Configuring Auto Policy-Based Routing

This chapter describes how to configure the Auto Policy-Based Routing (PBR) feature on the Citrix NetScaler Application Delivery Controller (ADC) appliance to ensure that return traffic from the real server (RS) reaches the RISE appliance.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your 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 "New and Changed Information" chapter or the Feature History table below.

Information About Auto Policy-Based Routing

This section includes the following topics:

Auto Policy-Based Routing

Policy-Based Routing (PBR) allows the creation of policies or rules that can selectively alter the path that packets take within the network. PBR can be used to mark packets so that certain types of traffic are prioritized over the rest, sent to a different destination, or exit through a different physical interface on the router. Classification of interesting traffic is performed using access control lists (ACLs).

PBR rules ensure that return traffic from the real server (RS) reaches the Remote Integrated Service Engine (RISE) appliance. The control channel on the Cisco Nexus 5600 Series switch is used to automate the creation of PBR rules.

After the RISE appliance applies the required configuration, the appliance sends auto PBR (APBR) messages to the Cisco Nexus switch including a list of servers (IP addresses, ports, and protocol) and the next-hop IP address of the appliance.

The Cisco Nexus switch creates the PBR rules for the associated switch virtual interfaces (SVIs). For the local servers, the switch creates the ACLs and route maps.

Use Source IP Option

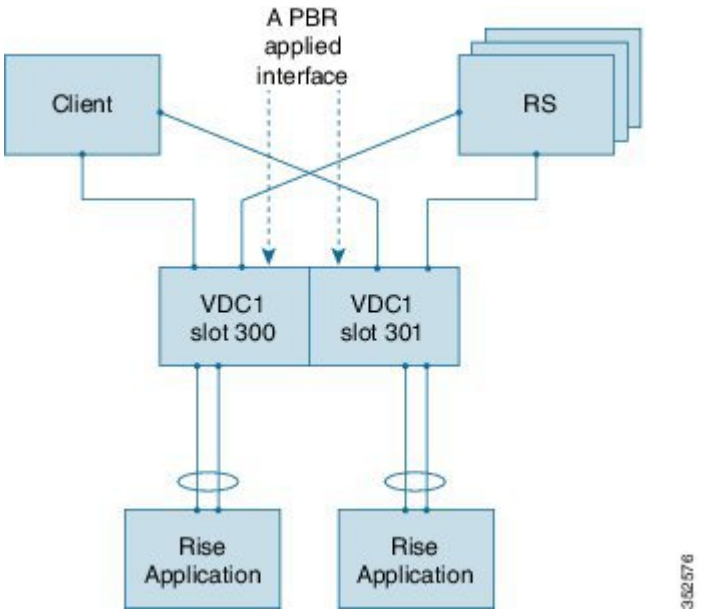
Auto policy-based routing (APBR) rules are configured on the Cisco Nexus switch by the Citrix NetScaler appliance only if the Use Source IP (USIP) option is enabled in the services or service groups on the Citrix NetScaler appliance. The rules are withdrawn when the USIP option is disabled. The USIP option can be configured locally or globally.

Appliance High Availability

High availability is supported for RISE appliances that share an APBR applied interface. Connect your appliances and Cisco Nexus switches using one of the following topologies to enable high availability:

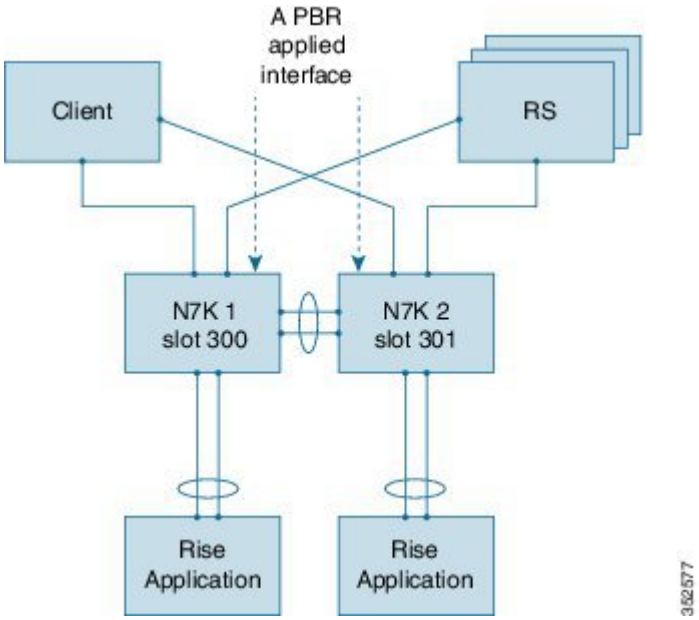
- Two appliances that are each connected to a different virtual device context (VDC) in the same Cisco Nexus 5600 Series switch.

Figure 1: Two Appliances, Two VDCs, One Switch



- Each appliance is connected to a different Cisco Nexus switch and each switch is in virtual port channel (vPC) mode through a peer link.

Figure 2: Two Appliances, Two vPC Peer Switches



- Two appliances are each connected to a different VDC in the same Cisco Nexus 5600 Series switch.

In each of the preceding topologies, one appliance is active and the other is in standby. Each connection acts as a separate service and is unaware of the other service. Each appliance sends APBR rules to the service in each VDC or in each switch, depending upon the topology. Each service sends the appropriate response to the appliance to which it is connected.

When a failover occurs, the standby appliance becomes the new active appliance. The old active appliance sends a PURGE message to the service. After the APBR purge is complete and the old active appliance receives a response, the appliance sends fresh APBR rules. Sending fresh rules ensures that the stale configuration does not remain on the old active appliance

Licensing for Cisco RISE

The following table shows the licensing requirements for this feature:

Product	License Requirements
Cisco NX-OS	The Cisco Remote Integrated Services Engine (RISE) requires the Network Services Package on the Cisco Nexus 5600 Series switch. The NETWORK_SERVICES_PKG license is available starting with Cisco NX-OS Release 7.2(0)N1(1). If you need to use RISE and ITD features with the Cisco NX-OS Release 7.1(1)N1(1), please use the ENHANCED_LAYER2_PKG license. For a complete explanation of the Cisco NX-OS licensing scheme and how to obtain and apply licenses, see the Cisco NX-OS Licensing Guide.

Product	License Requirements
Citrix Citrix Netscaler Application Delivery Controller (ADC) operation system	The Cisco Remote Integrated Services Engine (RISE) does not require a license on the Citrix NetScaler Application Delivery Controller (ADC) appliance for auto-attach. Advanced features, such as auto policy-based routing (APBR), require the NetScaler Platinum or Enterprise license on the Citrix NetScaler Application Delivery Controller (ADC) appliance. To display the license status, use the **show license** command in the NetScaler command line interface

Guidelines and Limitations for Auto Policy-Based Routing

Auto policy-based routing (APBR) has the following guidelines and limitations:

- The globally configured Use Source IP (USIP) takes precedence only when the user does not specify a local choice for the USIP option.
- If the USIP option is set on a service or service group by way of inheritance at the time you create either the service or group, the option is sticky on that service or group.
- If you modify a global property, such as USIP, after you create a service or service group, the global modification does not apply to either the service or group. However, you can modify a service or group locally by using the **set** commands.
- One RS cannot be connected through multiple VLAN interfaces. However, one or more RSs can be connected through the same interface on the Cisco Nexus device to which the APBR policy is applied.
- Multiple next-hop IP addresses for the same RS are not supported in RISE
- RISE does not support multiple services with the same RS IP address and port protocol. The only exception is as follows: Two identical services (with different service names) can be on the active and standby RISE-enabled appliance, pointing to the same APBR configuration.
- The virtual routing and forwarding (VRF) instance of the route to the RS must be the same as for the client VLAN switch virtual interface (SVI) to which the virtual IP (VIP) address is associated. The VRF does not need to be the default VRF.
- We do not recommend that you make any route changes on the egress interface to the RS. If you do make changes, see the troubleshooting information at http://support.citrix.com/proddocs/topic/netscaler/ns-gen-netscaler-wrapper-con.html.
- Equal Cost Multipath (ECMP) is not supported.

