Cisco IOS Intelligent Services Gateway Command Reference

November 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Introduction

Intelligent Services Gateway (ISG) is a Cisco IOS software feature set that provides a structured framework that enables edge devices to deliver flexible and scalable services to subscribers. The *Cisco IOS Intelligent Services Gateway Command Reference* describes the commands that can be used to configure ISG functionality.

For more information about ISG, including configuration procedures and examples, see the *Cisco IOS Intelligent Services Gateway Configuration Guide*.

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. Default is 1, which is the highest priority.
class-map-name	Name of a previously configured traffic class map.
default	Specifies the default traffic class.
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 higher priority. If the traffic class priority has not been specified, packets are matched according to the order in which the services are installed.

The default traffic class map handles all the traffic that is not handled by other traffic classes in the service. The default class 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.

match access-group (ISG)

To configure the match criteria for an Intelligent Services Gateway (ISG) traffic class map on the basis of the specified access control list (ACL), use the **match access-group** command in traffic class-map configuration mode. To remove ACL match criteria from a class map, use the **no** form of this command.

match access-group {**input** | **output**} {*access-group* | **name** *access-group-name*}

no match access-group {**input** | **output**} {*access-group* | **name** *access-group-name*}

Syntax Description

input	Specifies match criteria for input traffic.
output	Specifies match criteria for output traffic.
access-group	A numbered ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class. An ACL number can be a number from 1 to 2799.
name *access-group-name*	A named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class. The name can be a maximum of 40 alphanumeric characters

Command Default

No match criteria are configured.

Command Modes

Traffic class-map configuration

Command History

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

Usage Guidelines

The **match access-group** command specifies a numbered or named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to the class. Packets satisfying the match criteria for a class constitute the traffic for that class.

To use the **match access-group** command for traffic classes, you must first enter the **class-map type traffic** command to specify the name of the traffic class whose match criteria you want to establish.

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.

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.

Examples

The following example configures a class map called “acl144” and specifies the ACL numbered 144 to be used as the input match criterion for this class:

```
class-map type traffic match-any acl144
 match access-group input 144
```

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
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-list

To specify packets for port-mapping by specifying an access list to compare against the subscriber traffic, use the **destination access-list** command in portbundle configuration mode. To remove this specification, use the **no** form of this command.

match access-list *access-list-number*

no match access-list *access-list-number*

Syntax Description

access-list-number	Integer from 100 to 199 that is the number or name of an extended access list.

Command Default

The Intelligent Services Gateway (ISG) port-maps all TCP traffic.

Command Modes

IP portbundle configuration

Command History

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

Usage Guidelines

You can use multiple entries of the **match access-list** command. The access lists are checked against the subscriber traffic in the order in which they are defined.

Examples

In the following example, the ISG will port-map packets that are permitted by access list 100:

```
ip portbundle
 match access-list 100
 source ip Ethernet0/0/0
!
.
.
.
!
access-list 100 permit ip 10.0.0.0 0.255.255.255 host 10.13.6.100
access-list 100 deny   ip any any
```

Related Commands

Command	Description
ip portbundle (service)	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.

match authen-status

To create a condition that will evaluate true if a subscriber's authentication status matches the specified authentication status, use the **match authen-status** command in control class-map configuration mode. To remove the condition, use the **no** form of this command.

match authen-status {**authenticated** | **unauthenticated**}

no match authen-status {**authenticated** | **unauthenticated**}

Syntax Description

authenticated	Subscriber has been authenticated.
unauthenticated	Subscriber has not been authenticated.

Command Default

A condition that will evaluate true if a subscriber's authentication status matches the specified authentication status is not created.

Command Modes

Control class-map configuration

Command History

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

Usage Guidelines

The **match authen-status** 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 the configuration of a policy timer that starts at session start for unauthenticated subscribers. When the timer expires, the session is disconnected.

```
class-map type type control match-all CONDA
 match authen-status unauthenticated
 match timer TIMERA

policy-map type control RULEA
 class type control always event session-start
  1 set-timer TIMERA 1 [minutes]
!
class type control CONDA event timed-policy-expiry
 1 service disconnect
```

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.

match authenticated-domain

To create a condition that will evaluate true if a subscriber's authenticated domain matches the specified domain, use the **match authenticated-domain** command in control class-map configuration mode. To remove the condition, use the **no** form of this command.

match authenticated-domain {*domain-name* | **regexp** *regular-expression*}

no match authenticated-domain

Syntax Description

domain-name	Domain name.
regexp *regular-expression*	Regular expression to be matched against subscriber's authenticated domain name.

Command Default

A condition that will evaluate true if a subscriber's authenticated domain matches the specified domain is not created.

Command Modes

Control class-map configuration

Command History

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

Usage Guidelines

The **match authenticated-domain** 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 creates a control class map that will evaluate true if a subscriber's domain matches the regular expression ".*com".

```
class-map type control match-all MY-CONDITION1
 match authenticated-domain regexp ".*com"
```

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.

match authenticated-username

To create a condition that will evaluate true if a subscriber's authenticated username matches the specified username, use the **match authenticated-username** command in control class-map configuration mode. To remove the condition, use the **no** form of this command.

match authenticated-username {*username* | **regexp** *regular-expression*}

no match authenticated-username {*username* | **regexp** *regular-expression*}

Syntax Description

username	Username
regexp *regular-expression*	Matches the regular expression against the subscriber's authenticated username.

Command Default

A condition is not created.

Command Modes

Control class-map configuration (config-control-classmap)

Command History

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

Usage Guidelines

The **match authenticated-username** command is used to configure a condition within an Intelligent Services Gateway (ISG) 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 evaluates to either true or false. Match directives can be used to specify whether all, any, or none of the conditions must evaluate true for the class as a 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 authenticated-username regexp "user@.*com"
   match authenticated-domain regexp ".*com"
!
policy-map type control rule4
  class type control class3 event session-start
   1 authorize identifier authenticated-username
```

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.

match dnis

To create a condition that will evaluate true if a subscriber's Dialed Number Identification Service number (DNIS number, also referred to as *called-party number*) matches the specified DNIS, use the **match dnis** command in control class-map configuration mode. To remove the condition, use the **no** form of this command.

match dnis {*dnis* | **regexp** *regular-expression*}

no match dnis {*dnis* | **regexp** *regular-expression*}

Syntax Description

dnis	DNIS number.
regexp *regular-expression*	Matches the regular expression against the subscriber's DNIS number.

Command Default

A condition that will evaluate true if a subscriber's DNIS number matches the specified DNIS is not created.

Command Modes

Control class-map configuration

Command History

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

Usage Guidelines

The **match dnis** command is used to configure a condition within an Intelligent Services Gateway (ISG) 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 dnis reg-exp 5550100
!
policy-map type control rule4
  class type control class3 event session-start
   1 authorize identifier dnis!
```

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.

match media

To create a condition that will evaluate true if a subscriber's access media type matches the specified media type, use the **match media** command in control class-map configuration mode. To remove the condition, use the **no** form of this command.

match media {**async** | **atm** | **ether** | **ip** | **isdn** | **mpls** | **serial**}

no match media {**async** | **atm** | **ether** | **ip** | **isdn** | **mpls** | **serial**}

Syntax Description

async	Asynchronous media.
atm	ATM.
ether	Ethernet.
ip	IP.
isdn	ISDN.
mpls	Multiprotocol Label Switching (MPLS).
serial	Serial.

Command Default

A condition that will evaluate true if a subscriber's access media type matches the specified media type is not created.

Command Modes

Control class-map configuration

Command History

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

Usage Guidelines

The **match media** command is used to configure a condition within an Intelligent Services Gateway (ISG) 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 configures a control class map that evaluates true for subscribers that enter the router through Ethernet interface slot 3.

```
class-map type control match-all MATCHING-USERS
 match media ether
 match nas-port type ether slot 3
```

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.

match mlp-negotiated

To create a condition that will evaluate true depending on whether or not a subscriber's session was established using multilink PPP negotiation, use the **match mlp-negotiated** command in control class-map configuration mode. To remove the condition, use the **no** form of this command.

match mlp-negotiated {**no** | **yes**}

no match mlp-negotiated {**no** | **yes**}

Syntax Description

no	The subscriber's session was not multilink PPP negotiated.
yes	The subscriber's session was multilink PPP negotiated.

Command Default

A condition is not created.

Command Modes

Control class-map configuration

Command History

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

Usage Guidelines

The **match mlp-negotiated** command is used to configure a condition within an Intelligent Services Gateway (ISG) 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 configured with the **match mlp-negotiated** command:

```
class-map type control match-all class3
   match mlp-negotiated yes
 !
 policy-map type control rule4
  class type control class3 event session-start
   1 authorize authenticated-username
```

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.

match nas-port

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

match nas-port {**adapter** *adapter-number* | **channel** *channel-number* | **circuit-id** *name* | **ipaddr** *ip-address* | **port** *port-number* | **remote-id** *name* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}

no match 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

adapter *adapter-number*	Interface adapter number.
channel *channel-number*	Interface channel number.
circuit-id *name*	Circuit ID
ipaddr *ip-address*	IP address.
port *port-number*	Port number.
remote-id *name*	Remote ID.
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 a subscriber's NAS port identifier matches 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 **match nas-port** command is used to configure a condition within an Intelligent Services Gateway (ISG) 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 configures a control class map that evaluates true on PPPoE subscribers that enter the router through Ethernet interface slot 3.

```
class-map type control match-all MATCHING-USERS
 class type control name NOT-ATM
 match media ether
 match nas-port type ether slot 3
```

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.

match no-username

To create a condition that will evaluate true if a subscriber’s username is available, use the **match no-username** command in control class-map configuration mode. To remove the condition, use the **no** form of this command.

match no-username {**no** | **yes**}

no match no-username {**no** | **yes**}

Syntax Description

no	The subscriber’s username is available.
yes	The subscriber’s username is not available.

Command Default

A condition that will evaluate true if a subscriber’s username is 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 **match no-username** command is used to configure a condition within an Intelligent Services Gateway (ISG) 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 configured with the **match no-username** command:

```
class-map type control match-all class3
   match no-username yes
 !
 policy-map type control rule4
  class type control class3 event session-start
   1 service local
```

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.

match protocol (ISG)

To create a condition that will evaluate true if a subscriber's access protocol type matches the specified protocol type, use the **match protocol** command in control class-map configuration mode. To remove the condition, use the **no** form of this command.

match protocol {**atom** | **ip** | **pdsn** | **ppp** | **vpdn**}

no match protocol {**atom** | **ip** | **pdsn** | **ppp** | **vpdn**}

Syntax Description

atom	Any Transport over MPLS (AToM).
ip	IP.
pdsn	Packet Data Serving Node (PDSN).
ppp	Point-to-Point Protocol (PPP).
vpdn	Virtual Private Dialup Network (VPDN).

Command Default

A condition that will evaluate true if a subscriber's access protocol type matches the specified protocol type is not created.

Command Modes

Control class-map configuration

Command History

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

Usage Guidelines

The **match protocol** command is used to configure a condition within an Intelligent Services Gateway (ISG) 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 creates a control class map that evaluates true if subscribers arrive from a VPDN tunnel:

```
class-map type control match-any MY-CONDITION
 match protocol vpdn
```

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.

match service-name

To create a condition that will evaluate true if the service name associated with a subscriber matches the specified service name, use the **match service-name** command in control class-map configuration mode. To remove the condition, use the **no** form of this command.

match service-name {*service-name* | **regexp** *regular-expression*}

no service-name {*service-name* | **regexp** *regular-expression*}

Syntax Description

service-name	Service name.
regexp *regular-expression*	Regular expression to be matched against subscriber's service name.

Command Default

A condition that will evaluate true if the service name associated with a subscriber matches the specified service name is not created.

Command Modes

Control class-map configuration

Command History

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

Usage Guidelines

The **match service-name** command is used to configure a condition within an Intelligent Services Gateway (ISG) 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 configures ISG to authenticate subscribers associated with the service before downloading the service:

```
aaa authentication login AUTHEN local
aaa authorization network SERVICE group radius
!
class-map type control match-any MY-CONDITION2
 match service-name "gold"
 match service-name "bronze"
 match service-name "silver"
!
policy-map type control MY-RULE2
 class type control MY-CONDITION2 event service-start
  1 authenticate aaa list AUTHEN
  2 service-policy type service aaa list SERVICE identifier service-name
!
service-policy type control MY-RULE2
```

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.

match source-ip-address

To create a condition that will evaluate true if a subscriber's source IP address matches the specified IP address, use the **match source-ip-address** command in control class-map configuration mode. To remove the condition, use the **no** form of this command.

match source-ip-address *ip-address subnet-mask*

no match source-ip-address *ip-address subnet-mask*

Syntax Description

ip-address	IP address.
subnet-mask	Subnet mask.

Command Default

A condition that will evaluate true if a subscriber's source IP address matches the specified IP address is not created.

Command Modes

Control class-map configuration

Command History

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

Usage Guidelines

The **match source-ip-address** command is used to configure a condition within an Intelligent Services Gateway (ISG) 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 source-ip-address 10.0.0.0 255.255.255.0
!
policy-map type control rule4
 class type control class3 event session-start
  1 authorize identifier source-ip-address
!
```

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.

match timer

To create a condition that will evaluate true when the specified timer expires, use the **match timer** command in control class-map configuration mode. To remove the condition, use the **no** form of this command.

match timer {*timer-name* | **regexp** *regular-expression*}

no match timer {*timer-name* | **regexp** *regular-expression*}

Syntax Description

timer-name	Name of the policy timer.
regexp *regular-expression*	Regular expression to be matched against the timer name.

Command Default

A condition that will evaluate true when the specified timer expires is not created.

Command Modes

Control class-map configuration

Command History

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

Usage Guidelines

The **match timer** command is used to configure a condition within an Intelligent Services Gateway (ISG) 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 the configuration of a policy timer that starts at session start for unauthenticated subscribers. When the timer expires, the session is disconnected.

```
class-map type control match-all CONDA
 match authen-status unauthenticated
 match timer TIMERA

policy-map type control RULEA
 class type control always event session-start
  1 set-timer TIMERA 1
!
class type control CONDA event timed-policy-expiry
 1 service disconnect
```

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.

match tunnel-name

To create a condition that will evaluate true if a subscriber’s Virtual Private Dialup Network (VPDN) tunnel name matches the specified tunnel name, use the **match tunnel-name** command in control class-map configuration mode. To remove the condition, use the **no** form of this command.

match tunnel-name {*tunnel-name* | **regexp** *regular-expression*}

no match tunnel-name {*tunnel-name* | **regexp** *regular-expression*}

Syntax Description

tunnel-name	VPDN tunnel name.
regexp *regular-expression*	Regular expression to be matched against the subscriber’s tunnel name.

Command Default

A condition that will evaluate true if a subscriber’s VPDN tunnel name matches the specified tunnel name is not created.

Command Modes

Control class-map configuration

Command History

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

Usage Guidelines

The **match tunnel-name** command is used to configure a condition within an Intelligent Services Gateway (ISG) 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 tunnel-name LAC
!
policy-map type control rule4
 class type control class3 event session-start
  1 authorize identifier tunnel-name
!
```

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.

match unauthenticated-domain

To create a condition that will evaluate true if a subscriber's unauthenticated domain name matches the specified domain name, use the **match unauthenticated-domain** command in control class-map configuration mode. To remove the condition, use the **no** form of this command.

match unauthenticated-domain {*domain-name* | **regexp** *regular-expression*}

no match unauthenticated-domain {*domain-name* | **regexp** *regular-expression*}

Syntax Description

domain-name	Domain name.
regexp *regular-expression*	Regular expression to be matched against subscriber's domain name.

Command Default

A condition that will evaluate true if a subscriber's unauthenticated domain name matches the specified domain name is not created.

Command Modes

Control class-map configuration

Command History

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

Usage Guidelines

The **match unauthenticated-domain** command is used to configure a condition within an Intelligent Services Gateway (ISG) 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 configures a control class map that evaluates true for subscribers with the unauthenticated domain "abc.com":

```
class-map type control match-all MY-FORWARDED-USERS
 match unauthenticated-domain "xyz.com"
```

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.

match unauthenticated-username

To create a condition that will evaluate true if a subscriber’s unauthenticated username matches the specified username, use the **match unauthenticated-username** command in control class-map configuration mode. To remove the condition, use the **no** form of this command.

match unauthenticated-username {*username* | **regexp** *regular-expression*}

no match unauthenticated-username {*username* | **regexp** *regular-expression*}

Syntax Description

username	Username.
regexp *regular-expression*	Regular expression to be matched against the subscriber’s username.

Command Default

A condition that will evaluate true if a subscriber’s unauthenticated username matches the specified username is not created.

Command Modes

Control class-map configuration

Command History

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

Usage Guidelines

The **match unauthenticated-username** command is used to configure a condition within an Intelligent Services Gateway (ISG) 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 identifier unauthenticated-username regexp "user@.*com"
!
policy-map type control rule4
  class type control class3 event session-start
   1 authorize identifier unauthenticated-username!
```

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.

match vrf

To create a condition that evaluates true if a subscriber's VPN routing and forwarding instance (VRF) matches the specified VRF, use the **match vrf** command in control class-map configuration mode. To remove this condition, use the **no** form of this command.

match vrf {*vrf-name* | **regexp** *regular-expression*}

no match vrf {*vrf-name* | **regexp** *regular-expression*}

Syntax Description

vrf-name	Name of the VRF.
regexp *regular-expression*	Regular expression to be matched against the subscriber's VRF.

Command Default

A condition that will evaluate true if a subscriber's VRF matches the specified VRF is not created.

Command Modes

Control class-map configuration

Command History

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

Usage Guidelines

The **match vrf** command is used to configure a condition within an Intelligent Services Gateway (ISG) 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 configures a policy that will be applied to subscribers who belong to the VRF "FIRST".

```
class-map type control TEST
 match vrf FIRST

policy-map type control GLOBAL
 class type control TEST event session-start
  1 service-policy type service name FIRST-SERVICE
```

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.

message-authenticator ignore

To disable message-authenticator validation of packets from RADIUS clients, use the **message-authenticator ignore** command in RADIUS proxy server configuration mode or RADIUS proxy client configuration mode. To reenable message-authenticator validation, use the **no** form of this command.

message-authenticator ignore

no message-authenticator ignore

Syntax Description

This command has no arguments or keywords.

Command Default

Message-authenticator validation is performed.

Command Modes

RADIUS proxy server configuration
RADIUS proxy client configuration

Command History

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

Usage Guidelines

Use the **message-authenticator ignore** command when validation of the source of RADIUS packets is not required or in situations in which a RADIUS client is not capable of filling the message-authenticator field in the RADIUS packet.

Examples

The following example disables message-authenticator validation:

```
aaa server radius proxy
 message-authenticator ignore
```

Related Commands

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

method-list

To specify the authentication, authorization, and accounting (AAA) method list to which the Intelligent Services Gateway (ISG) will send prepaid accounting updates or prepaid authorization requests, use the **method-list** command in ISG prepaid configuration mode. To reset to the default value, use the **no** form of this command.

method-list {**accounting** | **authorization**} *name-of-method-list*

no method-list {**accounting** | **authorization**}*name-of-method-list*

Syntax Description

accounting	Specifies the AAA method list for ISG prepaid accounting.
authorization	Specifies the AAA method list for ISG prepaid authorization.
name-of-method-list	Name of the AAA method list to which ISG will send accounting updates or authorization requests.

Command Default

A method list is not specified.

Command Modes

Prepaid configuration

Command History

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

Usage Guidelines

The AAA method list that is specified by the **method-list** command must be configured by using the **aaa accounting** command. See the *Cisco IOS Security Configuration Guide* for information about configuring AAA method lists, server groups, and servers.

Examples

The following example shows an ISG prepaid feature configuration in which a method list called “ap-mlist” is specified for prepaid accounting and the default method list is specified for prepaid authorization:

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

password (ISG)

To specify the password that the Intelligent Services Gateway (ISG) will use in authorization and reauthorization requests, use the **password** command in prepaid configuration mode. To reset the password to the default, use the **no** form of this command.

password *password*

no password *password*

Syntax Description

password	Password that the ISG will use in authorization and reauthorization requests. The default password is cisco.

Command Default

ISG uses the default password (cisco).

Command Modes

Prepaid configuration

Command History

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

Examples

The following example shows an ISG prepaid feature configuration in which the password is “pword” :

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

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.

police (ISG)

To configure Intelligent Services Gateway (ISG) policing, use the **police** command in service policy-map class configuration mode. To disable upstream policing, use the **no** form of this command.

police {**input** | **output**} *committed-rate* [*normal-burst excess-burst*]

no police {**input** | **output**} *committed-rate* [*normal-burst excess-burst*]

Syntax Description

input	Specifies policing of upstream traffic, which is traffic flowing from the subscriber toward the network.
output	Specifies policing of upstream traffic, which is traffic flowing from the network toward the subscriber.
committed-rate	Amount of bandwidth, in bits per second, to which a subscriber is entitled. Range is from 8000 to 1000000000.
normal-burst	(Optional) Normal burst size, in bytes. Range is from 1000 to 512000000. If the normal burst size is not specified, it is calculated from the committed rate using the following formula: Normal burst = 1.5 * committed rate (scaled and converted to byte per msec)
excess-burst	(Optional) Excess burst size, in bytes. Range is from 1000 to 512000000. If the excess burst is not specified, it is calculated from the normal burst value using the following formula: Excess burst = 2 * normal burst

Command Default

ISG policing is not enabled.

Command Modes

Service policy-map class configuration

Command History

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

Usage Guidelines

ISG policing supports policing of upstream and downstream traffic and can be applied to a session or a flow.

Session-based policing applies to the aggregate of subscriber traffic for a session.

Session-based policing parameters can be configured on a AAA server in either a user profile or a service profile that does not specify a traffic class. It can also be configured on the router in a service policy map by using the **police** command. Session-based policing parameters that are configured in a user profile take precedence over session-based policing parameters configured in a service profile or service policy map.

Flow-based policing applies only to the destination-based traffic flows that are specified by a traffic class.

Flow-based policing can be configured on a AAA server in a service profile that specifies a traffic class. It can also be configured on the router under a traffic class in a service policy map by using the **police** command. Flow-based policing and session-based policing can coexist and operate simultaneously on subscriber traffic.

Examples

The following example shows the configuration of flow-based ISG policing in a service policy map:

```
class-map type traffic match-any C3
 match access-group in 103
 match access-group out 203

policy-map type service P3
 class type traffic C3
  police input 20000 30000 60000
  police output 21000 31500 63000
```

Related Commands

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

policy-map

To enter policy-map configuration mode and create or modify a policy map that can be attached to one or more interfaces to specify a service policy, use the **policy-map** command in global configuration mode. To delete a policy map, use the **no** form of this command.

Supported Platforms Other Than Cisco 10000 and Cisco 7600 Series Routers

policy-map [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging** *log-policy*}] *policy-map-name*

no policy-map [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging** *log-policy*}] *policy-map-name*

Cisco 10000 Series Router

policy-map [**type** {**control** | **service**}] *policy-map-name*

no policy-map [**type** {**control** | **service**}] *policy-map-name*

Cisco 7600 Series Router

policy-map [**type** {**class-routing ipv4 unicast** *unicast-name* | **control** *control-name* | **service** *service-name*}] *policy-map-name*

no policy-map [**type** {**class-routing ipv4 unicast** *unicast-name* | **control** *control-name* | **service** *service-name*}] *policy-map-name*

Syntax Description

type	Specifies the policy-map type.
stack	(Optional) Determines the exact pattern to look for in the protocol stack of interest.
access-control	(Optional) Enables the policy map for the flexible packet matching feature.
port-filter	(Optional) Enables the policy map for the port-filter feature.
queue-threshold	(Optional) Enables the policy map for the queue-threshold feature.
logging	(Optional) Enables the policy map for the control-plane packet logging feature.
log-policy	Type of log policy for control-plane logging.
policy-map-name	Name of the policy map. The name can be a maximum of 40 alphanumeric characters.
control	(Optional) Creates a control policy map.
control-name	Specifies the name of the control policy map.
service	(Optional) Creates a service policy map.
service-name	Specifies the policy-map service name.
class-routing	Configures the class-routing policy map.
ipv4	Configures the class-routing IPv4 policy map.

unicast	Configures the class-routing IPv4 unicast policy map.
unicast-name	Unicast policy-map name.

Command Default

The policy map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.4(4)T	The **type access-control** keywords were added to support flexible packet matching. The **type port-filter** and **type queue-threshold** keywords were added to support control-plane protection.
12.4(6)T	The **type logging** keywords were added to support control-plane packet logging.
12.2(31)SB	The **type control** and **type service** keywords were added to support the Cisco 10000 series router.
12.2(18)ZY	The following modifications were made to the **policy-map** command: • The **type access-control** keywords were integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series switch that is equipped with the Supervisor 32/programmable intelligent services accelerator (PISA) engine. • The command was modified to enhance Network-Based Application Recognition (NBAR) functionality on the Catalyst 6500 series switch that is equipped with the Supervisor 32/PISA engine.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	Support for this command was implemented on Cisco 7600 series routers.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

Use the **policy-map** command to specify the name of the policy map to be created, added to, or modified before you configure policies for classes whose match criteria are defined in a class map. The **policy-map** command enters policy-map configuration mode, in which you can configure or modify the class policies for a policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. Use the **class-map** and **match** commands to configure the match criteria for a class. Because you can configure a maximum of 64 class maps, a policy map cannot contain more than 64 class policies, except as noted for Quality of Service (QoS) class maps on Cisco 7600 systems.

Note For QoS class maps on Cisco 7600 systems, the limits are 1024 class maps and 256 classes in a policy map.

A single policy map can be attached to more than one interface concurrently. Except as noted, when you attempt to attach a policy map to an interface, the attempt is denied if the available bandwidth on the interface cannot accommodate the total bandwidth requested by class policies that make up the policy map. In this case, if the policy map is already attached to other interfaces, it is removed from them.

Note This limitation does not apply on Cisco 7600 systems that have SIP-400 access-facing line cards.

Whenever you modify class policy in an attached policy map, class-based weighted fair queueing (CBWFQ) is notified and the new classes are installed as part of the policy map in the CBWFQ system.

Note Policy-map installation via subscriber-profile is not supported. If you configure an unsupported policy map and there are a large number of sessions, then an equally large number of messages print on the console. For example, if there are 32,000 sessions, then 32,000 messages print on the console at 9,600 baud.

Class Queues (Cisco 10000 Series Routers Only)

The PRE2 allows you to configure 31 class queues in a policy map.

In a policy map, the PRE3 allows you to configure one priority level 1 queue, one priority level 2 queue, 12 class queues, and one default queue.

Control Policies (Cisco 10000 Series Routers Only)

Control policies define the actions that your system will take in response to specified events and conditions.

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.

There are three steps involved in defining a control policy:

1. Using the **class-map type control** command, create one or more control class maps.
2. Using the **policy-map type control** command, create a control policy map.

   A control policy map contains one or more control policy rules. A control policy rule associates a control class map with one or more actions. Actions are numbered and executed sequentially.
3. Using the **service-policy type control** command, apply the control policy map to a context.

Service Policies (Cisco 10000 Series Routers Only)

Service policy maps and service profiles contain a collection of traffic policies and other functionality. Traffic policies determine which functionality will be applied to which session traffic. A service policy map or service profile may also contain a network-forwarding policy, which is a specific type of traffic policy that determines how session data packets will be forwarded to the network.

Policy Map Restrictions (Catalyst 6500 Series Switches Only)

Cisco IOS Release 12.2(18)ZY includes software intended for use on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine. For this release and platform, note the following restrictions for using policy maps and **match** commands:

- You cannot modify an existing policy map if the policy map is attached to an interface. To modify the policy map, remove the policy map from the interface by using the **no** form of the **service-policy** command.
- Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) on the basis of a protocol type or application. You can create as many traffic classes as needed. However, the following restrictions apply:
  - A single traffic class can be configured to match a maximum of 8 protocols or applications.
  - Multiple traffic classes can be configured to match a cumulative maximum of 95 protocols or applications.

Examples

The following example creates a policy map called "policy1" and configures two class policies included in that policy map. The class policy called "class1" specifies policy for traffic that matches access control list (ACL) 136. The second class is the default class to which packets that do not satisfy configured match criteria are directed.

```
! The following commands create class-map class1 and define its match criteria:
class-map class1
 match access-group 136

! The following commands create the policy map, which is defined to contain policy
! specification for class1 and the default class:
policy-map policy1

class class1
 bandwidth 2000
 queue-limit 40

class class-default
 fair-queue 16
 queue-limit 20
```

The following example creates a policy map called "policy9" and configures three class policies to belong to that map. Of these classes, two specify policy for classes with class maps that specify match criteria based on either a numbered ACL or an interface name, and one specifies policy for the default class called "class-default" to which packets that do not satisfy configured match criteria are directed.

```
policy-map policy9

class acl136
 bandwidth 2000
 queue-limit 40

class ethernet101
 bandwidth 3000
 random-detect exponential-weighting-constant 10

class class-default
 fair-queue 10
 queue-limit 20
```

The following is an example of a modular QoS command-line interface (MQC) policy map configured to initiate the QoS service at the start of a session.

```
Router> enable
Router# configure terminal
Router(config)# policy-map type control TEST
Router(config-control-policymap)# class type control always event session-start
Router(config-control-policymap-class-control)# 1 service-policy type service name
QoS_Service
Router(config-control-policymap-class-control)# end
```

Examples for Cisco 10000 Series Routers Only

The following example shows the configuration of a control policy map named “rule4”. Control policy map rule4 contains one policy rule, which is the association of the control class named “class3” with the action to authorize subscribers using the network access server (NAS) port ID. The **service-policy type control** command is used to apply the control policy map globally.

```
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
!
service-policy type control rule4
```

The following example shows the configuration of a service policy map named “redirect-profile”:

```
policy-map type service redirect-profile
 class type traffic CLASS-ALL
  redirect to group redirect-sg
```

policy-map type control

To create or modify a control policy map, which defines an Intelligent Services Gateway (ISG) control policy, use the **policy-map type control** command in global configuration mode. To delete the control policy map, use the **no** form of this command.

policy-map type control *policy-map-name*

no policy-map type control *policy-map-name*

Syntax Description

policy-map-name	Name of the control policy map.

Command Default

A control policy map is not created.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Control policies define the actions that your system will take in response to specified events and conditions.

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.

There are three steps involved in defining a control policy:

1. Create one or more control class maps, by using the **class-map type control** command.
2. Create a control policy map, using the **policy-map type control** command.

   A control policy map contains one or more control policy rules. A control policy rule associates a control class map with one or more actions. Actions are numbered and executed sequentially.
3. Apply the control policy map to a context, using the **service-policy type control** command.

Examples

The following example shows the configuration of a control policy map called “rule4.” Control policy map “rule4” contains one policy rule, which is the association of the control class “class3” with the action to authorize subscribers using the network access server (NAS) port ID. The **service-policy type control** command is used to apply the control policy map globally.

```
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
!
service-policy type control rule4
```

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.
service-policy type control	Applies a control policy to a context.

policy-map type service

To create or modify a service policy map, which is used to define an Intelligent Services Gateway (ISG) subscriber service, use the **policy-map type service** command in global configuration mode. To delete a service policy map, use the **no** form of this command.

policy-map type service *policy-map-name*

no policy-map type service

Syntax Description

policy-map-name	Name of the service policy map.

Command Default

A service policy map is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS Release XE 2.4.

Usage Guidelines

Use the **policy-map type service** command to create or modify an ISG service policy map. Service policy maps define ISG subscriber services.

An ISG service is a collection of policies that may be applied to a subscriber session. Services can be defined in service policy maps and 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 an authentication, authorization, and accounting (AAA) server.

Service policy maps and service profiles contain a collection of traffic policies and other functionality. Traffic policies determine which functionality will be applied to which session traffic. A service policy map or service profile may also contain a network-forwarding policy, a specific type of traffic policy that determines how session data packets will be forwarded to the network.

Examples

The following example shows how to create a service policy map called redirect-profile:

```
policy-map type service redirect-profile
 class type traffic CLASS-ALL
  redirect to group redirect-sg
```

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	Displays the contents of all service policy maps.

policy-name

To configure a subscriber policy name, use the **policy-name** command in service policy map configuration mode. To remove a subscriber policy name, use the **no** form of this command.

policy-name *policy*

no policy-name *policy*

Syntax Description

policy	Name of policy configured on the Service Control Engine (SCE) device.

Command Default

The default policy is used for all subscribers.

Command Modes

Service policy map configuration (config-service-policymap)

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 **policy-name** command is used with the **policy-map type service** command and must be configured together with the **sg-service-type external-policy** command. The policy name configured on the Intelligent Services Gateway (ISG) device must be the name of an existing policy that has already been configured on the SCE device.

Examples

The following example shows how to configure the subscriber policy name “SCE-SERVICE”.

```
Router(config)# policy-map type service SCE-SERVICE
Router(config-service-policymap)# sg-service-type external-policy
Router(config-service-policymap)# policy-name GOLD
```

Related Commands

Command	Description
sg-service-type external-policy	Identifies a service as an external policy.

policy-peer

To configure a subscriber policy peer connection, use the **policy-peer** command in global configuration mode. To remove a subscriber policy peer connection, use the **no** form of this command.

policy-peer [**address** *ip-address*] {**keepalive** *seconds*}

no policy-peer [**address** *ip-address*] {**keepalive** *seconds*}

Syntax Description

address	(Optional) Configures the IP address of the peer that is to be connected.
ip-address	Specifies the IP address of the peer to be connected.
keepalive	Configures the keepalive value to be used to monitor the peering relationship.
seconds	Keepalive value, in seconds. Range: 5 to 3600. Default: 0.

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 Release 12.2(33)SB.

Usage Guidelines

Use the **keepalive** keyword with the **policy-peer** command to monitor the peering relationship between the Intelligent Services Gateway (ISG) device and the Service Control Engine (SCE). When the ISG and SCE establish a peering relationship, they negotiate the lowest **keepalive** value between them. If the ISG **keepalive** value is set to zero (0), the ISG accepts the value proposed by the SCE. The SCE sends **keepalive** packets at specified intervals. If twice the time specified by the *seconds* argument goes by without the ISG receiving a **keepalive** packet from the SCE, the peering relationship is ended. The ISG ignores any messages from the SCE unless they are messages to establish peering.

Examples:

The following example configures a subscriber policy peer connection with a keepalive value of 5 seconds.

```
Router(config)# policy-peer address 10.0.0.100 keepalive 5
```

Related Commands

Command	Description
aaa server radius policy-device	Enables ISG RADIUS server configuration mode.
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.

port

To specify the port on which a device listens for RADIUS requests from configured RADIUS clients, use the **port** command in dynamic authorization local server configuration mode. To restore the default, use the **no** form of this command.

port *port-number*

no port *port-number*

Syntax Description

port-number	Port number. The default value is port 1700.

Command Default

The device listens for RADIUS requests on the default port (port 1700).

Command Modes

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

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 **port** command to specify the ports on which the router will listen for requests from RADIUS clients.

Examples

The following example specifies port 1650 as the port on which the device listens for RADIUS requests:

```
aaa server radius dynamic-author
 client 10.0.0.1
 port 1650
```

Related Commands

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

prepaid config

To enable prepaid billing for an Intelligent Services Gateway (ISG) service and to reference a configuration of prepaid billing parameters, use the **prepaid config** command in service policy traffic class configuration mode. To disable prepaid billing for a service, use the **no** form of this command.

prepaid config {*name-of-configuration* | **default**}

no prepaid config {*name-of-configuration* | **default**}

Syntax Description

name-of-configuration	A named configuration of prepaid billing parameters.
default	The default configuration of prepaid billing parameters.

Command Default

Prepaid billing is not enabled.

Command Modes

Service policy traffic class configuration

Command History

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

Usage Guidelines

ISG prepaid billing is enabled in a service policy map on the router by entering the **prepaid config** command, or in a service profile on the authentication, authorization, and accounting (AAA) server by using the prepaid vendor-specific attribute (VSA). The **prepaid config** command and prepaid VSA reference a configuration that contains specific prepaid billing parameters.

To create or modify a prepaid billing parameter configuration, use the **subscriber feature prepaid** command to enter prepaid configuration mode. A default prepaid configuration exists with the following parameters:

```
subscriber feature prepaid default
 threshold time 0 seconds
 threshold volume 0 bytes
 method-list authorization default
 method-list accounting default
 password cisco
```

The default configuration will not show up in the output of the **show running-config** command unless you change any one of the parameters.

The parameters of named prepaid configurations are inherited from the default configuration, so if you create a named prepaid configuration and want only one parameter to be different from the default configuration, you have to configure only that parameter.

Examples

The following example shows prepaid billing enabled in a service called “mp3”. The prepaid billing parameters in the configuration “conf-prepaid” will be used for “mp3” prepaid sessions.

```
policy-map type service mp3
 class type traffic CLASS-ACL-101
  authentication method-list cp-mlist
  accounting method-list cp-mlist
  prepaid config conf-prepaid

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

Related Commands

Command	Description
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.

proxy (ISG RADIUS proxy)

To configure an Intelligent Services Gateway (ISG) device to send RADIUS packets to a method list, use the **proxy** command in control policy-map class configuration mode. To remove this action from the control policy, use the **no** form of this command.

action-number **proxy** [**aaa list** {*list-name* | **default**}] [**accounting aaa list** *acc-list-name*]

no *action-number* **proxy** [**aaa list** {*list-name* | **default**}] [**accounting aaa list** *acc-list-name*]

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.
aaa list	(Optional) Specifies that RADIUS packets will be sent to an authentication, authorization, and accounting (AAA) method list.
list-name	Name of the AAA method list to which RADIUS packets are sent.
default	Specifies that RADIUS packets will be sent to the default RADIUS server.
accounting aaa list	Defines a method list to which accounting is sent.
acc-list-name	Name of the accounting AAA method list to which RADIUS packets are sent.

Command Default

RADIUS packets are sent to the default method list.

Command Modes

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

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	The **accounting aaa list** keyword was added.
12.2(33)SB	This command was implemented on the Cisco 10000 series.

Usage Guidelines

The **proxy** command is used to configure a control policy that causes ISG to forward RADIUS packets to a specified AAA method list. The method list must be configured with the **aaa accounting** command.

Control policies define the actions that the system takes in response to specified events and conditions. A control policy is made up 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.

The **accounting aaa list** keyword is used configure the ISG device to forward incoming accounting requests from the SCE device to the AAA server.

Examples

The following example configures an accounting method list called “LIST-LOCAL”. The server group called “AAA-GROUP1” is the method specified in the method list. A control policy called “POLICY-LOCAL” is configured with a policy rule that causes ISG to forward SCE accounting packets to the server group defined in method list “LIST-LOCAL”.

```
Router(config)# aaa accounting network LIST-LOCAL start-stop group AAA-GROUP1
Router(config)# policy-map type control POLICY-LOCAL
Router(config-control-policymap)# class type control always event acct-notification
Router(config-control-policymap-class)# 1 proxy accounting aaa list LIST-LOCAL
```

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.

proxy (RADIUS proxy)

To configure Intelligent Services Gateway (ISG) to send RADIUS packets to a method list, use the **proxy** command in control policy-map class configuration mode. To remove this action from the control policy, use the **no** form of this command.

action-number **proxy** [**aaa list** {*list-name* | **default**}]

no *action-number* **proxy** [**aaa list** {*list-name* | **default**}

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.
aaa list	(Optional) Specifies that RADIUS packets will be sent to an authentication, authorization, and accounting (AAA) method list.
list-name	Name of the AAA method list to which RADIUS packets are sent.
default	Specifies that RADIUS packets will be sent to the default RADIUS server.

Command Default

RADIUS packets are sent to the default method list.

Command Modes

Control policy-map class configuration

Command History

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

Usage Guidelines

The **proxy** command is used to configure a control policy that causes ISG to forward RADIUS packets to a specified AAA method list. The method list must be configured with the **aaa authorization radius-proxy** command.

Control policies define the actions the system takes in response to specified events and conditions. 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 configures an ISG RADIUS proxy authorization method list called “RP”. The server group called “EAP” is the method specified in that method list. A control policy called “PROXYRULE” is configured with a policy rule that causes ISG to forward RADIUS packets to the method list “RP”.

```
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 radius-proxy	Configures AAA authorization methods for ISG RADIUS proxy subscribers.
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.

radius-server attribute 31

To configure Calling-Station-ID (attribute 31) options, use the **radius-server attribute 31** command in global configuration mode. To disable the Calling-Station-ID (attribute 31) options, use the **no** form of this command.

radius-server attribute 31 {**append-circuit-id** | **mac format** {**default** | **ietf** | **unformatted**} | **remote-id** | **send nas-port-detail** [**mac-only**]}

no radius-server attribute 31 {**append-circuit-id** | **mac format** {**default** | **ietf** | **unformatted**} | **remote-id** | **send nas-port-detail** [**mac-only**]}

Syntax Description

append-circuit-id	Appends the PPPoE tag circuit-id and the nas-port-id to the calling-station-id.
mac format	Specifies the format of the MAC address in the Calling Station ID. Select one of the following three options: • **default** (Example: 0000.4096.3e4a) • **ietf** (Example: 00-00-40-96-3E-4A) • **unformatted** (Example: 000040963e4a)
remote-id	Sends the remote ID as the Calling Station ID in the accounting records and access requests.
send nas-port-detail	Includes all NAS port details in the Calling Station ID.
mac-only	(Optional) Includes the MAC address only, if available, in the Calling Station ID.

Command Default

The Calling-Station-ID (attribute 31) is not sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SB2	The **mac format default**, the **mac format ietf**, the **mac format unformatted**, and the **send nas-port-detail** [**mac-only**] keyword options were added.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

- For PPP over Ethernet over ATM (PPPoEoA) sessions:

  When the **send nas-port-detail** keyword and the **mac-only** option are configured, the Calling-Station-ID (attribute 31) information is sent in Access and Accounting requests in the following format:

  ```
  host.domain:vp_descr:vpi:vci
  ```

- For PPP over Ethernet over Ethernet (PPPoEoE) sessions:

  When the **send nas-port-detail** keyword and the **mac-only** option are configured, the Calling-Station-ID (attribute 31) information is sent in Access and Accounting requests in the following format:

  ```
  mac_addr
  ```

- For PPP over ATM sessions:

  When the **send nas-port-detail** keyword and the **mac-only** option are configured, the Calling-Station-ID (attribute 31) information is sent in Access and Accounting requests in the following format:

  ```
  host.domain:vp_descr:vpi:vci
  ```

- For Intelligent Services Gateway RADIUS Proxy sessions:

  When DHCP lease query is used, ISG RADIUS proxy recieves MAC address as well as MSISDN as the Calling-Station-ID (attribute 31) from the downstream device. Therefore, ISG RADIUS proxy must be configured to choose one of them as the Calling Station ID and send it to the ISG accounting records.

The following example shows how to specify the MAC address in the Calling Station ID to be displayed in IETF format:

```
Router(config)# radius-server attribute 31 mac format ietf
```

The following example shows how to allow the remote ID to be sent as the Calling Station ID:

```
Router(config)# radius-server attribute 31 remote-id
```

The following example shows how to allow the NAS port details to be included in the Calling Station ID:

```
Router(config)# radius-server attribute 31 send nas-port-detail
```

The following example shows how to allow only the MAC address, if available, to be included in the Calling-Station-ID:

```
Router(config)# radius-server attribute 31 send nas-port-detail mac-onl
```

Related Commands

Command	Description
radius-server attribute nas-port-id include	Uses the DHCP relay agent information option 60 and option 82 and configures the NAS-Port-ID to authenticate a user.

radius-server attribute nas-port-id include

To include DHCP option 60 and option 82 (that is, any combination of circuit ID, remote ID, and vendor-class ID) in the NAS-Port-ID to authenticate a user, use the **radius-server attribute nas-port-id include** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

radius-server attribute nas-port-id include {*identifier1* [**plus** *identifier2*] [**plus** *identifier3*]} [**separator** *separator*]

no radius-server attribute nas-port-id include

Syntax Description

identifier1,2,3	Identifier for authorization. Valid keywords are: • **circuit-id** • **remote-id** • **vendor-class-id**
plus	(Optional) Separates identifiers if more than one is specified.
separator *separator*	(Optional) Symbol to be used for separating identifiers in accounting records and authentication requests. The symbol can be any alphanumeric character. The colon (:) is the default separator.

Command Default

The NAS-Port-ID is populated with the Intelligent Services Gateway (ISG) interface that received the DHCP relay agent information packet; for example, Ethernet1/0.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRD	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

When you use the **radius-server attribute nas-port-id include** command, you must specify at least one ID. You can use a single ID or any combination of the three, in any order. If you use more than one ID, use the **plus** keyword between each pair as a separator.

The NAS-Port-ID is shown in the accounting records as it is specified in this command, with the **plus** keyword replaced by a separator. The colon (:) is the default separator.

When the NAS-Port-ID is selected as the identifier for authorization, the NAS-Port-ID is sent as part of the username in the authentication request. It is sent as specified in this command, preceded by the string "nas-port:".

Examples

The following example shows an authentication request that specifies a circuit ID, a remote ID, and a vendor-class ID:

```
Router(config)# radius-server attribute nas-port-id include circuit-id plus remote-id plus
vendor-class-id
```

If the circuit ID is “xyz”, the remote ID is “abc”, and the vendor-class ID is “123”, the NAS-Port-ID will be sent to the accounting records as “abc:xyz:123” and the username will be sent as “nas-port:abc:xyz:123” in the authentication request.

The following example shows an authentication request that specifies a circuit ID and a vendor-class ID and also specifies a separator, “#”:

```
Router(config)# radius-server attribute nas-port-id include circuit-id plus
vendor-class-id separator #
```

If the circuit ID is “xyz” and the vendor-class ID is “123”, the NAS-Port-ID will be sent to the accounting records as “xyz#123” and the username will be sent as “nas-port:xyz#123” in the authentication request.

Related Commands

Command	Description
authorize identifier	Initiates a request for authorization based on a specified identifier in an ISG control policy.

redirect server-group

To define a group of one or more servers that make up a named Intelligent Services Gateway (ISG) Layer 4 redirect server group, use the **redirect server-group** command in global configuration mode. To remove a redirect server group and any servers configured within that group, use the **no** form of this command.

redirect server-group *group-name*

no server-group *group-name*

Syntax Description

group-name	Name of the server group.

Command Default

A redirect server group is not defined.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **redirect server-group** command to define and name an ISG Layer 4 redirect server group. Packets sent upstream from an unauthenticated subscriber can be forwarded to the server group, which will deal with the packets in a suitable manner, such as routing them to a logon page. You can also use server groups to handle requests from authorized subscribers who request access to services to which they are not logged in and for advertising captivation.

After defining a redirect server group with the **redirect server-group** command, identify individual servers for inclusion in the server group using the **server** command in Layer 4 redirect server group configuration mode.

Examples

The following example shows the configuration of a server group called “PORTAL”:

```
redirect server-group PORTAL
 server ip 10.2.36.253 port 80
```

Related Commands

Command	Description
redirect to (ISG)	Redirects ISG Layer 4 traffic to a specified server or server group.
server	Adds a server to an ISG Layer 4 redirect server group.
show redirect group	Displays information about ISG Layer 4 redirect server groups.
show redirect translations	Displays information about the ISG Layer 4 redirect mappings for subscriber sessions.

redirect session-limit

To set the maximum number of Layer 4 redirects allowed for each Intelligent Services Gateway (ISG) subscriber session, use the **redirect session-limit** command in global configuration mode. To reset to the default, use the **no** form of this command.

redirect session-limit *maximum-number*

no redirect session-limit

Syntax Description

maximum-number	The maximum number of Layer 4 redirects allowed. Range: 1 to 256.

Command Default

An unlimited number of redirects are allowed per session.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SB8	This command was introduced.
12.2(33)XNE1	This command was integrated into Cisco IOS Release 12.2(33)XNE1.
12.2(33)SRD4	This command was integrated into Cisco IOS Release 12.2(33)SRD4.
12.2(33)SRE1	This command was integrated into Cisco IOS Release 12.2(33)SRE1.

Usage Guidelines

The **redirect session-limit** command limits the number of redirect translations that can be created by unauthenticated subscribers that are redirected to the server group.

Examples

The following example limits the number of L4 redirects to five for a single session:

```
Router(config)# redirect session-limit 5
```

Related Commands

Command	Description
redirect server-group	Defines a group of one or more servers that make up a named ISG Layer 4 redirect server group.
redirect to (ISG)	Redirects ISG Layer 4 traffic to a specified server or server group.
show redirect translations	Displays information about the ISG Layer 4 redirect mappings for subscriber sessions.

redirect to (ISG)

To redirect Intelligent Services Gateway (ISG) Layer 4 traffic to a specified server or server group, use the **redirect to** command in service policy-map class configuration mode. To disable redirection, use the **no** form of this command.

redirect to {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]} [**duration** *seconds* [**frequency** *seconds*]]

no redirect [**list** *access-list-number*] **to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]} [**duration** *seconds* [**frequency** *seconds*]]

Syntax Description

group *server-group-name*	Server group to which traffic will be redirected.
ip *ip-address*	IP address of the server to which traffic will be redirected.
port *port-number*	(Optional) Port number on the server to which traffic will be redirected.
duration *seconds*	(Optional) Amount of time, in seconds, for which traffic will be redirected, beginning with the first packet that gets redirected.
frequency *seconds*	(Optional) Period of time, in seconds, between activations of redirection.

Command Default

Subscriber Layer 4 traffic is not redirected.

Command Modes

Service policy-map class configuration (config-service-policymap)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRE	This command was modified. It was removed from interface configuration mode.
Cisco IOS XE Release 2.5	This command was modified. It was removed from interface configuration mode.

Usage Guidelines

The ISG Layer 4 Redirect feature redirects specified Layer 4 subscriber packets to servers that handle the packets in a specified manner.

The Layer 4 Redirect feature supports three types of redirection, which can be applied to subscriber sessions or to flows:

- Permanent redirection—Specified traffic is redirected to the specified server all the time.
- Initial redirection—Specified traffic is redirected for a specific duration of time only, starting from when the feature is applied.
- Periodic redirection—Specified traffic is periodically redirected. The traffic is redirected for a specified duration of time. The redirection is then suspended for another specified duration. This cycle is repeated.

Examples

Redirecting Layer 4 Traffic to a Server Group: Example

The following example redirects Layer 4 traffic to the servers specified in server group "ADVT-SERVER":

```
redirect to group ADVT-SERVER
```

Redirecting Layer 4 Traffic to a Specific IP Address: Examples

The following example configures ISG to redirect all traffic coming from the subscriber interface to 10.2.36.253. The destination port is left unchanged, so traffic to 10.10.10.10 port 23 is redirected to 10.2.36.253 port 23, and traffic to 10.4.4.4 port 80 is redirected to 10.2.36.253 port 80.

```
redirect list 100 to ip 10.2.36.253
```

The following example configures ISG to redirect all traffic coming from the subscriber interface to 10.2.36.253 port 80:

```
redirect list 100 to ip 10.2.36.253 port 80
```

Initial Redirection: Example

The following example redirects all traffic to the servers configured in the server group "ADVT-SERVER" for the first 60 seconds of the session and then stops redirection for the rest of the lifetime of the session:

```
redirect to group ADVT-SERVER duration 60
```

Periodic Redirection: Example

The following example redirects all traffic to server group "ADVT-SERVER" for 60 seconds, every 3600 seconds. That is, the traffic will be redirected for 60 seconds, and subsequently the redirection is suspended for 3600 seconds, after which redirection resumes again for 60 seconds, and so on.

```
redirect to group ADVT-SERVER duration 60 frequency 3600
```

Related Commands

Command	Description
redirect server-group	Defines a group of one or more servers that make up a named ISG Layer 4 redirect server group.
server (ISG)	Adds a server to an ISG Layer 4 redirect server group.
show redirect group	Displays information about ISG Layer 4 redirect server groups.
show redirect translations	Displays information about the ISG Layer 4 redirect mappings for subscriber sessions.

server

To add a server to an Intelligent Services Gateway (ISG) Layer 4 redirect server group, use the **server** command in Layer 4 redirect server group configuration mode. To remove a server from a redirect server group, use the **no** form of this command.

server ip *ip-address* **port** *port*

no server ip *ip-address* **port** *port*

Syntax Description

ip *ip-address*	IP address of the server to be added to the redirect server group.
port *port*	TCP port of the server to be added to the redirect server group.

Command Default

A server is not added to the redirect server group.

Command Modes

Layer 4 redirect server group configuration

Command History

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

Usage Guidelines

Use the **server** command in Layer 4 redirect server group configuration mode to add a server, defined by its IP address and TCP port, to a redirect server group. The **server** command can be entered more than once to add multiple servers to the server group.

ISG Layer 4 redirection provides nonauthorized users with access to controlled services. Packets sent upstream from an unauthenticated user are forwarded to the server group, which deals with the packets in a suitable manner, such as routing them to a logon page. You can also use captive portals to handle requests from authorized users who request access to services to which they are not logged in.

Examples

The following example adds a server at IP address 10.0.0.0 and TCP port 8080 and a server at IP address 10.1.2.3 and TCP port 8081 to a redirect server group named “ADVT-SERVER”:

```
redirect server-group ADVT-SERVER
 server ip 10.0.0.0 port 8080
 server ip 10.1.2.3 port 8081
```

Related Commands

Command	Description
redirect server-group	Defines a group of one or more servers that make up a named ISG Layer 4 redirect server group.
redirect to (ISG)	Redirects ISG Layer 4 traffic to a specified server or server group.

Command	Description
show redirect group	Displays information about ISG Layer 4 redirect server groups.
show redirect translations	Displays information about the ISG Layer 4 redirect mappings for subscriber sessions.

server-key

To configure the RADIUS key to be shared between a device and RADIUS clients, use the **server-key** command in dynamic authorization local server configuration mode. To remove this configuration, use the **no** form of this command.

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

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

Syntax Description

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

Command Default

A server key is not configured.

Command Modes

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

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 **server-key** command to configure the key to be shared between the Intelligent Services Gateway (ISG) and RADIUS clients.

Examples

The following example configures “cisco” as the shared server key:

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

Related Commands

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

service (ISG)

To specify a network service type for PPP sessions, use the **service** 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 **service** {**disconnect** | **local** | **vpdn**}

no *action-number* **service** {**disconnect** | **local** | **vpdn**}

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.
disconnect	Disconnect the session.
local	Locally terminate the session.
VPDN	Virtual Private Dialup Network (VPDN) tunnel service.

Command Default

PPP sessions are locally terminated.

Command Modes

Control policy-map class configuration

Command History

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

Usage Guidelines

The **service** 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 configure ISG to locally terminate sessions for PPP subscribers:

```
policy-map type control MY-RULE1
 class type control MY-CONDITION2 event session-start
  1 service local
```

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.

service deny (ISG)

To deny network service to the Intelligent Services Gateway (ISG) subscriber session, use the **service deny** command in service policy-map configuration mode. To remove the configuration, use the **no** form of this command.

service deny

no service deny

Syntax Description

The command has no arguments or keywords.

Command Default

Service is not denied to the session.

Command Modes

Service policy-map configuration

Command History

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

Usage Guidelines

The **service deny** command denies network service to subscriber sessions that use the service policy map.

Examples

The following example denies service to subscriber sessions that use the service called “service1”:

```
policy-map type service service1
 service deny
```

Related Commands

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

service local (ISG)

To specify local termination service in an Intelligent Services Gateway (ISG) service policy map, use the **service local** command in service policy-map configuration mode. To remove the service, use the **no** form of this command.

service local

no service local

Syntax Description

This command has no arguments or keywords.

Command Default

Local termination service is not specified.

Command Modes

Service policy-map configuration

Command History

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

Usage Guidelines

The **service local** command is used to configure local termination service in a service policy map defined with the **policy-map type service** command.

When you configure the **service local** command in a service policy map, you can also use the **ip vrf forwarding** command to specify the routing domain in which to terminate the session. If you do not specify the routing domain, the global virtual routing and forwarding instance (VRF) will be used.

Examples

The following example provides local termination service to subscriber sessions for which the "my_service" service policy map is activated:

```
!
policy-map type service my_service
 service local
```

Related Commands

Command	Description
ip vrf forwarding (service policy map)	Associates the service with a VRF.
policy-map type service	Creates or modifies a service policy map, which is used to define an ISG service.
service vpdn group	Provides VPDN service.
vpdn-group	Associates a VPDN group with a customer or VPDN profile.

service relay (ISG)

To enable relay of PPPoE Active Discovery (PAD) messages over a Layer 2 Tunnel Protocol (L2TP) tunnel for an Intelligent Services Gateway (ISG) subscriber session, use the **service relay** command in service policy-map configuration mode. To disable message relay, use the **no** form of this command.

service relay pppoe vpdn group *vpdn-group-name*

no service relay pppoe vpdn group *vpdn-group-name*

Syntax Description

pppoe	Provides relay service using PPP over Ethernet (PPPoE) using a virtual private dialup network (VPDN) L2TP tunnel for the relay.
vpdn group *vpdn-group-name*	Provides VPDN service by obtaining the configuration from a predefined VPDN group.

Command Default

Relay of PAD messages over an L2TP tunnel is not enabled.

Command Modes

Service policy-map configuration

Command History

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

Usage Guidelines

The **service relay** command is configured as part of a service policy-map.

Examples

The following example configures sessions that use the service policy-map “service1” to contain outgoing tunnel information for the relay of PAD messages over an L2TP tunnel:

```
policy-map type service
 service relay pppoe vpdn group Sample1.net
```

Related Commands

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

service vpdn group (ISG)

To provide virtual private dialup network (VPDN) service for Intelligent Services Gateway (ISG) subscriber sessions, use the **service vpdn group** command in service policy-map configuration mode. To remove VPDN service, use the **no** form of this command.

service vpdn group *vpdn-group-name*

no service vpdn group *vpdn-group-name*

Syntax Description

vpdn-group-name	Provides the VPDN service by obtaining the configuration from a predefined VPDN group.

Command Default

VPDN service is not provided for ISG subscriber sessions.

Command Modes

Service policy-map configuration

Command History

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

Usage Guidelines

The **service vpdn group** command provides VPDN service by obtaining the configuration from a predefined VPDN group.

A service configured with the **service vpdn group** command (or corresponding RADIUS attribute) is a primary service.

Examples

The following example provides VPDN service to sessions that use the service called "service" and uses VPDN group 1 to obtain VPDN configuration information:

```
policy-map type service service1
 service vpdn group 1
```

Related Commands

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

service-monitor

To configure service monitoring for sessions on the Service Control Engine (SCE) that use the configured Intelligent Services Gateway (ISG) service, use the **service-monitor** command in service policy map configuration mode. To remove service monitoring, use the **no** form of this command.

service-monitor {**enable** | **disable**}

no service-monitor {**enable** | **disable**}

Syntax Description

enable	Enables service monitoring.
disable	Disables service monitoring.

Command Default

Service monitoring is not configured.

Command Modes

Service policy map configuration (config-service-policymap)

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 **service-monitor** command is used with the **policy-map type service** command and must be configured together with the **sg-service-type external-policy** command.

Examples

The following example configures service monitoring for a service policy called “SCE-SERVICE4”.

```
Router(config)# policy-map type service SCE-SERVICE4
Router(config-service-policymap)# sg-service-type external policy
Router(config-service-policymap)# service-monitor enable
```

Related Commands

Command	Description
policy-name	Configures a subscriber policy name.
sg-service-type external policy	Identifies an ISG service as an external policy.

service-policy

To attach a policy map to an input interface, a virtual circuit (VC), an output interface, or a VC that will be used as the service policy for the interface or VC, use the **service-policy** command in the appropriate configuration mode. To remove a service policy from an input or output interface or from an input or output VC, use the **no** form of this command.

service-policy [**type access-control**] {**input** | **output**} *policy-map-name*

no service-policy [**type access-control**] {**input** | **output**} *policy-map-name*

Cisco 10000 Series and Cisco 7600 Series Routers

service-policy [**history** | {**input** | **output**} *policy-map-name* | **type control** *control-policy-name*]

no service-policy [**history** | {**input** | **output**} *policy-map-name* | **type control** *control-policy-name*]

Syntax Description

type access-control	Determines the exact pattern to look for in the protocol stack of interest.
input	Attaches the specified policy map to the input interface or input VC.
output	Attaches the specified policy map to the output interface or output VC.
policy-map-name	The name of a service policy map (created using the **policy-map** command) to be attached. The name can be a maximum of 40 alphanumeric characters.
history	(Optional) Maintains a history of Quality of Service (QoS) metrics.
type control *control-policy-name*	(Optional) Creates a Class-Based Policy Language (CPL) control policy map that is applied to a context.

Command Default

No service policy is specified.
A control policy is not applied to a context.
No policy map is attached.

Command Modes

ATM bundle-VC configuration (config-atm-bundle)
ATM PVP configuration (config-if-atm-l2trans-pvp)
ATM VC mode (config-if-atm-vc)
Global configuration (config)
Interface configuration (config-if)
Map-class configuration (config-map-class)
PVC-in-range configuration (cfg-if-atm-range-pvc)
PVC range subinterface configuration (config-subif)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.0(17)SL	This command was implemented on the Cisco 10000 series routers.

Release	Modification
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(2)T	This command was modified to enable low latency queueing (LLQ) on Frame Relay VCs.
12.2(14)SX	Support for this command was implemented on Cisco 7600 series routers. This command was changed to support output policy maps.
12.2(15)BX	This command was implemented on the ESR-PRE2.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(2)T	This command was modified to support PVC range subinterface configuration mode and i PVC-in-range configuration mode to extend policy map functionality on an ATM VC to the ATM VC range.
12.4(4)T	The **type stack** and the **type control** keywords were added to support flexible packet matching (FPM).
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.3(7)XI2	This command was modified to support PVC range configuration mode and PVC-in-range configuration mode for ATM VCs on the Cisco 10000 series router and the Cisco 7200 series router.
12.2(18)ZY	The **type stack** and the **type control** keywords were integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).
12.2(33)SRC	Support for this command was enhanced on Cisco 7600 series routers.
12.2(33)SB	This command's behavior was modified and implemented on the Cisco 10000 series router for the PRE3 and PRE4.
Cisco IOS XE Release 2.3	This command was modified to support ATM PVP configuration mode.

Usage Guidelines

Choose the command mode according to the intended use of the command, as follows:

Application	Mode
Standalone VC	VC submode
ATM VC bundle members	Bundle-VC configuration
A range of ATM PVCs	PVC range subinterface configuration
Individual PVC within a PVC range	PVC-in-range configuration
Frame Relay VC	Map-class configuration

You can attach a single policy map to one or more interfaces or to one or more VCs to specify the service policy for those interfaces or VCs.

A service policy specifies class-based weighted fair queueing (CBWFQ). The class policies that make up the policy map are then applied to packets that satisfy the class map match criteria for the class.

To successfully attach a policy map to an interface or ATM VC, the aggregate of the configured minimum bandwidths of the classes that make up the policy map must be less than or equal to 75 percent (99 percent on the Cisco 10008 router) of the interface bandwidth or the bandwidth allocated to the VC.

To enable Low Latency queueing (LLQ) for Frame Relay (priority queueing [PQ]/CBWFQ), you must first enable Frame Relay Traffic Shaping (FRTS) on the interface using the **frame-relay traffic-shaping** command in interface configuration mode. You then attach an output service policy to the Frame Relay VC using the **service-policy** command in map-class configuration mode.

For a policy map to be successfully attached to an interface or ATM VC, the aggregate of the configured minimum bandwidths of the classes that make up the policy map must be less than or equal to 75 percent of the interface bandwidth or the bandwidth allocated to the VC. For a Frame Relay VC, the total amount of bandwidth allocated must not exceed the minimum committed information rate (CIR) configured for the VC less any bandwidth reserved by the **frame-relay voice bandwidth** or **frame-relay ip rtp priority** map-class commands. If these values are not configured, the minimum CIR defaults to half of the CIR.

Configuring CBWFQ on a physical interface is possible only if the interface is in the default queueing mode. Serial interfaces at E1 (2.048 Mbps) and below use weighted fair queueing (WFQ) by default. Other interfaces use first-in first-out (FIFO) by default. Enabling CBWFQ on a physical interface overrides the default interface queueing method. Enabling CBWFQ on an ATM permanent virtual circuit (PVC) does not override the default queueing method.

When you attach a service policy with CBWFQ enabled to an interface, commands related to fancy queueing such as those pertaining to fair queueing, custom queueing, priority queueing, and Weighted Random Early Detection (WRED) are available using the modular quality of service command-line interface (MQC). However, you cannot configure these features directly on the interface until you remove the policy map from the interface.

You can modify a policy map attached to an interface or VC, changing the bandwidth of any of the classes that make up the map. Bandwidth changes that you make to an attached policy map are effective only if the aggregate of the bandwidth amount for all classes that make up the policy map, including the modified class bandwidth, is less than or equal to 75 percent of the interface bandwidth or the VC bandwidth. If the new aggregate bandwidth amount exceeds 75 percent of the interface bandwidth or VC bandwidth, the policy map is not modified.

After you apply the **service-policy** command to set a class of service (CoS) bit to an Ethernet interface, the policy is set in motion as long as there is a subinterface that is performing 8021.Q or Inter-Switch Link (ISL) trunking. Upon reload, however, the service policy is removed from the configuration with the following error message:

```
Process 'set' action associated with class-map voip failed: Set cos supported only with
IEEE 802.1Q/ISL interfaces.
```

Cisco 10000 Series Router Usage Guidelines

The Cisco 10000 series router does not support applying CBWFQ policies to unspecified bit rate (UBR) VCs.

For a policy map to be successfully attached to an interface or a VC, the aggregate of the configured minimum bandwidth of the classes that make up the policy map must be less than or equal to 99 percent of the interface bandwidth or the bandwidth allocated to the VC. If you attempt to attach a policy map to an interface when the sum of the bandwidth assigned to classes is greater than 99 percent of the available bandwidth, the router logs a warning message and does not allocate the requested bandwidth to all of the classes. If the policy map is already attached to other interfaces, it is removed from them.

The total bandwidth is the speed (rate) of the ATM layer of the physical interface. The router converts the minimum bandwidth that you specify to the nearest multiple of 1/255 (ESR-PRE1) or 1/65535 (ESR-PRE2) of the interface speed. When you request a value that is not a multiple of 1/255 or 1/65535, the router chooses the nearest multiple.

The bandwidth percentage is based on the interface bandwidth. In a hierarchical policy, the bandwidth percentage is based on the nearest parent shape rate.

By default, a minimum bandwidth guaranteed queue has buffers for up to 50 milliseconds of 256-byte packets at line rate, but not less than 32 packets.

For Cisco IOS Release 12.0(22)S and later releases, to enable LLQ for Frame Relay (priority queueing (PQ)/CBWFQ) on the Cisco 10000 series router, first create a policy map and then assign priority to a defined traffic class using the **priority** command. For example, the following sample configuration shows how to configure a priority queue with a guaranteed bandwidth of 8000 kbps. In the example, the Business class in the policy map named “map1” is configured as the priority queue. The map1 policy also includes the Non-Business class with a minimum bandwidth guarantee of 48 kbps. The map1 policy is attached to serial interface 2/0/0 in the outbound direction.

