Cisco IOS Intelligent Services Gateway Commands

aaa authorization radius-proxy

To configure authentication, authorization, and accounting (AAA) authorization methods for Intelligent Services Gateway (ISG) RADIUS proxy subscribers, use the **aaa authorization radius-proxy** command in global configuration mode. To remove authorization methods for ISG RADIUS proxy subscribers, use the **no** form of this command.

aaa authorization radius-proxy {**default** | *list-name*} *method1* [*method2* [*method3...*]]

no aaa authorization radius-proxy {**default** | *list-name*} *method* [*method2* [*method3...*]]

Syntax Description

default	Configures the specified method list as the default method list for ISG RADIUS proxy subscriber authorization.
list-name	Character string used to name the list of authorization methods.
method1, *method2*, *method3*, etc.	Specifies an authorization method or multiple authorization methods to be used for authorization. A method may be any one of the following: • **group** *group-name*—Uses a subset of RADIUS servers for authorization as defined by the **server group** *group-name* command. • **group radius**—Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.

Command Default

A AAA method list for ISG RADIUS proxy clients is not specified.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **aaa authorization radius-proxy** command to enable authorization and to create named method lists, which define authorization methods that are used to authorize ISG RADIUS proxy subscribers. Method lists for authorization define the ways in which authorization is performed and the sequence in which these methods are performed. A method list is a named list describing the authorization methods to be used, in sequence. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted.

Examples

The following example configures an ISG RADIUS proxy authorization method list called “RP”. The server group called “EAP” is the method specified in that method list. The control policy called “PROXYRULE” contains a policy rule to send RADIUS proxy packets to the method list “RP”.

```
aaa group server radius EAP
 server 10.2.36.253 auth-port 1812 acct-port 1813

aaa authorization radius-proxy RP group EAP

policy-map type control PROXYRULE
 class type control always event session-start
  1 proxy aaa list RP
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

aaa authorization subscriber-service

To specify one or more authentication, authorization, and accounting (AAA) authorization methods for Intelligent Services Gateway (ISG) to use in providing subscriber service, use the **aaa authorization subscriber-service** command in global configuration mode. To remove this specification, use the **no** form of this command.

aaa authorization subscriber-service {**default** {**cache** | **group** | **local**} | *list-name*} *method1* [*method2*...]

no aaa authorization subscriber-service {**default** {**cache** | **group** | **local**} | *list-name*} *method1* [*method2*...]

Syntax Description

default	Used with either the **cache**, **group** or **local** keywords to select the default authorization method.
cache	Specifies the cached-group for the default authorization method.
group	Specifies the server-group for the default authorization method.
local	Specifies the local database for the default authorization method.
list-name	Character string used to name the list of authorization methods.
method1 [*method2*...]	Specifies an authorization method or (optionally) multiple authorization methods to be used for authorization. A method may be any one of the keywords listed in Table 1.

Command Default

A method list is not specified.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Table 1 lists the keywords that can be used with the **aaa authorization subscriber-service** command to specify authorization methods.

Table 1 aaa authorization subscriber-service Keywords

Keyword	Description
cache *name*	Uses the specified cache, which is located in the profile database, for authorization.
cache radius	Uses the cache for all RADIUS requests for subscriber service authorization.
cache tacacs	Uses the cache for all TACACS+ requests for subscriber service authorization.

Table 1 aaa authorization subscriber-service Keywords (continued)

Keyword	Description
group *name*	Uses a subset of RADIUS or TACACS+ servers for authorization as defined by the **server group** command.
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.
group tacacs	Uses the list of all TACACS+ servers for authorization as defined by the **aaa group server tacacs+** command.
local	Uses the local database for authorization.

Cisco IOS software supports the following methods of authorization of ISG subscriber services:

- RADIUS—The network access server requests authorization information from the RADIUS security server group. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.
- TACACS+—The network access server exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value (AV) pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.
- Local—The router or access server consults its local database, as defined by the username command, to authorize specific rights for users. Only a limited set of functions can be controlled via the local database.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, method lists must be applied to specific lines or interfaces before any of the defined methods will be performed.

The **authorization aaa subscriber-service** command causes a request packet containing a series of AV pairs to be sent to the RADIUS or TACACS daemon as part of the authorization process. The daemon can do one of the following:

- Accept the request as is.
- Make changes to the request.
- Refuse the request and refuse authorization.

Examples

The following example defines the subscriber service authorization method list named “mygroup”, which specifies RADIUS authorization. If the RADIUS server fails to respond, local authorization will be performed.

```
aaa authorization subscriber-service mygroup group radius local
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa group server tacacs+	Groups different TACACS+ server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
tacacs-server host	Specifies a TACACS+ host.

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.

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 server radius policy-device

To enable Intelligent Services Gateway (ISG) RADIUS server configuration mode, in which the ISG RADIUS server parameters can be configured, use the **aaa server radius policy-device** command in global configuration mode. To remove the RADIUS server configuration, use the **no** form of this command.

aaa server radius policy-device

no aaa server radius policy-device

Syntax Description

This command has no arguments or keywords.

Command Default

RADIUS ISG parameters are not configured. No external policy device is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB

Usage Guidelines

The **aaa server radius policy-device** command enables ISG RADIUS server configuration mode, in which global ISG RADIUS server parameters can be configured.

Examples

The following example configures a shared encryption key for the RADIUS client and specifies authentication details.

```
Router(config)#aaa server radius policy-device
Router(config-locsvr-policy-device-radius)#key cisco
Router(config-locsvr-policy-device-radius)#client 10.1.1.13
Router(config-locsvr-policy-device-radius)#message-authenticator ignore
```

Related Commands

Command	Description
key	Configures a shared encryption key for the RADIUS clients.
client	Allows modification of RADIUS clients at run time.
message-authenticator	Authenticates messages from clients.

aaa server radius proxy

To enable Intelligent Services Gateway (ISG) RADIUS proxy configuration mode, in which ISG RADIUS proxy parameters can be configured, use the **aaa server radius proxy** command in global configuration mode. To remove the ISG RADIUS proxy configuration, use the **no** form of this command.

aaa server radius proxy

no aaa server radius proxy

Syntax Description

This command has no arguments or keywords.

Command Default

ISG RADIUS proxy parameters are not configured, and ISG does not serve as a RADIUS proxy.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **aaa server radius proxy** command enables ISG RADIUS proxy server configuration mode, in which global RADIUS proxy parameters can be configured. The **client** command can be used in RADIUS proxy server configuration mode to specify a client for which RADIUS proxy parameters can be configured. Client-specific RADIUS proxy configurations take precedence over the global RADIUS proxy server configuration.

Examples

The following example configures the accounting port to be used by ISG for all RADIUS proxy clients:

```
aaa server radius proxy
 accounting port 1200
```

accounting aaa list

To enable Intelligent Services Gateway (ISG) accounting and specify an authentication, authorization, and accounting (AAA) method list to which accounting updates will be forwarded, use the **accounting aaa list** command in service policy-map configuration or service policy traffic class configuration mode. To disable ISG accounting, use the **no** form of this command.

accounting aaa list *aaa-method-list*

no accounting aaa list *aaa-method-list*

Syntax Description

aaa-method-list	AAA method list to which Accounting-Start, interim, and Accounting-Stop records will be sent.

Command Default

ISG accounting is not enabled.

Command Modes

Service policy-map configuration
Service policy traffic class configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

An ISG sends accounting records to the AAA method list specified by the **accounting aaa list** command. A AAA method list must also be configured by using the **aaa accounting** command. See the *Cisco IOS Security Command Reference* for more information.

Use the **accounting aaa list** command to enable per-session accounting by configuring the command in service policy-map configuration mode. Per-session accounting can also be configured on a remote AAA server by adding the ISG accounting attribute to a user profile or to a service profile that does not include a traffic class.

To enable per-flow accounting, enter the **accounting aaa list** command in service policy traffic class configuration mode. Per-flow accounting can also be configured on a remote AAA server by adding the ISG accounting attribute to a service profile that includes a traffic class.

Examples

The following example shows ISG per-session accounting configured for a service called “video1”:

```
policy-map type service video1
 accounting aaa list mlist1
```

The following example shows ISG per-flow accounting configured for a service called “video1”:

```
class-map type traffic match-any video1
 match access-group output 101
 match access-group input 100
!
policy-map type service video1
```

```
class type traffic video1
 accounting aaa list mlist1
```

Related Commands

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

accounting method-list

To configure Intelligent Services Gateway (ISG) to forward accounting packets from RADIUS proxy clients to a specified server, use the **accounting method-list** command in RADIUS proxy server configuration mode or RADIUS proxy client configuration mode. To disable the forwarding of accounting packets from RADIUS proxy clients, use the **no** form of this command.

accounting method-list {*list-name* | **default**}

no accounting method-list {*list-name* | **default**}

Syntax Description

list-name	Name of the method list to which accounting packets are sent.
default	Specifies that accounting packets will be forwarded to the default RADIUS server.

Command Default

ISG RADIUS proxy handles accounting packets locally.

Command Modes

RADIUS proxy server configuration
RADIUS proxy client configuration

Command History

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

Usage Guidelines

By default, ISG RADIUS proxy responds locally to accounting packets it receives. The **accounting method-list** command configures ISG to forward accounting packets from RADIUS proxy clients to a specified method list. Forwarding of accounting packets can be configured globally for all RADIUS proxy clients or on a per-client basis. The per-client configuration of this command overrides the global configuration.

The default method list is configured with the **aaa accounting** command.

Examples

The following example shows the ISG configured to forward accounting packets from all RADIUS proxy clients to the method list “RP-ACCT-MLIST”:

```
aaa group server radius RP-BILLING
 server 10.52.199.147 auth-port 1645 acct-port 1646
 server 10.52.199.148 auth-port 1812 acct-port 1813
!
aaa group server radius RP-BILLING-HOTSTANDBY
 server 10.52.200.20 auth-port 1645 acct-port 1646
 server 10.52.200.21 auth-port 1812 acct-port 1813
!
…
aaa accounting network RP-ACCT-MLIST start-stop broadcast group RP-BILLING group
RP-BILLING-HOTSTANDBY
…
```

```
aaa server radius proxy
 key cisco
 accounting method-list RP-ACCT-MLIST
 client 10.52.100.20
 !
…
radius-server host 10.52.199.147 auth-port 1645 acct-port 1646 key troy
radius-server host 10.52.199.148 auth-port 1812 acct-port 1813 key tempest
radius-server host 10.52.200.20 auth-port 1645 acct-port 1646 key captain
radius-server host 10.52.200.21 auth-port 1812 acct-port 11813 key scarlet
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa server radius proxy	Enables ISG RADIUS proxy configuration mode, in which ISG RADIUS proxy parameters can be configured.
client (ISG RADIUS proxy)	Enters ISG RADIUS proxy client configuration mode, in which client-specific RADIUS proxy parameters can be specified.

accounting port

To specify the port on which Intelligent Services Gateway (ISG) listens for accounting packets from RADIUS proxy clients, use the **accounting port** command in RADIUS proxy server configuration or RADIUS proxy client configuration mode. To return to the default value, use the **no** form of this command.

accounting port *port-number*

no accounting port

Syntax Description

port-number	Port on which ISG listens for accounting packets from RADIUS proxy clients. The default is 1646.

Command Default

ISG listens for accounting packets from RADIUS proxy clients on port 1646.

Command Modes

RADIUS proxy server configuration (config-locsvr-proxy-radius)
RADIUS proxy client configuration (config-locsvr-radius-client)

Command History

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

Usage Guidelines

The accounting port can be specified globally for all RADIUS proxy clients, or it can be specified per client. The per-client configuration of this command overrides the global configuration.

Examples

The following example configures ISG to listen for accounting packets on port 1200 for all RADIUS proxy clients:

```
aaa server radius proxy
 accounting port 1200
```

The following example configures ISG to listen for accounting packets on port 1200 for the RADIUS proxy client with the IP address 10.10.10.10:

```
aaa server radius proxy
 client 10.10.10.10
  accounting port 1200
```

Related Commands

Command	Description
aaa server radius proxy	Enables ISG RADIUS proxy configuration mode, in which ISG RADIUS proxy parameters can be configured.
client (ISG RADIUS proxy)	Enters ISG RADIUS proxy client configuration mode, in which client-specific RADIUS proxy parameters can be specified.

arp ignore local

To prevent Intelligent Services Gateway (ISG) from replying to incoming Address Resolution Protocol (ARP) requests for destinations on the same interface, use the **arp ignore local** command in IP subscriber configuration mode. To reset to the default, use the **no** form of this command.

arp ignore local

no arp ignore local

Syntax Description

This command has no arguments or keywords.

Command Default

ISG replies to incoming ARP requests for destinations on the same interface.

Command Modes

IP subscriber configuration (config-subscriber)

Command History

Release	Modification
12.2(33)SRE1	This command was introduced.

Usage Guidelines

The **arp ignore local** command blocks ISG from replying to ARP requests received on an interface if the source and destination IP addresses for an ARP request are on the same VLAN that the interface is connected to, or if the destination IP address is in a different subnet but is routable from the interface where the ARP is received. ISG does, however, reply to ARP requests when the source and destination IP addresses are in the same subnet if the IP addresses belong to different VLANs.

If the **arp ignore local** command is configured and a subscriber session is in virtual routing and forwarding (VRF) transfer mode, ISG will reply to an ARP request from the customer premises equipment (CPE) if:

- The ARP request is for an IP address on the access interface that is reachable by ISG within the VRF.
- The destination IP address is not in the same VRF subnet as the VRF's multiservice interface.

When the CPE receives the ARP reply and routes the corresponding IP packets to ISG, ISG routes the packets in the VRF domain.

Examples

The following example shows how to configure ISG to ignore ARP requests received on Ethernet interface 0/0.1 if the source and destination are in the same subnet:

```
Router(config)# interface ethernet 0/0.1
Router(config-subif)# ip subscriber l2-connected
Router(config-subscriber)# arp ignore local
```

Related Commands

Command	Description
show ip subscriber	Displays information about ISG IP subscriber sessions.

authenticate (control policy-map class)

To initiate an authentication request for an Intelligent Services Gateway (ISG) subscriber session, use the **authenticate** command in control policy-map class configuration mode. To remove an authentication request for an ISG subscriber session, use the **no** form of this command.

action-number **authenticate** [**variable** *varname*] [**aaa list** {*list-name* | *default*}]

no *action-number* **authenticate** [**variable** *varname*] [**aaa list** {*list-name* | *default*}]

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.
variable	(Optional) Authenticates using the contents of the *varname* value instead of the unauthenticated username. If you do not specify an **aaa list**, the default AAA authentication list is used.
varname	Specifies that user authentication will be performed on the contents of the *varname* value, if present.
aaa list	(Optional) Specifies that authentication will be performed using an authentication, authorization, and accounting (AAA) method list.
list-name	Specifies the AAA method list to which the authentication request will be sent.
default	Specifies the default AAA method list to which the authentication request will be sent.

Command Default

The control policy will not initiate authentication.

Command Modes

Control policy-map class configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SB2	The **variable** keyword and *varname* argument were added.

Usage Guidelines

The **authenticate** command configures an action in a control policy map.

Control policies define the actions the system will take in response to specified events and conditions. A control policy map is used to configure an ISG control policy. A control policy is made of one or more control policy rules. A control policy rule is an association of a control class and one or more actions. The control class defines the conditions that must be met before the actions will be executed. The actions are numbered and executed sequentially within the policy rule.

Note that if you specify the default method list, the default list will not appear in the output of the **show running-config** command. For example, if you configure the following command:

```
Router(config-control-policymap-class-control)# 1 authenticate aaa list default
```

the following will display in the output for the **show running-config** command:

```
1 authenticate
```

Named method lists will display in the **show running-config** command output.

Examples

The following example shows an ISG configured to initiate an authentication request upon account logon. The authentication request will be sent to the AAA method list called AUTH-LIST.

```
policy-map type control LOGIN
 class type control always event account-logon
  1 authenticate aaa list AUTH-LIST
  2 service-policy type service unapply BLIND-RDT
```

The following example shows the policy map configured to initiate an authentication request using a name stored in the variable NEWNAME, instead of unauthenticated-username, using the AAA list EXAMPLE. The authenticate statement is shown in bold:

```
policy-map type control REPLACE_WITH_example.com
 class type control always event session-start
  1 collect identifier unauthenticated-username
  2 set NEWNAME identifier unauthenticated-username
  3 substitute NEWNAME "(.*@).*" "\1example.com"
  4 authenticate variable NEWNAME aaa list EXAMPLE
  5 service-policy type service name example

policy-map type service abc
 service vpdn group 1

bba-group pppoe global
 virtual-template 1
!
interface Virtual-Template1
 service-policy type control REPLACE_WITH_example.com
```

Related Commands

Command	Description
class type control	Specifies a control class for which actions may be configured in an ISG control policy map.
policy-map type control	Creates or modifies a control policy map, which defines an ISG control policy.
set variable	Creates a temporary memory to hold the value of identifier types received by the policy manager.
substitute	Matches the contents, stored in temporary memory of identifier types received by the policy manager, against a specified matching pattern and performs the substitution defined in a rewrite pattern.

authenticate (service policy-map)

To specify authentication as a condition of service activation and initiate authentication requests for Intelligent Services Gateway (ISG) subscribers accessing a service, use the **authenticate** command in service policy-map configuration mode. To remove this specification, use the **no** form of this command.

authenticate aaa list *name-of-list*

no authenticate aaa list *name-of-list*

Syntax Description

aaa	Specifies that authentication will be performed using an authentication, authorization, and accounting (AAA) method list.
list *name-of-list*	Specifies the AAA method list to which the authentication request will be sent.

Command Default

Authentication is not specified as a condition of service activation.

Command Modes

Service policy-map configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

The **authenticate** (service policy-map) command specifies authentication as a condition of service activation in an ISG service policy map. Service policy maps define ISG subscriber services. Services can also be defined in service profiles. Service policy maps and service profiles serve the same purpose; the only difference between them is that a service policy map is defined on the local device using the **policy-map type service** command, and a service profile is configured on an external device, such as a AAA server.

Examples

The following example specifies authentication as a condition of service activation in the ISG service called “service1”:

```
policy-map type service service1
 authenticate aaa list mlist
```

Related Commands

Command	Description
policy-map type service	Creates or modifies a service policy map, which is used to define an ISG subscriber service.
show policy-map type service	Displays the contents of all service policy maps or a specific service policy map.

authentication port

To specify the port on which Intelligent Services Gateway (ISG) listens for authentication packets from RADIUS proxy clients, use the **authentication port** command in RADIUS proxy server configuration or RADIUS proxy client configuration mode. To return to the default setting in which ISG listens for accounting packets on port 1645, use the **no** form of this command.

authentication port *port-number*

no authentication port *port-number*

Syntax Description

port-number	Port on which ISG listens for authentication packets from RADIUS proxy clients. The default is 1645.

Command Default

ISG listens for authentication packets from RADIUS proxy clients on port 1645.

Command Modes

RADIUS proxy server configuration
RADIUS proxy client configuration

Command History

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

Usage Guidelines

The authentication port can be specified globally for all RADIUS proxy clients, or it can be specified per client. The per-client configuration of this command overrides the global configuration.

Examples

The following example configures ISG to listen for authentication packets on port 1200 for all RADIUS proxy clients:

```
aaa server radius proxy
 authentication port 1200
```

The following example configures ISG to listen for authentication packets on port 1200 for the RADIUS proxy client with the IP address 10.10.10.10 :

```
aaa server radius proxy
 client 10.10.10.10
  authentication port 1200
```

Related Commands

Command	Description
aaa server radius proxy	Enables ISG RADIUS proxy configuration mode, in which ISG RADIUS proxy parameters can be configured.
client (ISG RADIUS proxy)	Enters ISG RADIUS proxy client configuration mode, in which client-specific RADIUS proxy parameters can be specified.

authorize identifier

To initiate a request for authorization based on a specified identifier in an Intelligent Services Gateway (ISG) control policy, use the **authorize identifier** command in control policy-map class configuration mode. To remove this action from the control policy map, use the **no** form of this command.

action-number **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier** *identifier-type* [**plus** *identifier-type*]

no *action-number*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.
aaa	(Optional) Authorization is performed using authentication, authorization, and accounting (AAA).
list-name	(Optional) AAA method list to which the authorization request is sent.
default	Default AAA method list is used.
password *password*	(Optional) Password used for AAA requests.
upon network-service-found continue	(Optional) Specifies that when a network service for the session is identified, actions in the policy rule will continue to be executed. The network service is applied later. This is the default.
upon network-service-found stop	(Optional) Specifies that when a network service for the session is identified, actions in the policy rule will no longer be executed, and the network service is applied.
use method *authorization-type*	(Optional) Authorization library to use. Valid keywords for *authorization-type* are: • **aaa**—AAA authorization. Default method. • **legacy**—All authorization methods are attempted, in the following order: Xconnect, SSG, RM, AAA, SGF. • **rm**—Resource Manager (RM) authorization. • **sgf**—Stack Group Forwarding (SGF) authorization. • **ssg**—Service Selection Gateway (SSG) authorization. • **xconnect**—Internal cross-connect authorization.

identifier-type	Item on which authorization is based. Valid keywords are: • **authenticated-domain**—Authenticated domain name. • **authenticated-username**—Authenticated username. • **auto-detect**—Authorization is performed on the basis of circuit-ID or remote-ID, depending on which identifier is provided by the edge device. • **circuit-id**—Circuit ID. • **dnis**—Dialed Number Identification Service number (also referred to as the called-party number). • **mac-address**—MAC address. • **nas-port**—Network access server (NAS) port identifier. • **remote-id**—Remote ID. • **source-ip-address**—Source IP address. • **tunnel-name**—Virtual Private Dialup Network (VPDN) tunnel name. • **unauthenticated-domain**—Unauthenticated domain name. • **unauthenticated-username**—Unauthenticated username. • **vendor-class-id** *name*—Vendor class ID.
plus	(Optional) Separates identifiers if more than one is used for authorization. The circuit ID, remote ID, MAC address, and vendor class ID can be used in any combination.

Command Default

The control policy will not initiate authorization.

Command Modes

Control policy-map class configuration (config-control-policymap-class-control)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRD	The **vendor-class-id** keyword was added.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

The **authorize identifier** command configures an action in a control policy map. A control policy map is used to configure an ISG control policy, which defines the actions the system takes in response to specified events and conditions.

For sessions triggered by an unrecognized IP address, the MAC address should be used only when the subscriber is one hop away.

The **auto-detect** keyword allows authorization to be performed on Cisco Catalyst switches with remote-ID:circuit-ID and on DSL Forum switches with circuit-ID only.

Note that if you specify the default method list, the default list will not appear in the output of the **show running-config** command. For example, if you configure the following command:

```
Router(config-control-policymap-class-control)# 1 authorize aaa list default password ABC
identifier nas-port
```

the following will display in the output for the **show running-config** command:

```
1 authorize aaa password ABC identifier nas-port
```

Named method lists will display in the **show running-config** command output.

When ISG automatic subscriber login is configured using the **authorize identifier** command, the ISG uses specified identifiers in place of the username in authorization requests, enabling a user profile to be downloaded from a AAA server as soon as packets are received from a subscriber.

Examples

In the following example, ISG is configured to send a request for authorization on the basis of the source IP address. The system will perform this action at session start when the conditions that are defined in control class "CONDA" are met.

```
policy-map type control RULEA
 class type control CONDA event session-start
  1 authorize aaa list TAL_LIST password cisco identifier source-ip-address
  2 service-policy type service aaa list LOCAL service redirectprofile
```

Related Commands

Command	Description
class type control	Specifies a control class for which actions may be configured in an ISG control policy map.
policy-map type control	Creates or modifies a control policy map, which defines an ISG control policy.

auth-type (ISG)

To specify the type of authorization Intelligent Services Gateway (ISG) will use for RADIUS clients, use the **auth-type** command in dynamic authorization local server configuration mode. To return to the default authorization type, use the **no** form of this command.

auth-type {**all** | **any** | **session-key**}

no auth-type

Syntax Description

all	All attributes must match for authorization to be successful. This is the default.
any	Any attribute must match for authorization to be successful.
session-key	The session-key attribute must match for authorization to be successful. **Note** The only exception is if the session-id attribute is provided in the RADIUS Packet of Disconnect (POD) request, then the session ID is valid.

Command Default

All attributes must match for authorization to be successful.

Command Modes

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

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

An ISG can be configured to allow external policy servers to dynamically send policies to the ISG. This functionality 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. Use the **auth-type** command to specify the type of authorization ISG will use for RADIUS clients.

Examples

The following example configures the ISG authorization type:

```
aaa server radius dynamic-author
 client 10.0.0.1
 auth-type any
```

Related Commands

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

available

To create a condition in an Intelligent Services Gateway (ISG) control policy that will evaluate true if the specified subscriber identifier is locally available, use the **available** command in control class-map configuration mode. To remove this condition, use the **no** form of this command.

available {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}

no available {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}

Syntax Description

authen-status	Subscriber authentication status.
authenticated-domain	Authenticated domain name.
authenticated-username	Authenticated username.
dnis	Dialed Number Identification Service number (called-party number).
media	Subscriber access media type.
mlp-negotiated	Identifier indicating that the session was established using multilink PPP negotiation.
nas-port	NAS port identifier.
no-username	Identifier indicating that the username is not available.
protocol	Subscriber access protocol type.
service-name	Service name currently associated with user.
source-ip-address	Source IP address.
timer	Policy timer name.
tunnel-name	Virtual Private Dial-Up Network (VPDN) tunnel name.
unauthenticated-domain	Unauthenticated domain name.
unauthenticated-username	Unauthenticated username.

Command Default

A condition that will evaluate true if the specified subscriber identifier is locally available is not created.

Command Modes

Control class-map configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

The **available** command is used to configure a condition within a control class map. A control class map, which is configured with the **class-map type control** command, specifies conditions that must be met for a control policy to be activated, and, optionally, the event that causes the class to be evaluated. A

control class map can contain multiple conditions, each of which will evaluate to either true or false. Match directives can be used to specify whether all, any, or none of the conditions must evaluate true in order for the class as whole to evaluate true.

The **class type control** command is used to associate a control class map with a policy control map.

Examples

The following example shows a control class map called "class3" configured with three conditions. The **match-all** keyword indicates that all of the conditions must evaluate true before the class evaluates true. The **class type control** command associates "class3" with the control policy map called "rule4".

```
class-map type control match-all class3
  match access-type pppoe
  match domain cisco.com
  available nas-port-id
!
policy-map type control rule4
  class type control class3
   authorize nas-port-id
!
```

Related Commands

Command	Description
class-map type control	Creates or modifies an ISG control class map.
class type control	Specifies a control class for which actions may be configured in an ISG control policy map.
policy-map type control	Create or modifies a control policy map, which defines an ISG control policy.

calling-station-id format

To specify the format of the Calling-Station-ID in attribute 31, use the **calling-station-id format** command in RADIUS proxy server configuration mode or RADIUS proxy client configuration mode. To return to the default format, use the **no** form of this command.

calling-station-id format {**mac-address** | **msisdn**}

no calling-station-id format {**mac-address** | **msisdn**}

Syntax Description

mac-address	Specifies the MAC address in attribute 31.
msisdn	Specifies the Mobile Subscriber Integrated Services Digital Network Number (MSISDN) in attribute 31.

Command Default

The default format is MAC address.

Command Modes

RADIUS proxy server configuration (config-locsvr-proxy-radius)
RADIUS proxy client configuration (config-locsvr-radius-client)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

Use the **calling-station-id format** command to differentiate and identify the session based on the downstream device type and receive the values in attribute 31. For example, if the downstream device type is Public Wireless LAN (PWLAN), then the Intelligent Services Gateway (ISG) RADIUS proxy identifies the value in attribute 31 as MAC address and MSISDN for the Gateway GPRS Support Node (GGSN) device type.

Examples

The following example shows how to configure ISG to specify MSISDN as the calling station ID for a RADIUS proxy server:

```
Router(config)# aaa new-model
Router(config)# aaa server radius proxy
Router(config-locsvr-proxy-radius)# calling-station-id format msisdn
```

Related Commands

Command	Description
aaa server radius proxy	Enables ISG RADIUS proxy configuration mode, in which ISG RADIUS proxy parameters can be configured.
client (ISG RADIUS proxy)	Enters ISG RADIUS proxy client configuration mode, in which client-specific RADIUS proxy parameters can be specified.
session-identifier	Correlates RADIUS server requests and identifies a session in the ISG RADIUS proxy.

class type control

To specify a control class for which actions may be configured in an Intelligent Services Gateway (ISG) control policy, use the **class type control** command in control policy-map configuration mode. To remove the control class from the control policy map, use the **no** form of this command.

class type control {*control-class-name* | **always**} [**event** {**access-reject** | **account-logoff** | **account-logon** | **acct-notification** | **credit-exhausted** | **dummy-event** | **quota-depleted** | **radius-timeout** | **service-failed** | **service-start** | **service-stop** | **session-default-service** | **session-restart** | **session-service-found** | **session-start** | **timed-policy-expiry**}]

no class type control {*control-class-name* | **always**} [**event** {**access-reject** | **account-logoff** | **account-logon** | **acct-notification** | **credit-exhausted** | **dummy-event** | **quota-depleted** | **radius-timeout** | **service-failed** | **service-start** | **service-stop** | **session-default-service** | **session-restart** | **session-service-found** | **session-start** | **timed-policy-expiry**}]

Syntax Description

control-class-name	Name of the control class map.
always	Creates a control class that always evaluates true.
event	Causes the control class to be evaluated upon occurrence of a specific event.
access-reject	Event that fails the RADIUS authentication.
account-logoff	Event that occurs upon account logout.
account-logon	Event that occurs upon account login.
acct-notification	Event that occurs upon accounting notification.
credit-exhausted	Event that occurs when the prepaid billing server returns a quota of zero and a prepaid idle timeout greater than zero.
dummy-event	Event that tests suspendable actions.
quota-depleted	Event that occurs when the allocated quota has been used up.
radius-timeout	Event that times out the RADIUS during authentication.
service-failed	Event that occurs when a service fails.
service-start	Event that occurs upon receipt of a request to start a service.
service-stop	Event that occurs upon receipt of a request to stop a service.
session-default-service	Event that occurs when ISG has provided a default service.
session-restart	Event that occurs upon a session restart following the recovery of a Dynamic Host Configuration Protocol (DHCP)-initiated IP session.
session-service-found	Event that occurs when a network policy has been determined for the session.
session-start	Event that occurs upon session start.
timed-policy-expiry	Event that occurs when a timed policy expires.

Command Default

A control class is not specified in a control policy map.

Command Modes

Control policy-map configuration (config-control-policymap)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SB2	This command was modified. The **session-restart** keyword was added.
12.2(33)SRC	This command was modified. The **acct-notification** keyword was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.
12.2(33)SRE	This command was modified. The **access-reject** and **radius-timeout** keywords were added.
Cisco IOS XE Release 2.5	This command was modified. The **access-reject** and **radius-timeout** keywords were added.

Usage Guidelines

A control class map defines the conditions that must be met and events that must occur before a set of actions will be executed. Use the **class type control** command to associate a control class map with one or more actions in a control policy map. The association of a control class and a set of actions is called a *control policy rule*.

Using the **class type control** command with the **always** keyword creates a control policy rule that will always be treated as the lowest-priority rule in a control policy map.

To create a named control class map, use the **class-map type control** command.

The **session-restart** keyword applies to DHCP-initiated IP sessions only.

Using the **class type control** command with the **acct-notification** keyword causes the control class to be evaluated upon occurrence of an accounting notification.

Examples

The following example shows the configuration of a class map called “class3”. The **class type control** command adds “class3” to the control policy map “policy1”. When “class3” evaluates true, the action associated with the class will be executed.

```
class-map type control match-all class3
  match access-type pppoe
  match domain cisco.com
  available nas-port-id
!
policy-map type control policy1
  class type control class3
   authorize nas-port-id
!
service-policy type control rule4
```

Related Commands

Command	Description
class-map type control	Creates an ISG control class map.
policy-map type control	Creates or modifies a control policy map, which defines an ISG control policy.
service-policy type control	Applies a control policy to a context.

class type traffic

To specify the Intelligent Services Gateway (ISG) traffic class whose policy you want to create or change or to specify the default traffic class in order to configure its policy, use the **class type traffic** command in service policy-map configuration mode. To remove a class from the service policy map, use the **no** form of this command.

[*priority*] **class type traffic** {*class-map-name* | **default** {**in-out | input | output**}}

no [*priority*] **class type traffic** {*class-map-name* | **default** {**in-out | input | output**}}

Syntax Description

priority	(Optional) Specifies the relative priority of the traffic class. Traffic class priority determines the order in which traffic policies are applied to a session. Range is 1 to 1000, where 1 is the highest priority and 1000 is the lowest. Default is 0 (undefined).
class-map-name	Name of a previously configured traffic class map.
default	Specifies the default traffic class. Applied only if other configured classes do not match the traffic.
in-out	Specifies the default traffic class for input and output traffic.
input	Specifies the default traffic class for input traffic.
output	Specifies the default traffic class for output traffic.

Command Default

A traffic class is not specified.

Command Modes

Service policy-map configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Before you can specify a named traffic class map in a service policy map, the traffic class map must be configured using the **class-map type traffic** command.

The priority of a traffic class determines which class will be used first for a specified match in cases where more than one traffic policy has been activated for a single session. In other words, if a packet matches more than one traffic class, it will be classified to the class with the higher priority. The priority should be specified if packets must match a traffic class based on the order of the service policy.

The default traffic class map is applied if none of the other configured classes matches the traffic. At least one other traffic class must be configured. The default traffic class map is not applied if there are no other traffic classes configured. It cannot be assigned a priority because by default it is the lowest priority class. The default policy of the default traffic class is to pass traffic. You can also configure the default traffic class to drop traffic.

Examples

The following example shows the configuration of the traffic class “UNAUTHORIZED_TRAFFIC”:

```
class-map type traffic UNAUTHORIZED_TRAFFIC
 match access-group input 100

policy-map type service UNAUTHORIZED_REDIRECT_SVC
 class type traffic UNAUTHORIZED_TRAFFIC
  redirect to ip 10.0.0.148 port 8080
```

The following example shows the configuration of the default traffic class:

```
policy-map type service SERVICE1
 class type traffic CLASS1
  prepaid-config PREPAID
 class type traffic default in-out
  drop
```

Related Commands

Command	Description
class-map type traffic	Creates or modifies a traffic class map, which is used for matching packets to a specified ISG traffic class
policy-map type service	Creates or modifies a service policy map, which is used to define an ISG subscriber service.
show class-map type traffic	Displays traffic class maps and their matching criteria.

class-map type control

To create an Intelligent Services Gateway (ISG) control class map, which defines the conditions under which the actions of a control policy map will be executed, use the **class-map type control** command in global configuration mode. To remove a control class map, use the **no** form of this command.

class-map type control [**match-all** | **match-any** | **match-none**] *class-map-name*

no class-map type control [**match-all** | **match-any** | **match-none**] *class-map-name*

Syntax Description

match-all	(Optional) The class map evaluates true if all of the conditions in the class map evaluates true.
match-any	(Optional) The class map evaluates true if any of the conditions in the class map evaluates true.
match-none	(Optional) The class map evaluates true if none of the conditions in the class map evaluates true.
class-map-name	Name of the class map.

Command Default

A control class map is not created.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

A control class map specifies conditions that must be met for a control policy to be activated, and, optionally, the event that causes the class to be evaluated. A control class map can contain multiple conditions, each of which will evaluate to either true or false. Use the **match-any**, **match-all**, and **match-none** keywords to specify which, if any, conditions must evaluate true before the control policy will be executed.

A control policy map, which is configured with the **policy-map type control** command, contains one or more control policy rules. A control policy rule associates a control class map with one or more actions. Use the **class type control** command to associate a control class map with a control policy map.

Examples

The following example shows how to configure a control policy in which virtual private dial-up network (VPDN) forwarding is applied to anyone dialing in from “xyz.com”:

```
class-map type control match-all MY-FORWARDED-USERS
 match unauthenticated-domain "xyz.com"
!
policy-map type control MY-POLICY
 class type control MY-FORWARDED-USERS event session-start
  1 apply identifier nas-port
  2 service local
```

```
!
interface Dialer1
 service-policy type control MY-POLICY
```

Related Commands

Command	Description
class type control	Specifies a control class for which actions may be configured in an ISG control policy map.
policy-map type control	Creates or modifies a control policy map, which defines an ISG control policy.

class-map type traffic

To create or modify a traffic class map, which is used for matching packets to a specified Intelligent Services Gateway (ISG) traffic class, use the **class-map type traffic** command in global configuration mode. To remove a traffic class map, use the **no** form of this command.

class-map type traffic match-any *class-map-name*

no class-map type traffic match-any *class-map-name*

Syntax Description

match-any	Indicates that packets must meet one of the match criteria in order to be considered a member of the class.
class-map-name	Name of the class map.

Command Default

A traffic class map is not created.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Use the **class-map type traffic** command to specify the name of the ISG traffic class for which you want to create or modify traffic class map match criteria. Use of the **class-map type traffic** command enables traffic class-map configuration mode, in which you can enter match commands to configure the match criteria for this class. Packets are checked against the match criteria configured for a class map to determine if the packet belongs to that traffic class.

ISG traffic classes allow subscriber session traffic to be subclassified so that ISG features can be applied to constituent flows. Traffic policies, which define the handling of data packets, contain a traffic class and one or more features.

Once a traffic class map has been defined, use the **class type traffic** command to associate the traffic class map with a service policy map. A service can contain one traffic class, and the default class.

Examples

The following example shows the configuration of a traffic class map called “CLASS-ACL-101”. The class map is defined so that input traffic matching access list 101 will match the class. The traffic class map is then referenced in service policy map “mp3”.

