authentication command bounce-port ignore through auth-type

authentication command bounce-port ignore

To configure the router to ignore a RADIUS Change of Authorization (CoA) bounce port command, use the **authentication command bounce-port ignore** command in global configuration mode. To return to the default status, use the **no** form of this command.

authentication command bounce-port ignore

no authentication command bounce-port ignore

Syntax Description

This command has no arguments or keywords.

Command Default

The router accepts a RADIUS CoA bounce port command.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

A RADIUS CoA bounce port command sent from a RADIUS server can cause a link flap on an authentication port, which triggers Dynamic Host Configuration Protocol (DHCP) renegotiation from one or more hosts connected to this port. This incident can occur when there is a VLAN change and the endpoint is a device (such as a printer) that does not have a mechanism to detect a change on this authentication port. The **authentication command bounce-port ignore** command configures the router to ignore the RADIUS CoA bounce port command to prevent a link flap from occuring on any hosts that are connected to an authentication port.

Examples

This example shows how to configure the router to ignore a RADIUS CoA bounce port command:

```
Router(config)# aaa new-model
Router(config)# authentication command bounce-port ignore
```

Related Commands

Command	Description
authentication command disable-port ignore	Configures the router to ignore a RADIUS server CoA **disable port** command.

authentication command disable-port ignore

To allow the router to ignore a RADIUS server Change of Authorization (CoA) disable port command, use the **authentication command disable-port ignore** command in global configuration mode. To return to the default status, use the **no** form of this command.

authentication command disable-port ignore

no authentication command disable-port ignore

Syntax Description

This command has no arguments or keywords.

Command Default

The router accepts a RADIUS CoA disable port command.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

The RADIUS server CoA disable port command administratively shuts down the authentication port that is hosting a session, resulting in session termination. Use the **authentication command disable-port ignore** command to configure the router to ignore the RADIUS server CoA disable port command so that the authentication port and other hosts on this authentication port are not disconnected.

Examples

This example shows how to configure the router to ignore a CoA **disable port** command:

```
Router(config)# aaa new-model
Router(config)# authentication command disable-port ignore
```

Related Commands

Command	Description
authentication command bounce-port ignore	Configures the router to ignore a RADIUS server CoA bounce port command.

authentication control-direction

To set the direction of authentication control on a port, use the **authentication control-direction**command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication control-direction {**both**| **in**}

no authentication 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(33)SXI	This command was introduced.

Usage Guidelines

The IEEE 802.1x standard is implemented to block traffic between the nonauthenticated clients and network resources. This means that nonauthenticated clients cannot communicate with any device on the network except the authenticator. The reverse is true, except for one circumstance--when the port has been configured as a unidirectional controlled port.

Unidirectional State

The IEEE 802.1x standard defines a unidirectional controlled port, which enables a device on the network to "wake up" a client so that it continues to be reauthenticated. When you use the **authentication control-direction in** command to configure the port as unidirectional, the port changes to the spanning-tree forwarding state, thus allowing a device on the network to wake the client, and force it to reauthenticate.

Bidirectional State

When you use the **authentication control-direction both** command to configure a port as bidirectional, access to the port is controlled in both directions. In this state, the port does not receive or send packets.

Examples

The following example shows how to enable unidirectional control:

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

The following examples show how to enable bidirectional control:

```
Switch(config-if)# authentication control-direction both
```

authentication event fail

To specify how the Auth Manager handles authentication failures as a result of unrecognized user credentials, use the **authentication event fail**command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication event fail [**retry** *retry-count*] **action** {**authorize vlan** *vlan-id*| **next-method**}

no authentication event fail

Syntax Description

retry *retry-count*	(Optional) Specifies how many times the authentication method is tried after an initial failure.
action	Specifies the action to be taken after an authentication failure as a result of incorrect user credentials.
authorize vlan *vlan-id*	Authorizes a restricted VLAN on a port after a failed authentication attempt.
next-method	Specifies that the next authentication method be invoked after a failed authentication attempt. The order of authentication methods is specified by the **authentication order** command.

Command Default

Authentication is attempted two times after the initial failed attempt.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Only the dot1x authentication method can signal this type of authentication failure.

