



## M through Z

---

- [match \(radius-filter\), page 5](#)
- [match access-group \(ISG\), page 7](#)
- [match access-list, page 9](#)
- [match authen-status, page 11](#)
- [match authenticated-domain, page 13](#)
- [match authenticated-username, page 15](#)
- [match dnis, page 17](#)
- [match media, page 19](#)
- [match mlp-negotiated, page 21](#)
- [match nas-port, page 23](#)
- [match no-username, page 25](#)
- [match protocol \(ISG\), page 27](#)
- [match service-name, page 29](#)
- [match source-ip-address, page 31](#)
- [match timer, page 33](#)
- [match tunnel-name, page 35](#)
- [match unauthenticated-domain, page 37](#)
- [match unauthenticated-username, page 39](#)
- [match vrf, page 41](#)
- [matchnot \(radius-filter\), page 43](#)
- [message-authenticator ignore, page 45](#)
- [method-list, page 46](#)
- [passthru downstream ipv6, page 48](#)
- [password \(ISG\), page 50](#)

- [police \(ISG\), page 51](#)
- [policy-map, page 53](#)
- [policy-map type control, page 60](#)
- [policy-map type service, page 62](#)
- [policy-name, page 64](#)
- [policy-peer, page 65](#)
- [port, page 67](#)
- [prepaid config, page 68](#)
- [proxy \(ISG RADIUS proxy\), page 70](#)
- [radius filter, page 72](#)
- [radius-server attribute 31, page 74](#)
- [radius-server attribute nas-port-id include, page 77](#)
- [re-authenticate do-not-apply, page 79](#)
- [redirect log translations, page 81](#)
- [redirect server-group, page 83](#)
- [redirect session-limit, page 85](#)
- [redirect to \(ISG\), page 87](#)
- [server ip, page 90](#)
- [server-key, page 92](#)
- [service \(ISG\), page 94](#)
- [service deny \(ISG\), page 96](#)
- [service local \(ISG\), page 97](#)
- [service relay \(ISG\), page 99](#)
- [service vpdn group \(ISG\), page 100](#)
- [service-monitor, page 101](#)
- [service-policy, page 102](#)
- [service-policy type control, page 112](#)
- [service-policy type service, page 114](#)
- [session-identifier \(ISG\), page 116](#)
- [set-timer, page 118](#)
- [sgi beep listener, page 120](#)
- [sg-service-group, page 122](#)
- [sg-service-type, page 124](#)

- [sg-service-type external policy, page 126](#)
- [show class-map type control, page 128](#)
- [show class-map type traffic, page 130](#)
- [show database data, page 131](#)
- [show dnwld\\_mgr, page 133](#)
- [show idmgr, page 135](#)
- [show interface monitor, page 139](#)
- [show ip portbundle ip, page 142](#)
- [show ip portbundle status, page 144](#)
- [show ip subscriber, page 146](#)
- [show ipv6 nd ra session, page 150](#)
- [show platform isg session, page 151](#)
- [show platform isg session-count, page 154](#)
- [show policy-map type control, page 156](#)
- [show policy-map type service, page 157](#)
- [show processes cpu monitor, page 159](#)
- [show pxf cpu iedge, page 161](#)
- [show pxf cpu isg, page 162](#)
- [show radius-proxy client, page 163](#)
- [show radius-proxy session, page 165](#)
- [show redirect group, page 167](#)
- [show redirect translations, page 169](#)
- [show sgi, page 172](#)
- [show ssm , page 173](#)
- [show subscriber default-session, page 178](#)
- [show subscriber policy dpm statistics, page 179](#)
- [show subscriber policy peer, page 182](#)
- [show subscriber service, page 184](#)
- [show subscriber session, page 187](#)
- [show subscriber statistics, page 199](#)
- [show subscriber trace statistics, page 205](#)
- [show subscriber trace history, page 207](#)
- [show subscriber trace statistics, page 213](#)

- [show tech-support subscriber](#), page 215
- [source](#), page 221
- [subscriber accounting accuracy](#), page 223
- [subscriber accounting ssg](#), page 224
- [subscriber feature prepaid](#), page 225
- [subscriber policy recording](#), page 227
- [subscriber redundancy](#), page 228
- [subscriber trace event](#), page 231
- [subscriber trace history](#), page 233
- [test sgi xml](#), page 235
- [threshold \(ISG\)](#), page 236
- [timeout absolute \(ISG\)](#), page 238
- [timeout idle](#), page 240
- [timer \(ISG RADIUS proxy\)](#), page 243
- [trust](#), page 245

## match (radius-filter)

To configure a condition to check for filter match criteria, use the **match** command in RADIUS filter configuration mode. To remove filter match criteria, use the **no** form of this command.

**match** {**attribute** *att-type-number*| **vendor-type** *ven-type-number* [**attribute** *att-type-number*]}

**no match** {**attribute** *att-type-number*| **vendor-type** *ven-type-number* [**attribute** *att-type-number*]}

### Syntax Description

<b>attribute</b>	Specifies the attribute that should be included in the filter.
<i>att-type-number</i>	Attribute type number. The range is from 1 to 256.
<b>vendor-type</b>	Specifies the vendor type that should be included in the filter.
<i>ven-type-number</i>	Vendor type number. The range is from 1 to 256.

### Command Default

Filter match criteria are not configured.

### Command Modes

RADIUS filter configuration (config-radius-filter)

### Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

### Usage Guidelines

Use the **match** command to check for the attribute to be present in the packet. The **vendor-type** and *ven-type-number* keyword-argument pair specifies the attributes associated with a specific vendor. If no attribute is specified, the condition matches the filter for any attribute of the specific vendor:

### Examples

The following example shows how to enter the RADIUS filter configuration mode and configure a match attribute and a vendor type.

```
Device(config)# radius filter match-all filter1
Device (config-radius-filter) match vendor-type 15 attribute 45
```

**Related Commands**

Command	Description
<b>matchnot (radius-filter)</b>	Configures a filter criterion for an unsuccessful match.
<b>radius filter</b>	Configures RADIUS packet filters.

## 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 the ACL from a class map, use the **no** form of this command.

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

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

### Syntax Description

<b>input</b>	Specifies match criteria for input traffic.
<b>output</b>	Specifies match criteria for output traffic.
<i>access-list-number</i>	A numbered ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class. Range is 1 to 2799.
<b>name</b> <i>access-list-name</i>	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.

The ACL must be defined using the **ip access-list** command.

After 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 shows a class map named “acl144” that is configured to use ACL 144 as the input match criterion for this class:

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

### Related Commands

Command	Description
<b>class-map type traffic</b>	Creates or modifies a traffic class map, which is used for matching packets to a specified ISG traffic class.
<b>class type traffic</b>	Associates a traffic class map with a service policy map.
<b>ip access-list</b>	Defines an IP access list or object group access control list (OGACL).



# 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

<i>access-list-number</i>	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
<b>ip portbundle (service)</b>	Enables the ISG Port-Bundle Host Key feature for a service.

Command	Description
<b>show ip portbundle ip</b>	Displays information about a particular ISG port bundle.
<b>show ip portbundle status</b>	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

<b>authenticated</b>	Subscriber has been authenticated.
<b>unauthenticated</b>	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
<b>class-map type control</b>	Creates an ISG control class map.
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	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

<i>domain-name</i>	Domain name.
<b>regexp</b> <i>regular-expression</i>	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
<b>class-map type control</b>	Creates an ISG control class map.
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	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

<i>username</i>	Username
<b>regexp</b> <i>regular-expression</i>	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
<b>class-map type control</b>	Creates an ISG control class map.
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	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

<i>dnis</i>	DNIS number.
<b>regexp</b> <i>regular-expression</i>	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
<b>class-map type control</b>	Creates an ISG control class map.
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	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

<b>async</b>	Asynchronous media.
<b>atm</b>	ATM.
<b>ether</b>	Ethernet.
<b>ip</b>	IP.
<b>isdn</b>	ISDN.
<b>mpls</b>	Multiprotocol Label Switching (MPLS).
<b>serial</b>	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
<b>class-map type control</b>	Creates an ISG control class map.
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	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

<b>no</b>	The subscriber's session was not multilink PPP negotiated.
<b>yes</b>	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
<b>class-map type control</b>	Creates an ISG control class map.
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	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

<b>adapter</b> <i>adapter-number</i>	Interface adapter number.
<b>channel</b> <i>channel-number</i>	Interface channel number.
<b>circuit-id</b> <i>name</i>	Circuit ID
<b>ipaddr</b> <i>ip-address</i>	IP address.
<b>port</b> <i>port-number</i>	Port number.
<b>remote-id</b> <i>name</i>	Remote ID.
<b>shelf</b> <i>shelf-number</i>	Interface shelf number.
<b>slot</b> <i>slot-number</i>	Slot number.
<b>sub-interface</b> <i>sub-interface-number</i>	Subinterface number.
<b>type</b> <i>interface-type</i>	Interface type.
<b>vci</b> <i>vci-number</i>	Virtual channel identifier.
<b>vlan</b> <i>vlan-id</i>	VLAN ID.
<b>vpi</b> <i>vpi-number</i>	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
<b>class-map type control</b>	Creates an ISG control class map.
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	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

<b>no</b>	The subscriber's username is available.
<b>yes</b>	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
<b>class-map type control</b>	Creates an ISG control class map.
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	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

<b>atom</b>	Any Transport over MPLS (AToM).
<b>ip</b>	IP.
<b>pdsn</b>	Packet Data Serving Node (PDSN).
<b>ppp</b>	Point-to-Point Protocol (PPP).
<b>vpdn</b>	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 VPN tunnel:

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

## Related Commands

Command	Description
<b>class-map type control</b>	Creates an ISG control class map.
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	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

<i>service-name</i>	Service name.
<b>regexp</b> <i>regular-expression</i>	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
<b>class-map type control</b>	Creates an ISG control class map.
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	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

<i>ip-address</i>	IP address.
<i>subnet-mask</i>	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
<b>class-map type control</b>	Creates an ISG control class map.
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	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

<i>timer-name</i>	Name of the policy timer.
<b>regexp</b> <i>regular-expression</i>	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
<b>class-map type control</b>	Creates an ISG control class map.
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	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

<i>tunnel-name</i>	VPDN tunnel name.
<b>regexp</b> <i>regular-expression</i>	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
```

 match tunnel-name

```
1 authorize identifier tunnel-name
!
```

**Related Commands**

Command	Description
<b>class-map type control</b>	Creates an ISG control class map.
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	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

<i>domain-name</i>	Domain name.
<b>regexp</b> <i>regular-expression</i>	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
<b>class-map type control</b>	Creates an ISG control class map.
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	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

<i>username</i>	Username.
<b>regexp</b> <i>regular-expression</i>	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
<b>class-map type control</b>	Creates an ISG control class map.
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	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

<i>vrf-name</i>	Name of the VRF.
<b>regexp</b> <i>regular-expression</i>	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
<b>class-map type control</b>	Creates an ISG control class map.
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.

## matchnot (radius-filter)

To configure a condition to check for a filter criteria that do not match, use the **matchnot** command in RADIUS filter configuration mode. To remove a filter match criteria for an unsuccessful match, use the **no** form of this command.

**matchnot** {**attribute** *att-type-number*|**vendor-type** *ven-type-number* [**attribute** *att-type-number*]}

**no matchnot** {**attribute** *att-type-number*|**vendor-type** *ven-type-number* [**attribute** *att-type-number*]}

### Syntax Description

<b>attribute</b>	Specifies the attribute that should be included in the filter.
<i>att-type-number</i>	Attribute type number. The range is from 1 to 256.
<b>vendor-type</b>	Specifies the vendor type that should be included in the filter.
<i>ven-type-number</i>	Vendor type number. The range is from 1 to 256.

### Command Default

Filter criteria for an unsuccessful match is not configured.

### Command Modes

RADIUS filter configuration (config-radius-filter)

### Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

### Usage Guidelines

Use the **matchnot** command to check whether an attribute is absent from the packet. The **vendor-type** and *ven-type-number* keyword/argument pair specifies the attribute that is associated with a specific vendor. If no attribute option is specified, the condition matches the filter for any attribute of the specific vendor.

### Examples

The following example shows how to enter the RADIUS filter configuration mode and configure a match attribute and a vendor type.

```
Device(config)# radius filter match-all filter1
Device(config-radius-filter)# matchnot vendor-type 15 attribute 45
```

**Related Commands**

Command	Description
<b>match (radius-filter)</b>	Configures a condition to check for a filter match criteria.
<b>radius filter</b>	Configures RADIUS packet filters.

# 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

<b>accounting</b>	Specifies the AAA method list for ISG prepaid accounting.
<b>authorization</b>	Specifies the AAA method list for ISG prepaid authorization.
<i>name-of-method-list</i>	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
<b>aaa accounting</b>	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
<b>prepaid config</b>	Enables prepaid billing for an ISG service and references a configuration of prepaid billing parameters.
<b>subscriber feature prepaid</b>	Creates or modifies a configuration of ISG prepaid billing parameters that can be referenced from a service policy map or service profile

# passthru downstream ipv6

To allow IPv6 downstream traffic from an Intelligent Services Gateway (ISG) interface to pass through to a subscriber without an established subscriber session, use the **passthru downstream ipv6** command in IP subscriber configuration mode. To prevent downstream traffic from passing through without a subscriber session, use the **no** form of this command.

## passthru downstream ipv6

### Syntax Description

This command has no arguments or keywords.

### Command Default

Downstream IPv6 traffic cannot pass through without a subscriber session.

### Command Modes

IP subscriber configuration (config-subscriber)

### Command History

Release	Modification
Cisco IOS XE Release 3.6S	This command was introduced.

### Usage Guidelines

The **passthru downstream ipv6** command enables pass through of IPv6 downstream traffic if an IPv6-specific initiator is configured with the **initiator unclassified ip-address** or **initiator unclassified ip-address ipv6** command.

This command enables subscribers to receive services, such as support and security updates, even if a subscriber session is not present.

If an IPv4-specific initiator is configured on the interface with the **initiator unclassified ip-address ipv4** command, IPv6 downstream traffic is allowed without the pass through feature but IPv4 downstream traffic is blocked.

### Examples

The following example shows that Ethernet interface 0/0 has been configured to allow IPv6 downstream traffic to be forwarded to subscribers even if a subscriber session is not present.

