dnsix-dmdp retries through dynamic

dnsix-dmdp retries

To s et the retransmit count used by the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) Message Delivery Protocol (DMDP), use the **dnsix-dmdp retries** command in global configuration mode. To restore the default number of retries, use the **no**form of this command.

dnsix-dmdp retries *count*

no dnsix-dmdp retries *count*

Syntax Description

count	Number of times DMDP will retransmit a message. It can be an integer from 0 to 200. The default is 4 retries, or until acknowledged.

Command Default

Retransmits messages up to 4 times, or until acknowledged.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
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.

Examples

The following example sets the number of times DMDP will attempt to retransmit a message to 150:

```
dnsix-dmdp retries 150
```

Related Commands

Command	Description
dnsix-nat authorized-redirection	Specifies the address of a collection center that is authorized to change the primary and secondary addresses of the host to receive audit messages.
dnsix-nat primary	Specifies the IP address of the host to which DNSIX audit messages are sent.

Command	Description
dnsix-nat secondary	Specifies an alternate IP address for the host to which DNSIX audit messages are sent.
dnsix-nat source	Starts the audit-writing module and defines audit trail source address.
dnsix-nat transmit-count	Causes the audit-writing module to collect multiple audit messages in the buffer before sending the messages to a collection center.

dnsix-nat authorized-redirection

To sp ecify the address of a collection center that is authorized to change the primary and secondary addresses of the host to receive audit messages, use the **dnsix-nat authorized-redirection** command in global configuration mode. To delete an address, use the **no** form of this command.

dnsix-nat authorized-redirection *ip-address*

no dnsix-nat authorized-redirection *ip-address*

Syntax Description

ip-address	IP address of the host from which redirection requests are permitted.

Command Default

An empty list of addresses.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
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

Use multiple **dnsix-nat authorized-redirection** commands to specify a set of hosts that are authorized to change the destination for audit messages. Redirection requests are checked against the configured list, and if the address is not authorized the request is rejected and an audit message is generated. If no address is specified, no redirection messages are accepted.

Examples

The following example specifies that the address of the collection center that is authorized to change the primary and secondary addresses is 192.168.1.1:

```
dnsix-nat authorization-redirection 192.168.1.1
```

dnsix-nat primary

To s pecify the IP address of the host to which Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit messages are sent, use the **dnsix-nat primary** command in global configuration mode. To delete an entry, use the **no** form of this command.

dnsix-nat primary *ip-address*

no dnsix-nat primary *ip-address*

Syntax Description

ip-address	IP address for the primary collection center.

Command Default

Messages are not sent.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
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

An IP address must be configured before audit messages can be sent.

Examples

The following example configures an IP address as the address of the host to which DNSIX audit messages are sent:

```
dnsix-nat primary 172.16.1.1
```

dnsix-nat secondary

To sp ecify an alternate IP address for the host to which Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit messages are sent, use the **dnsix-nat secondary** command in global configuration mode. To delete an entry, use the **no** form of this command.

dnsix-nat secondary *ip-address*

no dnsix-nat secondary *ip-address*

Syntax Description

ip-address	IP address for the secondary collection center.

Command Default

No alternate IP address is known.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
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

When the primary collection center is unreachable, audit messages are sent to the secondary collection center instead.

Examples

The following example configures an IP address as the address of an alternate host to which DNSIX audit messages are sent:

```
dnsix-nat secondary 192.168.1.1
```

dnsix-nat source

To st art the audit-writing module and to define the audit trail source address, use the **dnsix-nat source**command in global configuration mode. To disable the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit trail writing module, use the **no** form of this command.

dnsix-nat source *ip-address*

no dnsix-nat source *ip-address*

Syntax Description

ip-address	Source IP address for DNSIX audit messages.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
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

You must issue the **dnsix-nat source** command before any of the other **dnsix-nat** commands. The configured IP address is used as the source IP address for DMDP protocol packets sent to any of the collection centers.

Examples

The following example enables the audit trail writing module, and specifies that the source IP address for any generated audit messages should be the same as the primary IP address of Ethernet interface 0:

```
dnsix-nat source 192.168.2.5
interface ethernet 0
 ip address 192.168.2.5 255.255.255.0
```

dnsix-nat transmit-count

To h ave the audit writing module collect multiple audit messages in the buffer before sending the messages to a collection center, use the **dnsix-nat transmit-count** command inglobal configuration mode. To revert to the default audit message count, use the **no** form of this command.

dnsix-nat transmit-count *count*

no dnsix-nat transmit-count *count*

Syntax Description

count	Number of audit messages to buffer before transmitting to the server. It can be an integer from 1 to 200.

