Configuring ISG Subscriber Services

Intelligent Services Gateway (ISG) is a software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. ISG defines a *service* as a collection of policies that can be applied to any subscriber session. This module describes how ISG subscriber services work, how to configure services and traffic classes that may be used to qualify policies defined within a service, and how to activate services.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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.

Restrictions for ISG Subscriber Services

- Only one nondefault traffic class can be configured in each service.
- When multiple services are active on a given session, class-based actions are executed on a first-match basis only; in other words, once a class is matched, the actions associated with that class will be executed, and no other class will be matched.
- Removing or modifying a feature in the configuration, for example an access control list (ACL), is not supported by active sessions that reference that feature.

- If the input ACL or output ACL that is configured in a traffic class map is not defined, or if the protocol of these ACLs is not the same (IPv4 versus IPv6), the traffic class installation fails and the service is not applied. If this failure occurs at session start, the session is not established. IPv4 ACLs are defined with the **ip access-list** command; IPv6 ACLs are defined with the **ipv6 access-list** command.
- ISG supports only single-stack traffic classes; a particular traffic class can classify either IPv4 or IPv6 traffic but not both.
- If any new service needs to be defined when the sessions are active, follow the order to update the configuration:
  1. ACL definition
  2. Class-map definition
  3. Policy-map service definition
  4. Service name in Policy rule or update dynamically through CoA.

Information About ISG Subscriber Services

ISG Services

An ISG service is a collection of policies that may be applied to a subscriber session. ISG services can be applied to any session, regardless of subscriber access media or protocol, and a single service may be applied to multiple sessions. An ISG service is not necessarily associated with a destination zone or a particular uplink interface.

Services can be defined in two ways: in a service policy map that is configured on the ISG device by using the CLI, and in a service profile that is configured on an external device, such as an authentication, authorization, and accounting (AAA) server. Although they are configured differently, service policy maps and service profiles serve the same purpose: they contain a collection of traffic policies and other functionality that can be applied to a subscriber session. 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.

Primary Services

When a network-forwarding policy is included in a service profile or service policy map, the service is known as a *primary service* . Primary services are mutually exclusive and may not be simultaneously active. Upon activation of a new primary service, ISG will deactivate the existing primary service and any other services dependent on the existing primary service through association with a service group.

If a primary service is deactivated, sessions may be left without a network-forwarding policy, that is, with no means to route or forward packets. A policy may be applied to defend against this condition such that a specific service is activated upon deactivation of all others (or all other primary services). This backup service would return network-forwarding policy to the session and allow the subscriber to reach a web portal. However, it should be noted that an IP session will not be automatically terminated when all services are deactivated unless such a policy has been defined and applied.

Traffic Classes and Traffic Class Priority

ISG traffic classes provide differentiated behavior for different traffic streams to and from a particular subscriber. Each traffic stream is represented by a classification and a set of applied features. A traffic class, also known as a flow, is a kind of service.

For traffic to be classified into streams, you must specify an access control list (ACL) that classifies the traffic and the direction of the traffic to which the ACL applies (inbound or outbound). Optionally, the priority of the traffic class can also be specified. Traffic that meets the specifications of a traffic class is said to *match* the traffic class. Once a match is made, features defined in the traffic policy are executed for that traffic class.

The priority of a traffic class determines which class is used first for a specified match if more than one traffic policy has been activated for a single session. In other words, if a packet matches more than one traffic class, it is classified to the class with the higher priority.

Packets that do not match any of the ACLs are considered part of the default traffic class and are processed as if a traffic policy was not applied to the session. A default class exists for every service. The default action of the default class is to pass traffic, or the default class can be configured to drop traffic. Default traffic is accounted for in the main session accounting. A service can contain one traffic class and one default class.

ISG traffic classes are created dynamically, either at session start or later during the life of the session, when a service with a classification (the class definition of the service contains at least one named or numbered ACL) is applied to a session. A service with a classification is called a flow service. A service without a classification is called a classless service.

