



dnsix-dmdp retries through dynamic

- [domain \(AAA\), page 2](#)
- [dot1x control-direction, page 4](#)
- [dot1x credentials, page 7](#)
- [dot1x critical \(global configuration\), page 9](#)
- [dot1x critical \(interface configuration\), page 11](#)
- [dot1x default, page 12](#)
- [dot1x guest-vlan, page 15](#)
- [dot1x guest-vlan supplicant, page 17](#)
- [dot1x initialize, page 18](#)
- [dot1x mac-auth-bypass, page 20](#)
- [dot1x max-reauth-req, page 22](#)
- [dot1x max-req, page 24](#)
- [dot1x multiple-hosts, page 27](#)
- [dot1x pae, page 29](#)
- [dot1x port-control, page 31](#)
- [dot1x re-authenticate \(privileged EXEC\), page 35](#)
- [dot1x reauthentication, page 37](#)
- [dot1x re-authentication \(EtherSwitch\), page 40](#)
- [dot1x system-auth-control, page 42](#)
- [dot1x timeout, page 44](#)
- [dot1x timeout \(EtherSwitch\), page 50](#)

domain (AAA)

To configure username domain options for the RADIUS application, use the **domain** command in dynamic authorization local server configuration mode. To disable the username domain options configured, use the **no** form of this command.

domain {*delimiter character*| **stripping** [**right-to-left**]}

no domain {*delimiter character*| **stripping** [**right-to-left**]}

Syntax Description

delimiter <i>character</i>	Specifies the domain delimiter. One of the following options can be specified: @, /, \$, %, \, # or -
stripping	Compares the incoming username with the names oriented to the left of the @ domain delimiter.
right-to-left	Terminates the string at the first delimiter going from right to left.

Command Default

No username domain options are configured.

Command Modes

Dynamic authorization local server configuration (config-locsvr-da-radius)

Command History

Release	Modification
12.2(31)SB14	This command was introduced.
12.2(33)SRC5	This command was integrated into Cisco IOS Release 12.2(33)SRC5.
Cisco IOS XE Release 2.3	This command was modified. This command was implemented on ASR 1000 series routers.
15.1(2)T	This command was integrated into Cisco IOS Release 15.1(2)T. This command was also modified. The right-to-left keyword was added.

Usage Guidelines

If domain stripping is not configured, the full username provided in the authentication, authorization, and accounting (AAA) packet of disconnect (POD) messages is compared with the online subscribers. Configuring domain stripping allows you to send disconnect messages with only the username present before the @ domain delimiter. The network access server (NAS) compares and matches this username with any online subscriber with a potential domain.

For instance, when domain stripping is configured and you send a POD message with the username “test,” a comparison between the POD message and online subscribers takes place, and subscribers with the username “test@cisco.com” or “test” match the specified username “test.”

Examples

The following configuration example is used to match a username from right to left. If the username is user1@cisco.com@test.com, then the username to be matched by the POD message is user1@cisco.com.

```
Router# configure terminal
Router(config)# aaa server radius dynamic-author
Router(config-locsvr-da-radius)# domain stripping right-to-left
Router(config-locsvr-da-radius)# domain delimiter @
Router(config-locsvr-da-radius)# end
```

The following configuration example is used to match a username from left to right. If the username is user1@cisco.com@test.com, then the username to be matched by the POD message is user1.

```
Router# configure terminal
Router(config)# aaa server radius dynamic-author
Router(config-locsvr-da-radius)# domain stripping
Router(config-locsvr-da-radius)# domain delimiter @
Router(config-locsvr-da-radius)# end
```

Related Commands

Command	Description
aaa server radius dynamic-author	Configures a device as a AAA server to facilitate interaction with an external policy server.

dot1x control-direction



Note

Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x control-direction** command is replaced by the **authentication control-direction** command. See the **authentication control-direction** command for more information.

To change an IEEE 802.1X controlled port to unidirectional or bidirectional, use the **dot1x control-direction** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

dot1x control-direction {both| in}

no dot1x control-direction

Syntax Description

both	Enables bidirectional control on the port.
in	Enables unidirectional control on the port.

Command Default

The port is set to bidirectional mode.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(25)SEC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Switches (ISRs) only.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was replaced by the authentication control-direction command.

Usage Guidelines

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making

available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

Unidirectional State

When you configure a port as unidirectional with the **dot1x control-direction in** interface configuration command, the port changes to the spanning-tree forwarding state.

When Unidirectional Controlled Port is enabled, the connected host is in the sleeping mode or power-down state. The host does not exchange traffic with other devices in the network. The host connected to the unidirectional port cannot send traffic to the network, the host can only receive traffic from other devices in the network.

Bidirectional State

When you configure a port as bidirectional with the **dot1x control-direction both** interface configuration command, the port is access-controlled in both directions. In this state, the switch port receives or sends only EAPOL packets; all other packets are dropped.

Using the **both** keyword or using the **no** form of this command changes the port to its bidirectional default setting.

Catalyst 6500 Series Switch

Setting the port as bidirectional enables 802.1X authentication with wake-on-LAN (WoL).

