802.1X Commands

dot1x authentication default

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

To specify the authentication mode for 802.1X authentication, use the **dot1x authentication default** command in switch configuration mode. To restore the default configuration, use the **no** form of this command.

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

no dot1x authentication default

Syntax Description

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

Command Default

RADIUS server

Command Modes

Switch configuration (config-switch)

Command History

Release	Modification
3.5.1	This command was introduced.

Usage Guidelines

None

Example

The following example sets the 802.1X authentication mode to RADIUS server authentication:

```
nfvis(config-switch)# dot1x authentication default radius
nfvis(config-switch)# commit
nfvis(config-switch)# end
```

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 switch configuration mode. To restore the default configuration, use the **no** form of this command.

dot1x guest-vlan timeout *timeout time*
no dot1x guest-vlan timeout

Syntax Description

timeout time	Specifies the time delay in seconds between enabling 802.1X (or port up) and adding the port to the guest VLAN. Valid range is from 30–180.

Command Default

The guest VLAN is applied immediately.

Command Modes

Switch configuration (config-switch)

Command History

Release	Modification
3.5.1	This command was introduced.

Usage Guidelines

This command is relevant if the guest VLAN is enabled on the port.

Example

The following example sets a delay of 90 seconds between enabling 802.1X and adding a port to a guest VLAN:

```
nfvis(config-switch)# dot1x guest-vlan timeout 90
nfvis(config-switch)# commit
nfvis(config-switch)# end
```

dot1x system-auth-control

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

dot1x system-auth-control
no dot1x system-auth-control

Syntax Description

This command has no arguments or keywords

Command Default

Disabled

Command Modes

Switch configuration (config-switch)

Command History

Release	Modification
3.5.1	This command was introduced.

Example

The code in the example enables 802.1X globally

```
nfvis(config-switch)# dot1x system-auth-control
nfvis(config-switch)# commit
nfvis(config-switch)# end
```

authentication open

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

authentication open
no authentication open

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface switch configuration (config-switch-if)

Command History

Release	Modification
3.5.1	This command was introduced.

Usage Guidelines

Open access or monitoring mode allows clients or devices to gain network access before authentication is performed. In this mode, the switch processes failure replies that are received from a Radius server as success.

Example

The following example shows how to enable open access (monitoring mode) on the Gigabit Ethernet interface 1/0:

```
nfvis(config-switch)# interface gigabitEthernet 1/0
nfvis(config-switch-if)# authentication open
nfvis(config-switch-if)# commit
nfvis(config-switch-if)# end
```

dot1x authentication

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

dot1x authentication {**802.1x** | **mac** | **both**}

no dot1x authentication

Syntax Description

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).
both	Enables both 802.1X-based authentication and MAC-based authentication.

Command Default

802.1X-based authentication is enabled.

Command Modes

Interface (Gigabit Ethernet) switch configuration (config-switch-if)

Command History

Release	Modification
3.5.1	This command was introduced.

Usage Guidelines

Static MAC addresses cannot be authorized by the MAC-based method. Do not change a dynamic MAC address to a static one or delete it if the MAC address was authorized by the MAC-based authentication:

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

Example

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

```
nfvis(config-switch)# interface gigabitEthernet 1/0
nfvis(config-switch-if)# dot1x authentication both
nfvis(config-switch-if)# commit
nfvis(config-switch-if)# end
```

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 switch configuration mode. To disable access, use the **no** form of this command.

dot1x guest-vlan enable

no dot1x guest-vlan enable

Syntax Description

This command has no arguments or keywords.

Command Default

By default, this configuration is disabled.

Command Modes

Interface (Gigabit Ethernet) switch configuration (config-switch-if)

Command History

Release	Modification
3.5.1	This command was introduced.

Usage Guidelines

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

Example

The following example enables unauthorized users on the Gigabit Ethernet 1/1 interface to access the guest VLAN:

```
nfvis(config-switch)# interface gigabitEthernet 1/1
nfvis(config-switch-if)# dot1x guest-vlan enable
nfvis(config-switch-if)# commit
nfvis(config-switch-if)# end
```

dot1x guest-vlan

To define a guest VLAN, use the **dot1x guest-vlan** command in interface switch configuration mode. To restore the default configuration, use the **no** form of this command.

dot1x guest-vlan

no dot1x guest-vlan

Syntax Description

This command has no arguments or keywords

Command Default

No VLAN is defined as a guest VLAN.