Command Default

One message is sent at a time.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
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

An audit message is sent as soon as the message is generated by the IP packet-processing code. The audit writing module can, instead, buffer up to several audit messages before transmitting to a collection center.

Examples

The following example configures the system to buffer five audit messages before transmitting them to a collection center:

```
dnsix-nat transmit-count 5
```

dns-timeout

To specify the Domain Name System (DNS) idle timeout (the length of time for which a DNS lookup session will continue to be managed while there is no activity), use the **dns-timeout** command in parameter-map type inspect configuration mode. To disable the timeout, use the **no** form of this command.

dns-timeout *seconds*

no dns-timeout *seconds*

Syntax Description

seconds	Length of time, in seconds, for which a DNS name lookup session will still be managed while there is no activity. The default is 5.

Command Default

The DNS idle timeout is disabled.

Command Modes

Parameter-map type inspect configuration

Command History

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

Usage Guidelines

You can use the **dns-timeout**subcommand when you are creating an inspect type parameter map. You can enter the **dns-timeout**subcommand after you enter the **parameter-map type inspect** command.

Use the **dns-timeout**command if you have DNS inspection configured and want to control the timeout of DNS sessions.

If DNS inspection is not configured, but you enter the **dns-timeout** command, the command does not take effect (that is, it is not applied to a DNS session).

For more detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example specifies that if there is no activity, a DNS lookup session will continue to be managed for 25 seconds:

```
parameter-map type inspect insp-params
 dns-timeout 25
```

Related Commands

Command	Description
ip inspect dns-timeout	Specifies the DNS idle timeout (the length of time during which a DNS name lookup session will still be managed while there is no activity).
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

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 *character*	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.

domain (isakmp-group)

To specify the Domain Name Service (DNS) domain to which a group belongs, use the **domain** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove this command from your configuration, use the **no** form of this command.

domain *name*

no domain *name*

Syntax Description

name	Name of the DNS domain.

Command Default

A DNS domain is not specified.

Command Modes

ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

Use the domain command to specify group domain membership.

You must enable the **crypto isakmp configuration group**command, which specifies group policy information that has to be defined or changed, before enabling the **domain**command.

Examples

The following example shows that members of the group “cisco” also belong to the domain “cisco.com”:

```
crypto isakmp client configuration group cisco
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
  domain cisco.com
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.
crypto isakmp keepalive	Specifies the primary and secondary DNS servers.

domain-stripping

To configure domain stripping at the server group level, use the **domain-stripping** command in server group RADIUS configuration mode. To disable the configuration, use the **no** form of this command.

domain-stripping [**strip-suffix** *word*] **[right-to-left]** [**prefix-delimiter** *word*] [**delimiter** *word*]

no domain-stripping [**strip-suffix** *word*] **[right-to-left]** [**prefix-delimiter** *word*] [**delimiter** *word*]

Syntax Description

strip-suffix	(Optional) Configures the suffix, which needs to be stripped.
word	(Optional) Suffix that needs to be stripped.
right-to-left	(Optional) Terminates the string at the first delimiter going from right to left.
prefix-delimiter	(Optional) Configures a set of prefix delimiters.
delimiter	(Optional) Configures a set of suffix delimiters.

Command Default

Stripping is disabled. The entire username (including the domain name) is sent to the RADIUS server.

Command Modes

Server group RADIUS configuration (config-sg-radius)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

Use the **radius-server domain-stripping** command to remove the domain name from the username received at the global level. All authentication, authorization, and accounting (AAA) requests with “user@example.com” will go to the remote RADIUS server with the reformatted username “user.” The domain name is removed from the request .

Use the **domain-stripping** command to configure domain stripping at the server group level. Per-server group configuration will override the global configuration. That is, if domain stripping is not enabled globally but enabled in the server group, it is enabled only for that server group. Also, if virtual routing and forwarding (VRF)-specific domain stripping is configured globally and in the server group for a different VRF, domain stripping is enabled in both the VRFs. After domain stripping and broadcast accounting are configured, you can create separate accounting records as per the configurations.

Examples

The following example shows how to configure domain stripping at the server group level:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server radius rad1
Device(config-sg-radius)# domain-stripping right-to-left delimiter @$/
Device(config-sg-radius)# end
```

Related Commands

Command	Description
aaa group server radius	Adds the RADIUS server group.

