aaa max-sessions through algorithm

aaa memory threshold

To set appropriate threshold values for the authentication, authorization, and accounting (AAA) memory parameters, use the **aaa memory threshold** command in global configuration mode. To remove threshold values for the AAA memory parameters, use the **no** form of this command.

aaa memory threshold {**accounting disable** *available-memory*| **authentication reject** *available-memory*}

no aaa memory threshold {**accounting disable**| **authentication reject**}

Syntax Description

accounting	Sets the AAA accounting low-memory threshold.
disable	Disables the accounting threshold, if the available memory falls below the specified percentage.
available-memory	Available memory threshold. The range is from 1 to 15.
authentication	Sets the AAA authentication low-memory threshold.
reject	Rejects the AAA authentication request, if the available memory falls below the specified percentage.
available-memory	Available memory threshold. The range is from 2 to 15.

Command Default

The default memory threshold value for authentication is 3, and the default memory threshold value for accounting is 2.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

You must use the **aaa new-model** command to enable AAA.

Examples

The following example shows how to set the threshold values for the AAA accounting low-memory threshold:

```
Router> enable
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa memory threshold accounting disable 2
```

Related Commands

Command	Description
show aaa memory	Displays the output of the AAA data structure memory tracing information.

aaa nas cisco-nas-port use-async-info

To display physical interface information and parent interface details as part of the of the cisco-nas-port vendor-specific attribute (VSA) for login calls, use the **aaa nas cisco-nas-port use-async-info**command in global configuration mode. To disable the command, use the **no** form of the command.

aaa nas cisco-nas-port use-async-info

no aaa nas cisco-nas-port use-async-info

Syntax Description

This command has no arguments or keywords.

Command Default

The cisco-nas-port attribute has the format of tty*x*/*y* for login calls. Physical interface information is not included.

Command Modes

Global configuration

Command History

Release	Modification
12.3(17)	This command was introduced on the Cisco AS5800.

Usage Guidelines

This command enables the display of interface and parent interface details for login calls.

When this command is not configured, the cisco-nas-port attribute provides only tty*x*/*y* information for login calls. No physical interface information is included. For example:

```
Oct 14 18:42:53.113: RADIUS:  Vendor, Cisco       [26]  17
Oct 14 18:42:53.113: RADIUS:   cisco-nas-port     [2]   11  "tty1/2/07"
```

Other calls, such as PPP, include the physical interface and parent interface details. For example:

```
Oct 14 18:36:00.692: RADIUS:  Vendor, Cisco       [26]  33
Oct 14 18:36:00.692: RADIUS:   cisco-nas-port     [2]   27  "Async1/2/07*Serial1/1/2:0"
```

When you issue the **aaa nas cisco-nas-port use-async-info**command, the interface and parent interface details are included in the login calls.

Examples

The following example shows how to enable the display of interface and parent interface details in the login calls :

```
aaa nas cisco-nas-port use-async-info
```

Related Commands

Command	Description
aaa nas port extended	Replaces the NAS-port attribute with RADIUS IETF attribute 26 and displays extended field information.

aaa nas port extended

To replace the NAS-Port attribute with RADIUS IETF attribute 26 and to display extended field information, use the **aaa nas port extended**command inglobal configuration mode. To display no extended field information, use the **no** form of this command.

aaa nas port extended

no aaa nas port extended

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3	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 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

On platforms with multiple interfaces (ports) per slot, the Cisco RADIUS implementation will not provide a unique NAS-Port attribute that permits distinguishing between the interfaces. For example, if a dual PRI interface is in slot 1, calls on both Serial1/0:1 and Serial1/1:1 will appear as NAS-Port = 20101 due to the 16-bit field size limitation associated with RADIUS IETF NAS-Port attribute.

In this case, the solution is to replace the NAS-Port attribute with a vendor-specific attribute (RADIUS IETF Attribute 26). Cisco's vendor ID is 9, and the Cisco-NAS-Port attribute is subtype 2. Vendor-specific attributes (VSAs) can be turned on by entering the **radius-server vsa send** command. The port information in this attribute is provided and configured using the **aaa nas port extended** command.

The standard NAS-Port attribute (RADIUS IETF attribute 5) will continue to be sent. If you do not want this information to be sent, you can suppress it by using the **no radius-server attribute nas-port** command. When this command is configured, the standard NAS-Port attribute will no longer be sent.

Examples

The following example specifies that RADIUS will display extended interface information:

```
radius-server vsa send
aaa nas port extended
```

Related Commands

Command	Description
radius-server extended-portnames	Displays expanded interface information in the NAS-Port attribute.
radius-server vsa send	Configures the network access server to recognize and use vendor-specific attributes.

aaa nas port option82

To send the remote-id and circuit-id as the NAS-Port-Id attribute in the Access-Request and Accounting-Request, use the **aaa nas port option82** command in global configuration mode. To disable this option, use the **no** form of this command.

aaa nas port option82

no aaa nas port option82

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2SB	This command was introduced in Cisco IOS Release 12.2SB.

Usage Guidelines

On platforms with multiple interfaces (ports) per slot, the Cisco RADIUS implementation will not provide a unique NAS-Port attribute that permits distinguishing between the interfaces. For example, if a dual PRI interface is in slot 1, calls on both Serial1/0:1 and Serial1/1:1 will appear as NAS-Port = 20101 due to the 16-bit field size limitation of the RADIUS IETF NAS-Port attribute.

In this case, the solution is to replace the NAS-Port attribute with the vendor-specific attribute (VSA) RADIUS IETF Attribute 26. The Cisco vendor ID is 9, and the Cisco-NAS-Port attribute is subtype 2. VSAs can be turned on by entering the **radius-server vsa send** command. The NAS-Port string information in this attribute is provided and configured using the **aaa nas port option82** command.

The standard NAS-Port attribute (RADIUS IETF attribute 5) will continue to be sent. If you do not want this information to be sent, you can suppress it by using the **no radius-server attribute nas-port** command. When this command is configured, the standard NAS-Port attribute will no longer be sent.

The NAS-Port information is populated in the Intelligent Service Gateway (ISG) interface that has received the DHCP **option82** packet. When the **aaa nas port option82** command is configured, the NAS-Port is populated with the information regarding the remote-id and circuit-id. If this command is not configured, the NAS-Port is populated with the local ISG NAS-Port-Id.

Examples

The following example specifies that RADIUS will display extended interface information:

```
radius-server vsa send
aaa nas port option82
```

Related Commands

Command	Description
radius-server vsa send	Configures the network access server to recognize and use VSAs.

aaa nas redirected-station

To include the original number in the information sent to the authentication server when the number dialed by a device is redirected to another number for authentication, use the **aaa nas redirected-station** command in global configuration mode. To leave the original number out of the information sent to the authentication server, use the **no** form of this command.

aaa nas redirected-station

no aaa nas redirected-station

Syntax Description

This command has no arguments or keywords.

Command Default

The original number is not included in the information sent to the authentication server.

Command Modes

Global configuration

Command History

Release	Modification
12.1 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 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 a customer is being authenticated by a RADIUS or TACACS+ server and the number dialed by the cable modem (or other device) is redirected to another number for authentication, the **aaa nas redirected-station** command will enable the original number to be included in the information sent to the authentication server.

This functionality allows the service provider to determine whether the customer dialed a number that requires special billing arrangements, such as a toll-free number.

The original number can be sent as a Cisco Vendor Specific Attribute (VSA) for TACACS+ servers and as RADIUS Attribute 93 (Ascend-Redirect-Number) for RADIUS servers. The RADIUS Attribute 93 is sent by default; to also send a VSA attribute for TACACS+ servers, use the **radius-server vsa send accounting** and **radius-server vsa send authentication** commands. To configure the RADIUS server to use RADIUS Attribute 93, add the non-standard option to the **radius-server host** command.

Note This feature is valid only when using port adapters that are configured for a T1 or E1 ISDN PRI or BRI interface. In addition, the telco switch performing the number redirection must be able to provide the redirected number in the Q.931 Digital Subscriber Signaling System Network Layer.

Examples

The following example enables the original number to be forwarded to the authentication server:

```
!
aaa authorization config-commands
aaa accounting exec default start-stop group radius
aaa accounting system default start-stop broadcast group apn23
aaa nas redirected-station
aaa session-id common
ip subnet-zero
!
```

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.
radius-server vsa	Configures the network access server to recognize and use vendor-specific attributes.

aaa new-model

To enable the authentication, authorization, and accounting (AAA) access control model, issue the **aaa new-model** command in global configuration mode. To disable the AAA access control model, use the **no** form of this command.

aaa new-model

no aaa new-model

Syntax Description

This command has no arguments or keywords.

Command Default

AAA is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2(33)SXI	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.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command enables the AAA access control system.

Examples

The following example initializes AAA:

```
aaa new-model
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication arap	Enables an AAA authentication method for ARAP using TACACS+.
aaa authentication enable default	Enables AAA authentication to determine if a user can access the privileged command level.
aaa authentication login	Sets AAA authentication at login.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.

aaa password

To configure restrictions for an authentication, authorization, and accounting (AAA) password, use the **aaa password** command in global configuration mode. To disable the password restriction, use the **no** form of this command.

aaa password restriction

no aaa password restriction

Syntax Description

restriction	Configures restrictions to the password.

Command Default

AAA passwords have no restrictions.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **aaa password** command can be used only if the **aaa new-model** command is configured. The restrictions are not applied to passwords in the startup configurations. The restrictions are not applied to passwords that are already present in the configurations before the **aaa password** command is enabled.

Passwords are subject to the following restrictions:

- The new password must contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- The new password should not have a character repeated more than three times consecutively.
- The new password should not be the same as the associated username. The password obtained by capitalization of the username or username reversed is not accepted.
- The new password should not be “cisco”, “ocsic”, or any variant obtained by changing the capitalization of letters therein, or by substituting “1”, “|”, or “!” for i, or by substituting “0” for “o”, or substituting “$” for “s”.

The restrictions can be applied to the passwords configured using the following commands: **aaa pod server**,**enable password**, **enable secret**, **radius-server host key**, **radius-server key**, **server-key**, and the**tacacs-server key**command.

Examples

The following example shows how to configure restrictions for an AAA password:

```
Router(config)# aaa password restriction
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
aaa pod server	Enables inbound user sessions to be disconnected when specific session attributes are present.
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the **enable password** command.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server host	Specifies a RADIUS server host.
server-key	Configure the RADIUS key to be shared between a device and RADIUS clients.
tacacs-server host	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.
tacacs-server key	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.

aaa pod server

To enable inbound user sessions to be disconnected when specific session attributes are presented, use the **aaa pod server** command in global configuration mode. To disable the configuration, use the **no** form of this command.

aaa pod server [**clients** *ip-address1 ip-address2 ... ip-addressn*] [**port** *port-number*] {**auth-type** [**all ignore**| **any ignore**] **session-key server-key** *string*| **ignore [session-key] server-key**| **server-key** *string*}

no aaa pod server

Syntax Description

clients *ip-address*	(Optional) Registers the IP address of all the clients who can send POD requests. If this configuration is present and a POD request originates from a device that is not on the list, it is rejected. You can specify only four client IP addresses.
port *port number*	(Optional) Network access server User Datagram Protocol (UDP) port to use for packet of disconnect (POD) requests. Default value is 1700.
auth-type	Type of authorization required for disconnecting sessions. If no authentication type is specified, **auth-type** is the default.
all	(Optional) Only a session that matches all four key attributes is disconnected.T he default is **all**.
any	(Optional) Session that matches all of the attributes sent in the POD packet is disconnected. The POD packet may contain one or more of four key attributes (user-name, framed-IP-address, session-ID, and session-key).
ignore	Ignores the session key or the server key received in the POD packet for session matching.
session-key	Session with a matching session-key attribute is disconnected. All other attributes are ignored.
server-key	Configures the shared-secret text string.
string	Shared-secret text string that is shared between the network access server and the client workstation. This shared-secret string must be the same on both systems.

Command Default The POD server function is disabled.

Command Modes Global configuration (config)

Command History

Release	Modification
12.1(2)XH	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.2(2)XB	The encryption-type argument was added, as well as support for the voice applications and the Cisco 3600 series, and Cisco AS5350, and Cisco AS5400 routers.
12.2(2)XB1	Support for the Cisco AS5800 was added.
12.2(11)T	The *encryption-type* argument and support for the voice applications were added. **Note** Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 is not included in this release.
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.
15.0(1)M	This command was modified. The **clients** and **ignore** keywords were added.

Usage Guidelines To disconnect a session, the values in one or more of the key fields in the POD request must match the values for a session on one of the network access server ports. Which values must match depends on the **auth-type** attribute defined in the command. If no **auth-type** attribute is specified, all three values must match. If no match is found, all connections remain intact and an error response is returned. The key fields are as follows:

- An h323-conf-id vendor-specific attribute (VSA) with the same content as received from the gateway for this call.
- An h323-call-origin VSA with the same content as received from the gateway for the leg of interest.
- A 16-byte Message Digest 5 (MD5) hash value that is carried in the *authentication* field of the POD request.

Examples The following example shows how to enable POD and set the secret key to “xyz123”:

```
aaa pod server server-key xyz123
```

Related Commands

Command	Description
aaa accounting delay-start	Delays generation of the start accounting record until the user IP address is established.
aaa accounting	Enables accounting records.
debug aaa pod	Displays debug messages for POD packets.
radius-server host	Identifies a RADIUS host.

aaa preauth

To enter authentication, authorization, and accounting (AAA) preauthentication configuration mode, use the **aaa preauth** command in global configuration mode. To disable preauthentication, use the **no** form of this command.

aaa preauth

no aaa preauth

Syntax Description

This command has no arguments or keywords.

Command Default

Preauthentication is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)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 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

To enter AAA preauthentication configuration mode, use the **aaa preauth** command. To configure preauthentication, use a combination of the **aaa preauth** commands: **group**, **clid**, **ctype**, **dnis**, and **dnis bypass**. You must configure the **group** command. You must also configure one or more of the **clid**, **ctype**, **dnis**, or **dnis bypass** commands.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

You can use the **clid**, **ctype**, or **dnis** commands to define the list of the preauthentication elements. For each preauthentication element, you can also define options such as password (for all the elements, the default password is cisco). If you specify multiple elements, the preauthentication process will be performed on each element according to the order of the elements that you configure with the preauthentication commands. In this case, more than one RADIUS preauthentication profile is returned, but only the last preauthentication profile will be applied to the authentication and authorization later on, if applicable.

