Network Switch CLI Guide

802.1x Commands

Contents

802.1x Commands

aaa authentication dot1x

Syntax	**aaaauthenticationdot1xdefault{radius|none|{radiusnone}}** **no aaa authentication dot1xdefault**
Parameters	**radius** - Uses the list of all RADIUS servers for authentication. **none-** Uses no authentication.
Default Configuration	Radius Server.
Command Mode	Global configuration mode.
Usage	To specify which servers are used for authentication when 802.1X authentication is enabled, use the **aaa authentication dot1x** command in Global Configurationmode. To restore the default configuration, use the **no** form of this command.
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
User Guideline	User 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.

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 **authenticationopen** 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 [***interface-id***]**
Parameters	***interface-id***–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	This command clears all the counters displayed in the **show dot1x** and **show dot1x statistics** command.

dot1x authentication

Syntax	**dot1xauthentication[802.1x][mac]** **no dot1xauthentication**
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).
Default Configuration	X-Based authentication is enabled.
Command Mode	Interface (Ethernet) Configuration mode.
Usage	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.
Example	The following example enables authentication based on 802.1x and the station's MAC address on portte1/0/1: switchxxxxxx(config)# **interface** te1/0/**1** switchxxxxxx(config-if)# **dot1x authentication 802.1x mac**
User Guideline	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: If a dynamic MAC address authenticated by MAC-based authentication is changed to a static one, it will not be manually re-authenticated. Removing a dynamic MAC address authenticated by the MAC-based authentication causes its re-authentication.

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	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.
Example	The following example defines VLAN 2 as a guest VLAN. switchxxxxxx(config)# **interface** vlan 2 switchxxxxxx(config-if)# **dot1x guest-vlan**
User Guideline	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.

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	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.
Example	The following example enables unauthorized users on te1/0/1 to access the guestVLAN. switchxxxxxx(config)# **interface** te1/0/1 switchxxxxxx(config-if)# **dot1x guest-vlan enable**
User Guideline	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. See the User Guidelines of the **dot1x host-mode** command for more information.

dot1x guest-vlan timeout

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.
Usage	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.
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
User Guideline	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.

dot1x host-mode

Syntax	dot1x host-mode {multi-host / single-host / multi-sessions}
Parameters	**multi-host**–Enables multiple-hosts mode. **single-host**–Enables single-hosts mode. **multi-sessions**–Enables multiple-sessions mode.
Default Configuration	Default mode is multi-host.
Command Mode	Interface (Ethernet) Configuration mode.
Usage	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.
Example	switchxxxxxx(config)# **interface** te1/0/1 switchxxxxxx(config-if)# **dot1x host-mode multi-host**
User Guideline	**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 re mapped 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. 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-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. 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 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 theTCAM, 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 authorized to unauthorized. The MAC address will be removed after the aging timeout expires.

dot1x max-hosts

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.
Usage	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.
Example	The following example limits the maximum number of authorized hosts on Ethernet port te1/0/1 to 6: switchxxxxxx(config)# **interface** te1/0/1 switchxxxxxx(config-if)# **dot1x max-hosts 6**
User Guideline	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 dot1xmax-hosts** command. This command is relevant only for multi-session mode.

dot1x max-req

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.
Usage	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.
Example	The following example sets the maximum number of times that the device sends an EAP request/identity frame to 6. switchxxxxxx(config)# **interface** te1/0/1 switchxxxxxx(config-if)# **dot1x max-req** 6
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	**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.
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	The following example sets 802.1X authentication on te1/0/1 to auto mode. switchxxxxxx(config)# **interface** te1/0/1 switchxxxxxx(config-if)# **dot1x port-control auto**
User Guideline	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 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.

dot1x re-authenticate

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.
Usage	To initiate manually re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port, use the **dot1x re-authenticate** commandinPrivilegedEXECmode.
Example	The following command manually initiates re-authentication of 802.1X-enabledte1/0/1: switchxxxxxx# **dot1x re-authenticate** te1/0/1
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	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.
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	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.
Example	The following example enables 802.1X globally. switchxxxxxx(config)# **dot1x system-auth-control**
User Guideline	-

dot1x timeout quiet-period

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.
Usage	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.
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** te1/0/1 switchxxxxxx(config-if)# **dot1x timeout quiet-period 120**
User Guideline	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 quiet period is applied after each failed attempt.

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	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.
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 *seconds*** **no dot1x timeout reauth-period**
Parameters	**reauth-period *seconds***–Number of seconds between re-authenticationattempts. (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	switchxxxxxx(config)# **interface** te1/0/1 switchxxxxxx(config-if)# **dot1x timeout reauth-period** 5000
User Guideline	The command is only applied to the 802.1x authentication method.

dot1x timeout server-timeout

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.
Usage	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. To restore the default configuration, use the **no** form of this command.
Example	The following example sets the time interval between retransmission of packets tothe authentication server to 3600 seconds.

	switchxxxxxx(config)# **interface** te1/0/1 switchxxxxxx(config-if)# **dot1x timeout server-timeout** 3600
User Guideline	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.

dot1x timeout supp-timeout

Syntax	**dot1x timeout supp-timeout *seconds*** **no dot1x timeout supp-timeout**
Parameters	**supp-timeout *seconds***–Specifies the time interval in seconds duringwhich 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.
Usage	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.
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 to3600 seconds. switchxxxxxx(config)# **interface** te1/0/1 switchxxxxxx(config-if)# **dot1x timeout supp-timeout** 3600
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. The command is only applied to the 802.1x authentication method.

