Configuring ISA Subscriber Services

The Intelligent Service Architecture (ISA) is a core set of Cisco IOS components that provides a structured framework in which access edge devices can deliver flexible and scalable services to subscribers. A Cisco device that is running a Cisco IOS image with ISA is called an Intelligent Service Gateway (ISG). ISA defines a *service* as a collection of policies that can be applied to any subscriber session. This module describes how ISA 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.

Module History

This module was first published on April 28, 2005, and last updated on April 28, 2005.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all features. To find information about feature support and configuration, use the "Feature Information for ISA Subscriber Services" section on page 104.

Contents

Restrictions for Configuring ISA Subscriber Services

Only one nondefault traffic class may 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.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Services defined locally cannot be selected externally because they will not be advertised to a portal.

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.

Information About ISA Subscriber Services

Before you configure ISA subscriber services, you should understand the following concepts:

- ISA Services, page 92
- Primary Services, page 92
- Traffic Classes, page 93
- Traffic Policies, page 93
- ISA Features, page 93
- Service Groups, page 94
- Service Activation Methods, page 94

ISA Services

An ISA service is a collection of policies that may be applied to a subscriber session. ISA 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 ISA service is not necessarily associated with a destination zone or a particular uplink interface.

Services are 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 by using the command-line interface (CLI), and the service profile is configured on an external device, such as a 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.

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, ISA 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 “back-up 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

ISA traffic classes allow subscriber session traffic to be subclassified so that ISA features can be applied to constituent flows. In order for traffic to be classified into flows, the following information must be specified:

- An access control list (ACL) that classifies the flow
- Direction of traffic to which the ACL applies (inbound or outbound)
- Priority of the traffic class

Traffic that meets the specifications of a traffic class is said to "match" the traffic class. The priority of a traffic class is used to determine which class will be used first for a specified match. In other words, if a packet matches more than one traffic class, it will be classified to the class with higher priority. Once a match is made, features defined in the traffic policy will be executed for that traffic class.

Packets that do not match any of the ACLs 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 for every service, and the default action of the default class is to pass traffic. The default class can be configured to drop traffic.

A service can contain one traffic class and one default class.

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

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 ISA 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.

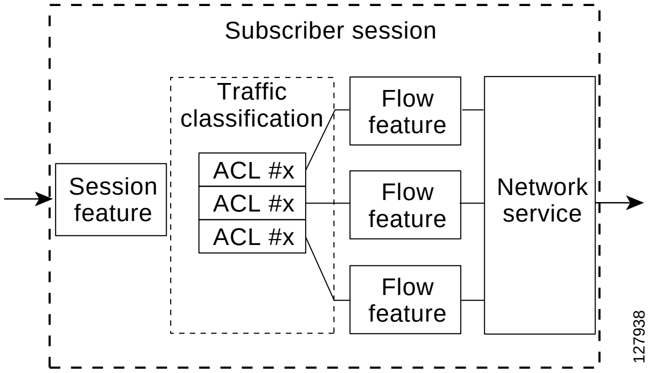
Traffic policies are only one component of service policy maps and service profiles. A service policy map can contain other information, in addition to a traffic policy, that applies to all the session traffic.

ISA Features

An ISA 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.

Figure 2 shows how features apply to a subscriber session and to flows within the session.

Figure 2 ISA 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

ISA 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 ISA 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:

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

The same default behavior applies to subscriber logoffs, with the ISA 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 ISA Services

There are two ways to configure an ISA 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 profile on the AAA server, see the document *RADIUS Attributes and Profiles for ISA* for a list of supported attributes.

To configure a service policy map directly on the ISG, perform the tasks in the following sections:

- Configuring ISA Services on the ISG, page 95
- Activating ISA Subscriber Services, page 100
- Verifying ISA Services, page 102

Configuring ISA Services on the ISG

To configure ISA services on the local device, perform the following tasks:

- Configuring an ISA Traffic Class Map, page 95
- Configuring an ISA Service Policy Map, page 97

Configuring an ISA Traffic Class Map

Perform this task to configure a traffic class map.

Prerequisites

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 ISA 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`
		Configures the match criteria for an input class map on the basis of the specified ACL.

Step 5	**match access-group output** {*access-list-number* | **name** *access-list-name*}
	Example:
	`Router(config-traffic-classmap)# match access-group output 102`
		Configures the match criteria for an output class map on the basis of the specified ACL.

Step 6	**exit** **Example:** `Router(config-traffic-classmap)# exit`	Returns to global configuration mode.