```
interface GigabitEthernet0/0/0
ip address 192.0.2.1 255.255.255.0
ipv6 address 2001:DB8::1/64
ipv6 enable
no cdp enable
service-policy type control my-policy2
ip subscriber routed
  initiator unclassified ip-address
  passthru downstream ipv6
```



**Related Commands**

Command	Description
<b>initiator</b>	Enables ISG to create an IP subscriber session upon receipt of a specified type of packet.

## 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 password** form of this command.

**password** *password*

**no password** *password*

### Syntax Description

<i>password</i>	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
<b>prepaid config</b>	Enables prepaid billing for an ISG service and references a configuration of prepaid billing parameters.
<b>subscriber feature prepaid</b>	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

<b>input</b>	Specifies policing of upstream traffic, which is traffic flowing from the subscriber toward the network.
<b>output</b>	Specifies policing of upstream traffic, which is traffic flowing from the network toward the subscriber.
<i>committed-rate</i>	Amount of bandwidth, in bits per second, to which a subscriber is entitled. Range is from 8000 to 128000000000 (or 128 Gbps).
<i>normal-burst</i>	(Optional) Normal burst size, in bytes. Range is from 1000 to 2000000000 (2 Gb). 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)
<i>excess-burst</i>	(Optional) Excess burst size, in bytes. Range is from 1000 to 2000000000 (2 Gb). 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 (config-service-policymap)

### Command History

Release	Modification
12.2(28)SB	This command was introduced.
15.0(1)SY	This command was modified. The maximum value for the <i>committed-rate</i> , <i>normal-burst</i> and <i>excess-burst</i> arguments was increased.

### 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
<b>class type traffic</b>	Associates a previously configured traffic class to a service policy map.
<b>policy-map type service</b>	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 CMTS and 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

<b>type</b>	(Optional) Specifies the policy-map type.
<b>stack</b>	(Optional) Determines the exact pattern to look for in the protocol stack of interest.
<b>access-control</b>	(Optional) Enables the policy map for the flexible packet matching feature.
<b>port-filter</b>	(Optional) Enables the policy map for the port-filter feature.
<b>queue-threshold</b>	(Optional) Enables the policy map for the queue-threshold feature.
<b>logging</b>	(Optional) Enables the policy map for the control-plane packet logging feature.
<i>log-policy</i>	(Optional) Type of log policy for control-plane logging.
<i>policy-map-name</i>	Name of the policy map.
<b>control</b>	(Optional) Creates a control policy map.

<i>control-name</i>	Name of the control policy map.
<b>service</b>	(Optional) Creates a service policy map.
<i>service-name</i>	Name of the policy-map service.
<b>class-routing</b>	Configures the class-routing policy map.
<b>ipv4</b>	Configures the class-routing IPv4 policy map.
<b>unicast</b>	Configures the class-routing IPv4 unicast policy map.
<i>unicast-name</i>	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	This command was modified. The <b>type</b> and <b>access-control</b> keywords were added to support flexible packet matching. The <b>port-filter</b> and <b>queue-threshold</b> keywords were added to support control-plane protection.
12.4(6)T	This command was modified. The <b>logging</b> keyword was added to support control-plane packet logging.
12.2(31)SB	This command was modified. The <b>control</b> and <b>service</b> keywords were added to support the Cisco 10000 series router.
12.2(18)ZY	This command was modified. <ul style="list-style-type: none"> <li>• The <b>type</b> and <b>access-control</b> 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.</li> <li>• The command was modified to enhance the Network-Based Application Recognition (NBAR) functionality on the Catalyst 6500 series switch that is equipped with the Supervisor 32/PISA engine.</li> </ul>
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.

Release	Modification
12.2(33)SRC	This command was modified. Support for this command was implemented on Cisco 7600 series routers.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 series routers.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.

### Usage Guidelines

Use the **policy-map** command to specify the name of the policy map to be created, added, 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 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 series routers, the limits are 1024 class maps and 256 classes in a policy map.

A policy map containing ATM set cell loss priority (CLP) bit QoS cannot be attached to PPP over X (PPPoX) sessions. The policy map is accepted only if you do not specify the **set atm-clp** command.

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 such cases, if the policy map is already attached to other interfaces, the map is removed from those interfaces.



#### Note

This limitation does not apply on Cisco 7600 series routers that have session initiation protocol (SIP)-400 access-facing line cards.

Whenever you modify a class policy in an attached policy map, class-based weighted fair queuing (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, 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 Performance Routing Engine (PRE)2 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 the 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 are 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.

- 1 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 functions. Traffic policies determine which function is 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. This release and platform has 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 shows how to create a policy map called “policy1” and configure two class policies included in that policy map. The class policy called “class1” specifies a policy for traffic that matches access control list (ACL) 136. The second class is the default class to which packets that do not satisfy the 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 shows how to create a policy map called “policy9” and configure three class policies to belong to that map. Of these classes, two specify the policy for classes with class maps that specify match criteria based on either a numbered ACL or an interface name, and one specifies a policy for the default class called “class-default” to which packets that do not satisfy the 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

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

```

## Examples

The following example shows how to define a policy map for the 802.1p domain:

```
enable
configure terminal
policy-map cos7
  class cos7
    set cos 2
  end
```

The following example shows how to define a policy map for the MPLS domain:

```
enable
configure terminal
policy-map exp7
  class exp7
    set mpls experimental topmost 2
  end
```

## Related Commands

Command	Description
<b>bandwidth (policy-map class)</b>	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
<b>class (policy-map)</b>	Specifies the name of the class whose policy you want to create or change, and its default class before you configure its policy.
<b>class class-default</b>	Specifies the default class whose bandwidth is to be configured or modified.
<b>class-map</b>	Creates a class map to be used for matching packets to a specified class.
<b>fair-queue (class-default)</b>	Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.
<b>match access-group</b>	Configures the match criteria for a class map on the basis of the specified ACL.
<b>queue-limit</b>	Specifies or modifies the maximum number of packets that the queue can hold for a class policy configured in a policy map.
<b>random-detect (interface)</b>	Enables WRED or DWRED.
<b>random-detect exponential-weighting-constant</b>	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
<b>random-detectservice-policy precedence</b>	Configures WRED and DWRED parameters for a particular IP precedence.

Command	Description
<b>service-policy</b>	Attaches a policy map to an input interface or VC or an output interface or VC to be used as the service policy for that interface or VC.
<b>set atm-clp precedence</b>	Sets the ATM CLP bit when a policy map is configured.

# 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 tag** *policy-map-name*

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

## Syntax Description

<b>tag</b>	Network Admission Control (NAC) specific policy type.
<i>policy-map-name</i>	Name of the control policy map.

## Command Default

A control policy map is not created.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE 2.3	This command was integrated into a release earlier than Cisco IOS XE Release 2.3.
15.0(1)M	This command was modified in a release earlier than 15.0(1)M. The <b>tag</b> keyword and <i>policy-map-name</i> argument were added.

## 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 by 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.

- 1 Apply the control policy map to a context by 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 tag rule4
  class type control class3
    authorize nas-port-id
!
service-policy type control rule4
```

### Related Commands

Command	Description
<b>class-map type control</b>	Creates an ISG control class map.
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>service-policy type control</b>	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

<i>policy-map-name</i>	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
<b>class type traffic</b>	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.
<b>policy-map type service</b>	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

<i>policy</i>	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
<b>sg-service-type external-policy</b>	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

<b>address</b>	(Optional) Configures the IP address of the peer that is to be connected.
<i>ip-address</i>	Specifies the IP address of the peer to be connected.
<b>keepalive</b>	Configures the keepalive value to be used to monitor the peering relationship.
<i>seconds</i>	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
<b>aaa server radius policy-device</b>	Enables ISG RADIUS server configuration mode.
<b>show subscriber policy peer</b>	Displays the details of a subscriber policy peer.
<b>subscriber-policy</b>	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

<i>port-number</i>	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
<b>aaa server radius dynamic-author</b>	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

<i>name-of-configuration</i>	A named configuration of prepaid billing parameters.
<b>default</b>	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
<b>subscriber feature prepaid</b>	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

<i>action-number</i>	Number of the action. Actions are executed sequentially within the policy rule.
<b>aaa list</b>	(Optional) Specifies that RADIUS packets will be sent to an authentication, authorization, and accounting (AAA) method list.
<i>list-name</i>	Name of the AAA method list to which RADIUS packets are sent.
<b>default</b>	Specifies that RADIUS packets will be sent to the default RADIUS server.
<b>accounting aaa list</b>	Defines a method list to which accounting is sent.
<i>acc-list-name</i>	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 <b>accounting aaa list</b> 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
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	Creates or modifies a control policy map, which defines an ISG control policy.

# radius filter

To filter RADIUS packets that are received by the Intelligent Services Gateway (ISG), use the **radius filter** command in global configuration mode. To remove the RADIUS packet filter configuration, use the **no** form of this command.

**radius filter** {**match-all**| **match-any**} *name*

**no radius filter** {**match-all**| **match-any**} *name*

## Syntax Description

<b>match-all</b>	Defines the condition to filter RADIUS packets if all attributes match.
<b>match-any</b>	Defines the condition to filter RADIUS packets if at least one attribute matches.
<i>name</i>	Name of the filter. The range is from 1 to 31 characters.

## Command Default

RADIUS packet filters are not configured.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

## Usage Guidelines

Use the **radius filter** command to enable ISG to filter RADIUS packets based on the filter criteria. Use this command along with **match** , **matchnot** , and **filter** commands.

## Examples

The following example shows how to configure a RADIUS packet filter with the **match-all** keyword.

```
Device(config)# radius filter match-all filter1
```

## Related Commands

Command	Description
<b>filter (ISG RADIUS proxy)</b>	Applies ISG RADIUS packet filters to the RADIUS proxy server or client.



Command	Description
<b>match (radius-filter)</b>	Configures a condition to check for a filter match criterion.
<b>matchnot (radius-filter)</b>	Configures a condition to check for a filter criterion that does not match.

## radius-server attribute 31

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

**radius-server attribute 31** {append-circuit-id| mac format {default| ietf| {one-byte| three-byte| two-byte} delimiter {colon| dot| hyphen}| unformatted} [lower-case| upper-case]] remote-id| send nas-port-detail [mac-only]}

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

### Syntax Description

<b>append-circuit-id</b>	Appends the PPP over Ethernet (PPPoE) tag circuit ID and the Network Access Server (NAS) port ID to the Calling-Station-ID (attribute 31).
<b>mac format</b>	Specifies the format used to display the MAC address in the calling station ID.
<b>default</b>	Specifies the MAC address in the default format (0000.4096.3e4a).
<b>ietf</b>	Specifies the MAC address in the IETF format (00-00-40-96-3E-4A).
<b>one-byte</b>	Specifies the MAC address in a one-byte format (00.00.40.96.3e.4a).
<b>three-byte</b>	Specifies the MAC address in a three-byte format (000040.963e4a).
<b>two-byte</b>	Specifies the MAC address in a two-byte format (0000.4096.3e4a).
<b>delimiter</b>	Specifies the delimiter used in the MAC address.
<b>colon</b>	Specifies colon (:) as the delimiter in the MAC address (00:00:40:96:3e:4a).
<b>dot</b>	Specifies dot (.) as the delimiter in the MAC address (00.00.40.96.3e.4a).
<b>hyphen</b>	Specifies hyphen (-) as the delimiter in the MAC address (00-00-40-96-3e-4a).
<b>unformatted</b>	Specifies an unformatted MAC address (000040963e4a).
<b>lower-case</b>	(Optional) Specifies the MAC address in lower case.

<b>upper-case</b>	(Optional) Specifies the MAC address in upper case.
<b>remote-id</b>	Specifies the remote ID as the calling station ID in accounting records and access requests.
<b>send nas-port-detail</b>	Includes all NAS port details in the calling station ID.
<b>mac-only</b>	(Optional) Includes only the MAC address, if available, in the calling station ID.

**Command Default**

The Calling-Station-ID (attribute 31) information is not sent to the authentication, authorization, and accounting (AAA) server.

**Command Modes**

Global configuration (config)

**Command History**

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SB2	This command was modified. The <b>mac format</b> , <b>default</b> , <b>ietf</b> , <b>unformatted</b> , <b>send nas-port-detail</b> , and <b>mac-only</b> keywords 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.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S. The <b>one-byte</b> , <b>three-byte</b> , <b>two-byte</b> , <b>delimiter</b> , <b>colon</b> , <b>dot</b> , <b>hyphen</b> , <b>lower-case</b> , and <b>upper-case</b> keywords were added.

**Usage Guidelines**

- Intelligent Services Gateway (ISG) RADIUS Proxy Sessions

When the DHCP lease query is used, ISG RADIUS proxy receives both the MAC address and the Mobile Station Integrated Services Digital Network Number (MSISDN) as the Calling-Station-ID (attribute 31) option from the downstream device. Therefore, ISG RADIUS proxy must be configured to choose either the MAC address or the MSISDN as the calling station ID and send the ID to ISG accounting records.

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

```
Device(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:

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

The following example shows how to include NAS port details in the Calling-Station-ID:

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

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

```
Device(config)# radius-server attribute 31 send nas-port-detail mac-only
```

- PPP over ATM Sessions

When you use the **send nas-port-detail mac-only** keyword, the calling station ID information is sent through access and accounting requests in the following format:

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

- PPP over Ethernet over ATM (PPPoEoA) Sessions

When you use the **send nas-port-detail mac-only** keyword, the calling station ID information is sent through access and accounting requests in the following format:

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

- PPP over Ethernet over Ethernet (PPPoEoE) Sessions

When you use the **send nas-port-detail mac-only** keyword, the calling station ID information is sent through access and accounting requests in the following format:

```
mac_addr
```

## Related Commands

Command	Description
<b>calling-station-id format</b>	Specifies the format — MAC address or MSISDN — of the Calling-Station-ID (attribute 31).
<b>radius-server attribute nas-port-id include</b>	Uses the DHCP relay agent information (option 60 and option 82) in 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

<i>identifier1,2,3</i>	Identifier for authorization. Valid keywords are: <ul style="list-style-type: none"> <li>• <b>circuit-id</b></li> <li>• <b>remote-id</b></li> <li>• <b>vendor-class-id</b></li> </ul>
<b>plus</b>	(Optional) Separates identifiers if more than one is specified.
<b>separator</b> <i>separator</i>	(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
<b>authorize identifier</b>	Initiates a request for authorization based on a specified identifier in an ISG control policy.

# re-authenticate do-not-apply

To prevent Intelligent Services Gateway (ISG) from applying data from reauthentication profiles to subscriber sessions, use the **re-authenticate do-not-apply** 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.

**re-authenticate do-not-apply**

**no re-authenticate do-not-apply**

**Syntax Description** This command has no arguments or keywords.

**Command Default** ISG applies data from the reauthentication profile to subscriber sessions.

**Command Modes** RADIUS proxy server configuration (config-locsvr-proxy-radius) RADIUS proxy client configuration (config-locsvr-radius-client)

Command History	Release	Modification
	15.0(1)S2	This command was introduced.

**Usage Guidelines** The **re-authenticate do-not-apply** command prevents ISG from updating the subscriber session with data from a reauthentication profile. During the Extensible Authentication Protocol (EAP) authentication process, for example, ISG will not update the subscriber session with the user-name from the reauthentication profile if this command is configured.

This command can be configured globally for all RADIUS proxy clients, or it can be configured for specific clients. The client-specific configuration of this command overrides the global configuration.

**Examples** The following example shows how to prevent ISG from applying reauthentication data to subscriber sessions, for all RADIUS proxy clients:

```
aaa server radius proxy
 re-authenticate do-not-apply
```

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

Command	Description
<b>client (ISG RADIUS proxy)</b>	Enters ISG RADIUS proxy client configuration mode, in which client-specific RADIUS proxy parameters can be specified.



# redirect log translations

To enable the Layer 4 Redirect Logging feature for Intelligent Services Gateway (ISG), use the **redirect log translations** command in global configuration mode. To disable Layer 4 redirect logging, use the **no** form of this command.

**redirect log translations** {**basic**|**extended**} **exporter** *exporter-name*  
**no redirect log translations**

## Syntax Description

<b>basic</b>	Exports Layer 4 redirect translation event information using the basic template format.
<b>extended</b>	Exports Layer 4 translation event information using the extended template format, which includes additional debugging information.
<i>exporter-name</i>	Name of the flow exporter to use for exporting the logging information, as defined by the <b>flow exporter</b> command.

## Command Default

Layer 4 redirect logging is disabled.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

## Usage Guidelines

The **redirect log translations** command allows ISG to export records for Layer 4 redirect translation events to an external collector. These records can be used to identify users with applications that do not react to HTTP redirect.

The name of the flow exporter specified for the *exporter-name* argument must be configured with the **flow exporter** command before using the **redirect log translations** command.

For a description of the fields included in the basic and extended template formats, see the “Configuring Layer 4 Redirect Logging” chapter in the [Intelligent Services Gateway Configuration Guide, Cisco IOS XE Release 3S](#).

## Examples

The following example shows that the flow exporter named L4R-EXPORTER is assigned as the exporter to use for logging redirect translations. There are two types of export templates for Layer 4 redirect logging: IPv4 and IPv6.

```
flow exporter L4R-EXPORTER
 destination 172.16.10.3
 transport udp 90
!
!
redirect log translations basic exporter L4R-EXPORTER
```

## Related Commands

Command	Description
<b>flow exporter</b>	Defines a flow exporter.
<b>show flow exporter statistics</b>	Displays flow exporter statistics.
<b>show flow exporter templates</b>	Displays flow exporter template information.

## 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 redirect server-group** *group-name*

### Syntax Description

<i>group-name</i>	Name of the server group.
-------------------	---------------------------

### Command Default

A redirect server group is not defined.

### Command Modes

Global configuration (config)

### Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 3.5S	This command was modified. Support for IPv6 addresses was added.

