

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Learn-List](#)

[Pfr-Map](#)

[Link-Group](#)

[Network Diagram](#)

[Relevant Configuration](#)

[Verify](#)

[Case 1: Delay on MPLS and INET Cloud is Same and Within Policy Limits](#)

[Case 2: Delay on MPLS and INET Cloud is Different and Crosses the Policy Limits](#)

[Case 3: Delay on INET Cloud Sees Increase of 100 msec](#)

[Troubleshoot](#)

Introduction

This document describes how learn lists and maps are defined and used in Performance Routing version 2 (PfRv2) in order to affect traffic flow for prefixes.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of PfR.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Learn-List

The learn-list feature in PfRv2 allows the router to learn and group certain traffic classes. An enterprise network is comprised of various types of traffic which includes application, voice, video and so on. Learn-list gives the flexibility to group this traffic as per network requirements. Categorize and group of traffic in learn-lists is generally achieved with an access-list that

matches some specific Differentiated Services Code Point (DSCP) value, however a prefix-list can also be used to match prefixes. This is an example of learn-list that learns and groups traffic based on DSCP value "ef".

A learn list can be subjected to any user defined policy. This is generally achieved with a pfr-map.

Pfr-Map

Pfr-map helps you to define a policy which comprises of a set of parameters. Traffic categorized or grouped via learn-list is then mapped to an individual sequence of a pfr-map. These are some parameters that could be defined using pfr-maps.

- Delay
- Loss
- Unreachable
- Jitter
- Mean Opinion Scores (MOS)

Note: Delay will be used as the key parameter for the rest of this document

A Pfr-Map can have multiple sequence numbers like a route-map and each sequence number can reference a different learn-list.

Link-Group

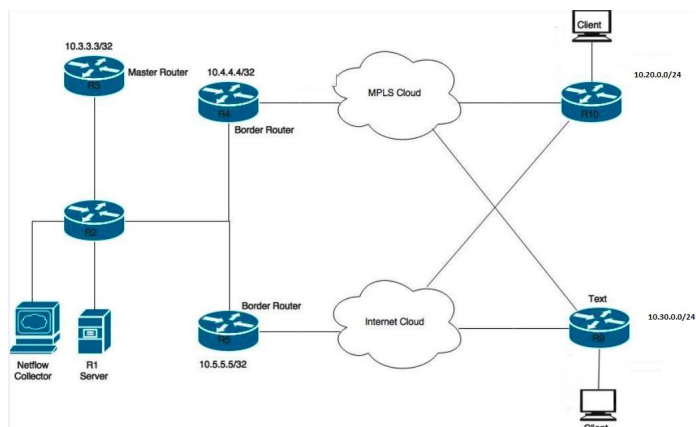
Link-Groups are used to group external interfaces so the traffic could be pushed out of the exit link of the selected border router (BR). A failover link-group can also be defined to do switchover in case the primary link-group goes out of policy. For example, this configuration defines link-group in this fashion:

```
set link-group INET fallback MPLS
```

This configuration statement used in pfr-map PFR under sequence 20 defines all DATA traffic to pass through INET as long as INET is in INPOLICY state. In case of a policy breach, traffic will failover to the MPLS link.

Network Diagram

This image provides a sample topology for the configuration examples:



Devices shown in the diagram:

R1 Server - Initiates traffic.

R3 - PfR Master Router.

R4 & R5 - PfR Border Router.

Clients connected to R9 and R10 are devices that receive the traffic from R1 server.

Relevant Configuration

For the previous scenario two learn lists will be configured, one for application (APPLICATION-LEARN-LIST) and the other for data (DATA-LEARN-LIST) traffic respectively. This scenario uses a prefix-list in order to define traffic. An access-list can also be used to match traffic types like TCP, UDP, Internet Control Message Protocol (ICMP) and so on. Other options like DSCP, Type of Service (ToS) and so on can also be used in order to match the traffic.

```
key chain pfr
  key 0
  key-string cisco
!
policy-rules PFR
!
  border 10.4.4.4 key-chain pfr
  interface Ethernet0/0 internal
  interface Ethernet0/1 external
  link-group MPLS
!
  border 10.5.5.5 key-chain pfr
  interface Ethernet0/0 internal
  interface Ethernet0/1 external
  link-group INET
!
learn
traffic-class filter access-list DENY-ALL
list seq 10 refname APPLICATION-LEARN-LIST
  traffic-class prefix-list APPLICATION
  throughput
list seq 20 refname DATA-LEARN-LIST
  traffic-class prefix-list DATA
  throughput
!
ip prefix-list DATA
  seq 5 permit 10.30.0.0/24
!
ip prefix-list APPLICATION
  seq 5 permit 10.20.0.0/24
!
pfr-map PFR 10
  match pfr learn list APPLICATION-LEARN-LIST
  set periodic 90
  set delay threshold 25
  set mode monitor active
  set resolve delay priority 1 variance 10
  set active-probe echo 10.20.0.12
  set probe frequency 5
  set link-group MPLS fallback INET
!
```

```
pfr-map PFR 20
  match pfr learn list DATA-LEARN-LIST
set periodic 90
  set delay threshold 25
  set mode monitor both
  set resolve delay priority 1 variance 10
  set probe frequency 5
  set link-group INET fallback MPLS
```

Verify

When traffic flows through the network, it matches the corresponding prefix-list and learn-list. Accordingly PFR-Map takes action on traffic as per the parameters defined for every learn-list.