Default Settings for Auto Policy-Based Routing

The following table lists the default settings for the Use Source IP (USIP) option on the Citrix NetScaler Application Delivery Controller (ADC) appliance:

Table 1: Default APBR Parameters on the Citrix NetScaler Application Delivery Controller (ADC) Appliance

Parameter	Default
USIP	Disabled

Configuring Auto Policy-Based Routing

This section includes the following topics:

Enabling the RISE Feature and NS Modes

To manually enable the RISE feature and any RISE_APBR NS modes for publishing APBR rules, type the following commands at the command prompt:

Step 1 (Optional) > **enable feature RISE**
This step is only required if you did not enable RISE when you configured Cisco RISE with Citrix Netscaler. See the "Configuring Rise" chapter.

Enables the RISE feature on the appliance.

Step 2 > **enable ns mode RISE_APBR**
Enables the modes of type RISE_APBR on the Citrix Netscaler.

Enabling APBR on the Cisco Nexus Switch

You must enable the policy-based routing feature on the Cisco Nexus 5600 Series switch to support auto policy-based routing (APBR). The Citrix Netscaler Application Delivery Controller (ADC) appliance automatically adds the appropriate rules to the Cisco Nexus switch for APBR.

Before You Begin

Make sure that you are in the correct VDC on the Cisco Nexus switch. To switch VDCs, use the **switchto vdc** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# config term	Enters global configuration mode
Step 2	switch(config)# feature pbr	Enables policy-based routing (PBR) on the Cisco Nexus 5600 Series switch.
Step 3	switch(config)# exit	Exits the global configuration mode.

Configuring APBR on the Citrix NetScaler Application Delivery Controller (ADC) Appliance

This section includes the following topics:

Configuring NSIP on the Appliance

The NetScaler management IP address (NSIP) is the IP address for management and general system access to the Citrix NetScaler Application Delivery Controller (ADC) appliance and for high availability (HA) communication.

Configuring NSIP Using the CLI

You can configure the NSIP on your appliance by using either the configuration prompts or the command-line interface (CLI).

Note To prevent an attacker from impeding your ability to send packets to the appliance, choose a nonroutable IP address on your organization's LAN as your appliance IP address.

Before You Begin

Ensure that a port channel is configured on the appliance and that the appliance's physical ports are mapped to this port channel.

Perform one of the following tasks:

Option	Description
config ns	Displays prompts for configuring the NSIP.
set ns config -ipaddress *address* **-netmask** *netmask* **add ns ip** *ip-address netmask* **-type** *type* **add route** *network netmask gateway* **save ns config** **reboot**	Configures the NSIP using the CLI.

Example:

The following example shows how to configure the NSIP using the CLI:

```
set ns config -ipaddress 10.102.29.60 -netmask 255.255.255.0
add ns ip 10.102.29.61 255.255.255.0 -type snip
add route 0.0.0.0 0.0.0.0 10.102.29.1
save ns
```

Configuring NSIP Using the Configuration Utility

Before You Begin

- Create a port channel on the Citrix NetScaler Application Delivery Controller (ADC) appliance and map its physical ports to this port channel.

Step 1 Navigate to **System > Settings**.

Step 2 In the details pane, under Settings, click **Change NSIP Settings**.

Step 3 In the Configure NSIP Settings dialog box, set the parameters. For a description of a parameter, hover the mouse cursor over the corresponding field.

Step 4 Under Interfaces, choose the interfaces from the Available Interfaces list and click **Add** to move them to the Configured Interfaces list.

Step 5 Click **OK**. In the Warning dialog box, click **OK**. The configuration takes effect after the Citrix NetScaler Application Delivery Controller (ADC) appliance is restarted.