### 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, add individual servers to the server group by using the **server ip** command. The server group must contain at least one redirect server before it can be configured under a traffic class service.

The IP addresses of all the servers configured under a redirect group must be either IPv4 or IPv6. A mix of IPv4 and IPv6 redirect server addresses within the same server group is not supported.

### Examples

The following example shows the configuration of a server group named PORTAL that contains two servers, both with an IPv4 address:

```
redirect server-group PORTAL
server ip 10.2.36.253 port 80
server ip 10.76.86.83 port 81
```

The following example shows the configuration of a server group named PORTAL2 that contains two servers, both with an IPv6 address:

```
redirect server-group PORTAL2
server ip 2001:DB8:C003:12::2918 port 8080
server ip 2001:DB8:1:1::26/64 port 8081
```

#### Related Commands

Command	Description
<b>redirect to (ISG)</b>	Redirects ISG Layer 4 traffic to a specified server or server group.
<b>server ip</b>	Adds a server to an ISG Layer 4 redirect server group.
<b>show redirect group</b>	Displays information about ISG Layer 4 redirect server groups.
<b>show redirect translations</b>	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 restore the default value, use the **no** form of this command.

**redirect session-limit** *maximum-number*

**no redirect session-limit**

## Syntax Description

<i>maximum-number</i>	The maximum number of Layer 4 redirects allowed. The range is from 1 to 512.
-----------------------	--

## 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.
Cisco IOS XE Release 3.5S	This command was modified. Support for IPv6 sessions was added.
Cisco IOS XE Release 3.8S	This command was modified. The <i>maximum-number</i> argument was modified to support a maximum of 512 Layer 4 redirects.

## 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.

The maximum number applies to both IPv4 and IPv6 single-stack sessions. For dual-stack sessions, this command limits the total translations per subscriber; IPv4 and IPv6 translations are added together.

## 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
<b>redirect server-group</b>	Defines a group of one or more servers that make up a named ISG Layer 4 redirect server group.
<b>redirect to (ISG)</b>	Redirects ISG Layer 4 traffic to a specified server or server group.
<b>show redirect translations</b>	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** *server-ip-address* [**port** *port-number*]} [**duration** *seconds* [**frequency** *seconds*]]

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

### Syntax Description

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

### Command Default

Subscriber Layer 4 traffic is not redirected.

### Command Modes

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

### 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.
Cisco IOS XE Release 3.5S	This command was modified. The <i>server-ip-address</i> argument accepts IPv6 addresses.

### Usage Guidelines

The **redirect to** command redirects specified Layer 4 subscriber packets to servers that handle the packets in a specified manner.

A redirect server group is defined with the **redirect server-group** command. The server group must contain at least one redirect server, defined with the **server ip** command, before it can be configured under a traffic class service.

The ISG 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.

This command can be configured only once under any traffic class service on the Cisco ASR 1000 Series Router.

### Examples

#### Examples

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

```
policy-map type service L4R-SERVICE
  class type traffic L4R-TC
    redirect to group ADVT-SERVER
```

#### 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 to ip 10.2.36.253
```

The following example configures ISG to redirect all traffic coming from the subscriber interface to 2001:DB8:C003:12::2918 port 80:

```
redirect to ip 2001:DB8:C003:12::2918 port 80
```

#### Examples

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
```

#### Examples

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
<b>redirect server-group</b>	Defines a group of one or more servers that make up a named ISG Layer 4 redirect server group.
<b>server ip</b>	Adds a server to an ISG Layer 4 redirect server group.
<b>show redirect group</b>	Displays information about ISG Layer 4 redirect server groups.
<b>show redirect translations</b>	Displays information about the ISG Layer 4 redirect mappings for subscriber sessions.

## server ip

To add a server to an Intelligent Services Gateway (ISG) Layer 4 redirect server group, use the **server ip** 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

<b>ip</b> <i>ip-address</i>	IP address of the server to be added to the redirect server group.
<b>port</b> <i>port</i>	(Optional) 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.
Cisco IOS XE Release 3.5S	This command was modified. The <i>ip-address</i> argument accepts IPv6 addresses.

### Usage Guidelines

Use the **server ip** 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 ip** 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
<b>redirect server-group</b>	Defines a group of one or more servers that make up a named ISG Layer 4 redirect server group.
<b>redirect to (ISG)</b>	Redirects ISG Layer 4 traffic to a specified server or server group.
<b>show redirect group</b>	Displays information about ISG Layer 4 redirect server groups.
<b>show redirect translations</b>	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

<b>0</b>	(Optional) An unencrypted key will follow.
<b>7</b>	(Optional) A hidden key will follow.
<i>word</i>	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
<b>aaa server radius dynamic-author</b>	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

<i>action-number</i>	Number of the action. Actions are executed sequentially within the policy rule.
<b>disconnect</b>	Disconnect the session.
<b>local</b>	Locally terminate the session.
<b>VPDN</b>	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
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	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
<b>policy-map type service</b>	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
<b>ip vrf forwarding (service policy map)</b>	Associates the service with a VRF.
<b>policy-map type service</b>	Creates or modifies a service policy map, which is used to define an ISG service.
<b>service vpdn group</b>	Provides VPDN service.

Command	Description
<b>vpdn-group</b>	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

<b>pppoe</b>	Provides relay service using PPP over Ethernet (PPPoE) using a virtual private dialup network (VPDN) L2TP tunnel for the relay.
<b>vpdn group</b> <i>vpdn-group-name</i>	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
<b>policy-map type service</b>	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

<i>vpdn-group-name</i>	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
<b>policy-map type service</b>	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

<b>enable</b>	Enables service monitoring.
<b>disable</b>	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
<b>policy-name</b>	Configures a subscriber policy name.
<b>sg-service-type external policy</b>	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

<b>type access-control</b>	(Optional) Determines the exact pattern to look for in the protocol stack of interest.
<b>input</b>	Attaches the specified policy map to the input interface or input VC.
<b>output</b>	Attaches the specified policy map to the output interface or output VC.
<i>policy-map-name</i>	The name of a service policy map (created using the <b>policy-map</b> command) to be attached. The name can be a maximum of 40 alphanumeric characters in length.
<b>history</b>	(Optional) Maintains a history of quality of service (QoS) metrics.
<b>type control</b> <i>control-policy-name</i>	(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 VC bundle configuration (config-atm-bundle)  
 ATM PVP configuration (config-if-atm-l2trans-pvp)  
 ATM VC configuration mode (config-if-atm-vc)  
 Ethernet service configuration (config-if-srv)  
 Global configuration (config)

Interface configuration (config-if)

Static maps class configuration (config-map-class)

ATM PVC-in-range configuration (cfg-if-atm-range-pvc)

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.
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. Support was added for 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. Support was added for subinterface configuration mode and for ATM PVC-in-range configuration mode to extend policy map functionality on an ATM VC to the ATM VC range.
12.4(4)T	The <b>type stack</b> and <b>type control</b> 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 subinterface configuration mode and ATM 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 <b>type stack</b> and <b>type control</b> 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).

Release	Modification
12.2(33)SRC	Support for this command was enhanced on Cisco 7600 series routers.
12.2(33)SB	This command was modified. The command was 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.
12.4(18e)	This command was modified to prevent simultaneous configuration of legacy traffic-shaping and Cisco Modular QoS CLI (MQC) shaping on the same interface.
Cisco IOS XE Release 3.3S	This command was modified to support Ethernet service configuration mode.
Cisco IOS XE Release 3.5S	This command was modified. An error displays if you try to configure the <b>service-policy input</b> or <b>service-policy output</b> command when the <b>ip subscriber interface</b> command is already configured on the interface.
15.2(1)S	This command was modified to allow simultaneous nonqueueing policies to be enabled on subinterfaces.

## Usage Guidelines

The table below shows which configuration mode to choose based on the intended use of the command.

**Table 1: Configuration Modes Based on Command Application**

Application	Mode
Standalone VC	ATM VC submode
ATM VC bundle members	ATM VC Bundle configuration
A range of ATM PVCs	Subinterface configuration
Individual PVC within a PVC range	ATM PVC-in-range configuration
Frame Relay VC	Static maps class configuration
Ethernet services, Ethernet VCs (EVCs)	Ethernet service 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.

Before you can 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.



Before you can 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 Static maps class configuration mode.

To 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 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** Static maps class configuration mode 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 CLI (MQC). However, you cannot configure these features directly on the interface until you remove the policy map from the interface.

**Note**

Beginning in Cisco IOS Release 12.4(18e), you cannot configure the traffic-shape rate and MQC shaping on the same interface at the same time. You must remove the traffic-shape rate configured on the interface before you attach the service policy. For example, if you try to enter the **service-policy {input | output} policy-map-name** command when the **traffic-shape rate** command is already in effect, this message is displayed:

```
Remove traffic-shape rate configured on the interface before attaching the service-policy.
If the MQC shaper is attached first, and you enter the legacy traffic-shape rate command on the same
interface, the command is rejected and an error message is displayed.
```

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 remains active as long as there is a subinterface that is performing 802.1Q 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.
```

**Note**

The **service-policy input** and **service-policy output** commands cannot be configured if the **ip subscriber interface** command is already configured on the interface; these commands are mutually exclusive.

### Simultaneous Nonqueueing QoS Policies

Beginning in Cisco IOS Release 15.2(1)S, you can configure simultaneous nonqueueing QoS policies on an ATM subinterface and ATM PVC, or on a Frame Relay (FR) subinterface and data-link connection identifier (DLCI). However, simultaneous queueing policies are still not allowed, because they create hierarchical queueing framework layer contention. If you try to configure simultaneous queueing policies, the policies are rejected and the router displays an error message.



#### Note

If both the PVC or DLCI and subinterface policies are applied under the same subinterface, the policy under the PVC or DLCI takes precedence and the subinterface policy has no effect.

### Cisco 10000 Series Router Usage Guidelines

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

To attach a policy map 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 1/65,535 (ESR-PRE2) of the interface speed. When you request a value that is not a multiple of 1/255 or 1/65,535, 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 kb/s. 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 kb/s. 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

Activate a control policy map 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.

### Abbreviated Form of the service-policy Command

In Cisco IOS Release 12.2(33)SB and later releases, the router does not accept 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- ?
input Assign policy-map to the input of an interface
output Assign policy-map to the output of an interface
type Configure 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
```

## 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, as shown in the example “how to attach the service policy map named “policy9” to DLCI 100 on output serial interface 1 and enable LLQ for Frame Relay”.

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



#### Note

The **atm pxf queueing** 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 apply the policy map named “policy1” to the virtual template named “virtual-template1” for all inbound traffic. In this example, the virtual template configuration also includes Challenge Handshake Authentication Protocol (CHAP) authentication and PPP authorization and accounting.

```
interface virtual-template1
  ip unnumbered Loopback1
  no peer default ip address
  ppp authentication chap vpn1
  ppp authorization vpn1
  ppp accounting vpn1
  service-policy input policy1
```

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 subinterface 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 ATM 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
```

The following example shows a policy map and interface configuration that supported simultaneous nonqueueing policies:

```
Policy-map p-map
class c-map
set mpls experimental imposition 4

interface ATM1/0/0.1 multipoint
no atm enable-ilmi-trap
xconnect 10.1.1.1 100001 encapsulation mpls
service-policy input p-map
pvc 1/41 l2transport
no epd
!
pvc 1/42 l2transport
no epd
!
pvc 1/43 l2transport
no epd
interface ATM1/0/0.101 multipoint
no atm enable-ilmi-trap
pvc 9/41 l2transport
xconnect 10.1.1.1 1001011 encapsulation mpls
service-policy input p-map
!
pvc 10/41 l2transport
xconnect 10.1.1.1 1001012 encapsulation mpls
!
```

The following example shows how to attach simultaneous nonqueueing QoS policies on an ATM subinterface and ATM PVC:

```
interface atm 1/0/0.101
pvc 9/41
service-policy input p-map
```

## Related Commands

Command	Description
<b>class-map</b>	Accesses QoS class-map configuration mode to configure QoS class maps.
<b>frame-relay ip rtp priority</b>	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,
<b>frame-relay traffic-shaping</b>	Enables both traffic shaping and per-virtual-circuit queueing for all PVCs and SVCs on a Frame Relay interface.
<b>frame-relay voice bandwidth</b>	Specifies the amount of bandwidth to be reserved for voice traffic on a specific DLCI.
<b>ip subscriber interface</b>	Creates an ISG IP interface session.
<b>policy-map</b>	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
<b>priority</b>	Gives priority to a class of traffic belonging to a policy map.

Command	Description
<b>show policy-map</b>	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
<b>show policy-map interface</b>	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.
<b>traffic-shape rate</b>	Enables traffic shaping for outbound traffic on an 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 remove a control policy, use the **no** form of this command.

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

**no service-policy type control** [*policy-map-name*| **default** [*def-policy-map-name*]]

## Syntax Description

<i>policy-map-name</i>	Name of the control policy map.
<b>default</b>	Specifies the default control policy map to be applied.
<i>def-policy-map-name</i>	(Optional) Name of the default policy map.

## Command Default

A control policy is not applied to a context.

## Command Modes

Global configuration (config)  
 Interface configuration (config-if)  
 Subinterface configuration (config-subif)  
 Virtual template configuration (config-if)  
 ATM VC class configuration (config-vc-class)  
 ATM VC configuration (config-if-atm-vc)

## Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S. The <b>default</b> keyword and <i>def-policy-map-name</i> argument were added.

## 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 Virtual circuit (VC) class

6 Permanent virtual circuit (PVC)

In the list above, the context types are numbered in the order of increasing precedence. Control policy maps that are applied to higher priority contexts take precedence over policy maps applied to more general contexts. For example, a control policy map that is applied to a PVC takes precedence over a control policy map that is applied to an interface.

Control policies apply to all sessions hosted in a context.

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

### Examples

The following example applies the control policy map “RULEA” to GigabitEthernet 0/2/0.2001:

```
Device(config)# interface GigabitEthernet0/2/0.2001
Device(config-if)# service-policy type control RULEA
```

### Related Commands

Command	Description
<b>policy-map type control</b>	Creates or modifies a control policy map that 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

<i>action-number</i>	Number of the action. Actions are executed sequentially within the policy rule.
<b>unapply</b>	(Optional) Deactivates the specified service.
<b>aaa</b>	(Optional) Specifies that a AAA method list will be used to activate the service.
<b>list</b> <i>list-name</i>	(Optional) Activates the service using the specified authentication, authorization, and accounting (AAA) method list.
<b>name</b> <i>service-name</i>	Name of the service.
<b>identifier</b>	Activates a service that has the same name as the specified identifier.
<b>authenticated-domain</b>	Authenticated domain name.
<b>authenticated-username</b>	Authenticated username.
<b>dnis</b>	Dialed Number Identification Service number (also referred to as the <i>called-party number</i> ).
<b>nas-port</b>	Network access server (NAS) port identifier.
<b>tunnel-name</b>	VPDN tunnel name.
<b>unauthenticated-domain</b>	Unauthenticated domain name.
<b>unauthenticated-username</b>	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
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	Creates or modifies a control policy map, which defines an ISG control policy.
<b>policy-map type service</b>	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

<b>attribute</b>	Specifies the calling station attribute of the session to be identified.
<i>number</i>	The attribute number. For example, attribute 1 denotes username.
<b>vsa</b>	Specifies the vendor-specific attribute (VSA) of the session to be identified.
<b>vendor</b> <i>id</i>	Specifies the vendor type and ID.
<b>type</b> <i>number</i>	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
<b>aaa server radius proxy</b>	Enables ISG RADIUS proxy configuration mode, in which ISG RADIUS proxy parameters can be configured.
<b>calling-station-id format</b>	Specifies the format if the attribute of the calling station is attribute 31.
<b>client ( ISG RADIUS proxy )</b>	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

<i>action-number</i>	Number of the action. Actions are executed sequentially within the policy rule.
<i>name-of-timer</i>	Name of the policy timer.
<i>minutes</i>	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
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>policy-map type control</b>	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

<i>port</i>	(Optional) TCP port on which to listen. The default is assigned by Internet Assigned Numbers Authority (IANA).
<i>acl</i>	(Optional) Applies an access control list (ACL) to restrict incoming client connections.
<i>access-list</i>	Name of the access list that is to be applied.
<i>sasl</i>	(Optional) Configures a Simple Authentication Security Layer (SASL) profile to use during the session establishment.
<i>sasl-profile</i>	Name of SASL profile being used during session establishment.
<i>encrypt</i>	(Optional) Configures transport layer security (TLS) for SGI.
<i>trustpoint</i>	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
<b>debug sgi</b>	Enables debugging for SGI.
<b>show sgi</b>	Displays information about current SGI sessions or statistics.
<b>test sgi xml</b>	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

<i>service-group-name</i>	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
<b>policy-map type service</b>	Creates or modifies a service policy map, which is used to define an ISG subscriber service.
<b>sg-service-type</b>	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

<b>primary</b>	Identifies the service as a primary service, which is a service that contains a network-forwarding policy.
<b>secondary</b>	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
<b>policy-map type service</b>	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

<i>external-policy</i>	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-policy-map)

### 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-policy-map)# sg-service-type external-policy
```

### Related Commands

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

The table below describes the significant fields shown in the display.