Case 1: Delay on MPLS and INET Cloud is Same and Within Policy Limits

Traffic for prefix 10.20.0.0/24 (Application) is in INPOLICY state and flows via link-group MPLS. Similarly, prefix 10.30.0.0/24 (Data) is also in the INPOLICY state and flows via link-group INET.

```
key chain pfr
  key 0
  key-string cisco
!
policy-rules PFR
!
  border 10.4.4.4 key-chain pfr
  interface Ethernet0/0 internal
  interface Ethernet0/1 external
  link-group MPLS
!
  border 10.5.5.5 key-chain pfr
  interface Ethernet0/0 internal
  interface Ethernet0/1 external
  link-group INET
!
learn
traffic-class filter access-list DENY-ALL
list seq 10 refname APPLICATION-LEARN-LIST
  traffic-class prefix-list APPLICATION
  throughput
list seq 20 refname DATA-LEARN-LIST
  traffic-class prefix-list DATA
  throughput
!
ip prefix-list DATA
  seq 5 permit 10.30.0.0/24
!
ip prefix-list APPLICATION
  seq 5 permit 10.20.0.0/24
!
pfr-map PFR 10
  match pfr learn list APPLICATION-LEARN-LIST
  set periodic 90
  set delay threshold 25
  set mode monitor active
  set resolve delay priority 1 variance 10
  set active-probe echo 10.20.0.12
  set probe frequency 5
  set link-group MPLS fallback INET
!
```

```

pfr-map PFR 20
  match pfr learn list DATA-LEARN-LIST
set periodic 90
  set delay threshold 25
  set mode monitor both
  set resolve delay priority 1 variance 10
  set probe frequency 5
  set link-group INET fallback MPLS

```

Case 2: Delay on MPLS and INET Cloud is Different and Crosses the Policy Limits

There is an increase in delay in the MPLS cloud of about 150 ms. This increase in delay violates the configured threshold delay value of 25 ms as per Pfr-Map statement set delay threshold 25.

This causes Application traffic (10.20.0.0/24) to failover to link-group INET as per the configured statement set link-group MPLS fallback INET. After a period of time, traffic again gets into the INPOLICY state and flows over link-group INET.

Note: There is no effect seen on DATA traffic as its primary path is INET and no delay has been introduced on it.

```

key chain pfr
  key 0
  key-string cisco
!
policy-rules PFR
!
  border 10.4.4.4 key-chain pfr
  interface Ethernet0/0 internal
  interface Ethernet0/1 external
  link-group MPLS
!
  border 10.5.5.5 key-chain pfr
  interface Ethernet0/0 internal
  interface Ethernet0/1 external
  link-group INET
!
learn
  traffic-class filter access-list DENY-ALL
  list seq 10 refname APPLICATION-LEARN-LIST
  traffic-class prefix-list APPLICATION
  throughput
  list seq 20 refname DATA-LEARN-LIST
  traffic-class prefix-list DATA
  throughput
!
ip prefix-list DATA
  seq 5 permit 10.30.0.0/24
!
ip prefix-list APPLICATION
  seq 5 permit 10.20.0.0/24
!
pfr-map PFR 10
  match pfr learn list APPLICATION-LEARN-LIST
  set periodic 90
  set delay threshold 25
  set mode monitor active
  set resolve delay priority 1 variance 10
  set active-probe echo 10.20.0.12

```

```

set probe frequency 5
set link-group MPLS fallback INET
!
pfr-map PFR 20
  match pfr learn list DATA-LEARN-LIST
set periodic 90
  set delay threshold 25
  set mode monitor both
  set resolve delay priority 1 variance 10
  set probe frequency 5
  set link-group INET fallback MPLS

```

From the output you can see up to 162 msec of surge is seen in delay in the MPLS cloud. This causes violation of policy as threshold delay is configured to be 25 msec.

Case 3: Delay on INET Cloud Sees Increase of 100 msec

This causes Data traffic(10.30.0.0/24) to failover to link-group MPLS as per the configured statement `set link-group INET fallback MPLS`. After a period of time, traffic again gets into INPOLICY state and flows over link-group MPLS.

Note: There is no effect seen on APPLICATION traffic as its primary path is MPLS and no delay has been introduced on it in this case.

```

key chain pfr
  key 0
  key-string cisco
!
policy-rules PFR
!
  border 10.4.4.4 key-chain pfr
  interface Ethernet0/0 internal
  interface Ethernet0/1 external
  link-group MPLS
!
  border 10.5.5.5 key-chain pfr
  interface Ethernet0/0 internal
  interface Ethernet0/1 external
  link-group INET
!
learn
traffic-class filter access-list DENY-ALL
list seq 10 rename APPLICATION-LEARN-LIST
  traffic-class prefix-list APPLICATION
  throughput
list seq 20 rename DATA-LEARN-LIST
  traffic-class prefix-list DATA
  throughput
!
ip prefix-list DATA
  seq 5 permit 10.30.0.0/24
!
ip prefix-list APPLICATION
  seq 5 permit 10.20.0.0/24
!
pfr-map PFR 10
  match pfr learn list APPLICATION-LEARN-LIST
  set periodic 90
  set delay threshold 25
  set mode monitor active

```

```
set resolve delay priority 1 variance 10
set active-probe echo 10.20.0.12
set probe frequency 5
set link-group MPLS fallback INET
!
pfr-map PFR 20
  match pfr learn list DATA-LEARN-LIST
set periodic 90
set delay threshold 25
set mode monitor both
set resolve delay priority 1 variance 10
set probe frequency 5
set link-group INET fallback MPLS
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.