PfR Target Discovery v1.0

The Performance Routing Target Discovery v1.0 feature introduces a scalable solution for managing the performance of video and voice applications across large enterprise branch networks by automating the identification and configuration of IP SLA responders and optimizing the use of Performance Routing (PfR) active probes. To optimize media applications using voice and video traffic, PfR uses jitter, loss, and delay measurements. The IP SLA udp-jitter probe provides these measurements but requires an IP SLA responder. Manual configuration of the IP SLA responder address for each destination prefix leads to scalability issues for large enterprise branch networks. The PfR Target Discovery v1.0 feature introduces master controller (MC) peering and uses Service Routing (SR) through EIGRP Service Advertisement Framework (SAF) to advertise, discover, and autoconfigure IP SLA responders and associated destination IP prefixes.

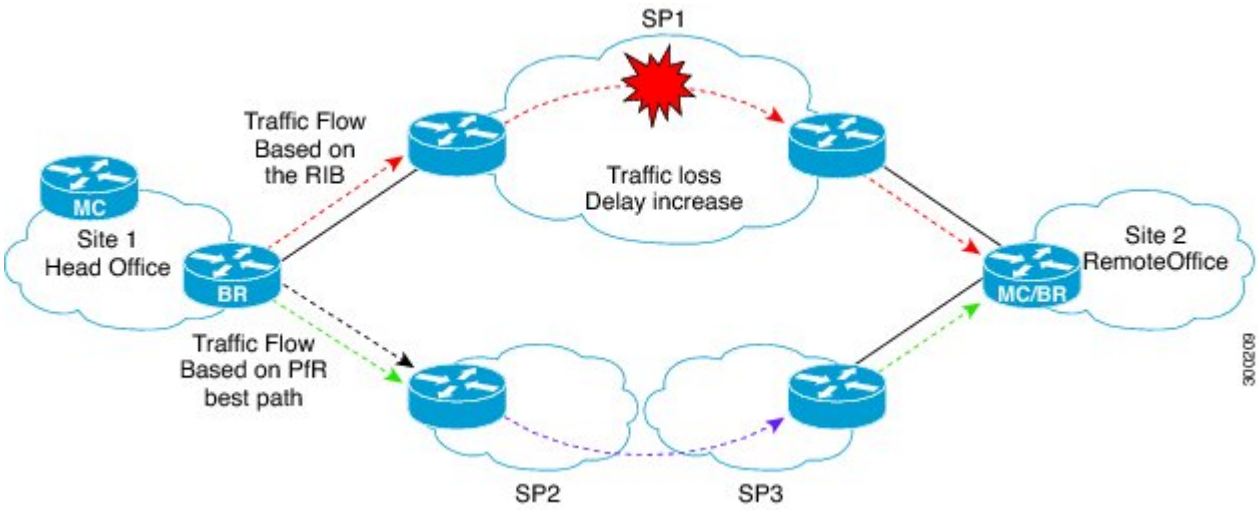
Information About PfR Target Discovery

PfR Target Discovery

Cisco Performance Routing (PfR) complements classic IP routing technologies by adding intelligence to select best paths to meet application performance requirements. The figure below illustrates the difference between PfR and classic IP routing technologies. In the figure below, the traffic is running from the head office at Site 1 to a remote office at Site 2. Traditional routing technologies would use the routing table information and route the traffic through Service Provider 1 because of the shorter path. If, however, there is heavy congestion leading to traffic loss and an increased delay through SP1, a traditional routing technology cannot see the performance degradation and will continue to route the traffic through SP1. PfR routes traffic across the network using a best path determined by data measurements such as reachability, delay, loss. jitter, MOS, throughput, and load, with the ability to consider monetary cost and user-defined policies. Unlike classic IP routing technologies, PfR provides adaptive routing adjustments based on real-time performance metrics. In the figure below, for example, PfR reroutes the traffic through SP2 and SP3 as the best path because of the poor performance measurements of traffic through SP1.

Note The network diagram below relates to both SPs within an MPLS VPN network and Internet Service Providers (ISPs) for a smaller enterprise network.

Figure 1: PfR Versus Classic Routing Technologies



To optimize voice and video applications, PfR uses jitter, loss, and delay measurements to determine the best media path. The IP SLA udp-jitter probe provides these measurements but requires an IP SLA responder. PfR needs to know the IP address of the nearest IP SLA responder to the destination prefix for a voice and video traffic class. Manual configuration of IP SLA responders for each destination IP prefix range within each PfR application policy is not seen as a scalable solution in Enterprise networks with hundreds or potentially thousands of branch sites over the WAN.

To address these manual configuration issues, PfR target-discovery introduces master controller peering and uses EIGRP Service Advertisement Facility (SAF) to advertize IP SLA responder IP addresses to allow automatic discovery and configuration of the responders and associated destination IP prefix ranges.

Target Discovery Data Distribution

PfR target discovery uses a data distribution mechanism that introduces two benefits:

- Reduces IP SLA target configuration per destination and per policy.
- Improves IP SLA probing efficiency by sharing probe data across multiple policies.

Each PfR master controller (MC) running target discovery advertises the local known IP prefix ranges and local IP SLA responder(s) for other MCs to discover or learn over the WAN. Each MC running target discovery also learns advertised IP SLA responders and associated destination IP prefix ranges from other MCs to dynamically configure policies requiring probe data from IP SLA responders. PfR uses the Cisco Service Routing (SR) and Service Advertisement Framework (SAF) to distribute and discover IP SLA target information.

