/0/1 00:01:12:af:00:56
```

dot1x violation-mode

To configure the action to be taken when an unauthorized host on authorized port in single-host mode attempts to access the interface, use the **dot1x violation-mode** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x violation-mode {restrict | **protect** | **shutdown**} [**traps** *seconds*]

no dot1x violation-mode

Parameters

- **restrict**—Generates a trap when a station, whose MAC address is not the supplicant MAC address, attempts to access the interface. The minimum time between the traps is 1 second. Those frames are forwarded but their source addresses are not learned.
- **protect**—Discard frames with source addresses that are not the supplicant address.
- **shutdown**—Discard frames with source addresses that are not the supplicant address and shutdown the port.
- **trap** *seconds* - Send SNMP traps, and specifies the minimum time between consecutive traps. If seconds = 0 traps are disabled. If the parameter is not specified, it defaults to 1 second for the restrict mode and 0 for the other modes.

Default Configuration

Protect

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The command is relevant only for single-host mode.

For BPDU messages whose MAC addresses are not the supplicant MAC address are not discarded in Protect mode.

BPDU message whose MAC addresses are not the supplicant MAC address cause a shutdown in Shutdown mode.

Example

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x violation-mode protect
```

password

To specify a password for an 802.1X credential structure, use the **password** command in Dot1x credentials configuration mode. To remove the password, use the **no** form of this command.

Syntax

encrypted password *encrypted-password*

password *password*

no password

Parameters

- ***encrypted-password***—The password in encrypted format.
- ***password***—The password up to 64 characters.

Default Configuration

A password is not specified.

Command Mode

Dot1x credentials configuration mode

User Guidelines

An 802.1X credential structure is necessary when configuring a supplicant (client). This credentials structure must contain a username and password and might contain a description.

Example

The following example configures an 802.1X credential structure:

```
switchxxxxxx(config)# dot1x credentials site-A
switchxxxxxx(config-dot1x-cred)# username inner-switch
switchxxxxxx(config-dot1x-cred)# password 87b$#9hv5*
switchxxxxxx(config-dot1x-cred)# description This credentials profile should be used to
connect to site-A.
```

show dot1x

To display the 802.1X interfaces or specified interface status, use the **show dot1x** command in Privileged EXEC mode.

Syntax

show dot1x [interface interface-id **| detailed**]

