Configuring ISG Access for PPP Sessions

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. This document provides information about how to configure ISG access for Point-to-Point Protocol (PPP) subscribers.

- Finding Feature Information, on page 1
- Prerequisites for ISG Access for PPP Sessions, on page 1
- Restrictions for ISG Access for PPP Sessions, on page 2
- Information About ISG Access for PPP Sessions, on page 2
- How to Configure ISG Access for PPP Sessions Using Control Policies, on page 3
- Configuration Examples for ISG Access for PPP Sessions, on page 8
- Additional References, on page 11
- Feature Information for ISG Access for PPP Sessions, on page 11

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.

Prerequisites for ISG Access for PPP Sessions

The specific access protocol that is being used must be provisioned on the interface.

If local PPP authentication is required, the **ppp authentication** command must be configured on the interface or virtual template.

The tasks and examples in this document assume that you know how to configure and use ISG control policies. See the module “Configuring ISG Control Policies” for information about how to configure control policies.

Restrictions for ISG Access for PPP Sessions

The idle timeout value configured with the **ppp timeout idle** command in a virtual template applies to a PPP session even when the session is forwarded.

Information About ISG Access for PPP Sessions

Overview of ISG Access for PPP Sessions

Layer 2 sessions are established by means of control protocols that operate between the peer entities and the ISG device. Typically, Layer 2 sessions are encapsulated to isolate them from other sessions on the same physical media.

Although the system provides default handling for Layer 2 sessions, you may want to configure policies to forward or locally terminate the protocol or to locally authenticate subscribers on the basis of identity data that is collected from the access protocol. ISG control policies can be configured to extract identity and credentials of peer entities from access protocols. This mechanism allows services to be provisioned for Layer 2 sessions on the basis of any identity pertaining to the session, whether explicitly provided via the protocol or native to the underlying media or access port.

ISG supports the following Layer 2 access protocols:

- PPP
- PPP over Ethernet (PPPoE)
- Layer 2 Tunnel Protocol (L2TP)

ISG Subscriber IP Address Management for PPP Sessions

ISG subscriber IP address management applies to IP sessions or Layer 2 (PPP) sessions that are terminated locally.

For a subscriber to be routable within a given IP service domain, the subscriber must present a domain-specific IP address to the network. If a subscriber transfers between IP service domains (which includes any private domain managed by the access provider), the IP address presented to the network must change to reflect the new domain. For locally terminated PPP sessions, ISG supports the following methods of IP address assignment:

- IP address in a user profile
- IP subnet in a user profile
- Named address pool in a user profile
- Local address pools
- Standard methods of IP address management for PPP

When a locally terminated PPP session is transferred from one virtual routing and forwarding (VRF) instance to another VRF, the peer IP address is renegotiated using IPCP.

VRF Transfer for PPP Sessions

VRF transfer enables an ISG subscriber session to move from one VRF to another following selection of a new primary service. Once a PPP session comes up with the IP address from the network access point (NAP), the subscriber can access a web portal and choose a service provider. On VRF transfers in PPP sessions, ISG must reassign the IP address from the new domain to the PPP session. In PPP sessions, the IP address is reassigned by IP Control Protocol (IPCP) renegotiation.

Without PPP renegotiation, VRF transfer is not supported for PPP sessions.

Default Policy for ISG Access for PPP Sessions

ISG provides default handling of Layer 2 sessions in the absence of a configured control policy. If the **vpdn enable** command is configured and a domain name is specified in the username (for example, user@domain) or a Dialed Number Identification Service (DNIS) number has been provided, the system will perform authorization on the basis of this information. If virtual private dialup network (VPDN) tunnel information is found, the session will be forwarded for handling at an L2TP network server (LNS). If authentication is required by the remote LNS, the **ppp authentication** command must be configured at the PPP interface or virtual template. If the **vpdn authen-before-forward** command is configured, the system will attempt to authenticate the PPP session locally before forwarding it on to the LNS.