For more details about SAF, see the *Service Advertisement Framework Configuration Guide*.

Master Controller Peering Using SAF

PfR master controller peering runs over Service Advertisement Framework (SAF). Using Service Routing (SR) forwarders on each master controller to establish peering between MCs at different sites, MC peering allows the advertisement and discovery of PfR target discovery data.

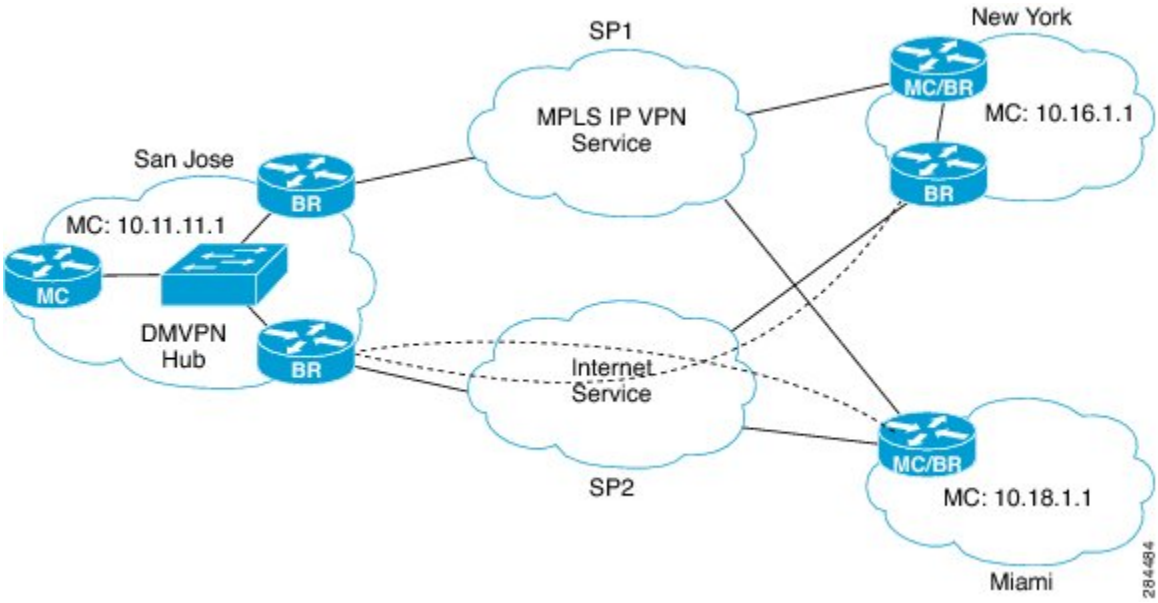
The target-discovery-enabled MCs at the hub site (known as a headend) and at the branch office serve as both an SR internal client and an SR forwarder. Before any of the target discovery services can be advertised, the MCs must be configured as SR forwarders and for SR peering. After MC peering is established, an MC can advertise local information to allow other MCs to perform target discovery and autoconfigure.

Every customer network deployment is different, and with each deployment there are various methods to configure an SR topology configuration. The deployment model used by the customer for the network dictates how the SR forwarder must be configured. The MC-MC peering aspect of the target discovery feature supports two different customer network deployments:

- Multihop—Networks in which the customer headend and branch offices are separated by one or more routers not under the administrative control of the customer or not SAF-enabled. An example would be an MPLS VPN WAN service.
- SAF-Everywhere—Networks in which all routers are enabled for EIGRP SAF in a contiguous path from the headend MC to the branch office MC. An example would be a DMVPN WAN.

The topology in the figure below illustrates an example deployment of MC peering in a multihop type of network. The hub site (San Jose) MC and the branch office sites (New York and Miami) MC systems peer across a logical unicast topology. In this model, the hub site and branch sites are separated by a network—typically a Service Provider (SP)—where EIGRP SR forwarders are not configured.