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows how to enable unidirectional control:

```
Switch(config-if) # dot1x control-direction in
```

The following examples show how to enable bidirectional control:

```
Switch(config-if) # dot1x control-direction both
or
```

```
Switch(config-if) # no dot1x control-direction
```

You can verify your settings by entering the show dot1x all privileged EXEC command. The show dot1x all command output is the same for all devices except for the port names and the state of the port. If a host is attached to the port but is not yet authenticated, a display similar to the following appears:

```
Supplicant MAC 0002.b39a.9275
AuthSM State = CONNECTING
BendsM State = IDLE
PortStatus = UNAUTHORIZED
```

If you enter the dot1x control-direction in command to enable unidirectional control, the following appears in the show dot1x all command output:

```
ControlDirection = In
```

If you enter the dot1x control-direction in command and the port cannot support this mode because of a configuration conflict, the following appears in the show dot1x all command output:

```
ControlDirection = In (Disabled due to port settings):
```

The following example shows how to reset the global 802.1X parameters:

```
Switch(config)# dot1x default
```

Examples

The following example shows how to enable 802.1X authentication with WoL and set the port as bidirectional:

```
Switch(config)# interface gigabitethernet 5/1
Switch(config-if)# dot1x control-direction both
```

Examples

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
description switchport connect to a client
!
interface FastEthernet1
description switchport connect to a client
!
interface FastEthernet2
description switchport connect to a client
!
interface FastEthernet3
description switchport connect to a client
!
interface FastEthernet4
description Connect to the public network
!
interface Vlan1
description Apply 802.1x functionality on SVI
dot1x pae authenticator
dot1x port-control auto
dot1x reauthentication
dot1x control-direction in
```

Related Commands

Command	Description
show dot1x	Displays details for an identity profile.

dot1x credentials

To specify which 802.1X credential profile to use when configuring a supplicant (client) or to apply a credentials structure to an interface and to enter dot1x credentials configuration mode, use the **dot1x credentials** command in global configuration or interface configuration mode. To remove the credential profile, use the **no** form of this command.

dot1x credentials *name*

no dot1x credentials

Syntax Description

<i>name</i>	Name of the credentials profile.
-------------	----------------------------------

Command Default

A credentials profile is not specified.

Command Modes

Global configuration Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

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

Examples

The following example shows which credentials profile should be used when configuring a supplicant:

```
dot1x credentials basic-user
username router
password secret
description This credentials profile should be used for most configured ports
```

The credentials structure can be applied to an interface, along with the **dot1x pae supplicant** command and keyword, to enable supplicant functionality on that interface.

```
interface fastethernet 0/1
dot1x credentials basic-user
dot1x pae supplicant
```

Related Commands

Command	Description
anonymous-id (dot1x credential)	Specifies the anonymous identity that is associated with a credentials profile.

Command	Description
description (dot1x credential)	Specifies the description for an 802.1X credentials profile.
password (dot1x credential)	Specifies the password for an 802.1X credentials profile.
username (dot1x credential)	Specifies the username for an 802.1X credentials profile.

dot1x critical (global configuration)

To configure the IEEE 802.1X critical authentication parameters, use the **dot1x critical** command in global configuration mode.

dot1x critical {**eapol**| **recovery delay** *milliseconds*}

Syntax Description

eapol	Specifies that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port.
recovery delay <i>milliseconds</i>	Specifies the recovery delay period that the switch waits to reinitialize a critical port when an unavailable RADIUS server becomes available; valid values are from 1 to 10000, in milliseconds.

Command Default

The default settings are as follows:

- **eapol** --Disabled
- *milliseconds* --1000 milliseconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SXI	The recovery delay keyword was replaced by the authentication critical recovery delay command.

Examples

This example shows how to specify that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port:

```
Switch(config)# dot1x critical eapol
```

This example shows how to set the recovery delay period that the switch waits to reinitialize a critical port when an unavailable RADIUS server becomes available:

```
Switch(config)# dot1x critical recovery delay 1500
```

Related Commands

Command	Description
dot1x critical (interface configuration)	Enables 802.1X critical authentication on an interface.

dot1x critical (interface configuration)

To enable 802.1X critical authentication, and optionally, 802.1X critical authentication recovery and authentication, on an interface, use the **dot1x critical** command in interface configuration mode. To disable 802.1X critical authentication, and optionally, 802.1X critical authentication recovery and authentication, use the **no** form of this command.

dot1x critical [recovery action reinitialize]

no dot1x critical [recovery action reinitialize]

Syntax Description

recovery action reinitialize	(Optional) Enables 802.1X critical authentication recovery and specifies that the port is authenticated when an authentication server is available.
-------------------------------------	---

Command Default

The 802.1X critical authentication is enabled on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Examples

This example shows how to enable 802.1X critical authentication on an interface:

```
Router(config-if)# dot1x critical
```

This example shows how to enable 802.1X critical authentication recovery and authenticate the port when an authentication server is available:

```
Router(config-if)# dot1x critical recovery action reinitialize
```

This example shows how to disable 802.1X critical authentication on an interface:

```
Router(config-if)# no  
dot1x critical
```

Related Commands

Command	Description
dot1x critical (global configuration)	Configures the 802.1X critical authentication parameters.

dot1x default

To reset the global 802.1X authentication parameters to their default values as specified in the latest IEEE 802.1X standard, use the **dot1x default** command in global configuration or interface configuration mode.

dot1x default

Syntax Description

This command has no arguments or keywords.

Command Default

The default values are as follows:

- The per-interface 802.1X protocol enable state is disabled (force-authorized).
- The number of seconds between reauthentication attempts is 3600 seconds.
- The quiet period is 60 seconds.
- The retransmission time is 30 seconds.
- The maximum retransmission number is 2 times.
- The multiple host support is disabled.
- The client timeout period is 30 seconds.
- The authentication server timeout period is 30 seconds.

Command Modes

Global configuration (config) Interface configuration (config-if)

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	This command was implemented on the Supervisor Engine 720 in Cisco IOS Release 12.2(14)SX.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 in Cisco IOS Release 12.2(17d)SXB.
12.4(6)T	Interface configuration was added as a configuration mode for this command.

Release	Modification
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

Use the **show dot1x** command to verify your current 802.1X settings.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows how to reset the global 802.1X parameters:

```
Router(config)# dot1x default
```

The following example show how to reset the global 802.1X parameters on FastEthernet interface 0:

```
Router(config)# interface FastEthernet0
Router(config-if)# dot1x default
```

Related Commands

Command	Description
dot1x critical (global configuration)	Configures the 802.1X critical authentication parameters.
dot1x critical (interface configuration)	Enables 802.1X critical authentication on an interface.
dot1x max-req	Sets the maximum number of times that the device sends an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
dot1x re-authentication (EtherSwitch)	Enables periodic reauthentication of the client for the Ethernet switch network module.

Command	Description
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.
show dot1x	Displays 802.1X information.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x guest-vlan

To specify an active VLAN as an IEEE 802.1x guest VLAN, use the **dot1x guest-vlan** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

dot1x guest-vlan vlan-id

no dot1x guest-vlan

Syntax Description

<i>vlan-id</i>	Specify an active VLAN as an IEEE 802.1x guest VLAN. The range is 1 to 4094.
----------------	--

Command Default

No guest VLAN is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)EA1	This command was introduced.
12.2(25)SE	This command was modified to change the default guest VLAN behavior.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

You can configure a guest VLAN on a static-access port.

For each IEEE 802.1x port, you can configure a guest VLAN to provide limited services to clients (a device or workstation connected to the switch) not running IEEE 802.1x authentication. These users might be upgrading their systems for IEEE 802.1x authentication, and some hosts, such as Windows 98 systems, might not be IEEE 802.1x capable.

When you enable a guest VLAN on an IEEE 802.1x port, the software assigns clients to a guest VLAN when it does not receive a response to its Extensible Authentication Protocol over LAN (EAPOL) request/identity frame or when EAPOL packets are not sent by the client.

With Cisco IOS Release 12.4(11)T and later, the switch port maintains the EAPOL packet history. If another EAPOL packet is detected on the interface during the lifetime of the link, the guest VLAN feature is disabled.

If the port is already in the guest VLAN state, the port returns to the unauthorized state, and authentication restarts. The EAPOL history is reset upon loss of link.

Any number of non-IEEE 802.1x-capable clients are allowed access when the switch port is moved to the guest VLAN. If an IEEE 802.1x-capable client joins the same port on which the guest VLAN is configured, the port is put into the unauthorized state in the RADIUS-configured or user-configured access VLAN, and authentication is restarted.

Guest VLANs are supported on IEEE 802.1x switch ports in single-host or multi-host mode.

You can configure any active VLAN except a Remote Switched Port Analyzer (RSPAN) VLAN or a voice VLAN as an IEEE 802.1x guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

After you configure a guest VLAN for an IEEE 802.1x port to which a DHCP client is connected, you might need to get a host IP address from a DHCP server. You can change the settings for restarting the IEEE 802.1x authentication process on the switch before the DHCP process on the client times out and tries to get a host IP address from the DHCP server. You should decrease the settings for the IEEE 802.1x authentication process using the **dot1x max-reauth-req** and **dot1x timeout tx-period** interface configuration commands. The amount of decrease depends on the connected IEEE 802.1x client type.

Examples

This example shows how to specify VLAN 5 as an IEEE 802.1x guest VLAN:

```
Switch(config-if) # dot1x guest-vlan 5
```

This example shows how to set 3 as the quiet time on the switch, to set 15 as the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request, and to enable VLAN 2 as an IEEE 802.1x guest VLAN when an IEEE 802.1x port is connected to a DHCP client:

```
Switch(config-if) # dot1x timeout max-reauth-req 3
Switch(config-if) # dot1x timeout tx-period 15
Switch(config-if) # dot1x guest-vlan 2
```

You can display the IEEE 802.1x administrative and operational status for the device or for the specified interface by entering the **show dot1x interface *interface-id***] privileged EXEC command.

Related Commands

Command	Description
dot1x max-reauth-req	Specifies the number of times that the switch retransmits an EAP-request/identity frame to the client before restarting the authentication process.
dot1x timeout	Sets authentication retry timeouts.
show dot1x	Displays details for an identity profile.

dot1x guest-vlan supplicant

To allow the 802.1x-capable supplicants to enter the guest VLAN, use the **dot1x guest-vlan supplicant** command in global configuration mode. To prevent the 802.1x-capable supplicants from entering the guest VLAN, use the **no** form of this command.

dot1x guest-vlan supplicant

no dot1x guest-vlan supplicant

Syntax Description This command has no arguments or keywords.

Command Default The 802.1x-capable supplicants are prevented from entering the guest VLAN.

Command Modes Global configuration (config)

Release	Modification
12.2(33)SXH	This command was introduced.

Examples This example shows how to allow the 802.1x-capable supplicants to enter the guest VLAN:

```
Router(config)# dot1x guest-vlan supplicant
```

This example shows how to prevent the 802.1x-capable supplicants from entering the guest VLAN:

```
Router(config)# no dot1x guest-vlan supplicant
```

Command	Description
dot1x critical (global configuration)	Configures the 802.1X critical authentication parameters.
dot1x critical (interface configuration)	Enables 802.1X critical authentication on an interface.

dot1x initialize



Note

Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x initialize** command is replaced by the **clear authentication session** command. See the **clear authentication session** command for more information.

To initialize 802.1X clients on all 802.1X-enabled interfaces, use the **dot1x initialize** command in privileged EXEC mode. This command does not have a **no** form.

dot1x initialize [*interface interface-name*]

Syntax Description

interface <i>interface-name</i>	(Optional) Specifies an interface to be initialized. If this keyword is not entered, all interfaces are initialized.
--	--

Command Default

State machines are not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)EA1	This command was introduced.
12.3(2)XA	This command was integrated into Cisco IOS Release 12.3(2)XA.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Use this command to initialize the 802.1X state machines and to set up a fresh environment for authentication. After you enter this command, the port status becomes unauthorized.

Examples

The following example shows how to manually initialize a port:

```
Router# dot1x initialize interface gigabitethernet2/0/2
```

You can verify the unauthorized port status by entering the **show dot1x** [*interface interface-name*] command.

Related Commands

Command	Description
show dot1x	Displays details for an identity profile.

dot1x mac-auth-bypass

To enable a switch to authorize clients based on the client MAC address, use the **dot1x mac-auth-bypass** command in interface configuration mode. To disable MAC authentication bypass, use the **no** form of this command.

dot1x mac-auth-bypass [eap]

no dot1x mac-auth-bypass

Syntax Description

eap	(Optional) Configures the switch to use Extensible Authentication Protocol (EAP) for authorization.
------------	---

Command Default

MAC authentication bypass is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Note

To use MAC authentication bypass on a routed port, ensure that MAC address learning is enabled on the port.

When the MAC authentication bypass feature is enabled on an 802.1X port, the switch uses the MAC address as the client identity. The authentication server has a database of client MAC addresses that are allowed network access. If authorization fails, the switch assigns the port to the guest VLAN if a VLAN is configured.

Examples

This example shows how to enable MAC authentication bypass:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x mac-auth-bypass
```

This example shows how to configure the switch to use EAP for authorization:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x mac-auth-bypass eap
```

This example shows how to disable MAC authentication bypass:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# no dot1x mac-auth-bypass
```

Related Commands

Command	Description
dot1x critical (global configuration)	Configures the 802.1X critical authentication parameters.
dot1x critical (interface configuration)	Enables 802.1X critical authentication on an interface.

dot1x max-reauth-req

To set the maximum number of times the authenticator sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client, use the **dot1x max-reauth-req** command in interface configuration mode. To set the maximum number of times to the default setting of 2, use the **no** form of this command.

dot1x max-reauth-req *number*

no dot1x max-reauth-req

Syntax Description

<i>number</i>	Maximum number of times. The range is 1 through 10. The default is 2.
---------------	---

Command Default

The command default is 2.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SE	This command was introduced.
12.2(25)SEC	The <i>number</i> argument was added.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.

Usage Guidelines

You should change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Verifying Settings

You can verify your settings by entering the show dot1x [interface interface-id] command.

Examples

The following example shows how to set 4 as the number of times that the authentication process is restarted before changing to the unauthorized state:

```
Router(config-if)# dot1x max-reauth-req 4
```

Examples

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
  description switchport connect to a client
!
interface FastEthernet1
  description switchport connect to a client
!
interface FastEthernet2
  description switchport connect to a client
!
interface FastEthernet3
  description switchport connect to a client
!
interface FastEthernet4
  description Connect to the public network
!
interface Vlan1
  description Apply 802.1x functionality on SVI
  dot1x pae authenticator
  dot1x port-control auto
  dot1x reauthentication
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a device can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process .
dot1x timeout tx-period	Sets the number of seconds that the switch waits for a response to an EAP request or identity frame from the client before resending the request.
show dot1x	Displays IEEE 802.1X status for the specified port.

dot1x max-req

To set the maximum number of times that a networking device or Ethernet switch network module can send an Extensible Authentication Protocol (EAP) request/identity frame to a client (assuming that a response is not received) before restarting the authentication process, use the **dot1x max-req** command in interface configuration or global configuration mode. To set the number of times to the default setting of 2, use the **no** form of this command.

dot1x max-req *retry-number*

no dot1x max-req

Syntax Description

retry-number	Maximum number of retries. The value is from 1 through 10. The default value is 2. The value is applicable to all EAP packets except for Request ID.
--------------	--

Command Default

The default number of retries is 2.

Command Modes

Interface configuration (config-if) Global configuration (config)

Command History

Release	Modification
12.1(6)EA2	This command was introduced on the Cisco Ethernet switch network module.
12.2(14)SX	This command was implemented on the Supervisor Engine 720 in Cisco IOS Release 12.2(14)SX.
12.2(15)ZJ	This command was implemented on the Cisco Ethernet switch network module on the following platforms in Cisco IOS Release 12.2(15)ZJ: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.
12.1(11)AX	This command was integrated into Cisco IOS Release 12.1(11)AX.
12.1(14)EA1	This command was integrated into Cisco IOS Release 12.1(14)EA1 and the configuration mode was changed to interface configuration mode except on the EtherSwitch network module.
12.3(2)XA	This command was integrated into Cisco IOS Release 12.3(2)XA and implemented on the following router platforms: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.

Release	Modification
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T and implemented on the following router platforms: Cisco 1751, Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 in Cisco IOS Release 12.2(17d)SXB.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.(33)SXH.