```
class-map type traffic CLASS-ACL-101
 match access-group input 101
!
policy-map type service mp3
 class type traffic CLASS-ACL-101
  authentication method-list cp-mlist
  accounting method-list cp-mlist
  prepaid conf-prepaid
```

Related Commands

Command	Description
class type traffic	Specifies a named traffic class whose policy you want to create or change or specifies the default traffic class in order to configure its policy.
match access-group (ISG)	Configures the match criteria for a class map on the basis of the specified access control list (ACL).

classname

To associate a Dynamic Host Configuration Protocol (DHCP) pool or remote DHCP server with an Intelligent Services Gateway (ISG) service policy map, use the **classname** command in service policy-map configuration mode. To remove this association, use the **no** form of this command.

classname *class-name*

no classname *class-name*

Syntax Description

class-name	Class name associated with a DHCP pool or remote server.

Command Default

An ISG service is not associated with a DHCP pool.

Command Modes

Service policy-map configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

ISG can influence the IP address pool and the DHCP server that are used to assign subscriber IP addresses. To enable ISG to influence the IP addresses assigned to subscribers, you associate a DHCP address pool class with an address domain. The DHCP address pool class must also be configured in a service policy map, service profile, or user profile, which is associated with a subscriber. When a DHCP request is received from a subscriber, DHCP uses the address pool class that is associated with the subscriber to determine which DHCP address pool should be used to service the request. As a result, on a per-request basis, an IP address is provided by the local DHCP server or relayed to a remote DHCP server that is defined in the selected pool.

Examples

In the following example, the DHCP class “blue” is specified in the service “my_service”. When “my_service” is activated, the local DHCP component will provide a new IP address from the pool “blue-pool” because (a) the classes match and (b) the subnet defined in “relay source” corresponds to one of the subnets defined at the interface. Hence the DHCP DISCOVER packet is relayed to the server at address 10.10.2.1, and the local DHCP component acts as a relay.

```
ip dhcp pool blue-pool
 relay source 10.1.0.0 255.255.0.0
 class blue
  relay destination 10.10.2.1 vrf blue

policy-map type service my_service
 classname blue
```

Related Commands

Command	Description
policy-map type service	Creates or modifies a service policy map, which is used to define an ISG service.

clear class-map control

To clear the Intelligent Services Gateway (ISG) control class map counters, use the **clear class-map control** command in privileged EXEC mode.

clear class-map control

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Examples

The following example shows how to clear the control class map counters:

```
Router# clear class-map control
```

Related Commands

Command	Description
class-map type control	Creates an ISG control class map.
class type control	Specifies a control class for which actions may be configured in an ISG control policy map.
show class-map type control	Displays information about ISG control class maps.

clear ip subscriber

To disconnect and remove all or specified Intelligent Services Gateway (ISG) IP subscriber sessions, use the **clear ip subscriber** command in privileged EXEC mode.

clear ip subscriber [**interface** *interface-name* | **mac** *mac-address* | **slot** *slot-number* **no-hardware** | [**vrf** *vrf-name*] [**dangling** *seconds* | **ip** *ip-address* | **statistics**]]

Syntax Description

interface *interface-name*	(Optional) Clears IP subscriber sessions associated with the specified interface on the Cisco 7600 series router.
mac *mac-address*	(Optional) Clears IP subscriber sessions that have the specified MAC address.
slot *slot-number* **no-hardware**	(Optional) Clears IP subscriber sessions associated with the specified slot from which a line card is removed on the Cisco 7600 series router.
vrf *vrf-name*	(Optional) Clears IP subscriber sessions associated with the specified virtual routing and forwarding (VRF) instance.
dangling *seconds*	(Optional) Clears IP subscriber sessions that have remained unestablished for the specified number of seconds. Range: 1 to 3600.
ip *ip-address*	(Optional) Clears IP subscriber sessions that have the specified IP address.
statistics	(Optional) Clears statistics for IP subscriber sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	Support was added for this command on Cisco 7600 series routers.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.
12.2(33)SRE1	This command was modified. The **statistics** keyword was added.

Usage Guidelines

A session that has not been fully established within a specified period of time is referred to as a dangling session. The **clear ip subscriber** command can be used with the **dangling** keyword to disconnect and remove dangling sessions. The *seconds* argument allows you to specify how long the session has to remain unestablished before it is considered dangling.

Session Removal: Cisco 7600 Series Routers Only

This command removes only IP sessions (MAC or IP), not IP interface sessions.

The **interface** and **slot no-hardware** keywords are available only on Cisco 7600 series routers.

Examples

The following example shows how to clear all dangling sessions that are associated with vrf1:

```
Router# clear ip subscriber vrf vrf1 dangling 10
```

Examples for Cisco 7600 Series Routers Only

The following example shows how to clear sessions that are associated with Gigabit Ethernet interface 0/1 on a Cisco 7600 series router:

```
Router# clear ip subscriber interface GigabitEthernet 0/1
```

The following example shows how to clear sessions that are associated with a line card that was removed from slot 1 on a Cisco 7600 series router:

```
Router# clear ip subscriber slot 1 no-hardware
```

Related Commands

Command	Description
show ip subscriber	Displays information about ISG IP subscriber sessions.

clear radius-proxy client

To clear all Intelligent Services Gateway (ISG) RADIUS proxy sessions for a specific client, use the **clear radius-proxy client** command in privileged EXEC mode.

clear radius-proxy client *ip-address* [**vrf** *vrf-name*]

Syntax Description

ip-address	IP address of the client device.
vrf *vrf-name*	(Optional) Virtual routing and forwarding instance (VRF) associated with the client. **Note** The **vrf** *vrf-name* option is not supported in Cisco IOS Release 12.2(31)SB2.

Command Modes

Privileged EXEC

Command History

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

Examples

The following example clears all sessions associated with the RADIUS proxy client that has the IP address 10.10.10.10 and associated is with the VRF “blue”:

```
clear radius-proxy client 10.10.10.10 vrf blue
```

Related Commands

Command	Description
clear radius-proxy session	Clears specified ISG RADIUS proxy sessions.

clear radius-proxy session

To clear specific Intelligent Services Gateway (ISG) RADIUS proxy sessions, use the **clear radius-proxy session** command in privileged EXEC mode.

clear radius-proxy session {**id** *radius-proxy-ID* | **ip** *ip-address* [**vrf** *vrf-name*]}

Syntax Description

id *radius-proxy-ID*	ISG RADIUS proxy ID.
ip *ip-address*	IP address associated with the RADIUS proxy session.
vrf *vrf-name*	(Optional) Virtual routing and forwarding instance (VRF) associated with the session. **Note** The **vrf** *vrf-name* option is not supported in Cisco IOS Release 12.2(31)SB2.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The RADIUS proxy session ID can be identified in the output of the **show radius-proxy client** command.

Examples

The following example shows how to identify the RADIUS proxy session ID by using the **show radius-proxy client** command:

```
show radius-proxy client 10.45.45.3

Configuration details for client 10.45.45.3
 Shared secret:     radprxykey           Msg Auth Ignore:   No
 Local auth port:   1111                 Local acct port:   1646
 Acct method list: FWDACCT
Session Summary:
      RP ID       IP Address
   1. 1694498816  unassigned ----> 1694498816 is the session id
```

The following example clears the ISG RADIUS proxy session with the ID 1694498816:

```
clear radius-proxy session id 1694498816
```

Related Commands

Command	Description
clear radius-proxy client	Clears all ISG RADIUS proxy sessions for a specific client.
show radius-proxy client	Displays information about ISG RADIUS proxy client devices.

clear subscriber policy dpm statistics

To clear the statistics for DHCP policy module (DPM) session contexts, use the **clear subscriber policy dpm statistics** command in privileged EXEC mode.

clear subscriber policy dpm statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SB9	This command was introduced.

Usage Guidelines

The **clear subscriber policy dpm statistics** command resets all DPM event trace counters to zero. To display the cumulative statistics for DPM session contexts, use the **show subscriber policy dpm statistics** command.

Examples

The following example shows how to clear DPM event trace statistics:

```
Router# clear subscriber policy dpm statistics
```

Related Commands

Command	Description
show subscriber policy dpm context	Displays event traces for DPM session contexts.
show subscriber policy dpm statistics	Displays statistics for DPM event traces.

clear subscriber policy peer

To clear the display of the details of a subscriber policy peer connection, use the **clear subscriber policy peer** command in privileged EXEC mode.

clear subscriber policy peer {**address** *ip-address* | **handle** *connection-handle-id* | **session** | **all**}

Syntax Description

address	Clears the display of a specific peer connection, identified by its IP address.
ip-address	IP address of the peer connection to be cleared.
handle	Clears the display of a specific peer connection, identified by its handle.
connection-handle-id	Handle ID for the peer connection handle.
session	Clears the display of sessions with the given peer.
all	Clears the display of all peer connections.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB

Usage Guidelines

The **clear subscriber policy peer** command ends the peering relationship between the Intelligent Services Gateway (ISG) device and selected Service Control Engine (SCE) devices. However, the SCE will attempt to reconnect with the ISG device after a configured amount of time. The **clear subscriber policy peer** command can remove select session associations from a particular SCE device.

Examples

The following example shows how the **clear subscriber policy peer** command is used at the router prompt to clear the display of all details of the subscriber policy peer connection.

```
Router# clear subscriber policy peer all
```

Related Commands

Command	Description
show subscriber-policy peer	Displays the details of a subscriber policy peer.
subscriber-policy	Defines or modifies the forward and filter decisions of the subscriber policy.

clear subscriber policy peer session

To clear the display of the details of a subscriber policy peer session, use the **clear subscriber policy peer session** command in privileged EXEC mode.

clear subscriber policy peer session {**guid** *guid-value* | **all**} [**address** *ip-address* | **handle** *connection-handle-id* | **all**]

Syntax Description

guid	Clears the display of a specific policy peer session, identified by a globally unique identifier.
guid-value	Globally unique identifier of the peer session to be cleared.
all	Clears the display of all peer sessions.
address	Clears the display of a specific peer session, identified by its IP address.
ip-address	IP address of the peer session to be cleared.
handle	Clears the display of a specific peer session, identified by its handle.
connection-handle-id	Handle ID for the peer session handle.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **clear subscriber policy peer session** command ends the peering relationship between the Intelligent Services Gateway (ISG) device and selected Service Control Engine (SCE) devices. However, the SCE will attempt to reconnect with the ISG device after a configured amount of time. The **clear subscriber policy peer session** command can remove select session associations from a particular SCE.

Examples

The following example shows how the **clear subscriber policy peer session** command is used at the router prompt to clear the display of all the details of a subscriber policy peer session.

```
Router# clear subscriber policy peer session all
```

Related Commands

Command	Description
clear subscriber-policy peer	Displays the details of a subscriber policy peer.
show subscriber-policy peer	Displays the details of a subscriber policy peer.
subscriber-policy	Defines or modifies the forward and filter decisions of the subscriber policy.

clear subscriber trace history

To clear the event trace history logs for Intelligent Services Gateway (ISG) subscriber sessions, use the **clear subscriber trace history** command in privileged EXEC mode.

clear subscriber trace history {**dpm** | **pm**}

Syntax Description

dpm	Clears DHCP policy module (DPM) trace history.
pm	Clears policy manager (PM) trace history.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SB9	This command was introduced.

Usage Guidelines

The **clear subscriber trace history** command deletes all event traces that are stored in the specified module's history log. This command also clears the current records counter and current log size counter for the **show subscriber trace statistics** command.

Examples

The following example shows how to clear the trace history for the DPM.

```
Router# clear subscriber trace history dpm
```

Related Commands

Command	Description
show subscriber trace history	Displays the event traces for ISG subscriber sessions that are saved in the trace history log.
show subscriber trace statistics	Displays statistics about the event traces for ISG subscriber sessions that were saved to the history log.
subscriber trace event	Enables event tracing for software modules involved in ISG subscriber sessions.
subscriber trace history	Enables saving the event traces for ISG subscriber sessions to the history log.

client

To specify a RADIUS client from which a device will accept Change of Authorization (CoA) and disconnect requests, use the **client** command in dynamic authorization local server configuration mode. To remove this specification, use the **no** form of this command.

client {*name* | *ip-address*} [**key** [**0** | **7**] *word*] [**vrf** *vrf-id*]

no client {*name* | *ip-address*} [**key** [**0** | **7**] *word*] [**vrf** *vrf-id*]

Syntax Description

name	Hostname of the RADIUS client.
ip-address	IP address of the RADIUS client.
key	(Optional) Configures the RADIUS key to be shared between a device and a RADIUS client.
0	(Optional) Specifies that an unencrypted key will follow.
7	(Optional) Specifies that a hidden key will follow.
word	(Optional) Unencrypted server key.
vrf *vrf-id*	(Optional) Virtual Routing and Forwarding (VRF) ID of the client.

Command Default

CoA and disconnect requests are dropped.

Command Modes

Dynamic authorization local server configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

A device (such as a router) can be configured to allow an external policy server to dynamically send updates to the router. This functionality is facilitated by the CoA RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling a router and external policy server each to act as a RADIUS client and server. Use the **client** command to specify the RADIUS clients for which the router will act as server.

Examples

The following example configures the router to accept requests from the RADIUS client at IP address 10.0.0.1:

```
aaa server radius dynamic-author
 client 10.0.0.1 key cisco
```

Related Commands

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

client (ISG RADIUS proxy)

To enter RADIUS proxy client configuration mode, in which client-specific RADIUS proxy parameters can be specified, use the **client** command in RADIUS proxy server configuration mode. To remove the RADIUS proxy client and configuration, use the **no** form of this command.

client {*ip-address* | *hostname*} [*subnet-mask*] [**vrf** *vrf-name*]

no client {*ip-address* | *hostname*} [*subnet-mask*] [**vrf** *vrf-name*]

Syntax Description

ip-address	IP address of the RADIUS proxy client.
hostname	Hostname of the RADIUS proxy client.
subnet-mask	(Optional) Subnet in which client resides.
vrf *vrf-name*	(Optional) Virtual routing and forwarding instance (VRF) associated with the session. **Note** The **vrf** *vrf-name* option is not supported in Cisco IOS Release 12.2(31)SB2.

Command Default

The global RADIUS proxy server configuration is used.

Command Modes

RADIUS proxy server configuration

Command History

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

Usage Guidelines

Use the **client** command in RADIUS proxy server configuration mode to specify a client for which RADIUS proxy parameters can be configured. Client-specific RADIUS proxy configurations take precedence over the global RADIUS proxy server configuration.

In cases where Intelligent Services Gateway (ISG) is acting as a proxy for more than one client device, all of which reside on the same subnet, client-specific parameters may be configured using a subnet definition rather than a discrete IP address for each device. This configuration method results in the sharing of a single configuration by all the client devices on the subnet. ISG is able to differentiate traffic from these devices based on the source and NAS IP address of RADIUS packets. To configure a client subnet, use the **client** command with the *subnet-mask* argument.

Examples

The following example shows the configuration of global RADIUS proxy parameters and client-specific parameters for two RADIUS proxy clients. Client 10.1.1.1 is configured to listen for accounting packets on port 1813 and authentication packets on port 1812. Because a shared secret is not configured specifically for client 10.1.1.1, it will inherit the shared secret specification, which is “cisco”, from the global RADIUS proxy configuration. Client 10.2.2.2 will use “systems” as the shared secret and will use the default ports for listening for accounting and authentication packets.

```
aaa server radius proxy
 key cisco
 client 10.1.1.1
  accounting port 1813
  authentication port 1812
!
 client 10.2.2.2
  key systems
!
```

Related Commands

Command	Description
aaa server radius proxy	Enables ISG RADIUS proxy configuration mode, in which ISG RADIUS proxy parameters can be configured.

collect identifier

To enable a control policy map to collect subscriber identifiers, use the **collect identifier** command in control policy-map class configuration mode. To disable a control policy from collecting subscriber identifiers, use the **no** form of this command.

action-number **collect** [**aaa list** *list-name*] **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **mac-address** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}

no *action-number* **collect** [**aaa list** *list-name*] **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.
aaa	(Optional) Specifies that authentication will be performed using an authentication, authorization, and accounting (AAA) method list.
list *list-name*	(Optional) Specifies the AAA method list to which the authentication request will be sent.
authen-status	Specifies the subscriber authentication status.
authenticated-domain	Specifies the authenticated domain name.
authenticated-username	Specifies the authenticated username.
dnis	Specifies the Dialed Number Identification Service (DNIS) number (also referred to as the called-party number).
media	Specifies the subscriber access media type.
mac-address	Specifies the MAC address to be used as an identity for Layer 3 IP sessions.
mlp-negotiated	Specifies the value indicating that the subscriber session was established using multilink PPP negotiation.
nas-port	Specifies the network access server (NAS) port identifier.
no-username	Specifies that the username is not available.
protocol	Specifies the subscriber access protocol type.
service-name	Specifies the service name currently associated with the user.
source-ip-address	Specifies the source IP address.
timer	Specifies the timer name.
tunnel-name	Specifies the Virtual Private Dialup Network (VPDN) tunnel name.
unauthenticated-domain	Specifies the unauthenticated domain name.
unauthenticated-username	Specifies the unauthenticated username.

Command Default

Control policies do not collect subscriber identifiers.

Command Modes

Control policy-map class configuration (config-control-policymap-class-control)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE. The **mac-address** keyword was added.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The **collect identifier** command configures an action in a control policy map.

Control policies define the actions the system will take in response to specified events and conditions. A control policy map is used to configure an Intelligent Services Gateway (ISG) control policy. A control policy is made of one or more control policy rules. A control policy rule is an association of a control class and one or more actions. The control class defines the conditions that must be met before the actions will be executed. The actions are numbered and executed sequentially within the policy rule.

Note that if you specify the default method list, the default list will not appear in the output of the **show running-config** command. For example, if you configure the following command:

```
Router(config-control-policymap-class-control)# 1 collect aaa list default
```

The following will display in the output for the **show running-config** command:

```
1 collect
```

Named method lists will display in the **show running-config** command output.

Examples

The following example shows how to configure ISG to collect a subscriber's authentication status at session start:

```
Router(config)# policy-map type control policy1
Router(config-control-policymap)# class type control always event session-start
Router(config-control-policymap-class-control)# 1 collect identifier authen-status
```

Related Commands

Command	Description
class type control	Specifies a control class for which actions may be configured in an ISG control policy map.
policy-map type control	Creates or modifies a control policy map, which defines an ISG control policy.

debug ip subscriber

To enable Intelligent Services Gateway (ISG) IP subscriber session debugging, use the **debug ip subscriber** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug ip subscriber {**all** | **error** | **event** | **fsm** | **packet**}

no debug ip subscriber {**all** | **error** | **event** | **fsm** | **packet**}

Syntax Description

all	Displays all debugging messages related to IP subscriber sessions.
error	Displays debugging messages about IP subscriber session errors.
event	Displays debugging messages about IP subscriber session events.
fsm	Displays debugging messages related to session state changes for IP subscriber sessions.
packet	Displays debugging messages related to IP subscriber session packets.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Examples

The following example show sample output for the **debug ip subscriber** command:

```
Router# debug ip subscriber packet

Packet debugs:

1d07h: IPSUB_DP: [Et0/0:I:CEF:0000.0000.0002] Rx driver forwarded packet via les, return
code = 0
1d07h: IPSUB_DP: [Et0/0:I:PROC:0000.0000.0002] Packet classified, results = 0x18
1d07h: IPSUB_DP: [ms1:I:PROC:0000.0000.0002] Rx driver forwarded the packet
1d07h: IPSUB_DP: [ms1:I:PROC:0000.0000.0002] Packet classified, results = 0x42
1d07h: IPSUB_DP: [ms1:O:PROC:RED:50.0.0.3] Packet classified, results = 0x14
Router#
1d07h: IPSUB_DP: [ms1:O:PROC:RED:50.0.0.3] Subscriber features executed, return code = 0
1d07h: IPSUB_DP: [ms1:O:PROC:RED:50.0.0.3] Tx driver forwarding the packet
1d07h: IPSUB_DP: [Et0/0:O:PROC:RED:50.0.0.3] Packet classified, results = 0x14
```

Related Commands

Command	Description
show ip subscriber	Displays information about ISG IP subscriber sessions.

debug radius-proxy

To display debugging messages for Intelligent Services Gateway (ISG) RADIUS proxy functionality, use the **debug radius-proxy** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug radius-proxy {**events** | **errors**}

no debug radius-proxy {**events** | **errors**}

Syntax Description

events	Displays debug messages related to ISG RADIUS proxy events.
errors	Displays debug messages related to ISG RADIUS proxy errors.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

See the following caution before using **debug** commands.

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, only use **debug** commands to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands during periods of lower network flows and fewer users.

Examples

The following example shows output for the **debug radius-proxy** command with the **events** keyword:

```
Router# debug radius-proxy events

*Nov  7 07:53:11.411: RP-EVENT: Parse Request: Username = 12345679@cisco
*Nov  7 07:53:11.411: RP-EVENT: Parse Request: Caller ID = 12345679@cisco
*Nov  7 07:53:11.411: RP-EVENT: Parse Request: NAS id = localhost
*Nov  7 07:53:11.411: RP-EVENT: Found matching context for user Caller ID:12345679@cisco
Name:aa
*Nov  7 07:53:11.411: RP-EVENT: Received event client Access-Request in state activated
*Nov  7 07:53:11.411: RP-EVENT: User Caller ID:12345679@cisco  Name:12 re-authenticating
*Nov  7 07:53:11.411: RP-EVENT: Forwarding Request to method list (handle=1979711512)
*Nov  7 07:53:11.411: RP-EVENT: Sending request to server group EAP
*Nov  7 07:53:11.411: RP-EVENT: State changed activated --> wait for Access-Response
```

debug sgi

To debug Service Gateway Interface (SGI), use the **debug sgi** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sgi [**error** | **info** | **xml** | **gsi** | **isg-api** | **all**]

no debug sgi

Syntax Description

error	Enables debugging at the error level, where all internal error messages are displayed.
info	Enables debugging at the informational level, where processing and progress information is displayed.
xml	Enables debugging at Extensible Markup Language (XML) parsing level.
gsi	Enables debugging for the Generic Service Interface (GSI) module.
isg-api	Enables debugging for the SGI Policy Manager interface operations.
all	Enables all debugging options.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The xml keyword turns on debugging for the Cisco Networking Services (CNS) XML parser and provides additional XML parsing debugging for SGI.

Examples

The following example shows all debugging options enabled and shows the output that is received when a message is sent.

```
Router# debug sgi all


Router# show debug
SGI:
SGI All debugging is on
SGI Errors debugging is on
SGI XML debugging is on
SGI Informational debugging is on
SGI Generic Service Interface debugging is on
SGI ISG_API Events debugging is on
SGI ISG_API Errors debugging is on
Router#



Router#
```

```
*Jul 1 20:55:11.364: SGI: Session created, session Id 7
*Jul 1 20:55:11.372: sgi beep listen app beep[0x66245188]: frame_available: type=M
number=1 answer=-1 more=* size=1400

*Jul 1 20:55:11.372: sgi beep listen app beep[0x66245188]: Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
...
*Jul 1 20:55:11.372: sgi beep listen app beep[0x66245188]: frame_available: type=M
number=1 answer=-1 more=. size=111

*Jul 1 20:55:11.372: sgi beep listen app beep[0x66245188]: gitypes:policyGroup>

</objects>
</sgiops:insertPolicyObjectsRequest>
...
*Jul 1 20:55:11.372: SGI: GSI message received, msgid 1, session 7
*Jul 1 20:55:11.376: SGI: XML parsed successfully, request insertPolicyObjectsRequest,
msgid 1
*Jul 1 20:55:11.376: SGI: authentication request sent to AAA
*Jul 1 20:55:11.376: SGI: req = [0x67454088] authentication succeeded
*Jul 1 20:55:11.376: SGI: Processing insertPolicyObjectsRequest
*Jul 1 20:55:11.376: SGI: insertPolicyObjectsRequest processing policyGroup:VPDN1, type 1,
result: 0
*Jul 1 20:55:11.376: SGI: Processing insertPolicyObjectsResponse
*Jul 1 20:55:11.376: SGI: GSI message sent, msgid 1, session 7
*Jul 1 20:55:12.088: sgi beep listen app beep[0x66245188]: close confirmation: status=+ no
error origin=L scope=C
*Jul 1 20:55:12.088: SGI: Session terminating, session Id 7
Router#
```

Related Commands

Command	Description
sgi beep listener	Enables SGI.
show sgi	Displays information about current SGI sessions or statistics.
text sgi xml	Allows onboard testing of SGI XML files when an external client is not available.

debug ssm

To display diagnostic information about the Segment Switching Manager (SSM) for switched Layer 2 segments, use the **debug ssm** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug ssm {**cm errors** | **cm events** | **fhm errors** | **fhm events** | **sm errors** | **sm events** | **sm counters** | **xdr**}

no debug ssm {**cm errors** | **cm events** | **fhm errors** | **fhm events** | **sm errors** | **sm events** | **sm counters** | **xdr**}

Syntax Description

cm errors	Displays Connection Manager (CM) errors.
cm events	Displays CM events.
fhm errors	Displays Feature Handler Manager (FHM) errors.
fhm events	Displays FHM events.
sm errors	Displays Segment Handler Manager (SM) errors.
sm events	Displays SM events.
sm counters	Displays SM counters.
xdr	Displays external data representation (XDR) messages related to traffic sent across the backplane between Router Processors and line cards.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated to Cisco IOS Release 12.2(25)S.
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.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The SSM manages the data-plane component of the Layer 2 Virtual Private Network (L2VPN) configuration. The CM tracks the connection-level errors and events that occur on an xconnect. The SM tracks the per-segment events and errors on the xconnect.

Use the **debug ssm** command to troubleshoot problems in bringing up the data plane.

This command is generally used only by Cisco engineers for internal debugging of SSM processes.

Examples

The following example shows sample output for the **debug ssm xdr** command:

```
Router# debug ssm xdr
```

```
SSM xdr debugging is on

2w5d: SSM XDR: [4096] deallocate segment, len 16
2w5d: SSM XDR: [8193] deallocate segment, len 16
2w5d: %LINK-3-UPDOWN: Interface FastEthernet2/1, changed state to down
2w5d: %LINK-3-UPDOWN: Interface FastEthernet2/1, changed state to up
2w5d: SSM XDR: [4102] provision segment, switch 4101, len 106
2w5d: SSM XDR: [4102] update segment status, len 17
2w5d: SSM XDR: [8199] provision segment, switch 4101, len 206
2w5d: SSM XDR: [4102] update segment status, len 17
2w5d: %SYS-5-CONFIG_I: Configured from console by console
2w5d: %LINK-3-UPDOWN: Interface FastEthernet2/1, changed state to down
2w5d: SSM XDR: [4102] update segment status, len 17
2w5d: %LINK-3-UPDOWN: Interface FastEthernet2/1, changed state to up
2w5d: SSM XDR: [4102] deallocate segment, len 16
2w5d: SSM XDR: [8199] deallocate segment, len 16
2w5d: SSM XDR: [4104] provision segment, switch 4102, len 106
2w5d: SSM XDR: [4104] update segment status, len 17
2w5d: SSM XDR: [8201] provision segment, switch 4102, len 206
2w5d: SSM XDR: [4104] update segment status, len 17
2w5d: SSM XDR: [4104] update segment status, len 17
2w5d: %SYS-5-CONFIG_I: Configured from console by console
```

The following example shows the events that occur on the segment manager when an Any Transport over MPLS (AToM) virtual circuit (VC) configured for Ethernet over MPLS is shut down and then enabled:

```
Router# debug ssm sm events

SSM Connection Manager events debugging is on

Router(config)# interface fastethernet 0/1/0.1
Router(config-subif)# shutdown

09:13:38.159: SSM SM: [SSS:AToM:36928] event Unprovison segment
09:13:38.159: SSM SM: [SSS:Ethernet Vlan:4146] event Unbind segment
09:13:38.159: SSM SM: [SSS:AToM:36928] free segment class
09:13:38.159: SSM SM: [SSS:AToM:36928] free segment
09:13:38.159: SSM SM: [SSS:AToM:36928] event Free segment
09:13:38.159: SSM SM: last segment class freed
09:13:38.159: SSM SM: [SSS:Ethernet Vlan:4146] segment ready
09:13:38.159: SSM SM: [SSS:Ethernet Vlan:4146] event Found segment data

Router(config-subif)# no shutdown

09:13:45.815: SSM SM: [SSS:AToM:36929] event Provison segment
09:13:45.815: label_oce_get_label_bundle: flags 14 label 16
09:13:45.815: SSM SM: [SSS:AToM:36929] segment ready
09:13:45.815: SSM SM: [SSS:AToM:36929] event Found segment data
09:13:45.815: SSM SM: [SSS:AToM:36929] event Bind segment
09:13:45.815: SSM SM: [SSS:Ethernet Vlan:4146] event Bind segment
```

The following example shows the events that occur on the CM when an AToM VC configured for Ethernet over MPLS is shut down and then enabled:

```
Router(config)# interface fastethernet 0/1/0.1
Router(config-subif)# shutdown

09:17:20.179: SSM CM: [AToM] unprovision segment, id 36929
09:17:20.179: SSM CM: CM FSM: state Open - event Free segment
09:17:20.179: SSM CM: [SSS:AToM:36929] unprovision segment 1
09:17:20.179: SSM CM: [SSS:AToM] shQ request send unprovision complete event
09:17:20.179: SSM CM: [SSS:Ethernet Vlan:4146] unbind segment 2
09:17:20.179: SSM CM: [SSS:Ethernet Vlan] shQ request send ready event
```

```
09:17:20.179: SSM CM: SM msg event send unprovision complete event
09:17:20.179: SSM CM: SM msg event send ready event

Router(config-subif)# no shutdown

09:17:35.879: SSM CM: Query AToM to Ethernet Vlan switching, enabled
09:17:35.879: SSM CM: [AToM] provision second segment, id 36930
09:17:35.879: SSM CM: CM FSM: state Down - event Provision segment
09:17:35.879: SSM CM: [SSS:AToM:36930] provision segment 2
09:17:35.879: SSM CM: [AToM] send client event 6, id 36930
09:17:35.879: SSM CM: [SSS:AToM] shQ request send ready event
09:17:35.883: SSM CM: SM msg event send ready event
09:17:35.883: SSM CM: [AToM] send client event 3, id 36930
```

The following example shows the events that occur on the CM and SM when an AToM VC is provisioned and then unprovisioned:

```
Router# debug ssm cm events

SSM Connection Manager events debugging is on

Router# debug ssm sm events

SSM Segment Manager events debugging is on

Router# configure terminal
Router(config)# interface ethernet1/0
Router(config-if)# xconnect 10.55.55.2 101 pw-class mpls

16:57:34: SSM CM: provision switch event, switch id 86040
16:57:34: SSM CM: [Ethernet] provision first segment, id 12313
16:57:34: SSM CM: CM FSM: state Idle - event Provision segment
16:57:34: SSM CM: [SSS:Ethernet:12313] provision segment 1
16:57:34: SSM SM: [SSS:Ethernet:12313] event Provison segment
16:57:34: SSM CM: [SSS:Ethernet] shQ request send ready event
16:57:34: SSM CM: SM msg event send ready event
16:57:34: SSM SM: [SSS:Ethernet:12313] segment ready
16:57:34: SSM SM: [SSS:Ethernet:12313] event Found segment data
16:57:34: SSM CM: Query AToM to Ethernet switching, enabled
16:57:34: SSM CM: [AToM] provision second segment, id 16410
16:57:34: SSM CM: CM FSM: state Down - event Provision segment
16:57:34: SSM CM: [SSS:AToM:16410] provision segment 2
16:57:34: SSM SM: [SSS:AToM:16410] event Provison segment
16:57:34: SSM CM: [AToM] send client event 6, id 16410
16:57:34: label_oce_get_label_bundle: flags 14 label 19
16:57:34: SSM CM: [SSS:AToM] shQ request send ready event
16:57:34: SSM CM: SM msg event send ready event
16:57:34: SSM SM: [SSS:AToM:16410] segment ready
16:57:34: SSM SM: [SSS:AToM:16410] event Found segment data
16:57:34: SSM SM: [SSS:AToM:16410] event Bind segment
16:57:34: SSM SM: [SSS:Ethernet:12313] event Bind segment
16:57:34: SSM CM: [AToM] send client event 3, id 16410

Router# configure terminal
Router(config)# interface e1/0
Router(config-if)# no xconnect

16:57:26: SSM CM: [Ethernet] unprovision segment, id 16387
16:57:26: SSM CM: CM FSM: state Open - event Free segment
16:57:26: SSM CM: [SSS:Ethernet:16387] unprovision segment 1
16:57:26: SSM SM: [SSS:Ethernet:16387] event Unprovison segment
16:57:26: SSM CM: [SSS:Ethernet] shQ request send unprovision complete event
16:57:26: SSM CM: [SSS:AToM:86036] unbind segment 2
16:57:26: SSM SM: [SSS:AToM:86036] event Unbind segment
```

```
16:57:26: SSM CM: SM msg event send unprovision complete event
16:57:26: SSM SM: [SSS:Ethernet:16387] free segment class
16:57:26: SSM SM: [SSS:Ethernet:16387] free segment
16:57:26: SSM SM: [SSS:Ethernet:16387] event Free segment
16:57:26: SSM SM: last segment class freed
16:57:26: SSM CM: unprovision switch event, switch id 12290
16:57:26: SSM CM: [SSS:AToM] shQ request send unready event
16:57:26: SSM CM: SM msg event send unready event
16:57:26: SSM SM: [SSS:AToM:86036] event Unbind segment
16:57:26: SSM CM: [AToM] unprovision segment, id 86036
16:57:26: SSM CM: CM FSM: state Down - event Free segment
16:57:26: SSM CM: [SSS:AToM:86036] unprovision segment 2
16:57:26: SSM SM: [SSS:AToM:86036] event Unprovison segment
16:57:26: SSM CM: [SSS:AToM] shQ request send unprovision complete event
16:57:26: SSM CM: SM msg event send unprovision complete event
16:57:26: SSM SM: [SSS:AToM:86036] free segment class
16:57:26: SSM SM: [SSS:AToM:86036] free segment
16:57:26: SSM SM: [SSS:AToM:86036] event Free segment
16:57:26: SSM SM: last segment class freed
```

Related Commands

Command	Description
show ssm	Displays SSM information for switched Layer 2 segments.

debug subscriber aaa authorization

To display diagnostic information about authentication, authorization, and accounting (AAA) authorization of Intelligent Services Gateway (ISG) subscriber sessions, use the **debug subscriber aaa authorization** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug subscriber aaa authorization {**event** | **fsm**}

no debug sss aaa authorization {**event** | **fsm**}

Syntax Description

event	Display information about AAA authorization events that occur during ISG session establishment.
fsm	Display information about AAA authorization state changes for ISG subscriber sessions.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Examples

The following is sample output of several **debug subscriber** commands, including the **debug subscriber aaa authorization** command. The reports from these commands should be sent to technical personnel at Cisco Systems for evaluation.

```
Router# debug subscriber event
Router# debug subscriber error
Router# debug subscriber state
Router# debug subscriber aaa authorization event
Router# debug subscriber aaa authorization fsm

SSS:
  SSS events debugging is on
  SSS error debugging is on
  SSS fsm debugging is on
  SSS AAA authorization event debugging is on
  SSS AAA authorization FSM debugging is on

*Mar  4 21:33:18.248: SSS INFO: Element type is Access-Type, long value is 3
*Mar  4 21:33:18.248: SSS INFO: Element type is Switch-Id, long value is -1509949436
*Mar  4 21:33:18.248: SSS INFO: Element type is Nasport, ptr value is 6396882C
*Mar  4 21:33:18.248: SSS INFO: Element type is AAA-Id, long value is 7
*Mar  4 21:33:18.248: SSS INFO: Element type is AAA-ACCT_ENBL, long value is 1
*Mar  4 21:33:18.248: SSS INFO: Element type is AccIe-Hdl, ptr value is 78000006
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Event service-request, state changed from
wait-for-req to wait-for-auth
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Handling Policy Authorize (1 pending sessions)
*Mar  4 21:33:18.248: SSS PM [uid:7]: Need the following key: Unauth-User
*Mar  4 21:33:18.248: SSS PM [uid:7]: Received Service Request
*Mar  4 21:33:18.248: SSS PM [uid:7]: Event <need keys>, State: initial-req to
need-init-keys
```

```
*Mar  4 21:33:18.248: SSS PM [uid:7]: Policy reply - Need more keys
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Got reply Need-More-Keys from PM
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Event policy-or-mgr-more-keys, state changed from
wait-for-auth to wait-for-req
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Handling More-Keys event
*Mar  4 21:33:20.256: SSS INFO: Element type is Unauth-User, string value is
nobody2@xyz.com
*Mar  4 21:33:20.256: SSS INFO: Element type is AccIe-Hdl, ptr value is 78000006
*Mar  4 21:33:20.256: SSS INFO: Element type is AAA-Id, long value is 7
*Mar  4 21:33:20.256: SSS INFO: Element type is Access-Type, long value is 0
*Mar  4 21:33:20.256: SSS MGR [uid:7]: Event service-request, state changed from
wait-for-req to wait-for-auth
*Mar  4 21:33:20.256: SSS MGR [uid:7]: Handling Policy Authorize (1 pending sessions)
*Mar  4 21:33:20.256: SSS PM [uid:7]: Received More Initial Keys
*Mar  4 21:33:20.256: SSS PM [uid:7]: Event <rcvd keys>, State: need-init-keys to
check-auth-needed
*Mar  4 21:33:20.256: SSS PM [uid:7]: Handling Authorization Check
*Mar  4 21:33:20.256: SSS PM [uid:7]: Event <send auth>, State: check-auth-needed to
authorizing
*Mar  4 21:33:20.256: SSS PM [uid:7]: Handling AAA service Authorization
*Mar  4 21:33:20.256: SSS PM [uid:7]: Sending authorization request for 'xyz.com'
*Mar  4 21:33:20.256: SSS AAA AUTHOR [uid:7]:Event <make request>, state changed from idle
to authorizing
*Mar  4 21:33:20.256: SSS AAA AUTHOR [uid:7]:Authorizing key xyz.com
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:AAA request sent for key xyz.com
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Received an AAA pass
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Event <found service>, state changed from
authorizing to complete
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Found service info for key xyz.com
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Event <free request>, state changed from
complete to terminal
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Free request
*Mar  4 21:33:20.264: SSS PM [uid:7]: Event <found>, State: authorizing to end
*Mar  4 21:33:20.264: SSS PM [uid:7]: Handling Service Direction
*Mar  4 21:33:20.264: SSS PM [uid:7]: Policy reply - Forwarding
*Mar  4 21:33:20.264: SSS MGR [uid:7]: Got reply Forwarding from PM
*Mar  4 21:33:20.264: SSS MGR [uid:7]: Event policy-start-service-fsp, state changed from
wait-for-auth to wait-for-service
*Mar  4 21:33:20.264: SSS MGR [uid:7]: Handling Connect-Forwarding-Service event
*Mar  4 21:33:20.272: SSS MGR [uid:7]: Event service-fsp-connected, state changed from
wait-for-service to connected
*Mar  4 21:33:20.272: SSS MGR [uid:7]: Handling Forwarding-Service-Connected event
```

Related Commands

Command	Description
debug sss error	Displays diagnostic information about errors that may occur during Subscriber Service Switch call setup.
debug sss event	Displays diagnostic information about Subscriber Service Switch call setup events.
debug sss fsm	Displays diagnostic information about the Subscriber Service Switch call setup state.

debug subscriber error

To display diagnostic information about errors that may occur during Intelligent Services Gateway (ISG) subscriber session setup, use the **debug subscriber error** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug subscriber error

no debug subscriber error

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Examples

The following sample output for the **debug subscriber error** command indicates that the session is stale since the session handle has already been destroyed.

