

Contents [[hide](#)]

- [1 QUANTUM QN-SW-325 Network Switch](#)
- [2 Specifications](#)
- [3 Product Usage Instructions](#)
- [4 Network Switch CLI Guide](#)
- [5 FAQs](#)
- [6 Documents / Resources](#)
 - [6.1 References](#)



QUANTUM QN-SW-325 Network Switch



Specifications

- Product: Network Switch CLI Guide
- Commands: 802.1x, aaa authentication dot1x, authentication open, clear dot1x statistics, dot1x authentication
- Configuration Modes: Global configuration mode, Interface (Ethernet, OOB) Configuration mode, Privileged EXEC mode

Product Usage Instructions

aaa authentication dot1x Command

- **Syntax:** aaa authentication dot1x
- **Parameters:** radius, none
- **Default Configuration:** Radius Server
- **Usage:** Specify servers for authentication when 802.1X authentication is enabled.
- **Example:** Set authentication mode to RADIUS server authentication.

authentication open Command

- **Syntax:** authentication open
- **Default Configuration:** Disabled
- **Usage:** Enable open access on a port for monitoring mode.

Clear dot1x statistics Command

- **Syntax:** clear dot1x statistics [interface-id]
- **Default Configuration:** Statistics on all ports are cleared
- **Usage:** Clear 802.1X statistics

dot1x authentication Command

- **Syntax:** dot1x authentication [802.1x] [mac]
- **Default Configuration:** 802.1X-based authentication is enabled
- **Usage:** Enable authentication methods on a port based on 802.1X or MAC address.

Network Switch CLI Guide

802.1x Commands

aaa authentication dot1x

Syntax	aaaauthenticationdot1xdefault{radius none {radiusnone}} no aaa authentication dot1x default
--------	--

Parameters	<p>radius – Uses the list of all RADIUS servers for authentication.</p> <p>none- Uses no authentication.</p>
Default Configuration	Radius Server.
Command Mode	Global configuration mode.
Usage	<p>To specify which servers are used for authentication when 802.1X authentication is enabled, use the <code>aaa authentication dot1x command</code> in Global Configuration mode.</p> <p>To restore the default configuration, use the <code>no</code> form of this command.</p>
Example	<p>The following example sets the 802.1X authentication mode to RADIUS server authentication. Even if no response was received, authentication succeeds.</p> <pre>switchxxxxxx(config)# aaa authentication dot1x default radius none</pre>
User Guideline	<p>User can select either authentication by a RADIUS server, no authentication (none), or both methods.</p> <p>If you require that authentication succeeds even if no RADIUS server response was received, specify none as the final method in the command line.</p>

authentication open

Syntax	authentication open no authentication open
Parameters	This command has no arguments or keywords.

Default Configuration	Disabled.
Command Mode	Interface (Ethernet, OOB) Configuration mode.
Usage	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.
Example	The following example enables open mode on interface te1/0/1: switchxxxxxx(config)# interface te1/0/1 switchxxxxxx(config-if)# authentication open
User Guideline	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.

clear dot1x statistics

Syntax	clear dot1x statistics [<i>interface-id</i>]
Parameters	<i>interface-id</i> —Specify an Ethernet port ID.
Default Configuration	Statistics on all ports are cleared.
Command Mode	Privileged EXEC mode.
Usage	To clear 802.1X statistics, use the clear dot1x statistics command in Privileged EXEC mode.

Example	switchxxxxxx# clear dot1x statistics
User Guideline	<p>This command clears all the counters displayed in the show dot1x</p> <p>and show dot1x statistics command.</p>

dot1x authentication

Syntax	dot1xauthentication [802.1x][mac] no dot1x authentication
Parameters	<p>802.1x—Enables authentication based on 802.1X (802.1X-based authentication).</p> <p>mac—Enables authentication based on the station's MAC address (MAC-Based authentication).</p>
Default Configuration	X-Based authentication is enabled.
Command Mode	Interface (Ethernet) Configuration mode.
Usage	<p>To enable authentication methods on a port, use the dot1x authentication command in Interface Configuration mode.</p> <p>To restore the default configuration, use the no form of this command.</p>
Example	<p>The following example enables authentication based on 802.1x and the station's MAC address on port te1/0/1:</p> <pre>switchxxxxxx(config)# interface te1/0/1 switchxxxxxx(config-if)# dot1x authentication 802.1x mac</pre>