Figure 2: Multihop Network Topology with MPLS IP VPN and DMVPN

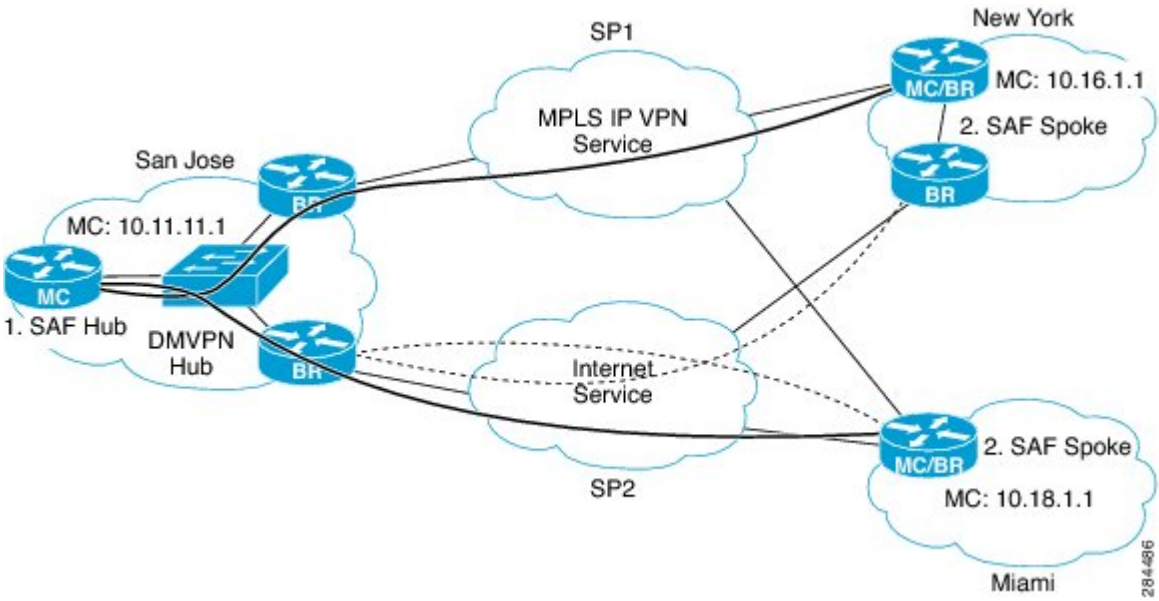


The figure below shows PfR target discovery implemented in the same enterprise WAN network as in the figure above running MPLS IP VPN and DMVPN. After MC peering is enabled, the San Jose master controller is the SAF hub forwarder and the New York and Miami MCs peer with the San Jose MC. Target discovery allows each MC to advertise local IP prefixes and IP SLA responders using SAF, and each MC learns the

remote IP prefixes and IP SLA responders from SAF. PfR probes the remote-site IP SLA responders to measure the network performance.

MC peering over a multihop network is an overlay model similar to a BGP route reflector. The MC peering system must configure a source loopback interface with an IP address that is reachable (routed) through the network.

Figure 3: MC Peering and Target Discovery Enabled in a Multihop Enterprise WAN Network



Master Controller Peering Configuration Options

Each PfR master controller (MC) running target discovery advertises the local known IP prefix ranges and local IP SLA responder(s) for other MCs to discover or learn over the WAN. Each MC running target discovery also learns advertised IP SLA responders and associated destination IP prefix ranges from other MCs to dynamically configure policies requiring probe data.

Depending on the network structure and the degree of control required over the configuration of probe targets and IP SLA responders, there are three main options available when configuring MC peering using the **mc-peer** command:

- Configuring the headend (at the hub site) or the peer IP address (at the branch site). When using this option, configuring a loopback interface as the source of EIGRP SAF adjacency is recommended. This configuration option is used in the multihop type of network.
- Configuring a SAF domain ID or using the default SAF domain ID of 59501. This option requires EIGRP SAF configuration on both hub-site and branch-site master controller routers and can be used in the SAF-everywhere type of network.
- Configuring the EIGRP option where there is no autoconfiguration of EIGRP SAF. This option is used in the SAF-everywhere type of network. If SAF is already configured on routers in the network, you can use the same network and overlay PfR target discovery. Please refer to the SAF configuration guide to learn how to configure SAF independent of PfR target discovery.

How to Configure PfR Target Discovery

Configuring PfR Target Discovery and MC Peering for a Hub Site in Multihop Networks

Perform this task to configure PfR master controller (MC) peering at the master controller at the headend of the network, usually a hub site master controller. The master controller must be a device with routing capability. This task assumes a multihop type of network where the network cloud between the hub site and the branch sites is not under the control of the customer or is not SAF-enabled. In this design, the hub site MC will be a Service Advertisement Facility (SAF) forwarder hub with which the branch MC SAF forwarders peer to exchange advertisements. The hub site MC will accept peering requests from branch MCs with the same SAF domain ID and MD5 authentication.

Note In this task, dynamic PfR target discovery is enabled. This method is desirable when SAF is already enabled in the network for other applications or there is existing neighbor adjacency between MCs and SAF. For example, in a DMVPN WAN, if the PfR MCs coexist on the DMVPN tunnel devices, they also have SAF adjacency and do not require static peering.

Note PfR does not support spoke-to-spoke tunneling. Disable spoke-to-spoke dynamic tunnels by configuring the **ip nhrp server-only** command under interface configuration mode as part of the Next Hop Resolution Protocol (NHRP) configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **target-discovery**
5. **mc-peer** [**head-end** | *peer-address*] [**loopback** *interface-number*] [**description** *text*] [**domain** *domain-id*]
6. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**pfr master** **Example:** `Device(config)# pfr master`	Enters PfR master controller configuration mode to configure a Cisco device as a master controller.
Step 4	**target-discovery** **Example:** `Device(config-pfr-mc)# target-discovery`	Configures PfR target discovery. • In this example, dynamic PfR target discovery is configured.
Step 5	**mc-peer** [**head-end** | *peer-address*] [**loopback** *interface-number*] [**description** *text*] [**domain** *domain-id*] **Example:** `Device(config-pfr-mc)# mc-peer head-end loopback1 description SJ-hub`	In this example, the PfR master controller peering is configured to show that this device is the hub (headend) device. • Use the **domain** keyword to specify a SAF domain ID to be used for MC peering. The *domain-id* argument is in the range of 1 to 65535. If the SAF domain ID is not specified, the default value of 59501 is used.
Step 6	**end** **Example:** `Device(config-pfr-mc)# end`	(Optional) Exits PfR master controller configuration mode and returns to privileged EXEC mode.

Configuring PfR Target Discovery and MC Peering for a Branch Office in Multihop Networks

Perform this task to configure PfR MC peering using static mode for PfR target discovery at a branch office that is acting as a spoke router. In this example, the IP address of the PfR master controller hub device at a head office (headend) of the network is configured as a loopback interface to allow MC peering. This task assumes a multihop type of network where the network cloud between the hub site and the branch offices is not under the control of the customer.