Traffic classes are assigned unique identifiers that can be tracked with Cisco IOS **show** commands.

Flow Classifiers

In Cisco IOS XE Release 3.3S and later releases, separate sessions are no longer created for each traffic class; the traffic class is handled as a flow within the parent subscriber session.

A flow, or traffic class, represents a subset of subscriber traffic identified by a pair of class identifiers. Each class identifier, or classifier, represents a single class or a directional flow. Traffic can have a classifier in either or both directions. If there is no classifier in a particular direction, traffic in that direction is not subjected to the flow.

The ISG classifier is responsible for managing and enforcing classifiers and the corresponding policies associated with ISG subscriber sessions, also called targets. Each ISG subscriber session can have one or more classifiers associated with it. The different classifiers that can be associated with a subscriber session are:

- Match-Always Classifier—Identifies the entire traffic of a target in a particular direction. A target may have only one match-always classifier in each direction.
- Flow Classifier—Identifies a subset of traffic of a target in a particular direction. A target may have any number of flow classifiers in each direction.
- Default Classifier—Identifies the traffic of a target that does not match any of the flow classifiers in a particular direction. A target may have only one default classifier in each direction.

A set of features represent a policy attached to a classifier. Two classifiers on a target may have the same policy or different policies attached to it. ISG, however, considers the policy of each classifier to be independent of the other classifiers on a target.

The priority defines the order in which a packet should be subjected to classifiers when multiple classifiers are associated with a target. If no priority is defined, the default priority is assumed, which is a lower priority than any of the defined priorities in other classes but higher than the default class.

Traffic Policies

Traffic policies define the handling of data packets. A traffic policy contains a traffic class and one or more features. Whereas you can specify the event that will trigger an ISG control policy, the trigger for a traffic policy is implicit--the arrival of a data packet.

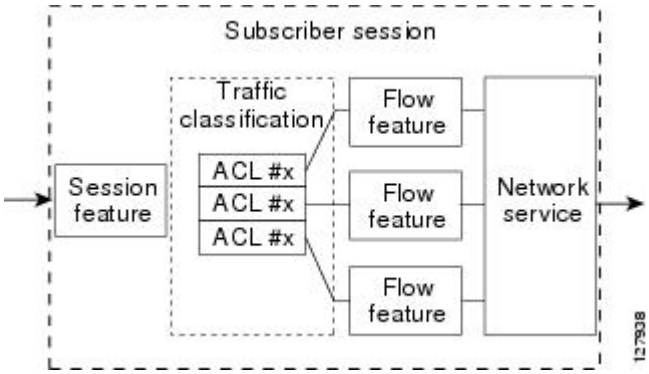
The features configured within a traffic policy apply only to the traffic defined by the traffic class. Multiple traffic policies with various features can be applied to a session.

ISG Features

An ISG feature is a functional component that performs a specific operation on a session's data stream. A feature may or may not be associated with a traffic class. However, once associated with a traffic class, a feature can be applied only to the packets that match that traffic class. Otherwise, the feature is applied to all packets for that session.

The figure below shows how features apply to a subscriber session and to traffic flows within the session.

Figure 1: ISG Feature Application on a Session and Flows



Note Two or more services that specify the same feature and apply to the entire session rather than to a specified traffic flow should not be activated for a session simultaneously. If two or more of these services are activated for a session, deactivation of one of the services will remove the feature from the session. If you need to offer to a subscriber multiple services that specify the same feature and apply to the session rather than a specific flow, configure the services so that they are mutually exclusive. That is, the subscriber should not be able to activate more than one such service at the same time. Similarly, control policies should not activate more than one such service at the same time.

Service Groups

A *service group* is a grouping of services that may be simultaneously active 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, may 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.