```
Router# debug subscriber error

*Sep 20 22:39:49.455: SSS MGR: Session handle [EF000002] destroyed already
```

Related Commands

Command	Description
debug sss aaa authorization event	Displays messages about AAA authorization events that are part of normal call establishment.
debug sss event	Displays diagnostic information about Subscriber Service Switch call setup events.
debug sss fsm	Displays diagnostic information about the Subscriber Service Switch call setup state.

debug subscriber event

To display diagnostic information about Intelligent Services Gateway (ISG) subscriber session setup events, use the **debug subscriber event** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug subscriber event

no debug subscriber event

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Examples

The following sample output for the **debug subscriber event** commands indicates that the system has determined that the session should be locally terminated. The local termination module determines that an interface description block (IDB) is not required for this session, and it sets up the data plane for packet switching.

```
Router# debug subscriber event

*Sep 20 22:21:08.223: SSS MGR [uid:2]: Handling Connect Local Service action
*Sep 20 22:21:08.223: SSS LTERM [uid:2]: Processing Local termination request
*Sep 20 22:21:08.223: SSS LTERM [uid:2]: L3 session - IDB not required for setting up
service
*Sep 20 22:21:08.223: SSS LTERM [uid:2]: Interface already present or not required for
service
*Sep 20 22:21:08.223: SSS LTERM [uid:2]: Segment provision successful
```

Related Commands

Command	Description
debug sss aaa authorization event	Displays messages about AAA authorization events that are part of normal call establishment.
debug sss error	Displays diagnostic information about errors that may occur during Subscriber Service Switch call setup.
debug sss fsm	Displays diagnostic information about the Subscriber Service Switch call setup state.

debug subscriber feature

To display diagnostic information about the installation and removal of Intelligent Services Gateway (ISG) features on ISG subscriber sessions, use the **debug subscriber feature** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug subscriber feature {**all** | **detail** | **error** | **event** | **name** *name-of-feature* {**detail** | **error** | **event** | **packet**} | **packet** [**detail** | **full**] [**issu** {**event** | **error**}] [**ccm** {**event** | **error**}]}

no debug subscriber feature {**all** | **detail** | **error** | **event** | **name** *name-of-feature* {**detail** | **error** | **event** | **packet**} | **packet** [**detail** | **full**] [**issu** {**event** | **error**}] [**ccm** {**event** | **error**}]}

Syntax Description

all	Displays information about all features.
detail	The **detail** keyword can be used in one of the following three ways: • If used with no other keywords, displays detailed information about all features • If a feature name is specified with the **name** *name-of-feature* keyword and argument, displays detailed information about the specific feature. The **detail** keyword can be used with the following *name-of-feature* values: – **accounting** – **compression** – **modem-on-hold** – **policing** – **traffic-classification** • If used with the **packet** keyword, displays a partial dump of packets as ISG features are being applied to the packets.
error	Displays information about errors for all features or a specified feature.
event	Displays information about events for all features or a specified feature.
name	Displays information specific to feature.
issu	Displays information about events and errors for all features or a specified feature as they occur.
ccm	Displays information about a specific feature checkpointing activity. If the **ccm** keyword is not specified, event and error logging is specific to the feature's interaction with the cluster control manager (CCM).

name-of-feature	Name of the ISG feature. Possible values are the following: • **access-list** • **accounting** • **compression** • **filter** • **idle-timer** • **interface-config** • **ip-config** • **l4redirect** • **modem-on-hold** • **policing** • **portbundle** • **prepaid-idle** • **session-timer** • **static-routes** • **time-monitor** • **traffic-classification** • **volume-monitor**
packet	Displays information about packets as ISG features are being applied to the packets. If a feature name is specified with the **name** *name-of-feature* keyword and argument, packet information about the specific feature is displayed. The **packet** keyword can be used with the following *name-of-feature* values: • **access-list** • **l4redirect** • **policing** • **portbundle**
full	(Optional) Displays a full dump of a packet as ISG features are being applied to it.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release12.2(33)SRC.

Examples

The following sample output for the **debug subscriber feature** command indicates that the idle timeout feature has been successfully installed on the inbound segment.

```
Router# debug subscriber feature event

*Sep 20 22:28:57.903: SSF[myservice/uid:6/Idle Timeout]: Group feature install
*Sep 20 22:28:57.903: SSF[uid:6/Idle Timeout]: Adding feature to inbound segment(s)
```

debug subscriber fsm

To display diagnostic information about Intelligent Services Gateway (ISG) subscriber session state change, use the **debug subscriber fsm** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug subscriber fsm

no debug subscriber fsm

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Examples

The following sample output for the **debug subscriber fsm** command indicates that the session has been disconnected by the client, and the system is cleaning up the session by disconnecting the network service and removing any installed features.

```
Router# debug subscriber fsm

*Sep 20 22:35:10.495: SSS MGR [uid:5]: Event client-disconnect, state changed from
connected to disconnecting-fsp-feat
```

debug subscriber packet

To display information about packets as they traverse the subscriber service switch (SSS) path, use the **debug subscriber packet** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug subscriber packet {**detail** | **error** | **event** | **full**}

no debug subscriber packet {**detail** | **error** | **event** | **full**}

Syntax Description

detail	Displays a partial dump of packets as they traverse the SSS path.
error	Displays any packet-switching errors that occur when a packet traverses the SSS path.
event	Displays packet-switching events that occur when a packet traverses the SSS path.
full	Displays a full dump of packets as they traverse the SSS path.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Examples

The following example show sample output for the **debug subscriber packet** command with the **full** keyword. This output is for a PPPoE session configured with forwarding.

```
SSS Switch: Pak encap size, old: 60, new: 24
SSS Switch: Pak 0285C458 sz 66 encap 14
*Feb  9 15:47:13.659: 000000 AA BB CC 00 0B 01 AA BB  D.......
*Feb  9 15:47:13.659: 000008 CC 00 0C 01 08 00 45 00  ......N.
*Feb  9 15:47:13.659: 000010 00 34 00 28 00 00 FE 11  .4.(....
*Feb  9 15:47:13.659: 000018 F2 9D AC 12 B8 E7 AC 12  ........
*Feb  9 15:47:13.659: 000020 B8 E6 06 A5 06 A5 00 20  .......
*Feb  9 15:47:13.659: 000028 00 00 C0 01 02 00 00 02  ........
*Feb  9 15:47:13.659: 000030 00 01 00 18 00 00 FC A7  ........
*Feb  9 15:47:13.659: 000038 2E B3 FF 03 C2 23 03 01  .....#..
*Feb  9 15:47:13.659: 000040 00 04                    ..
SSS Switch: Pak encap size, old: 60, new: 24
SSS Switch: Pak 0285C458 sz 72 encap 14
*Feb  9 15:47:13.691: 000000 AA BB CC 00 0B 01 AA BB  D.......
*Feb  9 15:47:13.691: 000008 CC 00 0C 01 08 00 45 00  ......N.
*Feb  9 15:47:13.691: 000010 00 3A 00 2A 00 00 FE 11  .:.*....
*Feb  9 15:47:13.691: 000018 F2 95 AC 12 B8 E7 AC 12  ........
*Feb  9 15:47:13.691: 000020 B8 E6 06 A5 06 A5 00 26  .......&
*Feb  9 15:47:13.691: 000028 00 00 C0 01 02 00 00 02  ........
*Feb  9 15:47:13.691: 000030 00 01 00 1E 00 00 FC A7  ........
*Feb  9 15:47:13.691: 000038 2E B3 FF 03 80 21 01 01  .....!..
*Feb  9 15:47:13.691: 000040 00 0A 03 06 3A 3A 3A 3A  ....::::
SSS Switch: Pak encap size, old: 24, new: 46
SSS Switch: Pak 027A5BE8 sz 36 encap 18
*Feb  9 15:47:13.691: 000000 AA BB CC 00 0B 00 AA BB  D.......
```

```
*Feb  9 15:47:13.691: 000008 CC 00 0A 00 81 00 01 41  .......a
*Feb  9 15:47:13.691: 000010 88 64 11 00 00 01 00 0C  .dN.....
*Feb  9 15:47:13.691: 000018 80 21 01 01 00 0A 03 06  .!......
*Feb  9 15:47:13.691: 000020 00 00 00 00              ....
SSS Switch: Pak encap size, old: 60, new: 24
SSS Switch: Pak 0285C458 sz 72 encap 14
*Feb  9 15:47:13.691: 000000 AA BB CC 00 0B 01 AA BB  D.......
*Feb  9 15:47:13.691: 000008 CC 00 0C 01 08 00 45 00  ......N.
*Feb  9 15:47:13.691: 000010 00 3A 00 2C 00 00 FE 11  .:.,....
*Feb  9 15:47:13.691: 000018 F2 93 AC 12 B8 E7 AC 12  ........
*Feb  9 15:47:13.691: 000020 B8 E6 06 A5 06 A5 00 26  .......&
*Feb  9 15:47:13.691: 000028 00 00 C0 01 02 00 00 02  ........
*Feb  9 15:47:13.691: 000030 00 01 00 1E 00 00 FC A7  ........
*Feb  9 15:47:13.691: 000038 2E B3 FF 03 80 21 03 01  .....!..
*Feb  9 15:47:13.691: 000040 00 0A 03 06 09 00 00 1F  ........
```

Related Commands

Command	Description
debug subscriber feature	Displays diagnostic information about the installation and removal of ISG features on subscriber sessions.

debug subscriber policy

To display diagnostic information about policy execution related to Intelligent Services Gateway (ISG) subscriber sessions, use the **debug subscriber policy** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug subscriber policy {**all** | **detail** | **error** | **event** | **fsm** | **prepaid** | {**condition** | **idmgr** | **profile** | **push** | **rule** | **service**} [**detail** | **error** | **event**] | **dpm** [**error** | **event**] | **webportal** {**detail** | **error** | **event**}}

no debug subscriber policy {**all** | **detail** | **error** | **event** | **fsm** | **prepaid** | {**condition** | **idmgr** | **profile** | **push** | **rule** | **service**} [**detail** | **error** | **event**] | **dpm** [**error** | **event**] | **webportal** {**detail** | **error** | **event**}}

Syntax Description

all	Displays information about all policies.
detail	Displays detailed information about all policies or the specified type of policy.
error	Displays policy execution errors for all policies or the specified type of policy.
event	Displays policy execution events for all policies or the specified type of policy.
fsm	Displays information about state changes during policy execution.
prepaid	Displays information about ISG prepaid policy execution.
condition	Displays information related to the evaluation of ISG control class maps.
idmgr	Displays information about policy execution related to identity.
profile	Displays information about the policy manager subscriber profile database.
push	Displays policy information about dynamic updates to subscriber profiles from policy servers.
rule	Displays information about control policy rules.
service	Displays policy information about service profile database events for subscriber sessions.
dpm	Displays information about Dynamic Host Configuration Protocol (DHCP) in relation to subscriber sessions.
webportal	Displays policy information about the web portal in relation to subscriber sessions.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Examples

The following example shows sample output for the **debug subscriber policy** command with the **events** keyword. This output indicates the creation of a new session. "Updated key list" indicates important attributes and information associated with the session.

```
*Feb  7 18:58:24.519: SSS PM [0413FC58]: Create context 0413FC58
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]: Authen status update; is now "unauthen"
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]: Updated NAS port for AAA ID 14
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]: Updated key list:
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   Access-Type = 15 (IP)
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   Protocol-Type = 4 (IP)
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   Media-Type = 2 (IP)
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   IP-Address = 10.0.0.2 (0A000002)
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   IP-Address-VRF = IP 10.0.0.2:0
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   source-ip-address = 037FBB78
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   Mac-Address = aabb.cc00.6500
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   Final = 1 (YES)
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   Authen-Status = 1 (Unauthenticated)
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   Nasport = PPPoEoE: slot 0 adapter 0 port
0
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]: Updated key list:
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   Access-Type = 15 (IP)
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   Protocol-Type = 4 (IP)
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   Media-Type = 2 (IP)
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   IP-Address = 10.0.0.2 (0A000002)
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   IP-Address-VRF = IP 10.0.0.2:0
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   source-ip-address = 037FBB78
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   Mac-Address = aabb.cc00.6500
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   Final = 1 (YES)
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   Authen-Status = 1 (Unauthenticated)
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   Nasport = PPPoEoE: slot 0 adapter 0 port
0
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]:   Session-Handle = 486539268 (1D000004)
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]: SM Policy invoke - Service Selection
Request
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]: Access type IP
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]: Access type IP: final key
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]: Received Service Request
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]: Handling Authorization Check
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]: SIP [IP] can NOT provide more keys
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]: SIP [IP] can NOT provide more keys
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]: Handling Default Service
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]: Providing Service
*Feb  7 18:58:24.519: SSS PM [uid:4][0413FC58]: Policy reply - Local Terminate
*Feb  7 18:58:24.523: SSS PM [uid:4][0413FC58]: SM Policy invoke - Apply Config Success
*Feb  7 18:58:24.523: SSS PM [uid:4][0413FC58]: Handling Apply Config; SUCCESS
```

debug subscriber policy dpm timestamps

To include timestamp information for DHCP policy module (DPM) messages in debugging output, use the **debug subscriber policy dpm timestamps** command in privileged EXEC mode. To remove timestamp information from output, use the **no** form of this command.

debug subscriber policy dpm timestamps

no debug subscriber policy dpm timestamps

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SB9	This command was introduced.

Usage Guidelines

The **debug subscriber policy dpm timestamps** command enables the timestamp information for the latest DPM message that was received to be saved after a session is established. The timestamp for DPM messages is displayed in debugging output, including output from the **show subscriber policy dpm context** command.

Timestamp information is removed by default after a session is established. Enabling this command preserves the timestamp information so that it can be included in debugging output. This command does not display any debugging output; it enables timestamp output for other **debug** and **show** commands.

Examples

The following example shows how to include timestamp information in debug output:

```
Router# debug subscriber policy dpm timestamps

SG dhcp message timestamps debugging is on
```

Related Commands

Command	Description
show subscriber policy dpm context	Displays event traces for DPM session contexts.

debug subscriber service

To display diagnostic information about the service profile database in an Intelligent Services Gateway (ISG), use the **debug subscriber service** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug subscriber service

no debug subscriber service

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Use the **debug subscriber service** command to diagnose problems with service profiles or service policy maps.

Examples

The following example shows sample output for the **debug subscriber service** command. This output indicates that a service logon has occurred for the service "prep_service".

```
*Feb 7 18:52:31.067: SVM [prep_service]: needs downloading
*Feb 7 18:52:31.067: SVM [D6000000/prep_service]: allocated version 1
*Feb 7 18:52:31.067: SVM [D6000000/prep_service]: [8A000002]: client queued
*Feb 7 18:52:31.067: SVM [D6000000/prep_service]: [PM-Download:8A000002] locked 0->1
*Feb 7 18:52:31.067: SVM [D6000000/prep_service]: [AAA-Download:040DD9D0] locked 0->1
*Feb 7 18:52:31.127: SVM [D6000000/prep_service]: TC feature info found
*Feb 7 18:52:31.127: SVM [D0000001/prep_service]: added child
*Feb 7 18:52:31.127: SVM [D6000000/prep_service]: [TC-Child:040DD130] locked 0->1
*Feb 7 18:52:31.127: SVM [D0000001/CHILD/prep_service]: [TC-Parent:040DD1A8] locked 0->1
*Feb 7 18:52:31.127: SVM [D6000000/prep_service]: TC flow feature info not found
*Feb 7 18:52:31.127: SVM [D6000000/prep_service]: downloaded first version
*Feb 7 18:52:31.127: SVM [D6000000/prep_service]: [8A000002]: client download ok
*Feb 7 18:52:31.127: SVM [D6000000/prep_service]: [SVM-to-client-msg:8A000002] locked 0->1
*Feb 7 18:52:31.127: SVM [D6000000/prep_service]: [AAA-Download:040DD9D0] unlocked 1->0
*Feb 7 18:52:31.131: SVM [D6000000/prep_service]: alloc feature info
*Feb 7 18:52:31.131: SVM [D6000000/prep_service]: [SVM-Feature-Info:040E2E80] locked 0->1
*Feb 7 18:52:31.131: SVM [D6000000/prep_service]: has Policy info
*Feb 7 18:52:31.131: SVM [D6000000/prep_service]: [PM-Info:0416BAB0] locked 0->1
*Feb 7 18:52:31.131: SVM [D6000000/prep_service]: populated client
*Feb 7 18:52:31.131: SVM [D6000000/prep_service]: [PM-Download:8A000002] unlocked 1->0
*Feb 7 18:52:31.131: SVM [D6000000/prep_service]: [SVM-to-client-msg:8A000002] unlocked
1->0
*Feb 7 18:52:31.131: SVM [D6000000/prep_service]: [PM-Service:040E31E0] locked 0->1
*Feb 7 18:52:31.131: SVM [D0000001/CHILD/prep_service]: [SM-SIP-Apply:D0000001] locked
0->1
*Feb 7 18:52:31.131: SVM [D6000000/prep_service]: [FM-Bind:82000002] locked 0->1
*Feb 7 18:52:31.131: SVM [D6000000/prep_service]: [SVM-Feature-Info:040E2E80] unlocked
```