If tunnel information is not found for the domain name or DNIS or the **vpdn enable** command is not configured, Stack Group Bidding Protocol (SGBP) authorization will be attempted (if SGBP is configured). If no authorization information is located using SGBP, the PPP session will be terminated locally. Local termination means that the PPP session will be established between the peer and the ISG device, and the IP payload will be routed. In the latter case, authentication will occur only if the **ppp authentication** command is configured on the PPP interface or virtual template.

If an ISG control policy is defined for the session-start event, that policy will override the default handling.

How to Configure ISG Access for PPP Sessions Using Control Policies

To configure ISG Layer 2 access, perform the following steps:

1. Decide how you want Layer 2 session handling to be influenced by subscriber identity. Do you want to forward the protocol or terminate it locally? Do you want to authenticate subscribers locally?
2. Configure control policies to provide Layer 2 session handling. See the module "Configuring ISG Control Policies" for information about how to configure control policies. See the "Configuration Examples for ISG Access for PPP Sessions" section for an example of a control policy for Layer 2 access.
3. Enable ISG VRF transfer for PPP sessions.
4. Verify and troubleshoot the configuration as needed.

This section contains the following tasks:

Enabling ISG VRF Transfer for PPP Sessions

VRF transfer enables an ISG subscriber session to move from one VRF to another when a new primary service is activated for a session. Services can be configured in service profiles on an external authentication, authorization, and accounting (AAA) server or they can be configured on the ISG device in service policy maps. Perform this task to configure a VRF in a service policy map on the ISG device.

Before you begin

This procedure assumes that you have configured support for PPP sessions by configuring a virtual template and method of IP address allocation. Note that the original VRF, loopback interface, and IP address pool must be specified in a virtual template rather than in a user profile in order for VRF transfer to work. For information about how to configure virtual templates and support for PPP sessions, see the *Dial Technologies Configuration Guide.*

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **ip vrf forwarding** *name-of-vrf*
5. **sg-service-type primary**
6. **sg-service-group** *service-group-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 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, and enters service policy-map configuration mode.
Step 4	**ip vrf forwarding** *name-of-vrf* **Example:** `Router(config-service-policymap)# ip vrf forwarding blue`	Associates the service with a VRF.
Step 5	**sg-service-type primary**	Defines the service as a primary service.

	Command or Action	Purpose
	Example: `Router(config-service-policymap)# sg-service-type primary`	• A primary service is a service that contains a network-forwarding policy. A primary 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 6	**sg-service-group** *service-group-name* **Example:** `Router(config-service-policymap)# sg-service-group group1`	(Optional) Associates an ISG service with a service group. • A service group is a grouping of services that may be active simultaneously for a given session. Typically, a service group includes one primary service and one or more secondary services.

Verifying VRF Transfer for PPP Sessions

Perform this task to verify VRF transfer for PPP sessions. All of the **show** steps are optional and may be performed in any order.

SUMMARY STEPS

1. **enable**
2. **show subscriber session all**
3. **show idmgr** {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id*| **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string*} | **statistics**}
4. **show ip route** [**vrf** *vrf-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show subscriber session all** **Example:** `Router# show subscriber session all`	Displays information pertaining to the service chosen by the subscriber.
Step 3	**show idmgr** {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address*	Displays information related to ISG session and service identity.

	Command or Action	Purpose
	vrf-id *vrf-id*| **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string*} | **statistics**} **Example:** `Router# show idmgr session key session-handle 48000002`	
Step 4	**show ip route** [**vrf** *vrf-name*] **Example:** `Router# show ip route`	Displays the current state of the routing table.

Troubleshooting ISG Access for PPP Sessions

The commands in this task can be used to monitor and troubleshoot Layer 2 sessions. All of these commands are optional and do not need to be entered in a particular order.