User Guideline	<p>Static MAC addresses cannot be authorized by the MAC-based method.</p> <p>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:</p> <p>If a dynamic MAC address authenticated by MAC-based authentication is changed to a static one, it will not be manually re-authenticated.</p> <p>Removing a dynamic MAC address authenticated by the MAC-based authentication causes its re-authentication.</p>
-----------------------	---

dot1x guest-vlan

Syntax	dot1x guest-vlan no dot1x guest-vlan
Parameters	N/A.
Default Configuration	No VLAN is defined as a guest VLAN.
Command Mode	Interface (VLAN) Configuration mode.
Usage	<p>To define a guest VLAN, use the dot1x guest-vlan mode command in Interface(VLAN) Configuration mode.</p> <p>To restore the default configuration, use the no form of this command.</p>
Example	<p>The following example defines VLAN 2 as a guest VLAN.</p> <pre>switchxxxxxx(config)# interface vlan 2 switchxxxxxx(config-if)# dot1x guest-vlan</pre>

User Guideline	<p>Use the <code>dot1x guest-vlan enable</code> command to enable unauthorized users on an interface to access the guest VLAN.</p> <p>A device can have only one global guest VLAN.</p> <p>The guest VLAN must be a static VLAN and it cannot be removed. An unauthorized VLAN cannot be configured as guest VLAN.</p>
-----------------------	--

dot1x guest-vlan enable

Syntax	dot1x guest-vlan enable no dot1x guest-vlan enable
Parameters	N/A.
Default Configuration	Disabled.
Command Mode	Interface (Ethernet) Configuration mode.
Usage	<p>To enable unauthorized users on the access interface to the guest VLAN, use the dot1x guest-vlan enable command in Interface Configuration mode.</p> <p>To disable access, use the no form of this command.</p>
Example	<p>The following example enables unauthorized users on te1/0/1 to access the guestVLAN.</p> <pre>switchxxxxxx(config)# interface te1/0/1 switchxxxxxx(config-if)# dot1x guest-vlan enable</pre>

User Guideline	<p>This command cannot be configured if the monitoring VLAN is enabled on the interface.</p> <p>If the port does not belong to the guest VLAN it is added to the guest VLAN as an egress untagged port.</p> <p>If the authentication mode is single-host or multi-host, the value of PVID is set to the guest VLAN_ID.</p> <p>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.</p> <p>If 802.1X is disabled, the port static configuration is reset.</p> <p>See the User Guidelines of the dot1x host-mode command for more information.</p>
-----------------------	---

dot1x guest-vlan timeout

Syntax	<p>dot1x guest-vlan timeout <i>timeout</i></p> <p>no dot1x guest-vlan timeout</p>
Parameters	<p><i>timeout</i> — Specifies the time delay in seconds between enabling 802.1X (or port up) and adding the port to the guest VLAN. (Range: 30–180).</p>
Default Configuration	<p>The guest VLAN is applied immediately.</p>
Command Mode	<p>Global Configuration mode.</p>

Usage	<p>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.</p> <p>To restore the default configuration, use the no form of this command.</p>
Example	<p>The following example sets the delay between enabling 802.1X and adding a port to a guest VLAN to 60 seconds.</p> <pre>switchxxxxxx(config)# dot1x guest-vlan timeout 60</pre>
User Guideline	<p>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.</p>

dot1x host-mode

Syntax	dot1x host-mode {multi-host / single-host / multi-sessions}
Parameters	<p>multi-host—Enables multiple-host mode.</p> <p>single-host—Enables single-host mode.</p> <p>multi-sessions—Enables multiple sessions mode.</p>
Default Configuration	Default mode is multi-host.
Command Mode	Interface (Ethernet) Configuration mode.