Usage Guidelines

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.



Note

You should change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows that the maximum number of times that the networking device will send an EAP request or identity message to the client PC is 6:

```
Router(config) configure terminal
Router(config)# interface ethernet 0
Router(config-if)# dot1x max-req 6
```

The following example shows how to set the number of times that a switch sends an EAP request or identity frame to 5 before restarting the authentication process:

```
Router(config-if)# dot1x max-req 5
```

Related Commands

Command	Description
dot1x port-control	Enables manual control of the authorization state of a controlled port.
dot1x re-authentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
dot1x reauthentication (EtherSwitch)	Enables periodic reauthentication of the Ethernet switch network module client on the 802.1X interface.
dot1x timeout	Sets retry timeouts.
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.
show dot1x	Displays details for an identity profile.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x multiple-hosts

**Note**

This command was replaced by the **dot1x host-mode** command effective with Cisco IOS Release 12.1(14)EA1 and Release 12.4(6)T.

To allow multiple hosts (clients) on an 802.1X-authorized switch port that has the **dot1x port-control** interface configuration command set to **auto**, use the **dot1x multiple-hosts** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

dot1x multiple-hosts

no dot1x multiple-hosts

Syntax Description

This command has no arguments or keywords.

Command Default

Multiple hosts are disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.1(14)EA1	This command was replaced by the dot1x host-mode command in Cisco IOS Release 12.1(14)EA1.
12.4(6)T	This command was replaced by the dot1x host-mode command on the T-train.

Usage Guidelines

This command is supported only on switch ports.

This command enables you to attach multiple clients to a single 802.1X-enabled port. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (reauthentication fails or an Extensible Authentication Protocol over LAN [EAPOL]-logoff message is received), all attached clients are denied access to the network.

Use the **show dot1x(EtherSwitch)** privileged EXEC command with the **interface** keyword to verify your current 802.1X multiple host settings.

Examples

The following example shows how to enable 802.1X on Fast Ethernet interface 0/1 and to allow multiple hosts:

```
Router(config)# interface fastethernet0/1
Router(config-if)# dot1x port-control auto
Router(config-if)# dot1x multiple-hosts
```

Related Commands

Command	Description
dot1x default	Enables manual control of the authorization state of the port.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x pae

To set the Port Access Entity (PAE) type, use the **dot1x pae** command in interface configuration mode. To disable the PAE type that was set, use the **no** form of this command.

dot1x pae [supplicant| authenticator| both]

no dot1x pae [supplicant| authenticator| both]

Syntax Description

supplicant	(Optional) The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.
authenticator	(Optional) The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.
both	(Optional) The interface behaves both as a supplicant and as an authenticator and thus will respond to all dot1x messages.

Command Default

PAE type is not set.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **dot1x system-auth-control** command has not been configured, the **supplicant** keyword will be the only keyword available for use with this command. (That is, if the **dot1x system-auth-control** command has not been configured, you cannot configure the interface as an authenticator.)

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows that the interface has been set to act as a supplicant:

```
Router (config)# interface Ethernet1
Router (config-if)# dot1x pae supplicant
```

Examples

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
description switchport connect to a client
!
interface FastEthernet1
description switchport connect to a client
!
interface FastEthernet2
description switchport connect to a client
!
interface FastEthernet3
description switchport connect to a client
!
interface FastEthernet4
description Connect to the public network
!
interface Vlan1
description Apply 802.1x functionality on SVI
dot1x pae authenticator
dot1x port-control auto
dot1x reauthentication
```

Related Commands

Command	Description
dot1x system-auth-control	Enables 802.1X SystemAuthControl (port-based authentication).
interface	Configures an interface type.

dot1x port-control



Note

Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x port-control** command is replaced by the **authentication port-control** command. See the **authentication port-control** command for more information.

To enable manual control of the authorization state of a controlled port, use the **dot1x port-control** command in interface configuration mode. To disable the port-control value, use the **no** form of this command.

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

no dot1x port-control

Syntax Description

auto	Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.
force-authorized	Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The force-authorized keyword is the default.
force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.

Command Default

The default is force-authorized.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced for the Cisco Ethernet switch network module.
12.1(11)AX	This command was integrated into Cisco IOS Release 12.1(11)AX.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.

Release	Modification
12.2(15)ZJ	This command was implemented on the following platforms for the Cisco Ethernet switch network module: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.
12.3(2)XA	This command was introduced on the following Cisco Switches: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. Switch support was added for the following platforms: Cisco 1751, Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was added for Cisco IOS Release 12.2(17d)SXB.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Switches (ISRs) only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was replaced by the authentication port-control command.

Usage Guidelines

For Ethernet Switch Network Modules

The following guidelines apply to Ethernet switch network modules:

- The 802.1X protocol is supported on Layer 2 static-access ports.
- You can use the **auto** keyword only if the port is not configured as one of these types:
 - Trunk port--If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
 - EtherChannel port--Before enabling 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable 802.1X on an EtherChannel or on an active port in an EtherChannel, an error appears, and 802.1X is not enabled. If you enable 802.1X on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.
 - Switch Port Analyzer (SPAN) destination port--You can enable 802.1X on a port that is a SPAN destination port; however, 802.1X is disabled until the port is removed as a SPAN destination. You can enable 802.1X on a SPAN source port.

To globally disable 802.1X on the device, you must disable it on each port. There is no global configuration command for this task.

For Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Verifying Settings

You can verify your settings by entering the **show dot1x** command and checking the Status column in the 802.1X Port Summary section of the display. An enabled status means that the port-control value is set to auto or to force-unauthorized.

Examples

The following example shows that the authentication status of the client PC will be determined by the authentication process:

```
Switch(config)# configure terminal
Switch(config)# interface ethernet 0
Switch(config-if)# dot1x port-control auto
```

Examples

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
description switchport connect to a client
!
interface FastEthernet1
description switchport connect to a client
!
interface FastEthernet2
description switchport connect to a client
!
interface FastEthernet3
description switchport connect to a client
!
interface FastEthernet4
description Connect to the public network
!
interface Vlan1
description Apply 802.1x functionality on SVI
dot1x pae authenticator
dot1x port-control auto
dot1x reauthentication
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a switch or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
dot1x re-authentication	Globally enables periodic reauthentication of the client on the 802.1X interface.
dot1x reauthentication (EtherSwitch)	Enables periodic reauthentication of the client on the 802.1X interface.

Command	Description
dot1x timeout	Sets retry timeouts.
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.
show dot1x	Displays details for an identity profile.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

dot1x re-authenticate (privileged EXEC)



Note

Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x re-authenticate** command is replaced by the **clear authentication session** command. See the **clear authentication session** command for more information.

To manually initiate a reauthentication of the specified 802.1X-enabled ports, use the **dot1x re-authenticate** command in privileged EXEC mode.

dot1x re-authenticate [**interface** *interface-name interface-number*]

Syntax Description

interface <i>interface-name interface-number</i>	(Optional) Interface on which reauthentication is to be initiated.
---	--

Command Default

There is no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was introduced.
12.3(2)XA	This command was integrated into Cisco IOS Release 12.3(2)XA.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.

Usage Guidelines

You can use this command to reauthenticate a client without having to wait for the configured number of seconds between reauthentication attempts (re-authperiod) and automatic reauthentication.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows how to manually reauthenticate the device that is connected to a port:

```
Router# dot1x re-authenticate interface gigabitethernet2/0/1
```

Examples

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
description switchport connect to a client
!
interface FastEthernet1
description switchport connect to a client
!
interface FastEthernet2
description switchport connect to a client
!
interface FastEthernet3
description switchport connect to a client
!
interface FastEthernet4
description Connect to the public network
!
interface Vlan1
description Apply 802.1x functionality on SVI
dot1x pae authenticator
dot1x port-control auto
dot1x reauthentication
```

Related Commands

Command	Description
dot1x reauthentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
dot1x timeout	Sets retry timeouts.

dot1x reauthentication



Note

Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x reauthentication** command is replaced by the **authentication periodic** command. See the **authentication periodic** command for more information.

To enable periodic reauthentication of the client PCs on the 802.1X interface, use the **dot1x reauthentication** command in interface configuration mode. To disable periodic reauthentication, use the **no** form of this command.

dot1x reauthentication

no dot1x reauthentication

Syntax Description

This command has no arguments or keywords.

Command Default

Periodic reauthentication is not set.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.3(2)XA	This command was integrated into Cisco IOS Release 12.3(2)XA.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 in Cisco IOS Release 12.2(17d)SXB.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was replaced by the authentication periodic command.

Usage Guidelines

The reauthentication period can be set using the **dot1x timeout** command.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows that reauthentication has been enabled and the reauthentication period as been set for 1800 seconds:

```
Router(config)# configure terminal
Router(config)# interface ethernet 0
Router(config-if)# dot1x reauthentication
Router(config-if)# dot1x timeout reauth-period 1800
```

Examples

The following example shows Layer 3 802.1X support on a switched virtual interface using a Cisco 870 ISR:

```
interface FastEthernet0
description switchport connect to a client
!
interface FastEthernet1
description switchport connect to a client
!
interface FastEthernet2
description switchport connect to a client
!
interface FastEthernet3
description switchport connect to a client
!
interface FastEthernet4
description Connect to the public network
!
interface Vlan1
description Apply 802.1x functionality on SVI
dot1x pae authenticator
dot1x port-control auto
dot1x reauthentication
```

Examples

The following example shows how to enable periodic reauthentication of the client:

```
Router(config-if)# dot1x reauthentication
Router(config-if)#
```

The following example shows how to disable periodic reauthentication of the client:

```
Router(config-if)# no dot1x reauthentication
Router(config-if)#
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a router can send an EAP request/identity frame to a client PC (assuming that a response is not received) before concluding that the client PC does not support 802.1X.
dot1x port-control	Sets an 802.1X port control value.

Command	Description
dot1x timeout	Sets retry timeouts.
show dot1x	Displays 802.1X information.

dot1x re-authentication (EtherSwitch)

To enable periodic reauthentication of the client for an Ethernet switch network module, use the **dot1x re-authentication** command in global configuration mode. To disable periodic reauthentication, use the **no** form of this command.

dot1x re-authentication

no dot1x re-authentication

Syntax Description This command has no arguments or keywords.

Command Default Periodic reauthentication is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.
	12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines You configure the amount of time between periodic reauthentication attempts by using the **dot1x timeout re-authperiod** global configuration command.

Examples The following example shows how to disable periodic reauthentication of the client:

```
Router(config)# no dot1x re-authentication
```

The following example shows how to enable periodic reauthentication and set the number of seconds between reauthentication attempts to 4000 seconds:

```
Router(config)# dot1x re-authentication
Router(config)# dot1x timeout re-authperiod 4000
```

Related Commands

Command	Description
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.

Command	Description
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x system-auth-control

To globally enable 802.1X SystemAuthControl (port-based authentication), use the **dot1x system-auth-control** command in global configuration mode. To disable SystemAuthControl, 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

System authentication is disabled by default. If this command is disabled, all ports behave as if they are force authorized.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

The **no** form of the command removes any 802.1X-related configurations.

Catalyst 6500 Series Switch and Cisco 7600 Series

You must enable Authentication, Authorization, and Accounting (AAA) and specify the authentication method list before enabling 802.1X. A method list describes the sequence and authentication methods to be queried to authenticate a user.

Examples

The following example shows how to enable SystemAuthControl:

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

Related Commands

Command	Description
aaa authentication dot1x	Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.
aaa new-model	Enables the AAA access-control model.
debug dot1x	Displays 802.1X debugging information.
description	Specifies a description for an 802.1X profile.
device	Statically authorizes or rejects individual devices.
dot1x initialize	Initializes 802.1X state machines on all 802.1X-enabled interfaces.
dot1x max-req	Sets the maximum number of times that a router or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
dot1x port-control	Enables manual control of the authorized state of a controlled port.
dot1x re-authenticate	Manually initiates a reauthentication of the specified 802.1X-enabled ports.
dot1x reauthentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
dot1x timeout	Sets retry timeouts.
identity profile	Creates an identity profile and enters identity profile configuration mode.
show dot1x	Displays details and statistics for an identity profile.
template	Specifies a virtual template from which commands may be cloned.

dot1x timeout

To configure the value for retry timeouts, use the **dot1x timeout** command in global configuration or interface configuration mode. To return to the default value for retry timeouts to, use the **no** form of this command.

All Platforms Except the Cisco 7600 Series Switch

dot1x timeout {*auth-period seconds*| *held-period seconds*| *quiet-period seconds*| *ratelimit-period seconds*| *reauth-period {seconds| server}*| *server-timeout seconds*| *start-period seconds*| *supp-timeout seconds*| *tx-period seconds*}

no dot1x timeout {*auth-period seconds*| *held-period seconds*| *quiet-period seconds*| *ratelimit-period seconds*| *reauth-period {seconds| server}*| *server-timeout seconds*| *start-period seconds*| *supp-timeout seconds*| *tx-period seconds*}

Cisco 7600 Series Switch

dot1x timeout {*reauth-period seconds*| *quiet-period seconds*| *tx-period seconds*| *supp-timeout seconds*| *server-timeout seconds*}

no dot1x timeout {*reauth-period*| *quiet-period*| *tx-period*| *supp-timeout*| *server-timeout*}

Syntax Description

auth-period <i>seconds</i>	Configures the time, in seconds, the supplicant (client) waits for a response from an authenticator (for packets other than Extensible Authentication Protocol over LAN [EAPOL]-Start) before timing out. • The range is from 1 to 65535. The default is 30.
held-period <i>seconds</i>	Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt). • The range is from 1 to 65535. The default is 60.
quiet-period <i>seconds</i>	Configures the time, in seconds, that the authenticator (server) remains quiet (in the HELD state) following a failed authentication exchange before trying to reauthenticate the client. • For all platforms except the Cisco 7600 series Switch, the range is from 1 to 65535. The default is 120. • For the Cisco 7600 series Switch, the range is from 0 to 65535. The default is 60.

ratelimit-period <i>seconds</i>	<p>Throttles the EAP-START packets that are sent from misbehaving client PCs (for example, PCs that send EAP-START packets that result in the wasting of switch processing power).</p> <ul style="list-style-type: none"> • The authenticator ignores EAPOL-Start packets from clients that have successfully authenticated for the rate-limit period duration. • The range is from 1 to 65535. By default, rate limiting is disabled.
reauth-period { <i>seconds</i> server }	<p>Configures the time, in seconds, after which an automatic reauthentication should be initiated.</p> <ul style="list-style-type: none"> • The server keyword indicates that the reauthentication period value for the client should be obtained from the authentication, authorization, and accounting (AAA) server as the Session-Timeout (RADIUS Attribute 27) value. If the server keyword is used, the action upon reauthentication is also decided by the server and sent as the Termination-Action (RADIUS Attribute 29) value. The termination action could be either "terminate" or "reauthenticate." If the server keyword is not used, the termination action is always "reauthenticate." • For all platforms except the Cisco 7600 series switch, the range is from 1 to 65535. The default is 3600. • For the Cisco 7600 series switch, the range is from 1 to 4294967295. The default is 3600. See the "Usage Guidelines" section for additional information. <p>Note Effective with Cisco IOS Release 12.2(33)SXI, this phrase is replaced by the authentication timer reauthenticate command. See the authentication timer reauthenticate command for more information.</p>

server-timeout <i>seconds</i>	<p>Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted.</p> <ul style="list-style-type: none"> • For all platforms except the Cisco 7600 series switch, the range is from 1 to 65535. The default is 30. • For the Cisco 7600 series switch, the range is from 30 to 65535. The default is 30. <p>If the server does not send a response to an 802.1X packet within the specified period, the packet is sent again.</p>
start-period <i>seconds</i>	<p>Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted.</p> <ul style="list-style-type: none"> • The value is from 1 to 65535. The default is 30.
supp-timeout <i>seconds</i>	<p>Sets the authenticator-to-supPLICANT retransmission time for all EAP messages other than EAP Request ID.</p> <ul style="list-style-type: none"> • For all platforms except the Cisco 7600 series Switch, the range is from 1 to 65535. The default is 30. • For the Cisco 7600 series Switch, the range is from 30 to 65535. The default is 30.
tx-period <i>seconds</i>	<p>Configures the number of seconds between retransmission of EAP request ID packets (assuming that no response is received) to the client.</p> <ul style="list-style-type: none"> • For all platforms except the Cisco 7600 series switch, the range is from 1 to 65535. The default is 30. • For the Cisco 7600 series switch, the range is from 30 to 65535. The default is 30. • If an 802.1X packet is sent to the supplicant and the supplicant does not send a response after the retry period, the packet will be sent again.

Command Default

Periodic reauthentication and periodic rate-limiting are not done.

Command Modes

Global configuration Interface configuration

Cisco 7600 Switch

Interface configuration

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.3(2)XA	This command was integrated into Cisco IOS Release 12.3(2)XA.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(18)SE	Ranges for the server-timeout , supp-timeout , and tx-period keywords were changed.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was added for Cisco IOS Release 12.2(17d)SXB.
12.3(11)T	The auth-period , held-period , and start-period keywords were added.
12.2(25)SEC	The range for the tx-period keyword was changed, and the reauth-period and server-timeout keywords were added.
12.1(11)AX	This command was introduced.
12.1(14)EA1	The supp-timeout and server-timeout keywords were added. The configuration mode for the command was changed to interface configuration mode.
12.4(6)T	The supp-timeout keyword was added, and this command was integrated into Cisco IOS Release 12.4(6)T.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Switches (ISRs) only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	The reauth-period keyword was replaced by the authentication timer reauthenticate command.

Usage Guidelines

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Cisco 7600 Switch

You must enable periodic reauthentication before you enter the **dot1x timeout reauth-period** command. Enter the **dot1x reauthentication** command to enable periodic reauthentication. The **dot1x timeout reauth-period** command affects the behavior of the system only if periodic reauthentication is enabled.

Examples

The following example shows that various 802.1X retransmission and timeout periods have been set:

```
Switch(config)# configure terminal
Switch(config)# interface ethernet 0
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout auth-period 2000
Switch(config-if)# dot1x timeout held-period 2400
Switch(config-if)# dot1x timeout reauth-period 1800
Switch(config-if)# dot1x timeout quiet-period 600
Switch(config-if)# dot1x timeout start-period 90
Switch(config-if)# dot1x timeout supp-timeout 300
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# dot1x timeout server-timeout 60
```

The following example shows how to return to the default reauthorization period:

```
Switch(config-if)# no dot1x timeout reauth-period
```

Examples

The following example shows how to set 802.1X retransmission and timeout periods on the Cisco 7600 Switch:

```
Switch(config-if)# dot1x timeout reauth-period 4000
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# dot1x timeout supp-timeout 25
Switch(config-if)# dot1x timeout server-timeout 25
```

Examples

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
description switchport connect to a client
!
interface FastEthernet1
description switchport connect to a client
!
interface FastEthernet2
description switchport connect to a client
!
interface FastEthernet3
description switchport connect to a client
!
interface FastEthernet4
description Connect to the public network
!
interface Vlan1
description Apply 802.1x functionality on SVI
dot1x pae authenticator
dot1x port-control auto
dot1x reauthentication
```


Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a switch or Ethernet switch module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
dot1x port-control	Sets an 802.1X port control value.
dot1x re-authentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
show dot1x	Displays 802.1X information.

dot1x timeout (EtherSwitch)

To set the number of retry seconds between 802.1X authentication exchanges when an Ethernet switch network module is installed in the router, use the **dot1x timeout** command in global configuration mode. To return to the default setting, use the **no** form of this command.

dot1x timeout {**quiet-period** *seconds*| **re-authperiod** *seconds*| **tx-period** *seconds*}

no dot1x timeout {**quiet-period** *seconds*| **re-authperiod** *seconds*| **tx-period** *seconds*}

Syntax Description

quiet-period <i>seconds</i>	Specifies the time in seconds that the Ethernet switch network module remains in the quiet state following a failed authentication exchange with the client. The range is from 0 to 65535 seconds. The default is 60 seconds.
re-authperiod <i>seconds</i>	Specifies the number of seconds between reauthentication attempts. The range is from 1 to 4294967295. The default is 3660 seconds.
tx-period <i>seconds</i>	Time in seconds that the switch should wait for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is from 1 to 65535 seconds. The default is 30 seconds.

Command Default

quiet-period : 60 seconds **re-authperiod**: 3660 seconds**tx-period**: 30 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

You should change the default values of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients or authentication servers.

quiet-period Keyword

During the quiet period, the Ethernet switch network module does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a smaller number than the default.

re-authperiod Keyword

The **re-authperiod** keyword affects the behavior of the the Ethernet switch network module only if you have enabled periodic reauthentication by using the **dot1x re-authentication** global configuration command.

Examples

The following example shows how to set the quiet time on the switch to 30 seconds:

```
Router(config)# dot1x timeout quiet-period 30
```

The following example shows how to enable periodic reauthentication and set the number of seconds between reauthentication attempts to 4000 seconds:

```
Router(config)# dot1x re-authentication
Router(config)# dot1x timeout re-authperiod 4000
```

The following example shows how to set 60 seconds as the amount of time that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request:

```
Router(config)# dot1x timeout tx-period 60
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that the device sends an EAP-request/identity frame before restarting the authentication process.
dot1x re-authentication (EtherSwitch)	Enables periodic reauthentication of the client for the Ethernet switch network module.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