SUMMARY STEPS

1. **enable**
2. **show subscriber session detailed**
3. **debug condition** *condition*
4. **debug subscriber packet** [**event**| **full**| **detail**]
5. **debug subscriber error**
6. **debug subscriber event**
7. **debug subscriber fsm**
8. **debug ppp** {**packet** | **negotiation** | **error** | **authentication** | **subscriber switch**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show subscriber session detailed** **Example:** `Router# show subscriber session detailed`	Displays information about ISG subscriber sessions.
Step 3	**debug condition** *condition* **Example:**	Filters debug output on the basis of the specified condition.

	Command or Action	Purpose
	`Router# debug condition username user5@isp.com`	**Note** See the module "Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging" for information about conditional debugging.
Step 4	**debug subscriber packet** [**event**| **full**| **detail**] **Example:** `Router# debug subscriber packet event`	Displays diagnostic information about packets during Subscriber Service Switch (SSS) call setup.
Step 5	**debug subscriber error** **Example:** `Router# debug subscriber error`	Displays diagnostic information about errors that can occur during SSS call setup.
Step 6	**debug subscriber event** **Example:** `Router# debug subscriber event`	Displays diagnostic information about SSS call setup events.
Step 7	**debug subscriber fsm** **Example:** `Router# debug subscriber fsm`	Displays diagnostic information about the SSS call setup state.
Step 8	**debug ppp** {**packet** | **negotiation** | **error** | **authentication** | **subscriber switch**} **Example:** `Router# debug ppp packet`	Displays information on traffic and exchanges in an internetwork that is implementing the PPP.

Example

In the following example, the output of the **debug subscriber packet detail** command is filtered on the basis of the username “cpe6_1@isp.com”:

```
Router# debug condition username cpe6_1@isp.com
Condition 1 set
Router# show debug

Condition 1: username cpe6_1@isp.com (0 flags triggered)

Router# debug subscriber packet detail
SSS packet detail debugging is on
Router# show debug
SSS:
  SSS packet detail debugging is on

Condition 1: username cpe6_1@isp.com (0 flags triggered)
```

Configuration Examples for ISG Access for PPP Sessions

Configuring ISG Access for PPP Sessions Example

The following example shows the configuration of an ISG policy that provides services to PPP subscribers. This example configures ISG to perform the following actions:

- PPP local termination

ISG will provide local termination by activating the service “ispa” for subscribers matching the domain “ispa”. The system will authenticate the subscriber using method-list “list1”. For local termination services, the global VRF is applied by default unless another VRF is specified in the service profile, on the interface, or in the virtual template.

- PPP authentication before forwarding

ISG will locally authenticate subscribers matching domain “ispb” before forwarding the sessions to an LNS. (Sessions are forwarded to an LNS because service policy map “ispb” specifies a VPDN group). The system will authenticate the subscribers using method-list “list2”.

- PPP forwarding without local authentication

ISG will forward sessions to an LNS without local authentication for subscribers matching domain “ispc”.

- PPP domain exclusion

ISG will deny service to and disconnect the session for subscribers matching domain “ispd”.

- PPP domain-based service activation

For subscribers matching all other domains, ISG will activate a service that has the same name as the specified domain.

Configure control class maps, which define the conditions that must be met before a control policy rule will be executed.

```
class-map type control match-all PPP_SESSION
  match protocol ppp

class-map type control match-all NAS_PORT_CONDITION
  class type control match identifier name PPP_SESSION
  less-than identifier nas-port type atm vpi 200 vci 100
class-map type control match-all ISPA
  match unauthenticated-domain ispa

class-map type control match-all ISPB
  match unauthenticated-domain ispb

class-map type control match-all ISPC
  match unauthenticated-domain ispc

class-map type control match-all ISPD
  match unauthenticated-domain ispd
```

Define the top-level control policy map.

```
policy-map type control L2_ACCESS
```

Define a control policy rule that activates a forwarding service on the basis of the ATM VPI/VCI on which the call came in.

```
 class type control NAS_PORT_CONDITION event session-start
  1 service-policy type service xconnect
```

Define a control policy rule that collects the domain name from the protocol. The domain name is available from a structured user name (e.g., user@domain).

```
 class type control PPP_SESSION event session-start
  1 collect identifier unauthenticated-domain
  2 service-policy type control DOMAIN_BASED_ACCESS
```