```
1->0
*Feb 7 18:52:31.139: SVM [D0000001/CHILD/prep_service]: alloc feature info
*Feb 7 18:52:31.139: SVM [D0000001/CHILD/prep_service]: [SVM-Feature-Info:040E2E80] locked
0->1
*Feb 7 18:52:31.159: SVM [D0000001/CHILD/prep_service]: [FM-Bind:2C000003] locked 0->1
*Feb 7 18:52:31.159: SVM [D0000001/CHILD/prep_service]: [SVM-Feature-Info:040E2E80]
unlocked 1->0
*Feb 7 18:52:31.159: SVM [D0000001/CHILD/prep_service]: [SM-SIP-Apply:D0000001] unlocked
1->0
```

debug subscriber testing

To display diagnostic information for Intelligent Services Gateway (ISG) simulator testing, use the **debug subscriber testing** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug subscriber testing

no debug subscriber testing

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Examples

The following example shows the configuration of the **debug subscriber testing** command:

```
Router# debug subscriber testing
```

drop (ISG)

To configure an Intelligent Services Gateway (ISG) to discard packets belonging to the default traffic class, use the **drop** command in service policy-map class configuration mode. To disable the packet-discarding action, use the **no** form of this command.

drop

no drop

Syntax Description

This command has no arguments or keywords.

Command Default

Packets will be passed.

Command Modes

Service policy-map configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

The **drop** command can only be configured in the default class of an ISG service policy map. The default traffic class handles all the traffic that is not handled by other traffic classes in a service.

Examples

The following example shows the default class configured to drop traffic for the service "SERVICE1":

```
policy-map type service SERVICE1
 class type traffic CLASS1
  prepaid-config PREPAID
 class type traffic default
  drop
```

Related Commands

Command	Description
class type traffic	Specifies a named traffic class whose policy you want to create or change or specifies the default traffic class in order to configure its policy.
policy-map type service	Creates or modifies a service policy map, which is used to define an ISG subscriber service.
show class-map type traffic	Displays traffic class maps and their matching criteria.

greater-than

To create a condition that will evaluate true if the subscriber network access server (NAS) port identifier is greater than the specified value, use the **greater-than** command in control class-map configuration mode. To remove the condition, use the **no** form of this command.

greater-than [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}

no greater-than [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}

Syntax Description

not	(Optional) Negates the sense of the test.
nas-port	NAS port identifier.
adapter *adapter-number*	Interface adapter number.
channel *channel-number*	Interface channel number.
ipaddr *ip-address*	IP address.
port *port-number*	Port number.
shelf *shelf-number*	Interface shelf number.
slot *slot-number*	Slot number.
sub-interface *sub-interface-number*	Subinterface number.
type *interface-type*	Interface type.
vci *vci-number*	Virtual channel identifier (VCI).
vlan *vlan-id*	VLAN ID.
vpi *vpi-number*	Virtual path identifier.

Command Default

A condition that will evaluate true if the subscriber NAS port identifier is greater than the specified value is not created.

Command Modes

Control class-map configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

The **greater-than** command is used to configure a condition within a control class map. A control class map, which is configured with the **class-map type control** command, specifies conditions that must be met for a control policy to be activated, and, optionally, the event that causes the class to be evaluated.

A control class map can contain multiple conditions, each of which will evaluate to either true or false. Match directives can be used to specify whether all, any, or none of the conditions must evaluate true in order for the class as whole to evaluate true.

The **class type control** command is used to associate a control class map with a policy control map.

Examples

The following example shows a control class map that evaluates true for only a specific range of ATM permanent virtual circuit (PVC) VCIs, 101-104 inclusive:

```
class-map type type control match-any MY-CONDITION
 greater-than nas-port type atm vpi 200 vci 100
 less-than nas-port type atm vpi 200 vci 105
```

Related Commands

Command	Description
class-map type control	Creates an ISG control class map.
class type control	Specifies a control class for which actions may be configured in an ISG control policy map.
policy-map type control	Creates or modifies a control policy map, which defines an ISG control policy.

greater-than-or-equal

To create a condition that will evaluate true if the subscriber identifier is greater than or equal to the specified value, use the **greater-than-or-equal** command in control class-map configuration mode. To remove the condition, use the **no** form of this command.

greater-than-or-equal [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}

no greater-than-or-equal [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}

Syntax Description

not	(Optional) Negates the sense of the test.
nas-port	NAS port identifier.
adapter *adapter-number*	Interface adapter number.
channel *channel-number*	Interface channel number.
ipaddr *ip-address*	IP address.
port *port-number*	Port number.
shelf *shelf-number*	Interface shelf number.
slot *slot-number*	Slot number.
sub-interface *sub-interface-number*	Subinterface number.
type *interface-type*	Interface type.
vci *vci-number*	Virtual channel identifier.
vlan *vlan-id*	VLAN ID.
vpi *vpi-number*	Virtual path identifier.

Command Default

A condition that will evaluate true if the subscriber identifier is greater than or equal to the specified value is not created.

Command Modes

Control class-map configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

The **greater-than-or-equal** command is used to configure a condition within a control class map. A control class map, which is configured with the **class-map type control** command, specifies conditions that must be met for a control policy to be activated, and, optionally, the event that causes the class to be

evaluated. A control class map can contain multiple conditions, each of which will evaluate to either true or false. Match directives can be used to specify whether all, any, or none of the conditions must evaluate true in order for the class as whole to evaluate true.

The **class type control** command is used to associate a control class map with a policy control map.

Examples

The following example shows a control class map called "class3" configured with three conditions. The **match-all** keyword indicates that all of the conditions must evaluate true before the class evaluates true. The **class type control** command associates "class3" with the control policy map called "rule4".

```
class-map type control match-all class3
 greater-than-or-equal nas-port port 1000
!
policy-map type control rule4
  class type control class3 event session-start
   1 authorize identifier nas-port
!
```

Related Commands

Command	Description
class-map type control	Creates an ISG control class map.
class type control	Specifies a control class for which actions may be configured in an ISG control policy map.
policy-map type control	Creates or modifies a control policy map, which defines an ISG control policy.

identifier interface

Note Effective with Cisco IOS Release 12.2(31)SB2, the **identifier interface** command is replaced by the **ip subscriber interface** command. See the **ip subscriber interface** command for more information.

To create an Intelligent Service Agent (ISG) IP interface session, use the **identifier interface** command in IP subscriber configuration mode. To remove the IP interface session, use the **no** form of this command.

identifier interface

no identifier interface

Syntax Description

This command has no arguments or keywords.

Command Default

An ISG IP interface session is not created.

Command Modes

IP subscriber configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SB2	This command was replaced by the **ip subscriber interface** command.

Usage Guidelines

An IP interface session includes all IP traffic received on a specific physical or virtual interface. IP interface sessions are provisioned through the command-line interface (CLI), that is, the session is created when the IP interface session commands are entered.

IP interface sessions might be used in situations in which a subscriber is represented by an interface (with the exception of PPP) and communicates using more than one IP address. For example, a subscriber using routed bridge encapsulation (RBE) access might have a dedicated ATM virtual circuit (VC) to home customer premises equipment (CPE) that is hosting multiple PCs.

Examples

The following example shows an IP interface session configured on Ethernet interface 0/0:

```
interface ethernet0/0
 ip subscriber
  identifier interface
```

Related Commands

Command	Description
identifier ip src-addr	Enables an ISG to create an IP session upon detection of the first IP packet from an unidentified subscriber.
ip subscriber	Enables ISG IP subscriber configuration mode.

identifier ip src-addr

Note Effective with Cisco IOS Release 12.2(31)SB2, the **identifier ip src-addr** command is replaced by the **initiator** command. See the **initiator** command for more information.

To enable an Intelligent Services Gateway (ISG) to create an IP session upon detection of the first IP packet from an unidentified subscriber, use the **identifier ip src-addr** command in IP subscriber configuration mode. To disable IP session creation upon receipt of IP packets from unidentified subscribers, use the **no** form of this command.

identifier ip src-addr [**match** *access-list-number*]

no identifier ip src-addr [**match** *access-list-number*]

Syntax Description

match *access-list-number*	(Optional) Causes IP sessions to be created only for subscriber traffic matching the access list.

Command Default

An ISG does not create IP sessions upon detection of the first IP packet from an unidentified subscriber.

Command Modes

IP subscriber configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SB2	This command was replaced by the **initiator** command.

Usage Guidelines

An ISG subscriber IP session includes all the traffic that is associated with a single subscriber IP address. An IP subnet session includes all the IP traffic that is associated with a single IP subnet.

IP subnet sessions are created the same way as IP sessions, except that when a subscriber is authorized or authenticated and the Framed-IP-Netmask attribute is present in the user or service profile, the ISG converts the source-IP-based session into a subnet session with the subnet value in the Framed-IP-Netmask attribute.

Examples

The following example shows how to configure an ISG to create IP sessions upon detection of the first IP packet from unidentified subscribers:

```
interface ethernet0/0
 ip subscriber
  identifier ip src-addr
```

Related Commands

Command	Description
identifier interface	Creates an ISG IP interface session.
ip subscriber	Enables ISG IP subscriber configuration mode.

if upon network-service-found

To specify whether the system should continue processing policy rules once a subscriber's network service has been identified, use the **if upon network-service-found** command in control policy-map class configuration mode. To remove this action from the control policy map, use the **no** form of this command.

action-number **if upon network-service-found** {**continue** | **stop**}

no *action-number* **if upon network-service-found** {**continue** | **stop**}

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.
continue	Specifies that when a network service for the session is identified, actions in the policy rule will continue to be executed. This is the default.
stop	Specifies that when a network service for the session is identified, no more actions in the policy rule will be executed.

Command Default

Actions will continue to be executed when a subscriber's network service is identified.

Command Modes

Control policy-map class configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

The **if upon network-service-found** command configures an action in a control policy map.

Control policies define the actions the system will take in response to specified events and conditions. A control policy map is used to configure an Intelligent Services Gateway (ISG) control policy. A control policy is made of one or more control policy rules. A control policy rule is an association of a control class and one or more actions. The control class defines the conditions that must be met before the actions will be executed. The actions are numbered and executed sequentially within the policy rule.

Examples

The following example shows how to configure ISG to stop executing actions once the subscriber's network service has been found:

```
policy-map type control policy1
 class type control always event session-start
  1 if upon network-service-found stop
```

ignore (ISG)

To configure an Intelligent Services Gateway (ISG) to ignore specific parameters in requests from RADIUS clients, use the **ignore** command in dynamic authorization local server configuration mode. To reinstate the default behavior, use the **no** form of this command.

ignore {**session-key** | **server-key**}

no ignore {session-key | server-key}

Syntax Description

session-key	Configures ISG to ignore the session key.
server-key	Configures ISG to ignore the server key.

Command Default

The ISG will not ignore the session key or server key.

Command Modes

Dynamic authorization local server configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

An ISG can be configured to allow external policy servers to dynamically send policies to the ISG. This functionality 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. Use the **ignore** command to configure the ISG to ignore the server key or session key in requests from RADIUS clients.

Examples

The following example configures ISG to ignore the server key in requests from RADIUS clients:

```
aaa server radius dynamic-author
 client 10.0.0.1
 ignore server-key
```

Related Commands

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

initiator

To enable Intelligent Services Gateway (ISG) to create an IP subscriber session upon receipt of a specified type of packet, use the **initiator** command in IP subscriber configuration mode. To disable IP session creation in response to specified packets, use the **no** form of this command.

initiator {**dhcp** [**class-aware**] | **radius-proxy** | **static ip subscriber list** *listname* | **unclassified ip** | **unclassified mac**}

no initiator {**dhcp** [**class-aware**] | **radius-proxy** | **static ip subscriber list** *listname* | **unclassified ip** | **unclassified mac**}

Syntax Description

dhcp	IP subscriber session is initiated upon receipt of a DHCP DISCOVER packet. **Note** The **class-aware** keyword is required when using the **dhcp** keyword.
class-aware	(Optional) Allows an ISG to influence the IP address assigned by DHCP by providing DHCP with a class name.
radius-proxy	IP subscriber session is initiated upon receipt of a RADIUS Access-Request packet.
unclassified ip	IP subscriber session is initiated upon receipt of the first IP packet with an unclassified IP source address.
unclassified mac	IP subscriber session is initiated upon receipt of the first IP packet with an unclassified MAC source address.
static ip subscriber list *listname*	IP static session is initiated upon receipt of the IP subscriber list name

Command Default

IP sessions are not created upon receipt of specified packets.

Command Modes

IP subscriber configuration (config-subscriber)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SB2	The following keywords were added: **radius-proxy**, **unclassified ip**, **unclassified mac**.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.
12.2(33)SRE	This command was modified. The **static** keyword was added.
Cisco IOS XE Release 2.5	This command was modified. The **static** keyword was added.

Usage Guidelines

DHCP and ISG IP Session Creation

If the following conditions are met, receipt of a DHCP DISCOVER packet will trigger the creation of an IP session:

- ISG serves as a DHCP relay or server for new IP address assignments.
- Subscribers are configured for DHCP.
- The DHCP DISCOVER packet is the first DHCP request received from the subscriber.

Note If the ISG device serves as either a DHCP relay or DHCP server in the assignment of client IP addresses, ISG must be configured to initiate IP sessions upon receipt DHCP DISCOVER packets. In other words, the **initiator dhcp** command must be configured instead of **initiator unclassified ip** or **initiator unclassified mac**.

DHCP and ISG IP Address Assignment

When ISG is in the path of DHCP requests (either as a DHCP server or as a relay), ISG can influence the IP address pool and the DHCP server that is used to assign subscriber IP addresses. To enable ISG to influence the IP addresses assigned to subscribers, you associate a DHCP address pool class with an address domain. When a DHCP request is received from a subscriber, DHCP uses the address pool class that is associated with the subscriber to determine which DHCP address pool should be used to service the request. As a result, on a per-request basis, an IP address is provided by the local DHCP server or relayed to a remote DHCP server that is defined in the selected pool. The **class-aware** keyword enables the ISG to provide DHCP with a class name.

Examples

The following example shows how to configure ISG to create IP sessions for subscribers who connect to ISG on Gigabit Ethernet interface 0/1.401 through a routed access network. ISG will create IP sessions upon receipt of DHCP DISCOVER packets, incoming valid IP packets, and RADIUS Access-Request packets.

```
interface GigabitEthernet0/1.401
 ip subscriber routed
  initiator dhcp class-aware
  initiator unclassified ip-address
  initiator radius-proxy
  initiator static ip subscriber list mylist
```

Related Commands

Command	Description
ip subscriber	Enables ISG IP subscriber support on an interface and specifies the access method that IP subscribers will use to connect to ISG on an interface.
ip subscriber list	Creates a ip subscriber static server list group list name

interface multiservice

To create a multiservice interface, which enables dynamic virtual private network (VPN) selection on an Intelligent Services Gateway (ISG), use the **interface multiservice** command in global configuration mode. To remove a multiservice interface, use the **no** form of this command.

interface multiservice *interface-number*

no interface multiservice *interface-number*

Syntax Description

interface-number	Number of the multiservice interface. Range is 0 to 1024.

Command Default

A multiservice interface is not created.

Command Modes

Global configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

IP interface features (such as quality of service (QoS) and access lists) are not supported on multiservice interfaces.

For a subscriber without a static VPN configuration, a multiservice interface must be configured on the ISG device to map the IP subscriber session to a VRF. The multiservice interface represents a boundary between a VPN routing domain and the default routing domain. In cases where an IP subscriber may be associated with several routing domains throughout the duration of a connection, multiservice interfaces serve as demarcation points for the IP subscriber to switch from one VPN domain to another.

One multiservice interface must be configured for each VPN routing domain.

Examples

The following example shows the configuration of two multiservice interfaces:

```
interface multiservice 1
 ip address 10.69.10.1 255.255.255.0
!
interface multiservice 2
 ip vrf forwarding Corporate-VPN
 ip address 10.1.1.1 255.255.255.0
```

interim-interval

To specify the interval at which the Intelligent Services Gateway (ISG) sends interim prepaid accounting records, use the **interim-interval** command in prepaid configuration mode. To disable interim prepaid accounting, use the **no** form of this command.

interim-interval *number-of-minutes*

no interim-interval *number-of-minutes*

Syntax Description

number-of-minutes	Interval, in minutes, between prepaid accounting record updates. Range is from 1 to 1440.

Command Default

Interim prepaid accounting is not enabled.

Command Modes

Prepaid configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

When the **interim-interval** command is configured, the ISG sends accounting records at the specified interval so there will be written log of accounting events that occurred between the Accounting-Start and Accounting-Stop records.

Examples

The following example shows an ISG prepaid feature configuration in which the interval for interim prepaid accounting is set to 5 minutes:

```
subscriber feature prepaid conf-prepaid
 interim-interval 5
 threshold time 20
 threshold volume 0
 method-list accounting ap-mlist
 method-list authorization default
 password cisco
```

Related Commands

Command	Description
prepaid config	Enables prepaid billing for an ISG service and references a configuration of prepaid billing parameters.
subscriber feature prepaid	Creates or modifies a configuration of ISG prepaid billing parameters that can be referenced from a service policy map or service profile.

ip access-group

To apply an IP access list or object group access control list (OGACL) to an interface or a service policy map, use the **ip access-group** command in the appropriate configuration mode. To remove an IP access list or OGACL, use the **no** form of this command.

ip access-group {*access-list-name* | *access-list-number*} {**in** | **out**}

no ip access-group {*access-list-number* | *access-list-name*} {**in** | **out**}

Syntax Description

access-list-name	Name of the existing IP access list or OGACL as specified by an **ip access-list** command.
access-list-number	Number of the existing access list. This is a decimal number from 1 to 199 or from 1300 to 2699.
in	Filters on inbound packets.
out	Filters on outbound packets.

Command Default

An access list is not applied.

Command Modes

Interface configuration (config-if)
Service policy-map configuration (config-service-policymap)

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-name* argument was added.
12.2(28)SB	This command was made available in service policy-map configuration mode.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	The *access-list-name* keyword was modified to accept the name of an OGACL.

Usage Guidelines

If the specified access list does not exist, all packets are passed (no warning message is issued).

Applying Access Lists to Interfaces

Access lists or OGACLs are applied on either outbound or inbound interfaces. For standard inbound access lists, after an interface receives a packet, the Cisco IOS software checks the source address of the packet against the access list. For extended access lists or OGACLs, the networking device also checks the destination access list or OGACL. If the access list or OGACL permits the address, the software continues to process the packet. If the access list or OGACL rejects the address, the software discards the packet and returns an Internet Control Management Protocol (ICMP) host unreachable message.

For standard outbound access lists, after a device receives and routes a packet to a controlled interface, the software checks the source address of the packet against the access list. For extended access lists or OGACLs, the networking device also checks the destination access list or OGACL. If the access list or OGACL permits the address, the software sends the packet. If the access list or OGACL rejects the address, the software discards the packet and returns an ICMP host unreachable message.

When you enable outbound access lists or OGACLs, you automatically disable autonomous switching for that interface. When you enable inbound access lists or OGACLs on any CBus or CxBus interface, you automatically disable autonomous switching for all interfaces (with one exception—a Storage Services Enabler (SSE) configured with simple access lists can still switch packets, on output only).

Applying Access Lists or OGACLs to Service Policy Maps

You can use the **ip access-group** command to configure Intelligent Services Gateway (ISG) per-subscriber firewalls. Per-subscriber firewalls are Cisco IOS IP access lists or OGACLs that are used to prevent subscribers, services, and pass-through traffic from accessing specific IP addresses and ports.

ACLs and OGACLs can be configured in user profiles or service profiles on an authentication, authorization, and accounting (AAA) server or in service policy maps on an ISG. OGACLS or numbered or named IP access lists can be configured on the ISG, or the ACL or OGACL statements can be included in the profile configuration.

When an ACL or OGACL is added to a service, all subscribers of that service are prevented from accessing the specified IP address, subnet mask, and port combinations through the service.

Examples

The following example applies list 101 on packets outbound from Ethernet interface 0:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 0
Router(config-if)# ip access-group 101 out
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or OGACL that will deny packets.
ip access-list	Defines an IP access list or OGACL by name or number.
object-group network	Defines network object groups for use in OGACLs.
object-group service	Defines service object groups for use in OGACLs.
permit	Sets conditions in a named IP access list or OGACL that will permit packets.
show ip access-list	Displays the contents of IP access lists or OGACLs.
show object-group	Displays information about object groups that are configured.

ip portbundle (global)

To enable portbundle configuration mode, in which Intelligent Services Gateway (ISG) port-bundle host key parameters can be configured, use the **ip portbundle** command in global configuration mode. To remove the configuration of the port-bundle host key parameters and release all the port bundles in use, use the **no** form of this command.

ip portbundle

no ip portbundle

Syntax Description

This command has no arguments or keywords.

Command Default

Portbundle configuration mode is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Entering the **no ip portbundle** command in global configuration mode removes the configuration of port-bundle host key parameters and releases all the port bundles in use by the sessions.

Examples

The following example shows how to configure the ISG Port-Bundle Host Key feature to apply to all sessions:

```
policy-map type service ISGPBHKService
 ip portbundle
!
policy-map type control PBHKRule
 class type control always event session-start
  1 service-policy type service ISGPBHKService
!
service-policy type control PBHKRule

interface ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip portbundle outside
!
ip portbundle
 match access-list 101
 length 5
 source ethernet0/0
```

Related Commands

Command	Description
ip portbundle (global)	Enters portbundle configuration mode, in which ISG port-bundle host key parameters can be configured.
ip portbundle outside	Configures the ISG to reverse translate the destination IP address and TCP port to the actual subscriber IP address and TCP port for traffic going from the portal to the subscriber.
length	Specifies the ISG port-bundle length.
match access-list	Specifies packets for port-mapping by specifying an access list to compare against the subscriber traffic.
show ip portbundle ip	Displays information about a particular ISG port bundle.
show ip portbundle status	Displays information about ISG port-bundle groups.
source	Specifies the interface for which the main IP address will be mapped by the ISG to the destination IP addresses in subscriber traffic.

ip portbundle (service policy-map)

To enable the Intelligent Services Gateway (ISG) Port-Bundle Host Key feature for a service, use the **ip portbundle** command in service policy-map configuration mode. To disable the ISG Port-Bundle Host Key feature, use the **no** form of this command.

ip portbundle

no ip portbundle

Syntax Description

This command has no arguments or keywords.

Command Default

ISG Port-Bundle Host Key feature is not enabled.

Command Modes

Service policy-map configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

When the ISG Port-Bundle Host Key feature is configured, TCP packets from subscribers are mapped to a local IP address for the ISG and a range of ports. This mapping allows the portal to identify the ISG gateway from which the session originated.

The ISG Port-Bundle Host Key feature can be enabled in a service policy map on the router by using the **ip portbundle** command. The feature can also be enabled in a service profile or user profile on a AAA server.

Examples

The following example shows how to configure the ISG Port-Bundle Host Key feature to apply to all sessions. The ISG Port-Bundle Host Key feature is enabled in the service policy map called "ISGPBHKService".

```
policy-map type service ISGPBHKService
 ip portbundle
!
policy-map type control PBHKRule
 class type control always event session-start
  1 service-policy type service ISGPBHKService
!
service-policy type control PBHKRule

interface ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip portbundle outside
!
ip portbundle
 match access-list 101
```

```
length 5
source ethernet0/0
```

Related Commands

Command	Description
ip portbundle (global)	Enters portbundle configuration mode, in which ISG port-bundle host key parameters can be configured.
ip portbundle outside	Configures the ISG to reverse translate the destination IP address and TCP port to the actual subscriber IP address and TCP port for traffic going from the portal to the subscriber.
policy-map type service	Create or modifies a service policy map, which is used to define an ISG subscriber service.
show ip portbundle ip	Displays information about a particular ISG port bundle.
show ip portbundle status	Displays information about ISG port-bundle groups.

ip portbundle outside

To configure an Intelligent Services Gateway (ISG) to translate the destination IP address and TCP port to the actual subscriber IP address and TCP port for traffic going from the portal to the subscriber, use the **ip portbundle outside** command in interface configuration mode. To disable ISG port-bundle host key translation, use the **no** form of this command.

ip portbundle outside

no ip portbundle outside

Syntax Description

This command has no arguments or keywords.

Command Default

Translation does not occur.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

The **ip portbundle outside** command must be configured on ISG interfaces that reach the portal.

Examples

The following example configures ISG to translate the destination IP address and TCP port to the actual subscriber IP address and TCP port for traffic going from the portal to the subscriber. Ethernet interface 0/0 is an interface that reaches the portal.

```
interface ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip portbundle outside
```

Related Commands

Command	Description
ip portbundle (global)	Enters portbundle configuration mode, in which ISG port-bundle host key parameters can be configured.
ip portbundle (service policy-map)	Enables the ISG Port-Bundle Host Key feature for a service
show ip portbundle ip	Displays information about a particular ISG port bundle.
show ip portbundle status	Displays information about ISG port-bundle groups.

ip route-cache

To control the use of switching methods for forwarding IP packets, use the **ip route-cache** command in interface configuration mode. To disable any of these switching methods, use the **no** form of this command.

ip route-cache [**cef | distributed | flow | policy | same-interface**]

no ip route-cache [**cef | distributed | flow | policy | same-interface**]

Syntax Description

cef	(Optional) Enables Cisco Express Forwarding operation on an interface.
distributed	(Optional) Enables distributed switching on the interface. (This keyword is not supported on the Cisco 7600 routers.) Distributed switching is disabled by default.
flow	(Optional) Enables NetFlow accounting for packets that are received by the interface. The default is disabled.
policy	(Optional) Enables fast-switching for packets that are forwarded using policy-based routing (PBR). Fast Switching for PBR (FSPBR) is disabled by default.
same-interface	(Optional) Enables fast-switching of packets onto the same interface on which they arrived.

Command Default

The switching method is not controlled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
11.1	The **flow** keyword was added.
11.2GS	The **cef** and **distributed** keywords were added.
11.1CC	**cef** keyword support was added for multiple platforms.
12.0	The **policy** keyword was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S. The **ip route-cache flow** command is automatically remapped to the **ip flow ingress** command.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB. This command is not supported on the Cisco 10000 series router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

IP Route Cache

Note The Cisco 10000 series routers do *not* support the **ip route-cache** command.

Using the route cache is often called *fast switching*. The route cache allows outgoing packets to be load-balanced on a *per-destination* basis rather than on a per-packet basis. The **ip route-cache** command with no additional keywords enables fast switching.

Entering the **ip route-cache** command has no effect on a subinterface. Subinterfaces accept the **no** form of the command; however, this disables Cisco Express Forwarding or distributed Cisco Express Forwarding on the physical interface and all subinterfaces associated with the physical interface

The default behavior for Fast Switching varies by interface and media.

Note IPv4 fast switching is removed with the implementation of the Cisco Express Forwarding infrastructure enhancements for Cisco IOS 12.2(25)S-based releases and Cisco IOS Release 12.4(20)T. For these and later Cisco IOS releases, switching path are Cisco Express Forwarding switched or process switched.

IP Route Cache Same Interface

You can enable IP fast switching when the input and output interfaces are the same interface, using the **ip route-cache same-interface** command. This configuration normally is not recommended, although it is useful when you have partially meshed media, such as Frame Relay or you are running Web Cache Communication Protocol (WCCP) redirection. You could use this feature on other interfaces, although it is not recommended because it would interfere with redirection of packets to the optimal path.

IP Route Cache Flow

The flow caching option can be used in conjunction with Cisco Express Forwarding switching to enable NetFlow, which allows statistics to be gathered with a finer granularity. The statistics include IP subprotocols, well-known ports, total flows, average number of packets per flow, and average flow lifetime.

Note The **ip route-cache flow** command has the same functionality as the **ip flow ingress** command, which is the preferred command for enabling NetFlow. If either the **ip route-cache flow** command or the **ip flow ingress** command is configured, both commands will appear in the output of the **show running-config** command.

IP Route Cache Distributed

The distributed option is supported on Cisco routers with line cards and Versatile Interface Processors (VIPs) that support Cisco Express Forwarding switching.

On Cisco routers with Route/Switch Processor (RSP) and VIP controllers, the VIP hardware can be configured to switch packets received by the VIP with no per-packet intervention on the part of the RSP. When VIP distributed switching is enabled, the input VIP interface tries to switch IP packets instead of forwarding them to the RSP for switching. Distributed switching helps decrease the demand on the RSP.

If the **ip route-cache distributed**, **ip cef distributed**, and **ip route-cache flow** commands are configured, the VIP performs distributed Cisco Express Forwarding switching and collects a finer granularity of flow statistics.

IP Route-Cache Cisco Express Forwarding

In some instances, you might want to disable Cisco Express Forwarding or distributed Cisco Express Forwarding on a particular interface because that interface is configured with a feature that Cisco Express Forwarding or distributed Cisco Express Forwarding does not support. Because all interfaces that support Cisco Express Forwarding or distributed Cisco Express Forwarding are enabled by default when you enable Cisco Express Forwarding or distributed Cisco Express Forwarding operation globally, you must use the **no** form of the **ip route-cache distributed** command in the interface configuration mode to turn Cisco Express Forwarding or distributed Cisco Express Forwarding operation off a particular interface.

Disabling Cisco Express Forwarding or distributed Cisco Express Forwarding on an interface disables Cisco Express Forwarding or distributed Cisco Express Forwarding switching for packets forwarded to the interface, but does not affect packets forwarded out of the interface.

Additionally, when you disable distributed Cisco Express Forwarding on the RSP, Cisco IOS software switches packets using the next-fastest switch path (Cisco Express Forwarding).

Enabling Cisco Express Forwarding globally disables distributed Cisco Express Forwarding on all interfaces. Disabling Cisco Express Forwarding or distributed Cisco Express Forwarding globally enables process switching on all interfaces.

Note On the Cisco 12000 series Internet router, you must not disable distributed Cisco Express Forwarding on an interface.

IP Route Cache Policy

If Cisco Express Forwarding is already enabled, the **ip route-cache route** command is not required because PBR packets are Cisco Express Forwarding-switched by default.

Before you can enable fast-switched PBR, you must first configure PBR.

FSPBR supports all of PBR's **match** commands and most of PBR's **set** commands, with the following restrictions:

- The **set ip default next-hop** and **set default interface** commands are not supported.
- The **set interface** command is supported only over point-to-point links, unless a route cache entry exists using the same interface specified in the **set interface** command in the route map. Also, at the process level, the routing table is consulted to determine if the interface is on a reasonable path to the destination. During fast switching, the software does not make this check. Instead, if the packet matches, the software blindly forwards the packet to the specified interface.

Note Not all switching methods are available on all platforms. Refer to the *Cisco Product Catalog* for information about features available on the platform you are using.

Examples

Configuring Fast Switching and Disabling Cisco Express Forwarding Switching

The following example shows how to enable fast switching and disable Cisco Express Forwarding switching:

```
Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache
```

The following example shows that fast switching is enabled:

```
Router# show ip interface fastEthernet 0/0/0
```

```
FastEthernet0/0/0 is up, line protocol is up
  Internet address is 10.1.1.254/24
  Broadcast address is 255.255.255.224
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Distributed switching is disabled
  IP Feature Fast switching turbo vector
  IP Null turbo vector
  IP multicast fast switching is enabled
```

The following example shows that Cisco Express Forwarding switching is disabled:

```
Router# show cef interface fastEthernet 0/0/0

FastEthernet0/0/0 is up (if_number 3)
  Corresponding hwidb fast_if_number 3
  Corresponding hwidb firstsw->if_number 3
  Internet address is 10.1.1.254/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  Hardware idb is FastEthernet0/0/0
  Fast switching type 1, interface type 18
  IP CEF switching disabled
  IP Feature Fast switching turbo vector
  IP Null turbo vector
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 1(1)
  Slot 0 Slot unit 0 VC -1
  Transmit limit accumulator 0x48001A02 (0x48001A02)
  IP MTU 1500
```

The following example shows the configuration information for interface fastethernet 0/0/0:

```
Router# show running-config
.
.
!
interface FastEthernet0/0/0
 ip address 10.1.1.254 255.255.255.0
 no ip route-cache cef
 no ip route-cache distributed
!
```

The following example shows how to enable Cisco Express Forwarding (and to disable distributed Cisco Express Forwarding if it is enabled):

```
Router(config-if)# ip route-cache cef
```

The following example shows how to enable VIP distributed Cisco Express Forwarding and per-flow accounting on an interface (regardless of the previous switching type enabled on the interface):

```
Router(config)# interface e0
Router(config-if)# ip address 10.252.245.2 255.255.255.0
Router(config-if)# ip route-cache distributed
Router(config-if)# ip route-cache flow
```

The following example shows how to enable Cisco Express Forwarding on the router globally (which also disables distributed Cisco Express Forwarding on any interfaces that are running distributed Cisco Express Forwarding), and disable Cisco Express Forwarding (which enables process switching) on Ethernet interface 0:

```
Router(config)# ip cef
Router(config)# interface e0
Router(config-if)# no ip route-cache cef
```

The following example shows how to enable distributed Cisco Express Forwarding operation on the router (globally), and disable Cisco Express Forwarding operation on Ethernet interface 0:

```
Router(config)# ip cef distributed
Router(config)# interface e0
Router(config-if)# no ip route-cache cef
```

The following example shows how to reenable distributed Cisco Express Forwarding operation on Ethernet interface 0:

```
Router(config)# ip cef distributed
Router(config)# interface e0
Router(config-if)# ip route-cache distributed
```

Configuring Fast Switching for Traffic That Is Received and Transmitted over the Same Interface

The following example shows how to enable fast switching and disable Cisco Express Forwarding switching:

```
Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache same-interface
```

The following example shows that fast switching on the same interface is enabled for interface fastethernet 0/0/0:

```
Router# show ip interface fastEthernet 0/0/0

FastEthernet0/0/0 is up, line protocol is up
  Internet address is 10.1.1.254/24
  Broadcast address is 255.255.255.224
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
```

```
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP Flow switching is disabled
  IP Distributed switching is disabled
  IP Feature Fast switching turbo vector
  IP Null turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  IP multicast multilayer switching is disabled
```

The following example shows the configuration information for interface fastethernet 0/0/0:

```
Router# show running-config
.
.
!
interface FastEthernet0/0/0
 ip address 10.1.1.254 255.255.255.0
 ip route-cache same-interface
 no ip route-cache cef
 no ip route-cache distributed
!
```

Enabling NetFlow Accounting

The following example shows how to enable NetFlow switching:

```
Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache flow
```

The following example shows that NetFlow accounting is enabled for interface fastethernet 0/0/0:

```
Router# show ip interface fastEthernet 0/0/0

FastEthernet0/0/0 is up, line protocol is up
  Internet address is 10.1.1.254/24
  Broadcast address is 255.255.255.224
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
```

```
  IP fast switching on the same interface is disabled
  IP Flow switching is enabled
  IP Distributed switching is disabled
  IP Flow switching turbo vector
  IP Null turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, Flow
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  IP multicast multilayer switching is disabled
```

Configuring Distributed Switching

The following example shows how to enable distributed switching:

```
Router(config)# ip cef distributed
Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache distributed
```

The following example shows that distributed Cisco Express Forwarding switching is for interface fastethernet 0/0/0:

```
Router# show cef interface fastEthernet 0/0/0

FastEthernet0/0/0 is up (if_number 3)
  Corresponding hwidb fast_if_number 3
  Corresponding hwidb firstsw->if_number 3
  Internet address is 10.1.1.254/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  Hardware idb is FastEthernet0/0/0
  Fast switching type 1, interface type 18
  IP Distributed CEF switching enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 1(1)
  Slot 0 Slot unit 0 VC -1
  Transmit limit accumulator 0x48001A02 (0x48001A02)
  IP MTU 1500
```

Configuring Fast Switching for PBR

The following example shows how to configure a simple policy-based routing scheme and to enable FSPBR:

```
Router(config)# access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)# route-map mypbrtag permit 10
Router(config-route-map)# match ip address 1
Router(config-route-map)# set ip next-hop 10.1.1.195
```

```
Router(config-route-map)# exit
Router(config)# interface fastethernet 0/0/0
Router(config-if)# ip route-cache policy
Router(config-if)# ip policy route-map mypbrtag
```

The following example shows that FSPBR is enabled for interface fastethernet 0/0/0:

```
Router# show ip interface fastEthernet 0/0/0

FastEthernet0/0/0 is up, line protocol is up
  Internet address is 10.1.1.254/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Distributed switching is enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, Distributed, Policy, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is enabled, using route map my_pbr_tag
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  IP multicast multilayer switching is disabled
```

Related Commands

Command	Description
exit	Leaves aggregation cache mode.
ip cef	Enables Cisco Express Forwarding on the RP card.
ip cef distributed	Enables distributed Cisco Express Forwarding operation.
ip flow ingress	Configures NetFlow on a subinterface.
show ip interface	Displays the usability status of interfaces configured for IP.
show cef interface	Displays detailed Cisco Express Forwarding information for interfaces.
show mpoa client	Displays the routing table cache used to fast switch IP traffic.

Command	Description
set ip default next-hop	Configures a default IP next hop for PBR.
set default interface	Configures a default interface for PBR.
set interface	Configures a specified interface for PBR.

ip source

To create a static session server source address, use the **ip source** command in server list configuration mode**.** To remove the static session server source address, use the **no** form of this command.

ip source *ip-address* [**mac** *mac-address* | **mask** *network-mask*]

no ip source *ip-address* [**mac** *mac-address* | **mask** *network-mask*]

Syntax Description

ip-address	Static session server ip-address.
mac *mac-address*	(Optional) Static session server mac address.
mask *mask-address*	(Optional) Static session server network mask.

Command Default

A static session server source address is not created.

Command Modes

Server list configuration (config-server-list)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The static session source address can be created only after creating an ip subscriber static server list name. The keyword **mask** needs to be used for routed interfaces and **mac** needs to be used for l2-connected interfaces.

Examples

In the following example a static session server source address for a routed interface list routed-server-list-name is created:

```
Router(config)# ip subscriber list my-connected-server-list
Router(config-server-list)# ip source 209.165.200.225 mask 255.255.255.224
```

Related Commands

Command	Description
ip subscriber list	Creates an ip subscriber static server list group name.

ip subscriber

To enable Intelligent Services Gateway (ISG) IP subscriber support on an interface and to specify the access method that IP subscribers will use to connect to ISG on an interface, use the **ip subscriber** command in interface configuration mode. To disable ISG IP session support on an interface, use the **no** form of this command.

ip subscriber {**l2-connected** | **routed**}

no ip subscriber {**l2-connected** | **routed**}

Syntax Description

l2-connected	Subscribers are either directly connected to an ISG physical interface or connected to ISG through a Layer 2 access network.
routed	Subscriber traffic is routed through a Layer 3 access network with at least one transit router before reaching ISG.

Command Default

An IP subscriber access method is not specified.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SB2	The **l2-connected** and **routed** keywords were added.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

One access method may be specified on an interface at a time.

The **ip subscriber** command enables IP subscriber configuration mode, in which the triggers for IP session initiation can be configured.

Use the **no ip subscriber** command to disable IP session support on the interface. Entering the **no ip subscriber** command removes the commands that were entered in IP subscriber configuration submode from the configuration. It also removes the **ip subscriber** command from the configuration. After the **no ip subscriber** command has been entered, no new IP sessions will be created on the interface. IP sessions that were already created will not be brought down, but ISG will not execute any features on those sessions.

Note For ATM interfaces, only point-to-point ATM interfaces support the **ip subscriber** command; it is not supported on multipoint ATM interfaces.

Examples

The following example shows how to configure ISG to create IP sessions for subscribers who connect to ISG on Gigabit Ethernet interface 0/1.401 through a Layer 2 connected access network. ISG will create IP sessions upon receipt of any frame with a valid source MAC address.

