IP Routing: Protocol-Independent Configuration Guide, Cisco IOS XE 17 (Cisco ASR 920 Series)

First Published: 2019-11-14

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1 **Policy-Based Routing** 1

Finding Feature Information 1

Information About Policy-Based Routing 1

Policy-Based Routing 1

Restrictions for Policy-Based Routing 2

How to Configure Policy-Based Routing 3

Configuring Policy-Based Routing 3

Verifying Policy-Based Routing 4

Configuration Examples for Policy-Based Routing 5

Example: Policy-Based Routing 5

Additional References 5

Feature Information for Policy-Based Routing 6

CHAPTER 2 **Segment Routing—IS-IS v4 node SID** 7

Information About Segment Routing IS-IS v4 Node SID 7

Segment Routing IS-IS v4 Node SID 7

How to Configure Segment Routing —IS-IS v4 Node SID 8

Configuring Segment Routing 8

Configuring Segment Routing on an IS-IS Network 9

Configuring Prefix-SID for IS-IS 10

Configuring Prefix Attribute N-Flag 11

Configuring the Explicit Null Attribute 12

Configuration Examples for Segment Routing —IS-IS v4 Node SID 13

Example: Configuring Segment Routing on IS-IS Network 13

Example: Configuring an Explicit Null Attribute 13

Additional References for Segment Routing-IS-IS v4 Node SID 13

Feature Information for Segment Routing with IS-IS v4 Node SID 14

CHAPTER 3 **PPPoE Intermediate Agent** 15

Information About PPPoE Intermediate Agent 16

Prerequisites for PPPoE Intermediate Agent 16

Restrictions for PPPoE Intermediate Agent 16

How to Configure PPPoE Intermediate Agent 17

Enabling or Disabling PPPoE IA on a Device 17

Configuring the Access Node Identifier for PPPoE IA 17

Configuring the Generic Error Message for PPPoE IA 18

Configuring the Identifier String, Option, and Delimiter for PPPoE IA 18

Enabling or Disabling PPPoE IA on an Interface 18

Enabling or Disabling PPPoE IA on BD 18

Configuring PPPoE IA Circuit-ID on an Interface 19

Configuring PPPoE IA Remote-ID on an Interface 19

Configuring PPPoE IA Rate Limiting Setting on an Interface 20

Configuring the PPPoE IA Trust Setting on an Interface 21

Configuring PPPoE IA Vendor-tag Stripping on an Interface 21

Verifying PPoE IA Configuration 21

Clearing Packet Counters 21

Verifying Interface Statistics 22

Verifying PPPoE IA is Enabled 23

Verifying Configuration for PPPoE IA on an Interface 23

Troubleshooting Tips 23

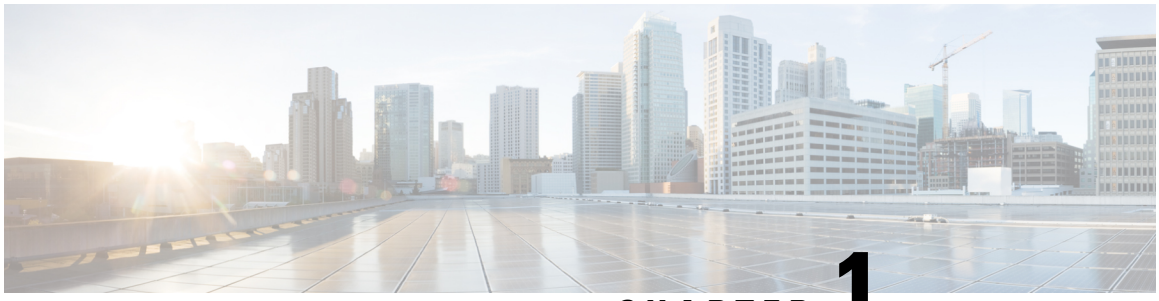
Configuration Examples 23

Configuration Example for PPPoE IA on an Interface 23

Configuration Example for PPPoE IA on a Bridge Domain Interface 24

Configuration Example with Multiple Bridge Domains 24

Additional References for PPPoE Intermediate Agent 25



CHAPTER 1

Policy-Based Routing

Note This feature is not applicable on the Cisco RSP3 module.

The Policy-Based Routing feature is a process whereby a device puts packets through a route map before routing the packets. The route map determines which packets are routed next to which device. Policy-based routing is a more flexible mechanism for routing packets than destination routing.

- Finding Feature Information, on page 1
- Information About Policy-Based Routing, on page 1
- How to Configure Policy-Based Routing, on page 3
- Configuration Examples for Policy-Based Routing, on page 5
- Additional References, on page 5
- Feature Information for Policy-Based Routing, on page 6

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 https://cfnng.cisco.com/. An account on Cisco.com is not required.