Service Activation Methods

There are three methods by which services can be activated:

- Automatic service activation
- Control policy service activation
- Subscriber-initiated service activation

Automatic Service Activation

The Auto Service attribute, which can be configured in user profiles, enables subscribers to be automatically logged in to specified services when the user profile is downloaded, usually following authentication. Features that are specified by the Auto Service attribute in a user profile are referred to as *auto services* . A user profile can specify more than one service as auto services.

Control Policy Service Activation

ISG control policies can be configured to activate services in response to specific conditions and events.

Subscriber-Initiated Service Activation

Subscriber-initiated service activation takes place when a subscriber manually selects a service at a portal.

When the system receives a subscriber request to activate a service, the ISG policy engine searches for a policy matching the event “service-start”. If no such policy is found, the policy engine will by default download the service via the default AAA network authorization method list. This default behavior is identical to the behavior generated by the following policy configuration:

```
class-map type control match-all SERVICE1_CHECK
   match service-name SERVICE1
policy-map type control SERVICE1_CHECK event service-start
   1 service-policy type service name SERVICE1
```

The same default behavior applies to subscriber logoffs, with the ISG policy engine searching for a policy that matches the event “service-stop”.

If a policy is configured, it is the responsibility of the policy to specify how the service should be applied.

How to Configure ISG Services on the Router

There are two ways to configure an ISG service. One way is to configure a service policy map on the local device by using the CLI. The second way is to configure a service profile on a remote AAA server. To configure a service policy map directly on the ISG, perform the tasks in the following sections:

Configuring an ISG Service with Per-Session Functionality

Certain types of functionality that are configured in a service must be applied to the entire subscriber session rather than to a specific traffic flow. Services that are configured with this type of per-session functionality must not contain a traffic class. Perform this task to configure a service policy map without a traffic class on the ISG.

Note Some of the commands that can be configured in a service policy map require other configuration in order to work properly. Details on how to configure specific ISG features and functionality are provided in other modules.

Note A service that is configured with per-session functionality and a traffic policy will not work correctly.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **authenticate aaa list** *name-of-list*
5. **classname** *dhcp-pool-name*
6. **ip portbundle**
7. **ip unnumbered** *interface-type interface-number*
8. **ip vrf forwarding** *name-of-vrf*
9. **service deny**
10. **service relay pppoe vpdn group** *VPDN-group-name*
11. **service vpdn group** *VPDN-group-name*
12. **sg-service-group** *service-group-name*
13. **sg-service-type** {**primary** | **secondary**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service.
Step 4	**authenticate aaa list** *name-of-list* **Example:** `Router(config-service-policymap)# authenticate aaa list mlist`	Indicates that the service requires authentication as a condition of activation and initiates an authentication request.
Step 5	**classname** *dhcp-pool-name* **Example:** `Router(config-service-policymap)# classname green`	Associates a Dynamic Host Configuration Protocol (DHCP) address pool with a service or specific subscriber.
Step 6	**ip portbundle** **Example:** `Router(config-service-policymap)# ip portbundle`	Enables the ISG Port-Bundle Host Key feature in the service policy map.
Step 7	**ip unnumbered** *interface-type interface-number* **Example:** `Router(config-service-policymap)# ip unnumbered ethernet 0`	Enables IP processing on an interface without assigning an explicit IP address to the interface.
Step 8	**ip vrf forwarding** *name-of-vrf* **Example:** `Router(config-service-policymap)# ip vrf forwarding blue`	Associates the service with a VRF. • Configuring this command will make the service a primary service.
Step 9	**service deny** **Example:** `Router(config-service-policymap)# service deny`	Denies network service to the subscriber session.
Step 10	**service relay pppoe vpdn group** *VPDN-group-name* **Example:** `Router(config-service-policymap)# service relay pppoe vpdn group group1`	Enables relay of PPPoE Active Discovery (PAD) messages over a Layer 2 Tunnel Protocol (L2TP) tunnel for a subscriber session.
Step 11	**service vpdn group** *VPDN-group-name* **Example:**	Provides virtual private dialup network (VPDN) service for ISG subscriber sessions. • Configuring this command will make the service a primary service.