Examples

The following example specifies that after three failed authentication attempts the port is assigned to a restricted VLAN:

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3
```

```
Switch(config-if)# authentication event fail retry 3 action authorize vlan 40
Switch(config-if)# end
```

Related Commands

Command	Description
authentication event no-response action	Specifies the action to be taken when authentication fails due to a nonresponsive host.
authentication order	Specifies the order in which authentication methods are attempted.

authentication event server alive action reinitialize

To reinitialize an authorized Auth Manager session when a previously unreachable authentication, authorization, and accounting (AAA) server becomes available, use the **authentication event server alive action reinitialize** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication event server alive action reinitialize

no authentication event server alive action reinitialize

Syntax Description

This command has no arguments or keywords.

Command Default

The session is not reinitialized .

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **authentication event server alive action reinitialize** command to reinitialize authorized sessions when a previously unreachable AAA server becomes available.

Examples

The following example specifies that authorized sessions are reinitialized when a previously unreachable AAA server becomes available:

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3

Switch(config-if)# authentication event server alive action reinitialize
Switch(config-if)# end
```

Related Commands

Command	Description
authentication event server dead action authorize	Specifies how to handle authorized sessions when the AAA server is unreachable.

authentication event server dead action authorize

To authorize Auth Manager sessions when the authentication, authorization, and accounting (AAA) server becomes unreachable, use the **authentication event server dead action authorize** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication event server dead action authorize vlan *vlan-id*

no authentication event server dead action authorize

Syntax Description

vlan *vlan-id*	Authorizes a restricted VLAN on a port after a failed authentication attempt.

Command Default

No session is authorized.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **authentication event server dead action authorize** command to authorize sessions even when the AAA server is unavailable.

Examples

The following example specifies that when the AAA server becomes unreachable, the port is assigned to a VLAN:

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3

Switch(config-if)# authentication event server dead action authorize vlan 40

Switch(config-if)# end
```

Related Commands

Command	Description
authentication event server alive action reinitialize	Reinitializes an authorized session when a previously unreachable AAA server becomes available.

authentication fallback

To enable a web authentication fallback method, use the **authentication fallback** command in interface configuration mode. To disable web authentication fallback, use the **no** form of this command.

authentication fallback *fallback-profile*

no authentication fallback

Syntax Description

fallback-profile	The name of the fallback profile for web authentication.

Command Default

Web authentication fallback is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Use the **authentication fallback** command to specify the fallback profile for web authentication. Use the **fallback profile** command to specify the details of the profile.

Examples

The following example shows how to specify a fallback profile on a port:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitethernet1/0/3
Router(config-if)# authentication fallback profile1
Router(config-if)# end
```

Related Commands

Command	Description
fallback profile	Specifies the profile for web authentication.

authentication host-mode

To allow hosts to gain access to a controlled port, use the **authentication host-mode** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication host-mode {**single-host**| **multi-auth**| **multi-domain**| **multi-host**} **[open]**

no authentication host-mode

Syntax Description

single-host	Specifies that only one client can be authenticated on a port at any given time. A security violation occurs if more than one client is detected.
multi-auth	Specifies that multiple clients can be authenticated on the port at any given time.
multi-domain	Specifies that only one client per domain (DATA or VOICE) can be authenticated at a time.
multi-host	Specifies that after the first client is authenticated all subsequent clients are allowed access.
open	(Optional) Specifies that the port is open; that is, there are no access restrictions.

Command Default

Access to a port is not allowed.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Before you use this command, you must use the **authentication port-control** command with the keyword **auto**.

In **multi-host** mode, only one of the attached hosts has to 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.

Examples

:The following example shows how to enable authentication in **multi-host** mode:

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet2/0/1

Switch(config-if)# authentication port-control auto

Switch(config-if)# authentication host-mode multi-host
```

Related Commands

Command	Description
authentication port-control	Displays information about interfaces.

authentication open

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

authentication open

no authentication open

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced.

Usage Guidelines

Open Access allows clients or devices to gain network access before authentication is performed.

You can verify your settings by entering the **show authentication** privileged EXEC command.

This command overrides the **authentication host-mode** *session-type* **open** global configuration mode command for the port only.

Examples

The following example shows how to enable open access to a port:

```
Router(config-if)# authentication open
Router(config-if)#
```

The following example shows how to enable open access to a port:

```
Router(config-if)# no authentication open
Router(config-if)#
```

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication order

To specify the order in which the Auth Manager attempts to authenticate a client on a port, use the **authentication order** command in interface configuration mode. To return to the default authentication order, use the **no** form of this command.

authentication order {**dot1x** [**mab**| **webauth**] **[webauth]**| **mab** [**dot1x**| **webauth**] **[webauth]**| **webauth**}

no authentication order

Syntax Description

dot1x	Specifies IEEE 802.1X authentication.
mab	Specifies MAC-based authentication(MAB).
webauth	Specifies web-based authentication.

Command Default

The default authentication order is **dot1x**, **mab**, and **webauth**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Use the **authentication order** command to specify explicitly which authentication methods are run and the order in which they are run. Each method may be entered only once in the list and no method can be listed after **webauth**.

Examples

The following example sets the authentication order for a port:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet0/1

Router(config-if)# authentication order mab dot1x
Router(config-if)# end
Router#
```

Related Commands

Command	Description
authentication priority	Specifies the priority of authentication methods on a port.

authentication periodic

To enable automatic reauthentication on a port, use the **authentication periodic** command in interface configuration mode. To disable, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.2(33)SXI, the **authentication periodic** command replaces the **dot1x reauthentication** command.

authentication periodic

no authentication periodic

Syntax Description

This command has no arguments or keywords.

Command Default

Reauthentication is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Use the **authentication periodic** command to enable automatic reauthentication on a port. To configure the interval between reauthentication attempts, use the **authentication timer reauthenticate** command.

Examples

The following example enables reauthentication and sets the interval to 1800 seconds:

```
Switch(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet0/2
Switch(config-if)# authentication periodic
Switch(config-if)# authentication timer reauthenticate 1800
```

Related Commands

Command	Description
authentication timer reauthenticate	Specifies the period of time between attempts to reauthenticate an authorized port.

authentication port-control

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

Note Effective with Cisco IOS Release 12.2(33)SXI, the **authentication port-control** command replaces the **dot1x port-control** command.

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

no authentication port-control

Syntax Description

auto	Enables 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 IEEE 802.1X on the interface and causes the port to change to the authorized state without requiring any authentication exchange. 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

Ports are authorized without authentication exchanges.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

To verify port-control settings, use the **show interfaces** command and check 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.

The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The system requests the identity of the client and begins relaying authentication messages between the client and the authentication server.

Examples

The following example shows the commands used to specify that the authorization status of the client be determined by the authentication process:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface ethernet0/2

Router(config-if)# authentication port-control auto
```

Related Commands

Command	Description
show interfaces	Configures the authorization state of a controlled port.

authentication priority

To specify the priority of authentication methods on a port, use the **authentication priority**command in interface configuration mode. To return to the default, use the **no** form of this command.

authentication priority {**dot1x** [**mab**| **webauth**] **[webauth]**| **mab** [**dot1x**| **webauth**] **[webauth]**| **webauth**}

no authentication priority

Syntax Description

dot1x	Specifies IEEE 802.1X authentication.
mab	Specifies MAC-based authentication.
webauth	Specifies web-based authentication.

Command Default

The default priority order is **dot1x**, **mab**, and **webauth**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

The **authentication order** command specifies the order in which authentication methods are attempted. This order is the default priority. To override the default priority and allow higher priority methods to interrupt a running authentication method, use the **authentication priority** command.

Examples

The following example shows the commands used to configure the authentication order and the authentication priority on a port:

```
Router# configure terminal
Router(config)# interface fastethernet0/1

Router(config-if)# authentication order mab dot1x webauth
Router(config-if)# authentication priority dot1x mab
Router(config-if)# end
Router#
```

Related Commands

Command	Description
authentication order	Specifies the order in which the Auth Manager attempts to authenticate a client on a port.

authentication timer inactivity

To configure the time after which an inactive Auth Manager session is terminated, use the **authentication timer inactivity**command in interface configuration mode. To disable the inactivity timer, use the **no** form of this command.

authentication timer inactivity {*seconds*| **server**}

no authentication timer inactivity

Syntax Description

seconds	The period of inactivity, in seconds, allowed before an Auth Manager session is terminated and the port is unauthorized. The range is from 1 to 65535.
server	Specifies that the period of inactivity is defined by the Idle-Timeout value (RADIUS Attribute 28) on the authentication, authorization, and accounting (AAA) server.

Command Default

The inactivity timer is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

In order to prevent reauthentication of inactive sessions, use the **authentication timer inactivity**command to set the inactivity timer to an interval shorter than the reauthentication interval set with the **authentication timer reauthenticate** command.

Examples

The following example sets the inactivity interval on a port to 900 seconds:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet6/0

Switch(config-if)# authentication timer inactivity 900

Switch(config-if)# end
```

Related Commands

Command	Description
configuration timer reauthenticate	Specifies the time after which the Auth Manager attempts to reauthenticate an authorized port.
authentication timer restart	Specifies the interval after which the Auth Manager attempts to authenticate an unauthorized port.

authentication timer reauthenticate

To specify the period of time between which the Auth Manager attempts to reauthenticate authorized ports, use the **authentication timer reauthenticate** command in interface configuration mode. To reset the reauthentication interval to the default, use the **no** form of this command.

authentication timer reauthenticate {*seconds*| **server**}

no authentication timer reauthenticate

Syntax Description

seconds	The number of seconds between reauthentication attempts. The default is 3600.
server	Specifies that the interval between reauthentication attempts is defined by the Session-Timeout value (RADIUS Attribute 27) on the authentication, authorization, and accounting (AAA) server.