**Table 2: 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
<b>class-map type control</b>	Creates an ISG control class map.
<b>class type control</b>	Specifies a control class for which actions may be configured in an ISG control policy map.
<b>clear class-map type control</b>	Clears the ISG control class map counters.
<b>show policy-map type control</b>	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
<b>show policy-map type traffic</b>	Displays the contents of ISG service policy maps.

## show database data

To display information about an identity manager (IDMGR) database, use the **show database data** command in privileged EXEC mode.

**show database data** *name type*

### Syntax Description

<i>name</i>	Name of the IDMGR database.
<i>type</i>	Client type. Valid values are from 0 to 2.

### Command Modes

Privileged EXEC (#)

### Command History

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

### Usage Guidelines

You can use the **show database names** command to get a list of database names. The **show database data** command displays information about the IDMGR for the specified database name.

### Examples

The following are sample output from the **show database data** command:

```
Router# show database data IDMGR-Session-DB 2
Total records = 1
-----
Record 0 (key 1)
session-handle = 88000002
aaa-unique-id = 0000000C
composite-key = 00174574302F303A313A656E63617020646F74317120313030
authen-status = unauthen
Router# show database data IDMGR-Service-DB 2
Total records = 1
-----
Record 0 (key 5)
session-handle = 2E000004
service-name = PBHK
idmgr-svc-key = 2E00000402000001
authen-status = unauthen
```

The table below describes the significant fields shown in the display.

**Table 3: show database data Field Descriptions**

Field	Description
Total records	Total number of records in the ISG session.

Field	Description
Record	Record number.
session-handle	Layer 2 (L2) session handling details for the ISG session.
service-name	Name of the ISG service.
idmgr-svc-key	IDMGR key used to identify the service.
authen-status	Status of authentication. Valid values are: <ul style="list-style-type: none"> <li>• unauthen-Indicates that the session is not authenticated.</li> <li>• authen-Indicates that the session is authenticated.</li> </ul>

**Related Commands**

Command	Description
<b>debug idmgr</b>	Enables debugging for the IDMGR.

# show dwnld\_mgr

To display information about the download manager, use the **show dwnld\_mgr** command in privileged EXEC mode.

**show dwnld\_mgr** {**AAA Unique ID** {*unique-ID*| **all**}| **profiles** {**all**| **name** *profile-name*}}

## Syntax Description

<b>AAA Unique ID</b>	Specifies the Accounting, Authentication, and Authorization (AAA) unique ID from where the profiles are downloaded.
<i>unique-ID</i>	Unique ID of the AAA server.
<b>all</b>	Specifies all the profiles.
<b>profiles</b>	Specifies the global configuration profile.
<b>name</b> <i>profile-name</i>	Specifies the name of the global configuration profile.

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

You can use the **show dwnld\_mgr** command to view information about the download manager. The download manager is used to download global configuration profiles such as connectivity fault management (CFM) maintenance association (MA) profile for Programmable Ethernet. These profiles contain configuration information that is consumed by the client and then applied at the global level. These profiles are shared, that is, they are applied to multiple sessions. The download manager downloads and adds the shared profiles to the cache.

The download manager serves two primary functions:

- Common interface to AAA to download profiles for any client
- Client-independent database that caches the downloaded profiles

## Examples

The following is sample output from the **show dwnld\_mgr profiles all** command:

```
Router# show dwnld_mgr profiles all
*****
Name: itag:3000
```

```

Reference: 1
Notification Type: DM_NOTIFICATION_PER_REQUEST_NOT_CACHED
Clients Waiting:
F1000003, 0A6AD658, 0000000C
*****

```

The following is sample output from the **show dnwld\_mgr profiles name** command:

```

Router# show dnwld_mgr profiles name itag:300
*****
Name: itag:3000
Reference: 1
Notification Type: DM_NOTIFICATION_PER_REQUEST_NOT_CACHED
Clients Waiting:
F1000003, 0A6AD658, 0000000C
*****

```

The table below describes the significant fields shown in the displays.

**Table 4: show dnwld\_mgr Field Descriptions**

Field	Description
Name	Name of the global configuration profile.
Notification Type	Notification sent from the client to the download manager.
Clients Waiting	IDs of the clients waiting to complete the download.

#### Related Commands

Command	Description
<b>debug idmgr</b>	Enables debugging for the IDMGR.

## 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* **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

<b>memory</b>	Displays memory-usage information related to ID management.
<b>detailed</b>	(Optional) Displays detailed memory-usage information related to ID management.
<b>component</b>	(Optional) Displays information for the specified ID management component.
<i>substring</i>	(Optional) Substring to match the component name.
<b>service key</b>	Displays ID information for a specific service.
<b>session-handle</b> <i>session-handle-string</i>	Displays the unique identifier for a session.
<b>service-key</b> <i>key-value</i>	Displays ID information for a specific service.
<b>session key</b>	Displays ID information for a specific session and its related services.
<b>aaa-unique-id</b> <i>aaa-unique-id-string</i>	Displays the authentication, authorization, and accounting (AAA) unique ID for a specific session.
<b>domainip-vrf ip-address</b> <i>ip-address</i>	Displays the service-facing IP address for a specific session.
<b>vrf-id</b> <i>vrf-id</i>	Displays the VPN routing and forwarding (VRF) ID for the specific session.
<b>nativeip-vrf ip-address</b> <i>ip-address</i>	Displays the subscriber-facing IP address for a specific session.
<b>portbundle ip</b> <i>ip-address</i>	Displays the port bundle IP address for a specific session.
<b>bundle</b> <i>bundle-number</i>	Displays the bundle number for a specific session.

<b>session-guid</b> <i>session-guid</i>	Displays the global unique identifier for a session.
<b>session-handle</b> <i>session-handle-string</i>	Displays the session identifier for a specific session.
<b>session-id</b> <i>session-id-string</i>	Displays the session identifier used to construct the value for RADIUS attribute 44 (Acct-Session-ID).
<b>circuit-id</b> <i>circuit-id</i>	Displays the user session information in the ID Manager (IDMGR) database when you specify the unique circuit ID tag.
<b>pppoe-unique-id</b> <i>pppoe-id</i>	Displays the PPPoE unique key information in the ID Manager (IDMGR) database when you specify the unique PPPoE unique ID tag
<b>statistics</b>	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 <i>circuit-id</i> 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
The table below describes the significant fields shown in the display.
```

**Table 5: 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
<b>subscriber access pppoe unique-key circuit-id</b>	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

<i>interface-type</i>	Type of the interface for which statistics will be displayed.
<i>interface-number</i>	Number of the interface for which statistics will be displayed.
<b>interval</b> <i>seconds</i>	(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:

The table below describes the significant fields shown in the display.

**Table 6: 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 runs, 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.

Field	Description
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.
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
<b>show interfaces</b>	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

<i>port-bundle-ip-address</i>	IP address used to identify the port bundle.
<b>bundle</b> <i>port-bundle-number</i>	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
The table below describes the significant fields shown in the display.
```

**Table 7: 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
<b>ip portbundle (global)</b>	Enters portbundle configuration mode, in which ISG port-bundle host key parameters can be configured.
<b>show ip portbundle status</b>	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

<b>free</b>	(Optional) Lists the port bundles that are available in each bundle group.
<b>inuse</b>	(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
```

The table below describes the significant fields shown in the display.

**Table 8: 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.



Field	Description
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
<b>ip portbundle (global)</b>	Enters portbundle configuration mode, in which ISG port-bundle host key parameters can be configured.
<b>show ip portbundle ip</b>	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** [**interface** *interface-name* [**detail**|**statistics**]] [**ip** *ip-address*|**mac** *mac-address*|**redundancy**|**static list** *list-name*|**statistics**{**arp**|**dangling**}| [**vrf** *vrf-name*] [**dangling** *seconds*] [**detail**]

## Syntax Description

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

**Command Modes**

User EXEC (>)  
Privileged EXEC (#)

**Command History**

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	Support for this command was added on the Cisco 7600 series router.
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 <b>static</b> and <b>list</b> keywords were added.
12.2(33)SRE1	This command was modified. The <b>statistics</b> and <b>arp</b> keywords were added.
Cisco IOS XE Release 3.4S	This command was modified. The output was enhanced to include information about IPv6 sessions.

**Command Modes**

User EXEC (>) Privileged EXEC (#)

**Usage Guidelines**

A session that is not 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 can remain unestablished before it is considered dangling.

**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

```

The table below describes the significant fields shown in the displays, in alphabetical order.

**Table 9: show ip subscriber Field Descriptions**

Field	Description
Dst on ISG	Number of ARP requests that ISG replied to for a destination on ISG.
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.
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.

Field	Description
Session initiator	Type of packet that initiated the subscriber session.

**Related Commands**

Command	Description
<b>clear ip subscriber</b>	Disconnects and removes all or specified ISG IP subscriber sessions.
<b>ip subscriber list</b>	Creates a subscriber list for ISG IP sessions.

# show ipv6 nd ra session

To display information about unicast IPv6 router advertisement (RA) sessions, use the **show ipv6 nd ra session** command in privileged EXEC mode.

**show ipv6 nd ra session** *interface-type interface-num*

## Syntax Description

<i>interface-type</i>	The type of interface.
<i>interface-num</i>	The number of the interface.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

## Usage Guidelines

Use the **show ipv6 nd ra session** command to display information about all unicast IPv6 RA sessions configured on a specific interface.

## Examples

```
Device# show ipv6 nd ra session ethernet 0/0
Interface Ethernet0/0, owner 2A, sessions 4, started 4
* Session 1
  3001::/64, flags C0, valid 1800, preferred 1800
* Session 2
  3001:0:0:1::/64, flags C0, valid 1800, preferred 1800
* Session 3
  3001:0:0:2::/64, flags C0, valid 1800, preferred 1800
* Session 4
  3001:0:0:3::/64, flags C0, valid 1800, preferred 1800
```

# 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 subinterface-number* [**detail**]

## Syntax Description

<i>session-id</i>	Specifies the ID of a particular session.
<i>subinterface-number</i>	Specifies the subinterface number.
<b>detail</b>	(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-brrr1-parent dir Output
np 1 port 0 pm_num 4 lookuptype 1 flowid 256
=====
policymap pmap-brrr1-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-brrr1-parent classid 0 dfs classid 2 level 0
=====
```

## show platform isg session

```

Statistics type      Packet count      Byte count
queue:
    commit           0                0
    excess           0                0
    drop            0                0
    cur depth        0
-----
polycymap 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_cosi 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_cosi 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_cosi 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: 62500000/1559756 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
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:0 Child 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
***
-----
polycymap 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
<b>show platform isg session-count</b>	Displays the number of active ISG subscriber sessions by line card.
<b>show subscriber session</b>	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

<i>all</i>	Displays information for all line cards on the router.
<i>slot</i>	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
```

The table below describes the significant fields shown in the display, in alphabetical order.

**Table 10: 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
<b>show subscriber session</b>	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
<b>clear policy-map type control</b>	Clears ISG control policy map counters.
<b>policy-map type control</b>	Creates or modifies a control policy map, which defines an ISG control policy.
<b>show class-map type control</b>	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.

**Examples**

```
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"
```

**Examples**

```
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"
```

The table below describes the significant fields shown in the display.

**Table 11: 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

<b>interval</b> <i>seconds</i>	(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:
```

The table below describes the significant fields shown in the display.

**Table 12: 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.

Field	Description
five minutes	CPU utilization for the last 5 minutes and the percentage of CPU time spent at the interrupt level.
PID	Process ID.
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
<b>show processes cpu</b>	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

<b>detail</b>	(Optional) Displays detailed information about policies and templates.
<b>policy</b> <i>policy-name</i>	(Optional) Displays summary policy information.
<b>template</b>	(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. The fields shown in the display are self-explanatory.

```
Router# show pxf cpu iedge template
Super ACL name      OrigCRC   Class Count   CalcCRC
lsacl_2             4EA94046   2             00000000
if_info 71BA3F20
```

## Related Commands

Command	Description
<b>show pxf statistics</b>	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

<b>detail</b>	(Optional) Displays detailed information about ISG policies and templates.
<b>policy</b> <i>policy-name</i>	(Optional) Displays summary ISG policy information.
<b>template</b>	(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
1sac1_2             4EA94046   2             00000000
if_info 71BA3F20
```

## Related Commands

Command	Description
<b>show pxf statistics</b>	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

<i>ip-address</i>	IP address of the RADIUS proxy client.
<b>vrf</b> <i>vrf-name</i>	(Optional) Displays information about the RADIUS proxy client associated with the specified virtual routing and forwarding (VRF) instance.  <b>Note</b> The <b>vrf</b> <i>vrf-name</i> keyword-argument pair 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.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S. The output was enhanced to display information about disconnect timers for accounting stop and reauthentication failure.

## Examples

The following is sample output from the **show radius-proxy client** *ip-address* command:

```
Device# show radius-proxy client 192.0.2.1
Configuration details for client 192.0.2.1
Shared secret:  password1      Msg Auth Ignore:  No
Local auth port: 1812          Local acct port: 1813
Acct method list: SVC_ACCT
Session Summary:
    RP ID      IP Address
  1. 3707764753 203.0.113.1
  2. 4110417938 203.0.113.2
```

The table below describes the significant fields shown in the display:

**Table 13: show radius-proxy client ip-address Field Descriptions**

Field	Description
Shared secret	Shared secret between the ISG RADIUS proxy server 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.
Acct method list	Method list to which the ISG RADIUS proxy client forwards accounting packets.
Session Summary	Summary of ISG sessions that are 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
<b>show radius-proxy session</b>	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** {**clid** *calling-line-ID*| **id** *radius-proxy-ID*| **ip** *ip-address* [**vrf** *vrf-name*]}

### Syntax Description

<b>clid</b> <i>calling-line-ID</i>	Displays information about the RADIUS proxy session associated with the specified calling line identifier (CLID).
<b>id</b> <i>radius-proxy-ID</i>	Displays information about a session associated with the specified RADIUS proxy ID.
<b>ip</b> <i>ip-address</i>	Displays information about the RADIUS proxy session associated with the specified IP address.
<b>vrf</b> <i>vrf-name</i>	(Optional) Displays information about the RADIUS proxy session associated with the specified virtual routing and forwarding (VRF) instance.  <b>Note</b> The <b>vrf</b> <i>vrf-name</i> keyword-argument 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.
Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S. The <b>clid</b> keyword was added.
Cisco IOS XE Release 3.7S	This command was modified. The output was enhanced to display information about disconnect timers for accounting stop and reauthentication failure.

### Examples

The following is sample output from the **show radius-proxy session id** *radius-proxy-ID* command. The fields in the output are self-explanatory.