```
class-map Business
    match ip precedence 3
policy-map map1
    class Business
    priority
    police 8000
    class Non-Business
    bandwidth 48
interface serial 2/0/0
    frame-relay encapsulation
    service-policy output map1
```

On the PRE2, you can use the **service-policy** command to attach a QoS policy to an ATM subinterface or to a PVC. However, on the PRE3, you can attach a QoS policy only to a PVC.

Cisco 7600 Series Routers

The **output** keyword is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Do not attach a service policy to a port that is a member of an EtherChannel.

Although the CLI allows you to configure QoS based on policy feature cards (PFCs) on the WAN ports on the OC-12 ATM optical services modules (OSM) and on the WAN ports on the channelized OSMs, PFC-based QoS is not supported on the WAN ports on these OSMs. OSMs are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

PFC QoS supports the optional **output** keyword only on VLAN interfaces. You can attach both an input policy map and an output-policy map to a VLAN interface.

Cisco 10000 Series Routers Control Policy Maps

A control policy map must be activated by applying it to a context. A control policy map can be applied to one or more of the following types of contexts, which are listed in order of precedence:

1. Global
2. Interface
3. Subinterface
4. Virtual template

5. VC class
6. PVC

In general, control policy maps that are applied to more specific contexts take precedence over policy maps applied to more general contexts. In the list, the context types are numbered in order of precedence. For example, a control policy map that is applied to a permanent virtual circuit (PVC) takes precedence over a control policy map that is applied to an interface.

Control policies apply to all sessions hosted on the context. Only one control policy map can be applied to a given context.

In Cisco IOS Release 12.2(33)SB and later releases, the router no longer accepts the abbreviated form (**ser**) of the **service-policy** command. Instead, you must spell out the command name **service-** before the router accepts the command.

For example, the following error message displays when you attempt to use the abbreviated form of the **service-policy** command:

```
interface GigabitEthernet1/1/0
 ser out ?
% Unrecognized command
 ser ?
% Unrecognized command
```

As shown in the following example, when you enter the command as **service-** followed by a space, the router parses the command as **service-policy**. Entering the question mark causes the router to display the command options for the **service-policy** command.

```
service- ?
inputAssign policy-map to the input of an interface
outputAssign policy-map to the output of an interface
typeConfigure CPL Service Policy
```

In releases prior to Cisco IOS Release 12.2(33)SB, the router accepts the abbreviated form of the **service-policy** command. For example, the router accepts the following commands:

```
interface GigabitEthernet1/1/0
 ser out test
```

Examples

The following example shows how to attach a policy map to a Fast Ethernet interface:

```
interface fastethernet 5/20
 service-policy input pmap1
```

The following example shows how to attach the service policy map named “policy9” to DLCI 100 on output serial interface 1 and enables LLQ for Frame Relay:

```
interface Serial1/0.1 point-to-point
 frame-relay interface-dlci 100
 class fragment
 map-class frame-relay fragment
 service-policy output policy9
```

The following example shows how to attach the service policy map named “policy9” to input serial interface 1:

```
interface Serial1
 service-policy input policy9
```

The following example attaches the service policy map named “policy9” to the input PVC named “cisco”:

```
pvc cisco 0/34
service-policy input policy9
vbr-nt 5000 3000 500
precedence 4-7
```

The following example shows how to attach the policy named “policy9” to output serial interface 1 to specify the service policy for the interface and enable CBWFQ on it:

```
interface serial1
 service-policy output policy9
```

The following example attaches the service policy map named “policy9” to the output PVC named “cisco”:

```
pvc cisco 0/5
service-policy output policy9
vbr-nt 4000 2000 500
precedence 2-3
```

Cisco 10000 Series Router Examples

The following example shows how to attach the service policy named “userpolicy” to DLCI 100 on serial subinterface 1/0/0.1 for outbound packets:

```
interface serial 1/0/0.1 point-to-point
 frame-relay interface-dlci 100
 service-policy output userpolicy
```

Note You must be running Cisco IOS Release 12.0(22)S or a later release to attach a policy to a DLCI in this way. If you are running a release prior to Cisco IOS Release 12.0(22)S, attach the service policy as described in the previous configuration examples using the legacy Frame Relay commands.

The following example shows how to attach a QoS service policy named “map2” to PVC 0/101 on the ATM subinterface 3/0/0.1 for inbound traffic:

```
interface atm 3/0/0
 atm pxf queuing
interface atm 3/0/0.1
 pvc 0/101
 service-policy input map2
```

Note The **atm pxf queuing** command is not supported on the PRE3 or PRE4.

The following example shows how to attach a service policy named “myQoS” to physical Gigabit Ethernet interface 1/0/0 for inbound traffic. VLAN 4, configured on Gigabit Ethernet subinterface 1/0/0.3, inherits the service policy of physical Gigabit Ethernet interface 1/0/0.

```
interface GigabitEthernet 1/0/0
 service-policy input myQoS
interface GigabitEthernet 1/0/0.3
 encapsulation dot1q 4
```

The following example shows how to attach the service policy map named “voice” to ATM VC 2/0/0 within a PVC range of a total of three PVCs and enable PVC range configuration mode where a point-to-point subinterface is created for each PVC in the range. Each PVC created as part of the range has the voice service policy attached to it.

```
configure terminal
 interface atm 2/0/0
 range pvc 1/50 1/52
 service-policy input voice
```

The following example shows how to attach the service policy map named “voice” to ATM VC 2/0/0 within a PVC range, where every VC created as part of the range has the voice service policy attached to it. The exception is PVC 1/51, which is configured as an individual PVC within the range and has a different service policy named “data” attached to it in PVC-in-range configuration mode.

```
configure terminal
 interface atm 2/0/0
 range pvc 1/50 1/52
 service-policy input voice
 pvc-in-range 1/51
 service-policy input data
```

The following example shows how to configure a service group named “PREMIUM-SERVICE” and apply the input policy named “PREMIUM-MARK-IN” and the output policy named “PREMIUM-OUT” to the service group:

```
policy-map type service PREMIUM-SERVICE
 service-policy input PREMIUM-MARK-IN
 service-policy output PREMIUM-OUT
```

Related Commands

Command	Description
class-map	Accesses the QoS class map configuration mode to configure QoS class maps.
frame-relay ip rtp priority	Reserves a strict priority queue on a Frame Relay PVC for a set of RTP packet flows belonging to a range of UDP destination ports,
frame-relay traffic-shaping	Enables both traffic shaping and per-virtual-circuit queueing for all PVCs and SVCs on a Frame Relay interface.
frame-relay voice bandwidth	Specifies the amount of bandwidth to be reserved for voice traffic on a specific DLCI.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.

service-policy type control

To apply a control policy to a context, use the **service-policy type control** command in the appropriate configuration mode. To unapply the control policy, use the **no** form of this command.

service-policy type control *policy-map-name*

no service-policy type control *policy-map-name*

Syntax Description

policy-map-name	Name of the control policy map.

Command Default

A control policy is not applied to a context.

Command Modes

Global configuration
Interface configuration
Subinterface configuration
Virtual template configuration
ATM VC class configuration
ATM VC configuration

Command History

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

Usage Guidelines

A control policy map must be activated by applying it to a context. A control policy map can be applied to one or more of the following types of contexts:

1. Global
2. Interface
3. Subinterface
4. Virtual template
5. VC class
6. PVC

In general, control policy maps that are applied to more specific contexts take precedence over policy maps applied to more general contexts. In the list, the context types are numbered in order of precedence. For example, a control policy map that is applied to a permanent virtual circuit (PVC) takes precedence over a control policy map that is applied to an interface.

Control policies apply to all sessions hosted on the context.

Only one control policy map may be applied to a given context.

Examples

The following example applies the control policy map “RULEA” to Ethernet interface 0:

```
interface Ethernet 0
 service-policy type control RULEA
```

Related Commands

Command	Description
policy-map type control	Creates or modifies a control policy map, which defines an ISG control policy.

service-policy type service

To activate an Intelligent Services Gateway (ISG) service, use the **service-policy type service** 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 **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}}

no *action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}}

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.
unapply	(Optional) Deactivates the specified service.
aaa	(Optional) Specifies that a AAA method list will be used to activate the service.
list *list-name*	(Optional) Activates the service using the specified authentication, authorization, and accounting (AAA) method list.
name *service-name*	Name of the service.
identifier	Activates a service that has the same name as the specified identifier.
authenticated-domain	Authenticated domain name.
authenticated-username	Authenticated username.
dnis	Dialed Number Identification Service number (also referred to as the *called-party number*).
nas-port	Network access server (NAS) port identifier.
tunnel-name	VPDN tunnel name.
unauthenticated-domain	Unauthenticated domain name.
unauthenticated-username	Unauthenticated username.

Command Default

A service is not activated.

Command Modes

Control policy-map class configuration

Command History

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

Usage Guidelines

The **service-policy type service** command configures an action in a control policy map. If you do not specify the AAA method list, the default method list will be used.

Note that if you use 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 service-policy type service aaa list
default identifier authenticated-domain
```

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

```
1 service-policy type service identifier authenticated-domain
```

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

Services are configured in service profiles on the AAA server or in service policy maps on the router.

Examples

The following example configures an ISG control policy that will initiate authentication of the subscriber and then apply a service that has a name matching the subscriber's authenticated domain name:

```
policy-map type control MY-RULE2
 class type control MY-CONDITION2 event service-start
  1 authenticate aaa list AUTHEN
  2 service-policy type service aaa list SERVICE identifier authenticated-domain
```

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

session-identifier (ISG)

To correlate RADIUS server requests and identify a session in the Intelligent Services Gateway (ISG) RADIUS proxy, use the **session-identifier** command in RADIUS proxy server configuration mode or RADIUS proxy client configuration mode. To disable this function, use the **no** form of this command.

session-identifier {**attribute** *number* | **vsa vendor** *id* **type** *number*}

no session-identifier {**attribute** *number* | **vsa vendor** *id* **type** *number*}

Syntax Description

attribute	Specifies the calling station attribute of the session to be identified.
number	The attribute number. For example, attribute 1 denotes username.
vsa	Specifies the vendor-specific attribute (VSA) of the session to be identified.
vendor *id*	Specifies the vendor type and ID.
type *number*	Specifies the VSA type and number.

Command Default

RADIUS proxy server correlates calling station attributes (attribute 31).

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

The ISG RADIUS proxy identifies a new session based on the calling station attributes. Usually, attribute 31 is used to identify the session for requests. However, it is possible that attribute 31 may not always be unique to identify the session. There are attributes such as username (RADIUS attribute 1), circuit-ID (RADIUS VSA), and so on, that could be used to identify the session and correlate RADIUS requests. By using the **session-identifier** command, you can configure the RADIUS proxy to accept other attributes or VSAs to identify the session in the RADIUS proxy and correlate requests from the downstream device. A downstream device is a device whose data is logged by a data recorder on a different node.

Examples

The following example shows how to configure the ISG to identify the session using the RADIUS VSA vendor type and correlate the requests for a RADIUS proxy client with IP address 10.0.0.16:

```
Router(config-locsvr-proxy-radius)# client 10.0.0.16 255.255.255.0
Router(config-locsvr-radius-client)# session-identifier vsa vendor 12 type 123
```

Related Commands

Command	Description
aaa server radius proxy	Enables ISG RADIUS proxy configuration mode, in which ISG RADIUS proxy parameters can be configured.
calling-station-id format	Specifies the format if the attribute of the calling station is attribute 31.
client (ISG RADIUS proxy)	Enters ISG RADIUS proxy client configuration mode, in which client-specific RADIUS proxy parameters can be specified.

set-timer

To start a named policy timer, use the **set-timer** 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 **set-timer** *name-of-timer minutes*

no *action-number* **set-timer** *name-of-timer minutes*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.
name-of-timer	Name of the policy timer.
minutes	Timer interval, in minutes. Range is from 1 to 10100.

Command Default

A named policy timer is not started.

Command Modes

Control policy-map class configuration

Command History

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

Usage Guidelines

The **set-timer** command configures an action in a control policy map.

Expiration of a named policy timer generates the timed-policy-expiry event.

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 configures a policy timer called "TIMERA". When TIMERA expires the service will be disconnected.

```
class-map type control match-all CONDE
 match timer TIMERA

policy-map type type control RULEA
 class type control <some_cond> event session-start
  1 set-timer TIMERA 1
 class type control CONDE event timed-policy-expiry
  1 service disconnect
```

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.

sgi beep listener

To enable Service Gateway Interface (SGI), use the **sgi beep listener** command in global configuration mode. To disable SGI, use the **no** form of this command.

sgi beep listener [*port*] [**acl** *access-list*] [**sasl** *sasl-profile*] [**encrypt** *trustpoint*]

no sgi beep listener

Syntax Description

port	(Optional) TCP port on which to listen. The default is assigned by Internet Assigned Numbers Authority (IANA).
acl	(Optional) Applies an access control list (ACL) to restrict incoming client connections.
access-list	Name of the access list that is to be applied.
sasl	(Optional) Configures a Simple Authentication Security Layer (SASL) profile to use during the session establishment.
sasl-profile	Name of SASL profile being used during session establishment.
encrypt	(Optional) Configures transport layer security (TLS) for SGI.
trustpoint	Name of trustpoint being used by the TLS connection.

Command Default

The SGI is not enabled.

Command Modes

Global configuration (config)

Command History

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

Examples

```
Router(config)# sgi beep listener 2089
```

Related Commands

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

sg-service-group

To associate an Intelligent Services Gateway (ISG) service with a service group, use the **sg-service-group** command in service policy-map configuration mode. To remove the association, use the **no** form of this command.

sg-service-group *service-group-name*

no sg-service-group *service-group-name*

Syntax Description

service-group-name	Name of the service group.

Command Default

The service is not part of a service group.

Command Modes

Service policy-map configuration

Command History

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

Usage Guidelines

A service group is a grouping of services that may be active simultaneously for a given session. Typically, a service group includes one primary service and one or more secondary services.

Secondary services in a service group are dependent on the primary service and should not be activated unless the primary service is already active. Once a primary service has been activated, any other services that reference the same group may also be activated. Services that belong to other groups, however, can be activated only if they are primary. If a primary service from another service group is activated, all services in the current service-group will also be deactivated because they have a dependency on the previous primary service.

Examples

The following example associates the service called “primarysvc1” with the service group “group1”:

```
policy-map type service primarysvc1
 sg-service-group group1
```

Related Commands

Command	Description
policy-map type service	Creates or modifies a service policy map, which is used to define an ISG subscriber service.
sg-service-type	Identifies an ISG service as primary or secondary.

sg-service-type

To identify an Intelligent Services Gateway (ISG) service as primary or secondary, use the **sg-service-type** command in service policy-map configuration mode. To remove this specification, use the **no** form of this command.

sg-service-type {**primary** | **secondary**}

no sg-service-type {**primary** | **secondary**}

Syntax Description

primary	Identifies the service as a primary service, which is a service that contains a network-forwarding policy.
secondary	Identifies the service as a secondary service, which is a service that does not contain a network-forwarding policy. This is the default.

Command Default

A service is not identified as a primary service.

Command Modes

Service policy-map configuration

Command History

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

Usage Guidelines

An ISG primary service is a service that contains a network-forwarding policy, such as a virtual routing or forwarding instance (VRF) or tunnel specification. A service must be identified as a primary service by using the **sg-service-type primary** command. Any service that is not a primary service is identified as a secondary service by default. In other words, the service policy map for a primary service must include a network-forwarding policy and the **sg-service-type primary** command. A secondary service must not include a network-forwarding policy, and inclusion of the **sg-service-type secondary** command is optional.

Examples

The following example identifies a service as a primary service:

```
policy-map type service service1
 ip vrf forwarding blue
 sg-service-type primary
```

Related Commands

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

sg-service-type external policy

To identify an Intelligent Services Gateway (ISG) service as an external policy, use the **sg-service-type external policy** command in service policy-map configuration mode. To remove this specification, use the **no** form of this command.

sg-service-type external policy *external-policy*

no sg-service-type external policy *external-policy*

Syntax Description

external-policy	External policy delegation Service Gateway service type.

Command Default

A service is not identified as an external policy.

Command Modes

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

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

An external policy service type identifies a service as being provided by an external device. The external device is configured in a peering relationship with the ISG device via the **aaa server radius policy-device** command. The external device handles policies for user sessions that use the service.

Examples

The following example identifies the ISG service as an external policy:

```
Router(config)# policy-map type service SCE-SERVICE-LOCAL
Router(config-service-policymap)# sg-service-type external-policy
```

Related Commands

Command	Description
aaa server radius policy-device	Enables ISG RADIUS server configuration mode, in which server parameters can be configured.
policy-name	Configures a subscriber policy name.
service-monitor	Configures service monitoring.

show class-map type control

To display information about Intelligent Services Gateway (ISG) control class maps, use the **show class-map type control** command in privileged EXEC mode.

show class-map type 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.

Usage Guidelines

Use the **show class-map type control** command to display information about ISG control class maps, including statistics on the number of times a particular class has been evaluated and what the results were.

Examples

The following example shows sample output for the **show class-map type control** command:

```
Router# show class-map type control

Condition                    Action                         Exec Hit Miss Comp
---------                    ------                         ---- --- ---- ----
```

Table 3 describes the significant fields shown in the display.

Table 3 show class-map type control Field Descriptions

Field	Description
Exec	Number of times this line was executed.
Hit	Number of times this line evaluated to true.
Miss	Number of times this line evaluated to false.
Comp	Number of times this line completed the execution of its condition without a need to continue on to the end.

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.

Command	Description
clear class-map type control	Clears the ISG control class map counters.
show policy-map type control	Displays information about ISG control policy maps.

show class-map type traffic

To display Intelligent Services Gateway (ISG) traffic class maps and their matching criteria, use the **show class-map type traffic** command in privileged EXEC mode.

show class-map type traffic

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 configuration of a traffic class-map and corresponding sample output for the **show class-map type traffic** command. The output is self-explanatory.

```
!
access-list 101 permit ip any any
access-list 102 permit ip any any
!
class-map type traffic match-any PEER_TRAFFIC
 match access-group output 102
 match access-group input 101
!

Router# show class-map type traffic

Class-map: match-any  PEER_TRAFFIC
------------------------------------------------------
Output:
Extended IP access list 102
    10 permit ip any any
Input:
Extended IP access list 101
    10 permit ip any any
```

Related Commands

Command	Description
show policy-map type traffic	Displays the contents of ISG service policy maps.

show idmgr

To display information related to the Intelligent Services Gateway (ISG) session identity, use the **show idmgr** command in privileged EXEC mode.

show idmgr {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string* | **circuit-id** *circuit-id* | **pppoe-unique-id** *pppoe-id*} | **statistics**}

Syntax Description

memory	Displays memory-usage information related to ID management.
detailed	(Optional) Displays detailed memory-usage information related to ID management.
component	(Optional) Displays information for the specified ID management component.
substring	(Optional) Substring to match the component name.
service key	Displays ID information for a specific service.
session-handle *session-handle-string*	Displays the unique identifier for a session.
service-key *key-value*	Displays ID information for a specific service.
session key	Displays ID information for a specific session and its related services.
aaa-unique-id *aaa-unique-id-string*	Displays the authentication, authorization, and accounting (AAA) unique ID for a specific session.
domainip-vrf ip-address *ip-address*	Displays the service-facing IP address for a specific session.
vrf-id *vrf-id*	Displays the VPN routing and forwarding (VRF) ID for the specific session.
nativeip-vrf ip-address *ip-address*	Displays the subscriber-facing IP address for a specific session.
portbundle ip *ip-address*	Displays the port bundle IP address for a specific session.
bundle *bundle-number*	Displays the bundle number for a specific session.
session-guid *session-guid*	Displays the global unique identifier for a session.
session-handle *session-handle-string*	Displays the session identifier for a specific session.
session-id *session-id-string*	Displays the session identifier used to construct the value for RADIUS attribute 44 (Acct-Session-ID).
circuit-id *circuit-id*	Displays the user session information in the ID Manager (IDMGR) database when you specify the unique circuit ID tag.
pppoe-unique-id *pppoe-id*	Displays the PPPoE unique key information in the ID Manager (IDMGR) database when you specify the unique PPPoE unique ID tag
statistics	Displays statistics related to storing and retrieving ID information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 2.6	The **circuit-id** keyword and *circuit-id* argument was added.

Examples

The following sample output for the **show idmgr** command displays information about the service called "service":

```
Router# show idmgr service key session-handle 48000002 service-key service

session-handle = 48000002
service-name = service
idmgr-svc-key = 4800000273657276696365
authen-status = authen
```

The following sample output for the **show idmgr** command displays information about a session and the service that is related to the session:

```
Router# show idmgr session key session-handle 48000002

session-handle = 48000002
aaa-unique-id = 00000002
authen-status = authen
username = user1

Service 1 information:
session-handle = 48000002
service-name = service
idmgr-svc-key = 4800000273657276696365
```

The following sample output for the **show idmgr** command displays information about the global unique identifier of a session:

```
Router# show idmgr session key session-guid 020202010000000C

session-handle = 18000003
aaa-unique-id = 0000000C
authen-status = authen
interface = nas-port:0.0.0.0:2/0/0/42
authen-status = authen
username = FortyTwo
addr = 100.42.1.1
session-guid = 020202010000000C
```

The following sample output for the **show idmgr** command displays information about the user session information in the ID Manager (IDMGR) database by specifying the unique circuit ID tag:

```
Router# show idmgr session key circuit-id Ethernet4/0.100:PPPoE-Tag-1

session-handle = AA000007
aaa-unique-id = 0000000E
circuit-id-tag = Ethernet4/0.100:PPPoE-Tag-1
interface = nas-port:0.0.0.0:0/1/1/100
authen-status = authen
username = user1@cisco.com
addr = 106.1.1.3
session-guid = 650101020000000E
The session hdl AA000007 in the record is valid
The session hdl AA000007 in the record is valid
No service record found
```

Table 4 describes the significant fields shown in the display.

Table 4 show idmgr Field Descriptions

Field	Description
session-handle	Unique identifier of the session.
service-name	Service name for this session.
idmgr-svc-key	The ID manager service key of this session.
authen-status	Indicates whether the session has been authenticated or unauthenticated.
aaa-unique-id	AAA unique ID of the session.
username	The username associated with this session.
interface	The interface details of this session.
addr	The IP address of this session.
session-guid	Global unique identifier of this session.

Related Commands

Command	Description
subscriber access pppoe unique-key circuit-id	Specifies a unique circuit ID tag for a PPPoE user session to be tapped on the router.

show interface monitor

To display interface statistics that will be updated at specified intervals, use the **show interface monitor** command in user EXEC or privileged EXEC mode.

show interface *interface-type interface-number* **monitor** [**interval** *seconds*]

Syntax Description

interface-type	Type of the interface for which statistics will be displayed.
interface-number	Number of the interface for which statistics will be displayed.
interval *seconds*	(Optional) Interval, in seconds, at which the display will be updated. Range: 5 to 3600. Default: 5.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

The **show interface monitor** command allows you to monitor an interface by displaying interface statistics and updating those statistics at regular intervals. While the statistics are being displayed, the command-line interface will prompt you to enter “E” to end the display, “C” to clear the counters, or “F” to freeze the display.