Usage	<p>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.</p> <p>To restore the default configuration, use the no form of this command.</p>
Example	<pre>switchxxxxxx(config)# interface te1/0/1 switchxxxxxx(config-if)# dot1x host-mode multi-host</pre>

User Guideline	<p>Single-Host Mode</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>In this case, tagged traffic is dropped unless the VLAN tag is the RADIUS-assigned VLAN or the unauthenticated VLANs. See the dot1x radius-attributes vlan command to enable RADIUS VLAN assignment at a port.</p> <p>The switch removes from FDB all MAC addresses learned on a port when its authentication status is changed from authorized to unauthorized.</p> <p>Multi-Host Mode</p> <p>The multi-host mode manages the authentication status of the</p>
	<p>port: the port is authorized after at least one host is authorized.</p> <p>When a port is unauthorized and the guest VLAN is enabled, untagged traffic is remapped to the guest VLAN. Tagged traffic is</p>

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. See the `dot1x radius-attributes vlan` command to enable RADIUS VLAN assignment at a port.

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 not have any authentication status. Any number of hosts can be authorized on the port. The `dot1x max-hosts` 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. multi-sessions mode cannot be configured on the same interface together with Policy Based VLANs configured by the following commands:

switchport general map protocol-group vlans switchport general map macs-group vlans

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. See the dot1x radius-attributes vlan command to enable RADIUS VLAN assignment at a port.

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

dot1x max-hosts

Syntax	dot1x max-hosts <i>count</i> no dot1x max-hosts
Parameters	<i>count</i> —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.
Usage	<p>To configure the maximum number of authorized hosts allowed on the interface, use the dot1x max-hosts command in Interface Configuration mode.</p> <p>To restore the default configuration, use the no form of this command.</p>
Example	<p>The following example limits the maximum number of authorized hosts on Ethernet port te1/0/1 to 6:</p> <pre>switchxxxxx(config)# interface te1/0/1 switchxxxxx(config-if)# dot1x max-hosts 6</pre>
User Guideline	<p>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.</p> <p>This command is relevant only for multi-session mode.</p>

dot1x max-req

Syntax	dot1x max-req <i>count</i> no dot1x max-req
Parameters	<i>count</i> — 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.
Usage	<p>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.</p> <p>To restore the default configuration, use the no form of this command.</p>
Example	<p>The following example sets the maximum number of times that the device sends an EAP request/identity frame to 6.</p> <pre>switchxxxxxx(config)# interface te1/0/1 switchxxxxxx(config-if)# dot1x max-req 6</pre>
User Guideline	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.

dot1x port-control

Syntax	dot1x port-control {auto force-authorized force-unauthorized} no dot1x port-control
Parameters	<p>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.</p> <p>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.</p> <p>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.</p>
Default Configuration	The port is in the force-authorized state.
Command Mode	Interface (Ethernet, OOB) Configuration mode.
Usage	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.
Example	<p>The following example sets 802.1X authentication on te1/0/1 to auto mode.</p> <pre>switchxxxxxx(config)# interface te1/0/1 switchxxxxxx(config-if)# dot1x port-control auto</pre>

User Guideline	<p>802.1X authentication cannot be enabled on an interface if port security feature is already enabled on the same interface.</p> <p>The switch removes all MAC addresses learned on a port when its authorization control is changed from force-authorized to another.</p> <p>Note. It is recommended to disable spanning tree or to enable spanning-tree Port Fast 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.</p>
-----------------------	--

dot1x re-authenticate

Syntax	dot1x re-authenticate [<i>interface-id</i>]
Parameters	<i>interface-id</i> —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.
Usage	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.
Example	<p>The following command manually initiates re-authentication of 802.1X-enabled te1/0/1:</p> <pre>switchxxxxxx# dot1x re-authenticate te1/0/1</pre>
User Guideline	—

dot1x reauthentication

Syntax	dot1x reauthentication no dot1x reauthentication
Parameters	N/A.
Default Configuration	Periodic re-authentication is disabled.
Command Mode	Interface (Ethernet, OOB) Configuration mode.
Usage	<p>To enable periodic re-authentication of the client, use the dot1x reauthentication command in Interface Configuration mode.</p> <p>To restore the default configuration, use the no form of this command.</p>
Example	switchxxxxxx(config)# interface te1/0/1 switchxxxxxx(config-if)# dot1x reauthentication
User Guideline	—

dot1x system-auth-control

Syntax	dot1x system-auth-control no dot1x system-auth-control
Parameters	N/A.
Default Configuration	Disabled.
Command Mode	Global Configuration mode.