Information About Policy-Based Routing

Policy-Based Routing

Policy-based routing is a process whereby the device puts packets through a route map before routing them. The route map determines which packets are routed next to which device. You might enable policy-based routing if you want certain packets to be routed in a certain way other than the obvious shortest path. Possible applications for policy-based routing are to provide equal access, protocol-sensitive routing, source-sensitive

routing, routing based on interactive versus batch traffic, and routing based on dedicated links. Policy-based routing is a more flexible mechanism for routing packets than destination routing.

To enable policy-based routing, you must identify which route map to use for policy-based routing and create the route map. The route map itself specifies the match criteria and the resulting action if all of the match clauses are met.

To enable policy-based routing on an interface, indicate which route map the device should use by using the **ip policy route-map** *map-tag* command in interface configuration mode. A packet arriving on the specified interface is subject to policy-based routing except when its destination IP address is the same as the IP address of the device's interface. This **ip policy route-map** command disables fast switching of all packets arriving on this interface.

To define the route map to be used for policy-based routing, use the **route-map** *map-tag* [**permit**] [*sequence-number*] global configuration command.

To define the criteria by which packets are examined to learn if they will be policy-based routed, use the **match ip address** {*access-list-number* | *access-list-name*} command or both in route map configuration mode. No match clause in the route map indicates no packet match.

To display the cache entries in the policy route cache, use the **show ip cache policy** command.

Note PBR is supported only in a video template.

Restrictions for Policy-Based Routing

- The following command is not supported:

```
ip local policy route-map <route-map_name>
```

Note Local Policy based routing is not supported.

- The following ACL statement is not supported:

```
permit ip any any
```

Note Use a specific prefix match for policy-based routing to work.

- The router does not support deny access control entries (ACE) in the access-lists when configured under route maps.
- If there is no match criteria in the route map, the traffic cannot be enabled for policy-based routing.

How to Configure Policy-Based Routing

Configuring Policy-Based Routing

Procedure

	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	**sdm prefer video** **Example:** `Router(config)#sdm prefer video`	Configures the video mode. **Note** This requires a reload of the system. The configuration of the following steps will only be effective after the SDM template is changed to video template.
Step 4	**ip access-list extended <name>** **Example:** `Router(config)#ip access-list extended pbr-acl1`	Configures an Extended ACL named "pbr-acl1" and enters extended-acl configuration mode.
Step 5	**permit protocol source [source-wildcard] destination [destination-wildcard]** **Example:** `Router(config-ext-nacl)#permit ip 10.0.0.0 0.255.255.255 200.0.0.0 0.255.255.255`	Creates a match statement to match the specified source & destination IP address.
Step 6	**exit** **Example:** `Router(config-ext-nacl)#exit`	Returns to global configuration mode.
Step 7	**Route-map <route_map_name> permit <sequence_number>** **Example:**	Creates a Route-map statement named "pbr" for redistributing routes from one routing protocol into another routing protocol or

	Command or Action	Purpose
	`Router(config)#route-map pbr permit 10`	enables policy-based routing and enters route-map configuration mode.
Step 8	**match ip address <match_criteria_name>** **Example:** `Router(config-route-map)#match ip address pbr-acl1`	Defines the match criteria by which packets are examined to learn if they will be policy-based routed.

Step 9	**set ip next-hop <ip_address> set ip vrf <vrf_name> next-hop <ip_address> set vrf <vrf_name>**
	Example:
	`Router(config-route-map)#set ip next-hop 30.0.0.2`
	`Router(config-route-map)#set ip vrf vrf1 next-hop 30.0.0.1`
	`Router(config-route-map)#set vrf vrf1`
		Specifies where to output packets that pass a match clause of a route map for policy routing.

Step 10	**exit** **Example:** `Router(config-route-map)#exit`	Returns to global configuration mode.
Step 11	**interface type number** **Example:** `Router(config)#interface Gi0/0/10`	Configures an interface type and enters interface configuration mode.
Step 12	**ip policy route-map <route_map_name>** **Example:** `Router(config-if)#ip policy route-map pbr`	Identifies a route map to use for policy routing on an interface.
Step 13	**exit** **Example:** `Router(config-if)#exit`	Returns to global configuration mode.

Verifying Policy-Based Routing

Use this command to verify that the SDM template is changed to video template.

show sdm prefer current

```
PE1#show sdm prefer current
The current template is "video" template
```

Use this command to display the cache entries in the policy route cache.

show ip cache policy

```
CE1#show ip policy
Interface      Route map
Gi0/0/10       equal-access
CE1#
```

Configuration Examples for Policy-Based Routing

This section shows sample configuration for Policy-Based Routing.