Parameters

- ***interface-id***—Specifies an Ethernet port or OOB port.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all ports. If **detailed** is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays authentication information for all interfaces on which 802.1x is enabled:

```
switchxxxxxx# show dot1x
Authentication is enabled
Authenticator Global Configuration:
Authenticating Servers: Radius, None
MAC-Based Authentication:
  Type: Radius
  Username Groupsize: 2
  Username Separator: -
  Username case: Lowercase
  Password: MD5 checksum 1238af77aaca17568f12988601fcabed
Unathenticated VLANs: 100, 1000, 1021
Guest VLAN: VLAN 11, timeout 30 sec
Authentication failure traps are enabled for 802.1x+mac
Authentication success traps are enabled for 802.1x
Authentication quiet traps are enabled for 802.1x
Supplicant Global Configuration:
Supplicant Authentication failure traps are enabled
Supplicant Authentication success traps are enabled
gi1/0/1
  Authenticator is enabled
  Supplicant is disabled
  Authenticator Configuration:
  Host mode: multi-sessions
  Authentication methods: 802.1x+mac
  Port Adminstrated status: auto
  Guest VLAN: enabled
  VLAN Radius Attribute: enabled, static
  Open access: disabled
  Time range name: work_hours (Active now)
  Server-timeout: 30 sec
```

```
  Maximum Hosts: unlimited
  Maximum Login Attempts: 3
  Reauthentication is enabled
  Reauthentication period: 3600 sec
  Silence period: 1800 sec
  Quiet Period: 60 sec
  Interfaces 802.1X-Based Parameters
    EAP Timeout: 30 sec
    EAP Max-Retrans: 2
    Tx period: 30 sec
    Supplicant timeout: 30 sec
    max-req: 2
  Authentication success: 9
  Authentication fails: 1
  Number of Authorized Hosts: 10
  Supplicant Configuration:
  retry-max: 2
  EAP time period: 15 sec
  Supplicant Held Period: 30 sec
gi1/0/2
  Authenticator is enabled
  Supplicant is disabled
  Authenticator Configuration:
  Host mode: single-host
  Authentication methods: 802.1x+mac
  Port Adminstrated status: auto
  Port Operational status: authorized
  Guest VLAN: disabled
  VLAN Radius Attribute: enabled
  Open access: enabled
  Time range name: work_hours (Active now)
  Server-timeout: 30 sec
  Aplied Authenticating Server: Radius
  Applied Authentication method: 802.1x
  Session Time (HH:MM:SS): 00:25:22
  MAC Address: 00:08:78:32:98:66
  Username: Bob
  Violation:
    Mode: restrict
    Trap: enabled
    Trap Min Interval: 20 sec
    Violations were detected: 9
  Reauthentication is enabled
  Reauthentication period: 3600 sec
  Silence period: 1800 sec
  Quiet Period: 60 sec
  Interfaces 802.1X-Based Parameters
    EAP Timeout: 30 sec
    EAP Max-Retrans: 2
    Tx period: 30 sec
    Supplicant timeout: 30 sec
    max-req: 2
  Authentication success: 2
  Authentication fails: 0
gi1/0/3
  Authenticator is enabled
  Supplicant is disabled
  Authenticator Configuration:
  Host mode: multi-host
  Authentication methods: 802.1x+mac
  Port Adminstrated status: auto
  Port Operational status: authorized
  Guest VLAN: disabled
  VLAN Radius Attribute: disabled
```

```
  Time range name: work_hours (Active now)
  Open access: disabled
  Server-timeout: 30 sec
  Aplied Authenticating Server: Radius
  Applied Authentication method: 802.1x
  Session Time (HH:MM:SS): 00:25:22
  MAC Address: 00:08:78:32:98:66
  Username: Bob
  Violation:
    Mode: restrict
    Trap: enabled
    Trap Min Interval: 20 sec
    Violations were detected: 0
  Reauthentication is enabled
  Reauthentication period: 3600 sec
  Silence period: 1800 sec
  Quiet Period: 60 sec
  Interfaces 802.1X-Based Parameters
    EAP Timeout: 30 sec
    EAP Max-Retrans: 2
    Tx period: 30 sec
    Supplicant timeout: 30 sec
    max-req: 2
  Authentication success: 20
  Authentication fails: 0
  Supplicant Configuration:
  retry-max: 2
  EAP time period: 15 sec
  Supplicant Held Period: 30 sec
gi1/0/4
  Authenticator is disabled
  Supplicant is enabled
  Authenticator Configuration:
  Host mode: multi-host
  Authentication methods: 802.1x+mac
  Port Adminstrated status: force-auto
  Guest VLAN: disabled
  VLAN Radius Attribute: disabled
  Time range name: work_hours (Active now)
  Open access: disabled
  Server-timeout: 30 sec
  Aplied Authenticating Server: Radius
  Applied Authentication method: 802.1x
  Session Time (HH:MM:SS): 00:25:22
  MAC Address: 00:08:78:32:98:66
  Username: Bob
  Violation:
    Mode: restrict
    Trap: enabled
    Trap Min Interval: 20 sec
    Violations were detected: 0
  Reauthentication is enabled
  Reauthentication period: 3600 sec
  Silence period: 1800 sec
  Quiet Period: 60 sec
  Interfaces 802.1X-Based Parameters
    EAP Timeout: 30 sec
    EAP Max-Retrans: 2
    Tx period: 30 sec
    Supplicant timeout: 30 sec
    max-req: 2
  Authentication success: 0
  Authentication fails: 0
  Supplicant Configuration:
```

```
retry-max: 2
EAP time period: 15 sec
Supplicant Held Period: 30 sec
Credentials Name: Basic-User
Supplicant Operational status: authorized
```

The following describes the significant fields shown in the display:

- **Port**—The port interface-id.
- **Host mode**—The port authentication configured mode. Possible values: single-host, multi-host, multi-sessions.
  - single-host
  - multi-host
  - multi-sessions
- **Authentication methods**—Authentication methods configured on port. Possible values are combinations of the following methods:
  - 802.1x
  - mac
  - wba
- **Port Administrated status**—The port administration (configured) mode. Possible values: **force-auth**, **force-unauth**, **auto**.
- **Port Operational status**—The port operational (actual) mode. Possible values: **authorized** or **unauthorized**.
- **Username**—Username representing the supplicant identity. This field shows the username if the port control is auto. If the port is Authorized, it displays the username of the current user. If the port is Unauthorized, it displays the last user authorized successfully.
- **Quiet period**—Number of seconds that the device remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password).
- **Silence period**—Number of seconds that If an authorized client does not send traffic during the silence period specified by the command, the state of the client is changed to unauthorized.
- **EAP timeout**—Time interval in seconds during which the EAP Server (EAPAuthenticator) waits for a response from the EAP client (EAP Peer) before the requestretransmission
- **EAP Max Retrans**—Maximum number of times that the EAP Server (EAPAuthenticator) retransmits an EAP request when no response from a EAP client (EAPPeer) was received.
- **Tx period**—Number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the client before resending the request.
- **Max req**—Maximum number of times that the device sends an EAP request frame (assuming that no response is received) to the client before restarting the authentication process.
- **Server timeout**—Number of seconds that the device waits for a response from the authentication server before resending the request.
- **Session Time**—Amount of time (HH:MM:SS) that the user is logged in.