Configuring a NSVLAN on Citrix NetScaler Application Delivery Controller (ADC) Appliance

The NSVLAN is a VLAN to which the NetScaler management IP (NSIP) address's subnet is bound. The NSIP subnet is available only on interfaces that are associated with NSVLAN. By default, NSVLAN is VLAN1, but you can designate a different VLAN as NSVLAN. If you designate a different VLAN as an NSVLAN, you must reboot the Citrix NetScaler Application Delivery Controller (ADC) appliance for the change to take effect. After the reboot, NSIP subnet traffic is restricted to the new NSVLAN.

Perform only one of the following tasks:

Configuring NSVLAN Using the CLI

Enter the following commands prompt to configure NSVLAN using the CLI:

Before You Begin

- Create a port channel on the Citrix NetScaler Application Delivery Controller (ADC) appliance and map its physical ports to this port channel.
- Configure the NS IP address (NSIP) on the appliance.

Step 1 **set ns config - nsvlan** *positive_integer* **- ifnum** *interface_name ...* [**-tagged** (**YES** | **NO**)]

Note You must reboot the appliance for the configuration to take effect.

Step 2 (Optional) **show ns config**

```
set ns config -nsvlan 300 -ifnum 1/1 1/2 1/3 -tagged NO
save config
```

Step 3 (Optional) **unset ns config -nsvlan**

Restores the default configuration.

Configuring NSVLAN Using the Configuration Utility

Before You Begin

- Create a port channel on the Citrix NetScaler Application Delivery Controller (ADC) appliance and map its physical ports to this port channel.
- Configure the NetScaler IP address (NSIP) on the appliance.

Step 1 Navigate to **System > Settings**.

Step 2 In the details pane, under Settings, click **Change NSVLAN Settings**.

Step 3 In the Configure NSVLAN Settings dialog box, set the parameters. For a description of a parameter, hover the mouse cursor over the corresponding field.

Step 4 Under Interfaces, choose the interfaces from the Available Interfaces list and click **Add** to move them to the Configured Interfaces list.

Step 5 Click **OK**. In the Warning dialog box, click **OK**. The configuration takes effect after the Citrix NetScaler Application Delivery Controller (ADC) appliance is restarted.

Enabling the USIP Option

APBR rules are configured on the Cisco Nexus 5600 Series switch by the Citrix Netscaler Application Delivery Controller (ADC) appliance when the Use Source IP (USIP) option is enabled. Perform only one of the following tasks to enable the USIP option on the Citrix Netscaler Application Delivery Controller (ADC) appliance:

Enabling the USIP Option for a Service

To create a service and enable and set the Use Source IP (USIP) option on that service, type the following commands at the command prompt:

Before You Begin

Ensure that the NSIP and NSVLAN are configured on the Citrix Netscaler Application Delivery Controller (ADC) appliance.

Step 1 Use one of the following commands:

Option	Description
add service *service_name ipaddress protocol-type port_number* [**-usip** [**yes** | **no**]	Creates a service and enables the USIP option. The RISE appliance sends the server address, port, protocol, and the IP address of the next-hop interface and the VLAN to the Cisco Nexus switch. The *protocol-type* argument specifies a supported protocol including but not limited to the following keywords: **dns**, **http**, **ssl**, **tcp**, or **udp**. **Note** IPv6 addresses are not supported.
set service *service_name* [**-usip yes**]	Enables the USIP option on a previously configured service. **Note** This command is not required if you previously configured the specified service using the **add service** command with the **-usip** keyword

Example:
The following example shows how to create a service named svc12 and enable the USIP option on the service:

```
> add service svc12 192.168.12.23 http 80 -usip YES
```

Example:
The following example shows how to change a previously created service (svc12) to enable APBR:

```
> set service svc12 -usip YES
```

Step 2 (Optional) **unset service** *service-name*
Disables disable the USIP option on an already configured service and deletes the corresponding APBR route on the Cisco Nexus device

Example:
The following example shows how to disable the USIP option on the service and delete the corresponding APBR route on the Cisco Nexus device:

```
unset service svc12
```

Enabling the USIP Option for a Service Group

To create a service group and enable the Use Source IP (USIP) option on that group, enter the following commands at the command prompt:

Before You Begin

Ensure that the NSIP and NSVLAN are configured on the Citrix Netscaler Application Delivery Controller (ADC) appliance.