Note PfR does not support spoke-to-spoke tunneling. Disable spoke-to-spoke dynamic tunnels by configuring the **ip nhrp server-only** command under interface configuration mode as part of the Next Hop Resolution Protocol (NHRP) configuration.

Before you begin

PfR master controller (MC) peering must be configured on a device with routing capability located at the hub site (headend) of the network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **mc-peer** [*peer-address* **loopback** *interface-number*] [**description** *text*] [**domain** *domain-id*]
5. **target-discovery**
6. **end**

DETAILED STEPS

	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	**pfr master** **Example:** `Device(config)# pfr master`	Enters PfR master controller configuration mode to configure a Cisco device as a master controller.
Step 4	**mc-peer** [*peer-address* **loopback** *interface-number*] [**description** *text*] [**domain** *domain-id*] **Example:** `Device(config-pfr-mc)# mc-peer 10.11.11.1 loopback1`	In this example, the IP address of the PfR master controller hub device at a head office (headend) of the network is configured as the peer address.
Step 5	**target-discovery** **Example:** `Device(config-pfr-mc)# target-discovery`	Configures dynamic PfR target discovery.
Step 6	**end** **Example:** `Device(config-pfr-mc)# end`	(Optional) Exits PfR master controller configuration mode and returns to privileged EXEC mode.

Enabling Static Definition of Targets and IP Prefix Ranges Using PfR Target Discovery

PfR target discovery can dynamically enable IP SLA responders on border devices with routing capability and learn site-specific IP prefix ranges. This information will be advertised from the local PfR master controller (MC) to other MCs. Perform this task to statically configure the IP SLA responder(s) and IP prefix ranges to be advertised by SAF. This task is performed on a master controller at the hub site.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*}
4. Repeat Step 3 to create prefix lists as needed.
5. **pfr master**
6. **target-discovery responder-list** *prefix-list-name* [**inside-prefixes** *prefix-list-name*]
7. **end**

DETAILED STEPS

	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	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} **Example:** `Device(config)# ip prefix-list ipfx permit 10.101.1.0/24`	Creates an IP prefix list of target prefixes for active probes. • An IP prefix list is used under learn list configuration mode to filter IP addresses that are learned. • The example creates an IP prefix list named ipfx in order for PfR to profile the prefix 10.101.1.0/24.
Step 4	Repeat Step 3 to create prefix lists as needed.	—
Step 5	**pfr master** **Example:** `Device(config)# pfr master`	Enters PfR master controller configuration mode to configure a Cisco device with routing capability as a master controller.
Step 6	**target-discovery responder-list** *prefix-list-name* [**inside-prefixes** *prefix-list-name*]	Configures PfR target discovery.

	Command or Action	Purpose
	Example: `Device(config-pfr-mc)# target-discovery responder-list tgt inside-prefixes ipfx`	• In this example, PfR target discovery is configured with static configuration of the IP SLA responder and inside prefix IP addresses.
Step 7	**end** **Example:** `Device(config-pfr-mc)# end`	(Optional) Exits PfR master controller configuration mode and returns to privileged EXEC mode.

Example

In this example, the hub device is a hub site master controller as shown in the prompts. For the example configuration of the spoke (branch office) devices, see the "Configuration Examples" section.

```
Device-hub> enable
Device-hub# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device-hub(config)# ip prefix-list ipfx permit 10.101.1.0/24
Device-hub(config)# ip prefix-list ipfx permit 10.101.2.0/24
Device-hub(config)# ip prefix-list tgt permit 10.101.1.1/32
Device-hub(config)# ip prefix-list tgt permit 10.101.1.2/32
Device-hub(config)# pfr master
Device-hub(config-pfr-mc)# mc-peer head-end loopback1
Device-hub(config-pfr-mc)# target-discovery responder-list tgt inside-prefixes ipfx
Device-hub(config-pfr-mc)# end
```

Displaying PfR Target Discovery Information

After configuring the PfR Target Discovery feature, enter the commands in this task to view information about local and remote master controller peers, responder lists, inside prefixes, and SAF domain IDs.

SUMMARY STEPS

1. **enable**
2. **show pfr master target-discovery**
3. **show pfr master active-probes target-discovery**
4. **debug pfr master target-discovery**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Device> enable
```

Step 2 **show pfr master target-discovery**

This command is used to display information about traffic classes that are monitored and controlled by a PfR master controller. In this example, the command is entered at the hub (head office) master controller and displays information about local and remote networks, domain IDs for the SAF configuration, and master controller peers. Information in the output section labeled (local) is advertised to other MCs, and information in the output section labeled (remote) is learned from other MCs through SAF.

Example:

```
Device# show pfr master target-discovery

PfR Target-Discovery Services
 Mode: Static  Domain: 59501
 Responder list: tgt  Inside-prefixes list: ipfx
 SvcRtg: client-handle: 3  sub-handle: 2  pub-seq: 1

PfR Target-Discovery Database (local)

 Local-ID: 10.11.11.1        Desc: Router-hub
   Target-list: 10.101.1.2, 10.101.1.1
   Prefix-list: 10.101.2.0/24, 10.101.1.0/24

PfR Target-Discovery Database (remote)