Command Modes

Interface (VLAN) switch configuration (config-switch-if)

Command History

Release	Modification
3.5.1	This command was introduced.

Usage Guidelines

- Use the **dot1x guest-vlan enable** command to enable unauthorized users on an interface to access the guest VLAN.
- 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 shows how to define a guest VLAN:

```
nfvis(config-switch)# interface vlan 2
nfvis(config-switch-if)# dot1x guest-vlan
nfvis(config-switch-if)# commit
nfvis(config-switch-if)# end
```

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 switch configuration mode. To restore the default configuration, use the **no** form of this command.

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

Syntax Description

multi-host	Enables multi-hosts mode.
single-host	Enables single-host mode.

Command Default

The default mode is multi-host mode.

Command Modes

Interface (Gigabit Ethernet) switch configuration (config-switch-if)

Command History

Release	Modification
3.5.1	This command was introduced.

Usage 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 on the port. Traffic from the other hosts is dropped.

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.

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

Example

The following example enables multi-host on the Gigabit Ethernet 1/1 interface:

```
nfvis(config-switch)# interface gigabitEthernet 1/1
nfvis(config-switch-if)# dot1x host-mode multi-host
nfvis(config-switch-if)# commit
nfvis(config-switch-if)# end
```

dot1x max-eap-req

To set the maximum number of times 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-eap-req** command in interface switch configuration mode. To restore the default configuration, use the **no** form of this command.

dot1x max-eap-req *count*
no dot1x max-eap-req

Syntax Description

count	Specifies the maximum number of times that the device sends an EAP request/identity frame before restarting the authentication process. Valid range is from 1 to 10.

Command Default

The default maximum number of attempts is 2.

Command Modes

Interface (Gigabit Ethernet) switch configuration (config-switch-if)

Command History

Release	Modification
3.5.1	This command was introduced.

Example

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

```
nfvis(config-switch)# interface gigabitEthernet 1/1
nfvis(config-switch-if)# dot1x max-eap-req 6
nfvis(config-switch-if)# commit
nfvis(config-switch-if)# end
```

dot1x port-control

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

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

Syntax Description

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.
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.

Command Default

The port is in the force-authorized state.

Command Modes

Interface (Gigabit Ethernet) switch configuration (config-switch-if)

Command History

Release	Modification
3.5.1	This command was introduced.

Usage Guidelines

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

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

Example

The following example sets 802.1X authentication on Gigabit Ethernet interface 1/1 to the auto mode:

```
nfvis(config-switch)# interface gigabitEthernet 1/1
nfvis(config-switch-if)# dot1x port-control auto
nfvis(config-switch-if)# commit
nfvis(config-switch-if)# end
```

dot1x reauthentication

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

dot1x reauthentication
no dot1x reauthentication

Syntax Description

This command has no arguments or keywords

Command Default

Periodic re-authentication is disabled.

Command Modes

Interface (Gigabit Ethernet) switch configuration (config-switch-if)

Command History

Release	Modification
3.5.1	This command was introduced.

Example

The code in the example enables periodic re-authentication of the client.

```
nfvis(config-switch)# interface gigabitEthernet 1/1
nfvis(config-switch-if)# dot1x reauthentication
nfvis(config-switch-if)# commit
nfvis(config-switch-if)# end
```

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 switch configuration mode. To restore the default configuration, use the **no** form of this command.

dot1x timeout quiet-period *seconds*
no dot1x timeout quiet-period

Syntax Description

seconds	Specifies the time interval in seconds that the device remains in a quiet state following a failed authentication exchange with a client. Valid range is from 10 to 65535 seconds.

Command Default

The default quiet period is 60 seconds.

Command Modes

Interface (Gigabit Ethernet) switch configuration (config-switch-if)

Command History

Release	Modification
3.5.1	This command was introduced.

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

Example

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

```
nfvis(config-switch)# interface gigabitEthernet 1/1
nfvis(config-switch-if)# dot1x timeout quiet-period 120
nfvis(config-switch-if)# commit
nfvis(config-switch-if)# end
```

dot1x timeout reauth-period

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

dot1x timeout reauth-period *seconds*
no dot1x timeout reauth-period

Syntax Description

reauth-period seconds	Number of seconds between re-authentication attempts. Valid range is from 300—4294967295.