Step 1 > **add serviceGroup** *service_name protocol-type port_number* [**-usip** [**yes** | **no**]
Creates a service group and enables the USIP option. The RISE appliance sends multiple APBR messages to the Cisco Nexus device.

The *protocol-type* argument specifies a supported protocol including but not limited to the following keywords: **dns**, **http**, **ssl**, **tcp**, or **udp**.

Note IPv6 addresses are not supported.

Example:
The following example shows how to create a service named svc12 and enable the USIP option on the service:

```
> add serviceGroup svc_grp_1 http 80 -usip YES
```

Step 2 > **bind serviceGroup** *service_group_name ipaddress port_number*
Associates an IP address and port to the service group being configured. Repeat this step for each member IP address and port.

Note IPv6 addresses are not supported.

Example:
The following example shows how to associate three IP addresses and ports to the group being configured.

```
> bind serviceGroup svc_grp_1 192.168.14.12 80
> bind serviceGroup svc_grp_1 192.168.14.13 80
> bind serviceGroup svc_grp_1 192.168.14.14 80
```

Step 3 > **set serviceGroup** *service_name* [**-usip** [**yes**]
Sets the specified service and enables the USIP option.

Note The **-usip** keyword is not required on each service if you use the **add serviceGroup** command with the **-usip** keyword.

Example:

```
> set serviceGroup svc_grp_1
```

The following example shows how to disable the USIP option on all members of a service group and delete the corresponding APBR rules on the Cisco Nexus device:

```
unset serviceGroup svc_grp_1
```

Enabling the USIP Option Globally

To globally enable Use Source IP (USIP) on the Citrix Netscaler Application Delivery Controller (ADC) appliance and set the USIP option on all services and service groups, enter the following command at the command prompt

SUMMARY STEPS

1. > **enable ns mode usip**

DETAILED STEPS

> **enable ns mode usip**
Enables USIP on the Netscaler Application Delivery Controller (ADC) appliance. All subsequent added services are APBR services.

Example:
The following example shows how to enable USIP on the Citrix Netscaler Application Delivery Controller (ADC) appliance and then create a service for which the USIP option is set because the setting is inherited from the global configuration:

```
> enable ns mode USIP
 Done
> add service svc_gl 192.168.12.72 http 80
 Done
```

Verifying the Auto Policy-Based Routing Configuration

To display the auto policy-based routing (APBR) configuration on the Citrix NetScaler Application Delivery Controller (ADC) appliance, perform one of the following tasks on appliance:

Command	Purpose
show apbrSvc service	Displays information about the APBR service.
show apbrSvc -summary [**detail**]	Displays information about the APBR service.
show license	Displays information about the license that is loaded on the Citrix NetScaler Application Delivery Controller (ADC) appliance.
show rise apbrSvc	Displays the RISE running configuration on the Cisco Nexus 5600 Series switch.
show rise profile	Displays information about service profile.
show service *service-name*	Displays information about the specified service.

The following example is sample output from the **show apbrSvc** command on the Citrix Netscaler Application Delivery Controller (ADC) appliance. The same information is displayed by using the **show rise apbrsvc** command.

```
> show apbrSvc

1) Entity Name    : s1
   Entity Type    : Service
   Server IP      : 192.168.15.252
   Server Port    : 80
   Protocol       : HTTP
   Nexthop IP     : 192.168.4.100
   VLAN           : 4
2) Entity Name    : s2
   Entity Type    : Service
   Server IP      : 192.168.15.253
   Server Port    : 80
   Protocol       : HTTP
   Nexthop IP     : 192.168.4.100
   VLAN           : 4
```

```
3) Entity Name    : s3
   Entity Type    : Service
   Server IP      : 192.168.15.254
   Server Port    : 80
   Protocol       : HTTP
   Nexthop IP     : 192.168.4.100
   VLAN           : 4
4) Entity Name    : sg2
   Entity Type    : ServiceGroup
   Server IP      : 192.168.13.202
   Server Port    : 101
   Protocol       : HTTP
   Nexthop IP     : 192.168.4.100
   VLAN           : 4
5) Entity Name    : sg2
   Entity Type    : ServiceGroup
   Server IP      : 192.168.13.202
   Server Port    : 102
   Protocol       : HTTP
   Nexthop IP     : 192.168.4.100
   VLAN           : 4
 Done
```