 MC-peer: 10.18.1.1         Desc: Router-spoke2
   Target-list: 10.121.1.2, 10.121.1.1
   Prefix-list: 10.121.2.0/26, 10.121.1.0/24

 MC-peer: 10.16.1.1         Desc: Router-spoke1
   Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
   Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24
```

Step 3 **show pfr master active-probes target-discovery**

This command is used to display the status of all active probes and the probe targets learned using target discovery. In this example, the command is entered at the hub (head office) master controller and displays information about two MC peers, listing the type of probe and the target IP addresses.

Example:

```
Device# show pfr master active-probes target-discovery

PfR Master Controller active-probes (TD)
Border = Border Router running this probe
MC-Peer = Remote MC associated with this target
Type = Probe Type
Target = Target Address
TPort = Target Port
N - Not applicable

Destination Site Peer Addresses:

MC-Peer           Targets
10.16.1.1         10.111.1.2, 10.111.1.1
10.18.1.1         10.121.1.1

The following Probes are running:

Border          Idx  State     MC-Peer           Type     Target          TPort
10.16.1.3       27   TD-Actv   10.16.1.1         jitter   10.111.1.2      5000
10.16.1.2       14   TD-Actv   10.16.1.1         jitter   10.111.1.2      5000
```

```
10.16.1.3       27   TD-Actv   10.16.1.1          jitter   10.111.1.1       5000
10.16.1.2       14   TD-Actv   10.16.1.1          jitter   10.111.1.1       5000
10.18.1.1       14   TD-Actv   10.18.1.1          jitter   10.121.1.1       5000
10.18.1.1       27   TD-Actv   10.18.1.1          jitter   10.121.1.1       5000
```

Step 4 **debug pfr master target-discovery**

This command is used to display debugging messages that can help troubleshoot issues. The example below shows the PfR messages after a master controller peering command, **mc-peer**, has been issued, changing the MC peering designation and causing PfR target discovery to be shut down and restarted.

Example:

```
Device# debug pfr master target-discovery

PfR Master Target-Discovery debugging is on
Device# configure terminal
Device(config)# pfr master
Device(config-pfr-mc)# mc-peer description branch office

*Oct 26 20:00:34.084: PFR_MC_TD: mc-peer cli chg, op:0/1 idb:0/115967296 ip:0.0.0.0/0.0.0.0
 dom:59501/45000
*Oct 26 20:00:34.084: PFR_MC_TD: mc-peer cli transition, shutting down TD
*Oct 26 20:00:34.084: PFR_MC_TD: TD teardown start, mode:4
*Oct 26 20:00:34.084: PFR_MC_TD: SvcUnreg: handle:5
*Oct 26 20:00:34.084: PFR_MC_TD: TD teardown fin, mode:4
*Oct 26 20:00:35.089: PFR_MC_TD: mc-peer cli enabled, starting TD, domain:59501
*Oct 26 20:00:35.089: PFR_MC_TD: TD startup, origin:192.168.3.1 handle:0 dyn_pid:4294967295
*Oct 26 20:00:35.089: PFR_MC_TD: Static mode start <-------
*Oct 26 20:00:35.090: PFR_MC_TD: Static Target list: 10.101.1.2, 10.101.1.1
*Oct 26 20:00:35.090: PFR_MC_TD: Static Prefix list: 10.101.2.0/24, 10.101.1.0/24
*Oct 26 20:00:35.090: PFR_MC_TD: SvcReg: handle:7
*Oct 26 20:00:35.093: PFR_MC_TD: SvcSub: success  102:1:FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF
*Oct 26 20:00:35.093: PFR_MC_TD: SvcSub: handle:7 subscription handle:6
*Oct 26 20:00:35.093: PFR_MC_TD: local data encode, pre-publish
*Oct 26 20:00:35.094: PFR_MC_TD: SvcPub: success  102:1:0.0.0.C0A80301
*Oct 26 20:00:35.094: PFR_MC_TD: SvcPub: handle:7 size:336 seq:3 reach via 192.168.3.1
*Oct 26 20:00:35.094: PFR_MC_TD: prereqs met, origin:192.168.3.1 handle:7 sub:6 pub(s:1/r:0)
```

Configuration Examples for PfR Target Discovery

Example: Configuring PfR Target Discovery in Multihop Networks in Dynamic Mode

The following configuration can be used in multihop networks where the network cloud between the head office and branch offices or remote sites is not controlled by the customer or is not SAF-enabled. Configuration examples are shown for three master controllers, one at the head office and two branch offices. Master controller peering is established between the three master controller routers and PfR target discovery is configured using dynamic mode. Output for the **show pfr master target-discovery** command is shown for all three sites.

Note In the following examples, the hub and spoke device host names were configured as "Router-hub," "Router-spoke1," or "Router-spoke2" but the device can be any device with routing capability that supports PfR.

Hub MC Peering and Target Discovery Configuration

The hub device has routing capability and is in the head office. In this example, the master controller peering is configured using the **head-end** keyword to show that this device is the hub device. A loopback interface must be specified and is used as the source of the EIGRP SAF adjacency.

```
Router-hub> enable
Router-hub# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-hub(config)# pfr master
Router-hub(config-pfr-mc)# mc-peer head-end Loopback1
Router-hub(config-pfr-mc)# target-discovery
Router-hub(config-pfr-mc)# end
```

Spoke1 MC Peering and Target Discovery Configuration

The spoke1 device has routing capability and is in the New York branch office. In this example, the master controller peering is configured to peer with the IP address (10.11.11.1) of the hub device.