```
interface GigabitEthernet0/1.401
 ip subscriber l2-connected
  initiator unclassified mac-address
```

Related Commands

Command	Description
initiator	Enables ISG to create an IP subscriber session upon receipt of a specified type of packet.
ip subscriber interface	Creates an ISG IP interface session.

ip subscriber interface

To create an Intelligent Services Gateway (ISG) IP interface session, use the **ip subscriber interface** command in interface configuration mode. To remove the IP interface session, use the **no** form of this command.

ip subscriber interface

no ip subscriber interface

Syntax Description

This command has no keywords or arguments.

Command Default

An IP interface session is not created.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

An IP interface session includes all IP traffic received on a specific physical or virtual interface. IP interface sessions are provisioned through the command-line interface (CLI); that is, a session is created when the IP interface session commands are entered, and the session is continuous, even when the interface is shut down. By default, IP interface sessions come up in the state “unauthenticated” with full network access.

When access interfaces are used to identify IP subscribers, each access interface corresponds to a single IP subscriber. As soon as the access interface becomes available, ISG creates an IP session using the interface as the key, and associates all IP traffic coming into and going out of this interface to the IP session. For interface IP sessions, ISG classifies IP traffic as follows:

- When receiving IP traffic from the access network (upstream direction), ISG uses the input interface to retrieve the IP session.
- When receiving IP traffic from the core network (downstream direction), ISG uses the output interface to retrieve the IP session.

IP interface sessions might be used in situations in which a subscriber is represented by an interface (with the exception of PPP) and communicates using more than one IP address. For example, a subscriber using routed bridge encapsulation (RBE) access might have a dedicated ATM virtual circuit (VC) to home customer premises equipment (CPE) that is hosting multiple PCs.

Examples

The following example shows an IP interface session configured on Ethernet interface 0/0:

```
interface ethernet0/0
 ip subscriber interface
```

Related Commands

Command	Description
ip subscriber	Enables ISG IP subscriber support on an interface and specifies the access method that IP subscribers will use to connect to ISG on an interface.

ip subscriber list

To create an ip subscriber static server list group name, use the **ip subscriber list** command in global configuration mode**.** To remove a static server list group, use the **no** form of this command.

ip subscriber list *server-list-name*

no ip subscriber list *server-list-name*

Syntax Description

server-list-name	Name of the static session server list.

Command Default

A static session server list group is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Static sessions are removed for all interfaces associated with the current list when you exit the ip subscriber list mode. The **no ip subscriber list** command is rejected if the server list is used by any other interface.

Examples

In the following example a static server list group called my-connected-server-list is created:

```
Router(config)# ip subscriber list my-connected-server-list
```

Related Commands

Command	Description
ip source	Creates a static session server source address.
show ip subscriber	Displays information about Intelligent Services Gateway (ISG) IP subscriber sessions.
clear ip subscriber	Disconnects and removes all or specified ISG IP subscriber sessions.

ip vrf autoclassify

To enable Virtual Routing and Forwarding (VRF) autoclassify on a source interface, use the **ip vrf autoclassify** command in interface configuration mode. To remove VRF autoclassify, use the no form of this command.

ip vrf autoclassify source

no ip vrf autoclassify source

Syntax Description

source	Specifies that the VRF classification is automatically performed based on the source.

Command Default

The VFR autoclassify functionality is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(27)SBA	This command was introduced.

Usage Guidelines

The **ip vrf autoclassify** command enables the capability to map packets from connected hosts to VRFs that are different from the VRF defined on the ingress interface. It also enables the configuration of policies that are required for the mapping of packets to the VRFs depending on whether the source address of the packet belong to those connected routes.

The routing information can be learned dynamically or statically defined.

Examples

In the following example, the Fast Ethernet interface 0/0 is configured with two secondary addresses, 1.1.1.1/24 and 2.1.1.1/24. The first address, 1.1.1.1/24, is assigned to VRF red, while the other, 2.1.1.1/24, is assigned to VRF green. So in the VRF red table, a connected route 1.1.1.0/24 is installed, while in VRF green, 2.1.1.0/24 is installed:

```
interface fast ethernet0/0
 ip address 1.1.1.1 255.255.255.0 secondary vrf red
 ip address 2.1.1.1 255.255.255.0 secondary vrf green
 ip vrf autoclassify source
```

There is a default route in VRF red that directs all traffic to Fast Ethernet interface 1/0, while in VRF green, another default route directs all traffic to Fast Ethernet interface 1/1. When packets arrive at Fast Ethernet interface 0/0, they are mapped to either VRF red or VRF green based on their source address. If the source address is 1.1.1.2, connected route 1.1.1.0/24 is used, and the packet is mapped to VRF red. Following the default route, it is forwarded out of Fast Ethernet interface 1/0.

The return packets are mapped to the VRF configured on the downstream interface. Refer to the **ip vrf forwarding** command for more information in the *Cisco IOS Switching Services Command Reference*, Release 12.3T.

Related Commands

Command	Description
ip address	Enables the Cisco IOS software to both route and bridge a given protocol on separate interfaces within a single router.
ip vrf forwarding	Associates a VPN VRF with an interface or subinterface.
match ip source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
source route-map	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show ip interface	Displays the usability status of interfaces configured for IP.
show route-map	Displays static and dynamic route maps.

ip vrf forwarding (service policy map)

To associate a virtual routing/forwarding instance (VRF) with an Intelligent Services Gateway (ISG) service policy map, use the **ip vrf forwarding** command in service policy map configuration mode. To disassociate a VRF, use the **no** form of this command.

ip vrf forwarding *vrf-name*

no ip vrf forwarding *vrf-name*

Syntax Description

vrf-name	Associates the service with the specified VRF.

Command Default

A VRF is not specified.

Command Modes

Service policy map configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Use the **ip vrf forwarding** command to configure a network-forwarding policy for IP sessions in an ISG service policy map.

Examples

The following example shows a service policy map configured with a network-forwarding policy for IP sessions:

```
policy-map type service my_service
 ip vrf forwarding vrf1
```

Related Commands

Command	Description
ip route vrf	Establishes static routes for a VRF.
ip vrf	Configures a VRF routing table.
policy-map type service	Creates or modifies a service policy map, which is used to define an ISG service.

keepalive (ISG)

To enable keepalive packets and to specify their transmission attributes, use the **keepalive** command in service policy map configuration mode. To disable keepalive packets, use the **no** form of this command.

keepalive [**idle** *idle-seconds*] [**attempts** *max-retries*] [**interval** *retry-seconds*] [**protocol** {**ARP** | **ICMP** [**broadcast**]}]

no keepalive

Syntax Description

idle	(Optional) Specifies the interval a connection can remain without traffic before a keepalive packet is sent.
idle-seconds	(Optional) Maximum number of seconds that a connection can remain open with no traffic. Following the configured number of seconds without traffic, a packet is sent, to determine whether the connection should be maintained. The range and default value are platform and release-specific. For more information, use the question mark (**?**) online help function.
attempts	(Optional) Specifies the number of times a keepalive packet will be sent without a response before the connection is closed.
max-retries	(Optional) Maximum number of times that the ISG device will continue to send keepalive packets without response before closing the connection. The range and default value are platform and release-specific. For more information, use the question mark (**?**) online help function. If this value is omitted, the value that was previously set is used; if no value was specified previously, the default is used.
interval	(Optional) Specifies the time between attempts to send keepalive packets.
retry-seconds	(Optional) Number of seconds the ISG device will allow to elapse between keepalive packets. The range and default value are platform and release-specific. For more information, use the question mark (**?**) online help function.
protocol	(Optional) Specifies the protocol to be used for transmission of keepalive packets.
ARP	(Optional) Specifies the Address Resolution Protocol (ARP) to be used for keepalive packet inquries.
ICMP	(Optional) Specifies the Internet Control Message Protocol (ICMP) for keepalive packets.
broadcast	(Optional) Configures the ISG to send an ICMP broadcast packet to all IP addresses on a subnet.

Command Default

Keepalive messages are not enabled.

Command Modes

Service policy map configuration (config-service-policymap)

Command History

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

Usage Guidelines

If you enter only the **keepalive** command with no keywords or arguments, default values are set. Values are platform and release-specific. For more information, use the question mark (**?**) online help function.

Keepalive Message Protocol

For a directly connected host, ARP must be used. When the session is established and the keepalive feature is configured to use ARP, the keepalive feature saves the ARP entry as a valid original entry for verifying future ARP responses.

Note In cases where the access interface does not support ARP, the protocol for keepalives defaults to ICMP.

For routed hosts, you can configure ICMP as the protocol for keepalive messages. If ICMP is configured, the ICMP "hello" request is sent to the subscriber and checked for a response, until the configured maximum number of attempts is exceeded.

For IP subnet sessions, the peer (destination) IP address to be used for ICMP "hello" requests will be all the IP addresses within the subnet. This means "hello" requests will be sent sequentially (not simultaneously) to all the possible hosts within that subnet. If there is no response from any host in that subnet, the session will be disconnected.

There is an option to configure ICMP directed broadcast for keepalive requests. If the subscriber hosts recognize the IP subnet broadcast address, the ISG can send the ICMP "hello" request to the subnet broadcast address. The subscribers need not be on the same subnet as the ISG for this configuration to work. A directed broadcast keepalive request can work multiple hops away as long as the following conditions are satisfied:

- The group of subscribers identified by the subnet must have the same subnet mask provisioned locally as the subnet provisioned on the subnet subscriber session on the ISG. Otherwise, the subscriber hosts will not recognize the subnet broadcast address.
- The router directly connected to the hosts must enable directed-broadcast forwarding, so that the IP subnet broadcast gets translated into a Layer 2 broadcast.

When these two conditions are satisfied, you can optimize the ICMP keepalive configuration to minimize the number of ICMP packets.

Note Because enabling directed broadcasts increases the risk of denial of service (DOS) attacks, the use of subnet directed broadcasts is not turned on by default.

Examples

The following example shows how to set the idle time to 120 seconds with 5 retry attempts at 5 second intervals using ARP protocol. Examples of both On Box and AAA Server configurations are provided:

```
<On Box Configuration>
policy-map type service Keepalive
keepalive idle 120 attempts 5 interval 5 protocol ARP

<AAA Server Configuration>
vsa cisco generic 1 string "subscriber:keepalive=idle 120 attempts 5 interval 5 protocol
ARP"
```

key (ISG RADIUS proxy)

To configure the shared key between Intelligent Services Gateway (ISG) and a RADIUS proxy client, use the **key** command in RADIUS proxy server configuration mode or RADIUS proxy client configuration mode. To remove this configuration, use the **no** form of this command.

key [**0** | **7**] *word*

no key [**0** | **7**] *word*

Syntax Description

0	(Optional) An unencrypted key will follow.
7	(Optional) A hidden key will follow.
word	Unencrypted shared key.

Command Default

A shared key is not configured.

Command Modes

RADIUS proxy server configuration
RADIUS proxy client configuration

Command History

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

Usage Guidelines

The shared key can be specified globally for all RADIUS proxy clients, or it can be specified per client. The per-client configuration of this command overrides the global configuration.

Examples

The following example shows the configuration of global RADIUS proxy parameters and client-specific parameters for two RADIUS proxy clients. Because a shared secret is not configured specifically for client 10.1.1.1, it will inherit the shared secret specification, which is “cisco”, from the global RADIUS proxy configuration. Client 10.2.2.2 will use “systems” as the shared secret.

```
aaa server radius proxy
 key cisco
 client 10.1.1.1
  accounting port 1813
  authentication port 1812
!
 client 10.2.2.2
  key systems
!
```

Related Commands

Command	Description
aaa server radius proxy	Enables ISG RADIUS proxy configuration mode, in which ISG RADIUS proxy parameters can be configured.
client (ISG RADIUS proxy)	Enters ISG RADIUS proxy client configuration mode, in which client-specific RADIUS proxy parameters can be specified.

length (ISG)

To specify the Intelligent Services Gateway (ISG) port-bundle length, which determines the number of bundles per group and the number of ports per bundle, use the **length** command in portbundle configuration mode. To return the port-bundle length to the default value, use the **no** form of this command.

length *bits*

no length *bits*

Syntax Description

bits	Port-bundle length, in bits. The range is from 0 to 10 bits. The default is 4 bits.

Command Default

The port-bundle length has a default value of 4 bits.

Command Modes

Portbundle configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

The port-bundle length is used to determine the number of bundles in one group and the number of ports in one bundle. The number of ports in a bundle is the number of simultaneous TCP sessions that a subscriber can have. By default, the port-bundle length is 4 bits. The maximum port-bundle length is 10 bits. See Table 2 for available port-bundle length values and the resulting port-per-bundle and bundle-per-group values. Increasing the port-bundle length can be useful when you see frequent error messages about running out of ports in a port bundle, but note that the new value does not take effect until ISG next reloads and the portal server restarts.

Note You must configure the same port-bundle length on both the ISG device and the portal.

Table 2 Port-Bundle Lengths and Resulting Port-per-Bundle and Bundle-per-Group Values

Port-Bundle Length (in Bits)	Number of Ports per Bundle	Number of Bundles per Group (and per-SSG Source IP Address)
0	1	64512
1	2	32256
2	4	16128
3	8	8064
4 (default)	16	4032

Table 2 Port-Bundle Lengths and Resulting Port-per-Bundle and Bundle-per-Group Values (continued)

Port-Bundle Length (in Bits)	Number of Ports per Bundle	Number of Bundles per Group (and per-SSG Source IP Address)
5	32	2016
6	64	1008
7	128	504
8	256	252
9	512	126
10	1024	63

Examples

The following example results in 64 ports per bundle and 1008 bundles per group:

```
ip portbundle
 length 6
```

Related Commands

Command	Description
ip portbundle (global)	Enters portbundle configuration mode, in which ISG port-bundle host key parameters can be configured.
show ip portbundle ip	Displays information about a particular ISG port bundle.
show ip portbundle status	Displays information about ISG port-bundle groups.

less-than

To create a condition that will evaluate true if the subscriber network access server (NAS) port identifier is less than the specified value, use the **less-than** command in control class-map configuration mode. To remove the condition, use the **no** form of this command.

less-than [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}

no less-than [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}

Syntax Description

not	(Optional) Negates the sense of the test.
nas-port	NAS port identifier.
adapter *adapter-number*	Interface adapter number.
channel *channel-number*	Interface channel number.
ipaddr *ip-address*	IP address.
port *port-number*	Port number.
shelf *shelf-number*	Interface shelf number.
slot *slot-number*	Slot number.
sub-interface *sub-interface-number*	Subinterface number.
type *interface-type*	Interface type.
vci *vci-number*	Virtual channel identifier (VCI).
vlan *vlan-id*	VLAN ID.
vpi *vpi-number*	Virtual path identifier.

Command Default

A condition that will evaluate true if the subscriber network access server (NAS) port identifier is less than the specified value is not created.

Command Modes

Control class-map configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

The **less-than** command is used to configure a condition within a control class map. A control class map, which is configured with the **class-map type control** command, specifies conditions that must be met for a control policy to be activated, and, optionally, the event that causes the class to be evaluated. A

control class map can contain multiple conditions, each of which will evaluate to either true or false. Match directives can be used to specify whether all, any, or none of the conditions must evaluate true in order for the class as whole to evaluate true.

The **class type control** command is used to associate a control class map with a policy control map.

Examples

The following example shows a control class map that evaluates true for only a specific range of ATM permanent virtual circuit (PVC) VCIs, 101-104 inclusive:

```
class-map type type control match-any MY-CONDITION
 greater-than nas-port type atm vpi 200 vci 100
 less-than nas-port type atm vpi 200 vci 105
```

Related Commands

Command	Description
class-map type control	Creates an ISG control class map.
class type control	Specifies a control class for which actions may be configured in an ISG control policy map.
policy-map type control	Creates or modifies a control policy map, which defines an ISG control policy.

less-than-or-equal

To create a condition that will evaluate true if the subscriber network access server (NAS) port identifier is less than or equal to the specified value, use the **less-than-or-equal** command in control class-map configuration mode. To remove the condition, use the **no** form of this command.

less-than-or-equal [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}

no less-than-or-equal [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}

Syntax Description

not	(Optional) Negates the sense of the test.
nas-port	NAS port identifier.
adapter *adapter-number*	Interface adapter number.
channel *channel-number*	Interface channel number.
ipaddr *ip-address*	IP address.
port *port-number*	Port number.
shelf *shelf-number*	Interface shelf number.
slot *slot-number*	Slot number.
sub-interface *sub-interface-number*	Subinterface number.
type *interface-type*	Interface type.
vci *vci-number*	Virtual channel identifier.
vlan *vlan-id*	VLAN ID.
vpi *vpi-number*	Virtual path identifier.

Command Default

A condition that will evaluate true if the subscriber NAS port identifier is less than or equal to the specified value is not created.

Command Modes

Control class-map configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

The **less-than-or-equal** command is used to configure a condition within a control class map. A control class map, which is configured with the **class-map type control** command, specifies conditions that must be met for a control policy to be activated, and, optionally, the event that causes the class to be

evaluated. A control class map can contain multiple conditions, each of which will evaluate to either true or false. Match directives can be used to specify whether all, any, or none of the conditions must evaluate true in order for the class as whole to evaluate true.

The **class type control** command is used to associate a control class map with a policy control map.

Examples

The following example shows a control class map called "class3" configured with three conditions. The **match-all** keyword indicates that all of the conditions must evaluate true before the class evaluates true. The **class type control** command associates "class3" with the control policy map called "rule4".

```
class-map type control match-all class3
 less-than-or-equal nas-port port 1000
!
policy-map type control rule4
  class type control class3 event session-start
   1 authorize identifier nas-port
```

Related Commands

Command	Description
class-map type control	Creates an ISG control class map.
class type control	Specifies a control class for which actions may be configured in an ISG control policy map.
policy-map type control	Creates or modifies a control policy map, which defines an ISG control policy.