Usage	<p>To enable 802.1X globally, use the dot1x system-auth-control command in Global Configuration mode.</p> <p>To restore the default configuration, use the no form of this command.</p>
Example	The following example enables 802.1X globally. switchxxxxxx(config)# dot1x system-auth-control
User Guideline	—

dot1x timeout quiet-period

Syntax	<p>dot1x timeout quiet-period <i>seconds</i></p> <p>no dot1x timeout quiet-period</p>
Parameters	<i>seconds</i> —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.
Usage	<p>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.</p> <p>To restore the default configuration, use the no form of this command.</p>

Example	The following example sets the time interval that the device remains in the quiet state following a failed authentication
----------------	---

	<p>exchange to 120 seconds.</p> <pre>switchxxxxxx(config)# interface te1/0/1 switchxxxxxx(config-if)# dot1x timeout quiet-period 120</pre>
User Guideline	<p>During the quiet period, the device does not accept or initiate authentication requests.</p> <p>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.</p> <p>To provide faster response time to the user, a smaller number than the default value should be entered.</p> <p>For 802.1x and MAC-based authentication, the number of failed logins is 1.</p> <p>For 802.1x-based and MAC-based authentication methods, the quiet period is applied after each failed attempt.</p>

dot1x timeout reauth-period

Syntax	dot1x system-auth-control no dot1x system-auth-control
Parameters	N/A.

Default Configuration	Disabled.
Command Mode	Global Configuration mode.
Usage	<p>To enable 802.1X globally, use the dot1x system-auth-control command in Global Configuration mode.</p> <p>To restore the default configuration, use the no form of this command.</p>
Example	The following example enables 802.1X globally. switchxxxxxx(config)# dot1x system-auth-control
User Guideline	—

dot1x timeout reauth-period

Syntax	dot1x timeout reauth-period <i>seconds</i> no dot1x timeout reauth-period
Parameters	reauth-period <i>seconds</i> —Number of seconds between re-attempts. (Range: 300-4294967295).
Default Configuration	3600
Command Mode	Interface (Ethernet, OOB) Configuration mode.
Usage	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.

Example	<pre>switchxxxxxx(config)# interface te1/0/1</pre> <pre>switchxxxxxx(config-if)# dot1x timeout reauth-period 5000</pre>
User Guideline	The command is only applied to the 802.1x authentication method.

dot1x timeout server-timeout

Syntax	<pre>dot1x timeout server-timeout <i>seconds</i></pre> <pre>no dot1x timeout server-timeout</pre>
Parameters	server-timeout <i>seconds</i> —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.
Usage	<p>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 InterfaceConfiguration mode.</p> <p>To restore the default configuration, use the no form of this command.</p>
Example	<p>The following example sets the time interval between retransmission of packets to the authentication server to 3600 seconds.</p>

	<pre>switchxxxxxx(config)# interface te1/0/1</pre> <pre>switchxxxxxx(config-if)# dot1x timeout server-timeout 3600</pre>
User Guideline	<p>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 retransmit command, and selecting the lower of the two values.</p>

dot1x timeout supp-timeout

Syntax	<pre>dot1x timeout supp-timeout <i>seconds</i></pre> <pre>no dot1x timeout supp-timeout</pre>
Parameters	<p>supp-timeout <i>seconds</i>—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).</p>
Default Configuration	<p>The default timeout period is 30 seconds.</p>
Command Mode	<p>Interface (Ethernet, OOB) Configuration mode.</p>
Usage	<p>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.</p> <p>To restore the default configuration, use the no form of this command.</p>