Examples

The following example shows sample output for the **show interface monitor** command. The display will be updated every 10 seconds.

```
Router# show interface ethernet 0/0 monitor interval 10

Router Name:  Scale3-Router8       Update Secs: 10
Interface Name:   Ethernet 0/0          Interface Status: UP, line is up

Line Statistics:          Total:        Rate(/s)    Delta
Input Bytes:              123456        123         7890
Input Packets:              3456         56          560
Broadcast:                  1333          6           60
OutputBytes:               75717        123         1230
Output Packets:              733         44          440

Error Statistics:         Total:        Delta:
Input Errors:              0               0
CRC  Errors:               0               0
Frame Errors:              0               0
Ignored:                   0               0
Output Errors:             0               0
Collisions:                0               0

No. Interface Resets:  2
```

```
End = e       Clear = c      Freeze = f
Enter Command:
```

Table 5 describes the significant fields shown in the display.

Table 5 show interface monitor Field Descriptions

Field	Description
Line Statistics	Information about the physical line. The delta column indicates the difference between the current display and the display before the last update.
Input Bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
Input Packets	Total number of error-free packets received by the system.
Broadcast	Total number of broadcast or multicast packets received by the interface.
OutputBytes	Total number of bytes sent by the system.
Output Packets	Total number of packets sent by the system.
Error Statistics	Displays statistics about errors. The delta column indicates the difference between the current display and the display before the last update.
Input Errors	Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC Errors	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
Frame Errors	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
Ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
Output Errors	Sum of all errors that prevented the final transmission of datagrams out of the interface from being examined. Note that this may not balance with the sum of the enumerated output errors, as some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.

Table 5 show interface monitor Field Descriptions (continued)

Field	Description
Collisions	Number of messages transmitted because of an Ethernet collision. A packet that collides is counted only once in output packets.
No. Interface Resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router or access server.

show ip portbundle ip

To display information about a particular Intelligent Services Gateway (ISG) port bundle, use the **show ip portbundle ip** command in privileged EXEC mode.

show ip portbundle ip *port-bundle-ip-address* **bundle** *port-bundle-number*

Syntax Description

port-bundle-ip-address	IP address used to identify the port bundle.
bundle *port-bundle-number*	Port bundle number.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use the **show ip portbundle ip** command to display the port mappings in a port bundle.

Examples

The following example is sample output for the **show ip portbundle ip** command:

```
Router# show ip portbundle ip 10.2.81.13 bundle 65

Portbundle IP address: 10.2.81.13  Bundlenumber: 65
Subscriber VRF: VRF2

Subscriber Portmappings:
Subscriber IP: 10.0.0.2 Subscriber Port: 11019  Mapped Port: 1040
```

Table 6 describes the significant fields shown in the display.

Table 6 show ip portbundle ip Field Descriptions

Field	Description
Subscriber IP	Subscriber IP address.
Subscriber Port	Subscriber port number.
Mapped Port	Port assigned by the ISG.

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 status	Displays information about ISG port-bundle groups.

show ip portbundle status

To display a information about Intelligent Services Gateway (ISG) port-bundle groups, use the **show ip portbundle status** command in privileged EXEC mode.

show ip portbundle status [**free** | **inuse**]

Syntax Description

free	(Optional) Lists the port bundles that are available in each bundle group.
inuse	(Optional) Lists the port bundles that are in use in each bundle group. Also displays the associated subscriber interface for each port bundle.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use the **show ip portbundle status** command to display a list of port-bundle groups, port-bundle length, and the number of free and in-use port bundles in each group.

Examples

The following example is sample output for the **show ip portbundle status** command when issued with no keywords:

```
Router# show ip portbundle status

Bundle-length = 4

Bundle-groups: -

IP Address              Free Bundles            In-use Bundles
10.2.81.13                       4031                       1
```

Table 7 describes the significant fields shown in the display.

Table 7 show ip portbundle status Field Descriptions

Field	Description
Bundle-length	Number of ports per bundle and number of bundles per bundle group.
Bundle-groups	List of bundle groups.
IP Address	IP address of a bundle group.
Free Bundles	Number of free bundles in the specified bundle group.
In-use Bundles	Number of in-use bundles in the specified bundle group.

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 subscriber

To display information about Intelligent Services Gateway (ISG) IP subscriber sessions, use the **show ip subscriber** command in user EXEC or privileged EXEC mode.

show ip subscriber [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]]

Syntax Description

mac *mac-address*	(Optional) Displays information about IP subscriber sessions that have the specified MAC address.
vrf *vrf-name*	(Optional) Displays IP subscriber sessions associated with the specified virtual routing and forwarding (VRF) instance.
dangling *seconds*	(Optional) Displays IP subscriber sessions that have remained unestablished for the specified number of seconds. Range: 1 to 3600.
detail	(Optional) Displays detailed information about IP subscriber sessions.
interface *interface-name*	(Optional) Displays information for IP subscriber sessions associated with the specified interface on the Cisco 7600 series router.
statistics	(Optional) Displays statistical information for IP subscriber sessions.
ip *ip-address*	(Optional) Displays information about IP subscriber sessions that have the specified IP address.
static list *listname*	(Optional) Displays information for static sessions associated with an IP subscriber list.
arp	(Optional) Displays Address Resolution Protocol (ARP) statistics.

Command Modes

User EXEC (>)
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)SRE	This command was modified. The **static** and **list** keywords were added.
Cisco IOS XE Release 2.5	This command was modified. The **static** and **list** keywords were added.
12.2(33)SRE1	This command was modified. The **statistics** and **arp** keywords were 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 **show ip subscriber** command can be used with the **dangling** keyword to display dangling sessions. The *seconds* argument allows you to specify how long the session has to remain unestablished before it is considered dangling.

The **interface** and **static list** keywords are available only on the Cisco 7600 series router.

Examples

The following is sample output from the **show ip subscriber** command without any keywords:

```
Router# show ip subscriber

Displaying subscribers in the default service vrf:

Type        Subscriber Identifier    Display UID    Status
---------   ----------------------   ------------   ------
connected   aaaa.1111.cccc           [1]            up
```

The following is sample output from the **show ip subscriber** command using the **detail** keyword. Detailed information is displayed about all the IP subscriber sessions associated with vrf1.

```
Router# show ip subscriber vrf vrf1 detail

IP subscriber: 0000.0000.0002, type connected, status up
 display uid: 6, aaa uid: 17
 segment hdl: 0x100A, session hdl: 0x96000005, shdb: 0xBC000005
 session initiator: dhcp discovery
 access address: 10.0.0.3
 service address: vrf1, 10.0.0.3
 conditional debug flag: 0x0
 control plane state: connected, start time: 1d06h
 data plane state: connected, start time: 1d06h
 arp entry: [vrf1] 10.0.0.3, Ethernet0/0
 midchain adj: 10.0.0.3 on multiservice1
forwarding statistics:
 packets total: received 3542, sent 3538
 bytes total: received 2184420, sent 1158510
 packets dropped: 0, bytes dropped: 0
```

The following is sample output from the **show ip subscriber** command using the **list** keyword. Detailed information is displayed about all the IP subscriber static sessions associated with the server list group called *l1* on the 7600 series router.

```
Router# show ip subscriber static list l1

Total static sessions for list l1: 1, Total IF attached: 1
Interface: GigabitEthernet0/3, VRF: 0, 1
```

The following is sample output from the **show ip subscriber** command using the **statistics arp** keywords:

```
Router# show ip subscriber statistics arp

Current IP Subscriber ARP Statistics

  Total number of ARP reqs received    : 27
  ARP reqs received on ISG interfaces  : 25
  IP subscriber ARP reqs replied to    : 1
              Dst on ISG               : 0
              Src/Dst in same subnet   : 0
  IP subscriber ARP reqs ignored       : 2
              For route back to CPE    : 2
              For no routes to dest.   : 0
              Gratuitous               : 0
              Due to invalid src IP    : 0
              Due to other errors      : 0
  IP sub ARP reqs with default action  : 24
```

Table 8 describes the significant fields shown in the display.

Table 8 show ip subscriber statistics arp Field Descriptions

Field	Description
Dst on ISG	Number of ARP requests that ISG replied to for a destination on ISG.
Src/Dst in same subnet	Number of ARP requests that ISG replied to that had a source and destination IP address in the same subnet.
For route back to CPE	Number of ARP requests that ISG ignored because the destination IP address is on the same VLAN as the customer premises equipment (CPE).
For no routes to dest.	Number of ARP requests ignored by ISG because there was no route to the destination.
Gratuitous	Number of ARP requests ignored by ISG because they are gratuitous. A gratuitous ARP request is issued by a device for the sole purpose of keeping other devices informed of its presence on the network.
IP sub ARP reqs with default action	Number of ARP requests for which ISG performed no special action.

Related Commands

Command	Description
clear ip subscriber	Disconnects and removes all or specified ISG IP subscriber sessions.
ip subscriber list	Creates an IP subscriber static server group.

show platform isg session

To display the number of active Intelligent Services Gateway (ISG) subscriber sessions for a line card and the features applied on a session, use the **show platform isg session** command in privileged EXEC mode.

show platform isg session *session-id subinteface-number* [**detail**]

Syntax Description

session-id	Specifies the ID of a particular session.
subinteface-number	Specifies the subinterface number.
detail	(Optional) Displays platform information for the features that are applied on the session.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)S	This command was introduced.

Usage Guidelines

The **show platform isg session** command displays the total number of active subscriber sessions on the line card and information about the features that are configured on a session. For example, QoS or SACL.

Examples

This example shows the output for all installed line cards:

```
Router# show platform isg session 15 0 detail

if_num 14 va_if_num 0 pid 15 type IPSIP flags 0x0 state BOUND hvlan v1(vc) 1014 v2 1200 0
dbg off
 STATS(pkts, bytes) RX(0, 0) ctrl(0, 0) drop(0, 0) TX(0, 0) ctrl(0, 0) drop(0, 0)
--------------------------------------------------========================================

TenGigabitEthernet4/2.1 - if_number 14 15 policymap pmap-brr1-parent dir Output
 np 1 port 0 pm_num 4 lookuptype 1 flowid 256
---------------------------------------------------
 policymap pmap-brr1-parent classid 0 dfs classid 2
 classmap config:   cmap flags 0x6 feature flags 0x9
  queue config: gqid/pgqid 4/2
  police config: N/A  marking config: N/A
  WRED config: N/A
 classmap instance: cfn statid 0
   node handle: B,4,128   queue: fid0/fid1/sel/spl 128/128/0/0
   statid: commit/excess/drop 1294464/1327232/1360000
 policy pmap-brr1-parent classid 0 dfs classid 2  level 0
---------------------------------------------------------------
```

```
  Statistics type      Packet count       Byte count
    queue:
           commit               0                0
           excess               0                0
             drop               0                0
        cur depth               0

---------------------------------------------------
 policymap pmap-brr-child1 classid 1 dfs classid 0
 classmap config:   cmap flags 0x4 feature flags 0x100
  police config:cir/cbs: 50000000/1562500 pir/pbs: 0/1562500 clr/mef/algo: 0/0/1
   0:XMIT, Mark , cosi_cos 0 cos_cosi 0 dscp 0/0 cos 0/0 cosi 0/0  exp_top 0/0 exp_imp 0/0
   1:DROP, Mark , cosi_cos 0 cos_cosi 0 dscp 0/0 cos 0/0 cosi 0/0  exp_top 0/0 exp_imp 0/0
  2:DROP, Mark , cosi_cos 0 cos_cosi 0 dscp 0/0 cos 0/0 cosi 0/0  exp_top 0/0 exp_imp 0/0
marking config: N/A
  WRED config: N/A
 classmap instance: cfn statid 508327
   node handle: B,4,128   queue: fid0/fid1/sel/spl 128/128/0/0
   statid: commit/excess/drop 1294464/1327232/1360000
   police handle: np/index/type 1/1/fast tb 65697 statid: conform/exceed/violate
115116/115117/115118
   POLICE profile[0] inuse 1 cir/cbs 50000000/1562500 pir/pbs 0/1562500 clr/mef/algo
0/0x0/1
   [D]POLICE - index 0 cir/cbs: 6250000/1559756 pir/pbs: 0/0 clr/mef/algo: 0/0/1
 policy pmap-brr-child1 classid 1 dfs classid 0  level 1
---------------------------------------------------------------
  Statistics type      Packet count       Byte count
   classification               0                0
   police:
          conform               0                0
           exceed               0                0
          violate               0                0

 --
  tcam index table result: 0x30000C001 0x0 0x0 0x0
  flow hash table result: 0x7C1A70301000080 0x100000003
 FLW-07C1A703 01000080 00000001 00000003
  TM - Concat:NO, TMc:NO, Special_Q:NO, FID1:128, FID2:128
  Flow Stat:508327, Plcr1 TB/Stat-1/3, Plcr2 TB/Stat-0/0

----------------------------------------------
 Level: 4 Index: 128 Child Index/Inuse: 65535/0 Flags: VHC PDL       Wf    M.WFQ 1020 QL
2/5-131072 norm
 WFQ level 4 index 0 weight 10 inuse 3
  [D]WFQ - level:4, index:0  Weight Commit/Excess: 10/10
  [D]Entity Param - level:4 index:128 Mode/Priority: Enabled/Normal
      Shape mode/factor: Unshaped/One Profiles- WRED/Scale:2/5 Shape:0 WFQ:0
 --
 Level: 3 Index: 16 Child Index/Inuse: 128/1 Flags: RHC PDL       WfSh
ServProf:1/flags/oh:---/0
 SHAPE level 3 index 1 inuse 1 cir 800000000 cbs 80216064 pir 800000000 pbs 3211264
  [D]SHAPE - level:3 index:1 bFS:0 cir:100000000 cbs:10027008 pir:100000000 pbs:401408
 WFQ level 3 index 1 weight 81 inuse 1
  [D]WFQ - level:4, index:33  Weight Commit/Excess: 81/1
  [D]Entity Param - level:3 index:16 Mode/Priority: Enabled/Normal
      Shape mode/factor: Explicit/One Profiles- WRED/Scale:0/0 Shape:1 WFQ:33
 --
 Level: 2 Index: 0 Child Index/Inuse: 0/2 Flags: RHC I         Wf
 SHAPE level 2 index 0 inuse 1 cir 9920000 cbs 1007616 pir 9920000 pbs 1007616
  [D]SHAPE - level:2 index:0 bFS:0 cir:1240000 cbs:125952 pir:1240000 pbs:125952
 WFQ level 2 index 0 weight 2 inuse 1
  [D]WFQ - level:2, index:0  Weight Commit/Excess: 2/2
  [D]Entity Topology - level:2 index:0Child First/Total:0/32 L34 mode:0 ServProf:0
  [D]Entity Param - level:2 index:0 Mode/Priority: Enabled/Propagated
```

```
      Shape mode/factor: Unshaped/Half Profiles- WRED/Scale:0/0 Shape:0 WFQ:0
 --
 Level: 1 Index: 0 Child Index/Inuse: 0/1 Flags: RNC I         Wf
 ***
---------------------------------------------------
 policymap pmap-brr-child1 classid 0 dfs classid 1
 classmap config:   cmap flags 0x4 feature flags 0x1000
  police config: N/A
  marking config: on  coso 1
  WRED config: N/A
 classmap instance: cfn statid 508328
   node handle: B,4,128   queue: fid0/fid1/sel/spl 128/128/0/0
   statid: commit/excess/drop 1294464/1327232/1360000
 policy pmap-brr-child1 classid 0 dfs classid 1  level 1
---------------------------------------------------------------
  Statistics type      Packet count       Byte count
   classification                0                0

 --
  tcam index table result: 0x101300000000 0x400500000000 0x0 0x0
  flow hash table result: 0x7C1A80301000080 0x0
 FLW-07C1A803 01000080 00000000 00000000
  TM - Concat:NO, TMc:NO, Special_Q:NO, FID1:128, FID2:128
  Flow Stat:508328, Plcr1 TB/Stat-0/0, Plcr2 TB/Stat-0/0

----------------------------------------------
 Level: 4 Index: 128 Child Index/Inuse: 65535/0 Flags: VHC PDL       Wf    M.WFQ 1020 QL
2/5-131072 norm
 WFQ level 4 index 0 weight 10 inuse 3
  [D]WFQ - level:4, index:0  Weight Commit/Excess: 10/10
  [D]Entity Param - level:4 index:128 Mode/Priority: Enabled/Normal
      Shape mode/factor: Unshaped/One Profiles- WRED/Scale:2/5 Shape:0 WFQ:0
 --
 Level: 3 Index: 16 Child Index/Inuse: 128/1 Flags: RHC PDL       WfSh
ServProf:1/flags/oh:---/0
 SHAPE level 3 index 1 inuse 1 cir 800000000 cbs 80216064 pir 800000000 pbs 3211264
  [D]SHAPE - level:3 index:1 bFS:0 cir:100000000 cbs:10027008 pir:100000000 pbs:401408
 WFQ level 3 index 1 weight 81 inuse 1
  [D]WFQ - level:4, index:33  Weight Commit/Excess: 81/1
  [D]Entity Param - level:3 index:16 Mode/Priority: Enabled/Normal
      Shape mode/factor: Explicit/One Profiles- WRED/Scale:0/0 Shape:1 WFQ:33
 --
 Level: 2 Index: 0 Child Index/Inuse: 0/2 Flags: RHC I         Wf
 SHAPE level 2 index 0 inuse 1 cir 9920000 cbs 1007616 pir 9920000 pbs 1007616
  [D]SHAPE - level:2 index:0 bFS:0 cir:1240000 cbs:125952 pir:1240000 pbs:125952
 WFQ level 2 index 0 weight 2 inuse 1
  [D]WFQ - level:2, index:0  Weight Commit/Excess: 2/2
  [D]Entity Topology - level:2 index:0Child First/Total:0/32 L34 mode:0 ServProf:0
  [D]Entity Param - level:2 index:0 Mode/Priority: Enabled/Propagated
      Shape mode/factor: Unshaped/Half Profiles- WRED/Scale:0/0 Shape:0 WFQ:0
 --
 Level: 1 Index: 0 Child Index/Inuse: 0/1 Flags: RNC I         Wf
```

Related Commands

Command	Description
show platform isg session-count	Displays the number of active ISG subscriber sessions by line card.
show subscriber session	Displays information about subscriber sessions on the ISG router.

show platform isg session-count

To display the number of active Intelligent Services Gateway (ISG) subscriber sessions by line card, use the **show platform isg session-count** command in privileged EXEC mode.

show platform isg session-count {**all** | *slot*}

Syntax Description

all	Displays information for all line cards on the router.
slot	Displays information for a specific line card.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)SRD4	This command was integrated into Cisco IOS Release 12.2(33)SRD4.
12.2(33)SRE1	This command was modified. The maximum session count, maximum session instance, and port group were added to the output.

Usage Guidelines

The **show platform isg session-count** command displays either the total number of active subscriber sessions on the router, with individual totals by line card, or it displays the details for an individual line card in a specific slot.

The Cisco 7600 router limits the number of supported subscriber sessions per line card and per router chassis. Use this command to monitor the number of currently active sessions to ensure that the following limits are not exceeded:

- Cisco 7600 chassis—32,000 subscriber sessions
- ES+ line card—4000 subscriber sessions per port group; 16,000 sessions per line card
- SIP400 line card—8000 subscriber sessions

Examples

The following example shows the output for all installed line cards:

```
Router# show platform isg session-count all

Total sessions per chassis : 8000
 Slot   Sess-count  Max Sess-count
 ----   ----------  --------------
    5         8000           16000
```

The following example shows the output for the ES+ line card in slot 5:

```
Router# show platform isg session-count 5

ES+ line card
 Sessions on a port-channel are instantiated on all member ports
```

```
Port-group          Sess-instance   Max Sess-instance
----------          -------------   -----------------
Gig5/1-Gig5/5            4000                4000
Gig5/16-Gig5/20          4000                4000
```

Table 9 describes the significant fields shown in the display, in alphabetical order.

Table 9 show platform isg session-count Field Descriptions

Field	Description
Max Sess-count	Maximum number of sessions allowed per line card.
Max Sess-instance	Maximum number of session instances allowed per port group.
Port-group	Port numbers included in each port group.
Sess-count	Total number of active sessions per line card.
Sess-instance	Total number of session instances per port group.
Slot	Number of the router slot in which the card is installed.
Total sessions per chassis	Total number of sessions for all line cards on the router.

Related Commands

Command	Description
show subscriber session	Displays information about subscriber sessions on the ISG router.

show policy-map type control

To display information about Intelligent Services Gateway (ISG) control policy maps, use the **show policy-map type control** command in privileged EXEC mode.

show policy-map type 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.

Usage Guidelines

Use the **show policy-map type control** command to display information about ISG control policies, including statistics on the number of times each policy-rule within the policy map has been executed

Examples

The following example shows sample output for the **show policy-map type control** command:

```
Router# show policy-map type control

Rule: internal-rule-acct-logon
  Class-map:  always event account-logon
    Action: 1 authenticate aaa list default
    Executed0

Key:
  "Exec" - The number of times this rule action line was executed
```

Related Commands

Command	Description
clear policy-map type control	Clears ISG control policy map counters.
policy-map type control	Creates or modifies a control policy map, which defines an ISG control policy.
show class-map type control	Displays information about ISG control class maps.

show policy-map type service

To displays the contents of Intelligent Services Gateway (ISG) service policy maps and service profiles and session-related attributes, use the **show policy-map type service** command in privileged EXEC mode.

show policy-map type 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.

Examples

The following example shows the configuration of a service profile called "prep_service" on a AAA server and the corresponding sample output for the **show policy-map type service** command.

Service Profile Configuration

```
Configuration of prep_service on simulator radius subscriber 8
 authentication prep_service pap cisco
 idle-timeout 600
 vsa cisco generic 1 string "traffic-class=input access-group 102"
```

Sample Output of show policy-map type service Command

```
Router# show policy-map type service

Current policy profile DB contents are:
  Profile name: prep_service, 4 references
    idletime             600 (0x258)
    traffic-class        "input access-group 102"
```

Table 10 describes the significant fields shown in the display.

Table 10 show policy-map type service Field Descriptions

Field	Description
Current policy profile DB contents are	Displays all of the service profiles and service policy maps on the system.
Profile name	Name of a service profile or policy map.

Related Commands

Command	Description
show class-map type traffic	Displays ISG traffic class maps and their matching criteria.

show processes cpu monitor

To display CPU utilization statistics that will be updated at specified intervals, use the **show processes cpu monitor** command in user EXEC or privileged EXEC mode.

show processes cpu monitor [**interval** *minutes*]

Syntax Description

interval *seconds*	(Optional) Interval, in minutes, at which the display will be updated. Range: 5 to 3600. Default: 5.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

The **show processes cpu monitor** command allows you to monitor CPU utilization statistics by displaying updated statistics at regular intervals. While the statistics are being displayed, the command-line interface will prompt you to enter "E" to end the display or "F" to freeze the display.