	Command or Action	Purpose
	`Router(config-service-policymap)# service vpdn group vpdn1`	
Step 12	**sg-service-group** *service-group-name* **Example:** `Router(config-service-policymap)# sg-service-group group1`	Associates the service with a specified service group.
Step 13	**sg-service-type** {**primary** | **secondary**} **Example:** `Router(config-service-policymap)# sg-service-type primary`	Defines the service as a primary or secondary service. • A primary service is a service that contains a network-forwarding policy. A service must be defined as a primary service by using the **sg-service-type primary** command. Any service that is not a primary service is defined as a secondary service by default.

Configuring an ISG Service with a Traffic Policy

An ISG traffic policy contains a traffic class and one or more ISG features. The traffic class defines the traffic to which the features will be applied. Perform the following tasks to configure an ISG service with a traffic policy on the router:

Defining an ISG Traffic Class Map

Perform this task to configure a traffic class map. A traffic class map usually specifies an access control list (ACL) that classifies the flow and the direction of traffic to which the ACL applies (inbound or outbound).

Note You can also configure an empty traffic class map, that is, a traffic class map that does not specify an access list, in order to configure a service with a traffic policy that applies to all session traffic.

Before you begin

This task assumes that access control lists (ACLs) have been configured for classifying traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type traffic match-any** *class-map-name*
4. **match access-group input** {*access-list-number* | **name** *access-list-name*}
5. **match access-group output** {*access-list-number* | **name** *access-list-name*}
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map type traffic match-any** *class-map-name* **Example:** `Router(config)# class-map type traffic match-any class1`	Creates or modifies a traffic class map, which is used for matching packets to a specified ISG traffic class.
Step 4	**match access-group input** {*access-list-number* | **name** *access-list-name*} **Example:** `Router(config-traffic-classmap)# match access-group input 101`	(Optional) Configures the match criteria for an input class map on the basis of the specified ACL. • Skip this step if you want to define a traffic policy that applies to all session traffic rather than to a specific traffic flow.
Step 5	**match access-group output** {*access-list-number* | **name** *access-list-name*} **Example:** `Router(config-traffic-classmap)# match access-group output 102`	(Optional) Configures the match criteria for an output class map on the basis of the specified ACL. • Skip this step if you want to define a traffic policy that applies to all session traffic rather than to a specific traffic flow.
Step 6	**exit** **Example:** `Router(config-traffic-classmap)# exit`	Returns to global configuration mode.

Configuring an ISG Service Policy Map with a Traffic Policy

ISG services are configured by creating service policy maps on the ISG or service profiles on an external AAA server. Perform this task to configure a traffic policy in a service policy map on the ISG.

Note Some of the commands that can be configured in a service policy map require other configuration in order to work properly. Details on how to configure specific ISG features and functionality are provided in other modules in the *Cisco IOS Intelligent Services Gateway Configuration Guide*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*] **class type traffic** *class-map-name*
5. **accounting aaa list** *AAA-method-list*
6. **police** {**input** | **output**} *committed-rate normal-burst excess-burst*
7. **prepaid config** *name-of-configuration*
8. **redirect** [**list** *access-list-number*] **to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]} [**duration** *seconds*] [**frequency** *seconds*]
9. **timeout absolute** *duration-in-seconds*
10. **timeout idle** *duration-in-seconds*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service.
Step 4	[*priority*] **class type traffic** *class-map-name* **Example:** `Router(config-service-policymap)# class type traffic classb`	Associates a traffic class map with the service policy map. • The *priority* argument determines which traffic class will be used first for a specified match. When a packet matches more than one traffic class, it is classified to the class with the higher priority.
Step 5	**accounting aaa list** *AAA-method-list* **Example:** `Router(config-service-policymap-class-traffic)# accounting aaa list mlist1`	Enables accounting and specifies the AAA method list to which accounting updates will be sent.
Step 6	**police** {**input**	**output**} *committed-rate normal-burst excess-burst* **Example:**	Enables ISG policing for upstream or downstream traffic. • This command can be entered twice to configure upstream and downstream policing.