Example	<p>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.</p> <pre>switchxxxxxx(config)# interface te1/0/1</pre> <pre>switchxxxxxx(config-if)# dot1x timeout supp-timeout 3600</pre>
User Guideline	<p>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.</p> <p>The command is only applied to the 802.1x authentication method.</p>

dot1x timeout tx-period

Syntax	<p>dot1x timeout tx-period <i>seconds</i></p> <p>no dot1x timeout tx-period</p>
Parameters	<p><i>seconds</i>—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).</p>
Default Configuration	<p>The default timeout period is 30 seconds.</p>
Command Mode	<p>Interface (Ethernet, OOB) Configuration mode.</p>

Usage	<p>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 <code>dot1x timeout tx-period</code> command in Interface Configuration mode.</p> <p>To restore the default configuration, use the no form of this command.</p>
Example	<p>The following command sets the time interval during which the device waits for a response to an EAP request/identity frame to 60 seconds.</p> <pre>switchxxxxxx(config)# interface te1/0/1 switchxxxxxx(config-if)# dot1x timeout tx-period 60</pre>
User Guideline	<p>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.</p> <p>The command is only applied to the 802.1x authentication method.</p>

dot1x traps authentication failure

Syntax	dot1xtrapsauthenticationfailure{[802.1x][mac]} no dot1x traps authenticationfailure
Parameters	<p>802.1x—Enables traps for 802.1X-based authentication.</p> <p>mac—Enables traps for MAC-based authentication.</p>

Default Configuration	All traps are disabled.
Command Mode	Global Configuration mode.
Usage	<p>To enable sending traps when an 802.1X authentication method failed, use the dot1x traps authentication failure command in Global Configuration mode.</p> <p>To restore the default configuration, use the no form of this command.</p>
Example	<p>The following example enables sending traps when a MAC address fails to be authorized by the 802.1X mac-authentication access control.</p> <pre>switchxxxxxx(config)#</pre>
User Guideline	<p>Any combination of the keywords are allowed. At least one keyword must be configured.</p> <p>A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.</p>

dot1x traps authentication quiet

Syntax	<p>dot1x traps authentication quiet</p> <p>no dot1x traps authentication quiet</p>
Parameters	N/A.
Default Configuration	Quiet traps are disabled.

Command Mode	Global Configuration mode.
Usage	<p>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.</p> <p>To disable the traps, use the no form of this command.</p>

Example	<p>The following example enables sending traps when a host is set in the quiet state:</p> <pre>switchxxxxx(config)# dot1x traps authentication quiet</pre>
User Guideline	<p>The traps are sent after the client is set to the quiet state after the maximum sequential attempts of login.</p> <p>A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.</p>

dot1x traps authentication success

Syntax	dot1xtrapsauthenticationsuccess{[802.1x][mac]} no dot1x traps authenticationsuccess
Parameters	<p>802.1x—Enables traps for 802.1X-based authentication.</p> <p>mac—Enables traps for MAC-based authentication.</p>
Default Configuration	Success traps are disabled.
Command Mode	Global Configuration mode.

Usage	<p>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.</p> <p>To disable the traps, use the no form of this command.</p>
Example	<p>The following example enables sending traps when a MAC address is successfully authorized by the 802.1X MAC-authentication access control.</p> <pre>switchxxxxxx(config)# dot1x traps authentication success mac</pre>
User Guideline	<p>Any combination of the keywords are allowed. At least one keyword must be configured.</p> <p>A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.</p>

dot1x unlock client

Syntax	dot1x unlock client interface-id mac-address
Parameters	<p>interface-id—Interface ID where the client is connected to.</p> <p>mac-address—Client MAC address.</p>
Default Configuration	The client is locked until the silence interval is over.
Command Mode	Privileged EXEC mode.
Usage	To unlock a locked (in the quiet period) client, use the dot1x unlock client command in Privileged EXEC mode.
Example	switchxxxxxx# dot1x unlock client te1/0/1 00:01:12:af:00:56

User Guideline	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.
-----------------------	--

dot1x violation-mode

Syntax	dot1x violation-mode {restrict / protect / shutdown}no dot1x violation-mode
Parameters	<p>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.</p> <p>protect—Discards frames with source addresses that are not the supplicant address.</p> <p>shutdown—Discards frames with source addresses that are not the supplicant address and shutdown the port.</p>
Default Configuration	Protect.
Command Mode	Interface (Ethernet) Configuration mode.