Examples

The following example enables dialed number identification service (DNIS) preauthentication using a RADIUS server and the password Ascend-DNIS:

```
aaa preauth
 dnis password Ascend-DNIS
```

Related Commands

Command	Description
dnis (authentication)	Enables AAA preauthentication using DNIS.
group (authentication)	Selects the security server to use for AAA preauthentication.
isdn guard-timer	Sets a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request.

aaa processes

To allocate a specific number of background processes to be used to process authentication, authorization, and accounting (AAA) authentication and authorization requests for PPP, use the **aaa processes**command in global configuration mode. To restore the default value for this command, use the **no** form of this command.

aaa processes *number*

no aaa processes *number*

Syntax Description

number	Specifies the number of background processes allocated for AAA requests for PPP. Valid entries are 1 to 2147483647.

Command Default

The default for this command is one allocated background process.

Command Modes

Global configuration

Command History

Release	Modification
11.3(2)AA	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 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 the **aaa processes** command to allocate a specific number of background processes to simultaneously handle multiple AAA authentication and authorization requests for PPP. Previously, only one background process handled all AAA requests for PPP, so only one new user could be authenticated or authorized at a time. This command configures the number of processes used to handle AAA requests for PPP, increasing the number of users that can be simultaneously authenticated or authorized.

The argument *number* defines the number of background processes earmarked to process AAA authentication and authorization requests for PPP. This argument also defines the number of new users that can be simultaneously authenticated and can be increased or decreased at any time.

Examples

The following examples shows the **aaa processes** command within a standard AAA configuration. The authentication method list “dialins” specifies RADIUS as the method of authentication, then (if the RADIUS

server does not respond) local authentication will be used on serial lines using PPP. Ten background processes have been allocated to handle AAA requests for PPP.

```
aaa new-model
aaa authentication ppp dialins group radius local
aaa processes 10
interface 5
encap ppp
ppp authentication pap dialins
```

Related Commands

Command	Description
show ppp queues	Monitors the number of requests processed by each AAA background process.

aaa route download

To enable the static route download feature and set the amount of time between downloads, use the **aaa route download** command in global configuration mode. To disable this function, use the **no** form of this command.

aaa route download [*time*] [**authorization** *method-list*]

no aaa route download

Syntax Description

time	(Optional) Time between downloads, in minutes. The range is from 1 to 1440 minutes.
authorization *method-list*	(Optional) Specify a named method list to which RADIUS authorization requests for static route downloads are sent. If these attributes are not set, all RADIUS authorization requests will be sent to the servers that are specified by the default method list.

Command Default

The default period between downloads (updates) is 720 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1	This command was integrated into Cisco IOS Release 12.1.
12.2(8)T	The **authorization** keyword was added; the *method-list* argument was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

This command is used to download static route details from the authorization, authentication, and accounting (AAA) server if the name of the router is *hostname*. The name passed to the AAA server for static routes is *hostname-1*, *hostname-2*... *hostname-n*--the router downloads static routes until it fails an index and no more routes can be downloaded.

Examples

The following example sets the AAA route update period to 100 minutes:

```
aaa route download 100
```

The following example sets the AAA route update period to 10 minutes and sends static route download requests to the servers specified by the method list name “list1”:

```
aaa route download 10 authorization list1
```

Related Commands

Command	Description
aaa authorization configuration default	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
clear ip route download	Clears static routes downloaded from a AAA server.
show ip route	Displays all static IP routes, or those installed using the AAA route download function.

aaa server radius dynamic-author

To configure a device as an authentication, authorization, and accounting (AAA) server to facilitate interaction with an external policy server, use the **aaa server radius dynamic-author**command in global configuration mode. To remove this configuration, use the **no** form of this command.

aaa server radius dynamic-author

no aaa server radius dynamic-author

Syntax Description

This command has no arguments or keywords.

Command Default

The device will not function as a server when interacting with external policy servers.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
12.2(5)SXI	This command was integrated into Cisco IOS Release 12.2(5)SXI.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Dynamic authorization allows an external policy server to dynamically send updates to a device. Once the **aaa server radius dynamic-author** command is configured, dynamic authorization local server configuration mode is entered. Once in this mode, the RADIUS application commands can be configured.

Dynamic Authorization for the Intelligent Services Gateway (ISG)

ISG works with external devices, referred to as policy servers, that store per-subscriber and per-service information. ISG supports two models of interaction between the ISG device and external policy servers: initial authorization and dynamic authorization.

The dynamic authorization model allows an external policy server to dynamically send policies to the ISG. These operations can be initiated in-band by subscribers (through service selection) or through the actions of an administrator, or applications can change policies on the basis of an algorithm (for example, change session quality of service (QoS) at a certain time of day). This model is facilitated by the Change of Authorization (CoA) RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling ISG and the external policy server each to act as a RADIUS client and server.

Examples

The following example configures the ISG to act as a AAA server when interacting with the client at IP address 10.12.12.12:

```
aaa server radius dynamic-author
 client 10.12.12.12 key cisco
 message-authenticator ignore
```

Related Commands

Command	Description
auth-type (ISG)	Specifies the server authorization type.
client	Specifies a RADIUS client from which a device will accept CoA and disconnect requests.
default	Sets a RADIUS application command to its default.
domain	Specifies username domain options.
ignore	Overrides a behavior to ignore certain paremeters.
port	Specifies a port on which local RADIUS server listens.
server-key	Specifies the encryption key shared with RADIUS clients.

aaa service-profile

To configure the service profile parameters for an authentication, authorization, and accounting (AAA) session, use the **aaa service-profile** command in global configuration mode. To disable the service profile parameters for AAA sessions, use the **no** form of this command.

aaa service-profile key username-with-nasport

no aaa service-profile key username-with-nasport

Syntax Description

key	Assigns a key to save and search service profiles.
username-with-nasport	Configures the AAA server to use the username and network access server (NAS) port as the service profile key.

Command Default

Service profiles are stored based on the username.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Examples

The following example shows how to configure the service profile parameters for a AAA session:

```
Router# enable
Router# configure terminal
Router(config)# aaa service-profile key username-with-nasport
```

Related Commands

Command	Description
show aaa service-profiles	Displays the service profiles downloaded and stored by a AAA session.

aaa session-id

To specify whether the same session ID will be used for each authentication, authorization, and accounting (AAA) accounting service type within a call or whether a different session ID will be assigned to each accounting service type, use the **aaa session-id** command in global configuration mode. To restore the default behavior after the **unique** keyword is enabled, use the **no** form of this command.

aaa session-id [**common**| **unique**]

no aaa session-id [unique]

Syntax Description

common	(Optional) Ensures that all session identification (ID) information that is sent out for a given call will be made identical. The default behavior is **common**.
unique	(Optional) Ensures that only the corresponding service access-requests and accounting-requests will maintain a common session ID. Accounting-requests for each service will have a different session ID.

Command Default

The **common**keyword is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
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

The **common**keywordbehaviorallows the first session ID request of the call to be stored in a common database; all proceeding session ID requests will retrieve the value of the first session ID. Because a common session ID is the default behavior, this functionality is written to the system configuration after the **aaa new-model**command is configured.

Note The router configuration will always have either the **aaa session-id common** or the **aaa session-id unique** command enabled; it is not possible to have neither of the two enabled. Thus, the **no aaa session-id unique** command will revert to the default functionality, but the **no aaa session-id common** command will not have any effect because it is the default functionality.

The **unique** keyword behavior assigns a different session ID for each accounting type (Auth-Proxy, Exec, Network, Command, System, Connection, and Resource) during a call. To specify this behavior, the unique keyword must be specified. The session ID may be included in RADIUS access requests by configuring the **radius-server attribute 44 include-in-access-req**command. The session ID in the access-request will be the same as the session ID in the accounting request for the same service; all other services will provide unique session IDs for the same call.

Examples

The following example shows how to configure unique session IDs:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
aaa session-id unique
```

Related Commands

Command	Description
aaa new model	Enables AAA.
radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication).

aaa session-mib

To configure MIB options for Simple Network Management Protocol (SNMP) authentication, authorization, and accounting (AAA) sessions, use the aaa session-mib command in global configuration mode. To disable these options, use the **no** form of this command.

aaa session-mib {**disconnect**| **populate** {**setup**| **start**}}

no aaa session-mib {**disconnect**| **populate** {**setup**| **start**}}

Syntax Description

disconnect	Enables an AAA session MIB to disconnect authenticated clients using SNMP.
populate setup	Specifies that the AAA session MIB starts to track a session at the setup of the session.
populate start	Specifies that the AAA session MIB starts to track a session when accounting starts (when the START record is sent).

Command Default

No MIB options for SNMP AAA sessions are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.3(5)	The populate, setup and start keywords were added.
12.3(5a)B	The populate, setup and start keywords were added.
12.3(7)T	The populate, setup and start keywords were added.
12.2(16)BX3	The populate, setup and start keywords were added.
12.3(7)XI	The populate, setup and start keywords were added.
12.3(12)	The populate, setup and start keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
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

The disconnect keyword enables termination of authenticated client connections via SNMP. Without this keyword, a network management station cannot perform set operations and disconnect users (it can only poll the table).

The populate keyword determines when reporting of a locally terminated sessions begins. Two options are provided: setup (default) and start. The setup keyword begins tracking the session parameters during the setup of a session while the start keyword begins when the accounting START notification is generated and sent. By default, Cisco AAA session MIB begins reporting sessions generated during setup.

Examples

The following example shows how to enable the disconnection of authenticated clients using SNMP:

```
Router> enable
Router# configure terminal
Router(config)# aaa session-mib disconnect
```

The following example shows how to start tracking of a session at setup:

```
Router> enable
Router# configure terminal
Router(config)# aaa session-mib populate setup
```

aaa traceback recording

To enable traceback recording on an authentication, authorization, and accounting (AAA) server, use the **aaa traceback recording** command in global configuration mode. To disable the configuration, use the **no** form of this command.

aaa traceback recording

no aaa traceback recording

Syntax Description

This command has no arguments or keywords.

Command Default

Traceback recording is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to enable traceback recording on a AAA server:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa traceback recording
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.

aaa user profile

To create an authentication, authorization, and accounting (AAA) named user profile, use the **aaa user profile**command in global configuration mode. To remove a user profile from the configuration, use the **no** form of this command.

aaa user profile *profile-name*

no aaa user profile *profile-name*

Syntax Description

profile-name	Character string used to name the user profile. The maximum length of the character string is 63 characters. Longer strings will be truncated.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.3(3.8)	The maximum length of the *profile-name* argument is set at 63 characters.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use the **aaa user profile**command to create a AAA user profile. Used in conjunction with the aaa attribute command, which adds calling line identification (CLID) and dialed number identification service (DNIS) attribute values, the user profile can be associated with the record that is sent to the RADIUS server (via the **test aaa group**command), which provides the RADIUS server with access to CLID or DNIS attribute information when the server receives a RADIUS record.

Examples

The following example shows how to configure a dnis = dnisvalue user profile named “prfl1”:

```
aaa user profile prfl1
 aaa attribute dnis
 aaa attribute dnis dnisvalue
 no aaa attribute clid
! Attribute not found.
 aaa attribute clid clidvalue
 no aaa attribute clid
```

Related Commands

Command	Description
aaa attribute	Adds DNIS or CLID attribute values to a user profile.
test aaa group	Associates a DNIS or CLID user profile with the record that is sent to the RADIUS server.

access (firewall farm)

To route specific flows to a firewall farm, use the **access**command in firewall farm configuration mode. To restore the default settings, use the **no** form of this command.

access [**source** *source-ip netmask*| **destination** *destination-ip netmask*| **inbound** {*inbound-interface*| **datagram connection**}| **outbound** *outbound-interface*]

no access [**source** *source-ip netmask*| **destination** *destination-ip netmask*| **inbound** {*inbound-interface*| **datagram connection**}| **outbound** *outbound-interface*]

Syntax Description

source	(Optional) Routes flows based on source IP address.
source-ip	(Optional) Source IP address. The default is 0.0.0.0 (all sources).
netmask	(Optional) Source IP network mask. The default is 0.0.0.0 (all source subnets).
destination	(Optional) Routes flows based on destination IP address.
destination-ip	(Optional) Destination IP address. The default is 0.0.0.0 (all destinations).
netmask	(Optional) Destination IP network mask. The default is 0.0.0.0 (all destination subnets).
inbound *inbound-interface*	(Optional) Indicates that the firewall farm is to accept inbound packets only on the specified inbound interface. You can specify a subinterface, such as Gigabitethernet7/3.100, for the *inbound-interface*argument.
inbound datagram connection	(Optional) Indicates that IOS SLB is to create connections for inbound traffic as well as outbound traffic.
outbound *outbound-interface*	(Optional) Indicates that the firewall farm is to accept outbound packets only on the specified outbound interface. You can specify a subinterface, such as Gigabitethernet7/3.100, for the *outbound-interface*argument.

Command Default

The default source IP address is 0.0.0.0 (routes flows from all sources to this firewall farm). The default source IP network mask is 0.0.0.0 (routes flows from all source subnets to this firewall farm). The default destination IP address is 0.0.0.0 (routes flows from all destinations to this firewall farm). The default destination IP network mask is 0.0.0.0 (routes flows from all destination subnets to this firewall farm). If you do not specify an inbound interface, the firewall farm accepts inbound packets on all inbound interfaces. If you do not specify the **inbound datagram connection** option, IOS SLB creates connections only for outbound traffic. If you do not specify an outbound interface, the firewall farm accepts outbound packets on all outbound interfaces.

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

Release	Modification
12.1(7)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	The **inbound** and **outbound** keywords and *inbound-interface* and *outbound-interface* arguments were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified. The **datagram connection** keywords were added. The *inbound-interface*and *outbound-interface*arguments can be subinterfaces.

Usage Guidelines

You can specify more than one source or destination for each firewall farm. To do so, configure multiple **access** statements, making sure the network masks do not overlap each other.

You can specify up to two inbound interfaces and two outbound interfaces for each firewall farm. To do so, configure multiple **access** statements, keeping the following considerations in mind:

- All inbound and outbound interfaces must be in the same Virtual Private Network (VPN) routing and forwarding (VRF).
- All inbound and outbound interfaces must be different from each other.
- You cannot change inbound or outbound interfaces for a firewall farm while it is in service.

If you do not configure an access interface using this command, IOS SLB installs the wildcards for the firewall farm in all of the available interfaces of the device, including the VRF interfaces. If IOS SLB is not required on the VRF interfaces, use this command to limit wildcards to the specified interfaces only.

By default, IOS SLB firewall load balancing creates connections only for outbound traffic (that is, traffic that arrives through the real server). Inbound traffic uses those same connections to forward the traffic, which can impact the CPU. To enable IOS SLB to create connections for both inbound traffic and outbound traffic, reducing the impact on the CPU, use the **access inbound datagram connection** command.

Examples

The following example routes flows with a destination IP address of 10.1.6.0 to firewall farm FIRE1:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# access destination 10.1.6.0 255.255.255.0
```

Related Commands

Command	Description
show ip slb firewallfarm	Displays information about the firewall farm configuration.

access (server farm)

To configure an access interface for a server farm, use the **access** command in server farm configuration mode. To disable the access interface, use the **no** form of this command.

access *interface*

no access *interface*

Syntax Description

interface	Interface to be inspected. The server farm will handle outbound flows from real servers only on the specified interface. You can specify a subinterface, such as Gigabitethernet7/3.100, for the *interface*argument.