Define the nested control policy.

```
policy-map type control DOMAIN_BASED_ACCESS
```

Define a control policy rule that provides local termination by activating the service “ispa”.

```
 class type control ISPA event session-start
  1 authenticate aaa list list1
  2 service-policy type service ispa
```

Define a control policy rule that configures the system to authenticate the subscriber locally before activating service “ispb”. The service “ispb” specifies forwarding the session to an LNS.

```
 class type control ISPB event session-start
  1 authenticate aaa list list2
  2 service-policy type service ispb
```

Define a control policy rule that activates service “ispc”, which specifies forwarding.

```
 class type control ISPC event session-start
  1 service-policy type service ispc
```

Define a control policy rule that results in session disconnection for subscribers that match service “ispd”.

```
 class type control ISPD event session-start
  service disconnect
```

Define a control policy rule that defines the default for all other domains, which is to activate a service having the same name as the specified domain.

```
 class type control always event session-start
    service-policy type service identifier unauthenticated-domain
```

Configure the service policy maps.

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

policy-map type service ispa
  service local
  ip vrf forwarding red

policy-map type service ispb
  service vpdn group 2

policy-map type service ispc
  service vpdn group 3
```

Apply the control policy map globally.

```
service-policy type control L2_ACCESS
```

VRF Transfer for PPP Sessions Using IPCP Renegotiation Example

The following example shows a configuration that uses PPPoE to establish a session, and the RADIUS service profile that is created to associate the VRF. In this example, when a PPP session initially comes up, it belongs to the default routing table, and the IP address is assigned from the default IP address pool “DEF-POOL”. When the subscriber selects the “ISP-RED” service, ISG downloads the “ISP-RED” service profile and applies it to the session. The PPP session is then transferred to VRF “RED”. IPCP renegotiation occurs between the client device and the ISG device, and the subscriber is assigned a new IP address from the pool “POOL-RED”.

```
ip vrf RED
 rd 1:1
interface Loopback0
 ip address 10.0.0.1 255.255.255.0
interface Loopback1
 ip address 10.0.1.0 255.255.255.0
 ip vrf forwarding RED
!
interface Ethernet0/0
  pppoe enable
interface Virtual-Template1
 ip unnumbered Loopback0
 service-policy control RULE2
 peer default ip address pool DEF-POOL
 ppp authentication chap
ip local pool DEF-POOL 172.16.5.1 172.16.5.250
ip local pool POOL-RED 172.20.5.1 172.20.5.250
```

Service Profile for ISP RED

```
Cisco-AVpair = ip:vrf-id=RED
Cisco-AVpair = "ip:ip-unnumbered=loopback 1"
Cisco-AVpair = ip:addr-pool=POOL-RED
Cisco-AVpair = subscriber:sg-service-type=primary
Cisco-AVpair = subscriber:sg-service-group=RED-GROUP
Cisco-SSG-Service-Info = IPPPOE-RED
Cisco-SSG-Service-Info = R10.1.1.0;255.255.255.0
Framed-Protocol = PPP
Service-Type = Framed
```

Additional References

Related Documents

Related Topic	Document Title
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
AAA configuration tasks	The "Authentication" section in the *Security Configuration Guide*
AAA commands	The "Authentication, Authorization, and Accounting (AAA)" section in the *Security Command Reference*
PPP configuration tasks	The “PPP Configuration►? section in the *Dial Services Configuration Guide*
PPP commands	*Dial Services Command Reference*

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/public/support/tac/home.shtml

Feature Information for ISG Access for PPP Sessions

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 Layer 2 Access

Feature Name	Releases	Feature Configuration Information
ISG:Session: Creation: P2P Session (PPPoE, PPPoXoX)	Cisco IOS XE Release 2.2	The ISG session is the primary context to which services and policies are associated across specific data flows. Point-to-point (P2P) sessions are established through a signaling protocol. ISG handles many variants of P2P encapsulation, such as PPP, PPPoE and PPPoA.