	Command or Action	Purpose
	`Router(config-service-policymap-class-traffic)# police input 20000 30000 60000`	
Step 7	**prepaid config** *name-of-configuration* **Example:** `Router(config-service-policymap-class-traffic)# prepaid config conf-prepaid`	Enables ISG support for prepaid billing and applies a configuration that defines the prepaid billing parameters.
Step 8	**redirect** [**list** *access-list-number*] **to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]} [**duration** *seconds*] [**frequency** *seconds*] **Example:** `Router(config-service-policymap-class-traffic)# redirect to ip 10.10.10.10`	Redirects traffic to a specified server or server group.
Step 9	**timeout absolute** *duration-in-seconds* **Example:** `Router(config-control-policymap-class-traffic)# timeout absolute 30`	Specifies the session lifetime, in a range from 30 to 4294967 seconds.
Step 10	**timeout idle** *duration-in-seconds* **Example:** `Router(config-control-policymap-class-traffic)# timeout idle 3000`	Specifies how long a connection can be idle before it is terminated. The range is platform and release-specific. For more information, use the question mark (?) online help function.
Step 11	**end** **Example:** `Router(config-service-policymap-class-traffic)#end`	(Optional) Returns to privileged EXEC mode.

Configuring the Default Class in an ISG Service Policy Map

Packets that do not match any traffic classes are considered to be part of default traffic and are processed as if a traffic policy were not applied to the session. A default class exists by default for every service, and the default action of the default class is to pass traffic. Perform this task to configure the default class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **class type traffic default** {**in-out** | **input** | **output**}
5. **drop**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service.
Step 4	**class type traffic default** {**in-out** | **input** | **output**} **Example:** `Router(config-service-policymap)# class type traffic default in-out`	Associates a default traffic class with a service policy map. • The default class is the class to which traffic is directed if that traffic does not match any of the match criteria in the configured class maps.
Step 5	**drop** **Example:** `Router(config-service-policymap-class-traffic)# drop`	Configures the default traffic class to discard packets matching that class.

Activating ISG Subscriber Services

There are three ways that ISG subscriber services can be activated: by specifying the service as an automatic activation service in a subscriber's user profile, by configuring control policies to activate the service, and by a subscriber-initiated service logon. No special configuration is necessary to enable a subscriber to log on to a service.

To configure a service for automatic activation and to configure control policies to activate services, perform the following tasks:

Configuring Automatic Service Activation in a User Profile

Perform this task to configure automatic service activation for a service in a subscriber's user profile.

SUMMARY STEPS

1. Add the Auto Service attribute to the user profile.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Add the Auto Service attribute to the user profile. **Example:** `26,9,251="A service-name[; username ; password]"`	Automatically logs the subscriber in to the specified service when the user profile is downloaded.

Configuring ISG Control Policies to Activate Services

Perform this task to configure a control policy to activate a service.

Before you begin

A control class map must be configured if you specify a named control class map in the control policy map. See the module "Configuring ISG Control Policies" for information about configuring control policies.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {**always** | *map-class-name*} [**event account-logon** | **credit-exhausted** | **quota-depleted** | **service-start** | **service-stop** | **session-default-service** | **session-service-found**| **session-start** | **timed-policy-expiry**]
5. *action-number* **service-policy type service** {**name** | **unapply**} *policy-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control policy1`	Creates or modifies a policy map to specify an ISG control policy.

	Command or Action	Purpose
Step 4	**class type control** {**always** | *map-class-name*} [**event account-logon** | **credit-exhausted** | **quota-depleted** | **service-start** | **service-stop** | **session-default-service** | **session-service-found**| **session-start** | **timed-policy-expiry**] **Example:** `Router(config-control-policymap)# class type control always event session-start`	Specifies a class and, optionally, an event for which actions may be configured.
Step 5	*action-number* **service-policy type service** {**name** | **unapply**} *policy-map-name* **Example:** `Router(config-control-policymap-class-control)# 1 service-policy type service service1`	Applies the specified service policy map. • To remove the service policy map, use the **unapply** keyword.