```
Router-spoke1> enable
Router-spoke1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-spoke1(config)# pfr master
Router-spoke1(config-pfr-mc)# mc-peer 10.11.11.1 Loopback1
Router-spoke1(config-pfr-mc)# target-discovery
Router-spoke1(config-pfr-mc)# end
```

Spoke2 MC Peering and Target Discovery Configuration

The spoke2 device has routing capability and is in the Miami branch office. In this example, the master controller peering is configured to peer with the IP address (10.11.11.1) of the hub device.

```
Router-spoke2> enable
Router-spoke2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-spoke2(config)# pfr master
Router-spoke2(config-pfr-mc)# mc-peer 10.11.11.1 Loopback1
Router-spoke2(config-pfr-mc)# target-discovery
Router-spoke2(config-pfr-mc)# end
```

Example Output for PfR Target Discovery Using Static Mode

The following output is for the hub device after PfR target discovery is configured in dynamic mode:

```
Router-hub# show pfr master target-discovery

PfR Target-Discovery Services
 Mode: Dynamic  Domain: 59501
 Responder list: tgt  Inside-prefixes list: ipfx
```

```
 SvcRtg: client-handle: 3  sub-handle: 2  pub-seq: 1

PfR Target-Discovery Database (local)

 Local-ID: 10.11.11.1        Desc: Router-hub
   Target-list: 10.101.1.2, 10.101.1.1
   Prefix-list: 10.101.2.0/24, 10.101.1.0/24

PfR Target-Discovery Database (remote)

 MC-peer: 10.18.1.1         Desc: Router-spoke2
   Target-list: 10.121.1.2, 10.121.1.1
   Prefix-list: 10.121.2.0/26, 10.121.1.0/24

 MC-peer: 10.16.1.1         Desc: Router-spoke1
   Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
   Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24
```

The following output is for the spoke1 device after PfR target discovery is configured in dynamic mode:

```
Router-spoke1# show pfr master target-discovery

PfR Target-Discovery Services
 Mode: Dynamic  Domain: 59501
 Responder list: tgt  Inside-prefixes list: ipfx
 SvcRtg: client-handle: 3  sub-handle: 2  pub-seq: 1

PfR Target-Discovery Database (local)

 Local-ID: 10.16.1.1        Desc: Router-spoke1
   Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
   Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24

PfR Target-Discovery Database (remote)

 MC-peer: 10.11.11.1         Desc: Router-hub
   Target-list: 10.101.1.2, 10.101.1.1
   Prefix-list: 10.101.2.0/24, 10.101.1.0/24

 MC-peer: 10.18.1.1         Desc: Router-spoke2
   Target-list: 10.121.1.2, 10.121.1.1
   Prefix-list: 10.121.2.0/26, 10.121.1.0/24
```

The following output is for the spoke2 device after PfR target discovery is configured in dynamic mode:

```
Router-spoke2# show pfr master target-discovery

PfR Target-Discovery Services
 Mode: Dynamic  Domain: 59501
 Responder list: tgt  Inside-prefixes list: ipfx
 SvcRtg: client-handle: 3  sub-handle: 2  pub-seq: 1

PfR Target-Discovery Database (local)

 Local-ID: 10.18.1.1        Desc: Router-spoke2
   Target-list: 10.121.1.2, 10.121.1.1
   Prefix-list: 10.121.2.0/26, 10.121.1.0/24

PfR Target-Discovery Database (remote)

 MC-peer: 11.11.11.1         Desc: Router-hub
   Target-list: 10.101.1.2, 10.101.1.1
   Prefix-list: 10.101.2.0/24, 10.101.1.0/24
```

```
 MC-peer: 10.16.1.1         Desc: Router-spoke1
   Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
   Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24
```

Example: Configuring PfR Target Discovery in SAF-Everywhere Networks Using Dynamic Mode

The following example configuration can be used in networks where all the routing-capable devices between the PfR MCs are configured to support SAF. In this model, the hub site and branch sites are separated by a network—typically a Service Provider (SP) network—where EIGRP SR forwarders are configured and all devices are SAF-enabled. The MC peering over a SAF-Everywhere type of network is similar to EIGRP peering between adjacent neighbors.

Configuration examples are shown for two master controllers, one at the head office and one at a branch office. Master controller peering is established between the two master controller routers, and PfR target discovery is enabled in dynamic mode at the head and branch offices.

Note For clarity, the configuration is shown without command prompts.

Head Office Master Controller Configuration

At the head office (head-end) router, the master controller peering is enabled and PfR target discovery is configured in dynamic mode. The SAF configuration is shown here under the **service-family** command section, and this configuration is assumed to exist before the PfR MC peering and target discovery overlay configuration is added.