The following example is sample output from the **show rise apbrsvc-summary** command:

```
> show rise apbrSvc -summary
-------------------------------------------------------------------------------
      EntityName IPAddress         Port  Protocol   NexthopIP         VLAN
-------------------------------------------------------------------------------
1     s1         192.168.15.252    80    HTTP       192.168.4.100     4
2     s2         192.168.15.253    80    HTTP       192.168.4.100     4
3     s3         192.168.15.254    80    HTTP       192.168.4.100     4
4     sg2        192.168.13.202    101   HTTP       192.168.4.100     4
5     sg2        192.168.13.202    102   HTTP       192.168.4.100     4
 Done
```

The following example is sample output from the **show service** command. This example shows that Use Source IP (USIP) is enabled on the service and that the APBR rules have been added to the service.

Note The following status messages for the APBR RISE code can be displayed in the output for this command:

- APBR rule successfully Added—The APBR rule was added on the Cisco Nexus device.
- APBR rule successfully Deleted—The APBR rule was deleted on the Cisco Nexus device.
- APBR rule fixed by Admin—The admin has fixed the discrepancy on the Cisco Nexus device.
- APBR rule not configured due to Timeout—The APBR rule was not configured even after retries.
- APBR rule not configured due to Lack of Memory—The APBR rule was not configured because there is not enough memory on the Netscaler appliance.
- APBR rule dispatch pending—The APBR rule is pending because it is waiting to be dispatched or it is waiting confirmation from the Cisco Nexus device.

```
> show service svc_grp_1

s1 (192.168.15.252:80) - HTTP
State: DOWN
Last state change was at Thu Apr  3 13:04:15 2014
Time since last state change: 0 days, 00:00:28.850
Server Name: 192.168.15.252
Server ID : None Monitor Threshold : 0
Max Conn: 0
Max Req: 0 Max Bandwidth: 0 kbits
Use Source IP: YES <===
Use Proxy Port: NO
```

```
Client Keepalive(CKA): YES
Access Down Service: NO
TCP Buffering(TCPB): YES
HTTP Compression(CMP): YES
Idle timeout: Client: 180 sec
Server: 360 sec
Client IP: DISABLED
Cacheable: NO
SC: OFF
SP: OFF
Down state flush: ENABLED
Appflow logging: ENABLED
TD: 0
RISE CODE:  APBR rule successfully Added <===
.
.
.
 Done
```

The following example is sample partial output from the **show rise profile** command:

```
> show rise profile

1) Service Name   : NS-rise
   Status         : Active
   Mode           : Indirect
   Device Id      : JAF1429CJLB
   Slot Number    : 300
   VDC Id         : 1
   vPC Id         : 0
   SUP IP         : 173.173.1.1
   VLAN           : 3
   VLAN Group     : 1
   ISSU           : None
   Interface      : N/A
```

To display the auto policy-based routing (APBR) configuration on the Cisco Nexus 5600 Series switch and verify that the APBR policy was added, perform one of the following tasks on the switch:

Command	Purpose
show access list dynamic	Displays information about the APBR service.
show rise [**detail**]	Displays information about the APBR service.
show route-map	Displays information about the license that is loaded on the Citrix Netscaler appliance.
show service rise auto-pbr ipv4 slot *slot*	Displays the RISE running configuration on the Cisco Nexus 5600 Series switch.