Command Default

The automatic reauthentication interval is set to 3600 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Use the **authentication timer reauthenticate** command to set the automatic reauthentication interval of an authorized port. If you use the **authentication timer inactivity** command to configure an inactivity interval, configure the reauthentication interval to be longer than the inactivity interval.

Examples

The following example sets the reauthentication interval on a port to 1800 seconds:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet6/0

Switch(config-if)# authentication timer reauthenticate 1800

Switch(config-if)# end
```

Related Commands

Command	Description
authentication periodic	Enables automatic reauthentication.
authentication timer inactivity	Specifies the interval after which the Auth Manager ends an inactive session.
authentication timer restart	Specifies the interval after which the Auth Manager attempts to authenticate an unauthorized port.

authentication timer restart

To specify the period of time after which the Auth Manager attempts to authenticate an unauthorized port, use the **authentication timer restart** command in interface configuration mode. To reset the interval to the default value, use the **no** form of this command.

authentication timer restart *seconds*

no authentication timer restart

Syntax Description

seconds	The number of seconds between attempts to authenticate an unauthorized port. The range is 1 to 65535. The default is 60.

Command Default

No attempt is made to authenticate unauthorized ports.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Use the **authentication timer restart** command to specify the interval between attempts to authenticate an unauthorized port. The default interval is 60 seconds.

Examples

The following example sets the authentication timer interval to 120 seconds:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface GigabitEthernet6/0

Router(config-if)# authentication timer restart 120

Router(config-if)# end
```

Related Commands

Command	Description
authentication timer inactivity	Specifies the period of time after which the Auth Manager attempts to authenticate an unauthorized port.
configuration timer reauthenticate	Specifies the time after which the Auth Manager attempts to reauthenticate an authorized port.

authentication violation

To specify the action to be taken when a security violation occurs on a port, use the **authentication violation**command in interface configuration mode. To return to the default action, use the **no** form of this command.

authentication violation {**restrict**| **shutdown**}

no authentication violation

Syntax Description

restrict	Specifies that the port restrict traffic with the domain from which the security violation occurs.
shutdown	Specifies that the port shuts down upon a security violation.

Command Default

Ports are shut down when a security violation occurs.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Use the **authentication violation** command to specify the action to be taken when a security violation occurs on a port.

Examples

The following example configures the GigabitEthernet interface to restrict traffic when a security violation occurs:

```
Switch(config)# interface GigabitEthernet6/2

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-if)# authentication violation restrict

Switch(config-if)# end
```

auth-type

To set policy for devices that are dynamically authenticated or unauthenticated, use the **auth-type** command in identity profile configuration mode. To remove the policy that was specified, use the **no** form of this command.

auth-type {**authorize| not-authorize**} **policy** *policy-name*

no auth-type {**authorize| not-authorize**} **policy** *policy-name*

Syntax Description

authorize	Policy is specified for all authorized devices.
not-authorize	Policy is specified for all unauthorized devices.
policy *policy-name*	Specifies the name of the identity policy to apply for the associated authentication result.

Command Default

A policy is not set for authorized or unauthorized devices.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

This command is used when a device is dynamically authenticated or unauthenticated by the network access device, and the device requires the name of the policy that should be applied for that authentication result.

Examples

The following example shows that 802.1x authentication applies to the identity policy “grant” for all dynamically authenticated hosts:

```
Router (config)# ip access-list extended allow-acl
Router (config-ext-nacl)# permit ip any any
Router (config-ext-nacl)# exit
Router (config)# identity policy grant
Router (config-identity-policy)# access-group allow-acl
Router (config-identity-policy)# exit
Router (config)# identity profile dot1x

Router (config-identity-prof)# auth-type authorize policy grant
```

Related Commands

Command	Description
identity policy	Creates an identity policy.
identity profile dot1x	Creates an 802.1x identity profile.