Example: Policy-Based Routing

The following is a sample configuration for Policy-Based Routing.

```
Device# conf t
Device(config)# access-list 1 permit host 10.1.1.1
Device(config)# access-list 2 permit host 172.17.2.2
Device(config)# exit

Device# conf t
Device(config)# route-map equal-access permit 10
Device(config-route-map)# match ip address 1
Device(config-route-map)# set ip next-hop 172.16.6.6
Device(config-route-map)# exit
Device(config)# route-map equal-access permit 20
Device(config-route-map)# match ip address 2
Device(config-route-map)# set ip next-hop 192.168.7.7
Device(config-route-map)# exit
Device(config)#exit

Device# conf t
Device(config)# interface GigabitEthernet0/0/2
Device(config-if)# ip policy route-map equal-access
Device(config-if)# exit
```

Additional References

Related Documents

Related Topic	Document Title
IP routing protocol-independent commands	Cisco IOS IP Routing: Protocol-Independent Command Reference

Technical Assistance

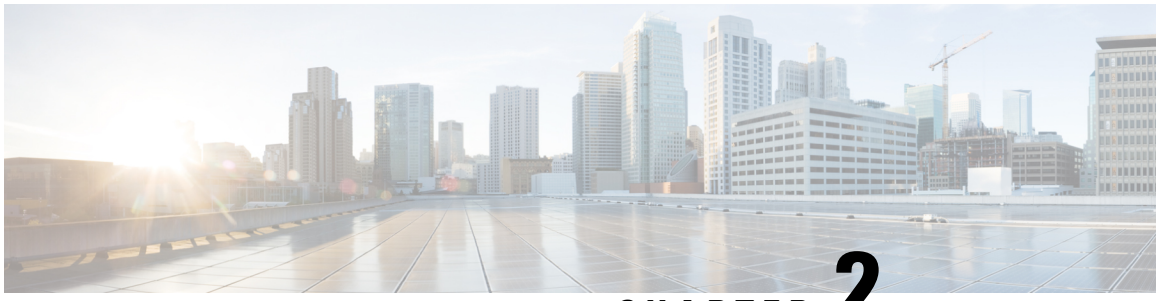
Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools 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 Policy-Based Routing

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 Policy-Based Routing



CHAPTER 2

Segment Routing—IS-IS v4 node SID

The Segment Routing—ISIS v4 node SID feature provides support for segment routing on Cisco Intermediate System-to-Intermediate System (IS-IS) networks.

- Information About Segment Routing IS-IS v4 Node SID, on page 7
- How to Configure Segment Routing —IS-IS v4 Node SID, on page 8
- Configuration Examples for Segment Routing —IS-IS v4 Node SID, on page 13
- Additional References for Segment Routing-IS-IS v4 Node SID, on page 13
- Feature Information for Segment Routing with IS-IS v4 Node SID, on page 14

Information About Segment Routing IS-IS v4 Node SID

Segment Routing IS-IS v4 Node SID

Segment Routing relies on a small number of extensions to Cisco Intermediate System-to-Intermediate System (IS-IS) and Open Shortest Path First (OSPF) protocols. There are two levels of configuration required to enable segment routing for a routing protocol instance. The top level segment routing configuration which is managed by segment routing infrastructure component enables segment routing, whereas, segment routing configuration at the router level enables segment routing for a specific address-family of a routing protocol instance. There are three segment routing states:

- SR_NOT_CONFIGURED
- SR_DISABLED
- SR_ENABLED

Segment routing configuration under the IGPs is allowed only if the SR state is either SR_DISABLED or SR_ENABLED. The SR_ENABLED state indicates that there is at least a valid SRGB range reserved through the MFI successfully. You can enable segment routing for IGPs under the router configuration sub mode, through commands. However, IGP segment routing are enabled only after the global SR is configured.

The SR_ENABLED is a necessary state for any protocol to enable SR, however, it is not a sufficient for enabling SR for a protocol instance. The reason being that the IS-IS still does not have any information about segment routing global block (SRGB) information. When the request to receive information about the SRGB is processed successfully, the IS-IS SR operational state is enabled.

Segment Routing requires each router to advertise its segment routing data-plane capability and the range of MPLS label values that are used for segment routing in the case where global SIDs are allocated. Data-plane

capabilities and label ranges are advertised using the SR-capabilities sub-TLV inserted into the IS-IS Router Capability TLV-242 that is defined in RFC4971.

ISIS SR-capabilities sub TLV includes all reserved SRGB ranges. However, the Cisco implementation supports only one SRGB range. The supported IPv4 prefix-SID sub TLV are TLV-135 and TLV-235.

How to Configure Segment Routing —IS-IS v4 Node SID

Configuring Segment Routing

Before you begin

Before configuring IS-IS to support segment routing you must first configure the segment routing feature in global configuration mode.

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	**segment-routing mpls** **Example:** `Device(config-sr)# segment-routing mpls`	Enables the segment feature using the MPLS data plane.
Step 4	**connected-prefix-sid-map** **Example:** `Device(config-srmpls)# connected-prefix-sid-map`	Enters a sub-mode where you can configure address-family specific mappings for local prefixes and SIDs.
Step 5	**address-family ipv4** **Example:** `Device(config-srmpls-conn)# address-family ipv4`	Specifies IPv4 address prefixes.
Step 6	**10.1.1.1/32 index 100 range 1** **Example:**	Associates SID 100 with the address 10.1.1.1/32.

	Command or Action	Purpose
	`Device(config-srmpls-conn-af)# 10.1.1.1/32 100 range 1`	
Step 7	**exit-address-family** **Example:** `Device(config-srmpls-conn-af)# exit-address-family`	Exits the address family.