Examples

The following example shows sample output for the **show processes cpu monitor** command:

```
Router# show processes cpu monitor

CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID Runtime(ms)   Invoked      uSecs    5Sec   1Min     5Min    TTY Process
   3       772         712       1084    0.08%  0.04%    0.02%    0    Exec
  67       276        4151         66    0.08%  0.03%    0.01%    0 L2TP mgmt daemon
 116       604        2263        266    0.16%  0.05%    0.01%    0 IDMGR CORE

End = e    Freeze = f
Enter Command:
```

Table 11 describes the significant fields shown in the display.

Table 11 show processes cpu monitor Field Descriptions

Field	Description
CPU utilization for five seconds	CPU utilization for the last 5 seconds and the percentage of CPU time spent at the interrupt level.
one minute	CPU utilization for the last minute and the percentage of CPU time spent at the interrupt level.
five minutes	CPU utilization for the last 5 minutes and the percentage of CPU time spent at the interrupt level.
PID	Process ID.

Table 11 show processes cpu monitor Field Descriptions (continued)

Field	Description
Runtime(ms)	CPU time the process has used (in milliseconds).
Invoked	Number of times the process has been invoked.
uSecs	Microseconds of CPU time for each process invocation.
5Sec	CPU utilization by task in the last 5 seconds.
1Min	CPU utilization by task in the last minute.
5Min	CPU utilization by task in the last 5 minutes.
TTY	Terminal that controls the process.
Process	Name of the process.

Related Commands

Command	Description
show processes cpu	Displays CPU utilization information about the active processes in a device.

show pxf cpu iedge

To display Parallel eXpress Forwarding (PXF) policy and template information, use the **show pxf cpu iedge** command in privileged EXEC mode.

show pxf cpu iedge [**detail** | **policy** *policy-name* | **template**]

Syntax Description

detail	(Optional) Displays detailed information about policies and templates.
policy *policy-name*	(Optional) Displays summary policy information.
template	(Optional) Displays summary template information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2S	This command was introduced.

Examples

The following example shows PXF template information:

```
Router# show pxf cpu iedge template

Super ACL name                   OrigCRC   Class Count    CalcCRC
1sacl_2                         4EA94046   2             00000000
if_info 71BA3F20
```

Related Commands

Command	Description
show pxf statistics	Displays a summary of PXF statistics.

show pxf cpu isg

To display Parallel eXpress Forwarding (PXF) Intelligent Services Gateway (ISG) policy and template information, use the **show pxf cpu isg** command in privileged EXEC mode.

show pxf cpu isg [**detail** | **policy** *policy-name* | **template**]

Syntax Description

detail	(Optional) Displays detailed information about ISG policies and templates.
policy *policy-name*	(Optional) Displays summary ISG policy information.
template	(Optional) Displays summary ISG template information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2SB	This command was introduced.

Examples

The following example shows the ISG template information:

```
Router# show pxf cpu isg template

Super ACL name                  OrigCRC   Class Count    CalcCRC
1sacl_2                        4EA94046   2             00000000
if_info 71BA3F20
```

Related Commands

Command	Description
show pxf statistics	Displays chassis-wide, summary PXF statistics.

show radius-proxy client

To display information about Intelligent Services Gateway (ISG) RADIUS proxy client devices, use the **show radius-proxy client** command in privileged EXEC mode.

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

Syntax Description

ip-address	IP address of the RADIUS proxy client.
vrf *vrf-name*	(Optional) VRF associated with the RADIUS proxy client. **Note** The **vrf** *vrf-name* option is not supported in 12.2(31)SB2.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The **show radius-proxy client** command can be used to find out which subscribers are associated with which RADIUS clients.

Examples

The following example shows sample output for the **show radius-proxy client** command:

```
Router# show radius-proxy client 10.45.45.3

Configuration details for client 10.45.45.3
 Shared secret:     blue#@!$%&/       Msg Auth Ignore:   No
 Local auth port:   1111                 Local acct port:   2222
 Acct method list: FWDACCT
Session Summary:
      RP ID       IP Address
   1. 687865867   10.1.1.1
```

Table 12 describes the significant fields shown in the display.

Table 12 show radius-proxy client Field Descriptions

Field	Description
Shared secret	Shared secret between ISG RADIUS proxy and the client device.
Msg Auth Ignore	Indicates whether message-authenticator validation is performed for RADIUS packets coming from this client.
Local auth port	Port on which ISG listens for authentication packets from this client.
Local acct port	Port on which ISG listens for accounting packets from this client.

Table 12 show radius-proxy client Field Descriptions (continued)

Field	Description
Acct method list	Method list to which ISG RADIUS proxy forwards accounting packets.
Session Summary	Summary of the ISG sessions associated with the specified client device.
RP ID	ISG RADIUS proxy identifier for the session.
IP Address	IP address associated with the session.

Related Commands

Command	Description
show radius-proxy session	Displays information about specific ISG RADIUS proxy sessions.

show radius-proxy session

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

show 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.

Examples

The following example shows sample output for the **show radius-proxy session** command:

```
Router# show radius-proxy session id 1694498816

Session Keys:
  Caller ID:         000b.4691.e2e3
Other Attributes:
  Username:          aash
  User IP:           unassigned
  Called ID:
Client Information:
  NAS IP:            10.45.45.2
  NAS ID:            localhost
State Details:
  State:             authenticated
  Timer:             ip-address (timeout: 240s, remaining: 166s)
```

Related Commands

Command	Description
show radius-proxy client	Displays information about ISG RADIUS proxy client devices.

show redirect group

To display information about Intelligent Services Gateway (ISG) Layer 4 redirect server groups, use the **show redirect group** command in privileged EXEC mode.

show redirect group [*group-name*]

Syntax Description

group-name	(Optional) Specific server group for which to display information.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use the **show redirect translations** command without the *group-name* argument to display information about all Layer 4 redirect server groups.

Examples

The following example shows sample output for the **show redirect group** command:

```
Router# show redirect group redirect-group-default

Showing all servers of the group redirect-group-default
Server created : using cli
Server Port
10.30.81.22 8090
```

Related Commands

Command	Description
redirect server-group	Defines a group of one or more servers that make up a named ISG Layer 4 redirect server group.
redirect to (ISG)	Redirects ISG Layer 4 traffic to a specified server or server group.
server (ISG)	Adds a server to an ISG Layer 4 redirect server group.
show redirect translations	Displays information about the ISG Layer 4 redirect mappings for subscriber sessions.

show redirect translations

To display information about the Intelligent Services Gateway (ISG) Layer 4 redirect mappings for subscriber sessions, use the **show redirect translations** command in privileged EXEC mode.

show redirect translations [**ip** *ip-address*]

Syntax Description

ip *ip-address*	(Optional) Subscriber IP address.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SB8	This command was modified. Information about the number of redirect translations was added to the output.
12.2(33)XNE1	This command was integrated into Cisco IOS Release 12.2(33)XNE1.
12.2(33)SRD4	This command was integrated into Cisco IOS Release 12.2(33)SRD4.
12.2(33)SRE1	This command was integrated into Cisco IOS Release 12.2(33)SRE1.

Usage Guidelines

Use the **show redirect translations** command without the **ip** *ip-address* keyword and argument to display Layer 4 redirect mappings for all subscriber sessions.

Examples

The following is sample output from the **show redirect translations** command displaying information about each active redirect translation:

```
Router# show redirect translations

Load for five secs: 1%/0%; one minute: 2%; five minutes: 2%
Time source is hardware calendar, *11:48:06.383 PST Wed Oct 21 2009
Maximum allowed number of L4 Redirect translations per session: 5

Destination IP/port    Server IP/port    Prot  In Flags  Out Flags  Timestamp
10.0.1.2        23     10.0.2.2   23     TCP                        Oct 21 2009 11:48:01
10.0.1.2        23     10.0.2.2   23     TCP                        Oct 21 2009 11:48:01
10.0.1.2        23     10.0.2.2   23     TCP                        Oct 21 2009 11:48:01

Total Number of Translations: 3

Highest number of L4 Redirect: 3 by session with source IP 10.0.0.2
```

Table 9 describes the significant fields shown in the display, in alphabetical order.

Table 13 show redirect translations Field Descriptions

Field	Description
Destination IP/port	IP address and port number of the connection destination.
Highest number of L4 Redirect	Highest number of current redirects for any active session.
In Flags, Out Flags	TCP flags. For example, ACK, FIN, SYN, or Null.
Load for five secs; one minute; five minutes	CPU usage (in percentage) at different time intervals.
Maximum number of L4 Redirect translations per session	Redirect limit set with the **redirect session-limit** command.
Prot	Protocol used, either TCP or User Data Protocol (UDP).
Server IP/port	IP address and port number of the redirect server.
Total Number of Translations	Total number of active translations.

Related Commands

Command	Description
redirect server-group	Defines a group of one or more servers that make up a named ISG Layer 4 redirect server group.
redirect session-limit	Sets the maximum number of Layer 4 redirects allowed for each ISG subscriber session.
redirect to (ISG)	Redirects ISG Layer 4 traffic to a specified server or server group.
server (ISG)	Adds a server to an ISG Layer 4 redirect server group.
show redirect group	Displays information about ISG Layer 4 redirect server groups.

show sgi

To display information about current Service Gateway Interface (SGI) sessions or statistics, use the **show sgi** command in privileged EXEC mode.

show sgi {**session** | **statistics**}

Syntax Description

session	Displays information about the current SGI session.
statistics	Displays information about the current SGI statistics

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows information about SGI sessions started and currently running, including the running state:

```
Router# show sgi session

sgi sessions: open 1(max 10, started 15
session id:1;started at 9:08:05; state OPEN
```

The following example shows statistical information about SGI and the SGI processes that have been started:

```
Router# show sgi statistics

sgi statistics
total messages received 45
current active messages 5; maximum active messages 7
total isg service requests 4
current active services 2; maximum active services 2

sgi process statistics
process sgi handler 1
pid 95, cpu percent (last minute) 1, cpu runtime 10(msec), memory accocated 4200 (bytes)
```

Related Commands

Command	Description
debug sgi	Enables debugging for SGI.
sgi beep listener	Enables SGI.
test sgi xml	Allows onboard testing of SGI XML files when an external client is not available.

show ssm

To display Segment Switching Manager (SSM) information for switched Layer 2 segments, use the **show ssm** command in privileged EXEC mode.

show ssm {**cdb** | **feature id** [*feature-id*] | **id** | **memory** [**chunk variable** {**feature** | **queue** | **segment**} | **detail**] | **segment id** [*segment-id*] | **switch id** [*switch-id*]}

Syntax Description

cdb	Displays information about the SSM capabilities database.
feature id	Displays information about SSM feature settings.
feature-id	(Optional) Displays information for a specific feature ID.
id	Displays information for all SSM IDs.
memory	Displays memory usage information.
chunk variable	(Optional) Displays memory usage information for memory consumed by variable chunks.
feature	Displays information about memory consumed by the feature.
queue	Displays information about memory consumed by the queue.
segment	Displays information about memory consumed by the segment.
detail	(Optional) Displays detailed memory usage information.
segment id	Displays information about SSM segment settings.
segment-id	(Optional) Displays information for a specific SSM segment.
switch id	Displays information about SSM switch settings.
switch-id	(Optional) Displays information for a specific SSM switch ID.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(22)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use the **show ssm** command to determine the segment ID for an active switched Layer 2 segment. The segment ID can be used with the **debug condition xconnect** command to filter debug messages by segment.

Examples

The following example shows sample output for the **show ssm cdb** command. The output for this command varies depending on the type of hardware being used.

```
Router# show ssm cdb

Switching paths active for class SSS:
-------------------------------------
```

```
        |FR |Eth|Vlan|ATM|HDLC|PPP/AC|L2TP|L2TPv3|L2F|PPTP|ATM/AAL5|ATM/VCC|
--------+---+---+----+---+----+------+----+------+---+----+--------+-------+
FR      | E | E | E  |E/-| E  |  E   | E  |  E   |-/-|-/- |   E    |   E   |
Eth     | E | E | E  |E/-| E  |  E   | E  |  E   |-/-|-/- |   E    |   E   |
Vlan    | E | E | E  |E/-| E  |  E   | E  |  E   |-/-|-/- |   E    |   E   |
ATM     |-/E|-/E|-/E |-/-|-/E | -/E  |-/E | -/E  |-/-|-/- |  -/E   |  -/E  |
HDLC    | E | E | E  |E/-| E  |  E   | E  |  E   |-/-|-/- |   E    |   E   |
PPP/AC  | E | E | E  |E/-| E  |  E   | E  |  E   |-/-|-/- |   E    |   E   |
L2TP    | E | E | E  |E/-| E  |  E   | E  | -/-  | E | E  |   E    |   E   |
L2TPv3  | E | E | E  |E/-| E  |  E   |-/- |  E   |-/-|-/- |   E    |   E   |
L2F     |-/-|-/-|-/- |-/-|-/- | -/-  | E  | -/-  | E | E  |  -/-   |  -/-  |
PPTP    |-/-|-/-|-/- |-/-|-/- | -/-  | E  | -/-  | E | E  |  -/-   |  -/-  |
ATM/AAL5| E | E | E  |E/-| E  |  E   | E  |  E   |-/-|-/- |   E    |   E   |
ATM/VCC | E | E | E  |E/-| E  |  E   | E  |  E   |-/-|-/- |   E    |   E   |
ATM/VPC | E | E | E  |E/-| E  |  E   | E  |  E   |-/-|-/- |   E    |   E   |
ATM/Cell| E | E | E  |E/-| E  |  E   | E  |  E   |-/-|-/- |   E    |   E   |
AToM    |-/E|-/E|-/E |-/-|-/E | -/E  |-/- | -/E  |-/-|-/- |  -/E   |  -/E  |
PPP     |-/-|-/-|-/- |-/-|-/- | -/-  | E  | -/-  | E | E  |  -/-   |  -/-  |
PPPoE   |-/-|-/-|-/- |-/-|-/- | -/-  | E  | -/-  | E | E  |  -/-   |  -/-  |
PPPoA   |-/-|-/-|-/- |-/-|-/- | -/-  | E  | -/-  | E | E  |  -/-   |  -/-  |
Lterm   |-/-|-/-|-/- |-/-|-/- | -/-  | E  | -/-  | E | E  |  -/-   |  -/-  |
TC      |-/-|-/-|-/- |-/-|-/- | -/-  |-/- | -/-  |-/-|-/- |  -/-   |  -/-  |
IP-If   |-/-|-/-|-/- |-/-|-/- | -/-  |-/- | -/-  |-/-|-/- |  -/-   |  -/-  |
IP-SIP  |-/-|-/-|-/- |-/-|-/- | -/-  |-/- | -/-  |-/-|-/- |  -/-   |  -/-  |
VFI     |-/E|-/E|-/E |-/-|-/E | -/E  |-/- | -/E  |-/-|-/- |  -/E   |  -/E  |

        |ATM/Cell|AToM|PPP|PPPoE|PPPoA|Lterm|TC |IP-If|IP-SIP|VFI|
--------+--------+----+---+-----+-----+-----+---+-----+------+---+
FR      |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
Eth     |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
Vlan    |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
ATM     |  -/E   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
HDLC    |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
PPP/AC  |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
L2TP    |   E    |-/- | E |  E  |  E  |  E  |-/-| -/- | -/-  |-/-|
L2TPv3  |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
L2F     |  -/-   |-/- | E |  E  |  E  |  E  |-/-| -/- | -/-  |-/-|
PPTP    |  -/-   |-/- | E |  E  |  E  |  E  |-/-| -/- | -/-  |-/-|
ATM/AAL5|   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
ATM/VCC |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
ATM/VPC |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
ATM/Cell|   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
AToM    |  -/E   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|

PPP     |  -/-   |-/- | E |  E  |  E  |  E  |-/-| -/- | -/-  |-/-|
PPPoE   |  -/-   |-/- | E |  E  |  E  |  E  |-/-| -/- | -/-  |-/-|
PPPoA   |  -/-   |-/- | E |  E  |  E  |  E  |-/-| -/- | -/-  |-/-|
Lterm   |  -/-   |-/- | E |  E  |  E  |  E  | E |  E  |  E   |-/-|
TC      |  -/-   |-/- |-/-| -/- | -/- |  E  | E |  E  |  E   |-/-|
IP-If   |  -/-   |-/- |-/-| -/- | -/- |  E  | E |  E  | -/-  |-/-|
IP-SIP  |  -/-   |-/- |-/-| -/- | -/- |  E  | E | -/- |  E   |-/-|
VFI     |  -/E   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|

Switching paths active for class ADJ:
-------------------------------------

        |FR |Eth|Vlan|ATM|HDLC|PPP/AC|L2TP|L2TPv3|L2F|PPTP|ATM/AAL5|ATM/VCC|
--------+---+---+----+---+----+------+----+------+---+----+--------+-------+
FR      | E | E | E  |E/-| E  |  E   |E/- |  E   |-/-|-/- |   E    |   E   |
Eth     | E | E | E  |E/-| E  |  E   |E/- |  E   |-/-|-/- |   E    |   E   |
Vlan    | E | E | E  |E/-| E  |  E   |E/- |  E   |-/-|-/- |   E    |   E   |
ATM     |-/E|-/E|-/E |-/-|-/E | -/E  |-/- | -/E  |-/-|-/- |  -/E   |  -/E  |
HDLC    | E | E | E  |E/-| E  |  E   |E/- |  E   |-/-|-/- |   E    |   E   |
PPP/AC  | E | E | E  |E/-| E  |  E   |E/- |  E   |-/-|-/- |   E    |   E   |
L2TP    |-/E|-/E|-/E |-/-|-/E | -/E  | E  | -/-  |E/-|E/- |  -/E   |  -/E   |
L2TPv3  | E | E | E  |E/-| E  |  E   |-/- |  E   |-/-|-/- |   E    |   E    |
L2F     |-/-|-/-|-/- |-/-|-/- | -/-  |-/E | -/-  |-/-|-/- |  -/-   |  -/-   |
PPTP    |-/-|-/-|-/- |-/-|-/- | -/-  |-/E | -/-  |-/-|-/- |  -/-   |  -/-   |
ATM/AAL5| E | E | E  |E/-| E  |  E   |E/- |  E   |-/-|-/- |   E    |   E    |
ATM/VCC | E | E | E  |E/-| E  |  E   |E/- |  E   |-/-|-/- |   E    |   E    |
ATM/VPC | E | E | E  |E/-| E  |  E   |E/- |  E   |-/-|-/- |   E    |   E    |
ATM/Cell| E | E | E  |E/-| E  |  E   |E/- |  E   |-/-|-/- |   E    |   E    |
AToM    |-/E|-/E|-/E |-/-|-/E | -/E  |-/- | -/E  |-/-|-/- |  -/E   |  -/E   |
PPP     |-/-|-/-|-/- |-/-|-/- | -/-  |-/E | -/-  |-/-|-/- |  -/-   |  -/-   |
PPPoE   |-/-|-/-|-/- |-/-|-/- | -/-  |-/E | -/-  |-/-|-/- |  -/-   |  -/-   |
PPPoA   |-/-|-/-|-/- |-/-|-/- | -/-  |-/E | -/-  |-/-|-/- |  -/-   |  -/-   |
Lterm   |-/-|-/-|-/- |-/-|-/- | -/-  |-/E | -/-  |-/-|-/- |  -/-   |  -/-   |
TC      |-/-|-/-|-/- |-/-|-/- | -/-  |-/- | -/-  |-/-|-/- |  -/-   |  -/-   |
IP-If   |-/-|-/-|-/- |-/-|-/- | -/-  |-/- | -/-  |-/-|-/- |  -/-   |  -/-   |
IP-SIP  |-/-|-/-|-/- |-/-|-/- | -/-  |-/- | -/-  |-/-|-/- |  -/-   |  -/-   |
VFI     |E/-| E | E  |E/-|E/- | E/-  |-/- | -/E  |-/-|-/- |   E    |   E    |

        |ATM/Cell|AToM|PPP|PPPoE|PPPoA|Lterm|TC |IP-If|IP-SIP|VFI|
--------+--------+----+---+-----+-----+-----+---+-----+------+---+
FR      |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/E|
Eth     |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  | E |
Vlan    |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  | E |
ATM     |  -/E   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/E|
HDLC    |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/E|
PPP/AC  |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/E|
L2TP    |  -/E   |-/- |E/-| E/- | E/- | E/- |-/-| -/- | -/-  |-/-|
L2TPv3  |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
L2F     |  -/-   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
PPTP    |  -/-   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
ATM/AAL5|   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  | E |
ATM/VCC |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  | E |
ATM/VPC |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  | E |
ATM/Cell|   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  | E |
AToM    |  -/E   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/E|
PPP     |  -/-   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
PPPoE   |  -/-   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
PPPoA   |  -/-   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
Lterm   |  -/-   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
TC      |  -/-   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
IP-If   |  -/-   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
IP-SIP  |  -/-   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
VFI     |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|

Key:
  '-' - switching type is not available
  'R' - switching type is available but not enabled
  'E' - switching type is enabled
  'D' - switching type is disabled
```

The following example displays SSM output of the **show ssm id** command on a device with one active Layer 2 Tunnel Protocol Version 3 (L2TPv3) segment and one active Frame Relay segment. The segment ID field is shown in bold.

```
Router# show ssm id

SSM Status: 1 switch
   Switch-ID 4096 State: Open
     Segment-ID: 8193 Type: L2TPv3[8]
       Switch-ID:                    4096
       Physical intf:                Remote
       Allocated By:                 This CPU
       Class:                        SSS
```

```
         State:                        Active
         L2X switching  context:
         Session ID Local 16666 Remote 54742
         TxSeq 0 RxSeq 0
         Tunnel end-point addr Local 10.1.1.2 Remote 10.1.1.1
         SSS Info Switch Handle 0x98000000 Ciruit 0x1B19510
         L2X Encap [24 bytes]
          45 00 00 00 00 00 00 00 FF 73 B7 86 01 01 01 02
          01 01 01 01 00 00 D5 D6
       Class:                        ADJ
         State:                        Active
         L2X H/W Switching Context:
         Session Id Local 16666 Remote 54742
         Tunnel Endpoint Addr Local 10.1.1.2 Remote 10.1.1.1
         Adjacency 0x1513348 [complete] PW IP, Virtual3:16666
         L2X Encap [24 bytes]
          45 00 00 00 00 00 00 00 FF 73 B7 86 01 01 01 02
          01 01 01 01 00 00 D5 D6

     Segment-ID: 4096 Type: FR[1]
       Switch-ID:                    4096
       Physical intf:                Local
       Allocated By:                 This CPU
       Class:                        SSS
         State:                        Active
         AC Switching Context:         Se2/0:200
         SSS Info - Switch Handle=0x98000000 Ckt=0x1B194B0
         Interworking 0 Encap Len 0 Boardencap Len 0 MTU 1584
       Class:                        ADJ
         State:                        Active
         AC Adjacency context:
         adjacency = 0x1513618 [complete] RAW Serial2/0:200
```

Additional output displayed by this command is either self-explanatory or used only by Cisco engineers for internal debugging of SSM processes.