- **MAC address**—Supplicant MAC address.
- **Authentication success**—Number of times the state machine received a Success message from the Authentication Server.
- **Authentication fails**—Number of times the state machine received a Failure message from the Authentication Server.

show dot1x credentials

To display 802.1X credentials, use the **show dot1x credentials** mode command in Privileged EXEC mode.

Syntax

show dot1x credentials

Command Mode

Privileged EXEC mode

Examples

The following example displays dot1x credentials:

```
switchxxxxxx# show dot1x credentials
downstream-interface
 description: should be used for downstream ports
 username: downstream
 password's MD5: 1238af77aaca17568f12988601fcabed
upstream-interface
 description: should be used for connection to ISP
 username: up2isp
 password's MD5: 1238bbff75431230965394466ac76549
```

show dot1x locked clients

To display all clients who are locked and in the quiet period, use the **show dot1x locked clients** command in Privileged EXEC mode.

Syntax

show dot1x locked clients

Command Mode

Privileged EXEC mode

User Guidelines

Use the **show dot1x locked clients** command to display all locked (in the quiet period) clients.

Example

The following example displays locked clients:

```
switchxxxxxx# show dot1x locked clients
```

Port	MAC Address	Remaining Time
-------	--------------	--------------
gi1/0/1	0008.3b79.8787	20
gi1/0/1	0008.3b89.3128	40
gi1/0/2	0008.3b89.3129	10

show dot1x sessions interface

To display active 802.1X sessions for the specified interface, use the show dot1x sessions interface command in Privileged EXEC mode.

Syntax

show dot1x sessions interface *interface-id* **[detailed]**

Parameters

- **interface** *interface-id* —Specifies an Ethernet port.
- **detailed** (optional) — displays detailed information for each session on the interface.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to display the list of 802.1x sessions on the interface. A session can be authorized or authenticated but not authorized.

If the detailed keyword is not specified then the command output will provide the following information for each session: the interface for which the command output was requested, the MAC address of the supplicant, the method in which the supplicant was authenticated (MAC, dot1x or WBA), the session status - Auth (authenticated) or Unauth (authenticated but not authorized) and the Session ID.

If the detailed keyword is specified then the command output will provide, in addition, the following information for each session: the supplicant IPv4 address (if known), the supplicant username, the reason for Unauthorized stated (if relevant), the interface Oper host mode, the session re-authentication timeout value and the seconds remaining until tineout, timeout action, the session up time, the Common Session ID (audit session ID) and the accounting session ID. In addition the output may detail the Server Policies that are applied to the session.

This includes downloadable ACLs redirect ACL and redirect URL.

Example

Example 1. The following example displays 802.1X sessions on interface gi1 without using the detailed keyword.

```
switchxxxxxx# show dot1x session interface gi1
Interface Mac Address Method Status Session ID
---------- ----------------- -------- -------- ------------------------
gi1 68:05:ca:21:28:e6 MAC Auth 8787020A05000003000278A8
```

Example 2. The following example displays 802.1X sessions on interface gi1 including the detailed keyword.

```
switchxxxxxx# show dot1x session interface gi1 detailed
Interface: gi1
```

```
MAC Address: 68:05:ca:21:28:e6
IPv4 Address: 10.2.135.69
User-Name: guest1
Status: Authorized
Oper host mode: multi-session
Session timeout: 300 sec, Remaining: 92 sec
Timeout action: Reauthenticate
Session Uptime: 13708 sec
Common Session ID: 8787020A05000003000278A8
Acct Session ID: 0x05000003
Server Policies:
URL Redirect ACL: redirect_ACL
URL Redirect:
https://ise-svr.company.com:8443/portal/gateway?sessionId=8787020A05000003000278
A8&portal=f09aaac2-f101-45ed-832f-fda201ab7639&action=cwa&token=2289745240da1822
bf2c7a8af4a08452
ACS ACL: xACSACLx-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3
Method status list:
Method State
MAC Authentication success
```

show dot1x statistics

To display 802.1X statistics for the specified port, use the **show dot1x statistics** command in Privileged EXEC mode.

Syntax

show dot1x statistics interface *interface-id*

Parameters

- ***interface-id***—Specifies an Ethernet port or OOB port.