Configuring Segment Routing on an IS-IS Network

Before you begin

Before you configure segment routing on IS-IS network, IS-IS must be enabled on your network.

Procedure

	Command or Action	Purpose
Step 1	**router isis** **Example:** `Device(config-router)# router isis`	Enables the IS-IS routing protocol and enters router configuration mode.
Step 2	**net network-entity-title** **Example:** `Device(config-router)# net 49.0000.0000.0003.00`	Configures network entity titles (NETs) for the routing instance.
Step 3	**metric-style wide** **Example:** `Device(config-router)# metric-style wide`	Configures the device to generate and accept only wide link metrics.
Step 4	**segment-routing** mpls **Example:** `Device(config-router)# segment-routing mpls`	Configures segment routing operation state.
Step 5	**exit** **Example:** `Device(config-router)# exit`	Exits segment routing mode and returns to the configuration terminal mode.

	Command or Action	Purpose
Step 6	**show isis segment-routing** **Example:** `Device# show is-is segment-routing`	Displays the current state of the IS-IS segment routing.

Example

The following example displays output from the **show isis segment-routing state** command for the segment routing under IS-IS:

```
Device# show isis segment-routing

ISIS protocol is registered with MFI
ISIS MFI Client ID:0x63
Tag 1 - Segment-Routing:
   SR State:SR_ENABLED
   Number of SRGB:1
   SRGB Start:16000, Range:8000, srgb_handle:0x4500AED0, srgb_state: created
   Address-family IPv4 unicast SR is configured
     Operational state:Enabled
```

Configuring Prefix-SID for IS-IS

This section explains how to configure prefix segment identifier (SID) index under each interface.

Before you begin

Segment routing must be enabled on the corresponding address family.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**segment-routing mpls** **Example:** `Device(config)# segment-routing mpls`	Configures segment routing mpls mode.

	Command or Action	Purpose
Step 4	**connected-prefix-sid-map** **Example:** `Device(config-srmpls)# connected-prefix-sid-map`	Enters a sub-mode where you can configure address-family specific mappings for local prefixes and SIDs.
Step 5	**address-family ipv4** **Example:** `Device(config-srmpls-conn)# address-family ipv4`	Specifies the IPv4 address family and enters router address family configuration mode.
Step 6	**10.1.1.1/32 index 100 range 1** **Example:** `Device(config-srmpls-conn-af)# 10.1.1.1/32 100 range 1`	Associates SID 100 with the address 10.1.1.1/32.
Step 7	**exit** **Example:** `Device(config-router)# exit`	Exits segment routing mode and returns to the configuration terminal mode.

Configuring Prefix Attribute N-Flag

By default, a flag called N-flag is set by IS-IS when advertising an SID that is associated with a loopback address. To clear this flag add explicit configuration.

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	**interface loopback3** **Example:** `Device(config)# interface loopback3`	Specifies the interface loopback.

	Command or Action	Purpose
Step 4	**isis prefix n-flag-clear** **Example:** `Device(config-if)# isis prefix n-flag-clear`	Clears the prefix N-flag.

Configuring the Explicit Null Attribute

To disable penultimate-hop-popping (PHP) and add explicit-Null label, explicit-null option needs to be specified. Once the option is given, IS-IS sets the E flag in the prefix-SID sub TLV.

By default, a flag called E-flag (Explicit-Null flag) is set to 0 by ISIS when advertising a Prefix SID which is associated with a loopback address. If you wish to set this flag add explicit configuration.

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	**segment-routing mpls** **Example:** `Device(config)# segment-routing mpls`	Configures segment routing mpls mode.
Step 4	**set-attributes** **Example:** `Device(config-srmpls)# set-attributes`	Sets the attribute.
Step 5	**address-family ipv4** **Example:** `Device(config-srmpls-attr)# address-family ipv4`	Specifies the IPv4 address family and enters router address family configuration mode.
Step 6	**explicit-null** **Example:**	Enables the explicit-null label.

	Command or Action	Purpose
	`Device(config-srmpls-attr-af)# explicit-null`	
Step 7	**exit-address-family** **Example:** `Device(config-srmpls-attr-af)# exit-address-family`	Exits the address family.

Configuration Examples for Segment Routing —IS-IS v4 Node SID

Example: Configuring Segment Routing on IS-IS Network

The following example shows how to configure prefix segment identifier (SID) index under each interface:

```
Device(config)#segment-routing mpls
 Device(config-srmpls)#connected-prefix-sid-map
  Device(config-srmpls-conn)#address-family ipv4
   Device(config-srmpls-conn-af)#10.1.2.2/32 index 2 range 1
  Device(config-srmpls-conn-af)#exit-address-family
 Device(config-srmpls-conn-af)#end
```

Example: Configuring an Explicit Null Attribute

The following is an example of configuring an explicit null attribute:

```
Device(config)# segment-routing mpls
Device(config-srmpls)# set-attributes
 Device(config-srmpls-attr)# address-family ipv4
  Device(config-srmpls-attr-af)# explicit-null
 Device (config-srmpls-attr-af)# exit-address-family
```

