

Configuring ISG Accounting

The Intelligent Services Gateway (ISG) is a Cisco software feature set that provides a structured framework to edge devices that can deliver flexible and scalable services to subscribers. This module describes how to configure ISG accounting, including per-session accounting or per-flow accounting, broadcast accounting, and postpaid tariff switching.

- Prerequisites for ISG Accounting, on page 1
- Restrictions for ISG Accounting, on page 1
- Information About ISG Accounting, on page 2
- How to Configure ISG Accounting, on page 5
- Configuration Examples for ISG Accounting, on page 17
- Additional References, on page 23
- Feature Information for ISG Accounting, on page 24

Prerequisites for ISG Accounting

- Configure the authentication, authorization, and accounting (AAA) method list using the **aaa accounting** command before configuring Intelligent Services Gateway (ISG) accounting. ISG sends accounting records to the AAA method list specified in the user profile, service profile, or service policy map. For more information about the AAA commands, see the *Cisco IOS Security Command Reference: Commands A to C* .
- AAA servers must be configured to support ISG accounting.

Restrictions for ISG Accounting

- Intelligent Services Gateway (ISG) accounting supports only the RADIUS protocol.
- If authentication, authorization, and accounting (AAA) broadcast accounting is used with periodic accounting, you cannot configure different accounting periods for different accounting groups.

Information About ISG Accounting

Overview of ISG Accounting

Intelligent Services Gateway (ISG) supports per-session, per-service, or per-flow accounting. Per-session accounting is the aggregate of all the flow traffic for a session and it can be enabled in a user profile.

Per-flow accounting, which accounts for a subset of session traffic as defined by a traffic class, is enabled in a service profile or service policy map. When per-flow accounting is configured, the Parent-Session-ID vendor-specific attribute (VSA) is included in accounting records so that per-session and per-flow accounting records can be correlated in the RADIUS server.

Within a subscriber session, per-service accounting enables RADIUS to track services when they become active and when they stop. Per-service accounting is the aggregate of all flow traffic for the duration of the service. Using this feature, the device includes all activated services for the session in a single accounting start message. Per-service accounting can be enabled in a service profile or service policy map. When per-service accounting is configured, the service name and Parent-Session-ID attributes are included in accounting records.



Note When accounting is configured in a user profile, the service name attribute is not included in accounting records.

Session accounting is enabled if the **aaa accounting network default** command is configured and a authentication, authorization, and accounting (AAA) method list is specified. We recommend that you use a named method list rather than the default method list. Flow accounting is disabled by default and will take place only if a AAA method list is specified in the service profile or a service policy map. ISG accounting sends Accounting-Start, interim, and Accounting-Stop records to the specified AAA method list.

ISG Accounting Messages on ANCP Ports

Accounting messages sent by Intelligent Services Gateway (ISG) for sessions on an Access Node Control Protocol (ANCP) port contain the following authentication, authorization, and accounting (AAA) attributes:

- nas-rx-speed
- nas-rx-speed-bps
- nas-tx-speed
- nas-tx-speed-bps

ISG retrieves the values for these attributes from the Digital Subscriber Line Access Multiplexer (DSLAM) ANCP notification sent to ISG or from the quality of service (QoS) policy configured on the interface.

When an ANCP port is in an up state, the attribute values are taken from the DSLAM ANCP notification sent to ISG. If the ANCP port state changes to a down state, the ANCP accounting messages will continue to contain the AAA attributes sent in the DSLAM notification.

If the ANCP port state has never been set to up, ISG can retrieve the nas-tx-speed, nas-tx-speed-bps, nas-rx-speed, and nas-rx-speed-bps AAA attributes from the QoS policy on that interface.

To retrieve the AAA attributes from the QoS policy, the policy must be configured before the configuration of the ANCP neighbor; otherwise, ISG uses the previous values (if any) for the AAA attributes when a session is established.

If the QoS policy values are changed, ISG continues to use the previous values until the ANCP neighbor is removed and reconfigured.

Service Activation and Deactivation Configuration on RADIUS

You can configure Cisco VSA 250 and VSA 252 in the service profile on RADIUS to dynamically activate and deactivate services. RADIUS uses VSA 250 in Access-Accept and VSA 252 in Change of Authorization (CoA) messages. These VSAs have the following syntax:

```
252 0b "service(parameter1=value,parameter2=value,...)"
250 "service(parameter1=value,parameter1=value,...)"
```

When deactivating a service, RADIUS sends the same information in VSA 252 that was used for service activation, except that service deactivation uses 0c parameters in the VSA instead of the 0b parameter used for service activation. VSA 252 has the following syntax for service deactivation:

```
252 0xC "service(parameter1=value,parameter2=value,...)"
```

ISG Accounting Records

Intelligent Services Gateway (ISG) accounting uses the RADIUS protocol to facilitate interaction between ISG and an external RADIUS-based authentication, authorization, and accounting (AAA) server or a mediation server. ISG sends accounting records with the associated attributes to the AAA accounting method list when the following events occur—account logon, account logoff, service logon, and service logoff. The accounting server can be configured to interpret the accounting records to generate bills for postpaid sessions.

Account Logon and Logoff

ISG sends a RADIUS Accounting-Request record to the specified AAA method list when a subscriber logs on to or out off ISG. The Acct-Status-Type attribute included in the Accounting-Request record indicates if the record marks the start (commencement) of the subscriber session or the stop (termination) of the session.

When the **aaa accounting** command is enabled with the **system**, **default**, **start-stop**, and **group** keywords, accounting records are sent to the AAA server. When a subscriber logs on, ISG sends an Accounting-Start record to the AAA server. When a subscriber logs off, ISG sends an Accounting-Stop record to the AAA server.

Service Logon and Logoff

ISG sends a RADIUS Accounting-Start record to the AAA server when a service is activated for a subscriber, and it sends an Accounting-Stop record when a service is deactivated. The record contains an accounting session ID that is different from the accounting session ID of the parent session.

The Acct-Status-Type attribute included in the Accounting-Request record indicates whether the record marks the start or the end of the service. The name of the service is included in accounting records for service logon and logoff.

Accounting records may be sent for events other than account and service logon and logoff. See the *Securing User Services Configuration Guide Library* for more information.

Interim ISG Accounting Updates

Intelligent Services Gateway (ISG) supports interim (intermittent) RADIUS accounting updates that work the same way as "watchdog" RADIUS accounting. Accounting updates are sent between the time that ISG sends Accounting-Start and Accounting-Stop records.

ISG supports two types of interim accounting—accounting updates for new information (such as a new IP address) and periodic accounting, in which accounting records are sent at a configurable interval.

Interim accounting can be enabled or disabled globally for new information. Periodic accounting can be enabled for specific contexts, such as globally, in user profiles, and in services.

Broadcast Accounting

Intelligent Services Gateway (ISG) supports authentication, authorization, and accounting (AAA) broadcast accounting, which is the ability to send user accounting records to multiple RADIUS servers. AAA broadcast accounting provides service providers with geographical redundancy for RADIUS servers and provides accounting records to partners in wholesale models. For information about configuring AAA broadcast accounting, see the "Configuring Accounting" chapter in the *Cisco Authentication, Authorization, and Accounting Configuration Guide.*

ISG Postpaid Tariff Switching

The Intelligent Services Gateway (ISG) Postpaid Tariff Switching feature allows changes in tariffs during the lifetime of a connection. This feature applies to time-based or volume-based postpaid sessions in which the tariff changes at certain times of the day.

Typically, a service provider would use postpaid tariff switching to offer different tariffs to a subscriber while the subscriber is still connected. For example, changing a subscriber to a less expensive tariff during off-peak hours.

To handle tariff switches for postpaid connections, accounting packets log the usage information during the various tariff-switch intervals. The service profile contains a weekly tariff-switch plan detailing the times of day during which tariff changes occur. ISG monitors the usage at every tariff-switch point and records this information in interim accounting records. The billing server monitors all the interim accounting updates and obtains the information about the traffic sent at each tariff rate.



Note Tariff switching is not required for time-based billing services. Because the billing server knows the service logon and logoff time stamps, it can calculate the various tariffs that apply during that time.

Subscriber Accounting Accuracy

The Subscriber Accounting Accuracy feature guarantees that the I/O packet/byte statistics in the Accounting-Stop record are accurate to within one second.

Subscriber accounting data is sent to authentication, authorization, and accounting (AAA) servers during the following events:

- Configured intervals during the lifetime of the session or service

- Service logoff
- Session tear down

Use the **subscriber accounting accuracy** *milliseconds* command to set the value for the Subscriber Accounting Accuracy feature.

HA Support for ISG Accounting

The accounting start and stop records that Intelligent Services Gateway (ISG) sends to an external RADIUS accounting server contains cumulative counters associated with subscriber sessions. ISG can also send interim accounting records containing the latest time and volume statistics at periodic intervals during a session's lifetime. This information is correlated by a third-party billing software to generate billing records for the subscriber.

The ISG stateful switchover (SSO) and In Service Software Upgrade (ISSU) feature adds high availability (HA) support to the ISG session, service, and flow accounting. This HA support includes a periodic session update feature that enables ISG to retain cumulative accounting counters associated with the subscriber sessions after an SSO or ISSU event. Configuring this feature prevents the new active processor from restarting the accounting counters from zero after an SSO event. You can also specify that the first record sent after an SSO event is an interim accounting record for sessions, services, and flows that survive the switchover.

The following are some of the counters and their associated counters that retain their value after Route Processor (RP) SSO:

- Session counters:
  - Acct-Input-Octets
  - Acct-Input-Packets
  - Acct-Output-Octets
  - Acct-Output-Packets
  - Acct-Session-Time
- Service counters:
  - Acct-Input-Octets
  - Acct-Input-Packets
  - Acct-Output-Octets
  - Acct-Output-Packets

For information about configuring HA on the ISG device, see the *High Availability Configuration Guide*.

How to Configure ISG Accounting

Enabling ISG per-Session Accounting

Per-session accounting can be configured in the user profile of a authentication, authorization, and accounting (AAA) server.

This task contains the following sections:

Enabling ISG per-Session Accounting in a User Profile on a AAA Server

Use the attributes given in this procedure to enable per-session accounting in a user profile on an authentication, authorization, and accounting (AAA) server.

Note You must configure a service for an accounting list before enabling a per-session accounting in a user profile. A per-session accounting list cannot be applied on a session in Intelligent Services Gateway (ISG) if a service is not configured; that is, you must have a dummy service configured under the accounting list when there is no service configured.

SUMMARY STEPS

1. Cisco-Attribute-Value pair (AVpair)="accounting-list=*accounting-mlist-name*"
2. IETF RADIUS attribute Acct-Interim-Interval (attribute 85)

DETAILED STEPS

Procedure

Step 1 Cisco-Attribute-Value pair (AVpair)="accounting-list=*accounting-mlist-name*"

Adds the Accounting attribute to the user profile. This attribute enables accounting and specifies the AAA method list to which accounting updates will be sent.

Step 2 IETF RADIUS attribute Acct-Interim-Interval (attribute 85)

(Optional) Adds the Acct-Interim-Interval (attribute 85) to the user profile. This attribute specifies the number of seconds between interim updates.

Enabling a per-User Accounting List

Perform this task to enable a dummy service on an accounting list. A dummy service is a string that is used to get an authorization from a server for a user profile when no service is configured.

SUMMARY STEPS

1. userxxx2@cisco.com Cleartext-Password := "cisco111"
2. Cisco-Account-Info += "ADUMMYSERVICE",

DETAILED STEPS

Procedure

Step 1 userxxx2@cisco.com Cleartext-Password := "cisco111"

Adds the username and password account information for a RADIUS user profile.

Step 2 Cisco-Account-Info += “ADUMMYSERVICE”,

Adds a dummy service to a RADIUS user profile for an accounting list on an authentication, authorization, and accounting (AAA) server.

Enabling ISG per-Flow Accounting

Intelligent Services Gateway (ISG) per-flow accounting can be configured in the following configuration sources:

- Service profile on a AAA server
- Service policy map on the ISG device

This procedure contains the following sections:

Enabling ISG per-Flow Accounting in a Service Profile on the AAA Server

Perform this task to configure a per-flow accounting in a service profile on the authentication, authorization, and accounting (AAA) server.

Before you begin

This task assumes that you have defined IP access lists for specifying the traffic.

SUMMARY STEPS

1. Cisco-AVpair=“ip:traffic-class={in | out} access-group [*acl-number* | name *acl-name*] [priority *n*]”
2. Cisco-AVpair=“accounting-list=*accounting-mlist-name*”
3. IETF RADIUS attribute Acct-Interim-Interval (attribute 85)

DETAILED STEPS

Procedure

Step 1 Cisco-AVpair=“ip:traffic-class={in | out} access-group [*acl-number* | name *acl-name*] [priority *n*]”

Adds the Intelligent Services Gateway (ISG) traffic class attribute to the service profile. This attribute specifies the input and output traffic to which the service will apply. Both an input and output traffic classifier can be added to a service profile.

Step 2 Cisco-AVpair=“accounting-list=*accounting-mlist-name*”

Adds the accounting attribute to the service profile on the AAA server. This attribute enables accounting and specifies the AAA method list to which accounting updates will be sent. The AAA method list must be configured.

Note

If this attribute is configured in a service profile that does not include a traffic class, accounting is performed on the session rather than on the flow.

Step 3 IETF RADIUS attribute Acct-Interim-Interval (attribute 85)

(Optional) Adds the IETF RADIUS attribute Acct-Interim-Interval (attribute 85) to the service profile on the AAA server. This attribute specifies the number of seconds between interim updates.

Enabling ISG per-Flow Accounting in a Service Policy Map

Perform this task to enable accounting in a local service policy map for the device for a specific flow.

Before you begin

This task assumes that you have defined a traffic class map and associated IP access lists. See the module "Configuring ISG Subscriber Services" for more information about configuring traffic classes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **class type traffic** *class-map-name*
5. **accounting aaa list** *AAA-method-list*
6. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Device(config)# policy-map type service service1`	Creates or defines a service policy map, which is used to define an Intelligent Services Gateway (ISG) service and enters service policy-map configuration mode.

	Command or Action	Purpose
Step 4	**class type traffic** *class-map-name* **Example:** `Device(config-service-policymap)# class type traffic firstclass`	Associates a previously configured traffic class with the policy map and enters control policy-map traffic class configuration.
Step 5	**accounting aaa list** *AAA-method-list* **Example:** `Device(config-control-policymap-class-traffic)# accounting aaa list list1`	Enables accounting and specifies the authentication, authorization, and accounting (AAA) method list to which accounting updates will be sent. • The AAA method list must be configured.
Step 6	**end** **Example:** `Device(config-control-policymap-class-traffic)# end`	Returns to privileged EXEC mode.

Enabling ISG per-Service Accounting

Per-service accounting can be configured in the following configuration sources:

- Service profile on a AAA server
- Service policy map on the ISG device

This procedure contains the following sections:

Enabling per-Service Accounting on ISG

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber service multiple-accept**
4. **subscriber service session-accounting**
5. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**subscriber service multiple-accept** **Example:** `Device(config)# subscriber service multiple-accept`	Enables multiple services in a single Access-Accept message.
Step 4	**subscriber service session-accounting** **Example:** `Device(config)# subscriber service session-accounting`	Enables subscriber services accounting. • All started services are included in the session accounting start message.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Enabling per-Service Accounting in a Service Profile on a AAA Server

Use the attributes in this procedure to enable per-service accounting in a service profile on a authentication, authorization, and accounting (AAA) server. Note that for per-service accounting, the traffic class attribute should not be included in the service profile.

SUMMARY STEPS

1. Cisco-AVpair="accounting-list=*accounting_mlist_name*"
2. IETF RADIUS attribute Acct-Interim-Interval (attribute 85)

DETAILED STEPS

Procedure

Step 1 Cisco-AVpair="accounting-list=*accounting_mlist_name*"

Adds the Accounting attribute to the service profile. This attribute enables accounting and specifies the AAA method list to which accounting updates will be sent.

Step 2 IETF RADIUS attribute Acct-Interim-Interval (attribute 85)

(Optional) Adds the Acct-Interim-Interval (attribute 85) to the service profile. This attribute specifies the number of seconds between interim updates.

Enabling per-Service Accounting in a Service Policy Map

To configure a per-service accounting in a service policy map on the device, you must configure an empty traffic class map (a traffic class map that does not specify an access list) and enable accounting within the empty traffic class in the service policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type traffic match-any** *class-map-name*
4. **exit**
5. **policy-map type service** *policy-map-name*
6. **class type traffic** *class-map-name*
7. **accounting aaa list** *AAA-method-list*
8. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**class-map type traffic match-any** *class-map-name* **Example:** `Device(config)# class-map type traffic match-any empty_class`	Creates or modifies a traffic class map, which is used for matching packets to a specified ISG traffic class, and enters traffic class-map configuration mode. • For per-session accounting, create an empty traffic class map, that is, a traffic class map that does not specify an access list for matching traffic.
Step 4	**exit** **Example:** `Device(config-traffic-classmap)# exit`	Exits traffic class-map configuration mode.

	Command or Action	Purpose
Step 5	**policy-map type service** *policy-map-name* **Example:** `Device(config)# policy-map type service polmap1`	Creates or defines a service policy map, which is used to define an ISG service, and enters service policy-map configuration mode.
Step 6	**class type traffic** *class-map-name* **Example:** `Device(config-service-policymap)# class type traffic empty_class`	Associates a traffic class map with the service policy map and enters service policy-map traffic class configuration mode. • In this step, reference the empty traffic class map that you created in Step 3.
Step 7	**accounting aaa list** *AAA-method-list* **Example:** `Device(config-service-policymap-class-traffic)# accounting aaa list list1`	Enables accounting and specifies the authentication, authorization, and accounting (AAA) method list to which accounting updates will be sent.
Step 8	**end** **Example:** `Device(config-service-policymap-class-traffic)# end`	Returns to privileged EXEC mode.

Configuring ISG Postpaid Tariff Switching

ISG postpaid tariff switching can be configured in the service profile on a authentication, authorization, and accounting (AAA) server.

If you include a traffic class in the service profile, postpaid tariff switching will apply to the specified flow. If you do not configure a traffic class, postpaid tariff switching will apply to the session. Perform this task to configure per-session or per-flow postpaid tariff switching.

Before you begin

Intelligent Services Gateway (ISG) per-session or per-flow accounting must be configured for postpaid tariff switching to work.

SUMMARY STEPS

1. Cisco-AVpair = “PPW*hh*:*mm*:*ss*:*d*”
2. Cisco-AVpair = “ip:traffic-class={in | out} access-group [*acl-number* | name *acl-name*] [priority *n*]”

DETAILED STEPS

Procedure

Step 1 Cisco-AVpair = "PPW*hh*:*mm*:*ss*:*d*"

Adds the postpaid VSA to the service profile. This attribute specifies the weekly tariff-switch points for postpaid tariff switching. The syntax description is as follows:

hh :*mm*:*ss*:*d*—Weekly tariff-switch time.

- hh = hour of day <0-23>
- mm = minutes <0-59>
- ss = seconds <0-59>
- d = bitmap format for the days of week. Each weekday is represented by one bit, as follows:
  - 00000001 = Monday
  - 00000010 = Tuesday
  - 00000100 = Wednesday
  - 00001000 = Thursday
  - 00010000 = Friday
  - 00100000 = Saturday
  - 01000000 = Sunday

Step 2 Cisco-AVpair = "ip:traffic-class={in | out} access-group [*acl-number* | name *acl-name*] [priority *n*]"

Adds the ISG traffic class attribute to the service profile. This attribute specifies input and output traffic to which the service will apply. Both an input and output traffic classifier can be added to a service profile.

What to Do Next

You may want to configure a method of activating the service policy map or service profile. For example, control policies can be used to activate services. For more information about methods of service activation, see the "Configuring ISG Subscriber Services" module.

Verifying ISG Accounting and Postpaid Tariff Switching

To verify and troubleshoot Intelligent Services Gateway (ISG) accounting and postpaid tariff switching, use any of the following commands in privileged EXEC mode. You can use these commands in any order.

SUMMARY STEPS

1. **show subscriber session**
2. **show aaa sessions**
3. **show aaa user** {**all** | *unique id*}
4. **show sss session** [**all**]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**show subscriber session** **Example:** `Device# show subscriber session`	Displays ISG subscriber session information.
Step 2	**show aaa sessions** **Example:** `Device# show aaa sessions`	Displays authentication, authorization, and accounting (AAA) subscriber session information.
Step 3	**show aaa user** {**all** | *unique id*} **Example:** `Device# show aaa user all`	Displays AAA subscriber information for all users or a specified user.
Step 4	**show sss session** [**all**] **Example:** `Device# show sss session`	Displays Subscriber Service Switch (SSS) session status.

Enabling Periodic Session Update

Perform this task to enable Intelligent Services Gateway (ISG) to periodically synchronize the dynamic accounting statistics (counters) for subscriber sessions on the standby processor, to suppress accounting on and accounting off messages during a switchover, or to send the interim accounting record first after a switchover.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber redundancy dynamic periodic-update interval** *minutes*
4. **aaa accounting redundancy suppress system-records**
5. **aaa accounting redundancy best-effort-reuse send-interim**
6. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**subscriber redundancy dynamic periodic-update interval** *minutes* **Example:** `Device(config)# subscriber redundancy dynamic periodic-update interval 30`	Enables periodic update of accounting statistics for subscriber sessions.
Step 4	**aaa accounting redundancy suppress system-records** **Example:** `Device(config)# aaa accounting redundancy suppress system-records`	Suppresses accounting on and accounting off messages during a switchover.
Step 5	**aaa accounting redundancy best-effort-reuse send-interim** **Example:** `Device(config)# aaa accounting redundancy best-effort-reuse send-interim`	Sends the interim accounting record first after a switchover for session and service accounting.
Step 6	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Verifying Periodic Session Update

To verify and troubleshoot the configuration of the periodic session update on the ISG device, use any of the following commands in privileged EXEC mode. You can use these commands in any order.

Command	Purpose
show ccm clients	Displays information about cluster control manager (CCM) clients in HA dual RP systems.
show ccm queues	Displays CCM queue statistics for HA dual RP systems.
show ccm sessions	Displays information about CCM sessions in HA dual RP systems.

Troubleshooting ISG Accounting

Use the commands in this task to monitor and troubleshoot Intelligent Services Gateway (ISG) accounting. All these commands are optional and can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **debug aaa accounting**
3. **debug radius brief**
4. **debug subscriber feature name accounting event**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug aaa accounting** **Example:** `Device# debug aaa accounting`	Displays information about authentication, authorization, and accounting (AAA) TACACS+ authentication.
Step 3	**debug radius brief** **Example:** `Device# debug radius brief`	Enables debugging of the RADIUS configuration.
Step 4	**debug subscriber feature name accounting event** **Example:** `Device# debug subscriber feature name accounting event`	Displays diagnostic information about the installation and removal of ISG features on ISG subscriber sessions.

Configuration Examples for ISG Accounting

Example: Enabling ISG per-Flow Accounting

Example: Enabling ISG per-Flow Accounting in a Service Profile on the AAA Server

The following example shows Intelligent Services Gateway (ISG) per-flow accounting configured in a remote service profile for a service called “video1”:

```
   video1        Password = "cisco"
   Cisco-AVpair = "traffic-class=input access-group 101 priority 20",
   Cisco-AVpair = "traffic-class=output access-group 112 priority 20",
   Cisco-Avpair = "accounting-list=remote-local",
   Service-Info = "QU;8000",
   Service-Info = "QD;64000"
```

Example: Enabling ISG per-Flow Accounting in a Service Policy Map

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

```
class-map type traffic match-any video1
 match access-group output 101
 match access-group input 100
!
policy-map type service video1
 class type traffic video1
  accounting aaa list mlist1
```

Example: Enabling ISG per-Service Accounting

The following configuration example allows multiple services in a single Access-Accept message and enables session accounting for services. The example also shows how to enable RADIUS to authorize the subscriber to access services.

```
subscriber service multiple-accept
subscriber service session-accounting
subscriber authorization enable
```

Example: Enabling a per-User Accounting List

The following example shows a dummy service configured for an Intelligent Services Gateway (ISG) per-session accounting list configured on an authentication, authorization, and accounting (AAA) server:

```
userxxx2@cisco.com Cleartext-Password := "cisco111"
         Service-Type = Framed-User,
         Framed-Protocol = PPP,
         Framed-IP-Address = 192.168.17.17,
         Cisco-Account-Info += "ADUMMYSERVICE",
```

```
DUMMYSERVICE Cleartext-Password := "cisco"
         Cisco-AVPair+= "accounting-list=testacct",
```

Example: Enabling ISG per-Service Accounting in a Service Policy Map

The following example shows how to configure per-service accounting in a service policy map on the Intelligent Services Gateway (ISG) device:

```
class-map type traffic match-any classmap1
!
policy-map type service polmap1
 class type traffic classmap1
  accounting aaa list mlist1
```

Example: Configuring Postpaid Tariff Switching

The following example shows the configuration of a postpaid tariff switch each day of the week at midnight:

```
Cisco-AVpair = "PPW00:00:00:127"
```

The following example shows the configuration of a postpaid tariff switch Monday through Friday at 8:00 p.m.:

```
Cisco-AVpair = "PPW20:00:00:31"
```

The following example shows the configuration of a postpaid tariff switch Monday through Friday at 6:00 a.m.:

```
Cisco-AVpair = "PPW06:00:00:31"
```

Example: Enabling Periodic Session Update

The following example shows that the Intelligent Services Gateway (ISG) device is configured to suppress accounting on and accounting off messages during a switchover and to send the interim accounting record first after a switchover. The ISG device also synchronizes the accounting counters for subscriber sessions on the standby processor every 30 minutes.

```
subscriber redundancy dynamic periodic-update interval 30
!
aaa accounting redundancy suppress system-records
aaa accounting redundancy best-effort-reuse send-interim
```

Examples: Verifying ISG Accounting and Postpaid Tariff Switching

This section contains examples of output for the “Verifying ISG Accounting and Postpaid Tariff Switching” task.

show subscriber session Output When ISG Accounting Is Applied to a Flow

In the following example, Intelligent Services Gateway (ISG) accounting is configured in a service profile that specifies a traffic class, which means that accounting will be performed on the flow and not the parent session. In this example, 157 is the unique ID of the traffic class.

```
Device# show subscriber session uid 157 detailed

Subscriber session handle: E5000092, state: connected, service: Ltm Internal
Unique Session ID: 157
Identifier:
SIP subscriber access type(s): Traffic-Class
Root SIP Handle: 2B000011, PID: 76
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 3 minutes, 45 seconds, Last Changed: 3 minutes, 45 seconds
AAA unique ID: 0
Switch handle: F300015F
Session inbound features:
Feature: Service accounting
 Service: video1
 Method List: remote-local
 Outbound direction:
 Packets = 84, Bytes = 33600


Feature: Policing
 Upstream Params:
Average rate = 8000, Normal burst = 1500, Excess burst = 3000
Config level = Service
Session outbound features:
Feature: Service accounting
 Service: video1
 Method List: remote-local
 Outbound direction:
        Packets = 84, Bytes = 33600
Feature: Policing
 Dnstream Params:
Average rate = 64000, Normal burst = 12000, Excess burst = 24000
Config level = Service
Configuration sources associated with this session:
Service: video1, Active Time = 3 minutes, 46 seconds
```

show subscriber session Output When ISG Accounting Is Applied to a Session

The following is sample output from the **show subscriber session** command for a session rather than a flow:

```
Device# show subscriber session uid 730 detailed

Subscriber session handle: 3800009A, state: connected, service: Local Term
Unique Session ID: 730
Identifier: igq2acct
SIP subscriber access type(s): IP-Interface/Account-Logon-CH
Root SIP Handle: A600000E, PID: 75
Child SIP Handle: F9000018, PID: 73
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 3 minutes, 57 seconds, Last Changed: 2 minutes, 59 seconds
AAA unique ID: 81
Switch handle: 890003A0
Interface: ATM6/0.1
Policy information:
  Authentication status: authen
  Config downloaded for session policy:
```

```
  From Access-Type: Account-Logon-CH, Client: SM, Event: Got More Keys
    Profile name: apply-config-only, 2 references
      ssg-account-info     "SAfoo"
  Rules, actions and conditions executed:
    subscriber rule-map rule1
      condition always event any-event
        action 1 authenticate
Session inbound features:
Feature: Session accounting
 Method List: foo
 Outbound direction:
        Packets = 10, Bytes = 1000
Session outbound features:
Feature: Session accounting
 Method List: foo
 Outbound direction:
        Packets = 10, Bytes = 1000
Configuration sources associated with this session:
Interface: ATM6/0.1, Active Time = 3 minutes, 58 seconds
```

The following is sample output from the **show aaa sessions** command:

```
Device# show aaa sessions

Total sessions since last reload: 141
Session Id: 167
   Unique Id: 151
   User Name: *not available*
   IP Address: 192.168.0.1
   Idle Time: 0
   CT Call Handle: 0
```

Output for a Specific User

The following is sample output from the **show aaa user** command:

```
Device# show aaa user

Unique id 151 is currently in use.
Accounting:
  log=0x20C201
  Events recorded :
    CALL START
    NET UP
    IPCP_PASS
    INTERIM START
    VPDN NET UP
  update method(s) :
    PERIODIC
  update interval = 60
Outstanding Stop Records : 0


1A1CABE8 0 00000001 connect-progress(68) 4 Call Up
    1A1CABF8 0 00000001 pre-session-time(294) 4 0(0)
    1A1CAC08 0 00000001 nas-tx-speed(421) 4 423630024(194014C8)
    1A1CAC18 0 00000001 nas-rx-speed(71) 4 139317740(84DD1EC)
    1A1CAC28 0 00000001 elapsed_time(364) 4 46122(B42A)
    1A1CAC50 0 00000001 bytes_in(135) 4 11434660(AE7AA4)
    1A1CAC60 0 00000001 bytes_out(274) 4 0(0)
    1A1CAC70 0 00000001 pre-bytes-in(290) 4 0(0)
    1A1CAC80 0 00000001 pre-bytes-out(291) 4 0(0)
    1A1CAC90 0 00000001 paks_in(136) 4 92215(16837)
```

```
    1A1CADF0 0 00000001 paks_out(275) 4 0(0)
    1A1CAE00 0 00000001 pre-paks-in(292) 4 0(0)
    1A1CAE10 0 00000001 pre-paks-out(293) 4 0(0)
  No data for type EXEC
  No data for type CONN
  NET: Username=(n/a)
    Session Id=000000A7 Unique Id=00000097
    Start Sent=1 Stop Only=N
    stop_has_been_sent=N
    Method List=189F046C : Name = CAR_mlist
    Attribute list:
      1A1CADF0 0 00000001 session-id(361) 4 167(A7)
1A1CAE00 0 00000001 protocol(297) 4 ip
      1A1CAE10 0 00000001 addr(8) 4 192.168.0.1
      1A1CAE20 0 00000001 Framed-Protocol(101) 4 PPP
      1A1CAE30 0 00000009 clid-mac-addr(37) 6 00 00 04 00 00 2A
--------
  No data for type CMD
  No data for type SYSTEM
  No data for type RM CALL
  No data for type RM VPDN
  No data for type AUTH PROXY
  No data for type 8
  No data for type CALL
  No data for type VPDN-TUNNEL
  No data for type VPDN-TUNNEL-LINK
  No data for type 12
  No data for type IPSEC-TUNNEL
  No data for type RESOURCE
  No data for type 15
Debg: No data available
Radi: No data available
Interface:
  TTY Num = -1
  Stop Received = 0
  Byte/Packet Counts till Call Start:
Start Bytes In = 0             Start Bytes Out = 0
    Start Paks  In = 0             Start Paks  Out = 0
  Byte/Packet Counts till Service Up:
    Pre Bytes In = 0             Pre Bytes Out = 0
    Pre Paks  In = 0             Pre Paks  Out = 0
  Cumulative Byte/Packet Counts :
    Bytes In = 11434660      Bytes Out = 0
    Paks  In = 92215         Paks  Out = 0
  StartTime = 12:02:40 IST Oct 16 2007
  AuthenTime = 12:02:40 IST Oct 16 2007
  Component = IEDGE_ACCOUNTING
Authen: service=NONE type=NONE method=RADIUS
Kerb: No data available
Meth: No data available
Preauth: No Preauth data.
General:
  Unique Id = 00000097
  Session Id = 000000A7
  Attribute List:
    1A1CADF0 0 00000001 port-type(198) 4 PPPoE over VLAN
    1A1CAE00 0 00000009 interface(194) 7 4/0/0/2
PerU: No data available
```

Output for All Users

```
Device# show aaa user all
```

```
-------------------------------------------------
Unique id 151 is currently in use.
Accounting:
  log=0x20C201
  Events recorded :
    CALL START
    NET UP
    IPCP_PASS
    INTERIM START
    VPDN NET UP
  update method(s) :
    PERIODIC
  update interval = 60
Outstanding Stop Records : 0
  Dynamic attribute list:
    1A1CABE8 0 00000001 connect-progress(68) 4 Call Up
    1A1CABF8 0 00000001 pre-session-time(294) 4 0(0)
    1A1CAC08 0 00000001 nas-tx-speed(421) 4 423630024(194014C8)
    1A1CAC18 0 00000001 nas-rx-speed(71) 4 139317740(84DD1EC)
    1A1CAC28 0 00000001 elapsed_time(364) 4 46122(B42A)
    1A1CAC50 0 00000001 bytes_in(135) 4 11434660(AE7AA4)
    1A1CAC60 0 00000001 bytes_out(274) 4 0(0)
    1A1CAC70 0 00000001 pre-bytes-in(290) 4 0(0)
    1A1CAC80 0 00000001 pre-bytes-out(291) 4 0(0)
    1A1CAC90 0 00000001 paks_in(136) 4 92215(16837)
    1A1CADF0 0 00000001 paks_out(275) 4 0(0)
    1A1CAE00 0 00000001 pre-paks-in(292) 4 0(0)
    1A1CAE10 0 00000001 pre-paks-out(293) 4 0(0)
  No data for type EXEC
  No data for type CONN
  NET: Username=(n/a)
    Session Id=000000A7 Unique Id=00000097
    Start Sent=1 Stop Only=N
    stop_has_been_sent=N
    Method List=189F046C : Name = CAR_mlist
    Attribute list:
      1A1CADF0 0 00000001 session-id(361) 4 167(A7)
1A1CAE00 0 00000001 protocol(297) 4 ip
      1A1CAE10 0 00000001 addr(8) 4 192.168.0.1
      1A1CAE20 0 00000001 Framed-Protocol(101) 4 PPP
      1A1CAE30 0 00000009 clid-mac-addr(37) 6 00 00 04 00 00 2A
--------
  No data for type CMD
  No data for type SYSTEM
  No data for type RM CALL
  No data for type RM VPDN
  No data for type AUTH PROXY
  No data for type 8
  No data for type CALL
  No data for type VPDN-TUNNEL
  No data for type VPDN-TUNNEL-LINK
  No data for type 12
  No data for type IPSEC-TUNNEL
  No data for type RESOURCE
  No data for type 15
Debg: No data available
Radi: No data available
Interface:
  TTY Num = -1
  Stop Received = 0
  Byte/Packet Counts till Call Start:
Start Bytes In = 0             Start Bytes Out = 0
    Start Paks  In = 0             Start Paks  Out = 0
  Byte/Packet Counts till Service Up:
```

```
    Pre Bytes In = 0             Pre Bytes Out = 0
    Pre Paks  In = 0             Pre Paks  Out = 0
  Cumulative Byte/Packet Counts :
    Bytes In = 11434660      Bytes Out = 0
    Paks  In = 92215         Paks  Out = 0
  StartTime = 12:02:40 IST Oct 16 2007
  AuthenTime = 12:02:40 IST Oct 16 2007
  Component = IEDGE_ACCOUNTING
Authen: service=NONE type=NONE method=RADIUS
Kerb: No data available
Meth: No data available
Preauth: No Preauth data.
General:
  Unique Id = 00000097
  Session Id = 000000A7
  Attribute List:
    1A1CADF0 0 00000001 port-type(198) 4 PPPoE over VLAN
    1A1CAE00 0 00000009 interface(194) 7 4/0/0/2
PerU: No data available
```

Example: Troubleshooting ISG Accounting

The following is sample output from the **debug aaa accounting** command:

```
Device# debug aaa accounting

16:49:21: AAA/ACCT: EXEC acct start, line 10
16:49:32: AAA/ACCT: Connect start, line 10, glare
16:49:47: AAA/ACCT: Connection acct stop:
task_id=70 service=exec port=10 protocol=telnet address=209.165.201.1 cmd=glare bytes_in=308
 bytes_out=76 paks_in=45
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
AAA configuration tasks	*Authentication, Authorization, and Accounting Configuration Guide*
AAA commands	*Cisco IOS Security Command Reference: Commands A to C*
Configuring ISG subscriber services	"Configuring ISG Subscriber Services" section in the *Intelligent Services Gateway Configuration Guide*
HA commands	Cisco IOS High Availability Command Reference
HA configuration	*Cisco IOS XE High Availability Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Accounting

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for ISG Accounting

Feature Name	Releases	Feature Information
1 second accuracy—IPv6 session counters and ISGv6 services	Cisco IOS XE Release 3.5S	Support for PPP IPv6 and dual-stack sessions was added to the Subscriber Accounting Accuracy feature.
ISG Accounting—Postpaid	Cisco IOS XE Release 2.2	ISG accounting provides the means to bill for account or service usage. ISG sends accounting start and accounting stop records for sessions and services to an accounting server for postpaid billing. The accounting server interprets the records to generate bills.
ISG Accounting—per-Service Accounting	Cisco IOS XE Release 2.4	ISG accounting provides the means to bill for account or service usage. ISG accounting uses the RADIUS protocol to facilitate interaction between ISG and an external RADIUS-based AAA or mediation server.
ISG Accounting—Tariff Switching	Cisco IOS XE Release 2.2	ISG accounting provides the means to bill for account or service usage. Where billing rates change at fixed times and sessions are active across the boundary at which the rates change, ISG will provide accounting data to the billing server indicating the boundary.
ISG Flow Control—SSO/ISSU	Cisco IOS XE Release 3.5S	HA support was added for ISG features including ISG accounting.