Configuring an ISA Service Policy Map

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

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 ISA features and functionality are provided in other modules in the *Cisco IOS Intelligent Service Architecture Configuration Guide*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **authenticate aaa list** *name-of-list*
4. **classname** *dhcp-pool-name*
5. **ip portbundle**
6. **ip unnumbered** *interface-type interface-number*
7. **ip vrf forwarding** *name-of-vrf*
8. **prepaid config** *name-of-configuratio*n
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**}
14. **class type traffic** *class-map-name*
15. **accounting aaa list** *AAA-method-list*
16. **police** {**input** | **output**} *committed-rate normal-burst excess-burst*
17. **redirect** [**list** *access-list-number*] **to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]} [**duration** *seconds*] [**frequency** *seconds*]
18. **timeout absolute** *duration-in-seconds*
19. **timeout idle** *duration-in-seconds*
20. **exit**
21. **class type traffic default**
22. **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 ISA 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 ISA 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	**prepaid config** *name-of-configuratio*n **Example:** `Router(config-service-policymap)# prepaid config conf-prepaid`	Enables ISA support for prepaid billing and applies a configuration that defines the prepaid billing parameters.

	Command or Action	Purpose
Step 10	**service deny** **Example:** `Router(config-service-policymap)# service deny`	Denies network service to the subscriber session.
Step 11	**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 12	**service vpdn group** *VPDN-group-name* **Example:** `Router(config-service-policymap)# service vpdn group vpdn1`	Provides virtual private dialup network (VPDN) service for ISA subscriber sessions. • Configuring this command will make the service a primary service.
Step 13	**sg-service-group** *service-group-name* **Example:** `Router(config-service-policymap)# sg-service-group group1`	Associates the service with a specified service group.

Step 14	**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.

Step 15	**class type traffic** *class-map-name*
	Example:
	`Router(config-service-policymap)# class type traffic classb`
		Specifies a named traffic class whose policy you want to create or change.

Step 16	**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 17	**police** {**input** | **output**} *committed-rate normal-burst excess-burst* **Example:** `Router(config-service-policymap-class-traffic)# police input 20000 30000 60000`	Enables ISA policing for upstream or downstream traffic. • This command can be entered twice to configure upstream and downstream policing.

	Command or Action	Purpose
Step 18	**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 19	**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 20	**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, in a range from 1 to 4294967 seconds.
Step 21	**exit** **Example:** `Router(config-service-policymap-class-traffic)# exit`	Returns to service policy map configuration mode.
Step 22	**class type traffic default** **Example:** `Router(config-service-policymap)# class type traffic default`	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 23	**drop** **Example:** `Router(config-service-policymap-class-traffic)# drop`	Configures the default traffic class to discard packets matching that class.

Activating ISA Subscriber Services

There are three ways that ISA subscriber services can be activated: by specifying the service as an auto 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 as an auto service and to configure control policies to activate services, perform the following tasks:

- Configuring Auto Services in a User Profile, page 101
- Configuring ISA Control Policies to Activate Services, page 101

Configuring Auto Services in a User Profile

Perform this task to configure an auto 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. 26,9,251="**A***service-name*[**;***username***;***password*]"	Automatically logs the subscriber in to the specified service when the user profile is downloaded.

Configuring ISA Control Policies to Activate Services

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

Prerequisites

A control class map must be configured if you specify a named control class map in the control policy map. See the module *Configuring ISA 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** [**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.

	Command or Action	Purpose
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 ISA control policy.

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** [**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 ISA Services

Perform this task to verify ISA 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`	Display 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 ISA Services

This section contains the following examples:

- Service for Redirecting Layer 4 Subscriber Traffic: Example, page 103
- Deactivating a Layer 4 Redirection Service Following Authorization: Example, page 103

Service for Redirecting Layer 4 Subscriber Traffic: Example

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.

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

class-map traffic UNAUTHORIZED_TRAFFIC
 match access-group input 100

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

Deactivating a Layer 4 Redirection Service Following Authorization: Example

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 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 service UNAUTHORIZED_REDIRECT_SVC
 class control CHECK_ISP1 event service-start
  1 service-policy service unapply UNAUTHORIZED_REDIRECT_SVC
  1 service-policy service ISP1
```

Additional References

The following sections provide references related to ISA subscriber services.

Related Documents

Related Topic	Document Title
ISA commands	*Cisco IOS Intelligent Service Architecture Command Reference*

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Feature Information for ISA Subscriber Services

Table 10 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(27)SB or later appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

If you are looking for information on a feature in this technology that is not documented here, see the “Intelligent Service Architecture Features Roadmap.”

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 10 Feature Information for ISA Subscriber Services

Feature Name	Releases	Feature Configuration Information
ISA:Policy Control: Service Profiles	12.2(27)SBA	ISA 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. The following sections provide information about this feature: • Information About ISA Subscriber Services, page 92 • How to Configure ISA Services, page 95

This module first published April 28, 2005. Last updated<April 28, 2005.