The following example shows sample output for the **show ssm memory** command:

```
Router# show ssm memory

  Allocator-Name                  In-use/Allocated            Count
  ----------------------------------------------------------------------------
  SSM CM API large segment  :        208/33600      (  0%) [      1] Chunk
  SSM CM API medium segment :        144/20760      (  0%) [      1] Chunk
  SSM CM API segment info c :        104/160        ( 65%) [      1]
  SSM CM API small segment  :          0/19040      (  0%) [      0] Chunk
  SSM CM inQ interrupt msgs :          0/20760      (  0%) [      0] Chunk
  SSM CM inQ large chunk ms :          0/33792      (  0%) [      0] Chunk
  SSM CM inQ msgs           :        104/160        ( 65%) [      1]
  SSM CM inQ small chunk ms :          0/20760      (  0%) [      0] Chunk
  SSM DP inQ msg chunks     :          0/10448      (  0%) [      0] Chunk
  SSM Generic CM Message    :          0/3952       (  0%) [      0] Chunk
  SSM HW Class Context      :         64/10832      (  0%) [      1] Chunk
  SSM ID entries            :        144/11040      (  1%) [      3] Chunk
  SSM ID tree               :         24/80         ( 30%) [      1]
  SSM INFOTYPE freelist DB  :       1848/2016       ( 91%) [      3]
  SSM SEG Base              :        240/34064      (  0%) [      2] Chunk
  SSM SEG freelist DB       :       5424/5592       ( 96%) [      3]
  SSM SH inQ chunk msgs     :          0/5472       (  0%) [      0] Chunk
  SSM SH inQ interrupt chun :          0/5472       (  0%) [      0] Chunk
  SSM SW Base               :         56/10920      (  0%) [      1] Chunk
  SSM SW freelist DB        :       5424/5592       ( 96%) [      3]
  SSM connection manager    :        816/1320       ( 61%) [      9]
  SSM seg upd info          :          0/2464       (  0%) [      0] Chunk
```

```
Total allocated: 0.246 Mb, 252 Kb, 258296 bytes
```

Related Commands

Command	Description
debug condition xconnect	Displays conditional xconnect debug messages.

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.

show subscriber policy dpm statistics

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

show 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 **show subscriber policy dpm statistics** command displays cumulative information about the event traces that are captured for DPM session contexts. To clear the statistics, use the **clear subscriber policy dpm statistics** command.

Examples

The following is sample output from the **show subscriber policy dpm statistics** command.

```
Router# show subscriber policy dpm statistics

         Message Received     Duplicate    Ignored      Total
    Discover Notification  :        284          0        291
       Offer Notification  :          0          0          2
 Address Assignment Notif  :          2          0          2
   DHCP Classname request  :          0        290        290
      Input Intf Override  :          0         10        293
  Lease Termination Notif  :          0          0          2
  Session Restart Request  :          0          0          0

Response to DHCP request for classname
Average Time : Max Time :
MAC address for Max Time :

Response to DHCP Offer Notification
Average Time : 30ms Max Time : 36ms
MAC address for Max Time : aaaa.2222.cccc

Overall since last clear
Total Discover Init Sessions : 2
Total Restarted Sessions : 0
Average set up time for Discover initiated sessions : 2s26ms
Min set up time among Discover initiated sessions : 2s20ms
Max set up time among Discover initiated sessions : 2s32ms

Current active Sessions
Total Discover Init Sessions : 0
Total Restarted Sessions : 0
Average set up time for Discover initiated sessions :
```

```
Min set up time among Discover initiated sessions: 2s20ms
Max set up time among Discover initiated sessions :
MAC of session with Max DHCP Setup Time : aaaa.2222.cccc

Total number of DPM contexts allocated : 7
Total number of DPM contexts freed : 6
Total number of DPM contexts currently without session : 1

  Elapsed time since counters last cleared : 2h15m20s
```

Table 14 describes some of the fields shown in the sample output, in alphabetical order.

Table 14 show subscriber policy dpm statistics Field Descriptions

Field	Description
Average set up time for Discover initiated sessions	Average amount of time that it took to set up a Discover initiated session, for overall sessions and currently active sessions.
Elapsed time since counters last cleared	Amount of time that has passed since the **clear subscriber policy dpm statistics** command was last used.
MAC of session with Max DHCP Setup Time	MAC address of the session with the longest DHCP setup time.
Max set up time among Discover initiated sessions	Amount of time that it took to set up the Discover initiated session with the longest setup time, for overall sessions and currently active sessions.
Message Received	Total number of messages that were received, by message type, and the number of messages that were duplicated or ignored.
Min set up time among Discover initiated sessions	Amount of time that it took to set up the Discover initiated session with the shortest setup time, for overall sessions and currently active sessions.
Overall since last clear	Cumulative statistics for all of the sessions that occurred since the last time the counters were cleared with the **clear subscriber policy dpm statistics** command.
Total Discover Init Sessions	Total number of Discover initiated sessions, for overall sessions and currently active sessions.
Total Restarted Sessions	Total number of sessions that were restarted, for overall sessions and currently active sessions.

Related Commands

Command	Description
clear subscriber policy dpm statistics	Clears the statistics for DPM session contexts.
show subscriber policy dpm context	Displays event traces for DPM session contexts.
subscriber trace event	Enables event tracing for software modules involved in ISG subscriber sessions.

show subscriber policy peer

To display the details of a subscriber policy peer, use the **show subscriber policy peer** command in user EXEC or privileged EXEC mode.

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

Syntax Description

address	Displays a specific peer, identified by its IP address.
ip-address	The IP address of the peer to be displayed.
handle	Displays a specific peer, identified by its handle.
connection-handle-id	Handle ID for the peer handle.
all	Displays all peers.

Command Modes

User EXEC (>)
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

PUSH mode or PULL mode is established when the peering relationship between the Intelligent Services Gateway (ISG) and Service Control Engine (SCE) devices is initiated. PUSH mode refers to the ISG device pushing out information to the SCE device about a new session. PULL mode refers to the SCE device requesting session identity when it first notices new unidentified traffic.

Only one SCE device in PUSH mode can be integrated with the ISG device. If another SCE device in PUSH mode requests a connection with the ISG device, a disconnect message is sent to the first SCE device that is in PUSH mode.

Examples

The following is sample output from the **show subscriber policy peer** command.

```
Router# show subscriber policy peer all

Peer IP: 10.1.1.3
Conn ID: 105
Mode: PULL
State: ACTIVE
Version: 1.0
Conn up time: 00:01:01
Conf keepalive: 0
Negotiated keepalive: 25
Time since last keepalive: 00:00:11
Inform owner on pull: TRUE
Total number of associated sessions: 2
Associated session details:
 1E010101000000A0
 1E010101000000A1
```

Table 15 describes some of the fields shown in the sample output.

Table 15 show subscriber policy peer Field Descriptions

Field	Description
Peer IP	IP address of subscriber policy peer.
Conn ID	Connection identifier.
Mode	Mode of subscriber policy peer: PUSH or PULL.
Conn up time	Connection up time.
Conf keepalive	Configured keepalive value, in seconds.

Related Commands

Command	Description
subscriber-policy	Defines or modifies the forward and filter decisions of the subscriber policy.

show subscriber session

To display information about subscriber sessions on an Intelligent Services Gateway (ISG), use the **show subscriber session** command in privileged EXEC mode.

show subscriber session [**identifier** {**authen-status** {**authenticated** | **unauthenticated**} | **authenticated-domain** *domain-name* | **authenticated-username** *username* | **auto-detect** | **dnis** *dnis-number* | **mac-address** *mac-address* | **media** *type* | **nas-port** *port-identifier* | **protocol** *type* | **source-ip-address** *ip-address subnet-mask* | **timer** *timer-name* | **tunnel-name** *tunnel-name* | **unauthenticated-domain** *domain-name* | **unauthenticated-username** *username* | **vrf** *vrf-name*} | **uid** *session-identifier* | **username** *username*] [**detailed**]

Syntax Description

identifier	(Optional) Displays information about subscriber sessions that match the specified identifier.
authen-status	(Optional) Displays information about sessions with a specified authentication status.
authenticated	(Optional) Displays information for sessions that have been authenticated.
unauthenticated	(Optional) Displays information for sessions that have not been authenticated.
authenticated-domain *domain-name*	(Optional) Displays information for sessions with a specific authenticated domain name.
authenticated-username *username*	(Optional) Displays information for sessions with a specific authenticated username.
auto-detect	(Optional) Displays information for sessions using auto-detect. (Authorization is performed on the basis of circuit-ID or remote-ID.)
dnis *dnis-name*	(Optional) Displays information for sessions with a specific Dialed Number Identification Service (DNIS) number.
mac-address *mac-address*	(Optional) Displays information for sessions with a specific MAC address.
media *type*	(Optional) Displays information for sessions that use a specific type of access media. Valid values for the *type* argument are as follows: • **async**—Async • **atm**—ATM • **ether**—Ethernet • **ip**—IP • **isdn**—ISDN • **mpls**—Multiprotocol Label Switching (MPLS) • **sync**—Serial

nas-port *port-identifier*	(Optional) Displays information for sessions with a specific network access server (NAS) port identifier. Valid values for the *port-identifier* argument can be one or more of the following: • **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*
protocol *type*	(Optional) Displays information for sessions that use a specific type of access protocol. Valid values for the *type* argument are as follows: • **atom**—Any Transport over MPLS (ATOM) Access Protocol • **ip**—IP Access Protocol • **pdsn**—Public Switch Data Network (PDSN) Access Protocol • **ppp**—PPP Access Protocol • **vpdn**—Virtual Private Dialup Network (VPDN) Access Protocol
source-ip-address*ip-address subnet-mask*	(Optional) Displays information for sessions associated with a specified source IP address.
timer *timer-name*	(Optional) Displays information for sessions that use a specified timer.
tunnel-name *tunnel-name*	(Optional) Displays information for sessions associated with a specific VPDN tunnel.
unauthenticated-domain *domain-name*	(Optional) Displays information for sessions with a specific unauthenticated domain name.
unauthenticated-username *username*	(Optional) Displays information for sessions with a specific unauthenticated username.
vrf *vrf-name*	(Optional) Displays information for sessions with a specific virtual routing and forwarding (VRF) identifier.
uid *session-identifier*	(Optional) Displays information for sessions with a specific unique identifier.
username *username*	(Optional) Displays information for sessions associated with a specific username.
detailed	(Optional) Displayed detailed information about sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was modified. Support for this command was implemented on Cisco 7600 series routers.
15.0(1)S	This command replaces the **show sss session** command.

Usage Guidelines

If the **show subscriber session** command is entered without any keywords or arguments, information is displayed for all sessions on the ISG. When an identifier is specified, information is displayed for only those sessions that match the identifier.

Examples

The following is sample output from the **show subscriber session** command:

```
Router# show subscriber session

Current Subscriber Information: Total sessions 1
Uniq ID        Interface  State Service  Identifier    Up-time
6    Traffic-Cl unauthen  Ltm   Internal rouble-pppoe  00:09:04
5    Vi3       authen     Local Term     rouble-pppoe  00:09:04
```

The following is sample output from the **show subscriber session** command with an identifier specified. In this case, information is displayed for the session with the session identifier 3.

```
Router# show subscriber session identifier uid 3

Current Subscriber Information: Total sessions 1
Uniq ID Interface State Service Identifier Up-time
--------------------------------------------------
Unique Session ID: 3
Identifier: 10.0.0.2
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:00:15, Last Changed: 00:00:15

Policy information:
Authentication status: authen
Rules, actions and conditions executed:
subscriber rule-map RULEB
condition always event session-start
1 authorize identifier source-ip-address

Configuration sources associated with this session:
Interface: Ethernet0/0, Active Time = 00:00:15
```

Table 16 describes the significant fields shown in the displays.

Table 16 show subscriber session Field Descriptions

Field	Description
Total sessions	Number of main sessions on the ISG.
Uniq ID	Session identifier.
Interface	For main sessions, the interface is displayed. For traffic flows, the value "Traffic-Cl" is displayed.

Table 16 show subscriber session Field Descriptions

Field	Description
State	Indicates whether the session has been authenticated or is unauthenticated.
Service	May be one of the following values: • Local Term—The session is terminated locally. • Ltm Internal—A flow that was created internally.
Identifier	Username that is used for authorization.
Up-time	Length of time the session has been up.
Unique Session ID	Session identifier.
SIP subscriber access type(s)	Subscriber's access protocol.
Rules, actions and conditions executed	Control policy rules, actions, and control class maps (conditions) that have been executed for the session.
Configuration sources associated with this session	Sources of configuration that have been applied to the session.

Related Commands

Command	Description
show vpdn session	Displays session information about the L2TP and L2F protocols, and PPPoE tunnels in a VPDN.

show subscriber trace history

To display the event traces for Intelligent Services Gateway (ISG) subscriber sessions that are saved in the trace history log, use the **show subscriber trace history** command in user EXEC or privileged EXEC mode.

show subscriber trace history {**all** | **dpm** | **pm**} [**all** | **client-ip-address** *ip-address* | **mac-address** *mac-address* | **reason** *number* | **uid** *session-id*]

Syntax Description

all	Displays trace information for both the DHCP policy module (DPM) and the policy manager (PM).
dpm	Displays trace information for the DPM.
pm	Displays trace information for the PM.
all	(Optional) Displays all trace information. Output is not filtered based on the specific IP address, MAC address, reason, or unique ID.
client-ip-address *ip-address*	(Optional) Displays trace information for sessions that match the specified client IP address.
mac-address *mac-address*	(Optional) Displays trace information for sessions that match the specified client MAC address.
reason *number*	(Optional) Displays trace information for sessions that match the specified logging reason. Range: 1 to 6. • 1—Dangling session cleared. • 2—PM callback to clear. • 3—Discover IDMGR required failure. • 4—Get class IDMGR required failure. • 5—Session termination error. • 6—Restart error.
uid *session-id*	(Optional) Displays trace information for sessions that match the specified unique ID of the subscriber session. Range: 1 to 4294967295.

Command Default

Displays all session traces saved in the respective history log.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

Use the **show subscriber trace history** command, without any optional keywords, to display all session traces that are saved in the respective history log. To display the trace data for specific sessions, use one of the optional keywords for the IP address, MAC address, logging reason, or unique ID (UID). The router filters the output based on the keyword and displays only those traces that match the selected keyword.

Sessions that are marked as interesting, either because of an error or because the session failed, are saved to the trace history buffer if the **subscriber trace history** command is enabled. To clear the trace history logs, use the **clear subscriber trace history** command.

Examples

The following is sample output from the **show subscriber trace history** command with the **client-ip-address** keyword.

```
Router# show subscriber trace history dpm client-ip-address 10.0.0.2

DPM session info: 5CC14D0
MAC: aaaa.2222.cccc  IP: 10.0.0.2
UID: 2  reason: PM callback to clear
=========================

ET  11:46:03.959 PST Mon Aug 30 2010  PM invoke
        rc OK, Session-Start
ET  11:46:03.959 PST Mon Aug 30 2010  dhcp discover
        rc OK,No Sess,sess alloc,sess-start OK
ET  11:46:03.959 PST Mon Aug 30 2010  dhcp discover
        rc OK,proc prev req
ET  11:46:03.959 PST Mon Aug 30 2010  dhcp get class
        rc no c-aware cfg
ET  11:46:03.975 PST Mon Aug 30 2010  PM callback
        Got Keys, rc dhcp wait no cb,upd msi vrf=0,Case: GOT_KEYS
ET  11:46:05.959 PST Mon Aug 30 2010  PM invoke
        rc OK, Session-Update
ET  11:46:05.959 PST Mon Aug 30 2010  dhcp offer
        rc OK w delay,acc.if ret
ET  11:46:05.983 PST Mon Aug 30 2010  PM callback
        Session Update Succes, rc offer cb no-err,notify stdby,Case:               \
UPDATE_SUCCESS
ET  11:46:05.987 PST Mon Aug 30 2010  dhcp discover
        rc OK,proc prev req
ET  11:46:05.991 PST Mon Aug 30 2010  i-if change
        ,MAC ok,ignore: same i/f
ET  11:46:05.995 PST Mon Aug 30 2010  dhcp assign OK
        rc same IP
ET  11:56:52.743 PST Mon Aug 30 2010  PM invoke
        rc OK, Session-Stop
ET  11:56:52.743 PST Mon Aug 30 2010  dhcp lease term
        rsn 4, rc OK
ET  11:56:52.759 PST Mon Aug 30 2010  PM callback
        Terminate, rc end sess,Case: REQ_TERMINATE
```

The following is sample output from the **show subscriber trace history** command with the **reason** keyword.

```
Router# show subscriber trace history dpm reason 2

DPM session info: 5CC14D0
MAC: aaaa.2222.cccc  IP: 10.0.0.2
UID: 2  reason: PM callback to clear
=========================
ET  11:46:03.959 PST Mon Aug 30 2010  PM invoke
        rc OK, Session-Start
ET  11:46:03.959 PST Mon Aug 30 2010  dhcp discover
        rc OK,No Sess,sess alloc,sess-start OK
ET  11:46:03.959 PST Mon Aug 30 2010  dhcp discover
        rc OK,proc prev req
ET  11:46:03.959 PST Mon Aug 30 2010  dhcp get class
        rc no c-aware cfg
ET  11:46:03.975 PST Mon Aug 30 2010  PM callback
        Got Keys, rc dhcp wait no cb,upd msi vrf=0,Case: GOT_KEYS
ET  11:46:05.959 PST Mon Aug 30 2010  PM invoke
        rc OK, Session-Update
ET  11:46:05.959 PST Mon Aug 30 2010  dhcp offer
        rc OK w delay,acc.if ret
ET  11:46:05.983 PST Mon Aug 30 2010  PM callback
        Session Update Succes, rc offer cb no-err,notify stdby,Case:               \
UPDATE_SUCCESS
ET  11:46:05.987 PST Mon Aug 30 2010  dhcp discover
        rc OK,proc prev req
ET  11:46:05.991 PST Mon Aug 30 2010  i-if change
        ,MAC ok,ignore: same i/f
ET  11:46:05.995 PST Mon Aug 30 2010  dhcp assign OK
        rc same IP
ET  11:56:52.743 PST Mon Aug 30 2010  PM invoke
        rc OK, Session-Stop
ET  11:56:52.743 PST Mon Aug 30 2010  dhcp lease term
        rsn 4, rc OK
ET  11:56:52.759 PST Mon Aug 30 2010  PM callback
        Terminate, rc end sess,Case: REQ_TERMINATE
```

The following is sample output from the **show subscriber trace history** command with the **all** keyword. Note that this is the same output that displays if you use the **show subscriber trace history dpm** command, without any of the optional keywords.

```
Router# show subscriber trace history dpm all

DPM session info: 5CC14D0
MAC: aaaa.2222.cccc  IP: 10.0.0.2
UID: 2  reason: PM callback to clear
=========================

ET  11:46:03.959 PST Mon Aug 30 2010  PM invoke
        rc OK, Session-Start
ET  11:46:03.959 PST Mon Aug 30 2010  dhcp discover
        rc OK,No Sess,sess alloc,sess-start OK
ET  11:46:03.959 PST Mon Aug 30 2010  dhcp discover
        rc OK,proc prev req
ET  11:46:03.959 PST Mon Aug 30 2010  dhcp get class
        rc no c-aware cfg
ET  11:46:03.975 PST Mon Aug 30 2010  PM callback
        Got Keys, rc dhcp wait no cb,upd msi vrf=0,Case: GOT_KEYS
ET  11:46:05.959 PST Mon Aug 30 2010  PM invoke
        rc OK, Session-Update
ET  11:46:05.959 PST Mon Aug 30 2010  dhcp offer
        rc OK w delay,acc.if ret
ET  11:46:05.983 PST Mon Aug 30 2010  PM callback
        Session Update Succes, rc offer cb no-err,notify stdby,Case:               \
UPDATE_SUCCESS
ET  11:46:05.987 PST Mon Aug 30 2010  dhcp discover
        rc OK,proc prev req
ET  11:46:05.991 PST Mon Aug 30 2010  i-if change
        ,MAC ok,ignore: same i/f
ET  11:46:05.995 PST Mon Aug 30 2010  dhcp assign OK
        rc same IP
```

```
ET  11:56:52.743 PST Mon Aug 30 2010  PM invoke
        rc OK, Session-Stop
ET  11:56:52.743 PST Mon Aug 30 2010  dhcp lease term
        rsn 4, rc OK
ET  11:56:52.759 PST Mon Aug 30 2010  PM callback
        Terminate, rc end sess,Case: REQ_TERMINATE
DPM session info: 5CC1708
MAC: aaaa.2222.cccc  IP: 0.0.0.0
UID: 3  reason: PM callback to clear
=========================

ET  12:11:04.279 PST Mon Aug 30 2010  dhcp get class
        rc no c-aware cfg
ET  12:12:17.351 PST Mon Aug 30 2010  i-if change
        ,MAC ok,ignore: same i/f
ET  12:12:17.351 PST Mon Aug 30 2010  dhcp discover
        rc OK,proc prev req
ET  12:12:17.351 PST Mon Aug 30 2010  dhcp get class
        rc no c-aware cfg
ET  12:12:20.487 PST Mon Aug 30 2010  i-if change
        ,MAC ok,ignore: same i/f
ET  12:12:20.487 PST Mon Aug 30 2010  dhcp discover
        rc OK,proc prev req
ET  12:12:20.487 PST Mon Aug 30 2010  dhcp get class
        rc no c-aware cfg
ET  12:12:24.503 PST Mon Aug 30 2010  i-if change
        ,MAC ok,ignore: same i/f
ET  12:12:24.503 PST Mon Aug 30 2010  dhcp discover
        rc OK,proc prev req
ET  12:12:24.503 PST Mon Aug 30 2010  dhcp get class
        rc no c-aware cfg
ET  12:13:38.383 PST Mon Aug 30 2010  i-if change
        ,MAC ok,ignore: same i/f
ET  12:13:38.383 PST Mon Aug 30 2010  dhcp discover
        rc OK,proc prev req
ET  12:13:38.383 PST Mon Aug 30 2010  dhcp get class
        rc no c-aware cfg
ET  12:13:41.719 PST Mon Aug 30 2010  i-if change
        ,MAC ok,ignore: same i/f
ET  12:13:41.719 PST Mon Aug 30 2010  dhcp discover
        rc OK,proc prev req
ET  12:13:41.719 PST Mon Aug 30 2010  dhcp get class
        rc no c-aware cfg
ET  12:13:45.727 PST Mon Aug 30 2010  i-if change
        ,MAC ok,ignore: same i/f
ET  12:13:45.727 PST Mon Aug 30 2010  dhcp discover
        rc OK,proc prev req
ET  12:13:45.727 PST Mon Aug 30 2010  dhcp get class
        rc no c-aware cfg
ET  12:13:59.475 PST Mon Aug 30 2010  PM callback
        Terminate, rc end sess,Case: REQ_TERMINATE
DPM session info: 5CC1940
MAC: aaaa.2222.cccc  IP: 0.0.0.0
UID: 4  reason: PM callback to clear
=========================
.
.
.
DPM session info: 5CC1B78
MAC: aaaa.2222.cccc  IP: 0.0.0.0
UID: 5  reason: PM callback to clear
=========================
.
.
.
DPM session info: 5CC1DB0
MAC: aaaa.2222.cccc  IP: 0.0.0.0
UID: 6  reason: PM callback to clear
=========================

.
.
.
PM session info: 5CBCE98
MAC: aaaa.2222.cccc  IP: 0.0.0.0
UID: 3  reason: dangling session cleared
=========================

ET  11:57:31.531 PST Mon Aug 30 2010  init request
        OLDST[0]:initial-req
        NEWST[0]:initial-req
        fxn[0]:sss_policy_invoke_service_sel  FLAGS:0
ET  11:57:31.535 PST Mon Aug 30 2010  got apply config success
        OLDST[8]:wait-for-events
        NEWST[8]:wait-for-events
        fxn[3]:sss_pm_action_sm_req_apply_config_success  FLAGS:2B7

PM session info: 5CBCFB0
MAC: aaaa.2222.cccc  IP: 0.0.0.0
UID: 4  reason: dangling session cleared
=========================

ET  12:14:59.467 PST Mon Aug 30 2010  init request
        OLDST[0]:initial-req
        NEWST[0]:initial-req
        fxn[0]:sss_policy_invoke_service_sel  FLAGS:0
ET  12:14:59.475 PST Mon Aug 30 2010  got apply config success
        OLDST[8]:wait-for-events
        NEWST[8]:wait-for-events
        fxn[3]:sss_pm_action_sm_req_apply_config_success  FLAGS:2B7

PM session info: 5CBD0C8
MAC: aaaa.2222.cccc  IP: 0.0.0.0
UID: 5  reason: dangling session cleared
=========================

ET  12:44:42.127 PST Mon Aug 30 2010  init request
        OLDST[0]:initial-req
        NEWST[0]:initial-req
        fxn[0]:sss_policy_invoke_service_sel  FLAGS:0
ET  12:44:42.135 PST Mon Aug 30 2010  got apply config success
        OLDST[8]:wait-for-events
        NEWST[8]:wait-for-events
        fxn[3]:sss_pm_action_sm_req_apply_config_success  FLAGS:2B7

PM session info: 5CBD1E0
MAC: aaaa.2222.cccc  IP: 0.0.0.0
UID: 6  reason: dangling session cleared
=========================

ET  13:14:24.983 PST Mon Aug 30 2010  init request
        OLDST[0]:initial-req
        NEWST[0]:initial-req
        fxn[0]:sss_policy_invoke_service_sel  FLAGS:0
ET  13:14:24.991 PST Mon Aug 30 2010  got apply config success
        OLDST[8]:wait-for-events
```

```
NEWST[8]:wait-for-events
fxn[3]:sss_pm_action_sm_req_apply_config_success  FLAGS:2B7
```