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 Switchs (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

name	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 *milliseconds*	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

vlan-id	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)

Command History

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
```

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 host-mode

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

To allow hosts on an IEEE 802.1X-authorized port, use the **dot1x host-mode** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

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

no dot1x host-mode {**multi-auth**| **multi-host**| **single-host**}

Syntax Description

multi-auth	Specifies that all clients are authenticated individually on the port. The multi-auth mode is not supported on switch ports and is the default mode for switch ports.
multi-host	Ensures that the first client and all subsequent clients are allowed access to the port if the first client is successfully authenticated.
single-host	Ensures that only the first client is authenticated. All other clients are ignored and may cause a violation. The single-host mode is the default mode for switch ports.

Command Default

Hosts are not allowed on an 802.1X-authorized port.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)EA1	This command was introduced for switches. It replaced the **dot1x multiple-hosts** command.
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 Switchs (ISRs) only.
12.2(33)SXI	This command was replaced by the **authentication host-mode** command.

Usage Guidelines

Before you use this command, use the **dot1x port-control auto**command to enables IEEE 802.1X port-based authentication, and cause the port to begin in the unauthorized state.

The **multi-auth** mode authenticates each new client separately.

In **multi-host** mode, only one of the attached hosts has to be successfully authorized for all hosts to be granted network access (the **multi-host** mode authenticates one client, but after the client is authenticated, traffic is allowed from all other MAC addresses.). 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.

The **single-host** mode allows only one client per port; that is, one MAC address is authenticated, and all others are blocked.

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 IEEE 802.1X globally, to enable IEEE 802.1x on a port, and to enable multiple-hosts mode:

```
Switch(config)# dot1x system-auth-control
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host:
```

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 port-control	Enables 802.1X port-based authentication.

Command	Description
show dot1x	Displays details for an identity profile.

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 *interface-name*	(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 Guidelin

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

number	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 *number* 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 max-start

To set the maximum number of Extensible Authentication Protocol (EAP) start frames that a supplicant sends (assuming that no response is received) to the client before concluding that the other end is 802.1X unaware, use the **dot1x max-start**command in global configuration or interface configuration mode. To remove the maximum number-of-times setting, use the **no** form of this command.

dot1x max-start *number*

no dot1x max-start

Syntax Description

number	Maximum number of times that the router sends an EAP start frame. The value is from 1 to 65535. The default is 3.

Command Default

The default maximum number setting is 3.

Command Modes

Global configuration Interface configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4(6)T	Global configuration mode was added for this command.
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

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 EAP over LAN- (EAPOL-) Start requests has been set to 5:

```
Router (config)# interface Ethernet1
Router (config-if)# dot1x pae supplicant
Router (config-if)# dot1x max-start 5
```

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 pae	Sets the PAE type during 802.1X authentication.
interface	Configures an interface type.

dot1x multi-hosts

To allow multiple hosts (clients) on an 802.1X-authorized port in interface configuration command mode, use the **dot1x multi-hosts** command. Use the **no** form of this command to disallow multiple hosts.

dot1x multi-hosts

no dot1x multi-hosts

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Before entering this command, ensure that the **dot1x port-control**command is set to **auto** for the specified interface.

Examples

This example shows how to allow multiple hosts:

```
Router(config-if)# dot1x multi-hosts
Router(config-if)#
```

This example shows how to disallow multiple hosts:

```
Router(config-if)# no dot1x multi-hosts
Router(config-if)#
```

Related Commands

Command	Description
dot1x port-control	Sets the port control value.
show dot1x	Displays 802.1X information.

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 Switchs (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** ommand 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 (EtherSwitch)

To manually initiate a reauthentication of all 802.1X-enabled ports or the specified 802.1X-enabled port on a router with an Ethernet switch network module installed, use the **dot1x re-authenticate** command in privileged EXEC mode.

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

Syntax Description

interface *interface-type interface-number*	(Optional) Specifies the slot and port number of the interface to reauthenticate.

Command Default

There is no default setting.

Command Modes

Privileged EXEC

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 can use this command to reauthenticate a client without waiting for the configured number of seconds between reauthentication attempts (reauthperiod) and automatic reauthentication.

Examples

The following example shows how to manually reauthenticate the device connected to Fast Ethernet interface 0/1:

```
Router# dot1x re-authenticate interface fastethernet 0/1
Starting reauthentication on FastEthernet0/1.
```

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 *interface-name interface-number*	(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 Release12.3(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 supplicant interface

To configure the dot1x supplicant for a given interface, use the **dot1x supplicant interface**command in privileged EXEC mode. To disable the configuration, use the **no** form of this command.

dot1x supplicant {**start**| **stop**} *profile-name* **interface** *type number*

Syntax Description

start	Starts the supplicant for a given interface.
stop	Stops the supplicant for a given interface.
profile-name	Profile name.
type number	Interface type and number.

Command Default

The dot1x supplicant interface is not configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure the dot1x supplicant for a Gigabit Ethernet interface:

```
Router# dot1x supplicant start n1 interface GigabitEthernet 0/0/1
```

Related Commands

Command	Description
dot1x default	Resets the global 802.1X authentication parameters to their default values as specified in the latest IEEE 802.1X standard.

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 *seconds*	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 *seconds*	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 *seconds*	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 *seconds*	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). • 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 {*seconds* | **server**}	Configures the time, in seconds, after which an automatic reauthentication should be initiated. • 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. **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.

server-timeout *seconds*	Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. • 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 the server does not send a response to an 802.1X packet within the specified period, the packet is sent again.
start-period *seconds*	Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. • The value is from 1 to 65535. The default is 30.
supp-timeout *seconds*	Sets the authenticator-to-supplicant retransmission time for all EAP messages other than EAP Request ID. • 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 *seconds*	Configures the number of seconds between retransmission of EAP request ID packets (assuming that no response is received) to the client. • 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 Switchs (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 *seconds*	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 *seconds*	Specifies the number of seconds between reauthentication attempts. The range is from 1 to 4294967295. The default is 3660 seconds.
tx-period *seconds*	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.

dpd

To configure Dead Peer Detection (DPD), use the **dpd**command in IKEv2 profile configuration mode. To delete DPD, use the **no** form of this command.

dpd *interval retry-interval* {**on-demand**| **periodic**}

no dpd

Syntax Description

interval	Specifies the keepalive interval in seconds. The range is 10 to 3600.
retry-interval	Specifies the retry interval in seconds when there is no reply from the peer.
on-demand	Specifies the on-demand mode to send the keepalive only in the absence of any incoming data traffic, to check the liveness of the peer before sending any data.
periodic	Specifies the periodic mode to send keepalives regularly at a specified interval.

Command Default

DPD is disabled by default.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use this command to configure DPD globally for peers matching a profile. The DPD configuration in an Internet Key Exchange Version 2 (IKEv2) profile overrides the global DPD configuration.

Examples

The following example shows how to configure the periodic mode for DPD:

```
Router(config)# crypto ikev2 profile prf1
Router(config-ikev2-profile)# dpd 1000 250 periodic
```

Related Commands

Command	Description
crypto ikev2 dpd	Defines DPD globally for all peers.
crypto ikev2 profile	Defines IKEv2 profile.

drop (type access-control)

Note Effective with Cisco IOS Release 15.2(4)M, the **drop** command is not available in Cisco IOS software.

To configure a traffic class to discard packets belonging to a specific class, use the **drop** command in policy-map class configuration mode. To disable the packet discarding action in a traffic class, use the **no** form of this command.

drop [all]

no drop [all]

Syntax Description

all	(Optional) Discards the entire stream of packets belonging to the traffic class.

Command Default

The packet discarding action in a traffic class is disabled.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
15.1(3)T	This command was introduced.
15.2(4)M	This command was removed from the Cisco IOS software.

Usage Guidelines

Once the match criteria are applied to packets belonging to the specific traffic class using the **match class session** command in a class map, these packets can be discarded by configuring the **drop** command with the **all** keyword in a policy map. Packets match only on the packet session (flow) entry of the Flexible Packet Matching (FPM) access control list (ACL) pattern matching tool, and skip user-configured classification filters. When the **drop** command is specified with the **all** keyword, this command can only be associated with a class map that was created with the **class-map** command and **type access-control** keyword and used in a policy map that can be attached to one or more interfaces to specify a service policy that is created with the **policy-map** command and **type access-control** keyword.

Examples

The following example shows how to create and configure a traffic class called class1 for use in a policy map called **policy1**. The policy map (service policy) is attached to output serial interface 2/0. All packets that match access group 101 are placed in class1. Packets that belong to this class are discarded.