```
key chain metals
 key 1
   key-string gold
!
pfr master
 mc-peer
 target-discovery
 no keepalive
 !
 border 10.1.1.2 key-chain metals
  interface Ethernet0/2 external
  interface Ethernet0/3 external
  interface Ethernet0/0 internal
  interface Ethernet0/1 internal
 !
 learn
 throughput
 periodic-interval 0
 monitor-period 1
 delay threshold 100
 mode route control
 mode select-exit best

interface Loopback1
 ip address 10.100.100.101 255.255.255.255
!
interface Ethernet0/0
```

```
 ip address 10.1.1.1 255.255.255.0
!
router eigrp
 !
 service-family ipv4 autonomous-system 59501
  !
 remote-neighbors source Loopback1 unicast-listen
 exit-service-family
```

Branch Office Master Controller Configuration

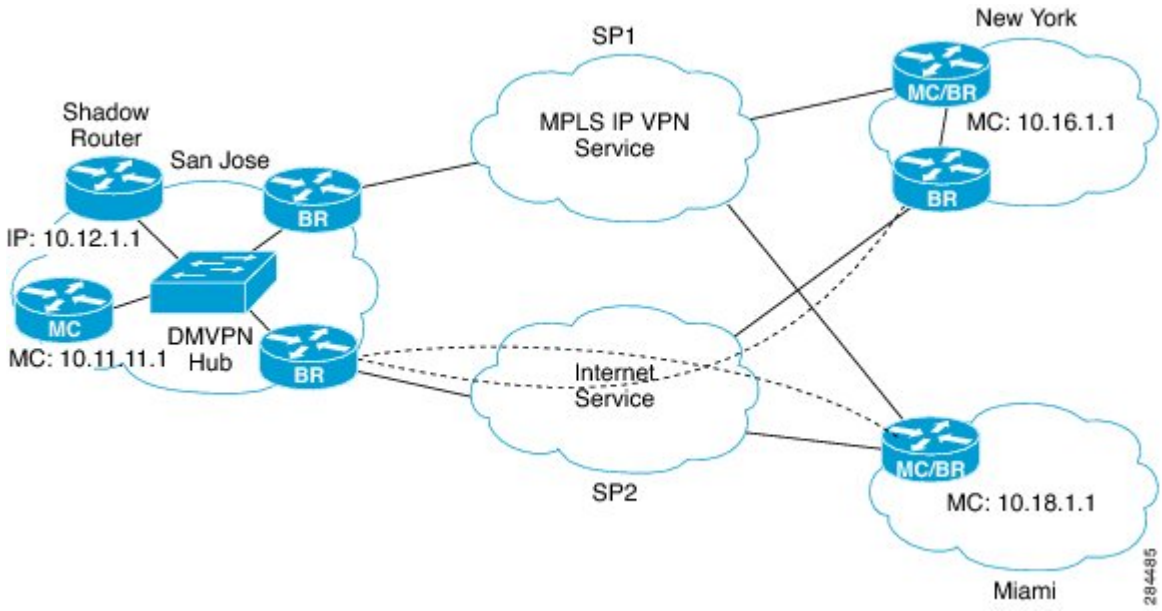
At the branch office router, the master controller peering is enabled and PfR target discovery is configured in dynamic mode.

```
key chain metals
 key 1
   key-string gold
pfr master
 mc-peer
 target-discovery
 !
 border 172.16.1.3 key-chain metals
  interface Ethernet0/0 external
  interface Ethernet0/1 external
  interface Ethernet0/2 internal
  interface Ethernet0/3 internal
 !
 learn
 throughput
 periodic-interval 0
 monitor-period 1
!
interface Loopback1
 ip address 172.16.100.121 255.255.255.255
!
interface Ethernet0/2
 ip address 172.16.1.4 255.255.255.0
!
router eigrp
 !
 service-family ipv4 autonomous-system 59501
  !
 neighbor 10.100.100.101 Loopback1 remote 10
 exit-service-family
```

Example: Configuring PfR Target Discovery Using Static Definition of Targets and IP Prefix Ranges

The following configuration example can be used when you want to specify the IP SLA responders and IP prefix ranges to be advertised by SAF. This configuration can be performed in multihop networks where the network cloud between the head office and the branch offices or remote sites is not SAF-enabled. In the figure below, a shadow router is configured as the hub site. A shadow router is a dedicated router used as an IP SLA responder—a source of IP SLA measurement. Configuration examples are shown for three master controllers, one at the head office and two at branch offices. Master controller peering is established between the three master controller routers, and prefix lists are configured to identify the local responders and inside prefixes at each site. Output from the **show pfr master target-discovery** command is shown for all three sites.

Figure 4: Multihop with Shadow Router Network Topology with MPLS IP VPN and DMVPN



Hub MC Peering and Target Discovery Configuration

The hub router is in the Head Office. In this example, the master controller peering is configured using the **head-end** keyword to show that this router is the hub router. A loopback interface must be specified and is used as the source of the EIGRP SAF adjacency.

Note In the following examples, the hub and spoke device host names were configured as "Router-hub," "Router-spoke1," or "Router-spoke2" but the device can be any device with routing capability that supports PfR.

```
Router-hub> enable
Router-hub# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-hub(config)# ip prefix-list ipfx permit 10.101.1.0/24
Router-hub(config)# ip prefix-list ipfx permit 10.101.2.0/24
Router-hub(config)# ip prefix-list tgt permit 10.101.1.1/32
Router-hub(config)# ip prefix-list tgt permit 10.101.1.2/32
Router-hub(config)# pfr master
Router-hub(config-pfr-mc)# mc-peer head-end loopback1
Router-hub(config-pfr-mc)# target-discovery responder-list tgt inside-prefixes ipfx
Router-hub(config-pfr-mc)# end
```

Spoke1 MC Peering and Target Discovery Configuration

The spoke1 router is in the New York branch office. In this example, the master controller peering is configured to peer with the IP address (10.12.1.1) of the shadow (hub) router.