Additional References for Segment Routing-IS-IS v4 Node SID

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html
IP Routing ISIS commands	Cisco IOS IP Routing ISIS commands http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html

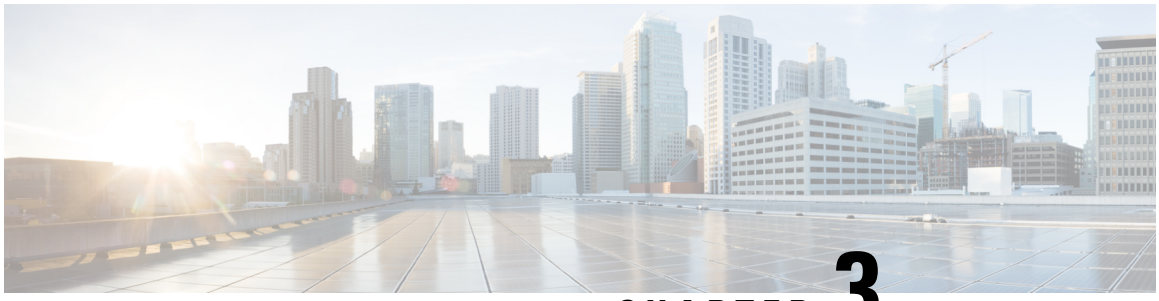
Technical Assistance

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 Segment Routing with IS-IS v4 Node SID

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.

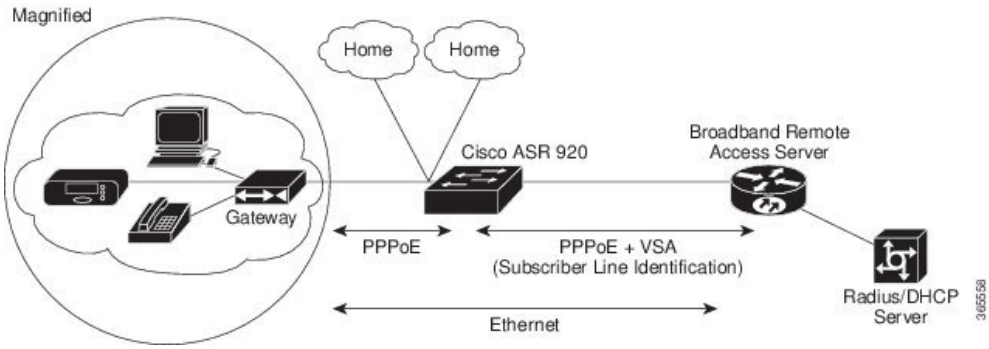


CHAPTER 3

PPPoE Intermediate Agent

Point-to-point protocol over Ethernet intermediate agent (PPPoE IA) is placed between a subscriber and broadband remote access server (BRAS). PPPoE IA helps the service provider BRAS to distinguish between end hosts connected over Ethernet and an access device. The topology of a typical PPPoE implementation is shown in the figure below.

Figure 1: PPP in an Ethernet Scenario



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 Toolkit 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 at the end of this module.

- Information About PPPoE Intermediate Agent, on page 16
- Prerequisites for PPPoE Intermediate Agent, on page 16
- Restrictions for PPPoE Intermediate Agent, on page 16
- How to Configure PPPoE Intermediate Agent, on page 17
- Verifying PPoE IA Configuration, on page 21
- Troubleshooting Tips, on page 23
- Configuration Examples, on page 23
- Additional References for PPPoE Intermediate Agent, on page 25

Information About PPPoE Intermediate Agent

On the access switch, PPPoE IA enables subscriber line identification by appropriately tagging Ethernet frames of different users. The tag contains specific information such as, which subscriber is connected to the switch and ethernet flow point (EFP).

PPPoE IA acts as mini security firewall between host and BRAS by intercepting all PPPoE Active Discovery (PAD) messages on a per-port per-EFP basis. It provides specific security feature such as, verifying the intercepted PAD message from untrusted port, performing per-port PAD message rate limiting, inserting and removing VSA Tags into and from PAD messages respectively.

Prerequisites for PPPoE Intermediate Agent

- Interface and per-Bridge Domain(per-BD) based PPPoE IA configurations take effect only when the PPPoE IA feature is enabled globally. Discovery packets are switched or bridged if PPPoE IA is disabled globally.
- PPPoE IA feature supports global/per-port/per-BD based format configuration for generating the circuit-id and remote-id. Choose the appropriate option to meet the requirements.
- To configure a large number of intermediate agent devices for PPPoE IA, use the **pppoe intermediate-agent** command for automatically generating subscriber-line information in the VSA tag by the feature.
- Enable PPoE IA globally, per-Interface and per-BD.