Command Default

The server farm handles outbound flows from real servers on all interfaces.

Command Modes

Server farm configuration (config-slb-sfarm)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified. The *interface*argument can be a subinterface.

Usage Guidelines

The virtual server and its associated server farm interfaces must be in the same Virtual Private Network (VPN) routing and forwarding (VRF).

You can specify up to two access interfaces for each server farm. To do so, configure two **access** statements, keeping the following considerations in mind:

- The two interfaces must be in the same VRF.
- The two interfaces must be different from each other.
- The access interfaces of primary and backup server farms must be the same.
- You cannot change the interfaces for a server farm while it is in service.

If you do not configure an access interface using this command, IOS SLB installs the wildcards for the server farm in all of the available interfaces of the device, including the VRF interfaces. If IOS SLB is not required on the VRF interfaces, use this command to limit wildcards to the specified interfaces only.

Examples

The following example limits the server farm to handling outbound flows from real servers only on access interface Vlan106:

```
Router(config)# ip slb serverfarm SF1
Router(config-slb-sfarm)# access Vlan106
```

Related Commands

Command	Description
show ip slb serverfarms	Displays information about the server farms.

access (virtual server)

To enable framed-IP routing to inspect the ingress interface, use the **access** command in virtual server configuration mode. To disable framed-IP routing, use the **no** form of this command.

access *interface* [**route framed-ip**]

no access *interface* [**route framed-ip**]

Syntax Description

interface	Interface to be inspected. You can specify a subinterface, such as Gigabitethernet7/3.100, for the *interface*argument.
route framed-ip	(Optional) Routes flows using framed-IP routing.

Command Default

Framed-IP routing cannot inspect the ingress interface.

Command Modes

Virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.1(12c)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	The command was modified to accept up to two framed-IP access interfaces (specified on separate commands).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified. The *interface*argument can be a subinterface.

Usage Guidelines

This command enables framed-IP routing to inspect the ingress interface when routing subscriber traffic. All framed-IP sticky database entries created as a result of RADIUS requests to this virtual server will include the interface in the entry. In addition to matching the source IP address of the traffic with the framed-IP address, the ingress interface must also match this interface when this command is configured.

You can use this command to allow subscriber data packets to be routed to multiple service gateway service farms.

The virtual server and its associated server farm interfaces must be in the same Virtual Private Network (VPN) routing and forwarding (VRF).

You can specify up to two framed-IP access interfaces for each virtual server. To do so, configure two **access** statements, keeping the following considerations in mind:

- The two interfaces must be in the same VRF.
- The two interfaces must be different from each other.
- You cannot change the interfaces for a virtual server while it is in service.

If you do not configure an access interface using this command, IOS SLB installs the wildcards for the virtual server in all of the available interfaces of the device, including the VRF interfaces. If IOS SLB is not required on the VRF interfaces, use this command to limit wildcards to the specified interfaces only.

Examples

The following example enables framed-IP routing to inspect ingress interface Vlan20:

```
Router(config)# ip slb vserver SSG_AUTH
Router(config-slb-vserver)# access Vlan20 route framed-ip
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers defined to IOS SLB.

access-class

To restrict incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list, use the **access-class** command in line configuration mode. To remove access restrictions, use the **no** form of this command.

access-class *access-list-number* {**in [vrf-also]| out**}

no access-class *access-list-number* {**in| out**}

Syntax Description

access-list-number	Number of an IP access list. This is a decimal number from 1 to 199 or from 1300 to 2699 .
in	Restricts incoming connections between a particular Cisco device and the addresses in the access list.
vrf-also	(Optional) Accepts incoming connections from interfaces that belong to a VRF.
out	Restricts outgoing connections between a particular Cisco device and the addresses in the access list.

Command Default

No access lists are defined.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2	The **vrf-also** keyword was added.
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

Remember to set *identical restrictions* on all the virtual terminal lines because a user can connect to any of them.

To display the access lists for a particular terminal line, use the **show line** EXEC command and specify the line number.

If you do not specify the **vrf-also** keyword, incoming Telnet connections from interfaces that are part of a VRF are rejected.

Examples

The following example defines an access list that permits only hosts on network 192.89.55.0 to connect to the virtual terminal ports on the router:

```
access-list 12 permit 192.89.55.0 0.0.0.255
 line 1 5
 access-class 12 in
```

The following example defines an access list that denies connections to networks other than network 10.0.0.0 on terminal lines 1 through 5:

```
access-list 10 permit 10.0.0.0 0.255.255.255
 line 1 5
 access-class 10 out
```

Related Commands

Command	Description
show line	Displays the parameters of a terminal line.

access-enable

To e na b le the router to create a temporary access list entry in a dynamic access list, use the **access-enable** command in EXEC mode.

access-enable [host] [**timeout** *minutes*]

Syntax Description

host	(Optional) Tells the software to enable access only for the host from which the Telnet session originated. If not specified, the software allows all hosts on the defined network to gain access. The dynamic access list contains the network mask to use for enabling the new network.
timeout *minutes*	(Optional) Specifies an idle timeout for the temporary access list entry. If the access list entry is not accessed within this period, it is automatically deleted and requires the user to authenticate again. The default is for the entries to remain permanently. We recommend that this value equal the idle timeout set for the WAN connection.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
11.1	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 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

This command enables the lock-and-key access feature.

You should always define either an idle timeout (with the **timeout** keyword in this command) or an absolute timeout (with the **timeout** keyword in the **access-list** command). Otherwise, the temporary access list entry will remain, even after the user terminates the session.

Use the **autocommand** command with the **access-enable** command to cause the **access-enable** command to execute when a user opens a Telnet session into the router.

Examples

The following example causes the software to create a temporary access list entry and tells the software to enable access only for the host from which the Telnet session originated. If the access list entry is not accessed within 2 minutes, it is deleted.

```
autocommand access-enable host timeout 2
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
autocommand	Configures the Cisco IOS software to automatically execute a command when a user connects to a particular line.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

access-group (identity policy)

To specify an access group to be applied to an identity policy, use the **access-group** command in identity policy configuration mode. To remove the access group, use the **no** form of this command.

access-group group-name

no access-group group-name

Syntax Description

group-name	Access list name.

Command Default

An access group is not specified.

Command Modes

Identity policy configuration

Command History

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

Usage Guidelines

Using this command, you can access only named access lists.

Examples

The following example shows that access group "exempt-acl" is to be applied to the identity policy "policyname1":

```
Router (config)# identity policy policyname1
Router (config-identity-policy)# access-group exempt-acl
```

Related Commands

Command	Description
identity profile	Creates an identity profile.

access-group mode

To specify override and nonoverride modes for an access group, use the **access-group mode** command in interface configuration mode. To return to merge mode, use the **no** form of this command.

access-group mode {**prefer** {**port**| **vlan**}| **merge**}

no access-group mode {**prefer** {**port**| **vlan**}| **merge**}

Syntax Description

prefer port	Specifies that port access control list (ACL) features that are configured on an interface port take precedence over features configured on a VLAN interface. (That is, features configured on the switch virtual interface [SVI] and the port are not merged.)
prefer vlan	Specifies that the VLAN-based ACL mode takes precedence if VLAN-based ACL features are configured on a VLAN interface. If no VLAN-based ACL features are configured on the VLAN interface, port ACL features are applied on the interface port.
merge	Merges features configured on the interface port and the interface VLAN. This merged feature is programmed into the hardware.

Command Default

The default is merge mode.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SXI4	This command was modified. Support for IPv6 was added. The **prefer vlan** keyword combination is not supported on Cisco IOS Release 12.2(33)SXI4.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

An SVI is a VLAN of switch ports that are represented by one interface to a routing or bridging system. VLAN ACLs or VLAN maps control the access of all packets (bridged and routed) to an interface.

Port ACLs perform access control on the traffic that enters a Layer 2 interface. Layer 2 interfaces support prefer ports, prefer VLANs, and merge modes. Layer 2 interfaces can have one IP ACL applied in either direction (one at the ingress and one at the egress). Layer 2 interfaces can have only one IPv6 ACL; either in the ingress or egress direction.

In Cisco IOS Release 12.2(33)SXI4, only prefer ports and merge modes are supported on Layer 2 interfaces.

To apply an IPv4 port ACL and a MAC ACL on a trunk port, you must configure the **access-group mode prefer port** command on the trunk port.

Examples

The following example shows how to configure an interface to use prefer port mode:

```
Device(config-if)# access-group mode prefer port
```

The following example shows how to configure an interface to use merge mode:

```
Device(config-if)# access-group mode merge
```

Related Commands

Command	Description
show access-group mode interface	Displays the ACL configuration on a Layer 2 interface.

access-list (IP extended)

To define an extended IP access list, use the extended version of the **access-list** command in global configuration mode . To remove the access lists, use the **no** form of this command.

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny**| **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence* | **dscp** *dscp* | **tos** *tos* | **time-range** *time-range-name* | **fragments** | **log** [*word*] | | **log-input** [*word*]]

no access-list *access-list-number*

Internet Control Message Protocol (ICMP)

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny**| **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*]| *icmp-message*] [**precedence** *precedence* | **dscp** *dscp* | **tos** *tos* | **time-range** *time-range-name* | **fragments** | **log** [*word*] | | **log-input** [*word*]]

Internet Group Management Protocol (IGMP)

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny**| **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence* | **dscp** *dscp* | **tos** *tos* | **time-range** *time-range-name* | **fragments** | **log** [*word*] | | **log-input** [*word*]]

Transmission Control Protocol (TCP)

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny**| **permit**} **tcp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] **[established]** [**precedence** *precedence* | **dscp** *dscp* | **tos** *tos* | **time-range** *time-range-name* | **fragments** | **log** [*word*] | | **log-input** [*word*]]

User Datagram Protocol (UDP)

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny**| **permit**} **udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence* | **dscp** *dscp* | **tos** *tos* | **time-range** *time-range-name* | **fragments** | **log** [*word*] | | **log-input** [*word*]]

Syntax Description

access-list-number	Number of an access list. This is a decimal number from 100 to 199 or from 2000 to 2699.
dynamic *dynamic-name*	(Optional) 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 IOS Security 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 IOS Security 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**, **pim**, **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 below.
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. Each wildcard bit 0 indicates the corresponding bit position in the source. Each wildcard bit set to 1 indicates that both a 0 bit and a 1 bit in the corresponding position of the IP address of the packet will be considered a match to this access list entry. 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. Wildcard bits set to 1 need not be contiguous in the source wildcard. For example, a source wildcard of 0.255.0. would be valid.
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 level, as specified by a number from 0 to 15, or by name as listed in the section "Usage Guidelines."
dscp	Enter to match packets with the DSCP value specified by a number from 0 to 63, or use the question mark (?) to see a list of available values.
time-range *time-range-name*	(Optional) Name of the time range that applies to this statement. The name of the time range and its restrictions are specified by the **time-range** command.
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 listed 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." TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP. 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 control bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
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 (IP extended), on page 51" and "access-list (IP extended), on page 51" sections in the "Usage Guidelines" section.
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 log 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 port numbers and the user-defined cookie or router-generated hash value. 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 may 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. After you specify the **log** keyword (and the associated *word* argument), you cannot specify any other keywords or settings for this command.

word	(Optional) User-defined cookie appended to the log message. The cookie: • cannot be more than characters • cannot start with hexadecimal notation (such as 0x) • cannot be the same as, or a subset of, the following keywords: **reflect**, **fragment**, **time-range** • must contain alphanumeric characters only The user-defined cookie is appended to the access control entry (ACE) syslog entry and uniquely identifies the ACE, within the access control list, that generated the syslog entry.
log-input	(Optional) Includes the input interface and source MAC address or virtual circuit in the logging output. After you specify the **log-input** keyword (and the associated *word* argument), you cannot specify any other keywords or settings for this command.

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

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.

Release	Modification
10.3	The following keywords and arguments were added: • *source* • *source-wildcard* • *destination* • *destination-wildcard* • **precedence** *precedence* • *icmp-type* • *icmp-code* • *icmp-message* • *igmp-type* • *operator* • *port* • **established**
11.1	The dynamic dynamic-name keyword and argument were added.
11.1	The timeout minutes keyword and argument were added.
11.2	The **log-input**keyword was added.
12.0(1)T	The **time-range** *time-range-name* keyword and argument were added.
12.0(11)	The **fragments**keyword was added.
12.2(13)T	The **non500-isakmp** keyword was added to the list of UDP port names. The igrp keyword was removed because the IGRP protocol is no longer available in Cisco IOS software.
12.4	The **drip** keyword was added to specify the TCP port number used for OER communication.
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.
12.4(22)T	The *word* argument was added to the **log** and **log-input** keywords.
15.1(2)SNG	This command was integrated into the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

You can use access lists to control the transmission of packets on an interface, control Virtual Terminal Line (VTY) access, and restrict the 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 type of service (ToS) value, or the precedence of the packet.

Note After a numbered 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 numbered 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**
- **drip**
- **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**
- **dnsix**
- **domain**
- **echo**
- **mobile-ip**
- **nameserver**
- **netbios-dgm**
- **netbios-ns**
- **non500-isakmp**
- **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,	The access-list entry is applied only to noninitial fragments. **Note** 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 addres**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.

Permitting Optimized Edge Routing (OER) Communication

The drip keyword was introduced under the **tcp** keyword to support packet filtering in a network where OER is configured. The drip keyword specifies port 3949 that OER uses for internal communication. This option allows you to build a packet filter that permits communication between an OER master controller and border router(s). The drip keyword is entered following the TCP source, destination, and the **eq** operator. See the example at the end of this command reference page.