dot1x timeout tx-period

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.
Usage	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.
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** te1/0/1 switchxxxxxx(config-if)# **dot1x timeout tx-period 60**
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. The command is only applied to the 802.1x authentication method.

dot1x traps authentication failure

Syntax	**dot1xtrapsauthenticationfailure{[802.1x][mac]}** **no dot1x traps authenticationfailure**
Parameters	**802.1x**—Enables traps for 802.1X-based authentication. **mac**—Enables traps for MAC-based authentication.
Default Configuration	All traps are disabled.
Command Mode	Global Configuration mode.
Usage	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.
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**
User Guideline	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.

dot1x traps authentication quiet

Syntax	**dot1x traps authentication quiet** **no dot1x traps authentication quiet**
Parameters	N/A.
Default Configuration	Quiet traps are disabled.
Command Mode	Global Configuration mode.
Usage	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.

Example	The following example enables sending traps when a host is set in the quiet state: switchxxxxxx(config)# **dot1x traps authentication quiet**
User Guideline	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.

dot1x traps authentication success

Syntax	**dot1xtrapsauthenticationsuccess{[802.1x][mac]}** **no dot1x traps authenticationsuccess**
Parameters	**802.1x**—Enables traps for 802.1X-based authentication. **mac**—Enables traps for MAC-based authentication.
Default Configuration	Success traps are disabled.
Command Mode	Global Configuration mode.
Usage	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.
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**
User Guideline	Any combination of the keywords are allowed. At least one keyword must beconfigured. A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

dot1x unlock client

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.
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 thequiet period, the command has no affect.

dot1x violation-mode

Syntax	**dot1x violation-mode {restrict / protect / shutdown}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**—Discards frames with source addresses that are not the supplicant address. **shutdown**—Discards frames with source addresses that are not the supplicant address and shutdown the port.
Default Configuration	Protect.
Command Mode	Interface (Ethernet) Configuration mode.

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

show dot1x

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. If the MAC-Based password is configured the **dot1x mac-auth password** command, its MD5 checksum is displayed, else he Usernameword 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	The following example displays authentication information for all interfaces on which 802.1x is enabled: Authentication is enabled Critical VLAN: disabled Authenticator Global Configuration: Authenticating Servers: Radius, None MAC-Based Authentication: Type: Eap Username Group size: 12 Username Separator: - Username case: Lowercase Password: MD5 checksum Unauthenticated VLANs: Authentication failure traps are enabled for 802.1x

	Authentication success traps are enabled for mac Authentication quiet traps are enabled Supplicant Global Configuration: Supplicant Authentication success traps are disabled Supplicant Authentication failure traps are disabled te1/0/1 Authenticator is enabled Supplicant is disabled Authenticator Configuration: Host mode: multi-host Authentication methods: 802.1x+mac Port Administrated Status: auto Guest VLAN: disabled VLAN Radius Attribute: disabled Open access: enabled Server timeout: 3600 sec Port Operational Status: unauthorized* Reauthentication is enabled Reauthentication period: 5000 sec Silence period: 0 sec Quiet period: 120 sec Interfaces 802.1X-Based Parameters Tx period: 60 sec Supplicant timeout: 3600 sec Max req: 6 Authentication success: 0 Authentication fails: 0 Supplicant Configuration: retry-max: 2 EAP time period: 30 Supplicant Held Period: 60
User Guideline	-

show dot1x locked clients

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

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 te1/0/2 0008.3b89.3129 10
User Guideline	Use the **show dot1x locked clients** command to display all locked (in the quiet period) clients.

show dot1x statistics

Syntax	**show dot1x statistics interface** *interface-id*
Parameters	***interface-id*** – 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 EXECmode.
Example	The following example displays 802.1X statistics for te1/0/1. switchxxxxxx# **show dot1x statistics interface te1/0/1** EapolFramesRx: 11 EapolFramesTx: 12 EapolStartFramesRx: 1 EapolLogoffFramesRx: 1 EapolRespIdFramesRx: 3 EapolRespFramesRx: 6 EapolReqIdFramesTx: 3 EapolReqFramesTx: 6 InvalidEapolFramesRx: 0 EapLengthErrorFramesRx: 0 LastEapolFrameVersion: 1 LastEapolFrameSource: 00:08:78:32:98:78 The following table describes the significant fields shown in the display:

Field	Description
EapolFramesRx	Number of valid EAPOL frames of anytype that have been received by this Authenticator.
EapolFramesTx	Number of EAPOL frames of any typethat 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 thathave been received by this Authenticator.
EapolRespIdFramesRx	Number of EAP Resp/Id frames thathave been received by this Authenticator.
EapolRespFramesRx	Number of valid EAP Response frames(other than Resp/Id frames) that havebeen received by this Authenticator.
EapolReqIdFramesTx	Number of EAP Req/Id frames that havebeen transmitted by this Authenticator.
EapolReqFramesTx	Number of EAP Request frames (otherthan Req/Id frames) that have been transmitted by this Authenticator.
InvalidEapolFramesRx	Number of EAPOL frames that have been received by this Authenticator forwhich the frame type is not recognized.
EapLengthErrorFramesRx	Number of EAPOL frames that havebeen received by this Authenticator in which the Packet Body Length field is invalid
LastEapolFrameVersion	Protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	Source MAC address carried in the most recently received EAPOL frame.

User Guideline	–

show dot1x users

Syntax	**show dot1x users [username username]**
Parameters	**username** *username*—Specifies the supplicant username (Length: 1–160characters).
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 supplicant 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	-