Verifying ISG Services

Perform this task to verify ISG service configuration.

SUMMARY STEPS

1. **enable**
2. **show class-map type traffic**
3. **show policy-map type service**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show class-map type traffic** **Example:** `Router# show class-map type traffic`	Displays all traffic class maps and their matching criteria.
Step 3	**show policy-map type service** **Example:** `Router# show policy-map type service`	Displays the contents of all service policy maps.

Configuration Examples for ISG Services

Example Service for Per-Flow Accounting

In the following examples, the service “SERVICE1” is configured with per-flow accounting. The access lists “SERVICE1_ACL_IN” and “SERVICE1_ACL_OUT” are used to define the traffic class. These examples are equivalent and show the two alternative methods of service configuration: in a service policy map that is configured directly on the ISG, and in a service profile that is configured on a AAA server.

ISG Configuration

```
class-map type traffic match-any SERVICE1_TC
 match access-group input name SERVICE1_ACL_IN
 match access-group output name SERVICE1_ACL_OUT
!
policy-map type service SERVICE1
 10 class type traffic SERVICE1_TC
  accounting aaa list CAR_ACCNT_LIST
 class type traffic default in-out
  drop
```

AAA Server Configuration

```
Attributes/
 Cisco-AVPair = "ip:traffic-class=in access-group name SERVICE1_ACL_IN priority 10"
 Cisco-AVPair = "ip:traffic-class=in default drop"
 Cisco-AVPair = "ip:traffic-class=out access-group name SERVICE1_ACL_OUT priority 10"
 Cisco-AVPair = "ip:traffic-class=out default drop"
 Cisco-AVPair = subscriber:accounting-list=CAR_ACCNT_LIST
 Cisco-SSG-Service-Info = ISERVICE1
```

Example Service for Absolute Timeout and Idle Timeout

In the following examples, the service “SERVICE1” is configured with per-flow accounting, an absolute timeout, and an idle timeout. The access lists “SERVICE1_ACL_IN” and “SERVICE1_ACL_OUT” are used to define the traffic class. These examples are equivalent and show the two methods of service configuration: in a service policy map that is configured directly on the ISG, and in a service profile that is configured on a AAA server.

ISG Configuration

```
class-map type traffic match-any SERVICE1_TC
 match access-group input name SERVICE1_ACL_IN
 match access-group output name SERVICE1_ACL_OUT
!
policy-map type service SERVICE1
 10 class type traffic SERVICE1_TC
  timeout idle 600
  timeout absolute 1800
  accounting aaa list CAR_ACCNT_LIST
 class type traffic default in-out
  drop
```

AAA Server Configuration

```
Attributes/
 Cisco-AVPair = "ip:traffic-class=in access-group name SERVICE1_ACL_IN priority 10"
 Cisco-AVPair = "ip:traffic-class=in default drop"
 Cisco-AVPair = "ip:traffic-class=out access-group name SERVICE1_ACL_OUT priority 10"
 Cisco-AVPair = "ip:traffic-class=out default drop"
 Cisco-AVPair = subscriber:accounting-list=CAR_ACCNT_LIST
 Cisco-SSG-Service-Info = ISERVICE1
  session-timeout = 1800
  idle-timeout = 600
```

Example Service for ISG Policing

In the following examples, the service “BOD1M” is configured with per-flow accounting and ISG policing. The access lists “BOD1M_IN_ACL_IN” and “BOD1M_ACL_OUT” are used to define the traffic class. These examples are equivalent and show the two methods of service configuration: in a service policy map that is configured directly on the ISG, and in a service profile that is configured on a AAA server.