Examples

In the following example, serial interface 0 is part of a Class B network with the address 10.88.0.0, and the address of the mail host is 10.88.1.2. Th e **established** keyword is used only for the TCP protocol to indicate an established connection. A match occurs if the TCP datagram has the ACK or RST bits set, which indicates that the packet belongs to an existing connection.

```
access-list 102 permit tcp 0.0.0.0 255.255.255.255 10.88.0.0 0.0.255.255 established
access-list 102 permit tcp 0.0.0.0 255.255.255.255 10.88.1.2 0.0.0.0 eq 25
interface serial 0
 ip access-group 102 in
```

The following example permits Domain Naming System (DNS) packets and ICMP echo and echo reply packets:

```
access-list 102 permit tcp any 10.88.0.0 0.0.255.255 established
access-list 102 permit tcp any host 10.88.1.2 eq smtp
access-list 102 permit tcp any any eq domain
access-list 102 permit udp any any eq domain
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

The following examples show how wildcard bits are used to indicate the bits of the prefix or mask that are relevant. Wildcard bits are similar to the bitmasks that are used with normal access lists. Prefix or mask bits corresponding to wildcard bits set to 1 are ignored during comparisons and prefix or mask bits corresponding to wildcard bits set to 0 are used in comparison.

The following example permits 192.168.0.0 255.255.0.0 but denies any more specific routes of 192.168.0.0 (including 192.168.0.0 255.255.255.0):

```
access-list 101 permit ip 192.168.0.0 0.0.0.0   255.255.0.0 0.0.0.0
access-list 101 deny ip 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255
```

The following example permits 10.108.0/24 but denies 10.108/16 and all other subnets of 10.108.0.0:

```
access-list 101 permit ip 10.108.0.0 0.0.0.0     255.255.255.0 0.0.0.0
access-list 101 deny ip 10.108.0.0 0.0.255.255 255.255.0.0   0.0.255.255
```

The following example uses a time range to deny HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m.:

```
time-range no-http
 periodic weekdays 8:00 to 18:00
!
access-list 101 deny tcp any any eq http time-range no-http
!
interface ethernet 0
 ip access-group 101 in
```

The following example permits communication, from any TCP source and destination, between an OER master controller and border router:

```
access-list 100 permit tcp any eq drip any eq drip
```

The following example shows how to configure the access list with the **log** keyword. It sets the *word* argument to UserDefinedValue. The word UserDefinedValue is appended to the related syslog entry:

```
Router(config)# access-list 101 permit tcp host 10.1.1.1 host 10.1.1.2 log UserDefinedValue
```

This example shows how to create an ACL that permits IP traffic from any source to any destination that has the DSCP value set to 32:

```
Router(config)# access-list 100 permit ip any any dscp 32
```

This example shows how to create an ACL that permits IP traffic from a source host at 10.1.1.1 to a destination host at 10.1.1.2 with a precedence value of 5:

```
Router(config)# access-list 100 permit ip host 10.1.1.1 host 10.1.1.2 precedence 5
```

Related Commands

Command	Description
access-class	Restricts incoming and outgoing connections between a particular VTY (into a Cisco device) and the addresses in an access list.
access-list (IP standard)	Defines a standard IP access list.
access-list remark	Writes a helpful comment (remark) for an entry in a numbered IP access list.
clear access-template	Clears a temporary access list entry from a dynamic access list.
delay (tracking)	Sets conditions under which a packet does not pass a named access list.
distribute-list in (IP)	Filters networks received in updates.

Command	Description
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.
ip access-list logging hash-generation	Enables hash value generation for ACE syslog entries.
ip accounting	Enables IP accounting on an interface.
logging console	Controls which messages are logged to the console, based on severity.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list.
permit (IP)	Sets conditions under which a packet passes a named access list.
remark	Writes a helpful comment (remark) for an entry in a named IP access list.
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.
time-range	Specifies when an access list or other feature is in effect.

access-list (IP standard)

To define a standard IP access list, use the s tandard version of the **access-list** command in global configuration mode. To remove a standard access list, use the **no** form of this command.

access-list *access-list-number* {**deny**| **permit**} *source* [*source-wildcard*] [**log** [*word*]]

no access-list *access-list-number*

Syntax Description

access-list-number	Number of an access list. This is a decimal number from 1 to 99 or from 1300 to 1999.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
source	Number of the network or host from which the packet is being sent. There are two 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.
source-wildcard	(Optional) Wildcard bits to be applied to the source. There are two 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.

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 log message includes the access list number, whether the packet was permitted or denied, the source address, the number of packets, and if appropriate, the user-defined cookie or router-generated hash value. 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.
word	(Optional) User-defined cookie appended to the log message. The cookie: • cannot be more than characters • cannot start with hexadecimal notation (such as 0x) • cannot be the same as, or a subset of, the following keywords: **reflect**, **fragment**, **time-range** • must contain alphanumeric characters only The user-defined cookie is appended to the access control entry (ACE) syslog entry and uniquely identifies the ACE, within the access control list, that generated the syslog entry.

Command Default The access list defaults to an implicit deny statement for everything. The access list is always terminated by an implicit deny statement for everything.

Command Modes Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
11.3(3)T	The **log** keyword was added.
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.
12.4(22)T	The *word* argument was added to the **log** keyword.

Usage Guidelines

Plan your access conditions carefully and be aware of the implicit deny statement at the end of the access list.

You can use access lists to control the transmission of packets on an interface, control vty access, and restrict the contents of routing updates.

Use the **show access-lists** EXEC command to display the contents of all access lists.

Use the **show ip access-list** EXEC command to display the contents of one access list.

Caution Enhancements to this command are backward compatible; migrating from releases prior to Cisco IOS Release 10.3 will convert your access lists automatically. However, releases prior to Release 10.3 are not upwardly compatible with these enhancements. Therefore, if you save an access list with these images and then use software prior to Release 10.3, the resulting access list will not be interpreted correctly. **This condition could cause you severe security problems**. Save your old configuration file before booting these images.

Examples

The following example of a standard access list allows access for only those hosts on the three specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the access list statements will be rejected.

```
access-list 1 permit 192.168.34.0 0.0.0.255
access-list 1 permit 10.88.0.0 0.0.255.255
access-list 1 permit 10.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)
```

The following example of a standard access list allows access for devices with IP addresses in the range from 10.29.2.64 to 10.29.2.127. All packets with a source address not in this range will be rejected.

```
access-list 1 permit 10.29.2.64 0.0.0.63
! (Note: all other access implicitly denied)
```

To specify a large number of individual addresses more easily, you can omit the wildcard if it is all zeros. Thus, the following two configuration commands are identical in effect:

```
access-list 2 permit 10.48.0.3
access-list 2 permit 10.48.0.3 0.0.0.0
```

The following example of a standard access list allows access for devices with IP addresses in the range from 10.29.2.64 to 10.29.2.127. All packets with a source address not in this range will be rejected.

```
access-list 1 permit 10.29.2.64 0.0.0.63
! (Note: all other access implicitly denied)
```

The following example of a standard access list allows access for devices with IP addresses in the range from 10.29.2.64 to 10.29.2.127. All packets with a source address not in this range will be rejected. In addition, the logging mechanism is enabled and the word SampleUserValue is appended to each syslog entry.

```
Router(config)# access-list 1 permit 10.29.2.64 0.0.0.63 log SampleUserValue
```

Related Commands

Command	Description
access-class	Restricts incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list.
access-list (IP extended)	Defines an extended IP access list.
access-list remark	Writes a helpful comment (remark) for an entry in a numbered IP access list.
deny (IP)	Sets conditions under which a packet does not pass a named access list.
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 logging hash-generation	Enables hash value generation for ACE syslog entries.
permit (IP)	Sets conditions under which a packet passes a named access list.
remark (IP)	Writes a helpful comment (remark) for an entry in a named IP access list.
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.

access-list (NLSP)

To define an access list that denies or permits area addresses that summarize routes, use the NetWare Link-Services Protocol (NLSP) route aggregation version of the **access-list** command in global configuration mode. To remove an NLSP route aggregation access list, use the **no**form of this command.

access-list *access-list-number* {**deny**| **permit**} *network network-mask* [*interface*] [**ticks** *ticks*] [**area-count** *area-count*]

no access-list *access-list-number* {**deny**| **permit**} *network network-mask* [*interface*] [**ticks** *ticks*] [**area-count** *area-count*]

Syntax Description

access-list-number	Number of the access list. This is a number from 1200 to 1299.
deny	Denies redistribution of explicit routes if the conditions are matched. If you have enabled route summarization with route-aggregation command, the router redistributes an aggregated route instead.
permit	Permits redistribution of explicit routes if the conditions are matched.
network	Network number to summarize. An IPX network number is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
network-mask	Specifies the portion of the network address that is common to all addresses in the route summary. The high-order bits of *network-mask* must be contiguous Fs, while the low-order bits must be contiguous zeros (0). An arbitrary mix of Fs and 0s is not permitted.
interface	(Optional) Interface on which the access list should be applied to incoming updates.
ticks *ticks*	(Optional) Metric assigned to the route summary. The default is 1 tick.
area-count *area-count*	(Optional) Maximum number of NLSP areas to which the route summary can be redistributed. The default is 6 areas.

Command Default No access lists are predefined.

Command Modes Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.0	The *interface* argument was added.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in12.2S-Family releases.
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 Use the NLSP route aggregation access list in the following situations:

- When redistributing from an Enhanced IGRP or RIP area into a new NLSP area.

Use the access list to instruct the router to redistribute an aggregated route instead of the explicit route. The access list also contains a "permit all" statement that instructs the router to redistribute explicit routes that are not subsumed by a route summary.

- When redistributing from an NLSP version 1.0 area into an NLSP version 1.1 area, and vice versa.

From an NLSP version 1.0 area into an NLSP version 1.1 area, use the access list to instruct the router to redistribute an aggregated route instead of an explicit route and to redistribute explicit routes that are not subsumed by a route summary.

From an NLSP version 1.1 area into an NLSP version 1.0 area, use the access list to instruct the router to filter aggregated routes from passing into the NLSP version 1.0 areas and to redistribute explicit routes instead.

Note NLSP version 1.1 routers refer to routers that support the route aggregation feature, while NLSP version 1.0 routers refer to routers that do not.

Examples

The following example uses NLSP route aggregation access lists to redistribute routes learned from RIP to NLSP area1. Routes learned via RIP are redistributed into NLSP area1. Any routes learned via RIP that are subsumed by aaaa0000 ffff0000 are not redistributed. An address summary is generated instead.

```
ipx routing
ipx internal-network 2000
interface ethernet 1
 ipx network 1001
 ipx nlsp area1 enable
interface ethernet 2
 ipx network 2001
access-list 1200 deny aaaa0000 ffff0000
access-list 1200 permit -1
ipx router nlsp area
 area-address 1000 fffff000
 route-aggregation
 redistribute rip access-list 1200
```

Related Commands

Command	Description
area-address (NLSP)	Defines a set of network numbers to be part of the current NLSP area.
deny (NLSP)	Filters explicit routes and generates an aggregated route for a named NLSP route aggregation access list.
ipx access-list	Defines an IPX access list by name.
ipx nlsp enable	Configures the interval between the transmission of hello packets.
ipx router	Specifies the routing protocol to use.
permit (NLSP)	Allows explicit route redistribution in a named NLSP route aggregation access list.
prc-interval	Controls the hold-down period between partial route calculations.
redistribute (IPX)	Redistributes from one routing domain into another.

access-list compiled

To enable the Turbo Access Control Lists (Turbo ACL) feature, use the **a ccess-list compiled**commandinglobal configuration mode. To disable the Turbo ACL feature, use the **no**form of this command.

access-list compiled

no access-list compiled

Syntax Description

This command has no arguments or keywords.

Command Default

Turbo ACL is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.1(1)E	This command was introduced for Cisco 7200 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(4)E	This command was implemented on the Cisco 7100 series.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
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

By default, the Turbo ACL feature is disabled. When Turbo ACL is disabled, normal ACL processing is enabled, and no ACL acceleration occurs.

When the Turbo ACL feature is enabled using the access-list compiled command, the ACLs in the configuration are scanned and, if suitable, compiled for Turbo ACL acceleration. This scanning and compilation may take a few seconds when the system is processing large and complex ACLs, or when the system is processing a configuration that contains a large number of ACLs.

Any configuration change to an ACL that is being accelerated, such as the addition of new ACL entries or the deletion of the ACL, triggers a recompilation of that ACL.

When Turbo ACL tables are being built (or rebuilt) for a particular ACL, the normal sequential ACL search is used until the new tables are ready for installation.

Examples The following example enables the Turbo ACL feature:

```
access-list compiled
```

access-listcompileddata-linklimitmemory

To change the amount of memory reserved for Turbo ACL processing for Layer 2 traffic in the Route Processor path for a Cisco 7304 router using a network services engine (NSE), use the **access-list compiled data-link limit memory** command in global configuration mode. To place no restrictions on the amount of memory reserved for Turbo ACL processing of Layer 2 traffic in the Route Processor path for a Cisco 7304 router using an NSE, use the **no** form of this command. To restore the default amount of memory reserved for Turbo ACL processing for Layer 2 traffic in the Route Processor path for a Cisco 7304 router using an NSE, use the **default** form of this command.

access-list compiled data-link limit memory *number*

no access-list compiled data-link limit memory

default access-list compiled data-link limit memory

Syntax Description

number	A number between 8 and 4095 that specifies the amount of memory, in megabytes, reserved for Turbo ACL processing of Layer 2 traffic in the Route Processor path for the Cisco 7304 router using an NSE.

Command Default

The default for *number* is 128.

Command Modes

Global configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

The **show access-list compiled** command output provides information useful in helping to consider the exact memory limit to configure. The following sections of the **show access-list compiled**output, which are found in the “Compiled ACL statistics for Data-Link” section of the output, are especially useful:

- The “mem limits” output shows the number of times a compile has occurred and the ACL has reached its configured limit.
- The “Mb limit” output shows the current memory limit setting.
- The “Mb max memory” output shows the maximum amount of memory the current ACL configuration could actually consume under maximum usage conditions.

Note that there is a direct trade-off between memory used for ACL processing in the RP path and the memory used for other RP processes. Memory reserved for ACL processing cannot be used for other RP processes, and vice versa. If you need more memory for ACL processing, you should set a higher value for *number*. If you need more memory for other RP processes, you should set a lower value for *number*.

When configuring this memory limit, also note that a certain amount of RP memory is reserved for Layer 3 and Layer 4 ACL data. The amount of memory reserved for ACL data can be viewed using the **show access-list compiled** command, and can be changed using the **access-list compiled ipv4 limit memory** command.

Note that the **no** form of this command removes all memory limits for ACL processing, thereby allowing as much memory as is needed for Layer 2 ACL processing in the RP path.

To restore a default configuration of this command, which is 128 MB, enter the **default** form of this command.

Examples

The following example reserves 100 MB of memory for Layer 2 ACL processing in the RP path:

```
access-list compiled data-link limit memory 100
```

The following example allows Layer 2 ACL processing to use as much memory as is needed for Layer 2 ACL processing:

```
no access-list compiled data-link limit memory
```

The following example restores the default amount of memory reserved for Layer 2 ACL processing in the RP path:

```
default access-list compiled data-link limit memory
```

Related Commands

Command	Description
access-list compiled ipv4 limit memory	Configures limits on the amount of memory used for Turbo ACL processing of Layer 3 and Layer 4 traffic.
show access-list compiled	Displays the status and condition of the Turbo ACL tables associated with each access list.

access-listcompiledipv4limitmemory

To change the amount of memory reserved for Turbo ACL processing for Layer 3 and Layer 4 traffic in the Route Processor path for a Cisco 7304 router using a network services engine (NSE), use the **access-list compiled ipv4 limit memory** command in global configuration mode. To place no restrictions on the amount of memory reserved for Turbo ACL processing for Layer 3 and Layer 4 traffic in the Route Processor path for a Cisco 7304 router using an NSE, use the **no** form of this command. To restore the default amount of memory reserved for Turbo ACL processing for Layer 3 and Layer 4 traffic in the Route Processor path for a Cisco 7304 router using an NSE, use the **default** form of this command.

access-list compiled ipv4 limit memory *number*

no access-list compiled ipv4 limit memory

default access-list compiled ipv4 limit memory

Syntax Description

number	A number between 8 and 4095 that specifies the memory limit in megabytes.

Command Default

On an NSE-150, the default for *number* is always 256.

On an NSE-100, the default for *number* is determined by the amount of SDRAM on the NSE-100. If the NSE-100 has 512 MB of DRAM, the default for *number* is 256. If the NSE-100 has less than 512 MB DRAM, the default for *number* is 128.

Command Modes

Global configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

The **show access-list compiled** command output provides information useful in helping to consider the exact memory limit to configure. The following sections of the **show access-list compiled**output, which are found in the “Compiled ACL statistics for IPv4:” section of the output, are especially useful:

- The “mem limits” output shows the number of times a compile has occurred and the ACL has reached its configured limit.
- The “Mb limit” output shows the current memory limit setting.
- The “Mb max memory” output shows the maximum amount of memory the current ACL configuration could actually consume under maximum usage conditions.

Note that there is a direct trade-off between memory used for ACL processing in the RP path and the memory used for other RP processes. Memory reserved for ACL processing cannot be used for other RP processes, and vice versa. If you need more memory for ACL processing, you should set a higher value for *number*. If you need more memory for other RP processes, you should set a lower value for *number*.

When configuring this memory limit, also note that a certain amount of RP memory is reserved for Layer 2 ACL data. The amount of memory reserved for ACL data can be viewed using the **show access-list compiled** command, and can be changed using the **access-list compiled data-link limit memory** command.

Note that the **no** form of this command removes all memory limits for ACL processing, thereby allowing as much memory as is needed for Layer 3 and Layer 4 ACL processing in the RP path.

To restore a default configuration of this command, enter the **default** form of this command.

Examples

The following example reserves 100 MB of memory for Layer 3 and Layer 4 ACL processing in the RP path:

```
access-list compiled ipv4 limit memory 100
```

The following example allows Layer 3 and Layer 4 ACL processing to use as much memory as is needed for Layer 3 and Layer 4 ACL processing:

```
no access-list compiled ipv4 limit memory
```

The following example restores the default amount of memory reserved for Layer 3 and Layer 4 ACL processing in the RP path:

default access-list compiled ipv4 limit memory

Related Commands

Command	Description
access-list compiled data-link limit memory	Configures memory limits on the amount of memory reserved for Turbo ACL processing of Layer 2 traffic.
show access-list compiled	Displays the status and condition of the Turbo ACL tables associated with each access list

access-list dynamic-extend

To allow the absolute timer of the dynamic acce ss control list (ACL) to be extended an additional six minutes, use the **access-list dynamic-extend** command in global configuration mode. To disable this functionality, use the **no** form of this command.

access-list dynamic-extend

no access-list dynamic-extend

Syntax Description

This command has no arguments or keywords.

Command Default

6 minutes

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)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 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 you try to create a Telnet session to the router to re-authenticate yourself by using the lock-and-key function, use the **access-list dynamic-extend** command to extend the absolute timer of the dynamic ACL by six minutes.

The router must already be configured with the lock-and-key feature, and you must configure the extension before the ACL expires.

Examples

The following example shows how to extend the absolute timer of the dynamic ACL:

```
! The router is configured with the lock-and-key feature as follows
access-list 132 dynamic tactik timeout 6 permit ip any any
! The absolute timer will extended another six minutes.
access-list dynamic-extend
```

access-list remark

To write a helpful comment (remark) for an entry in a numbered IP access list, use the **access-list remark** command in global configuration mode.To remove the remark, use the **no** form of this command.

access-list *access-list-number* **remark** [*line*]

no access-list *access-list-number* **remark** [*line*]

Syntax Description

access-list-number	Number of an IP access list.
line	(Optional) Comment that describes the access list entry, up to 100 characters long.

Command Default

The access list entries have no remarks.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(2)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 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

The remark can be up to 100 characters long; anything longer is truncated.

Examples

The following example shows how to write comments for workstation abc, which is allowed access, and workstation xyz, which is not allowed access:

```
access-list 1 remark Permit only abc workstation comment
access-list 1 permit 192.0.2.0
access-list 1 remark Do not allow xyz workstation comment
access-list 1 deny 192.0.2.13
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.

Command	Description
access-list (IP standard)	Defines a standard IP access list.
ip access-list	Defines an IP access list by name.
remark	Writes a helpful comment (remark) for an entry in a named IP access list.

access-profile

To apply your per-user authorization attributes to an interface during a PPP session, use the **access-profile** command in privileged EXEC mode.

access-profile [**merge**| **replace**] **[ignore-sanity-checks]**

Syntax Description

merge	(Optional) Removes existing access control lists (ACLs) while retaining other existing authorization attributes for the interface. • However, using this option installs per-user authorization attributes in addition to the existing attributes. (The default form of the command installs only new ACLs.) The per-user authorization attributes come from all attribute-value (AV) pairs defined in the authentication, authorization, and accounting (AAA) per-user configuration (the user's authorization profile).
replace	(Optional) Removes existing ACLs and all other existing authorization attributes for the interface. • A complete new authorization configuration is then installed, using all AV pairs defined in the AAA per-user configuration. • This option is not normally recommended because it initially deletes all existing configurations, including static routes. This could be detrimental if the new user profile does not reinstall appropriate static routes and other critical information.
ignore-sanity-checks	(Optional) Enables you to use any AV pairs, whether or not they are valid.

Command Default

By default this command removes existing ACLs while retaining other existing authorization attributes for the interface.

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.
12.2(33)SRB	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

Remote users can use the **access-profile** command to activate double authentication for a PPP session. Double authentication must be correctly configured for this command to have the desired effect.

You should use this command when remote users establish a PPP link to gain local network access.

The resulting authorization attributes of the interface are a combination of the previous and new configurations.

After you have been authenticated with Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP), you will have limited authorization. To activate double authentication and gain your appropriate user network authorization, you must open a Telnet session to the network access server and execute the **access-profile** command. (This command could also be set up as an autocommand, which would eliminate the need to enter the command manually.)

This command causes all subsequent network authorizations to be made in your username instead of in the remote host's username.

Any changes to the interface caused by this command will stay in effect for as long as the interface stays up. These changes will be removed when the interface goes down. This command does not affect the normal operation of the router or the interface.

The default form of the command, **access-profile**, causes existing ACLs to be unconfigured (removed), and new ACLs to be installed. The new ACLs come from your per-user configuration on an AAA server (such as a TACACS+ server). The ACL replacement constitutes a reauthorization of your network privileges.

The default form of the command can fail if your per-user configuration contains statements other than ACL AV pairs. Any protocols with non-ACL statements will be deconfigured, and no traffic for that protocol can pass over the PPP link.

The **access-profile merge** form of the command causes existing ACLs to be unconfigured and new authorization information (including new ACLs) to be added to the interface. This new authorization information consists of your complete per-user configuration on an AAA server. If any of the new authorization statements conflict with existing statements, the new statements could override the old statements or be ignored, depending on the statement and applicable parser rules. The resulting interface configuration is a combination of the original configuration and the newly installed per-user configuration.

Caution The new user authorization profile (per-user configuration) must *not* contain any invalid mandatory AV pairs, because the command will fail and PPP (containing the invalid pair) will be dropped. If invalid AV pairs are included as *optional* in the user profile, the command will succeed, but the invalid AV pair will be ignored. Invalid AV pair types are listed later in this section.

The **access-profile replace** form of the command causes the entire existing authorization configuration to be removed from the interface, and the complete per-user authorization configuration to be added. This per-user authorization consists of your complete per-user configuration on an AAA server.

Caution Use extreme caution when using the **access-profile replac**e form of the command. It might have detrimental and unexpected results, because this option deletes all authorization configuration information (including static routes) before reinstalling the new authorization configuration.

The following are invalid AV pair types:

- addr
- addr-pool
- frame-relay
- ip-addresses
- source-ip
- tunnel-id
- x25-addresses
- zonelist

Note These AV pair types are invalid only when used with double authentication in the user-specific authorization profile; they cause the **access-profile**command to fail. However, these AV pair types can be appropriate when used in other contexts.

Examples

The following example shows how to apply the per-user authorization attributes to an interface during a PPP session:

```
Router# access-profile merge ignore-sanity-checks
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
telnet	Logs in to a host that supports Telnet.

access-restrict

To tie a particular Virtual Private Network (VPN) to a specific interface for access to the Cisco IOS gateway and the services it protects, use the **access-restrict** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove the VPN, use the **no** form of this command.

access-restrict interface-name

no access-restrict interface-name

Syntax Description

interface-name	Interface to which the VPN should be tied.

Command Default

The VPN is not tied to a specific interface.

Command Modes

ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.2(13)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

The Access-Restrict attribute ties a particular VPN group to a specific interface for access to the Cisco IOS gateway and the services it provides.

It may be a requirement that particular customers or groups connect to the VPN gateway via a specific interface that uses a particular policy (as applied by the crypto map on that interface). If this specific interface is required, using the **access-restrict** command will result in validation that a VPN connection is connecting only via that interface (and hence, crypto map) to which it is allowed. If a violation is detected, the connection is terminated.

Multiple restricted interfaces may be defined per group. The Access-Restrict attribute is configured on a Cisco IOS router or in the RADIUS profile. This attribute has local (gateway) significance only and is not passed to the client.

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

Note The Access-Restrict attribute can be applied only by a RADIUS user.

- The attribute can be applied on a per-user basis after the user has been authenticated.
- The attribute can override any similar group attributes.
- User-based attributes are available only if RADIUS is used as the database.The attribute can override any similar group attributes.
- The Access-Restrict attribute is not required if ISAKMP profiles are implemented. ISAKMP profiles with specific policies per VPN group (as defined via the **match identity group** command, which is a subcommand of the **crypto isakmp profile** command), will achieve the same result.

An example of an attribute-value (AV) pair for the Access-Restrict attribute is as follows:

```
ipsec:access-restrict=<interface-name>
```

Examples

The following example shows that the VPN is tied to “ethernet 0”:

```
crypto isakmp client configuration group cisco
 access-restrict ethernet 0
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

access-template

To manually place a temporary access list entry on a router to which you are connected, use the **access-template** command in privileged EXEC mode.

access-template {*access-list-number*| *name*} *template-name* {*source-address source-wildcard-bit*| **any**| **host** {*hostname*| *source-address*}} {*destination-address dest-wildcard-bit*| **any**| **host** {*hostname*| *destination-address*}} [**timeout** *minutes*]

Syntax Description

access-list-number	Number of the dynamic access list. The ranges are from 100 to 199 and from 2000 to 2699.
name	Name of an IP access list. • The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.
template-name	Name of a dynamic access list.
source-address	Source address in a dynamic access list. • All other attributes are inherited from the original access-list entry.
source-wildcard-bit	Source wildcard bits.
any	Specifies any source hostname.
host	Specifies a specific source host.
hostname	Name of the host.
destination-address	Destination address in a dynamic access list. • All other attributes are inherited from the original access-list entry.
dest-wildcard-bit	Destination wildcard bits.

timeout *minutes*	(Optional) Specifies a maximum time limit, in minutes for each entry within this dynamic list. The range is from 1 to 9999. • This is an absolute time, from creation, that an entry can reside in the list. The default is an infinite time limit and allows an entry to remain permanently.

Command Default

Temporary access lists are not placed on the router.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1	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 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 the **access-template** to enable the lock-and-key access feature.

You must always define either an idle timeout (with the **timeout** keyword in this command) or an absolute timeout (with the **timeout** keyword in the **access-list** command). Otherwise, the dynamic access list will remain, even after the user has terminated the session.

Examples

The following example shows how to enable IP access on incoming packets in which the source address is 172.29.1.129 and the destination address is 192.168.52.12. All other source and destination pairs are discarded.

```
Router> enable
Router# access-template 101 payroll host 172.29.1.129 host 192.168.52.12 timeout 2
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
autocommand	Configures the Cisco IOS software to automatically execute a command when a user connects to a particular line.

Command	Description
clear access-template	Clears a temporary access list entry from a dynamic access list manually.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

accounting

To enable authentication, authorization, and accounting (AAA) accounting services to a specific line or group of lines, use the **accounting** command in line configuration mode. To disable AAA accounting services, use the **no** form of this command.

accounting {**arap**| **commands** *level*| **connection**| **exec**} [**default**| *list-name*]

no accounting {**arap**| **commands** *level*| **connection**| **exec**} [**default**| *list-name*]

Syntax Description

arap	Enables accounting on lines configured for AppleTalk Remote Access Protocol (ARAP).
commands *level*	Enables accounting on the selected lines for all commands at the specified privilege level. Valid privilege level entries are 0 through 15.
connection	Enables both CHAP and PAP, and performs PAP authentication before CHAP.
exec	Enables accounting for all system-level events not associated with users, such as reloads on the selected lines.
default	(Optional) The name of the default method list, created with the **aaa accounting**command.
list-name	(Optional) Specifies the name of a list of accounting methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa accounting** command.

Command Default

Accounting is disabled.

Command Modes

Line configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
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

After you enable the **aaa accounting** command and define a named accounting method list (or use the default method list) for a particular type of accounting, you must apply the defined lists to the appropriate lines for accounting services to take place. Use the **accounting** command to apply the specified method lists (or if none is specified, the default method list) to the selected line or group of lines.

Examples

The following example enables command accounting services (for level 15) using the accounting method list named charlie on line 10:

```
line 10
 accounting commands 15 charlie
```

accounting (gatekeeper)

To enable and define the gatekeeper-specific accounting method, use the **accounting** command in gatekeeper configuration mode. To disable gatekeeper-specific accounting, use the **no**form of this command.

accounting {**username h323id| vsa**}

no accounting

Syntax Description

username h323id	Enables H323ID in the user name field of accounting record.
vsa	Enables the vendor specific attribute accounting format.

Command Default

Accounting is disabled.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.1(5)XM	The **vsa** keyword was added.
12.2(2)T	The **vsa** keyword was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850 universal gateway.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.3(9)T	This **username h323id**keyword was added.
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

To collect basic start-stop connection accounting data, the gatekeeper must be configured to support gatekeeper-specific H.323 accounting functionality. The **accounting** command enables you to send accounting data to the RADIUS server via IETF RADIUS or VSA attriibutes.

Specify a RADIUS server before using the **accounting** command.

There are three different methods of accounting. The H.323 method sends the call detail record (CDR) to the RADIUS server, the syslog method uses the system logging facility to record the CDRs, and the VSA method collects VSAs.

Examples

The following example enables the gateway to report user activity to the RADIUS server in the form of connection accounting records:

```
aaa accounting connection start-stop group radius
gatekeeper
 accounting
```

The following example shows how to enable VSA accounting:

```
aaa accounting connection start-stop group radius
gatekeeper
 accounting exec vsa
```

The following example configures H.323 accounting using IETF RADIUS attributes:

```
Router(config-gk)# accounting
username
 h323id
```

The following example configures H.323 accounting using VSA RADIUS attributes:

Router(config-gk)# **accounting vsa**

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
gatekeeper	Enters gatekeeper configuration mode.

accounting (line)

To enable authentication, authorization, and accounting (AAA) accounting services to a specific line or group of lines, use the **accounting** command in line configuration mode. To disable AAA accounting services, use the **no** form of this command.

accounting {**arap**| **commands** *level*| **connection**| **exec**} [**default**| *list-name*]

no accounting {**arap**| **commands** *level*| **connection**| **exec**} [**default**| *list-name*]

Syntax Description

arap	Enables accounting on lines configured for AppleTalk Remote Access Protocol (ARAP).
commands *level*	Enables accounting on the selected lines for all commands at the specified privilege level. Valid privilege level entries are 0 through 15.
connection	Enables both CHAP and PAP, and performs PAP authentication before CHAP.
exec	Enables accounting for all system-level events not associated with users, such as reloads on the selected lines.
default	(Optional) The name of the default method list, created with the **aaa accounting**command.
list-name	(Optional) Specifies the name of a list of accounting methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa accounting** command.

Command Default

Accounting is disabled.

Command Modes

Line configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
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

After you enable the **aaa accounting** command and define a named accounting method list (or use the default method list) for a particular type of accounting, you must apply the defined lists to the appropriate lines for accounting services to take place. Use the **accounting** command to apply the specified method lists (or if none is specified, the default method list) to the selected line or group of lines.

Examples

The following example enables command accounting services (for level 15) using the accounting method list named charlie on line 10:

```
line 10
 accounting commands 15 charlie
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.

accounting (server-group)

To specify RADIUS accounting filters for attributes that are to be sent to the RADIUS server in accounting requests, use the **accounting** command in server-group configuration mode. To disable specific RADIUS accounting filters for attributes that are to be sent to the RADIUS server, use the **no** form of this command.

accounting {**accept** *list-name*| **reject** *list-name*| **acknowledge broadcast**| **reply** {**accept** *list-name*| **reject** *list-name*}| **request** {**accept** *list-name*| **reject** *list-name*}| **system host-config**}

no accounting {**accept** *list-name*| **reject** *list-name*| **acknowledge broadcast**| **reply** {**accept** *list-name*| **reject** *list-name*}| **request** {**accept** *list-name*| **reject** *list-name*}| **system host-config**}

Syntax Description

accept	All attributes are rejected except for required attributes and the attributes specified by the list-name argument.
reject	All attributes are accepted except for the attributes listed in the specified list-name argument .
list-name	The name of a specific configured RADIUS attribute list.
acknowledge	Sends the specified accounting response.
broadcast	Specifies broadcast accounting.
reply	Reply attributes are accepted or rejected as specified by the *list-name* argument.
request	Request attributes are accepted or rejected as specified by the *list-name* argument.
system	Enables system accounting generation.
host-config	Generates system accounting records when private servers are added or deleted.

Command Default

If specific attributes are not accepted or rejected, all attributes will be accepted.

Command Modes

Server-group configuration (config-sg-radius)#

Command History

Release	Modification
12.2(1)DX	This command was introduced.

Release	Modification
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401ASR.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
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.
12.4(20)T	The following new keywords were added: **system and host-config**

Usage Guidelines

An accept or reject list (also known as a filter) for RADIUS accounting allows users to send only the accounting attributes their business requires, thereby reducing unnecessary traffic and allowing users to customize their own accounting data.

Only one filter may be used for RADIUS accounting per server group.

Note The listname must be the same as the listname defined in the **radius-server attribute list**command, which is used with the **attribute**(server-group configuration) command to add to an accept or reject list.

Examples

The following example shows how to specify accept list “usage-only” for RADIUS accounting:

```
Router> enable
Router# configure terminal
Router(config
)# aaa new-model
Router(config
)# aaa authentication ppp default group radius-sg
Router(config
)# aaa authorization network default group radius-sg
Router(config
)# aaa group server radius radius-sg
Router(config-sg-radius)# server 10.1.1.1
Router(config-sg-radius)# accounting accept usage-only
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list usage-only
 attribute 1,40,42-43,46
```

The following examples show how Accounting-On records or Accounting-Off records are generated when the **system host-config** keywords are configured using the **accounting** command in server-group configuration mode:

Examples

In this example, Accounting-On records are generated when private server (server-private 10.10.1.1) is added to a server-group.

```
Router> enable
Router# configure terminal
Router(config
)# aaa new-model
Router(config
)# aaa group server radius g2
Router#(config-sg-radius)# accounting system host-config
Router#(config-sg-radius)# server-private 10.10.1.1
 --> Debugs when adding a private server.
*May  6 05:23:25.530: RADIUS/ENCODE(00000011):Orig. component type = AAA
*May  6 05:23:25.530: RADIUS(00000011): Config NAS IP: 0.0.0.0
*May  6 05:23:25.530: RADIUS(00000011): sending
*May  6 05:23:25.530: RADIUS/ENCODE: Best Local IP-Address 10.10.55.9 for Radius-Server
10.64.67.15
*May  6 05:23:25.530: RADIUS(00000011): Send Accounting-Request to 10.10.67.15:1646 id
1646/1, len 48
*May  6 05:23:25.530: RADIUS:  authenticator 9A 10 D2 10 10 10 10 9D - 75 EE D4 AF 5D CC
8F 6A
*May  6 05:23:25.530: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
*May  6 05:23:25.530: RADIUS:  Acct-Status-Type    [40]  6   Accounting-On             [7]
*May  6 05:23:25.530: RADIUS:  NAS-IP-Address      [4]   6   10.10.55.9
*May  6 05:23:25.530: RADIUS:  Acct-Delay-Time     [41]  6   0
*May  6 05:23:25.550: RADIUS: Received from id 1646/10 10.10.67.15:1646, Accounting-response,
 len 20
*May  6 05:23:25.550: RADIUS: authenticator 10 A1 10 10 1A 3F E5 C9 - D1 D1 D6 92 4D 0A F9
 04
```

Examples

In this example, Accounting-Off records are generated when private server (server-private 10.10.10.10) is deleted from a server-group.

```
Router> enable
Router# configure terminal
Router(config
)# aaa new-model
Router(config
)# aaa group server radius g2
Router#(config-sg-radius)# accounting system host-config
Router#(config-sg-radius)# no
 server-private 10.10.10.10
 --> Debugs when a private server is deleted.
*May  6 05:23:34.162: RADIUS/ENCODE(00000011):Orig. component type = AAA
*May  6 05:23:34.162: RADIUS(00000011): Config NAS IP: 0.0.0.0
*May  6 05:23:34.162: RADIUS(00000011): sending
*May  6 05:23:34.166: RADIUS/ENCODE: Best Local IP-Address 10.10.55.9 for Radius-Server
10.64.67.15
*May  6 05:23:34.166: RADIUS(00000011): Send Accounting-Request to 10.10.67.15:1646 id
1646/2, len 48
*May  6 05:23:34.166: RADIUS:  authenticator 0A 1E D6 A9 4C 5A 4B 5B - 2A F4 E1 28 3A CF
87 03
*May  6 05:23:34.166: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
*May  6 05:23:34.166: RADIUS:  Acct-Status-Type    [40]  6   Accounting-Off            [8]
*May  6 05:23:34.166: RADIUS:  NAS-IP-Address      [4]   6   10.10.55.9
*May  6 05:23:34.166: RADIUS:  Acct-Delay-Time     [41]  6   0
*May  6 05:23:34.166: RADIUS: Received from id 1646/10 10.10.67.15:1646, Accounting-response,
 len 20
*May  6 05:23:34.166: RADIUS:  authenticator 79 ED 10 55 84 5A 08 8D - 74 03 CE 05 12 A5
DE 75
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict network access to the user.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
attribute (server-group configuration)	Adds attributes to an accept or reject list.
authorization (server-group configuration)	Specifies an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server.
radius-server attribute list	Defines an accept or reject list name.

accounting acknowledge broadcast

To define a designated broadcast accounting server group, use the **accounting acknowledge broadcast**command in server group RADIUS configuration mode. To disable the broadcast functionality, use the no form of this command.

accounting acknowledge broadcast

no accounting acknowledge broadcast

Syntax Description

This command has no arguments or keywords.

Command Default

Accounting broadcast functionality is disabled for the RADIUS server group.

Command Modes

Server group RADIUS configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example enables accounting broadcast functionality on RADIUS server group abcgroup:

```
Router(config)# aaa group server radius abcgroup
Router(config-sg-radius)# accounting acknowledge broadcast
```

Related Commands

Command	Description
aaa accounting update	Enables periodic interim accounting records to be sent to the accounting server.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
gw-accounting aaa	Enables VoIP gateway accounting through the AAA system.

accounting dhcp source-ip aaa list

To enable Per IP Subscriber DHCP Triggered RADIUS Accounting for billing or security purposes, use the **accounting dhcp source-ip aaa list** command in access interface configuration mode. To disable Per IP Subscriber DHCP Triggered RADIUS Accounting, use the **no** form of this command.

accounting dhcp source-ip aaa list *method-list-name*

no accounting

Syntax Description

method-list-name	Character string used to name at least one of the accounting methods, tried in a given sequence. Valid values are **default** or a named method list as defined by the **aaa accounting**command.

Command Default

This command is disabled by default. If the **accounting dhcp source-ip aaa list**command for RADIUS accounting is issued without a named method list specified, the default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list. If no default method list is defined, then no accounting takes place.

Command Modes

Access interface

Command History

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

Usage Guidelines

Enter the **accounting dhcp source-ip aaa list** *command to enable accounting.*Use the **aaa accounting** command to create a named method list.

Examples

The following example shows how to define a command accounting method list named “default”.

```
accounting dhcp source-ip aaa list default
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.

Command	Description
ip dhcp limit lease per interface	Limits the number of leases offered to DHCP clients behind an ATM RBE unnumbered or serial unnumbered interface.

acl (ISAKMP)

To configure split tunneling, use the **acl** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove this command from your configuration and restore the default value, use the **no** form of this command.

acl *number*

no acl *number*

Syntax Description

number	Specifies a group of access control lists (ACLs) that represent protected subnets for split tunneling purposes.

Command Default

Split tunneling is not enabled; all data is sent via the Virtual Private Network (VPN) tunnel.

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 **acl** command to specify which groups of ACLs represent protected subnets for split tunneling. Split tunneling is the ability to have a secure tunnel to the central site and simultaneous clear text tunnels to the Internet.

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

Examples

The following example shows how to correctly apply split tunneling for the group name “cisco.” In this example, all traffic sourced from the client and destined to the subnet 192.168.1.0 will be sent via the VPN tunnel.

```
crypto isakmp client configuration group cisco
  key cisco
  dns 10.2.2.2 10.3.2.3
```

```
  pool dog
  acl 199
!
access-list 199 permit ip 192.168.1.0 0.0.0.255 any
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies the policy profile of the group that will be defined.

acl (WebVPN)

To define an access control list (ACL) using a Secure Socket Layer Virtual Private Network (SSL VPN) gateway at the Application Layer level and to associate an ACL with a policy group, use the **acl** command in webvpn context configuration and webvpn group policy configuration modes. To remove the ACL definition, use the **no** form of this command.

acl *acl-name*

no acl *acl-name*

Syntax Description

acl-name	Name of the ACL.

Command Default

If a user session has no ACL attributes configured, all application requests are permitted.

Command Modes

Web context configuration Webvpn group policy configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The ACL can be defined for an individual user or for a policy group.

A defined ACL can be overridden by an individual user when the user logs on to the gateway (using AAA policy attributes).

Examples

The following example shows that “acl1” has been defined as the ACL and that it has been associated with policy group “default.”

```
webvpn context context1
 acl acl1
  permit url "http://www.example.com"
 policy group default
  acl acl1
```

Related Commands

Command	Description
policy group	Configures a policy group and enters group policy configuration mode.

Command	Description
webvpn context	Configures the SSL VPN context and enters webvpn context configuration mode.

acl drop

To configure an access control list (ACL) drop enforcement action in a Transitory Messaging Services (TMS) Rules Engine configuration, use the **acl drop** command in policy-map class configuration mode. To remove the enforcement action from the Rules Engine configuration, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.4(20)T, the **acl drop** command is not available in Cisco IOS software.

acl drop

no acl drop

Syntax Description

This command has no keywords or arguments.

Command Default

None.

Command Modes

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

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **acl drop** command is entered in a mitigation type policy map. This command configures the TMS Rules Engine to drop packets that match a predefined extended access list. The **ip access-group** command is configured to attach the access list to the interface. The **tms-class** command is configured to associate the interface with the ACL drop enforcement action.

A mitigation service policy (TMS Rules Engine configuration) is configured on a consumer to customize or override a Threat Information Message (TIM) enforcement action sent by the controller. The TMS Rules Engine can be configured to perform an ACL drop, an ignore, or a redirect enforcement action. Only one action can configured for each mitigation type class of traffic.

Examples

The following example configures an ACL drop enforcement action. Traffic that matches the extended access list (172.16.1/24) is dropped.