Command Mode

Privileged EXEC mode

Example

The following example displays 802.1X statistics for gi1/0/1.

```
switchxxxxxx# show dot1x statistics interface gi1/0/1
EapolEapFramesRx: 10
EapolStartFramesRx: 0
EapolLogoffFramesRx: 1
EapolAnnouncementFramesRx: 0
EapolAnnouncementReqFramesRx: 0
EapolInvalidFramesRx: 0
EapolEapLengthErrorFramesRx: 0
EapolMkNoCknFramesRx: 0
EapolMkInvalidFramesRx: 0
EapolLastRxFrameVersion: 3
EapolLastRxFrameSource: 00:08:78:32:98:78
EapolSuppEapFramesTx: 0
EapolStartFramesTx: 1
EapolLogoffFramesTx: 0
EapolAnnouncementFramesTx: 0
EapolAnnouncementReqFramesTx: 0
EapolAuthEapFramesTx: 9
EapolMkaFramesTx: 0
```

The following table describes the significant fields shown in the display:

Field	Description
EapolInvalidFramesRx	The number of invalid EAPOL frames of any type that have been received by this PAE.
EapolEapLengthErrorFramesRx	The number of EAPOL frames that the Packet Body Length does not match a Packet Body that is contained within the octets of the received EAPOL MPDU in this PAE.
EapolAnnouncementFramesRx	The number of EAPOL-Announcement frames that have been received by this PAE.

Field	Description
EapolAnnouncementReqFramesRx	The number of EAPOL-Announcement-Req frames that have been received by this PAE.
EapolStartFramesRx	The number of EAPOL-Start frames that have been received by this PAE.
EapolEapFramesRx	The number of EAPOL-EAP frames that have been received by this PAE.
EapolLogoffFramesRx	The number of EAPOL-Logoff frames that have been received by this PAE.
EapolMkNoCknFramesRx	The number of MKPDUs received with MKA not enabled or CKN not recognized in this PAE.
EapolMkInvalidFramesRx	The number of MKPDUs failing in message authentication on receipt process in this PAE.
EapolLastRxFrameVersion	The version of last received EAPOL frame by this PAE.
EapolLastRxFrameSource	The source MAC address of last received EAPOL frame by this PAE.
EapolSuppEapFramesTx	The number of EAPOL-EAP frames that have been transmitted by the supplicant of this PAE.
EapolLogoffFramesTx	The number of EAPOL-Logoff frames that have been transmitted by this PAE.
EapolAnnouncementFramesTx	The number of EAPOL-Announcement frames that have been transmitted by this PAE.
EapolAnnouncementReqFramesTx	The number of EAPOL-Announcement-Req frames that have been transmitted by this PAE.
EapolStartFramesTx	The number of EAPOL-Start frames that have been received by this PAE.
EapolAuthEapFramesTx	The number of EAPOL-EAP frames that have been transmitted by the authenticator of this PAE.
EapolMkaFramesTx	The number of EAPOL-MKA frames with no CKN information that have been transmitted by this PAE.

show dot1x users

To display active 802.1X authorized users for the device, use the **show dot1x users** command in Privileged EXEC mode.

Syntax

show dot1x users [username *username*]

Parameters

- **username** username—Specifies the supplicant username (Length: 1–160 characters).

Default Configuration

Display all users.

Command Mode

Privileged EXEC mode

Example 1. The following commands displays all 802.1x users:

```
show dot1x users
```

Port	Username	MAC Address	Auth Method	Auth Server	Session Time	VLAN
gi1/0/1	Bob	0008.3b71.1111	802.1x	Remote	09:01:00	1020
gi1/0/2	00083b798787	0008.3b79.8787	MAC	Remote	00:11:12	
gi1/0/2	John	0008.3baa.0022	WBA	Remote	00:27:16	

Example 2. The following example displays 802.1X user with supplicant username Bob:

```
switchxxxxxx# show dot1x users username Bob
```

Port	Username	MAC Address	Auth Method	Auth Server	Session Time	VLAN
gi1/0/1	Bob	0008.3b71.1111	802.1x	Remote	09:01:00	1020

username (dot1x credentials)

To specify a username for an 802.1X credential structure, use the **username** command in Dot1x credentials configuration mode. To remove the username, use the **no** form of this command.

Syntax

username *username*

no username

Parameters

- ***username***—The user name up to 32 characters.

Default Configuration

A username is not specified.

Command Mode

Dot1x credentials configuration mode

User Guidelines

An 802.1X credential structure is necessary when configuring a supplicant (client). This credentials structure may contain a username, password, and description.

Example

The following example configures an 802.1X credential structure:

```
switchxxxxxx(config)# dot1x credentials site-A
switchxxxxxx(config-dot1x-cred)# username inner-switch
switchxxxxxx(config-dot1x-cred)# password 87%$#bgd98^
switchxxxxxx(config-dot1x-cred)# description This credentials profile should be used to
connected to site-A
```