```
Router(config)# class-map class1
```

```
Router(config-cmap)# match access-group 101
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial2/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
```

The following example shows how to configure a class map and policy map to specify the protocol stack class, the match criteria and action to take, and a combination of classes using session-based (flow-based) and nonsession-based actions. The **drop all** command is associated with the action to be taken on the policy.

```
Router(config)# class-map type access-control match-all my-HTTP
Router(config-cm)# match field tcp destport eq 8080
Router(config-cm)# match start tcp payload-start offset 20 size 10 regex "GET"
Router(config)# class-map type access-control match-all my-FTP
Router(config-cmap)# match field tcp destport eq 21
Router(config)# class-map type access-control match all class1
Router(config-cmap)# match class my-HTTP session
Router(config-cmap)# match start tcp payload-start offset 40 size 20 regex "abc.*def"
Router(config)# policy-map type access-control my_http_policy
Router(config-pmap)# class class1
Router(config-pmap-c)# drop all
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input my_http_policy
```

Related Commands

Command	Description
class	Specifies the name of a predefined traffic class, which was configured with the **class-map** command. The **class** command also classifies traffic to the traffic policy and enters policy-map class configuration mode.
class-map type access-control	Creates a class map to be used for matching packets to a specified class and enters class-map configuration mode for determining the exact pattern to look for in the protocol stack of interest.
log	Generates log messages for a predefined traffic class.
match class session	Configures match criteria for a class map used to identify a session (flow) containing packets of interest, which is then applied to all packets transmitted during the session.
policy-map type access-control	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy, and enters policy-map configuration mode.
show class-map	Displays all class maps and their matching criteria.

Command	Description
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

drop (zone-based policy)

To drop packets that are sent to the router, use the **drop** command in policy-map-class configuration mode.

drop [log]

Syntax Description

log	(Optional) Displays logging messages about dropped packets.

Command Default

Packets are not dropped.

Command Modes

Policy-map-class configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(1)S	This command was introduced into Cisco IOS Release 15.1(1)S.

Usage Guidelines

You can use this command only after entering the **policy-map type inspect** and **class type inspect** commands.

In Cisco IOS Release 15.1(2)T and earlier releases, if you use the **drop** command to configure a zone-based firewall with IP multicast traffic, all multicast updates are dropped by the zone-based firewall.

In Cisco IOS Release 15.1(3)T and later releases, all multicast updates are passed by the zone-based firewall even if you explicitly configure the **drop** command for a zone-based firewall with IP multicast traffic.

Examples

The following example creates an inspect policy map named p1 and specifies that packets will be dropped on the traffic at c1:

```
policy-map type inspect p1
 class type inspect c1
  drop
```

The following example defines a policy map that will drop HTTP traffic:

```
access-list 101 permit ip 192.168.1 0.0.0.255 any
 class-map type inspect match-all c1
  match access-group 101
  match protocol http
policy-map type inspect p1
 class type inspect c1
 drop
```

Related Commands

Command	Description
class type inspect	Specifies the traffic (class) on which an action is to be performed.
policy-map type inspect	Creates Layer 3 and Layer 4 inspect type policy maps.

drop-unsecure

To drop messages with no or invalid options or an invalid signature, use the **drop-unsecure**command in neighbor discovery (ND) inspection policy configuration mode or or router advertisement (RA) guard policy configuration mode. To disable this function, use the **no** form of this command.

drop-unsecure

no drop-unsecure

Syntax Description

This command has no arguments or keywords.

Command Default

No ND inspection policies are configured.

Command Modes

ND inspection policy configuration (config-nd-inspection)

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **drop-unsecure** command drops messages with no or invalid Cryptographically Generated Address (CGA) options or Rivest, Shamir, and Adleman (RSA) signature as per RFC 3971, *Secure Discovery (SeND)*. However, note that messages with an RSA signature or CGA options that do not conform with or are not verified per RFC 3972, *Cryptographically Generated Addresses (CGA)*, are dropped.

Use the **drop-unsecure** command after enabling ND inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an ND policy name as policy1, places the router in ND inspection policy configuration mode, and enables the router to drop messages with invalid CGA options or an invalid RSA signature:

```
Router(config)# ipv6 nd-inspection policy policy1
Router(config-nd-inspection)# drop-unsecure
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy name and enters ND inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

dtls port

To configure a desired port for the Datagram Transport Layer Security (DTLS) to listen, use the **dtls port**command in WebVPN gateway configuration mode. To disable the port, use the **no** form of this command.

dtls port *port-number*

no dtls port *port-number*

Syntax Description

port-number	DTLS port number. Range: 1025 to 65535. Default: 443.

Command Default

The default DTLS port is 443.

Command Modes

WebVPN gateway configuration (config-webvpn-gateway)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

DTLS listens on port 443 by default. You can configure the desired DTLS port using the **dtls port** command.

Examples

The following example shows how to configure 1055 as the DTLS port for a WebVPN gateway “gateway1”:

```
Router# configure terminal
Router(config)# webvpn gateway gateway1
Router(config-webvpn-gateway)# dtls port 1055
```

Related Commands

Command	Description
svc dtls	Enables DTLS support on the Cisco IOS SSL VPN.

dynamic

To define a named dynamic IP access list, use the **dynamic** command in access-list configuration mode . To remove the access lists, use the **no** form of this command.

dynamic *dynamic-name* [**timeout** *minutes*] {**deny**| **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] **[log] [fragments]**

no dynamic *dynamic-name*

Internet Control Message Protocol (ICMP)

dynamic *dynamic-name* [**timeout** *minutes*] {**deny**| **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*]| *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] **[log] [fragments]**

Internet Group Management Protocol (IGMP)

dynamic *dynamic-name* [**timeout** *minutes*] {**deny**| **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] **[log] [fragments]**

Transmission Control Protocol (TCP)

dynamic *dynamic-name* [**timeout** *minutes*] {**deny**| **permit**} **tcp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] **[established]** [**precedence** *precedence*] [**tos** *tos*] **[log] [fragments]**

User Datagram Protocol (UDP)

dynamic *dynamic-name* [**timeout** *minutes*] {**deny**| **permit**} **udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] **[log] [fragments]**

Syntax Description

dynamic-name	Identifies this access list as a dynamic access list. Refer to lock-and- key access documented in the "Configuring Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Cisco IOSSecurity Configuration Guide* .
timeout *minutes*	(Optional) Specifies the absolute length of time (in minutes) that a temporary access-list entry can remain in a dynamic access list. The default is an infinite length of time and allows an entry to remain permanently. Refer to lock-and-key access documented in the "Configuring Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Cisco IOSSecurity Configuration Guide* .
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.

protocol	Name or number of an Internet protocol. It can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the **ip**keyword. Some protocols allow further qualifiers described later.
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted decimal format. • Use the **any**keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard*of *source* 0.0.0.0.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part, dotted decimal format . • Use the **any**keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.

destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place 1s in the bit positions you want to ignore. • Use the **any**keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7, or by name as listed in the section "Usage Guidelines."
tos *tos*	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by name as listed in the section "Usage Guidelines."
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

fragments	(Optional) The access-list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
icmp-code	(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are found in the section "Usage Guidelines."
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the section "Usage Guidelines."
operator	(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.
port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535 . TCP and UDP port names are listed in the section "Usage Guidelines" of the **access-list**(IP extended) command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.

Command Default

An extended access list defaults to a list that denies everything. An extended access list is terminated by an implicit deny statement.

Command Modes

Access-list configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(11)	The **fragments**keyword was added.
12.2(13)T	The igrp keyword was removed because the IGRP protocol is no longer available in Cisco IOS software.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(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

You can use named access lists to control the transmission of packets on an interface and restrict contents of routing updates. The Cisco IOS software stops checking the extended access list after a match occurs.

Fragmented IP packets, other than the initial fragment, are immediately accepted by any extended IP access list. Extended access lists used to control vty access or restrict the contents of routing updates must not match against the TCP source port, the ToS value, or the precedence of the packet.

Note Named IP access lists will not be recognized by any software release prior to Cisco IOS Release 11.2.

Note After an access list is created, any subsequent additions (possibly entered from the terminal) are placed at the end of the list. In other words, you cannot selectively add or remove access list command lines from a specific access list.