Usage	<p>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 Configuration mode.</p> <p>To restore the default configuration, use the no form of this command.</p>
--------------	--

Example	switchxxxxxx(config)# interface te1/0/1 switchxxxxxx(config-if)# dot1x violation-mode protect
User Guideline	<p>The command is relevant only for single-host mode.</p> <p>For BPDU messages whose MAC addresses are not the supplicant MAC address are not discarded in Protect mode.</p> <p>BPDU message whose MAC addresses are not the supplicant MAC address cause a shutdown in Shutdown mode.</p>

show dot1x

Syntax	show dot1x [interface <i>interface-id</i> / detailed]
Parameters	<i>interface-id</i> —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. If the MAC-Based password is configured the dot1x mac-auth password command, its MD5 checksum is displayed, else the Username word is displayed.
Command Mode	Privileged EXEC mode.
Usage	To display the 802.1X interfaces or specified interface status, use the show dot1x command in Privileged EXEC mode.

Example	<p>The following example displays authentication information for all i nterfaces on which 802.1x is enabled:</p> <p>Authentication is enabled Critical VLAN: disabled</p> <p>Authenticator Global Configuration: Authenticating Servers: Radi us, None MAC-Based Authentication:</p> <p>Type: Eap</p> <p>Username Group size: 12 Username Separator: – Username cas e: Lowercase Password: MD5 checksum Unauthenticated VLANs :</p> <p>Authentication failure traps are enabled for 802.1x</p>
----------------	--

	<p>Authentication success traps are enabled for mac Authentication quiet traps are enabled Supplicant Global Configuration:</p> <p>Supplicant Authentication success traps are disabled Supplicant Authentication failure traps are disabled</p> <p>te1/0/1</p> <p>Authenticator is enabled Supplicant is disabled Authenticator Con figuration: Host mode: multi-host</p> <p>Authentication methods: 802.1x+mac Port Administrated Status: auto Guest VLAN: disabled</p> <p>VLAN Radius Attribute: disabled Open access: enabled</p> <p>Server timeout: 3600 sec</p> <p>Port Operational Status: unauthorized*</p>
--	---

	<p>Reauthentication is enabled Reauthentication period: 5000 sec Silence period: 0 sec</p> <p>Quiet period: 120 sec</p> <p>Interfaces 802.1X-Based Parameters Tx period: 60 sec</p> <p>Supplicant timeout: 3600 sec Max req: 6</p> <p>Authentication success: 0</p> <p>Authentication fails: 0 Supplicant Configuration: retry-max: 2</p> <p>EAP time period: 30</p> <p>Supplicant Held Period: 60</p>
User Guideline	—

show dot1x locked clients

Syntax	show dot1x locked clients
Parameters	N/A.
Default Configuration	—
Command Mode	Privileged EXEC mode.
Usage	<p>To display all clients who are locked and in the quiet period, use the</p> <p>show dot1xlocked clients command in Privileged EXEC mode.</p>

Example	The following example displays locked clients:		
	Port	MAC Address	Remaining Time
	te1/0/1	0008.3b79.8787	20
	te1/0/1	0008.3b89.3128	40
User Guideline	te1/0/2	0008.3b89.3129	10
	Use the show dot1x locked clients command to display all locked (in the quiet period) clients.		

show dot1x statistics

Syntax	show dot1x statistics interface <i>interface-id</i>
Parameters	<i>interface-id</i> — Specifies an Ethernet port or OOB port.
Default Configuration	N/A.
Command Mode	Privileged EXEC mode.
Usage	To display 802.1X statistics for the specified port, use the show dot1x statistics command in Privileged EXEC mode.