```
Router(config)# ip access-list extended 100
Router(config-ipacl)# permit ip 172.16.1.0 0.0.0.255 any
```

```
Router(config-ipacl)# exit

Router(config)# interface Ethernet 0/0

Router(config-if)# ip access-group 100 in
Router(config-if)# tms-class
Router(config-if)# exit
Router(config)# class-map type control mitigation match-all MIT_CLASS_1

Router(config-cmap)# match priority 3

Router(config-cmap)# match primitive block

Router(config-cmap)# exit

Router(config)# policy-map type control mitigation MIT_POL_1
Router(config-pmap)# class MIT_CLASS_1

Router(config-pmap-c)# acl drop

Router(config-pmap-c)# end
```

Related Commands

Command	Description
class-map type control mitigation	Configures a mitigation type class map.
ignore (TMS)	Configures the TMS Rules Engine to ignore a mitigation enforcement action.
match primitive	Configures a primitive match in a mitigation type class map.
match priority	Configures the match priority level for a mitigation enforcement action.
parameter-map type mitigation	Configures a mitigation type parameter map.
policy-map type control mitigation	Configures a mitigation type policy map.
redirect route	Configures a redirect enforcement action in a mitigation type policy map.
tms-class	Associates an interface with an ACL drop enforcement action.
variable	Defines the next-hop variable in a mitigation type parameter map.

action-type

To enable the type of action to be performed on accounting records, use the **action-type** command in accounting method list configuration mode. To disable the action for the accounting records, use the **no** form this command.

action-type {**none**| **start-stop**| **stop-only**}

no action-type {**none**| **start-stop**| **stop-only**}

Cisco 1000 Series Router

action-type {**none**| **start-stop** [**periodic** {**disable**| **interval** *minutes*}]| **stop-only**}

no action-type {**none**| **start-stop** [**periodic** {**disable**| **interval** *minutes*}]| **stop-only**}

Syntax Description

none	Sets the action-type of the accounting records to none.
start-stop	Sets the start and stop action for the accounting records.
stop-only	Sets the stop action for the accounting records when service terminates.
periodic	(Optional) Specifies the periodic accounting action.
disable	Disables periodic accounting action.
interval	Sets the periodic accounting interval.
minutes	Periodic interval, in minutes, for accounting update records.

Command Default

If the periodic interval is not specified, information of all periodic accounting records is displayed.

Command Modes

accounting method list configuration (cfg-acct-mlist)

Command History

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

Usage Guidelines

Use the **action-type** command to enable the type of action to be performed on accounting records.

Examples

The following is sample output from the **action-type**command:

```
Router(config)# aaa accounting network default
Router(cfg-acct-mlist)# action-type start-stop periodic interval 1
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.

activate

To activate fail-close mode so that unencrypted traffic cannot pass through a group member before that member is registered with a key server, use the **activate** command in crypto map fail-close configuration mode. To disable fail-close mode, use the **no** form of this command.

activate

no activate

Syntax Description

This command has no arguments or keywords.

Command Default

Fail-close mode is not activated.

Command Modes

Crypto map fail-close configuration (crypto-map-fail-close)

Command History

Release	Modification
12.4(22)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

The **crypto map** command and **gdoi fail-clos**e keywords must precede this command. However, fail-close mode is not activated until the **activate** command is also configured.

Examples

The following example shows that fail-close mode has been activated, and unencrypted traffic from access list 102 is allowed before the group member is registered:

```
crypto map map1 gdoi fail-close
 match address 102
 activate crypto map map1 10 gdoi
 set group ks1_group
 match address 101
!
access-list 101 deny ip 10.0.1.0 0.0.0.255 10.0.1.0 0.0.0.255
access-list 102 deny tcp any eq telnet any
```

Related Commands

Command	Description
show crypto map gdoi fail-close	Displays information about the status of the fail-close mode.

add (WebVPN)

To add an ACL entry at a specified position, use the **add** command in webvpn acl configuration mode. To remove an entry from the position specified, use the **no** form of this command.

add *position acl-entry*

no add *position acl-entry*

Syntax Description

position	Position in the entry list to which the ACL rule is to be added.
acl-entry	Permit or deny command string.

Command Default

The ACL entry is appended to the end of the entry list.

Command Modes

Webvpn acl configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Examples

The following example shows that the ACL rule should be added to the third position of the ACL list:

```
webvpn context context1
 acl acl1
  add 3 permit url any
```

Related Commands

Command	Description
acl	Defines an ACL using a SSL VPN gateway at the Application Layer level.
wevpn context	Configures the SSL VPN context and enters webvpn context configuration mode.

address

To specify the IP address of the Rivest, Shamir, and Adelman (RSA) public key of the remote peer that you will manually configure in the keyring, use the **address** command inrsa-pubkey configuration mode. To remove the IP address, use the **no** form of this command.

address *ip-address*

no address *ip-address*

Syntax Description

ip-address	IP address of the remote peer.

Command Default

No default behavior or values

Command Modes

Rsa-pubkey configuration

Command History

Release	Modification
11.3 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 Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Before you can use this command, you must enter the **rsa-pubkey** command in the crypto keyring mode.

Examples

The following example specifies the RSA public key of an IP Security (IPSec) peer:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
```

```
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

Related Commands

Command	Description
crypto keyring	Defines a crypto keyring to be used during IKE authentication.
key-string	Specifies the RSA public key of a remote peer.
rsa-pubkey	Defines the RSA manual key to be used for encryption or signatures during IKE authentication.

address (IKEv2 keyring)

To specify an IPv4 or IPv6 address or the range of the peer in an Internet Key Exchange Version 2 (IKEv2) keyring, use the **address** command inIKEv2 keyring peer configuration mode. To remove the IP address, use the **no** form of this command.

address {*ipv4-address* [*mask*] | *ipv6-address prefix*}

no address

Syntax Description

ipv4-address	IPv4 address of the remote peer.
mask	(Optional) Subnet mask.
ipv6-address	IPv6 address of the remote peer.
prefix	Prefix length

Command Default

The IP address is not specified.

Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
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 specify the peer's IP address, which is the IKE endpoint address and independent of the identity address.

Examples

The following examples show how to specify the preshared key of an IP Security (IPsec) peer:

```
Router(config)# crypto ikev2 keyring keyring1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# address 10.0.0.1 255.255.255.0
Router(config)# crypto ikev2 keyring keyring2
```

```
Router(config-ikev2-keyring)# peer peer2
Router(config-ikev2-keyring-peer)# address 2001:DB8:0:ABCD::1/2
```

Related Commands

Command	Description
crypto ikev2 keyring	Defines an IKEv2 keyring.
description (ikev2 keyring)	Describes an IKEv2 peer or a peer group for the IKEv2 keyring.
hostname (ikev2 keyring)	Specifies or modifies the hostname for the network server or peer.
peer	Defines a peer or a peer group for the keyring.
identity (ikev2 keyring)	Identifies the peer with IKEv2 types of identity.
pre-shared-key (ikev2 keyring)	Defines a preshared key for the IKEv2 peer.

address ipv4

To configure the IP address of a Diameter peer, use the **address ipv4** command in Diameter peer configuration submode. To disable the configured address, use the **no** form of this command.

address ipv4 *ip-address*

no address ipv4 *ip-address*

Syntax Description

ip address	The IP address of the host.

Command Default

No IP address is configured.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Examples

The following example shows how to configure the IP address of a Diameter peer:

```
Router (config-dia-peer)# address ipv4
 192.0.2.0
```

Related Commands

Command	Description
diameter peer	Defines a Diameter peer and enters Diameter peer configuration mode.

address ipv4 (config-radius-server)

To configure the IPv4 address for the RADIUS server accounting and authentication parameters, use the **address ipv4** command in RADIUS server configuration mode. To remove the specified RADIUS server accounting and authentication parameters, use the **no** form of this command.

address ipv4 {*hostname*| *ipv4address*} [**acct-port** *port*| **alias** {*hostname*| *ipv4address*}| **auth-port** *port* [**acct-port** *port*]]

no address ipv4 {*hostname*| *ipv4address*} [**acct-port** *port*| **alias** {*hostname*| *ipv4address*}| **auth-port** *port* [**acct-port** *port*]]

Syntax Description

hostname	Domain Name System (DNS) name of the RADIUS server host.
ipv4address	RADIUS server IPv4 address.
acct-port *port*	(Optional) Specifies the User Datagram Protocol (UDP) port for the RADIUS accounting server for accounting requests. The default port is 1646.
alias {*hostname* | *ipv4address*}	(Optional) Specifies an alias for this server. The alias can be an IPv4 address or hostname. Up to eight aliases can be configured for this server.
auth-port *port*	(Optional) Specifies the UDP port for the RADIUS authentication server. The default port is 1645.

Command Default

The RADIUS server accounting and authentication parameters are not configured.

Command Modes

RADIUS server configuration (config-radius-server)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

The **aaa new-model** command must be configured before issuing this command.

The Cisco TrustSec (CTS) feature uses Secure RADIUS to prescribe a process of authentication, authorization, session association, encryption, and traffic filtering.

Before an alias can be configured for the RADIUS server, the server's IPv4 address or DNS name must be configured. This is accomplished by using the **address ipv4** command and the *hostname* argument. An alias can then be configured by using the **address ipv4** command, **alias** keyword, and the *hostname* argument.

Examples

The following example shows how to configure the RADIUS server accounting and authentication parameters:

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2 acct-port 1813 auth-port 1812
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
address ipv6	Configures the IPv6 address for the RADIUS server accounting and authentication parameters.
radius server	Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode.

address ipv6 (config-radius-server)

To configure the IPv6 address for the RADIUS server accounting and authentication parameters, use the **address ipv6** command in RADIUS server configuration mode. To remove the specified RADIUS server accounting and authentication parameters, use the **no** form of this command.

address ipv6 {*hostname*| *ipv6address*} [**acct-port** *port*| **alias** {*hostname*| *ipv6address*}| **auth-port** *port* [**acct-port** *port*]]

no address ipv6 {*hostname*| *ipv6address*} [**acct-port** *port*| **alias** {*hostname*| *ipv6address*}| **auth-port** *port* [**acct-port** *port*]]

Syntax Description

hostname	Domain Name System (DNS) name of the RADIUS server host.
ipv6address	RADIUS server IPv6 address.
acct-port *port*	(Optional) Specifies the User Datagram Protocol (UDP) port for the RADIUS accounting server for accounting requests. The default port is 1646.
alias {*hostname* | *ipv6address*}	(Optional) Specifies an alias for this server. The alias can be an IPv6 address or hostname. Up to eight aliases can be configured for this server.
auth-port *port*	(Optional) Specifies the UDP port for the RADIUS authentication server. The default port is 1645.

Command Default

The RADIUS server accounting and authentication parameters are not configured.

Command Modes

RADIUS server configuration (config-radius-server)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

The **aaa new-model** command must be configured before accessing this command.

The Cisco TrustSec (CTS) feature uses Secure RADIUS to prescribe a process of authentication, authorization, session association, encryption, and traffic filtering.

Before an alias can be configured for the RADIUS server, the server's IPv6 address or DNS name must be configured. This is accomplished by using the **address ipv6** command and the *hostname* argument. An alias can then be configured by using the **address ipv6** command, the **alias** keyword, and the *hostname* argument.

Examples

The following example shows how to configure the RADIUS server accounting and authentication parameters:

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv6 2001:DB8:1::1 acct-port 1813 auth-port 1812
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
address ipv4	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.
radius server	Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode.

address ipv4 (GDOI)

To set the source address, which is used as the source for packets originated by the local key server, use the **address ipv4**command in GDOI local server configuration mode. To remove the source address, use the **no** form of this command.

address ipv4 *ip-address*

no address ipv4 *ip-address*

Syntax Description

ip-address	Source address of the local key server.

Command Default

A source address is not configured.

Command Modes

GDOI local server configuration (config-local-server)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

When this command is used with unicast rekeys, the address is used as the source of the outgoing rekey message. When this command is used with redundancy, the address is used as the source of the outgoing announcement message. If both unicast rekeying and redundancy are configured, the same address is the source of both types of packets.

If multicast rekeying is configured and the **address ipv4** command is configured, the address (*ip-address)*is the source of the outgoing multicast packet. If multicast is configured but the **address ipv4** command is not configured, the access control list (ACL) specified in the **rekey address ipv4** command identifies the source of the outgoing multicast packet.

Examples

The following example shows the local server IP address is 10.1.1.0:

```
server local
 rekey algorithm aes 192
 rekey address ipv4 121
 rekey lifetime seconds 300
 rekey retransmit 10 number 2
 rekey authentication mypubkey rsa mykeys
 address ipv4 10.1.1.0
 sa ipsec 1
```

Related Commands

Command	Description
rekey address ipv4	Sends a rekey to a destination multicast address.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

address ipv6 (TACACS+)

To configure the IPv6 address of the TACACS+ server, use the **address ipv6** command in TACACS+ server configuration mode. To remove the IPv6 address, use the **no** form of this command.

address ipv6 *ipv6-address*

no address ipv6 *ipv6-address*

Syntax Description

ipv6-address	The private TACACS+ server host.

Command Default

No TACACS+ server is configured.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Use the address ipv6 (TACACS+) command after you have enabled the TACACS+ server using the **tacacs server** command.

Examples

The following example shows how to specify the IPv6 address on a TACACS+ server named server1:

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# address ipv6 2001:0DB8:3333:4::5
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters config server tacacs mode.

addressed-key

To specify which peer's RSA public key you will manually configure, use the **addressed-key**command in public key chain configuration mode .

addressed-key *key-address* [**encryption**| **signature**]

Syntax Description

key-address	Specifies the IP address of the remote peer's RSA keys.
encryption	(Optional) Indicates that the RSA public key to be specified will be an encryption special usage key.
signature	(Optional) Indicates that the RSA public key to be specified will be a signature special usage key.

Command Default

If neither the **encryption** nor **signature** keywords are used, general purpose keys will be specified.

Command Modes

Public key chain configuration. This command invokes public key configuration mode.

Command History

Release	Modification
11.3 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 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 this command or the **named-key** com mand to specify which IP Security peer's RSA public key you will manually configure next.

Follow this command with the **key string** command to specify the key.

If the IPSec remote peer generated general-purpose RSA keys, do not use the **encryption** or **signature** keywords.

If the IPSec remote peer generated special-usage keys, you must manually specify both keys: use this command and the **key-string** command twice and use the **encryption** and **signature** keywords respectively.

Examples

The following example manually specifies the RSA public keys of two IPSec peers. The peer at 10.5.5.1 uses general-purpose keys, and the other peer uses special-usage keys.

```
Router(config)# crypto key pubkey-chain rsa
Router(config-pubkey-chain)# named-key otherpeer.example.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 005C300D 06092A86 4886F70D 01010105
Router(config-pubkey)# 00034B00 30480241 00C5E23B 55D6AB22
Router(config-pubkey)# 04AEF1BA A54028A6 9ACC01C5 129D99E4
Router(config-pubkey)# 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
Router(config-pubkey)# BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
Router(config-pubkey)# D58AD221 B583D7A4 71020301 0001
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# addressed-key 10.1.1.2 encryption
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# addressed-key 10.1.1.2 signature
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 0738BC7A 2BC3E9F0 679B00FE 53987BCC
Router(config-pubkey)# 01030201 42DD06AF E228D24C 458AD228
Router(config-pubkey)# 58BB5DDD F4836401 2A2D7163 219F882E
Router(config-pubkey)# 64CE69D4 B583748A 241BED0F 6E7F2F16
Router(config-pubkey)# 0DE0986E DF02031F 4B0B0912 F68200C4
Router(config-pubkey)# C625C389 0BFF3321 A2598935 C1B1
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# exit
Router(config)#
```

Related Commands

Command	Description
crypto key pubkey-chain rsa	Enters public key configuration mode (to allow you to manually specify the RSA public keys of other devices).
key-string (IKE)	Specifies the RSA public key of a remote peer.
named-key	Specifies which peer RSA public key you will manually configure.
show crypto key pubkey-chain rsa	Displays peer RSA public keys stored on your router.

administrator authentication list

To authenticate an administrative introducer for a Secure Device Provisioning (SDP) transaction, use the **administrator authentication list** command in tti-registrar configuration mode. To disable administrative introducer authentication, use the **no** form of this command.

administrator authentication list *list-name*

no administrator authentication list *list-name*

Syntax Description

list-name	Name of list.