The following is a list of precedence names:

- **critical**
- **flash**
- **flash-override**
- **immediate**
- **internet**

- **network**
- **priority**
- **routine**

The following is a list of ToS names:

- **max-reliability**
- **max-throughput**
- **min-delay**
- **min-monetary-cost**
- **normal**

The following is a list of ICMP message type and code names:

- **administratively-prohibited**
- **alternate-address**
- **conversion-error**
- **dod-host-prohibited**
- **dod-net-prohibited**
- **echo**
- **echo-reply**
- **general-parameter-problem**
- **host-isolated**
- **host-precedence-unreachable**
- **host-redirect**
- **host-tos-redirect**
- **host-tos-unreachable**
- **host-unknown**
- **host-unreachable**
- **information-reply**
- **information-request**
- **mask-reply**
- **mask-request**
- **mobile-redirect**
- **net-redirect**
- **net-tos-redirect**
- **net-tos-unreachable**

- **net-unreachable**
- **network-unknown**
- **no-room-for-option**
- **option-missing**
- **packet-too-big**
- **parameter-problem**
- **port-unreachable**
- **precedence-unreachable**
- **protocol-unreachable**
- **reassembly-timeout**
- **redirect**
- **router-advertisement**
- **router-solicitation**
- **source-quench**
- **source-route-failed**
- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**
- **traceroute**
- **ttl-exceeded**
- **unreachable**

The following is a list of IGMP message names:

- **dvmrp**
- **host-query**
- **host-report**
- **pim**
- **trace**

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current assigned numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found if you type a ? in the place of a port number.

- **bgp**
- **chargen**
- **daytime**

- **discard**
- **domain**
- **echo**
- **finger**
- **ftp**
- **ftp-data**
- **gopher**
- **hostname**
- **irc**
- **klogin**
- **kshell**
- **lpd**
- **nntp**
- **pop2**
- **pop3**
- **smtp**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **telnet**
- **time**
- **uucp**
- **whois**
- **www**

The following is a list of UDP port names that can be used instead of port numbers. Refer to the current assigned numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found if you type a ? in the place of a port number.

- **biff**
- **bootpc**
- **bootps**
- **discard**
- **dns**
- **dnsix**

- **echo**
- **mobile-ip**
- **nameserver**
- **netbios-dgm**
- **netbios-ns**
- **ntp**
- **rip**
- **snmp**
- **snmptrap**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **tftp**
- **time**
- **who**
- **xdmcp**

Access List Processing of Fragments

The behavior of access-list entries regarding the use or lack of the **fragments** keyword can be summarized as follows:

If the Access-List Entry has...	Then..

...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access-list entry containing only Layer 3 information:
	• The entry is applied to nonfragmented packets, initial fragments and noninitial fragments.
	For an access-list entry containing Layer 3 and Layer 4 information:
	• The entry is applied to nonfragmented packets and initial fragments.
	  • If the entry is a **permit**statement, the packet or fragment is permitted.
	  • If the entry is a **deny**statement, the packet or fragment is denied.
	• The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and
	  • If the entry is a **permit**statement, the noninitial fragment is permitted.
	  • If the entry is a **deny** statement, the next access-list entry is processed.
	Note The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.

...the **fragments** keyword, and assuming all of the access-list entry information matches,	**Note** The access-list entry is applied only to noninitial fragments.The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information.

Be aware that you should not simply add the **fragments** keyword to every access-list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments**keyword, the packet is compared to the next access-list entry, and so on, until it is either permitted or denied by an access-list entry that does not contain the **fragments** keyword. Therefore, you may need two access-list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where there are multiple **deny** access-list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments**keyword cannot solve all cases involving access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address**s command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access-list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

Examples

The following example defines a dynamic access list named abclist:

```
ip access-group abclist in
!
ip access-list extended abclist
 dynamic testlist timeout 5
 permit ip any any
 permit tcp any host 10.302.21.2 eq 23
```

Related Commands

Command	Description
clear access-template	Clears a temporary access-list entry from a dynamic access list manually.
distribute-list in (IP)	Filters networks received in updates.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
logging console	Limits messages logged to the console based on severity.
show access-lists	Displays the contents of current IP and rate-limit access lists.
show ip access-list	Displays the contents of all current IP access lists.