Example	<p>The following example displays 802.1X statistics for te1/0/1. switc hxxxxxx# show dot1x statistics interface te1/0/1</p> <p>EapolFramesRx: 11</p> <p>EapolFramesTx: 12</p> <p>EapolStartFramesRx: 1</p> <p>EapolLogoffFramesRx: 1</p> <p>EapolRespIldFramesRx: 3</p> <p>EapolRespFramesRx: 6</p> <p>EapolReqIldFramesTx: 3</p> <p>EapolReqFramesTx: 6</p> <p>InvalidEapolFramesRx: 0</p> <p>EapLengthErrorFramesRx: 0</p> <p>LastEapolFrameVersion: 1</p> <p>LastEapolFrameSource: 00:08:78:32:98:78</p> <p>The following table describes the significant fields shown in the di splay:</p>
---------	---

--	--

Field	Description
EapolFramesRx	Number of valid EAPOL frames of any type that have been received by this Authenticator.
EapolFramesTx	Number of EAPOL frames of any type that have been transmitted by this Authenticator.
EapolStartFramesRx	Number of EAPOL Start frames that have been received by this Authenticator.
EapolLogoffFramesRx	Number of EAPOL Logoff frames that have been received by this Authenticator.
EapolRespIdFramesRx	Number of EAP Resp/Id frames that have been received by this Authenticator.
EapolRespFramesRx	Number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
EapolReqIdFramesTx	Number of EAP Req/Id frames that have been transmitted by this Authenticator.
EapolReqFramesTx	Number of EAP Request frames (other than Req/Id frames) that have been transmitted by this Authenticator.
InvalidEapolFramesRx	Number of EAPOL frames that have been received by this Authenticator for which the frame type is not recognized.
EapLengthErrorFramesRx	Number of EAPOL frames that have been received by this Authenticator in which the Packet Body

	<p>y Length field is invalid</p> <p>LastEapolFrameVersion Protocol version number carried in the most recently received EAPOL frame.</p> <p>LastEapolFrameSource Source MAC address carried in the most recently received EAPOL frame.</p>
User Guideline	—

show dot1x users

Syntax	show dot1x users [username username]
Parameters	username <i>username</i> —Specifies the supplicant username (Length: 1–160 characters).
Default Configuration	Display all users.
Command Mode	Privileged EXEC mode.
Usage	To display active 802.1X authorized users for the device, use the show dot1x users command in Privileged EXEC mode.

Example

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

show dot1x users

Port	Username	MAC Address	Auth Method	Auth Server
Session Time	VLAN			
te1/0/1	Bob	0008.3b71.1111	802.1x	Remote
09:01:00	1020			
te1/0/2	John	0008.3b79.87871	802.1x	Remote
00:11:12	1020			
te1/0/3	George	0008.3baa.0022	802.1x	Remote
00:27:16	1020			

Example 2. The following example displays 802.1X user with sup plicant username.

Bob:

switchxxxxxx# **show dot1x users username Bob**

Port	Username	MAC Address	Auth Method	Auth Server	Session Time	VLAN
—						
te1/0/1	Bob	0008.3b71.1111	802.1x	Remote	09:01:00	1020

User Guideline

—

FAQs

Q: What is the purpose of 802.1X authentication?

A: 802.1X authentication provides secure access to the network by requiring user authentication before granting access.

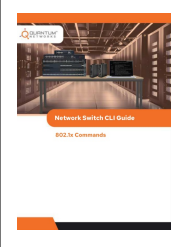
Q: How can I clear 802.1X statistics?

A: Use the 'clear dot1x statistics' command in Privileged EXEC mode to clear all counters displayed in the show dot1x and show dot1x statistics commands.

Q: Can I enable open access on specific ports?

A: Yes, you can enable open access (monitoring mode) on a specific port using the 'authentication open' command in Interface Configuration mode.

Documents / Resources

	QNTMNET QN-SW-325 Network Switch [pdf] User Guide not provided in the text, QN-SW-325 Network Switch, QN-SW-325, Network Switch, Switch
---	--

References

- [User Manual](#)

📁 quantum 📄 Network Switch, Not Provided In The Text, QN-SW-325, QN-SW-325 Network Switch, QNTMNET, switch

Leave a comment

Your email address will not be published. Required fields are marked *

Comment *

Name

Email

Website

☐ Save my name, email, and website in this browser for the next time I comment.

Post Comment

Search:

e.g. whirlpool wrf535swhz

Search

[Manuals+](#) | [Upload](#) | [Deep Search](#) | [Privacy Policy](#) | [@manuals.plus](#) | [YouTube](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.