Command Default

3600

Command Modes

Interface (Gigabit Ethernet) switch configuration (config-switch-if)

Usage Guidelines

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

Command History

Release	Modification
3.5.1	This command was introduced.

Example

```
nfvis(config-switch)# interface gigabitEthernet 1/0
nfvis(config-switch-if)# dot1x timeout reauth-period 5000
nfvis(config-switch-if)# commit
nfvis(config-switch-if)# end
```

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 switch configuration mode. To restore the default configuration, use the **no** form of this command.

dot1x timeout server-timeout *seconds*
no dot1x timeout server-timeout

Syntax Description

server-timeout seconds	Specifies the time interval in seconds during which the device waits for a response from the authentication server. Valid range is from 1 to 65535 seconds.

Command Default

The default timeout period is 30 seconds.

Command Modes

Interface (Gigabit Ethernet) switch configuration (config-switch-if)

Command History

Release	Modification
3.5.1	This command was introduced.

Usage 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 with the timeout period specified by the radius-server retransmit command, and selecting the lower of the two values.

Example

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

```
nfvis(config-switch)# interface gigabitEthernet 1/0
nfvis(config-switch-if)# dot1x timeout server-timeout 3600
nfvis(config-switch-if)# commit
nfvis(config-switch-if)# end
```

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 switch configuration mode. To restore the default configuration, use the **no** form of this command.

dot1x timeout supp-timeout *seconds*
no dot1x timeout supp-timeout

Syntax Description

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. Valid range is from 1 to 65535 seconds.

Command Default

The default timeout period is 30 seconds

Command Modes

Interface (Gigabit Ethernet) switch configuration (config-switch-if)

Command History

Release	Modification
3.5.1	This command was introduced.

Usage 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.

```
nfvis(config-switch)# interface gigabitEthernet 1/1
nfvis(config-switch-if)# dot1x timeout supp-timeout 3600
nfvis(config-switch-if)# commit
nfvis(config-switch-if)# end
```

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 switch configuration mode. To restore the default configuration, use the **no** form of this command.

dot1x timeout tx-period *seconds*
nodot1x timeout tx-period

Syntax Description

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 to 65535 seconds).

Command Default

The default timeout period is 30 seconds.

Command Modes

Interface (Gigabit Ethernet) switch configuration (config-switch-if)

Command History

Release	Modification
3.5.1	This command was introduced.

Usage 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/identity frame, to 60 seconds.

```
nfvis(config-switch)# interface gigabitEthernet 1/0
nfvis(config-switch-if)# dot1x timeout tx-period 60
nfvis(config-switch-if)# commit
nfvis(config-switch-if)# end
```

dot1x violation mode

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

dot1x violation-mode {**restrict** | **protect** | **shutdown**}
no dot1x violation-mode

Syntax Description

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.

Command Default

Protect

Command Modes

Interface (Gigabit Ethernet) switch configuration (config-switch-if)

Command History

Release	Modification
3.5.1	This command was introduced.

Usage Guidelines

The command is relevant only for the single-host mode.

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

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

Example

The following example sets the interface to the protect mode.

```
nfvis(config-switch)# interface gigabitEthernet 1/0
nfvis(config-switch-if)# dot1x violation-mode protect
nfvis(config-switch-if)# commit
nfvis(config-switch-if)# end
```

show switch dot1x

To display information about 802.1X interfaces, use the **show switch dot1x** command in privileged EXEC mode.

switch show dot1x [**interface gigabitEthernet** *interface-id* | **statistics** | **summary** | **users**]

Syntax Description

interface gigabitEthernet *interface-id*	Displays the information for the specified interface ID.
statistics	Displays 802.1x statistics.
summary	Displays interface summary.
users	Displays information about authenticated users.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
3.5.1	This command was introduced.

Example

The following is a sample output of the **show switch dot1x** command for Gigabit Ethernet interface 1/0:

```
nfvis# show switch dot1x interface gigabitEthernet 1/0
dot1x interface gigabitEthernet 1/0
 host-mode                multiple
 port-admin-status        force-authorized
 guest-vlan               "Guest VLAN: disabled"
 open-access              "Open access: disabled"
 server-timeout           30
 port-oper-status         "Port Operational Status: authorized*"
 reauthentication         "Reauthenticaion is disabled"
 reauthentication-timeout 3600
 quiet-period             60
 auth-tx-period           30
 auth-supplicant-timeout  30
 max-req                  2
 auth-failure-count       0
 auth-success-count       0
```