Restrictions for PPPoE Intermediate Agent

- PPPoE IA is not supported on routed interfaces.
- PPPoE IA is not supported on Port-Channel.
- You can enable either PPPoE IA or PPPoE client on the device. You can not have PPPoE IA and PPPoE client on the same device.
- More than 6000 PPPoE sessions are not supported in the device acting as an intermediate agent.
- PPoE IA is only supported on physical interface and Bridge Domain.
- BRAS connected ports are configured as trusted and Host connected port as untrusted.
- When PPPoE IA is enabled globally on the device, the discovery packets received on the Interface, which has PPPoE IA disabled, is dropped.
- Circuit-id and remote-id is configured globally, at interface or at the Bridge Domain level. PPPoE IA uses this to create tag in the following way:
    - If PPoE IA is enabled per-BD, the circuit-id and remote-id configured for that BD is used. If not global values are used.

- If PPoE IA is enabled per-interface, the circuit-id and remote-id configured for that interface is used. If not global values are used.

- PPPoE is not supported with L2VPN.

How to Configure PPPoE Intermediate Agent

The following tasks describe how to configure PPPoE IA on a device:

- Enabling or Disabling PPPoE IA on a Device, on page 17
- Configuring the Access Node Identifier for PPPoE IA, on page 17
- Configuring the Generic Error Message for PPPoE IA, on page 18
- Configuring the Identifier String, Option, and Delimiter for PPPoE IA, on page 18
- Enabling or Disabling PPPoE IA on an Interface, on page 18
- Configuring PPPoE IA Circuit-ID on an Interface, on page 19
- Configuring PPPoE IA Remote-ID on an Interface, on page 19
- Configuring PPPoE IA Rate Limiting Setting on an Interface, on page 20
- Configuring the PPPoE IA Trust Setting on an Interface, on page 21
- Configuring PPPoE IA Vendor-tag Stripping on an Interface, on page 21
- Enabling or Disabling PPPoE IA on BD, on page 18
- Configuring PPPoE IA Circuit-ID on BD, on page 19
- Configuring PPPoE IA Remote-ID on BD, on page 20

Enabling or Disabling PPPoE IA on a Device

To enable or disable PPPoE IA globally on the device, complete the following steps:

```
enable
configure terminal
pppoe intermediate-agent
end
```

Configuring the Access Node Identifier for PPPoE IA

Note If you do not specify the access node identifier of the switch, the value is automatically set as 0.0.0.0.

```
enable
configure terminal
pppoe intermediate-agent format-type access-node-id string switch123
end
```

Configuring the Generic Error Message for PPPoE IA

Note PPPoE IA sends a generic error message only on specific error condition. If you do not specify **string** {*message*}, the error message is not added.

```
enable
configure terminal
pppoe intermediate-agent format-type generic-error-message string
end
```

Configuring the Identifier String, Option, and Delimiter for PPPoE IA

The **pppoe intermediate-agent format-type identifier-string string circuit1 option** command has the following options

- pv Port + Vlan
- sp Slot + Port
- spv Slot + Port + Vlan
- sv Slot + Vlan

```
enable
configure terminal
pppoe intermediate-agent format-type identifier-string string circuit1 option spv delimiter
 :
end
```

Enabling or Disabling PPPoE IA on an Interface

Note This setting applies to all frames passing through this interface, regardless of the EFP to which they belong. By default the PPPoE IA feature is disabled on all interfaces. You need to run this command on every interface that requires this feature.

Before You Begin

You must enable PPPoE IA on the device in the global configuration mode.

```
enable
configure terminal
interface GigabitEthernet 0/0/1
pppoe intermediate-agent
end
```

Enabling or Disabling PPPoE IA on BD

PPPoE IA can be configured to add specific information as part of subscriber identification. This can be configured on a per-port and per-port-per-bridge domain basis. When specific packets received on a particular Bridge-domain need to be differentiated with other packets received on that interface.

To enable or disable PPPoE IA on BD, complete the following steps:

Before You Begin

You must enable PPPoE IA on the device in the global configuration mode.

```
enable
configure terminal
interface GigabitEthernet 0/1/1
pppoe intermediate-agent bridge-domain 40
end
```

Configuring PPPoE IA Circuit-ID on an Interface

You can configure Circuit-ID on interface level. The PADI, PADR and PADT packets (PPPoE Discovery packets) received on this physical interface gets IA-tagged using the configured circuit-id using the **pppoe intermediate-agent format-type circuit-id string word** command, irrespective of the Bridge Domain (BD). This command over-writes global level circuit-id configuration or automatic generation of circuit-id by the Switch.

This parameter is not set by default.

Note If BD is enabled with PPPoE IA, BD level circuit-id configuration overwrites all other circuit-id configuration, for the packets that are received on that particular BD.

To configure the circuit-ID on an interface, complete the following steps:

```
enable
configure terminal
interface GigabitEthernet 0/0/1
pppoe intermediate-agent format-type circuit-id string root
end
```

Configuring PPPoE IA Circuit-ID on BD

This configuration overrides the circuit-id configuration specified at interface or global level. The packets received on the specified bridge-domain gets the PPPoE IA tag with configured circuit-id. By default the **pppoe intermediate-agent bridge-domain <bridge-domain_num> circuit-id {string {WORD}}** command is not configured.