```
Device# show radius-proxy session id 1234567890
```

```
Session Keys:
  Caller ID:      aaaa.bbbb.cccc
```

```

Other Attributes:
  Username:      username1
  User IP:       unassigned
  Called ID:
Client Information:
  NAS IP:        192.0.2.1
  NAS ID:        localhost
State Details:
  State:         authenticated
  Timer:         ip-address (timeout: 240s, remaining: 166s)

```

The following sample output from the **show radius-proxy session ip ip-address** command displays details of the disconnect timer for accounting stop. The fields in the output are self-explanatory:

```
Device# show radius-proxy session ip 203.0.113.1
```

```

Session Keys:
  Calling-Station-Id:aaaa.bbbb.cccc
Other Attributes:
  Caller ID:      aaaa.bbbb.cccc
  Username:       username1
  User IP:        203.0.113.1
  Called ID:
Client Information:
  NAS IP:         192.0.2.1
  NAS ID:         localhost
  AP1 IP:         192.0.2.1
  AP2 IP:         192.0.2.2
  HOTSPOT IP:     192.0.2.1
State Details:
  State:          activated
  Timer:          none
                  disconnect acct-stop (timeout: 150s, remaining: 143s)

```

The following sample output from the **show radius-proxy session ip ip-address** command displays details of the disconnect timer for reauthentication failure. The fields in the output are self-explanatory:

```
Device# show radius-proxy session ip 203.0.113.1
```

```

Session Keys:
  Calling-Station-Id:aaaa.bbbb.cccc
Other Attributes:
  Caller ID:      aaaa.bbbb.cccc
  Username:       username1
  User IP:        203.0.113.1
  Called ID:
Client Information:
  NAS IP:         192.0.2.1
  NAS ID:         localhost
  AP1 IP:         192.0.2.1
  AP2 IP:         192.0.2.2
  HOTSPOT IP:     192.0.2.1
State Details:
  State:          activated
  Timer:          none
                  disconnect reauth-fail (timeout: 150s, remaining: 143s)

```

## Related Commands

Command	Description
<b>show radius-proxy client</b>	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

<i>group-name</i>	(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.
Cisco IOS XE Release 3.5S	This command was modified. The output was enhanced to include information about IPv6 redirect groups and servers.

## 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
<b>redirect server-group</b>	Defines a group of one or more servers that make up a named ISG Layer 4 redirect server group.
<b>redirect to</b> (ISG)	Redirects ISG Layer 4 traffic to a specified server or server group.
<b>server</b> (ISG)	Adds a server to an ISG Layer 4 redirect server group.

Command	Description
<b>show redirect translations</b>	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*] **ipv4** | **ipv6** [**verbose**]

## Syntax Description

<b>ip</b> <i>ip-address</i>	(Optional) Displays all active translations for the specified subscriber source IP address.
<b>ipv4</b>	(Optional) Displays all active IPv4 translations.
<b>ipv6</b>	(Optional) Displays all active IPv6 translations.
<b>verbose</b>	(Optional) Displays detailed information about the translations.

## 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.
Cisco IOS XE Release 3.5S	This command was modified. The <b>ipv4</b> , <b>ipv6</b> , and <b>verbose</b> keywords were added.

## 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

Prot Destination IP/Port          Server IP/Port
TCP  10.0.1.2 23                  10.0.2.2 23
TCP  10.0.1.2 23                  10.0.2.2 23
TCP  10.0.1.2 23                  10.0.2.2 23
Total Number of Translations: 3
```

The following is sample output from the **show redirect translations ipv6** command displaying information about each active IPv6 redirect translation:

```
Router# show redirect translations ipv6

Prot Destination IP/Port          Server IP/Port
TCP  2001:DB8:2222:1044::72 80    2001:DB8:C003:12::2918 8080
TCP  2001:DB8:2222:1044::73 80    2001:DB8:C003:12::2918 8080
Total Number of Translations: 5
```

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

```
Router# show redirect translations verbose

Prot Destination IP/Port          Server IP/Port
      Source IP/Port              InFlags OutFlags Timestamp
TCP  10.1.0.1 80                  10.10.0.1 8080
      10.0.0.1 3881              - -      02/28/11 11:48:01
TCP  10.1.0.2 80                  10.10.0.1 8080
      10.0.0.1 3882              FIN -    02/28/11 11:50:01
TCP  10.1.0.4 80                  10.10.0.1 8080
      10.0.0.2 4002              - -      02/28/11 11:55:08
TCP  2001:DB8:2222:1044::72 80    2001:DB8:C003:12::2918 8080
      2001:DB8:C003:13::2928 5001  SYN -    02/28/11 10:25:12
TCP  2001:DB8:2222:1044::73 80    2001:DB8:C003:12::2918 8080
      2001:DB8:C003:13::2928 8002  - FIN    02/28/11 10:22:15

Total Number of Translations: 5
```

The table below describes the significant fields shown in the display, in alphabetical order.

**Table 14: show redirect translations Field Descriptions**

Field	Description
Destination IP/port	IP address and port number of the connection destination.
In Flags, Out Flags	TCP flags. For example, ACK, FIN, SYN, or Null.
Prot	Protocol used, either TCP or User Data Protocol (UDP).

Field	Description
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
<b>redirect server-group</b>	Defines a group of one or more servers that make up a named ISG Layer 4 redirect server group.
<b>redirect session-limit</b>	Sets the maximum number of Layer 4 redirects allowed for each ISG subscriber session.
<b>redirect to (ISG)</b>	Redirects ISG Layer 4 traffic to a specified server or server group.
<b>server ip (ISG)</b>	Adds a server to an ISG Layer 4 redirect server group.
<b>show redirect group</b>	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

<b>session</b>	Displays information about the current SGI session.
<b>statistics</b>	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
<b>debug sgi</b>	Enables debugging for SGI.
<b>sgi beep listener</b>	Enables SGI.
<b>test sgi xml</b>	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

<b>cdb</b>	Displays information about the SSM capabilities database.
<b>feature id</b>	Displays information about SSM feature settings.
<i>feature-id</i>	(Optional) Displays information for a specific feature ID.
<b>id</b>	Displays information for all SSM IDs.
<b>memory</b>	Displays memory usage information.
<b>chunk      variable</b>	(Optional) Displays memory usage information for memory consumed by variable chunks.
<b>feature</b>	Displays information about memory consumed by the feature.
<b>queue</b>	Displays information about memory consumed by the queue.
<b>segment</b>	Displays information about memory consumed by the segment.
<b>detail</b>	(Optional) Displays detailed memory usage information.
<b>segment    id</b>	Displays information about SSM segment settings.
<i>segment-id</i>	(Optional) Displays information for a specific SSM segment.
<b>switch id</b>	Displays information about SSM switch settings.
<i>switch-id</i>	(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	-/-	-/-
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 | 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 |
          |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 Circuit 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
<b>debug condition xconnect</b>	Displays conditional xconnect debug messages.

# show subscriber default-session

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

**show subscriber default-session**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

## Examples

The following is sample output from the **show subscriber default-session** command. The fields in the output are self-explanatory.

```
Device# show subscriber default-session
UID      Lite-sessions  Interface
5         0                GigabitEthernet0/0/4
```

## Related Commands

Command	Description
<b>show subscriber session</b>	Displays information about ISG subscriber sessions.

# 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 s ubscriber 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

The table below describes some of the fields shown in the sample output, in alphabetical order.

**Table 15: 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 <b>clear subscriber policy dpm statistics</b> 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 <b>clear subscriber policy dpm statistics</b> 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
<b>clear subscriber policy dpm statistics</b>	Clears the statistics for DPM session contexts.
<b>show subscriber policy dpm context</b>	Displays event traces for DPM session contexts.

Command	Description
<b>subscriber trace event</b>	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

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

```

The table below describes some of the fields shown in the sample output.

**Table 16: 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
<b>subscriber-policy</b>	Defines or modifies the forward and filter decisions of the subscriber policy.

# show subscriber service

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

**show subscriber service** [**name** *service-name*] [**detailed**]

## Syntax Description

<b>name</b> <i>service-name</i>	(Optional) Displays information about the subscriber service profile with the specific name.
<b>detailed</b>	(Optional) Displays detailed information about subscriber service profiles.

## Command Modes

User EXEC (>)

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 the Cisco 7600 series router.
15.1(2)S	This command was modified. The <b>name</b> keyword and <i>service-name</i> argument were added.
Cisco IOS XE Release 3.3	This command was modified. The <b>name</b> keyword and <i>service-name</i> argument were added.

## Usage Guidelines

If you enter the **show subscriber service** command without any keywords or arguments, information is displayed for all services on the ISG router.

## Examples

The following example shows output from the **show subscriber service** command for a service named platinum:

```
Router# show subscriber service name platinum

Service "Platinum":
Profile name: Platinum, 4 references
    traffic-class      "input access-group 102"
    policy-directive   "authenticate aaa list PPP1"

Class Id   In: 00000002
```



```
Class Id Out: 00000003
```

```
Current Subscriber Information using service "Platinum":
Total sessions: 1
```

```
Codes: lterm - Local Term, fwd - forwarded, unauth - unauthenticated, authen -
authenticated, TC Ct. - Number of Traffic Classes on the main session
```

```
Uniq ID Interface State Service Up-time TC Ct. Identifier
1 IP auth lterm 19:32:05 2 jsmith
```

The following example shows output from the **show subscriber service** command using the **name** and **detailed** keywords:

```
Router# show subscriber service name platinum detailed
```

```
Service "Platinum":
Version 1:
SVM ID : DC000001
Class Id In: 00000000
Class Id Out: 00000001
Locked by : SVM-Printer [1]
Locked by : PM-Service [1]
Locked by : PM-Info [1]
Locked by : FM-Bind [1]
Locked by : Accounting-Feature [1]
Profile : 07703430
Profile name: Platinum, 3 references
password <hidden>
username "Platinum"
accounting-list "default"
Feature : Accounting
Feature IDB type : Sub-if or not required
Feature Data : 24 bytes:
: 000000 00 00 DC 00 00 01 07 6F .....o
: 000008 CB C8 00 00 04 0F 00 00 .....
: 000010 00 03 00 00 00 00 00 00 .....
```

```
Current Subscriber Information using service "Platinum"
Total sessions: 1
```

```
Codes: lterm - Local Term, Fwd - forwarded, unauth - unauthenticated, authen -
authenticated, TC Ct. - Number of Traffic Classes on the main session
```

```
Uniq ID Interface State Service Up-time TC Ct. Identifier
1 IP authen lterm 00:26:02 1 jsmith
```

The table below describes the significant fields shown in the displays, in alphabetical order.

**Table 17: show subscriber service Field Descriptions**

Field	Description
accounting-list	AAA method list to which accounting updates are sent.
Child ID	Identifier of the parent session.
Class Id In	Class identifier of the class used by the service in the input direction.
Class Id Out	Class identifier of the class used by the service in the output direction.
Parent ID	Identifier of the parent session.

Field	Description
policy-directive	Directive defined in the service profile to authenticate the service at the specified server.
SVM ID	Service manager identifier.
State	Indicates whether the session has been authenticated or is unauthenticated.
Total sessions	Number of main sessions on the ISG.
traffic-class	Traffic class used by the service.
Uniq ID	Unique session identifier.

#### Related Commands

Command	Description
<b>show subscriber session</b>	Displays information about ISG subscriber sessions.
<b>show subscriber statistics</b>	Displays statistics about ISG subscriber sessions.

## show subscriber session

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

**show subscriber session** [**identifier** *identifier* | **uid** *session-identifier* | **username** *username*][**detailed** | **feature name** | **flow service** *service-name*]

### Syntax Description

<b>identifier</b> <i>identifier</i>	<p>(Optional) Displays information about subscriber sessions that match the specified identifier. Valid keywords and arguments are as follows:</p> <ul style="list-style-type: none"> <li>• <b>authen-status</b>—Displays information about subscriber sessions with the specified authentication status. To identify the subscriber sessions that are authenticated or not, specify one of the following keywords: <ul style="list-style-type: none"> <li>• <b>authenticated</b>—Displays information about sessions that are authenticated.</li> <li>• <b>unauthenticated</b>—Displays information about sessions that are not authenticated.</li> </ul> </li> <li>• <b>authenticated-domain</b> <i>domain-name</i>—Displays information about sessions with the specified authenticated domain name.</li> <li>• <b>authenticated-username</b> <i>username</i>—Displays information about sessions with the specified authenticated username.</li> <li>• <b>auto-detect</b>—Displays information about sessions that use autodetect. (Authorization is performed on the basis of the circuit ID or remote ID.)</li> <li>• <b>dnis</b> <i>number</i>—Displays information about sessions with the specified dialed number identification service (DNIS) number.</li> <li>• <b>mac-address</b> <i>mac-address</i>—Displays information about sessions with the specified MAC address.</li> </ul>
-------------------------------------	--

--	--

- **media *type***—Displays information about sessions that use the specified 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 *identifier***—Displays information about sessions with the specified network access server (NAS) port identifier. Valid keywords and arguments are as follows:
  - **adapter** *number*
  - **channel** *number*
  - **ipaddr** *ip-address*
  - **port** *number*
  - **shelf** *number*
  - **slot** *number*
  - **sub-interface** *number*
  - **type** *interface-type*
  - **vci** *virtual-channel-identifier*
  - **vlan** *virtual-lan-id*
  - **vpi** *virtual-path-identifier*
- **protocol *type***—Displays information about sessions that use the specified type of access protocol. Valid values for the *type* argument are as follows:
  - **atom**—Any Transport over MPLS (ATOM) access protocol
  - **ether**—Ethernet access protocol
  - **ip**—IP access protocol
  - **pdsn**—Packet Data Serving Node (PDSN) access protocol
  - **ppp**—PPP access protocol

	<ul style="list-style-type: none"> <li>• <b>vpdn</b>—Virtual private dialup network (VPDN) access protocol</li> <li>• <b>source-ip-address</b> <i>ip-address subnet-mask</i>—Displays information about sessions that are associated with the specified source IP address.</li> <li>• <b>timer</b> <i>name</i>—Displays information about sessions that use the specified timer.</li> <li>• <b>tunnel-name</b> <i>name</i>—Displays information about sessions that are associated with the specified VPDN tunnel.</li> <li>• <b>unauthenticated-domain</b> <i>domain-name</i>—Displays information about sessions with the specified unauthenticated domain name.</li> <li>• <b>unauthenticated-username</b> <i>username</i>—Displays information about sessions with the specified unauthenticated username.</li> <li>• <b>vrf</b> <i>vrf-name</i>—Displays information about sessions with the specified VPN routing and forwarding (VRF) identifier.</li> </ul>
<b>uid</b> <i>session-identifier</i>	(Optional) Displays information about sessions with the specified unique identifier.
<b>username</b> <i>username</i>	(Optional) Displays information about sessions that are associated with the specified username.
<b>detailed</b>	(Optional) Displays detailed information about sessions.

<b>feature name</b>	<p>(Optional) Displays information about specific Layer 2 features installed on the parent session. To display feature names, use the question mark (?) online help function.</p> <p>Valid keywords and arguments are as follows:</p> <ul style="list-style-type: none"> <li>• <b>access-list</b>—Per-user access control list (ACL) feature</li> <li>• <b>accounting</b>—Accounting feature</li> <li>• <b>compression</b>—Compression feature</li> <li>• <b>filter</b>—Per-user filter feature</li> <li>• <b>idle-timer</b>—Idle timeout feature</li> <li>• <b>ip-config</b>—IP configuration feature</li> <li>• <b>keepalive</b>—Keepalive feature</li> <li>• <b>l4redirect</b>—Layer 4 redirect (L4R) feature</li> <li>• <b>modem-on-hold</b>—Modem-on-hold feature</li> <li>• <b>policing</b>—Policing feature</li> <li>• <b>portbundle</b>—Portbundle hostkey feature</li> <li>• <b>prepaid-absolute</b>—Prepaid absolute timeout feature</li> <li>• <b>prepaid-idle</b>—Prepaid idle timeout feature</li> <li>• <b>qos-peruser</b>—Quality of service (QoS) policy map feature</li> <li>• <b>session-timer</b>—Absolute timeout feature</li> <li>• <b>tariff-switching</b>—Tariff switching feature</li> <li>• <b>time-monitor</b>—Prepaid time monitor feature</li> <li>• <b>volume-monitor</b>—Prepaid volume monitor feature</li> </ul>
<b>flow service service-name</b>	<p>(Optional) Displays detailed information about the specified flow service installed on the parent session.</p>

**Command Default**

If you enter the command without any keywords or arguments, the output displays information about all sessions on the ISG device.

**Command Modes**

Privileged EXEC (#)

**Command History**

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

Release	Modification
12.2(33)SRC	This command was modified. Support for this command was implemented on the Cisco 7600 series routers.
15.0(1)S	This command replaced the <b>show sss session</b> command.
15.1(2)S	This command was modified. The <b>feature name</b> and <b>flow service service-name</b> keyword-argument pairs were added. The output of the <b>identifier</b> , <b>uid</b> , and <b>username</b> keywords was enhanced to include classifier information.
Cisco IOS XE Release 3.3S	This command was modified. The <b>feature name</b> and <b>flow service service-name</b> keyword-argument pairs were added. The output of the <b>identifier</b> , <b>uid</b> , and <b>username</b> keywords was enhanced to include classifier information.
Cisco IOS XE Release 3.4S	This command was modified. The output was enhanced to include information about IPv6 sessions, and the <b>tariff-switching</b> keyword was added for the <i>name</i> argument in the <b>feature</b> keyword.
Cisco IOS XE Release 3.5S	This command was modified. The output of the <b>detailed</b> keyword was enhanced to include the IP address of sessions.
15.2(1)S	This command was modified. The output of the <b>detailed</b> and <b>uid</b> keywords was enhanced to indicate that the active L4R rules are unavailable when no policy rules exist in a subscriber session.
Cisco IOS XE Release 3.7S	This command was modified. The output of the <b>detailed</b> keyword was enhanced to include the RADIUS proxy ID of sessions.

### Usage Guidelines

When an identifier is specified, the output displays only those sessions that match the identifier.

You must configure the **policy-map type control** *policy-map-name* command to display the following fields in the **show subscriber session detailed** command output:

- Downloaded user profile, excluding services
- Downloaded user profile, including services
- Session configuration history

### Examples

The following is sample output from the **show subscriber session** command:

```
Device# show subscriber session
```

```
Current Subscriber Information: Total sessions 1
Uniq ID Interface State Service Up-time TC Ct. Identifier
1 IP authen lterm 00:27:18 1 10.10.10.10
2 Vi3 authen lterm 00:09:04 1 rouble-pppoe
```



The following is sample output from the **show subscriber session** command with the **uid** and **flow service** keywords specifying the service named Service1:

```
Device# show subscriber session uid 1 flow service Service1

Codes: Class-id - Classification Identifier, Pri. - Priority
-----
Type: IP, UID: 1, Identity: user1, State: authen
Session Up-time: 00:05:20, Last Changed: 00:04:56
Switch-ID: 4096

Service Name: Service1, Active Time = 00:05:20

Classifiers:
Class-id   Dir   Packets   Bytes           Pri.  Definition
2          Out    0         0              0     Match ACL 101
3          In    0         0              0     Match ACL 101

Features:

L4 Redirect:
Class-id   Rule cfg  Definition           Source
2          #1  SVC  to ip 10.0.2.2      Service1

Policing:
Class-id   Dir   Avg. Rate   Normal Burst   Excess Burst   Source
2          In    8000        1000           1000           Service1
3          Out   8000        1000           1000           Service1
```

The following is sample output from the **show subscriber session** command with the **uid** and **feature** keywords specifying the accounting feature:

```
Device# show subscriber session uid 1 feature accounting

Type: IP, UID: 1, Identity: user1, State: authen
Session Up-time: 00:05:50, Last Changed: 00:05:26
Switch-ID: 4096

Features:

Accounting:
Class-id   Dir   Packets   Bytes           Source
0          In    1         100             Service3
1          Out   0         0              Service3
```

The following is sample output from the **show subscriber session** command with the **detailed** keyword:



#### Note

The Classifiers section is not displayed when the **detailed** keyword is used in the Cisco 7600 series routers.

```
Device# show subscriber session detailed

Current Subscriber Information: Total sessions 1
-----
Type: IP, UID: 1, Identity: user1, State: authen
IPv4 Address: 192.168.2.1
Session Up-time: 00:04:51, Last Changed: 00:04:27
Switch-ID: 4096
Radius-Proxy ID: 4227858433

Policy information:
Context 076B8F48: Handle 50000001
AAA_id 0000000C: Flow handle 0
Authentication status: authen
Downloaded User profile, excluding services:
  sub-qos-policy-in    "QoSService1"
  sub-qos-policy-out    "QoSService2"
  prepaid-config        "default"
Downloaded User profile, including services:
```

```

accounting-list      "default"
username             "Service1"
traffic-class        "output access-group 101"
traffic-class        "input access-group 101"
l4redirect           "redirect to ip 10.0.2.2"
ssg-service-info     "QU;8000;1000;1000;D;8000;1000;1000"
sub-qos-policy-in    "QoSService1"
sub-qos-policy-out   "QoSService2"
prepaid-config       "default"
Config history for session (recent to oldest):
Access-type: Web-service-logon Client: SM
Policy event: Apply Config Success (Unapplied) (Service)
Profile name: prep_service, 9 references
  traffic-class      "input access-group 102"
  traffic-class      "output access-group 102"
Access-type: Web-user-logon Client: Account Command-Handler
Policy event: Got More Keys
Profile name: user1, 2 references
  sub-qos-policy-in  "QoSService1"
  sub-qos-policy-out "QoSService2"
  prepaid-config     "default"
Access-type: Web-service-logon Client: SM
Policy event: Apply Config Success (Unapplied) (Service)
Profile name: prep_service, 9 references
  traffic-class      "input access-group 102"
  traffic-class      "output access-group 102"
Access-type: Web-service-logon Client: SM
Policy event: Apply Config Success (Unapplied) (Service)
Profile name: prep_service, 9 references
  traffic-class      "input access-group 102"
  traffic-class      "output access-group 102"
Access-type: IP Client: SM
Policy event: Service Selection Request (Service)
Profile name: prep_service, 9 references
  traffic-class      "input access-group 102"
  traffic-class      "output access-group 102"
Access-type: IP Client: SM
Policy event: Service Selection Request (Service)
Profile name: Service1, 3 references
  password           <hidden>
  username            "Service1"
  traffic-class       "output access-group 101"
  traffic-class       "input access-group 101"
  l4redirect          "redirect to ip 10.0.2.2"
  ssg-service-info    "QU;8000;1000;1000;D;8000;1000;1000"
Access-type: IP Client: SM
Policy event: Service Selection Request (Service)
Profile name: Service3, 3 references
  password           <hidden>
  username            "Service3"
  accounting-list     "default"
Active services associated with session:
  name "Service1", applied before account logon
  name "Service3", applied before account logon
Rules, actions and conditions executed:
subscriber rule-map RULEB
  condition always event session-start
  1 service-policy type service name Service3
  2 service-policy type service name Service1
  3 service-policy type service name prep_service
subscriber rule-map RULEB
  condition always event account-logon
  1 authenticate aaa list PPPI

Classifiers:
Class-id  Dir  Packets  Bytes  Pri.  Definition
0         In   1        100    0     Match Any
1         Out  0         0      0     Match Any
2         In   0         0      0     Match ACL 101
3         Out  0         0      0     Match ACL 101

Features:

```

```

IP Config:
M=Mandatory, T=Tag, Mp=Mandatory pool
Flags Peer IP Address Pool Name Interface
      172.16.0.0 pool2 Lo0
      :: pppv6_1 Lo0

QoS Policy Map:
Class-id Dir Policy Name Source
0 In QoSService1 Peruser
1 Out QoSService2 Peruser

Accounting:
Class-id Dir Packets Bytes Source
0 In 1 100 Service3
1 Out 0 0 Service3

L4 Redirect:
Class-id Rule cfg Definition Source
2 #1 SVC to ip 10.0.2.2 Service1

Policing:
Class-id Dir Avg. Rate Normal Burst Excess Burst Source
2 In 8000 1000 1000 Service1
3 Out 8000 1000 1000 Service1

Configuration Sources:
Type Active Time AAA Service ID Name
SVC 00:04:51 - Service1
USR 00:04:27 - Peruser
SVC 00:04:51 570425346 Service3
INT 00:04:51 - Ethernet0/0

```

The following is sample output from the **show subscriber session** command with the **detailed** keyword when no policy rules exist in a subscriber session.



#### Note

The message "No Active Installed Rules" under the L4 Redirect field header of the output is displayed only when no policy rules of the L4R feature exist in a subscriber session. If any L4R rules exist in any of the flow services of the session, the output displays the existing L4R rules.

```

Device# show subscriber session detailed

Current Subscriber Information: Total sessions 1
-----
Type: IP, UID: 1, Identity: user1, State: authen
IPv4 Address: 192.68.2.1
Session Up-time: 00:04:51, Last Changed: 00:04:27
Switch-ID: 4096
Radius-Proxy ID: 4227858433

Policy information:
Context 076B8F48: Handle 50000001
AAA_id 0000000C: Flow_handle 0
Authentication status: authen
Downloaded User profile, excluding services:
  sub-qos-policy-in "QoSService1"
  sub-qos-policy-out "QoSService2"
  prepaid-config "default"
Downloaded User profile, including services:
  accounting-list "default"
  username "Service1"
  traffic-class "output access-group 101"
  traffic-class "input access-group 101"
  l4redirect "redirect to ip 10.0.2.2"
  ssg-service-info "QU;8000;1000;1000;D;8000;1000;1000"
  sub-qos-policy-in "QoSService1"
  sub-qos-policy-out "QoSService2"
  prepaid-config "default"
Config history for session (recent to oldest):

```

```

Access-type: Web-service-logon Client: SM
Policy event: Apply Config Success (Unapplied) (Service)
Profile name: prep_service, 9 references
  traffic-class      "input access-group 102"
  traffic-class      "output access-group 102"
Access-type: Web-user-logon Client: Account Command-Handler
Policy event: Got More Keys
Profile name: user1, 2 references
  sub-qos-policy-in  "QoSService1"
  sub-qos-policy-out "QoSService2"
  prepaid-config     "default"
Access-type: Web-service-logon Client: SM
Policy event: Apply Config Success (Unapplied) (Service)
Profile name: prep_service, 9 references
  traffic-class      "input access-group 102"
  traffic-class      "output access-group 102"
Access-type: Web-service-logon Client: SM
Policy event: Apply Config Success (Unapplied) (Service)
Profile name: prep_service, 9 references
  traffic-class      "input access-group 102"
  traffic-class      "output access-group 102"
Access-type: IP Client: SM
Policy event: Service Selection Request (Service)
Profile name: prep_service, 9 references
  traffic-class      "input access-group 102"
  traffic-class      "output access-group 102"
Access-type: IP Client: SM
Policy event: Service Selection Request (Service)
Profile name: Service1, 3 references
  password           <hidden>
  username           "Service1"
  traffic-class      "output access-group 101"
  traffic-class      "input access-group 101"
  l4redirect         "redirect to ip 10.0.2.2"
  ssg-service-info   "QU;8000;1000;1000;D;8000;1000;1000"
Access-type: IP Client: SM
Policy event: Service Selection Request (Service)
Profile name: Service3, 3 references
  password           <hidden>
  username           "Service3"
  accounting-list     "default"
Active services associated with session:
name "Service1", applied before account logon
name "Service3", applied before account logon
Rules, actions and conditions executed:
subscriber rule-map RULEB
  condition always event session-start
    1 service-policy type service name Service3
    2 service-policy type service name Service1
    3 service-policy type service name prep_service
subscriber rule-map RULEB
  condition always event account-logon
    1 authenticate aaa list PPP1

```

## Classifiers:

Class-id	Dir	Packets	Bytes	Pri.	Definition
0	In	1	100	0	Match Any
1	Out	0	0	0	Match Any
2	In	0	0	0	Match ACL 101
3	Out	0	0	0	Match ACL 101

## Features:

## L4 Redirect:

Class-id	Rule	cfg	Definition	Source
	No Active		Installed Rules.	

## Portbundle Hostkey:

Class-id	IP address	Bundle Number	Source
0	10.5.1.1	65	service-pbkh

## Configuration Sources:

```

Type  Active Time  AAA Service ID  Name
SVC   00:01:20    -                l4redirect
SVC   00:01:20    -                service-pbhk
INT   00:01:20    -                GigabitEthernet0/1/0

```

The following table describes the significant fields in alphabetical order, shown in the displays.

**Table 18: show subscriber session Field Descriptions**

Field	Description
Class-id	Classification identifier in inbound and outbound directions.
Definition	Class definition for the match criteria.
Dir	Direction of the class, either in or out.
Identifier	Username that is used for authorization.
Interface	Interface displayed for main sessions. For traffic flows, the value "Traffic-CI" is displayed.
Packets	Number of packets that are classified to a particular class.
Pri.	Configured priority of the class.
Rules, actions and conditions executed	Control policy rules, actions, and control class maps (conditions) that have been executed for the session.
Service	Signifies the network plumbing service. Possible values are: <ul style="list-style-type: none"> <li>• lterm—Indicates that the session is terminated locally by ISG.</li> <li>• Forwarding—Indicates that the requests are forwarded from an ISG to another ISG.</li> </ul>
State	Indicates whether the session is authenticated or unauthenticated.
Total sessions	Number of main sessions on the ISG.
Up-time	Duration (in hh:mm:ss format) for which the session is running.
Uniq ID	Unique session identifier.

#### Related Commands

Command	Description
<b>show vpdn session</b>	Displays session information about the L2TP and L2F protocols and PPPoE tunnels in a VPDN.

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

## show subscriber statistics

To display statistics about Intelligent Services Gateway (ISG) subscriber sessions, use the **show subscriber statistics** command in privileged EXEC mode.

**show subscriber statistics** [*identifier identifier*]

Syntax Description

<b>identifier</b> <i>identifier</i>	
--	--



(Optional) Displays information about subscriber sessions that match the specified identifier. Valid keywords and arguments are:

- **authen-status**—Displays information about sessions with the specified authentication status.
  - **authenticated**—Displays information about sessions that are authenticated.
  - **unauthenticated**—Displays information about sessions that are not authenticated.
- **authenticated-domain** *domain-name*—Displays information about sessions with the specified authenticated domain name.
- **authenticated-username** *username*—Displays information about sessions with the specified authenticated username.
- **auto-detect**—Displays information about sessions that use auto-detect. (Authorization is performed on the basis of circuit ID or remote ID.)
- **dnis** *number*—Displays information about sessions with the specified Dialed Number Identification Service (DNIS) number.
- **mac-address** *mac-address*—Displays information about sessions with the specified MAC address.
- **media** *type*—Displays information about sessions that use the specified type of access media. Valid values for the *type* argument are:
  - **async**—Async
  - **atm**—ATM
  - **ether**—Ethernet
  - **ip**—IP
  - **isdn**—ISDN
  - **mpls**—Multiprotocol Label Switching (MPLS)
  - **sync**—Serial
- **nas-port** *port-identifier*—Displays information about sessions with the specified network access server (NAS) port identifier. Valid keywords and arguments are one or more of the following:
  - **adapter** *adapter-number*
  - **channel** *channel-number*
  - **circuit-id** *circuit-identifier*
  - **ipaddr** *ip-address*
  - **port** *port-number*
  - **remote-id** *shelf-number*

- **shelf** *shelf-number*
  - **slot** *slot number*
  - **sub-interface** *sub-interface-number*
  - **type** *interface type*
  - **vci** *virtual-channel-identifier*
  - **vendor-class-id** *vendor-class-identifier*
  - **vlan** *virtual-lan-id*
  - **vpi** *virtual-path-identifier*
- **protocol**—Displays information about sessions that use the specified type of access protocol. Valid values for the *type* argument are:
    - **atom**—Any Transport over MPLS (AToM) access protocol.
    - **ether**—Ethernet access protocol.
    - **ip**—IP access protocol.
    - **pdsn**—Packet Data Serving Node (PDSN) access protocol.
    - **ppp**—PPP access protocol.
    - **vpdn**—Virtual Private Dialup Network (VPDN) access protocol.
  - **source-ip-address** *ip-address subnet-mask*—Displays information about sessions associated with the specified source IP address.
  - **timer** *timer-name*—Displays information about sessions that use the specified timer.
  - **tunnel-name** *tunnel-name*—Displays information about sessions associated with the specified VPDN tunnel.
  - **unauthenticated-domain** *domain-name*—Displays information about sessions with the specified unauthenticated domain name.
  - **unauthenticated-username** *username*—Displays information about sessions with the specified unauthenticated username.
  - **vrf** *vrf-name*—Displays information about sessions with the specified virtual routing and forwarding (VRF) identifier.

**Command Modes**

Privileged EXEC (#)

**Command History**

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

Release	Modification
12.2(33)SRC	This command was modified. Support for this command was implemented on the Cisco 7600 series router.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S. The output was enhanced to display statistics on flows and features.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. The output was enhanced to display statistics of flows and features.
Cisco IOS XE Release 3.7S	This command was modified. The output was enhanced to display statistics of lite sessions.

### Usage Guidelines

If you enter the **show subscriber statistics** command without any keywords or arguments, statistics are displayed for all sessions on the ISG device.

### Examples

The following is sample output from the **show subscriber statistics** command:

```
Device# show subscriber statistics

Current Subscriber Statistics:
Number of sessions currently up: 1
Number of sessions currently pending: 0
Number of sessions currently authenticated: 0
Number of sessions currently unauthenticated: 1
Highest number of sessions ever up at one time: 1
Mean up-time duration of sessions: 00:20:30
Total number of sessions up so far: 1
Mean call rate per minute: 0, per hour: 1
Number of sessions failed to come up: 0

Current Lite Session Statistics:
Number of lite sessions currently up: 1
Number of lite sessions up so far: 2
Number of lite sessions converted to full session: 0
Number of lite sessions failed to convert to dedicated sessions: 0
Number of account logons failed to find lite sessions: 0
Mean call rate per minute: 0, per hour: 2
Number of lite session failed to come up: 0
PBHK zero: 0
Default Session not in Connected State 0

Current Flow Statistics:
Number of flows currently up: 3
Highest number of flows ever up at one time: 3
Mean up-time duration of flows: 00:20:30
Number of flows failed to come up: 0
Total number of flows up so far: 3

Access type based session count:
IP-Interface sessions = 1

Feature Installation Count:

```

Feature Name	None	Inbound	Outbound
Accounting	0	1	1
L4 Redirect	0	2	1
Policing	0	1	1
Portbundle Hostkey	0	1	0

```
SHDBs in use      : 1
SHDBs allocated  : 1
SHDBs freed       : 0
```

SHDB handles associated with each client type

```
Client Name      Count
=====
LTerm            1
AAA              1
CCM              1
SSS_FM          1
IP_IF           1
ISG Classifier   1
CCM Group        1
PM              1
PM cluster       0
```

The table below describes the significant fields shown in the display:

**Table 19: show subscriber statistics Field Descriptions**

Field	Description
Mean call rate per minute, per hour	Total number of sessions that have come up per minute and per hour since the device has been up or since the last statistics were cleared.
Current Flow Statistics	Statistics about flows installed on parent sessions.
Mean up-time duration of sessions	Mean amount of time for which a session is up across sessions.
Access type based session count	Number of PPP over Ethernet (PPPoE) and IP sessions.
Feature Installation Count	Names of features installed on parent sessions and the number of instances of each feature in the inbound, outbound, and non-data path direction.

#### Related Commands

Command	Description
<b>show subscriber session</b>	Displays information about ISG subscriber sessions.

# 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
```

The table below describes some of the fields shown in the sample output, in the order in which they display.

**Table 20: show subscriber trace statistics Field Descriptions**

Field	Description
Logging enabled/disabled	Displays whether history logging is enabled with the <b>subscriber trace history</b> command.

Field	Description
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 <b>subscriber trace history</b> command. This value becomes the current log size when the log is cleared with the <b>clear subscriber trace history</b> 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
<b>clear subscriber trace history</b>	Clears the trace history log for ISG subscriber sessions.
<b>show subscriber trace history</b>	Displays the event traces for ISG subscriber sessions that are saved in the trace history log.
<b>subscriber trace event</b>	Enables event tracing for software components involved in ISG subscriber sessions.
<b>subscriber trace history</b>	Enables saving the event traces for ISG subscriber sessions to a history log.

## 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

<b>all</b>	Displays trace information for both the DHCP policy module (DPM) and the policy manager (PM).
<b>dpm</b>	Displays trace information for the DPM.
<b>pm</b>	Displays trace information for the PM.
<b>all</b>	(Optional) Displays all trace information. Output is not filtered based on the specific IP address, MAC address, reason, or unique ID.
<b>client-ip-address</b> <i>ip-address</i>	(Optional) Displays trace information for sessions that match the specified client IP address.
<b>mac-address</b> <i>mac-address</i>	(Optional) Displays trace information for sessions that match the specified client MAC address.
<b>reason</b> <i>number</i>	(Optional) Displays trace information for sessions that match the specified logging reason. Range: 1 to 6. <ul style="list-style-type: none"> <li>• 1--Dangling session cleared.</li> <li>• 2--PM callback to clear.</li> <li>• 3--Discover IDMGR required failure.</li> <li>• 4--Get class IDMGR required failure.</li> <li>• 5--Session termination error.</li> <li>• 6--Restart error.</li> </ul>
<b>uid</b> <i>session-id</i>	(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

```

## show subscriber trace history

```

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

```

The table below describes some of the significant fields shown in the sample output.

**Table 21: 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
<b>clear subscriber trace history</b>	Clears the trace history log for ISG subscriber sessions.
<b>show subscriber trace statistics</b>	Displays statistics about the event traces for ISG subscriber sessions that were saved to the history log.
<b>subscriber trace history</b>	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
```

The table below describes some of the fields shown in the sample output, in the order in which they display.

**Table 22: show subscriber trace statistics Field Descriptions**

Field	Description
Logging enabled/disabled	Displays whether history logging is enabled with the <b>subscriber trace history</b> command.

Field	Description
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 <b>subscriber trace history</b> command. This value becomes the current log size when the log is cleared with the <b>clear subscriber trace history</b> 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
<b>clear subscriber trace history</b>	Clears the trace history log for ISG subscriber sessions.
<b>show subscriber trace history</b>	Displays the event traces for ISG subscriber sessions that are saved in the trace history log.
<b>subscriber trace event</b>	Enables event tracing for software components involved in ISG subscriber sessions.
<b>subscriber trace history</b>	Enables saving the event traces for ISG subscriber sessions to a history log.

# show tech-support subscriber

To display device-state information for an Intelligent Services Gateway (ISG) subscriber to assist in troubleshooting, use the **show tech-support subscriber** command in privileged EXEC mode.

**show tech-support subscriber** [**platform**]

## Syntax Description

<b>platform</b>	(Optional) Displays platform-specific information about an ISG subscriber.
-----------------	--

## Command Default

Device-state information for all platforms for an ISG subscriber is displayed.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

## Usage Guidelines

The **show tech-support subscriber** command displays a large amount of configuration information about a Cisco device. The output can be used to troubleshoot an issue or be provided to a technical support representative when reporting a problem.



### Tip

This command can generate a large amount of output. You may want to redirect the output to a file using the **show <command> | redirect** command syntax extension. Redirecting the output to a file also makes sending the output to your Cisco Technical Support representative easier.

The output of the **show tech-support subscriber** command contains output from the following **show** commands, as listed in the order below:

- **show clock**
- **show version**
- **show running-config**
- **show subscriber statistics**
- **show pppoe statistics**
- **show pppoe summary**
- **show ppp statistics**
- **show ppp summary**

- **show processes memory | include SSS**
- **show processes cpu | include SSS**

The output of the **show tech-support subscriber platform** command contains output from the above **show** commands as well as the following **show** commands, as listed in the order below:

- **show platform software status control-process brief**
- **show platform software subscriber counters**
- **show platform software subscriber template state**
- **show platform software subscriber template**
- **show platform software subscriber rp active counters**
- **show platform software subscriber rp active data-base summary**
- **show platform software subscriber rp active data-base template**
- **show platform software subscriber fp active counters**
- **show platform software subscriber fp active accounting**
- **show platform software subscriber fp active policing**
- **show platform software subscriber fp active l4redirect**
- **show platform software subscriber fp active portbundle**
- **show platform software subscriber fp active ffr**
- **show platform software subscriber fp active ipv6-accounting**
- **show platform software subscriber fp active template state**
- **show platform software subscriber fp active template**
- **show platform software object fp active stat**
- **show platform software object fp active object-type-count | exc \_0\_**
- **show platform software object fp active error-object**
- **show platform hardware qfp active feature subscriber state**
- **show platform hardware qfp active feature subscriber state ac**
- **show platform hardware qfp active feature subscriber state ipsub**
- **show platform hardware qfp active feature subscriber state ipsub template**
- **show platform hardware qfp active feature subscriber state l2tp**
- **show platform hardware qfp active feature subscriber state l2tpv3**
- **show platform hardware qfp active feature subscriber state pppoe**
- **show platform hardware qfp active feature subscriber state pppoa**
- **show platform hardware qfp active feature subscriber state feature**
- **show platform hardware qfp active feature subscriber state feature accounting**



- **show platform hardware qfp active feature subscriber state feature policing**
- **show platform hardware qfp active feature subscriber state feature l4redirect**
- **show platform hardware qfp active feature subscriber state feature portbundle**
- **show platform hardware qfp active feature subscriber state feature ffr**
- **show platform hardware qfp active feature subscriber state feature tc**
- **show platform hardware qfp active class class statistics | exc \_0\_**
- **show platform hardware qfp active class class class client tc all**
- **show platform hardware qfp active team resource-manager usage**
- **show platform hardware qfp active infra shared-memory all**
- **show platform hardware qfp act infra exmem statistics**
- **show platform hardware qfp act infra exmem statistics user**
- **show platform hardware qfp act infra punt stat type per-cause | exc \_0\_**
- **show platform hardware qfp act infra punt stat type global-drop | exc \_0\_**
- **show platform hardware qfp act infra punt stat type inject-drop | exc \_0\_**
- **show platform hardware qfp act infra punt stat type punt-drop | exc \_0\_**
- **show platform hardware qfp act stat drop**
- **show platform hardware qfp act datapath util summary**

## Examples

The following is sample output from the **show tech-support subscriber** command:

```
Device# show tech-support subscriber | inc show
----- show clock -----
*17:35:23.481 EDT Thu Feb 21 2013

----- show version -----
----- show running-config -----

.
.
.
aaa authentication login default none
aaa authentication ppp default local
aaa authorization network default local
aaa authorization network AAA_METHOD group AUTH_SG local
aaa authorization subscriber-service default local
aaa accounting network AAA_METHOD start-stop group FREERAD
!
!
aaa server radius proxy
  key <removed>
  session-identifier attribute 31
  accounting port 6618
  client 10.0.0.1
!
!
.
.
.
```

```

subscriber service multiple-accept
subscriber authorization enable
service-policy type control LOGON_RULE_PASS
!
.
.
.
interface GigabitEthernet0/0/2.44
 encapsulation dot1Q 44
 ip address 10.0.0.2 255.0.0.0
 service-policy type control LOG_TC_4
 ip subscriber routed
  initiator unclassified ip-address
!
.
.
.
----- show sss tech-support -----

----- show subscriber statistics -----

.
.
.

Current Subscriber Statistics:
Number of sessions currently up: 1
Number of sessions currently pending: 0
Number of sessions currently authenticated: 0
Number of sessions currently unauthenticated: 1
Highest number of sessions ever up at one time: 1
Mean up-time duration of sessions: 1d20h
Total number of sessions up so far: 1
Mean call rate per minute: 0, per hour: 0
Number of sessions failed to come up: 0
.
.
.

----- show pppoe statistics -----

----- show pppoe summary -----

----- show ppp statistics -----

----- show ppp summary -----

----- show processes memory | include SSS -----

----- show processes cpu | include SSS -----

```

The following is sample output from the **show tech-support subscriber platform** command:

```

Device# show tech-support subscriber platform | inc show
----- show clock -----
----- show version -----
----- show running-config -----
----- show sss tech-support -----
----- show subscriber statistics -----
----- show pppoe statistics -----
----- show pppoe summary -----
----- show ppp statistics -----
----- show ppp summary -----
----- show processes memory | include SSS -----
----- show processes cpu | include SSS -----
----- show platform software status control-process brief -----
----- show platform software subscriber counters -----
----- show platform software subscriber template state -----
Templating is turned OFF, 0 templates, 0 sessions
----- show platform software subscriber template -----

```

Templating is turned OFF, 0 templates, 0 sessions

```

----- show platform software subscriber rp active counters -----
----- show platform software subscriber rp active data-base summary -----
----- show platform software subscriber rp active data-base template -----
----- show platform software subscriber fp active counters -----
----- show platform software subscriber fp active accounting -----
Subscriber Accounting records: Total : 3

```

Segment	Class Id In/Out	EVSI	QFP Hdl	AOM State
0x0102001000001004	2/3	16908305	148	created
0x0102001000001004	4/5	16908306	149	created
0x0102001000001004	6/7	16908307	150	created

```

----- show platform software subscriber fp active policing -----
----- show platform software subscriber fp active l4redirect -----
----- show platform software subscriber fp active portbundle -----
----- show platform software subscriber fp active ffr -----
----- show platform software subscriber fp active ipv6-accounting -----
----- show platform software subscriber fp active template state -----
----- show platform software subscriber fp active template -----
----- show platform software object fp active stat -----
----- show platform software object fp active object-type-count | exc _0_ -----
----- show platform software object fp active error-object -----
----- show platform hardware qfp active feature subscriber state -----
----- show platform hardware qfp active feature subscriber state ac -----
----- show platform hardware qfp active feature subscriber state ipsub -----

```

Subscriber IPSUB State:

```

  Current number of IP L2/Routed session: 1
  Current number of IP Interface session: 0

```

IPSUB L2 Session Lookup Depth:  
Distribution: 100%

QFP Number 0:

ipsub\_dbg\_cfg: 0x00000000

```

----- show platform hardware qfp active feature subscriber state ipsub template -----
----- show platform hardware qfp active feature subscriber state l2tp -----
----- show platform hardware qfp active feature subscriber state l2tpv3 -----
----- show platform hardware qfp active feature subscriber state pppoe -----
----- show platform hardware qfp active feature subscriber state pppoa -----
----- show platform hardware qfp active feature subscriber state feature -----
----- show platform hardware qfp active feature subscriber state feature accounting -----
----- show platform hardware qfp active feature subscriber state feature policing -----
----- show platform hardware qfp active feature subscriber state feature l4redirect -----
----- show platform hardware qfp active feature subscriber state feature portbundle -----
----- show platform hardware qfp active feature subscriber state feature ffr -----
----- show platform hardware qfp active feature subscriber state feature tc class-group -----
----- show platform hardware qfp active feature subscriber state feature tc transaction -----
----- show platform hardware qfp active class class statistics | exc _0_ -----
----- show platform hardware qfp active class class class client tc all -----
----- show platform hardware qfp active tcam resource-manager usage -----
----- show platform hardware qfp active infra shared-memory all -----

```

QFP shared-memory info

shm_win_name frees	max_win_size	curr_win_size	alloc_space	free_space	allocs
CGM	301989888	8785920	6868784	1917136	2206
231					
CPP_EXMEM	67108864	4206592	3751824	454768	588
0					
CPP_FM_STAT	4194304	2101248	32	2101216	1

```

0
CPP_HA          4194304          2101248          32          2101216          1
0
DRV_CPP0        4194304          2363392          278784          2084608          261
0
DRV_HAL         4194304          2101248          64          2101184          1
0
IFM             134217728        55197696          53147040        2050656          1098
0
TCAM_RM_IPC     5767336          2101248          32          2101216          1
0
TCAM_RM_REGINFO 4194304          2101248          160          2101088          2
0
.
.
.
----- show platform hardware qfp act infra exmem statistics -----
----- show platform hardware qfp act infra exmem statistics user -----
----- show platform hardware qfp act infra punt stat type per-cause | exc _0_ -----

----- show platform hardware qfp act infra punt stat type global-drop | exc _0_ -----
----- show platform hardware qfp act infra punt stat type inject-drop | exc _0_ -----
----- show platform hardware qfp act infra punt stat type punt-drop | exc _0_ -----
----- show platform hardware qfp act stat drop -----
-----
Global Drop Stats          Packets          Octets
-----
BadUidbIdx                15238          2285862
BadUidbSubIdx              8              1168
Disabled                  15             1698
Esfl4rBadConfig           10             1460
EssIpsubFsoldDrop         63             9198
InjectErr                 61             8070
Ipv4NoAdj                  3              168
Ipv4NoRoute               159700908      23316332568

----- show platform hardware qfp act datapath util summary -----
  CPP 0:          5 secs          1 min          5 min          60 min
Input:   Total (pps)          1004          1005          1005          1005
         (bps)          1203776          1204440          1204424          1204432
Output:   Total (pps)           3           4           4           4
         (bps)          13240           9088           8488           8384
Processing: Load (pct)         0           0           0           0

```

## 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

<i>interface-type interface-number</i>	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
<b>ip portbundle (service)</b>	Enables the ISG Port-Bundle Host Key feature for a service.
<b>length</b>	Specifies the ISG port-bundle length.
<b>show ip portbundle ip</b>	Displays information about a particular ISG port bundle.
<b>show ip portbundle status</b>	Displays information about ISG port-bundle groups.