The following example displays dynamic access list matching the Real Server IP addresses:

```
switch# show access-lists dynamic

Example correct output:

IPV4 ACL _rise-system-acl-172.16.10.5-Vlan1010
        10 permit tcp 10.10.10.11/32 eq 80 any
        20 permit tcp 10.10.10.12/32 eq 80 any
IPV4 ACL _rise-system-acl-172.16.11.5-Vlan1011
        10 permit tcp 10.10.11.11/32 eq 50000 any
```

The following example is sample output from the **show rise** command:

```
switch# show rise

Name            Slot Vdc Rise-Ip         State        Interface
```

```
                 Id  Id
--------------- ---- --- --------------- ------------ ---------
MPX             300  1   10.175.1.11     active       Po10
Emu             301  1   100.0.1.4       active       N/A
VPX             302  1   100.0.1.6       active       N/A

APBR Configuration <===
rs ip           rs port protocol nhop ip         rs nhop  apbr state slot-id
--------------- ------- -------- --------------- -------- ---------- -------
100.0.1.1       33275   TCP      100.0.1.2       Vlan100  ADD FAIL   301
100.0.1.3       64301   TCP      100.0.1.4       Vlan100  ADD DONE   301
100.0.1.5       21743   TCP      100.0.1.6       Vlan100  ADD DONE   301
```

The following partial output from the **show rise detail** command includes all of the APBR entries that were automatically added to the Cisco Nexus 5600 Series switch:

```
switch# show rise detail

RISE module name: MPX
  State: active
  Admin state: enabled
  Interface: Po10
  Mode: direct
  Slot id: 300
  Service token: 0x6
  Serial number: AJSFH28FUF
  SUP IP: 10.175.1.99
  RISE IP: 10.175.1.11
  VDC id: 1
  VLAN: 175
  VLAN group: N/A
  VLAN list: N/A
  Data Interface: N/A

RISE module name: Emu
  State: active
  Admin state: enabled
  Interface: N/A
  Mode: indirect
  Slot id: 301
  Service token: 0x7
  Serial number: 123-SERIAL
  SUP IP: 100.0.1.1
  RISE IP: 100.0.1.4
  VDC id: 1
  VLAN: 100
  VLAN group: N/A
  VLAN list: N/A
  Data Interface: N/A

RISE module name: VPX
  State: active
  Admin state: enabled
  Interface: N/A
  Mode: indirect
  Slot id: 302
  Service token: 0x8
  Serial number: HE2H81UJ47
  SUP IP: 100.0.1.1
  RISE IP: 100.0.1.6
  VDC id: 1
  VLAN: 100
  VLAN group: N/A
  VLAN list: N/A
  Data Interface: N/A

APBR Configuration
rs ip           rs port protocol nhop ip         rs nhop  apbr state slot-id
--------------- ------- -------- --------------- -------- ---------- -------
100.0.1.1       33275   TCP      100.0.1.2       Vlan100  ADD FAIL   301
100.0.1.3       64301   TCP      100.0.1.4       Vlan100  ADD DONE   301
100.0.1.5       21743   TCP      100.0.1.6       Vlan100  ADD DONE   301
```

The following partial output from the **show service rise auto-pbr** command lists all APBR entries on the Cisco Nexus 5600 Series switch:

```
switch# show service rise ipv4 auto-pbr slot 301

APBR routes added by slot 301
rs ip            port    protocol  nhop ip          rs nexthop inf
---------------  ------  --------  ---------------  --------------
100.0.1.1        33275   TCP       100.0.1.2        Vlan100
100.0.1.3        64301   TCP       100.0.1.4        Vlan100
100.0.1.5        21743   TCP       100.0.1.6        Vlan100
```

Feature History for Auto Policy-Based Routing

The following table lists the feature history for this feature.

Table 2: Feature History for APBR

Feature Name	Release	Feature Information
Auto policy-based routing (APBR)	Cisco NX-OS 7.1(1)N1(1)	Support for this feature was introduced on the Cisco Nexus 5600 Series switches.
Appliance high availability		
APBR on vPC		