Before You Begin

You must enable PPPoE IA globally and on particular BD.

To configure the circuit-ID on BD, complete the following steps:

```
enable
configure terminal
interface GigabitEthernet 0/0/1
pppoe intermediate-agent bridge-domain 50 circuit-id ct1
end
```

Configuring PPPoE IA Remote-ID on an Interface

You can configure remote-id on interface level. The PADI, PADR and PADT packets (PPPoE Discovery packets) received on this physical interface gets IA-tagged using the configured remote-id using the **pppoe intermediate-agent format-type remote-id string word** command irrespective of the BD. This command over-writes global level remote-id configuration or automatic generation of remote-id by the device.

This parameter is not set by default.

Note If BD is enabled with PPPoE IA, BD level remote-id configuration overwrites all other remote-id configuration, for the packets that are received on that particular BD.

```
enable
configure terminal
interface GigabitEthernet 0/0/1
pppoe intermediate-agent format-type remote-id string granite
end
```

Configuring PPPoE IA Remote-ID on BD

This configuration overrides the remote-id configuration specified at interface/global level and the packets received on the specified bridge-domain, will get PPPoE IA tag with remote-id configured. By default the **pppoe intermediate-agent bridge-domain <bridge-domain_num> remote-id {string {WORD}}** command is not configured.

Note The default value of remote-id is the router MAC address (for all bridge-domains).

Before You Begin

You must enable PPPoE IA globally and on particular BD.

To configure the remote-ID on BD, complete the following steps:

```
enable
configure terminal
interface GigabitEthernet 0/1/1
pppoe intermediate-agent bridge-domain 50 remote-id RD1
end
```

Configuring PPPoE IA Rate Limiting Setting on an Interface

You can limit the rate (packets per second) at which PPPoE discovery packets (PADI, PADO, PADR, PADS, and PADT) are received on an interface. When the incoming packet rate achieves or exceeds the configured limit, a port enters an error-disabled state and shuts down.

Note This limit applies to the physical interface to counter misbehaving hosts. Even if a single EFP misbehaves on an interface in trunk mode, the entire interface is shut down (error-disabled), bringing down other EFP traffic on the interface.

If you set the limit on the interface that connect the access switch to BRAS, use a higher value since the BRAS aggregates all the PPPoE traffic to the access switch through this interface.

```
enable
configure terminal
interface GigabitEthernet 0/1/1
pppoe intermediate-agent limit rate 30
end
```

Configuring the PPPoE IA Trust Setting on an Interface

Interfaces that connect the device to the PPPoE server are configured as trusted. Interfaces that connect the device to users (PPPoE clients) are untrusted.

This setting is disabled by default.

```
enable
configure terminal
interface GigabitEthernet 0/0/1
pppoe intermediate-agent
pppoe intermediate-agent trust
end
```

Configuring PPPoE IA Vendor-tag Stripping on an Interface

Vendor-specific tags (VSAs) carry subscriber and line identification information in the packets.

Vendor-tag stripping involves removing the VSAs from PADO, PADS, and PADT packets that are received on an interface before forwarding them to the user.

You can configure vendor-tag stripping on interfaces connected to the PPPoE server.

This setting is disabled by default.

Note BRAS automatically strips the vendor-specific tag off of the PPPoE discovery packets before sending them downstream to the access switch. To operate with older BRAS which does not possess this capability, use the **pppoe intermediate-agent vendor-tag strip** command on the interface connecting the access switch to BRAS

To enable stripping on an interface , complete the following steps:

Before You Begin

1. Enable PPPoE on an interface.
2. Set the PPPoE interface to trust.

```
enable
configure terminal
interface GigabitEthernet 0/0/1
pppoe intermediate-agent vendor-tag strip
end
```

Verifying PPoE IA Configuration

Clearing Packet Counters

Use the following command to clear packet counters for all PPPoE discovery packets (PADI,PADO,PADR,PADS,PADT) on all interfaces (per-port and per-port-per-EFP):

```
Router# clear pppoe intermediate-agent statistics
```

Use the following command to clear packet counters on a selected interface:

```
Router# clear pppoe intermediate-agent statistics interface type typeslot /subslot /port
```

Example:

```
Router# clear pppoe intermediate-agent statistics interface gigabitEthernet 0/0/3
```