ISG Configuration

```
class-map type traffic match-any BOD1M_TC
 match access-group input name BOD1M_IN_ACL_IN
 match access-group output name BOD1M_ACL_OUT
!
policy-map type service BOD1M
 10 class type traffic BOD1M_TC
  accounting aaa list CAR_ACCNT_LIST
  police input 512000 256000 5000
  police output 1024000 512000 5000
 class type traffic default in-out
  drop
```

AAA Server Configuration

```
Attributes/
 Cisco-AVPair = "ip:traffic-class=in access-group name BOD1M_IN_ACL priority 10"
 Cisco-AVPair = "ip:traffic-class=in default drop"
 Cisco-AVPair = "ip:traffic-class=out access-group name BOD1M _OUT_ACL priority 10"
 Cisco-AVPair = "ip:traffic-class=out default drop"
 Cisco-AVPair = subscriber:accounting-list=CAR_ACCNT_LIST
 Cisco-SSG-Service-Info = IBOD1M
 Cisco-SSG-Service-Info = QU;512000;256000;5000;D;1024000;512000;5000
```

Example Service for Per-Subscriber Firewall

In the following examples, the service “SERVICE2” is configured with a per-subscriber firewall. The service does not include a traffic class, so it will apply to the entire session. These examples are equivalent and show the two methods of service configuration: in a service policy map that is configured directly on the ISG, and in a service profile that is configured on a AAA server.

ISG Configuration

```
policy-map type service SERVICE2
```

```
 ip access-group INTERNET_IN_ACL in
 ip access-group INTERNET_OUT_ACL out
```

AAA Server Configuration

```
Attributes/
 Cisco-AVPair = ip:inacl=INTERNET_IN_ACL
 Cisco-AVPair = ip:outacl=INTERNET_OUT_ACL
```

Example Service for Redirecting Layer 4 Subscriber Traffic

The following example shows the configuration of a service called “UNAUTHORIZED_REDIRECT_SVC”. The control policy “UNAUTHEN_REDIRECT” is configured to apply the service upon session start.

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

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

policy-map type control UNAUTHEN_REDIRECT
 class type control always event session-start
  1 service-policy type service name UNAUTHORIZED_REDIRECT_SVC
```

Example Deactivating a Layer 4 Redirection Service Following Authorization

In the following example, a service configured with Layer 4 redirection is deactivated when traffic becomes authorized; that is, following activation of the appropriate service.

```
class-map traffic UNAUTHORIZED_TRAFFIC
match access-group input 100
policy-map type service UNAUTHORIZED_REDIRECT_SVC
 class traffic UNAUTHORIZED_TRAFFIC
  redirect to ip 10.0.0.148 port 8080
class-map control match-all CHECK_ISP1
 match service ISP1
policy-map control UNAUTHEN_REDIRECT
 class control always event session-start
  1 service-policy type service name UNAUTHORIZED_REDIRECT_SVC
 class control CHECK_ISP1 event service-start
  1 service-policy type service unapply UNAUTHORIZED_REDIRECT_SVC
  1 service-policy type service name ISP1
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference

Standards

Standard	Title
No new or modified standards are supported.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Subscriber Services

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 Subscriber Services

Feature Name	Releases	Feature Configuration Information
ISG: Policy Control: Service Profiles	Cisco IOS XE Release 2.2	ISG defines a service as a collection of policies that can be applied to any subscriber session. Services can be configured on the router or on an external AAA server.
ISG: Policy Control: User Profiles	Cisco IOS XE Release 2.2	ISG user profiles specify services and functionality that can be applied to ISG sessions for the specified subscriber. User profiles are defined on an external AAA server.
ISG: Flow Control: SSO/ISSU	Cisco IOS XE Release 3.3S	ISG no longer creates separate sessions for each traffic class; the traffic class is handled as a flow within the parent subscriber session. The following commands were introduced or modified: **debug subscriber classifier**, **debug subscriber feature**, **show subscriber service**, **show subscriber statistics**.