```
Router-spoke1> enable
Router-spoke1# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router-spoke1(config)# ip prefix-list ipfx permit 10.111.1.0/24
Router-spoke1(config)# ip prefix-list ipfx permit 10.111.2.0/26
Router-spoke1(config)# ip prefix-list tgt permit 10.111.3.1/32
Router-spoke1(config)# !
Router-spoke1(config)# pfr master
Router-spoke1(config-pfr-mc)# mc-peer 10.12.1.1 loopback1
Router-spoke1(config-pfr-mc)# target-discovery responder-list tgt inside-prefixes ipfx
Router-spoke1(config-pfr-mc)# end
```

Spoke2 MC Peering and Target Discovery Configuration

The spoke2 router is in the Miami branch office. In this example, the master controller peering is configured to peer with the IP address (10.12.1.1) of the shadow (hub) router.

```
Router-spoke2> enable
Router-spoke2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-spoke2(config)# ip prefix-list ipfx permit 10.121.1.0/24
Router-spoke2(config)# ip prefix-list ipfx permit 10.121.2.0/26
Router-spoke2(config)# ip prefix-list tgt permit 10.121.1.1/32
Router-spoke2(config)# ip prefix-list tgt permit 10.121.2.1/32
Router-spoke2(config)# pfr master
Router-spoke2(config-pfr-mc)# mc-peer 10.12.1.1 loopback1
Router-spoke2(config-pfr-mc)# target-discovery responder-list tgt inside-prefixes ipfx
Router-spoke2(config-pfr-mc)# end
```

Example Output for PfR Target Discovery Using Static Mode

The following output is for the hub router after PfR target discovery is configured in static mode:

```
Router-hub# show pfr master target-discovery

PfR Target-Discovery Services
 Mode: Static  Domain: 59501
 Responder list: tgt  Inside-prefixes list: ipfx
 SvcRtg: client-handle: 3  sub-handle: 2  pub-seq: 1

PfR Target-Discovery Database (local)

 Local-ID: 10.12.1.1        Desc: Router-hub
   Target-list: 10.101.1.2, 10.101.1.1
   Prefix-list: 10.101.2.0/24, 10.101.1.0/24

PfR Target-Discovery Database (remote)

 MC-peer: 10.18.1.1         Desc: Router-spoke2
   Target-list: 10.121.1.2, 10.121.1.1
   Prefix-list: 10.121.2.0/26, 10.121.1.0/24

 MC-peer: 10.16.1.1         Desc: Router-spoke1
   Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
   Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24
```

The following output is for the spoke1 router after PfR target discovery is configured in static mode:

```
Router-spoke1# show pfr master target-discovery

PfR Target-Discovery Services
 Mode: Static  Domain: 59501
```

```
 Responder list: tgt  Inside-prefixes list: ipfx
 SvcRtg: client-handle: 3  sub-handle: 2  pub-seq: 1

PfR Target-Discovery Database (local)

 Local-ID: 10.16.1.1        Desc: Router-spoke1
   Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
   Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24

PfR Target-Discovery Database (remote)

 MC-peer: 10.12.1.1         Desc: Router-hub
   Target-list: 10.101.1.2, 10.101.1.1
   Prefix-list: 10.101.2.0/24, 10.101.1.0/24

 MC-peer: 10.18.1.1         Desc: Router-spoke2
   Target-list: 10.121.1.2, 10.121.1.1
   Prefix-list: 10.121.2.0/26, 10.121.1.0/24
```

The following output is for the spoke2 router after PfR target discovery is configured in static mode:

```
Router-spoke2# show pfr master target-discovery

PfR Target-Discovery Services
 Mode: Static  Domain: 59501
 Responder list: tgt  Inside-prefixes list: ipfx
 SvcRtg: client-handle: 3  sub-handle: 2  pub-seq: 1

PfR Target-Discovery Database (local)

 Local-ID: 10.18.1.1        Desc: Router-spoke2
   Target-list: 10.121.1.2, 10.121.1.1
   Prefix-list: 10.121.2.0/26, 10.121.1.0/24

PfR Target-Discovery Database (remote)

 MC-peer: 10.12.1.1         Desc: Router-hub
   Target-list: 10.101.1.2, 10.101.1.1
   Prefix-list: 10.101.2.0/24, 10.101.1.0/24

 MC-peer: 10.16.1.1         Desc: Router-spoke1
   Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
   Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco IOS PfR commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Performance Routing Command Reference
Basic PfR configuration for Cisco IOS XE releases	“Configuring Basic Performance Routing” module

Related Topic	Document Title
Information about configuration for the border router only functionality for Cisco IOS XE Releases 3.1 and 3.2	"Performance Routing Border Router Only Functionality" module
Concepts required to understand the Performance Routing operational phases for Cisco IOS XE releases	"Understanding Performance Routing" module
Advanced PfR configuration for Cisco IOS XE releases	"Configuring Advanced Performance Routing" module
IP SLAs overview	"Cisco IOS IP SLAs Overview" module
PfR home page with links to PfR-related content on our DocWiki collaborative environment	PfR:Home

MIBs

MIB	MIBs Link
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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 PfR Target Discovery

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 PfR Target Discovery

Feature Name	Releases	Feature Information
PfR Target Discovery v1.0	Cisco IOS XE Release 3.5S	The PfR Target Discovery feature introduces a scalable solution for managing the performance of video and voice applications across large Enterprise branch networks by automating the identification and configuration of IP SLA responders. The following commands were introduced or modified: **debug pfr master target-discovery**, **mc-peer**, **show pfr master active-probes**, **show pfr master target-discovery**, and **target-discovery**.