# subscriber accounting accuracy

To guarantee Input/Output Packet/Byte statistics in the accounting Stop record are accurate within 1 second, use the **subscriberaccountingaccuracy** command in privileged EXEC mode. To disable this statistics setting, use the **no** form of this command.

**subscriber accounting accuracy** *value*

**no subscriber accounting accuracy**

## Syntax Description

<i>value</i>	Value for the Subscriber Accounting Accuracy feature in milliseconds. The range is 1,000 to 10,000.
--------------	---

## Command Default

The default value is 1000 milliseconds.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS Release XE 3.2S	This command was introduced on the ASR 1000 Series Routers.

## Examples

This section shows an example of the **subscriberaccountingaccuracy** command set to its default value:

```
Router# subscriber accounting accuracy 1000
```

# 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
	<b>aaa accounting</b>	Enables TACACS+ or RADIUS user accounting.
	<b>accounting aaa list</b>	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

<i>name-of-configuration</i>	Name of the configuration.
<b>default</b>	Specifies the default configuration.

## Command Default

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
<b>prepaid config</b>	Enables prepaid billing for an ISG service and references a configuration of prepaid billing parameters.

# subscriber policy recording

To enable iEdge policy subscriber recording use the **subscriber policy recording** command in global configuration mode. To disable the iEdge subscriber recording settings, use the **no** form of this command.

**subscriber policy recording** {**profile** {**service**| **user**}| **rules**[ **limit** *number* ]}

## Syntax Description

<b>profile</b>	Records subscriber policy profiles as they download.
<b>service</b>	Records subscriber service profiles as they download.
<b>user</b>	Records subscriber user profiles as they download.
<b>rules</b>	Records subscriber rules, condition, and actions as they execute.
<b>limit</b> <i>number</i>	Limits the number of rule events that get recorded. The range is from 0 to 4294967294

## Command Default

iEdge policy subscriber recording is not enabled.

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

When both user and service profile recording is enabled they are not saved in the running or start-up configuration.

## Examples

```
Router(config)#subscriber policy recording rules limit 100
```

## Related Commands

Command	Description
<b>show sss session</b>	Displays SSS session status.

# subscriber redundancy

To configure the broadband subscriber session redundancy policy for synchronization between High Availability (HA) active and standby processors, use the **subscriber redundancy** command in global configuration mode. To delete the policy, use the **no** form of this command.

**subscriber redundancy** {**bulk limit** {**cpu percent** **delay seconds** [**allow sessions**] | **time seconds**} | **dynamic limit** {**cpu percent** **delay seconds** [**allow sessions**] | **periodic-update interval** [ *minutes* ]} | **delay seconds** | **rate sessions seconds** | **disable**}

**no subscriber redundancy** {**bulk limit** {**cpu** | **time**} | **dynamic limit** {**cpu** | **periodic-update interval** [ *minutes* ]} | **delay** | **rate** | **disable**}

## Syntax Description

<b>bulk</b>	Configures a bulk synchronization redundancy policy.
<b>limit</b>	Specifies the synchronization limit.
<b>dynamic</b>	Configures a dynamic synchronization redundancy policy.
<b>cpu percent</b>	Specifies, in percent, the CPU busy threshold value. Range: 1 to 100. Default: 90.
<b>delay seconds</b>	Specifies the minimum time, in seconds, for a session to be ready before bulk or dynamic synchronization occurs. Range: 1 to 33550.
<b>allow sessions</b>	(Optional) Specifies the minimum number of sessions to synchronize when the CPU busy threshold is exceeded and the specified delay is met. Range: 1 to 2147483637. Default: 25.
<b>time seconds</b>	Specifies the maximum time, in seconds, for bulk synchronization to finish. Range: 1 to 3000.
<b>periodic-update interval</b>	Enables the periodic update of accounting statistics for subscriber sessions.
<i>minutes</i>	(Optional) Interval, in minutes, for the periodic update. Range: 10 to 1044. Default: 15.
<b>rate sessions seconds</b>	Specifies the number of sessions per time period for bulk and dynamic synchronization. <ul style="list-style-type: none"> <li>• <i>sessions</i>—Range: 1 to 32000. Default: 250.</li> <li>• <i>seconds</i>—Range: 1 to 33550. Default: 1.</li> </ul>

<b>disable</b>	Disables stateful switchover (SSO) for all subscriber sessions.
----------------	---

**Command Default** The default subscriber redundancy policy is applied.

**Command Modes** Global configuration (config)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
	Cisco IOS XE Release 3.5S	This command was modified. The <b>periodic-update interval</b> keyword and <i>minutes</i> argument were added.
	15.2(1)S	This command was modified. The <b>disable</b> keyword was added.

**Usage Guidelines** Cisco IOS HA functionality for broadband protocols and applications allows for SSO and In-Service Software Upgrade (ISSU) features that minimize planned and unplanned downtime and failures. HA uses the cluster control manager (CCM) to manage the capability to synchronize subscriber session initiation on the standby processor of a redundant processor system.

- Use the **bulk** keyword to create and modify the redundancy policy used during bulk (startup) synchronization.
- Use the **dynamic** keyword with the **limit** keyword to tune subscriber redundancy policies that throttle dynamic synchronization by monitoring CPU usage and synchronization rates.
- Use the **delay** keyword to establish the minimum session duration for synchronization and to manage dynamic synchronization of short-duration calls.
- Use the **rate** keyword to throttle the number of sessions to be synchronized per period.
- Use the **dynamic** keyword with the **periodic-update interval** keyword to enable subscriber sessions to periodically synchronize their dynamic accounting statistics (counters) on the standby processor. The periodic update applies to new and existing subscriber sessions. All subscriber sessions do not synchronize their data at exactly the same time. Session synchronization is spread out based on the session creation time and other factors. This command is rejected if a previous instance of the command has not finished processing.
- Use the **disable** keyword to disable SSO for all subscriber sessions.

## Examples

The following example shows how to configure a 10-second delay when CPU usage exceeds 90 percent during bulk synchronization, after which 25 sessions will be synchronized before the CCM again checks the CPU usage:

```
Router(config)# subscriber redundancy bulk limit cpu 90 delay 10 allow 25
```

The following example shows how to configure a maximum time of 90 seconds for bulk synchronization to be completed:

```
Router(config)# subscriber redundancy bulk limit time 90
```

The following example shows how to configure a 15-second delay when CPU usage exceeds 90 percent during dynamic synchronization, after which 25 sessions will be synchronized before the CCM again checks the CPU usage:

```
Router(config)# subscriber redundancy dynamic limit cpu 90 delay 15 allow 25
```

The following example shows how to configure 2000 sessions to be synchronized per second during bulk and dynamic synchronization:

```
Router(config)# subscriber redundancy rate 2000 1
```

The following example shows how to configure a periodic update so that subscriber sessions synchronize their accounting statistics every 30 minutes:

```
Router(config)# subscriber redundancy dynamic periodic-update interval 30
```

The following example shows how to disable SSO for all subscriber sessions:

```
Router(config)# subscriber redundancy disable
```

## Related Commands

Command	Description
<b>show ccm sessions</b>	Displays CCM session information.
<b>show pppatm statistics</b>	Displays PPPoA statistics.
<b>show pppoe statistics</b>	Displays PPPoE statistics.
<b>show ppp subscriber statistics</b>	Displays PPP subscriber statistics.

## 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

<b>dpm</b>	Enables event tracing for the DHCP policy module (DPM).
<b>pm</b>	Enables event tracing for the policy manager (PM) module.
<b>retain</b>	(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
<b>show subscriber policy dpm context</b>	Displays event traces for DPM session contexts.
<b>show subscriber trace history</b>	Displays the event traces for ISG subscriber sessions that are saved in the history log.
<b>subscriber trace history</b>	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

<b>dpm</b>	Saves DHCP policy module (DPM) event traces to the history log.
<b>pm</b>	Saves policy manager (PM) event traces to the history log.
<b>size</b> <i>max-records</i>	(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
<b>clear subscriber trace history</b>	Clears the trace history log for ISG subscriber sessions.
<b>show subscriber trace history</b>	Displays the event traces for ISG subscriber sessions that are saved in the trace history log.
<b>show subscriber trace statistics</b>	Displays statistics about the event traces for ISG subscriber sessions that were saved to the history log.
<b>subscriber trace event</b>	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

<i>filename</i>	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
<b>debug sgi</b>	Enables debugging on SGI.
<b>sgi beep listener</b>	Enables SGI.
<b>show sgi</b>	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

<b>time</b>	Specifies the threshold for time-based prepaid sessions.
<i>number-of-seconds</i>	When a quota, in seconds, has been depleted to this number, ISG will send a reauthorization request. Default = 0.
<b>volume</b>	Specifies the threshold for volume-based prepaid sessions.
<i>number-of-bytes</i>	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
<b>prepaid config</b>	Enables prepaid billing for an ISG service and references a configuration of prepaid billing parameters.
<b>subscriber feature prepaid</b>	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 return to the default value, use the **no** form of this command.

**timeout absolute** *duration-in-seconds*

**no timeout absolute**

## Syntax Description

*duration-in-seconds*

Maximum subscriber session lifetime, in seconds. Range: 0 to 31104000. 0 sets the amount of time to unlimited.

## Command Default

Session timeout is disabled.

## Command Modes

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

## Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 3.5S	This command was modified. The maximum value of the <i>duration-in-seconds</i> argument was increased from 4294967 seconds to 31104000 seconds.

## 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
<b>timeout idle</b>	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* [**both** | **inbound**]

**no timeout idle**

## Syntax Description

<i>duration-in-seconds</i>	Number of seconds a subscriber session can be idle before it is terminated. Range: <i>n</i> to 15552000. The minimum value is platform and release-specific. For more information, use the question mark (?) online help function.
<b>both</b>	(Optional) Applies the idle timer to traffic in both the inbound and outbound directions.
<b>inbound</b>	(Optional) Applies the idle timer to traffic in the inbound direction only.

## Command Default

Idle timeout is disabled.

## Command Modes

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

## 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 <i>duration-in-seconds</i> argument was changed from 1 to a platform-specific number.
Cisco IOS XE Release 3.5S	This command was modified. The maximum value of the <i>duration-in-seconds</i> argument was increased from 4294967 seconds to 15552000 seconds.
Cisco IOS XE Release 3.6S	This command was modified. The <b>both</b> and <b>inbound</b> keywords were added.



## 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.

If the **timeout idle** command is configured under a traffic class, and it is configured without any keywords, the timer applies in the direction of the traffic class.

The table below shows the keywords that are available based on the direction of the traffic class where the **timeout idle** command is configured. It also shows the default behavior if the command is configured without a keyword.

Idle Timer Is Configured Here	Keywords Available	Default Behavior if No Keyword
Inbound and outbound IP sessions	<b>both, inbound</b>	Timer is applied to the configured direction. If no timer direction is specified, the timer is applied in the outbound direction.
Inbound and outbound traffic class, or classless service	<b>both, inbound</b>	Timer is applied to the configured direction for an inbound and outbound traffic class. If no direction is specified, the timer is applied in the outbound direction.  <b>Note</b> In releases before Cisco IOS XE Release 3.6S, the idle timer is always applied in the inbound direction for classless services.
Inbound traffic class only	<b>inbound</b>	Timer is applied in the inbound direction.
Outbound traffic class only	—	Timer is applied in the outbound direction.

## Examples

The following example shows that the idle connection time is limited to 30 seconds in the inbound direction:

```
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 inbound
 class type traffic default
 drop
```

## Related Commands

Command	Description
<b>timeout absolute</b>	Specifies the maximum ISG subscriber session lifetime.



## timer (ISG RADIUS proxy)

To configure the maximum amount of time for which an Intelligent Services Gateway (ISG) session waits for an event before terminating the 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** {**disconnect** {**acct-stop**| **reauth-fail**}| **ip-address**| **reconnect**| **request**| **roaming**} *seconds*

**no timer** {**disconnect** {**acct-stop**| **reauth-fail**}| **ip-address**| **reconnect**| **request**| **roaming**}

### Syntax Description

<b>disconnect</b>	Specifies a timer for disconnecting the session.
<b>acct-stop</b>	Specifies a timer for disconnecting the session after an accounting-stop request is received by ISG.
<b>reauth-fail</b>	Specifies a timer for disconnecting the session during an Extensible Authentication Protocol-Subscriber Identity Module (EAP-SIM) reauthentication failure.
<b>ip-address</b>	Specifies a timer for the IP address assigned to the session.
<b>reconnect</b>	Specifies a timer for reconnecting the session.
<b>request</b>	Specifies a timer for receiving an access request from a client device.
<b>roaming</b>	Specifies a timer for hotspot roaming.
<i>seconds</i>	Duration (in seconds) for which ISG waits before terminating a RADIUS proxy session. The range is from 0 to 43200. The default is 0.

### 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.

Release	Modification
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S. The <b>reconnect</b> keyword was added.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S. The <b>roaming</b> keyword was added.
Cisco IOS XE Release 3.7S	This command was modified. The <b>disconnect</b> 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 per client or globally for all RADIUS proxy clients. The per-client configuration overrides the global configuration. The timer is set by the RADIUS proxy in response to the termination of a subscriber IP session that is associated with the RADIUS proxy session. While the timer is running, the RADIUS proxy session is maintained regardless of whether the subscriber IP session (that was created after the timer was started) exists or not. If a subscriber 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

The following example shows how to configure ISG to wait for 20 seconds for an access request packet before terminating the RADIUS proxy session:

```
Device(config)# aaa server radius proxy
Device(config-locsvr-proxy-radius)# timer request 20
```

The following example shows how to configure the RADIUS proxy session roaming timer:

```
Device(config)# aaa server radius proxy
Device(config-locsvr-proxy-radius)# timer roaming 60
```

The following example shows how to configure the RADIUS proxy session disconnect delay timer for accounting stop in RADIUS proxy client mode:

```
Device(config)# aaa server radius proxy
Device(config-locsvr-proxy-radius)# client 192.0.2.1
Device(config-locsvr-radius-client)# timer disconnect acct-stop 30
```

The following example shows how to configure the RADIUS proxy session disconnect delay timer for reauthentication failure in RADIUS proxy client mode:

```
Device(config)# aaa server radius proxy
Device(config-locsvr-proxy-radius)# client 192.0.2.1
Device(config-locsvr-radius-client)# timer disconnect reauth-failure 20
```

### Related Commands

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

# 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

<b>cos</b>	(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.
<b>dscp</b>	(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.
<b>precedence</b>	(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
<b>class</b>	Specifies the name of the class whose traffic policy you want to create or change.
<b>police</b>	Configures the Traffic Policing feature.
<b>policy-map</b>	Creates a policy map that can be attached to multiple ports to specify a service policy and enters policy-map configuration mode.
<b>set</b>	Marks IP traffic by setting a CoS, DSCP, or IP-precedence in the packet.
<b>show policy-map</b>	Displays information about the policy map.