Table 17 describes some of the significant fields shown in the sample output.

Table 17 show subscriber trace history Field Descriptions

Field	Description
DPM session info	Unique identifier for the DPM context.
PM session info	Unique identifier for the PM context.
MAC	MAC address of the subscriber session.
IP	IP address of the subscriber session.
UID	Unique ID of the subscriber session.
reason	Reason that the event trace was logged to the history buffer.

Related Commands

Command	Description
clear subscriber trace history	Clears the trace history log for ISG subscriber sessions.
show subscriber trace statistics	Displays statistics about the event traces for ISG subscriber sessions that were saved to the history log.
subscriber trace history	Enables saving the event traces for ISG subscriber sessions to a history log.

show subscriber trace statistics

To display statistics about the event traces for Intelligent Services Gateway (ISG) subscriber sessions that were saved to the history log, use the **show subscriber trace statistics** command in user EXEC or privileged EXEC mode.

show subscriber trace statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

The **show subscriber trace statistics** command displays cumulative statistics about the event traces that were saved to the history log when the **subscriber trace history** command is enabled. Individual statistics display for each of the modules. To clear the trace history logs, use the **clear subscriber trace history** command.

Examples

The following is sample output from the **show subscriber trace statistics** command, showing information for both the DPM and the PM.

```
Router# show subscriber trace statistics

Event Trace History Statistics: DPM
Logging enabled
All time max records: 5
Max records: 5
Current records: 5
Current log size: 200
Proposed log size 200
Oldest, newest index: 0 : 4

Event Trace History Statistics: Policy Manager
Logging enabled
All time max records: 4
Max records: 4
Current records: 4
Current log size: 64
Proposed log size 64
Oldest, newest index: 0 : 3
```

Table 18 describes some of the fields shown in the sample output, in the order in which they display.

Table 18 show subscriber trace statistics Field Descriptions

Field	Description
Logging enabled/disabled	Displays whether history logging is enabled with the **subscriber trace history** command.
All time max records	Maximum number of trace records that were ever saved in this history log.
Max records	Number of trace records that were saved in this history log before it was last cleared.
Current records	Number of trace records that are currently saved in this history log.
Current log size	Number of trace records that can be saved in this history log.
Proposed log size	Number of records that can be saved to the history log as defined by the **subscriber trace history** command. This value becomes the current log size when the log is cleared with the **clear subscriber trace history** command.
Oldest, newest index	Oldest and newest indexes of the array that is used to store the records saved to the history log.

Related Commands

Command	Description
clear subscriber trace history	Clears the trace history log for ISG subscriber sessions.
show subscriber trace history	Displays the event traces for ISG subscriber sessions that are saved in the trace history log.
subscriber trace event	Enables event tracing for software components involved in ISG subscriber sessions.
subscriber trace history	Enables saving the event traces for ISG subscriber sessions to a history log.

source

To specify the interface for which the main IP address will be mapped by the Intelligent Services Gateway (ISG) to the destination IP addresses in subscriber traffic, use the **source** command in IP portbundle configuration mode. To remove this specification, use the **no** form of this command.

source *interface-type interface-number*

no source *interface-type interface-number*

Syntax Description

interface-type interface-number	Interface whose main IP address is used as the ISG source IP address.

Command Default

An interface is not specified.

Command Modes

IP portbundle configuration

Command History

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

Usage Guidelines

The ISG Port-Bundle Host Key feature enables an ISG to map the destination IP addresses in subscriber traffic to the IP address of a specified ISG interface.

All ISG source IP addresses specified with the **source** command must be routable in the management network in which the portal resides.

If the interface for the source IP address is deleted, the port-map translations will not work correctly.

Because a subscriber can have several simultaneous TCP sessions when accessing a web page, ISG assigns a bundle of ports to each subscriber. Because the number of available port bundles is limited, you can assign multiple ISG source IP addresses (one for each group of port bundles). By default, each group has 4032 bundles, and each bundle has 16 ports. To modify the number of bundles per group and the number of ports per bundle, use the **length** command.

Examples

In the following example, the ISG will map the destination IP addresses in subscriber traffic to the main IP address of Ethernet interface 0/0/0:

```
ip portbundle
 source ethernet 0/0/0
```

Related Commands

Command	Description
ip portbundle (service)	Enables the ISG Port-Bundle Host Key feature for a service.
length	Specifies the ISG port-bundle length.

Command	Description
show ip portbundle ip	Displays information about a particular ISG port bundle.
show ip portbundle status	Displays information about ISG port-bundle groups.

subscriber accounting ssg

To display the subscriber inbound and outbound data in accounting records in Service Selection Gateway (SSG) format, use the **subscriber accounting ssg** command in global configuration mode. To disable the SSG accounting format, use the **no** form of this command.

subscriber accounting ssg

no subscriber accounting ssg

Syntax Description

This command has no arguments or keywords.

Command Default

SSG accounting format is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)S1	This command was introduced.

Usage Guidelines

The **subscriber accounting ssg** command allows Intelligent Services Gateway (ISG) to use the same format as SSG for the subscriber inbound and outbound byte counts in the ssg-control-info accounting attribute. By default, ISG reverses the inbound and outbound values in the ssg-control-info attribute. This command makes ISG compatible with SSG accounting.

Examples

The following example shows how to enable ISG to use the SSG accounting format:

```
subscriber accounting ssg
```

Related Commands

Command	Description
aaa accounting	Enables TACACS+ or RADIUS user accounting.
accounting aaa list	Enables ISG accounting and specifies an authentication, authorization, and accounting (AAA) method list to which accounting updates are forwarded.

subscriber feature prepaid

To create or modify a configuration of Intelligent Services Gateway (ISG) prepaid billing parameters that can be referenced from a service policy map or service profile, use the **subscriber feature prepaid** command in global configuration mode. To delete the configuration, use the **no** form of this command.

subscriber feature prepaid {*name-of-configuration* | **default**}

no subscriber feature prepaid {*name-of-configuration* | **default**}

Syntax Description

name-of-configuration	Name of the configuration.
default	Specifies the default configuration.

Defaults

The default configuration is used.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **subscriber feature prepaid** command to create or modify a prepaid billing parameter configuration.

ISG prepaid billing is enabled in a service policy map on the router by entering the **prepaid config** command, or in a service profile on the AAA server by using the prepaid vendor-specific attribute (VSA). The **prepaid config** command and prepaid VSA reference a configuration that contains specific prepaid billing parameters.

A default prepaid configuration exists with the following parameters:

```
subscriber feature prepaid default
 threshold time 0 seconds
 threshold volume 0 bytes
 method-list authorization default
 method-list accounting default
 password cisco
```

The default configuration will not show up in the output of the **show running-config** command unless you change any one of the parameters.

You can also use the **subscriber feature prepaid** command to create a named prepaid configuration. Named prepaid configurations are inherited from the default configuration, so if you create a named prepaid configuration and want only one parameter to be different from the default configuration, you have to configure only that parameter.

Examples

The following example shows prepaid billing enabled in a service called “mp3”. The prepaid billing parameters in the configuration “conf-prepaid” will be used for “mp3” prepaid sessions.

```
policy-map type service mp3
 class type traffic CLASS-ACL-101
  authentication method-list cp-mlist
  accounting method-list cp-mlist
  prepaid config conf-prepaid

subscriber feature prepaid conf-prepaid
 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 trace event

To enable event tracing for software modules that are involved in Intelligent Services Gateway (ISG) subscriber sessions, use the **subscriber trace event** command in global configuration mode. To disable event tracing, use the **no** form of this command.

subscriber trace event {**dpm** | **pm**} [**retain**]

no subscriber trace event {**dpm** | **pm**} [**retain**]

Syntax Description

dpm	Enables event tracing for the DHCP policy module (DPM).
pm	Enables event tracing for the policy manager (PM) module.
retain	(Optional) Saves event traces for existing subscriber sessions until the DPM context is destroyed.

Command Default

Event tracing is enabled for the DPM and PM. Retain functionality is disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **subscriber trace event** command enables event traces to be collected for existing subscriber sessions. It allows you to capture the trace of an event immediately as it occurs, before the session ends and the data is lost. Cisco Technical Assistance Center (TAC) personnel may request this event trace information when resolving issues with ISG subscriber sessions.

Sessions that are marked as interesting, because the session became stuck in a state, entered an error state, or failed due to an error, can be saved to a trace history buffer if the **subscriber trace history** command is enabled.

The system deletes (prunes) the event traces for sessions that are not considered interesting. Traces for existing sessions are maintained until the session is removed or pruned.

Event traces are retained until the corresponding IP session reaches the up state. If the **retain** keyword is configured, the trace data is retained until the DPM context is destroyed.

There is a limit of 20 event traces for each DPM session and eight for each PM session.

Examples

The following example shows how to enable event tracing for the DPM component:

```
Router(config)# subscriber trace event dpm retain
```

Related Commands

Command	Description
show subscriber policy dpm context	Displays event traces for DPM session contexts.
show subscriber trace history	Displays the event traces for ISG subscriber sessions that are saved in the history log.
subscriber trace history	Enables the event traces for ISG subscriber sessions to be saved to a history log.

subscriber trace history

To enable saving event traces for Intelligent Services Gateway (ISG) subscriber sessions to a history log, use the **subscriber trace history** command in global configuration mode. To disable saving the event trace history, use the **no** form of this command.

subscriber trace history {**dpm** | **pm**} [**size** *max-records*]

no subscriber trace history {**dpm** | **pm**} [**size** *max-records*]

Syntax Description

dpm	Saves DHCP policy module (DPM) event traces to the history log.
pm	Saves policy manager (PM) event traces to the history log.
size *max-records*	(Optional) Maximum number of subscriber session traces that can be stored in the history log buffer. Range: 10 to 1000. Default: 100.

Command Default

DPM and PM history logs are disabled; maximum size of history log buffers is 100 sessions.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **subscriber trace history** command allows event traces to be saved to a history log and optionally modifies the size of the history log buffer. Sessions that are marked as interesting, because the session became stuck in a state, entered an error state, or failed due to an error, are saved to the trace history log. Event tracing must be enabled for the module using the **subscriber trace event** command.

Each software module has its own history log buffer. When the history log buffer reaches its configured capacity, the oldest event trace is written over by the newest event trace until you increase the size of the history log with this command or you clear the history log using the **clear subscriber trace history** command.

Modifying the size of the buffer with this command does not change the number of sessions that are currently saved to the history buffer. The **no subscriber trace history** command prevents any new sessions from being saved to the history log; it does not clear the current history log.

Examples

The following example shows how to set the DPM history log size to 200 sessions.

```
Router(config)# subscriber trace history dpm size 200
```

Related Commands

Command	Description
clear subscriber trace history	Clears the trace history log for ISG subscriber sessions.
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.

test sgi xml

To feed a file into the Service Gateway Interface (SGI) process for testing of SGI XML files when an external client is not available, use the **test sgi xml** command in privileged EXEC configuration mode.

test sgi xml *filename*

Syntax Description

filename	Name of the file being used to test SGI.

Command Default

A file is not submitted for testing.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

This command is used to verify the format of an SGI XML request. The XML file must be copied onto the router before it can be used by the **test sgi xml** command.

The external client is currently under development. In the absence of an external client, the test command can be used to verify the XML for specific SGI operations.

Examples

The following example shows the file ‘test.xml’ run by the **test sgi xml** command:

```
Router# test sgi xml disk0:test.xml
```

Related Commands

Command	Description
debug sgi	Enables debugging on SGI.
sgi beep listener	Enables SGI.
show sgi	Displays information about current SGI sessions or statistics.

threshold (ISG)

To configure the threshold at which the Intelligent Services Gateway (ISG) will send a reauthorization request to the prepaid billing server, use the **threshold** command in ISG prepaid configuration mode. To reset the threshold to the default value, use the **no** form of this command.

threshold {**time** *number-of-seconds* | **volume** *number-of-bytes*}

no threshold {**time** *number-of-seconds* | **volume** *number-of-bytes*}

Syntax Description

time	Specifies the threshold for time-based prepaid sessions.
number-of-seconds	When a quota, in seconds, has been depleted to this number, ISG will send a reauthorization request. Default = 0.
volume	Specifies the threshold for volume-based prepaid sessions.
number-of-bytes	When a quota, in bytes, has been depleted to this number, ISG will send a reauthorization request. Default = 0.

Command Default

ISG sends reauthorization requests when the subscriber runs out of quota, which is equivalent to a prepaid threshold of 0 seconds or 0 bytes.

Command Modes

ISG prepaid configuration

Command History

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

Usage Guidelines

By default, an ISG sends reauthorization requests to the billing server when a subscriber has run out of quota. ISG prepaid thresholds allows an ISG to send reauthorization requests before subscribers completely run out of quota. When a prepaid threshold is configured, the ISG sends a reauthorization request to the billing server when the amount of quota remaining is equal to the value of the threshold.

Examples

The following example shows an ISG prepaid feature configuration in which the threshold for time-based sessions is 20 seconds and the threshold for volume-based sessions is 0 bytes. When a time-based prepaid session has 20 seconds of quota remaining, the ISG will send a reauthorization request to the prepaid billing server. For volume-based prepaid sessions, the ISG will send a reauthorization request when the entire quota has been used up.

```
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.

timeout absolute (ISG)

To specify the maximum Intelligent Services Gateway (ISG) subscriber session lifetime, use the **timeout absolute** command in service policy map class configuration mode. To remove this specification, use the **no** form of this command.

timeout absolute *duration-in-seconds*

no timeout absolute *duration-in-seconds*

Syntax Description

duration-in-seconds	Maximum subscriber session lifetime, in seconds. Range is from 30 to 4294967.

Command Default

There is no maximum subscriber session lifetime.

Command Modes

Service policy map class configuration

Command History

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

Usage Guidelines

The **timeout absolute** command controls how long an ISG subscriber session can be connected before it is terminated.

Examples

The following example sets the subscriber session limit to 300 seconds:

```
class-map type traffic match-any traffic-class
 match access-group input 101
 match access-group output 102
policy-map type service video-service
 class type traffic traffic-class
  police input 20000 30000 60000
  police output 21000 31500 63000
  timeout absolute 300
 class type traffic default
 drop
```

Related Commands

Command	Description
timeout idle	Specifies how long an ISG subscriber session can be idle before it is terminated.

timeout idle

To specify how long an Intelligent Services Gateway (ISG) subscriber session can be idle before it is terminated, use the **timeout idle** command in service policy map class configuration mode. To return to the default value, use the **no** form of this command.

timeout idle *duration-in-seconds*

no timeout idle

Syntax Description

duration-in-seconds	Number of seconds a subscriber session can be idle before it is terminated. The range is *n* to 4294967 seconds. The minimum value is platform and release-specific. For more information, use the question mark (**?**) online help function.

Command Default

Idle timeout is disabled.

Command Modes

Service policy map class configuration (config-service-policymap)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was modified. The minimum value of the *duration-in-seconds* argument was changed from 1 to a platform-specific number.

Usage Guidelines

The **timeout idle** command controls how long a connection can be idle before it is terminated. If this command is not configured, the connection is not terminated regardless of how long it is idle.

Examples

The following example limits idle connection time in a service policy map to 30 seconds:

```
class-map type traffic match-any traffic-class
 match access-group input 101
 match access-group output 102
policy-map type service video-service
 class type traffic traffic-class
  police input 20000 30000 60000
  police output 21000 31500 63000
  timeout idle 30
 class type traffic default
 drop
```

Related Commands

Command	Description
timeout absolute	Specifies the maximum ISG subscriber session lifetime.

timer (ISG RADIUS proxy)

To configure the maximum amount of time that Intelligent Services Gateway (ISG) waits for an event before terminating a session, use the **timer** command in RADIUS proxy server configuration mode or RADIUS proxy client configuration mode. To disable the timer, use the **no** form of this command.

timer {**ip-address** | **reconnect** | **request**} *seconds*

no timer {**ip-address** | **reconnect** | **request**}

Syntax Description

ip-address	Timer for an IP address to be assigned to the session.
reconnect	Timer for reconnect.
request	Timer for receiving an Access-Request from a client device.
seconds	Number of seconds ISG waits for the specified event before terminating the session. Range is from 0 to 43200.

Command Default

The default is 0 seconds. This indicates that the timer has not started.

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.
15.0(1)S	This command was modified. The **reconnect** keyword was added.

Usage Guidelines

Use the **timer** command to adjust your network to accommodate slow-responding devices.

ISG RADIUS proxy timers can be specified globally for all RADIUS proxy clients or per client. The per-client configuration overrides the global configuration. The timer is set by the RADIUS Proxy in response to termination of a subscriber’s IP session associated with the RADIUS Proxy session. While the timer is running, the RADIUS Proxy session is maintained regardless of whether the subscriber’s IP session (that got created after the timer was started) exists or not. If a subscriber’s IP session does not exist when the timer expires, the RADIUS Proxy session is deleted. The timer is available only for Open-Authenticated RADIUS Proxy sessions.

Examples

In the following example, ISG is configured to wait 20 seconds for an Access-Request packet before terminating a RADIUS proxy session.

```
aaa server radius proxy
 timer request 20
!
```

Related Commands

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

trust

To define a trust state for traffic that is classified through the **class** policy-map configuration command, use the **trust** command in policy-map class configuration mode. To return to the default setting, use the **no** form of this command.

trust [**cos** | **dscp** | **precedence**]

no trust [**cos** | **dscp** | **precedence**]

Syntax Description

cos	(Optional) Classifies an ingress packet by using the packet class of service (CoS) value. For an untagged packet, the port default CoS value is used.
dscp	(Optional) Classifies an ingress packet by using the packet differentiated services code point (DSCP) values (most significant 6 bits of the 8-bit service-type field). For a non-IP packet, the packet CoS value is used if the packet is tagged. If the packet is untagged, the default port CoS value is used to map CoS to DSCP.
precedence	(Optional) Classifies the precedence of the ingress packet.

Command Default

The action is not trusted.

Command Modes

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

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Catalyst 6500 series.
12.2(33)SRA	This command was implemented on the Catalyst 7600 series.

Usage Guidelines

Use this command to distinguish the quality of service (QoS) trust behavior for certain traffic from other traffic. For example, inbound traffic with certain DSCP values can be trusted. You can configure a class map to match and trust the DSCP values in the inbound traffic.

Trust values set with this command supersede trust values set with the **qos trust** interface configuration command.

If you specify the **trust cos** command, QoS uses the received or default port CoS value and the CoS-to-DSCP map to generate a DSCP value for the packet.

If you specify the **trust dscp** command, QoS uses the DSCP value from the ingress packet. For non-IP packets that are tagged, QoS uses the received CoS value; for non-IP packets that are untagged, QoS uses the default port CoS value. In either case, the DSCP value for the packet is derived from the CoS-to-DSCP map.

Examples

The following example shows how to define a port trust state to trust inbound DSCP values for traffic classified with "class1":

```
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# trust dscp
Router(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Router(config-pmap-c)# end
Router#
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Related Commands

Command	Description
class	Specifies the name of the class whose traffic policy you want to create or change.
police	Configures the Traffic Policing feature.
policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and enters policy-map configuration mode.
set	Marks IP traffic by setting a CoS, DSCP, or IP-precedence in the packet.
show policy-map	Displays information about the policy map.