Verifying Interface Statistics

Use the following command to view the statistics of all the interfaces on which PPPoEIA is enabled:

```
Router# show pppoe intermediate-agent statistics
```

```
PPPOE IA Per-Port Statistics
---- -----------------

Interface : GigabitEthernet0/0/24
Packets received
 All = 53
 PADI = 17 PADO = 0
 PADR = 17 PADS = 0
 PADT = 19
Packets dropped:
 Rate-limit exceeded = 0
 Server responses from untrusted ports = 0
 Client requests towards untrusted ports = 0
 Malformed PPPoE Discovery packets = 0
BD 40: Packets received PADI = 8 PADO = 0 PADR = 8 PADS = 0 PADT = 9
BD 50: Packets received PADI = 9 PADO = 0 PADR = 9 PADS = 0 PADT = 10
Interface : GigabitEthernet0/0/24
Packets received
 All = 59
 PADI = 0 PADO = 19
 PADR = 0 PADS = 26
 PADT = 14
Packets dropped:
 Rate-limit exceeded = 0
 Server responses from untrusted ports = 0
 Client requests towards untrusted ports = 0
 Malformed PPPoE Discovery packets = 0
BD 40: Packets received PADI = 0 PADO = 12 PADR = 0 PADS = 15 PADT = 7
BD 50: Packets received PADI = 0 PADO = 7 PADR = 0 PADS = 11 PADT = 7
```

Use the following command to view the packet details on an interface:

```
Router# show pppoe intermediate-agent statistics interface type typeslot /subslot /port
```

Example:

```
Router# show pppoe intermediate-agent statistics interface gigabitEthernet 0/0/3
```

```
Interface : Gi 0/0/3
 Packets received
  All = 0
  PADI = 0 PADO = 0
  PADR = 0 PADS = 0
  PADT = 0
 Packets dropped:
  Rate-limit exceeded = 0
  Server responses from untrusted ports = 0
  Client requests towards untrusted ports = 0
  Malformed PPPoE Discovery packets = 0
```

```
BD 40: Packets received PADI = 0 PADO = 0 PADR = 0 PADS = 0 PADT = 0
BD 50: Packets received PADI = 0 PADO = 0 PADR = 0 PADS = 0 PADT = 0
```

Verifying PPPoE IA is Enabled

```
show pppoe intermediate-agent info

PPPoE Intermediate-Agent is enabled

Global access-node-id is default
Global generic error msg is not set
Global identifier-string and delimiter are not set

PPPoE Intermediate-Agent trust/rate is configured on the following Interfaces:

Interface               IA         Trusted    Vsa Strip   Rate limit (pps)
----------------------- --------   -------    ---------   ----------------
GigabitEthernet0/0/10        yes        no         no          unlimited
PPPoE Intermediate-Agent is configured on following bridge domains:
40,50
```

Verifying Configuration for PPPoE IA on an Interface

```
show pppoe intermediate-agent info interface GigabitEthernet 0/0/10

Interface               IA         Trusted    Vsa Strip   Rate limit (pps)
----------------------- --------   -------    ---------   ----------------
Gi 0/0/10         yes        no         no          unlimited
PPPoE Intermediate-Agent is configured on following bridge domains:
40,50
```

Troubleshooting Tips

The following debug commands can help you troubleshoot an improper PPPoE intermediate agent configuration and its related features:

- **debug pppoe intermediate-agent packet**—Displays the contents of a packet received in the software: source and destination MAC address of Ethernet frame, code, version and type of PPPoE Discovery packet and a list of TAGs present.
- **debug pppoe intermediate-agent event**—Provides debugging information about PPPoE events.
- **debug radius**—Generates a report that includes information about the incoming access interface, where discovery frames are received, and about the session being established in PPPoE extended NAS-Port format (format d).

Configuration Examples

Configuration Example for PPPoE IA on an Interface

```
enable
configure terminal
```

```
interface GigabitEthernet0/0/1
no ip address
media-type rj45
negotiation auto
pppoe intermediate-agent format-type circuit-id string cktid10
pppoe intermediate-agent format-type remote-id string rmtid10
pppoe intermediate-agent
service instance 1 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  bridge-domain 40
!
end
```

Configuration Example for PPPoE IA on a Bridge Domain Interface

```
enable
configure terminal
interface GigabitEthernet0/0/1
no ip address
media-type rj45
negotiation auto
pppoe intermediate-agent bridge-domain 40 circuit-id string cktid-20
pppoe intermediate-agent bridge-domain 40 remote-id string rmtid-20
pppoe intermediate-agent bridge-domain 40
service instance 1 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  bridge-domain 40
!
end
```

Configuration Example with Multiple Bridge Domains

```
enable
configure terminal
interface GigabitEthernet0/0/1
no ip address
media-type rj45
negotiation auto
pppoe intermediate-agent bridge-domain 40 circuit-id string cktid-20
pppoe intermediate-agent bridge-domain 40 remote-id string rmtid-20
pppoe intermediate-agent format-type circuit-id string cktid10
pppoe intermediate-agent format-type remote-id string rmtid10
pppoe intermediate-agent bridge-domain 40
pppoe intermediate-agent
service instance 1 ethernet
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
  bridge-domain 40
!
service instance 2 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  bridge-domain 30
!
end
```

In this example:

- the packet received on bd 40 will have circuit and remote id as cktid-20 and rmtid-20 respectively

- the packet received on bd 30 will have circuit & remote id as cktid-10 and rmtid-10 respectively

Additional References for PPPoE Intermediate Agent

The following sections provide references related to the PPPoE IA feature.

MIBs

MIB	MIBs link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

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