Command Default

All introducers are authenticated as users; their username is used directly to build the device name.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

When you use the **administrator authentication list** command in SDP transactions, the RADIUS or TACACS+ authentication, authorization, and accounting (AAA) server checks for a valid account by looking at the username and password.

The authentication list and the authorization list usually both point to the same AAA list. It is possible that the lists can be on different databases, but it is generally not recommended.

Examples

The following example shows that an administrative authentication list named authen-rad and an administrative authorization list named author-rad have been configured on a RADIUS AAA server; a user authentication list named authen-tac and a user authorization list named author-tac have been configured on a TACACS+ server:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# pki-server mycs
Router(tti-registrar)# administrator
 authentication list authen-rad
Router(tti-registrar)# administrator
 authorization list author-rad
Router(tti-registrar)# authentication list authen-tac
Router(tti-registrar)# authorization list author-tac
Router(tti-registrar)# template username ftpuser password ftppwd
Router(tti-registrar)# template config ftp://ftp-server/iossnippet.txt
Router(tti-registrar)# end
```

Related Commands

Command	Description
administrator authorization list	Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner for an administrative introducer in an SDP transaction.
authentication list (tti-registrar)	Authenticates an introducer in an SDP transaction.
authorization list (tti-registrar)	Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner for a user introducer in an SDP transaction.

administrator authorization list

To specify the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS command-line interface (CLI) snippet that is sent back to the petitioner for an administrative introducer in a Secure Device Provisioning (SDP) transaction, use the **administrator authorization list** command in tti-registrar configuration mode. To disable the subject name and list of template variables, use the **no** form of this command.

administrator authorization list *list-name*

no administrator authorization list *list-name*

Syntax Description

list-name	Name of list.

Command Default

There is no authorization information requested from the authentication, authorization, and accounting (AAA) server for the administrator.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(14)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 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 you use the **administrator authorization list** command in SDP transactions, the RADIUS or TACACS+ AAA server stores the subject name and template variables. The name and variables are sent back to the petitioner in the Cisco IOS CLI snippets. This list and the authorization list are usually on the same database, but they can be on different AAA databases. (Storing lists on different databases is not recommended.)

When a petitioner makes an introducer request, multiple queries are sent to the AAA list database on the RADIUS or TACACS+ server. The queries search for entries of the following form:

```
user Password <userpassword>
   cisco-avpair="ttti:subjectname=<<DN subjectname>>"
   cisco-avpair="tti:iosconfig#<<value>>"
   cisco-avpair="tti:iosconfig#<<value>>"
   cisco-avpair="tti:iosconfig#=<<value>>"
```

Note The existence of a valid AAA username record is enough to pass the authentication check. The cisco-avpair=tti information is necessary only for the authorization check.

If a subject name were received in the authorization response, the registrar stores it in the enrollment database, and that subject name overrides the subject name that is supplied in the subsequent certificate request (PKCS10) from the petitioner device.

The numbered tti:iosconfig values are expanded into the Cisco IOS snippet that is sent to the petitioner. The configurations replace any numbered ($1 through $9) template variable. Because the default Cisco IOS snippet template does not include the variables $1 through $9, these variables are ignored unless you configure an external Cisco IOS snippet template. To specify an external configuration, use the **template config** command.

Note The template configuration location may include a variable $n, which is expanded to the name that the administrator enters in the additional SDP dialog.

Examples

The following example shows that an administrative authentication list named authen-rad and an administrative authorization list named author-rad have been configured on a RADIUS AAA server; a user authentication list named authen-tac and a user authorization list named author-tac have been configured on a TACACS+ server:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# pki-server mycs
Router(tti-registrar)# administrator
 authentication list authen-rad
Router(tti-registrar)# administrator
 authorization list author-rad
Router(tti-registrar)# authentication list authen-tac
Router(tti-registrar)# authorization list author-tac
Router(tti-registrar)# template username ftpuser password ftppwd
Router(tti-registrar)# template config ftp://ftp-server/iossnippet.txt
Router(tti-registrar)# end
```

Related Commands

Command	Description
administrator authentication list	Authenticates an administrative introducer for an SDP transaction.
authentication list (tti-registrar)	Authenticates a user introducer for an SDP transaction.
authorization list (tti-registrar)	Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner for a user introducer in an SDP operation.

alert

To enable message logging when events, such as a text-chat, begin, use the **alert** command in the appropriate configuration mode. To change the configured setting or revert to the default setting, use the **no** form of this command.

alert {**on**| **off**}

no alert

Syntax Description

on	Enables message logging for instant messenger application policy events.
off	Disables message logging for instant messenger application policy events.

Command Default

If this command is not configured, the global setting for the **ip inspect alert-off** command will take effect.

Command Modes

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Examples

The following example shows to enable audit trail messages for all AOL instant messenger traffic:

```
appfw policy-name my-im-policy
 application http
  port-misuse im reset
!
 application im aol
  server deny name login.user1.aol.com
  audit trail on
  alert on
```

Related Commands

Command	Description
ip inspect alert-off	Disables Cisco IOS firewall alert messages.

alert (zone-based policy)

To turn on or off console display of Cisco IOS stateful packet inspection alert messages, use the **alert** command in parameter-map type inspect configuration mode. To change the configured setting or revert to the default setting, use the **no** form of this command.

alert {**on**| **off**}

no alert {**on**| **off**}

Syntax Description

on	Alert messages are generated.
off	Alert messages are not generated.

Command Default

Alert messages are not issued.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.4S	This command was modified to enable its use only after configuration of the **parameter-map type inspect-vrf**, **parameter-map type inspect-zone**, or **parameter-map type inspect global** commands.

Usage Guidelines

You can use the **alert** command when you are creating a parameter map.

You must configure the **parameter-map type inspect**, **parameter-map type inspect-vrf**, **parameter-map type inspect-zone**, **parameter-map type inspect global**, or **parameter-map type urlfilter** command before you can configure the **alert** command.

You must configure the **alert on** command for the alert messages to be logged. You can configure the **log** command to log the alert messages to either the syslog or the high-speed logger (HSL).

You must configure the **alert on** command for the parameter map for which the alert messages are to be logged. For example, to log zone-related alert messages, you must configure the **alert on** command after you configure the **parameter-map type inspect-zone** command.

Examples

The following example shows a sample inspect parameter map with the Cisco IOS stateful packet inspection alert messages enabled:

```
Router(config)# parameter-map type inspect insp-params
Router(config-profile)# alert on
```

Related Commands

Command	Description
ip inspect alert-off	Disables the Cisco IOS firewall alert messages.
log	Logs the firewall activity for an inspect parameter map.
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
parameter-map type inspect-vrf	Configures an inspect VRF-type parameter map and enters parameter-map type inspect configuration mode.
parameter-map type inspect-zone	Configures an inspect zone-type parameter map and enters parameter-map type inspect configuration mode.
parameter-map type inspect global	Configures a global parameter map and enters parameter-map type inspect configuration mode.
parameter-map type urlfilter	Creates or modifies a parameter map for URL filtering parameters.

alert-severity

To change the alert severity rating for a given signature or signature category, use the **alert-severity** command in signature-definition-action (config-sigdef-action) or IPS-category-action (config-ips-category-action) configuration mode. To return to the default action, use the **no** form of this command.

alert-severity {**high**| **medium**| **low**| **informational**}

no alert-severity

Syntax Description

high **medium** | **low** | **informational**	Alert severity action for a given signature or signature category.

Command Default

No default behavior or values

Command Modes

Signature-definition-action configuration (config-sigdef-action) IPS-category-action configuration (config-ips-category-action)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Before issuing the **alert-severity** command, you must specify either a signature via the **signature** command or a signature category (such as attack-type) via the **category** command.

Examples

The following example shows how to set the alert severity value to low for signature 5760:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature-definition

Router(config-sigdef)# signature 5726 0

Router(config-sigdef-sig)# alert-severity low

Router(config-sigdef)#^ZDo you want to accept these changes? [confirm]
Router#
*Nov 9 21:50:55.847: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 12 of 11 engines
*Nov 9 21:50:55.859: %IPS-6-ENGINE_READY: multi-string - build time 12 ms - packets for
this engine will be scanned
*Nov 9 21:50:55.859: %SYS-5-CONFIG_I: Configured from console by cisco on console
```

Related Commands

Command	Description
category	Specifies a signature category that is to be used for multiple signature actions or conditions.
signature	Specifies a signature for which the CLI user tunings will be changed.

alg sip blacklist

To configure a dynamic Session Initiation Protocol (SIP) application layer gateway (ALG) blacklist for destinations, use the **alg sip blacklist** command in global configuration mode. To remove a blacklist, use the **no** form of this command.

alg sip blacklist trigger-period *seconds* **trigger-size** *number-of-events* [**block-time** *block-time*] [**destination** *ipv4-address*]

no alg sip blacklist trigger-period *seconds* **trigger-size** *number-of-events* [**block-time** *block-time*] [**destination** *ipv4-address*]

Syntax Description

trigger-period *seconds*	Specifies the time period, in seconds, during which events are monitored before a blacklist is triggered. Valid values are from 10 to 60000.
trigger-size *number-of-events*	Specifies the number of events that are allowed from a source before the blacklist is triggered and all packets from that source are blocked. Valid values are from 1 to 65535.
block-time *block-time*	(Optional) Specifies the time period, in seconds, when packets from a source are blocked if the configured limit is exceeded. Valid values are from 0 to 2000000. The default is 30.
destination *ipv4-address*	(Optional) Specifies the destination IP address to be monitored.

Command Default

A blacklist is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

If the configured block time is zero, it means that a blacklist is not configured for the source. If no destination is specified, all destinations are monitored for denial of service (DoS) attacks.

The following events trigger a blacklist:

- In the configured period of time if a source sends multiple requests to a destination and receives non-2xx (as per RFC 3261, any response with a status code between 200 and 299 is a "2xx response") final responses from the destination.

- In the configured period of time if a source sends multiple requests to a destination and does not receive any response from the destination.

Examples

The following example shows how to configure a blacklist for the destination IP address 10.2.2.23:

```
Device(config)# alg sip blacklist trigger-period 100 trigger-size 10 destination 10.2.2.23
```

Related Commands

show alg sip	Displays all SIP ALG information.

alg sip processor

To configure the maximum number of backlog messages that wait for shared processor resources, use the **alg sip processor** command in global configuration mode. To disable the configuration, use the **no** form of this command.

alg sip processor {**global** | **session**} **max-backlog** *concurrent-usage*

no alg sip processor {**global** | **session**} **max-backlog** *concurrent-usage*

Syntax Description

global	Sets the maximum number of backlog messages that are waiting for shared resources for all Session Initiation Protocol (SIP) sessions. The default is 100.
session	Sets a per session limit for the number of backlog messages waiting for shared resources. The default is 10.
max-backlog	Specifies the maximum backlog for all sessions or for a single session.
concurrent-usage	Maximum number of backlog messages waiting for concurrent processor usage. Valid values are from 1 to 200 for the **global** keyword and from 1 to 20 for the **session** keyword.

Command Default

Blacklist messages are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

Use this command to configure parameters against distributed denial of service (DoS) attacks.

Examples

The following example shows set the per session limit for the number of backlog messages:

```
Device(config)# alg sip processor session max-backlog 5
```

Related Commands

show alg sip	Displays all SIP ALG information.

alg sip timer

To configure a timer that the Session Initiation Protocol (SIP) application layer gateway (ALG) uses to manage SIP calls, use the **alg sip timer** command in global configuration mode. To remove the configured timer, use the **no** form of this command.

alg sip timer {**call-proceeding-timeout** *call-proceeding-time* | **max-call-duration** *call-duration*}

no alg sip timer {**call-proceeding-timeout** *call-proceeding-time* | **max-call-duration** *call-duration*}

Syntax Description

call-proceeding-timeout *call-proceeding-time*	Sets the call proceeding time interval, in seconds, for SIP calls that do not receive a response. The range is from 30 to 1800. The default is 180.
max-call-duration *call-duration*	Sets the maximum call duration, in seconds, for a successful SIP call. The range is from 0 to 65535. The default is 3600.

Command Default

A timer is not configured for SIP ALG calls.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

The timer that you configure with the **alg sip timer call-proceeding-timeout** command is similar to the number of times a phone rings for a call; the SIP ALG releases the SIP call if the call is not connected after the final ring.

When you configure the **alg sip timer max-call-duration** command, all SIP calls whose duration exceeds the configured value is released. The SIP ALG only releases resources that are used by the calls; and the SIP ALG is not torn down.

Examples

The following example shows how to configure a maximum time interval after which an unsuccessful SIP call is released:

```
Device(config)# alg sip timer call-proceeding-timeout 200
```

The following example shows how to configure a call duration time for a successful SIP call:

```
Device(config)# alg sip timer max-call-duration 180
```

Related Commands

show alg sip	Displays all SIP ALG information.

algorithm

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

To specify the algorithm to be used for decrypting the filters, use the **algorithm** command in FPM match encryption filter configuration mode.

algorithm *algorithm*

Syntax Description

algorithm	The algorithm to be used for decrypting. Currently, aes256cbc is the only algorithm supported.

Command Default

No algorithm is specified.

Command Modes

FPM match encryption filter configuration (c-map-match-enc-config)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.2(4)M	This command was removed from the Cisco IOS software.

Usage Guidelines

If you have access to an encrypted traffic classification definition file (eTCDF) or if you know valid values to configure encrypted Flexible Packet Matching (FPM) filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the **algorithm** command to specify the algorithm used for decrypting the filters.

Examples

The following example shows how to specify the algorithm for decrypting the filter:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# algorithm aes256cbc
Router(c-map-match-enc-config)#
```

Related Commands

Command	Description
class-map type	Creates a class map to be used for matching packets to a specified class.
match encrypted	Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode.