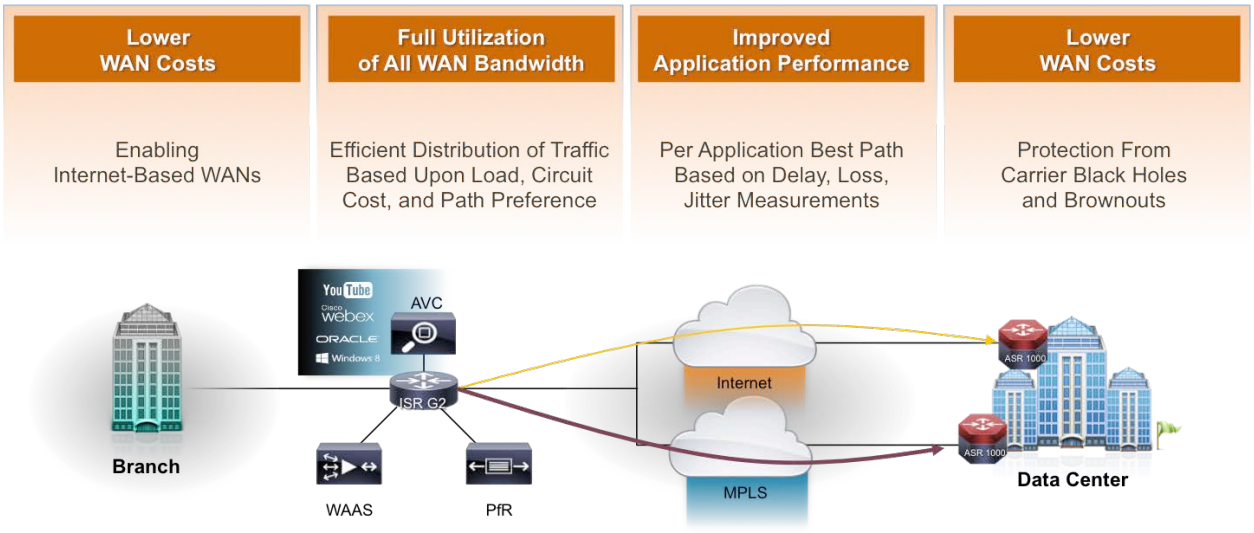
Performance Routing version 3 for IOS-XE release

Workflow and Operation Guide



Version:

1.0 November 2014

PfR allows network administrators to minimize bandwidth cost, enable intelligent load distribution, improve application performance, and deploy dynamic failure detection at the WAN access edge. Cisco IOS/IOS-XE PfR makes real-time routing adjustments based on the criteria other than static routing metrics such as delay, packet loss, jitter, path availability, and traffic load distribution.

Contents

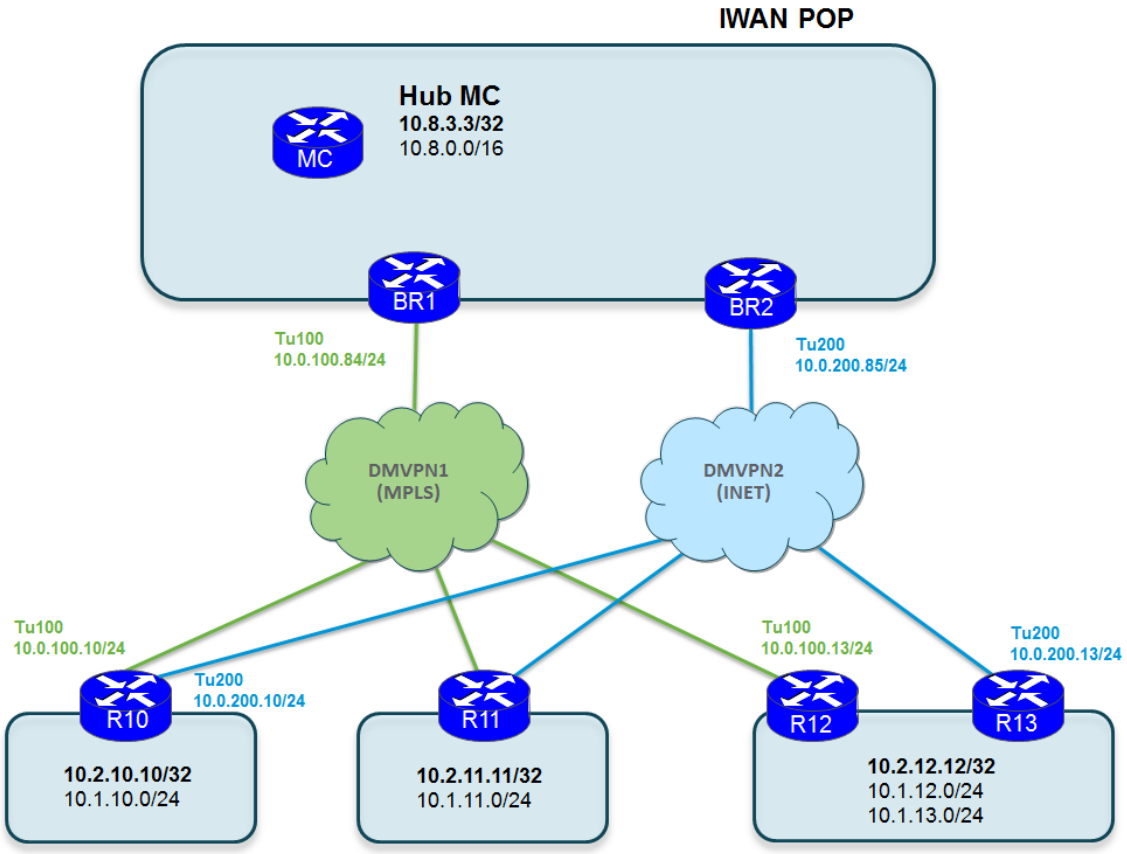
1 What is PfRv3?

PfR v3 is the evolution of Performance Routing (PfR). It is a one-touch provisioning and multisite coordination solution that simplifies network provisioning. PfRv3 is an DSCP and application-based policy framework that provides a multi-site aware bandwidth and path control optimization for WAN and cloud-based applications. It is integrated with existing AVC components such as Performance Monitoring, QoS, and NBAR2. This is extremely useful for enterprise and managed service providers who are looking for methods to increase the WAN reliability and availability while saving cost.

PfR/OER version 1 IOS 12.3(8)T, XE 2.6.1	PfR version 2 IOS 15.2(3)T, IOS-XE 3.6	PfR version 3 IOS 15.4(3)M, IOS-XE 3.13
Per Device provisioning Passive monitoring with Traditional NetFlow (TNF) Active monitoring with IP SLA Manual provisioning jitter probes 1000's lines of configuration (pfr-map per site)	Per Device provisioning Target Discovery (TD) Automatic provisioning of jitter probes Passive monitoring with Traditional NetFlow (TNF) Active monitoring with IP SLA 10's lines of configuration	PfR Domain One touch provisioning Auto Discovery of sites NBAR2 support Passive Monitoring (performance monitor) Smart Probing VRF Awareness IPv4/IPv6 (Future) <10 lines of configuration and centralized
Blackout 6 seconds Brownout 9 seconds Limited scalability due to provisioning (~ tens of sites)	Blackout 6 seconds Brownout 9 seconds Scale 500 sites	Blackout ~ sub second Brownout ~ 2 sec Scale 2000 sites

2 Enterprise Domain Topology

The typical IWAN topology includes a central site called the IWAN Hub and several branch sites. A branch site can include a single CPE or dual CPEs.



Intelligent Path Control using Cisco Performance Routing (PfR) improves application delivery and WAN efficiency. PfR enables intelligence of Cisco IOS routers to improve application performance and availability. PfR allows customers to protect critical applications from fluctuating WAN performance while intelligently load balancing traffic over all WAN paths. PfR monitors network performance and selects the best path for each application based on advanced criteria such as reachability, delay, jitter and loss.

In this workflow, we focus on the step-by-step workflow guide for PfRv3 provision, operation and troubleshooting on IOS-XE platforms. Basic VPN configuration is not covered in this document, for more information about VPN WAN Design configuration, see the latest Cisco Validated Designs for Enterprise WAN.

3 Enterprise Domain Provisioning

3.1 Device Setup and Role

There are four different roles a device can play in PfRv3 configuration:

- **Hub Master Controller (Hub MC)** - The master controller at the hub site, which can be either a data center or a head quarter. All policies are configured on the hub MC. It acts as master controller for the site and makes optimization decision.
- **Hub Border Router (Hub BR)** - The border controller at the hub site. WAN interface terminates in the hub border routers. PfRv3 is enabled on these interfaces. You can configure more than one WAN interface on the same device. You can have multiple hub border devices.
- **Branch Master Controller (Branch MC)** - The branch master controller is the master controller at the branch site. There is no policy configuration on this device. It receives policy from the hub MC. This device acts as master controller for that site for making optimization decision.
- **Branch Border Router (Branch BR)** - The border device at the branch site. There is no configuration other than enabling of PfRv3 border MC on the device. The WAN interface that terminates on the device is detected automatically.

In general, Hub Master Controller like CSR1000v or ASR1002x router with 8G/16G DRAM memory size, and RP2/ESP100, RP2/ESP200 as Hub Border Router can support up to 2000 branch sites deployment. On the branch site, ISR G2 or ISR4400/4300 Series Router can be deployed depending on performance requirements.

3.2 Hub Master Controller (Hub MC)

The hub master controller is the master controller at the hub site (Datacenter1 is our deployment example; we focus on one DC only). This is the device where all policies are configured. It also acts as master controller for that site and makes optimization decision. It is important to note that the Hub MC is NOT a centralized Master Controller for all Border Routers on all sites. This is the central point of provisioning for the entire Enterprise Domain.

In this deployment example, IWAN POP is the primary datacenter and MC is configured as the Hub MC.

```
!
interface Loopback0
 ip address 10.8.3.3 255.255.255.255
!
domain one
 vrf default
  master hub
   source-interface Loopback0
   enterprise-prefix  prefix-list ENTERPRISE
   site-prefixes prefix-list DATA_CENTER_1
!
ip prefix-list DATA_CENTER_1 seq 5 permit 10.8.0.0/16 le 24
ip prefix-list ENTERPRISE seq 5 permit 10.0.0.0/8 le 24
```

```
!
```

Notes:

- Site-prefix prefix-list define static site-prefix for local-site, and this disable automatic site-prefix learning on the border router;
- Static site-prefixes prefix-list is only required for transit sites like DMVPN Hub site for spoke to spoke traffic which disable Automatic prefix learn;
- Enterprise-prefix prefix-list define the boundary for all inside enterprise prefix; any prefix out range of these prefix-list and not advertised by any remote sites are considered as internet prefix, and should be controlled and routed over internet-bound links;
- EIGRP SAF auto-configuration enabled and unicast-listen request from remote site when domain hub master configured.

3.3 Hub Border Routers (Hub BR1 and BR2)

A Hub Border Router is a border controller at the hub site. This is the device where WAN interface terminates. PfR is enabled on these interfaces. There could be one or more WAN interface on the same device. There can be one or more Hub BRs.

On the Hub Border Routers, PfR must be configured with:

- The source-interface of local border router
- The address of the local MC
- The path name on external interfaces

The border routers on the central site register to the central MC with their external interface definition together with their path names. You can use the global routing table (default VRF) or define specific VRFs for hub border routers.

BR1 example configuration:

```
!
interface Loopback0
 ip address 10.8.1.1 255.255.255.255
!
domain one
 vrf default
  border
   source-interface Loopback0
   master 10.8.3.3
!
!
interface Tunnel100
 bandwidth 100000
 ip address 10.0.100.84 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
```

```
 ip nhrp network-id 1
 ip nhrp holdtime 600
 ip tcp adjust-mss 1360
 load-interval 30
 tunnel source GigabitEthernet3
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile DMVPN-PROFILE1
 domain one path MPLS
!
```

Notes:

- When config **path name**, there are two kinds of external interfaces, one is enterprise link by default which is normally a DMVPN Tunnel overlay interface connected with remote branch sites here; the other is internet link with **"internet-bound"** option which is used only for internet edge load balance.
- **"internet-bound"** external interface is enabled on Hub site only for internet edge deployment, and cannot be discovered by any branch site.
- **"bandwidth 100000"** indicates the bandwidth capacity on the tunnel interface, and this BW exported to Hub MC each 30 seconds, and used for bandwidth control and optimization. By default, it is 100kbps, and should be configured based on the bandwidth provided by Service Provider.
- **"ip mtu 1400"** and **"ip tcp mss 1360"** are suggested MTU settings to avoid fragmentation, please refer to latest IWAN technology design and deployment guide.

BR2 example configuration:

```
!
interface Loopback0
 ip address 10.8.2.2 255.255.255.255
!
domain one
 vrf default
  border
   source-interface Loopback0
   master 10.8.3.3
!
!
interface Tunnel200
 bandwidth 50000
 ip address 10.0.200.85 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 2
 ip nhrp holdtime 600
 ip tcp adjust-mss 1360
 load-interval 30
 delay 1000
 tunnel source GigabitEthernet4
 tunnel mode gre multipoint
 tunnel key 200
 tunnel vrf INET2
 tunnel protection ipsec profile DMVPN-PROFILE2
 domain one path INET
!
```

Notes:

- For enterprise links over Internet ISP, we suggest to enable front VRF on the tunnel interface for security, please refer to latest IWAN technology design and deployment guide.

This is a one-time configuration. Once done, all changes will be centralized on the Hub MC.

3.4 Branch Routers

The Branch Master Controller is the master controller at a branch site. There is no policy configuration on this device. It receives policy from the Hub MC. This device acts as master controller for that site for making optimization decision. The path names for external WAN interface on the branch-border router gets discovered automatically.

Example configuration for single CPE branch (R10), similar config on branch R11:

```
!
interface Loopback0
 ip address 10.2.10.10 255.255.255.255
!
domain one
 vrf default
  border
   source-interface Loopback0
   master local
  master branch
   source-interface Loopback0
   hub 10.8.3.3
!
interface Tunnel100
 bandwidth 100000
 ip address 10.0.100.10 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map 10.0.100.84 172.16.84.4
 ip nhrp map multicast 172.16.84.4
 ip nhrp network-id 1
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.100.84
 ip nhrp registration timeout 60
 ip tcp adjust-mss 1360
 load-interval 30
 delay 1000
 tunnel source GigabitEthernet2
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile DMVPN-PROFILE1
!
interface Tunnel200
 bandwidth 50000
 ip address 10.0.200.10 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map 10.0.200.85 172.16.85.5
```

```
 ip nhrp map multicast 172.16.85.5
 ip nhrp network-id 2
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.200.85
 ip nhrp registration timeout 60
 ip tcp adjust-mss 1360
 load-interval 30
 delay 1000
 tunnel source GigabitEthernet3
 tunnel mode gre multipoint
 tunnel key 200
 tunnel vrf INET2
 tunnel protection ipsec profile DMVPN-PROFILE2
!
```

Notes:

- On branch MC/BR, the MC and BR is co-located on the same router, branch MC peer and get connected with hub MC to receive updates for policy and services.
- There is no explicit configured domain name CLI on the WAN interface as hub BR, they are discovered automatically and reported to local branch master controller.

Example configuration for dual CPE branch (R12/R13):

R12 Configuration (Branch MC and BR) – includes the IP address of the Hub MC (MC1)

```
!
interface Loopback0
 ip address 10.2.12.12 255.255.255.255
!
domain one
 vrf default
  border
   source-interface Loopback0
   master local
 master branch
   source-interface Loopback0
   hub 10.8.3.3
!
interface Tunnel100
 bandwidth 100000
 ip address 10.0.100.12 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map 10.0.100.84 172.16.84.4
 ip nhrp map multicast 172.16.84.4
 ip nhrp network-id 1
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.100.84
 ip nhrp registration timeout 60
 ip tcp adjust-mss 1360
 load-interval 30
 delay 1000
 tunnel source GigabitEthernet3
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile DMVPN-PROFILE1
!
```

R13 Configuration (BR) – includes the IP address of the local MC R12

```
!
interface Loopback0
 ip address 10.2.13.13 255.255.255.255
!
domain one
 vrf default
  border
   source-interface Loopback0
   master 10.2.12.12
!
interface Tunnel200
 bandwidth 50000
 ip address 10.0.200.13 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map 10.0.200.85 172.16.85.5
 ip nhrp map multicast 172.16.85.5
 ip nhrp network-id 2
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.200.85
 ip nhrp registration timeout 60
 ip tcp adjust-mss 1360
 load-interval 30
 delay 1000
 tunnel source GigabitEthernet6
 tunnel mode gre multipoint
 tunnel key 200
 tunnel vrf INET2
 tunnel protection ipsec profile DMVPN-PROFILE2
!
```

Notes:

- For medium or large branch site, dual border routers get deployed like above configuration, R12 is a co-located MC/BR peering with hub MC, and R13 is a separate BR with front VRF design over internet Service provider.

4 Defining Domain Policies

Domain policies are only defined on the Hub Master Controller and then sent over the peering infrastructure to all MC peers. Policies can be defined per application or per DSCP. You cannot mix and match DSCP and application-based policies in the same class group. Traffic that doesn't match any of the classification and match statements falls into a default class which is load-balanced (no performance measurements done).

You can either select an existing template as domain type for policy or a customized one. The available templates for domain-policy types are listed below:

Pre-defined Template	Threshold Definition
Voice	priority 1 one-way-delay threshold 150 threshold 150 (msec) priority 2 packet-loss-rate threshold 1 (%) priority 2 byte-loss-rate threshold 1 (%) priority 3 jitter 30 (msec)
Real-time-video	priority 1 packet-loss-rate threshold 1 (%) priority 1 byte-loss-rate threshold 1 (%) priority 2 one-way-delay threshold 150 (msec) priority 3 jitter 20 (msec)
Low-latency-data	priority 1 one-way-delay threshold 100 (msec) priority 2 byte-loss-rate threshold 5 (%) priority 2 packet-loss-rate threshold 5 (%)
	priority 1 one-way-delay threshold 300 (msec) priority 2 byte-loss-rate threshold 5 (%) priority 2 packet-loss-rate threshold 5 (%)
Best-effort	priority 1 one-way-delay threshold 500 (msec) priority 2 byte-loss-rate threshold 10 (%) priority 2 packet-loss-rate threshold 10 (%)
Scavenger	priority 1 one-way-delay threshold 500 (msec) priority 2 byte-loss-rate threshold 50 (%) priority 2 packet-loss-rate threshold 50 (%)
custom	Defines customized user-defined policy values

Enterprise Domain policies are configured on the Hub MC (MC1):

```
!
domain one
 vrf default
  master hub
   monitor-interval 2 dscp ef
```

```
    load-balance
    class VOICE sequence 10
     match dscp ef policy voice
     path-preference MPLS fallback INET
    class VIDEO sequence 20
     match dscp af41 policy real-time-video
     match dscp cs4 policy real-time-video
     path-preference INET fallback MPLS
    class CRITICAL sequence 30
     match dscp af31 policy custom
      priority 2 loss threshold 10
      priority 1 one-way-delay threshold 600
     path-preference MPLS fallback INET
!
```

Notes:

- Configures policy on per DSCP basis only - The assumption is that DSCP marking is done on ingress (LAN interface of the BRs) or even within the site (access switch).
- Path preference for MPLS for all voice/video and critical applications.
- Predefined or custom policies can be used.
- Monitor interval is set to 2 second for critical applications. Default is 30 seconds. You can lower the monitor interval for a couple of critical applications in order to achieve a fast failover to the secondary path. This is called quick monitor.
- Load balancing is enabled for default class traffic. When load balancing is enabled, PfR adds a default class for match all DSCP (lowest priority compared to all the other classes) and influences this traffic. When load balancing is disabled, PfR deletes this “default class” and as a part of that frees up the TCs that was learnt as a part of LB – they follow the routing table.

You can check the detail policy by using the show domain <name> master policy command

```
HubMC#show domain one master policy
 No Policy publish pending
------------------------------------------------------------------------------

  class VOICE sequence 10
    path-preference MPLS fallback INET
    class type: Dscp Based
      match dscp ef policy custom
        priority 2 packet-loss-rate threshold 5.0 percent
        priority 1 one-way-delay threshold 150 msec
        priority 2 byte-loss-rate threshold 5.0 percent
        Number of Traffic classes using this policy: 1

  class VIDEO sequence 20
    path-preference INET fallback MPLS
    class type: Dscp Based
      match dscp af41 policy custom
        priority 2 packet-loss-rate threshold 5.0 percent
        priority 1 one-way-delay threshold 150 msec
        priority 2 byte-loss-rate threshold 5.0 percent
        Number of Traffic classes using this policy: 1
      match dscp cs4 policy custom
        priority 2 packet-loss-rate threshold 5.0 percent
        priority 1 one-way-delay threshold 150 msec
        priority 2 byte-loss-rate threshold 5.0 percent
```

```
        Number of Traffic classes using this policy: 1

  class CRITICAL sequence 30
    path-preference MPLS fallback INET
    class type: Dscp Based
      match dscp af31 policy custom
        priority 2 packet-loss-rate threshold 10.0 percent
        priority 1 one-way-delay threshold 600 msec
        priority 2 byte-loss-rate threshold 10.0 percent
        Number of Traffic classes using this policy: 1

  class default
      match dscp all
        Number of Traffic classes using this policy: 3
------------------------------------------------------------------------------
HubMC#
```

Notes:

- Check whether policy publish pending to remote sites.
- Check detailed policy threshold per class, based on DSCP or application.
- Class default is enabled when load-balance configured, and match any traffic-classes there is no performance policy enabled.

5 Checking Domain Discovery

5.1 Check Hub MC status

```
HubMC#show domain one master status

  *** Domain MC Status ***

 Master VRF: Global

  Instance Type:    Hub
  Instance id:      0
  Operational status:  Up
  Configured status:  Up
  Loopback IP Address: 10.8.3.3
  Load Balancing:
   Admin Status: Enabled
   Operational Status: Up
   Enterprise top level prefixes configured: 1
   Max Calculated Utilization Variance: 1%
   Last load balance attempt: 00:27:23 ago
   Last Reason:  Variance less than 20%
   Total unbalanced bandwidth:
         External links: 0 Kbps  Internet links: 0 Kpbs
  Route Control: Enabled
  Mitigation mode Aggressive: Disabled
  Policy threshold variance: 20
  Minimum Mask Length: 28
  Sampling: off

  Borders:
    IP address: 10.8.2.2
    Connection status: CONNECTED (Last Updated 1d11h ago )
    Interfaces configured:
```

```
      Name: Tunnel200 | type: external | Service Provider: INET | Status: UP
          Number of default Channels: 3

    Tunnel if: Tunnel0

    IP address: 10.8.1.1
    Connection status: CONNECTED (Last Updated 1d11h ago )
    Interfaces configured:
      Name: Tunnel100 | type: external | Service Provider: MPLS | Status: UP
          Number of default Channels: 3

    Tunnel if: Tunnel0

------------------------------------------------------------------------------
HubMC#
```

Notes:

- Check Operational status is up
- Check Configured status is up
- Check external interfaces are correctly defined with appropriate Path names
- Check load-balancing is in the correct state
- Two kinds of interfaces for bandwidth balance: Enterprise External links and Internet links
- Disabled – MC will uncontrol default class Traffic Classes
- Enabled – MC will control and load-share default-class Traffic Classes among all external interfaces
- Number of default Channels that can be counted for load-share between external interfaces

```
HubMC#show domain one master exits

  BR address: 10.8.2.2 | Name: Tunnel200 | type: external | Path: INET |
      Egress capacity: 50000 Kbps | Egress BW: 17514 Kbps | Ideal:17948 Kbps | under:
434 Kbps | Egress Utilization: 35 %
      DSCP: cs4[32]-Number of Traffic Classes[1]
      DSCP: af41[34]-Number of Traffic Classes[1]
      DSCP: cs5[40]-Number of Traffic Classes[1]

  BR address: 10.8.1.1 | Name: Tunnel100 | type: external | Path: MPLS |
      Egress capacity: 100000 Kbps | Egress BW: 36331 Kbps | Ideal:35896 Kbps | over:
435 Kbps | Egress Utilization: 36 %
      DSCP: cs1[8]-Number of Traffic Classes[1]
      DSCP: af11[10]-Number of Traffic Classes[1]
      DSCP: af31[26]-Number of Traffic Classes[1]
      DSCP: ef[46]-Number of Traffic Classes[1]

------------------------------------------------------------------------------
HubMC#
```

Notes:

- Check external interfaces capacity and egress utilization
- Check number of Traffic Classes per DSCP on external interface
- Check the range of egress utilization

```
HubMC#show domain one master peering
Peering state: Enabled
Origin:         Loopback0(10.8.3.3)
Peering type:      Listener
Subscribed service:
     cent-policy (2) :
     site-prefix (1) :
       Last Notification Info: 00:23:15 ago, Size: 160, Compressed size: 144, Status:
No Error, Count: 3
     service-provider (4) :
     globals (5) :
       Last Notification Info: 00:03:09 ago, Size: 325, Compressed size: 218, Status:
No Error, Count: 6
     pmi (3) :

Published service:
     site-prefix (1) :
       Last Publish Info: 00:03:10 ago, Size: 209, Compressed size: 138, Status: No
Error
     cent-policy (2) :
       Last Publish Info: 00:02:58 ago, Size: 2244, Compressed size: 468, Status: No
Error
     pmi (3) :
       Last Publish Info: 02:03:12 ago, Size: 2088, Compressed size: 458, Status: No
Error
     globals (5) :
       Last Publish Info: 00:03:09 ago, Size: 325, Compressed size: 198, Status: No
Error
HubMC#HubMC#
```

Notes:

- Check master peering status
- site-prefix, cent-policy, pmi, and globals service Publish and Subscription status
- All of the services are automatically generated by Hub MC, then published by EGIRP SAF framework
- Hub MC publish all of four type of services, and subscribe site-prefix and globals service from remote branch sites at the same time

5.2 Check Hub BR Status

```
HubBR1#show domain one border status

Thu Oct 30 05:25:00.876
------------------------------------------------------------------------------
  ****Border Status****

Instance Status: UP
Present status last updated: 02:07:43 ago
Loopback: Configured Loopback0 UP (10.8.2.2)
Master: 10.8.3.3
Connection Status with Master: UP
MC connection info: CONNECTION SUCCESSFUL
Connected for: 02:07:42
Route-Control: Enabled
Minimum Mask length: 28
Sampling: off
```

```
Minimum Requirement: Met
External Wan interfaces:
     Name: Tunnel100 Interface Index: 14 SNMP Index: 9 SP:MPLS Status: UP

Auto Tunnel information:

   Name:Tunnel0 if_index: 15
   Borders reachable via this tunnel:  10.8.2.2,
------------------------------------------------------------------------------
HubBR1#
```

Notes:

- Check external interfaces are correctly defined
- Check that connection status with MC is up
- Check that remote BR is discovered
- Check that Minimum requirement met
- PFR auto-tunnel interface is created automatically to all other border routers in the same site

```
HubBR1#show domain one border peering
Peering state: Enabled
Origin:         Loopback0(10.8.2.2)
Peering type: Peer(With 10.8.3.3)
Subscribed service:
     pmi (3) :
       Last Notification Info: 02:09:49 ago, Size: 2088, Compressed size: 478, Status:
No Error, Count: 1
     site-prefix (1) :
       Last Notification Info: 00:06:19 ago, Size: 128, Compressed size: 134, Status:
No Error, Count: 6
     globals (5) :
       Last Notification Info: 00:09:48 ago, Size: 325, Compressed size: 218, Status:
No Error, Count: 9

Published service:

HubBR1#
```

Notes:

- Check border router peering status
- Border router subscribe pmi, site-prefix and globals service;

To check the CENT border status on ASR1000 platform, we need IOS-XE platform specific show command:

```
HubBR2#show platform software pfrv3 rp active smart-probe
CENT smart probe parameters :

Total number of CENT smart probe: 1

Parameters :
  vrf id = 0
```

```
  Probe src = 10.8.3.3
  Src port = 18000, Dst port = 19000
  Unreach time = 1000, Probe period = 500
  Discovery = false
  Dscp bitmap = 0xffffffffffffffff
  interval = 10000
  Discovery_probe = true
  minimum prefix length = 28


HubBR2#show platform software pfrv3 fp active smart-probe
CENT smart probe parameters :

Total number of CENT smart probe: 1

Parameters :
  vrf id = 0
  Probe src = 10.8.3.3
  Src port = 18000, Dst port = 19000
  Unreach time = 1000, Probe period = 500
  Discovery = false
  Dscp bitmap = 0xffffffffffffffff
  interval = 10000
  Discovery_probe = true
  minimum prefix length = 28


HubBR2#show platform hardware qfp active feature pfrv3 client global pfrv3-instance
detail
CENT QFP CLIENT GLOBAL INFO

Number of Instances: 1

Instance
  hash val:  5
  tbl id:    0
  symmetry:  Off
  discovery: Off
  discovery_probe: On
  probe info:
    probe src: 10.8.3.3, src port: 18000, dst port: 19000
    unreach time: 1000, probe period: 500
    dscp bitmap: 0xffffffffffffffff, interval: 10000
    mml: 28
  exmem info:
    PPE addr: 0xe80b7830
```

Notes:

- Check PfR border router instance in data-plane;
- Check PfR border instance and smart-probe related parameter: unreachable and probe timer and minimum prefix length, etc;
- Check the fast-monitor DSCP bitmap which DSCP get enabled for fast borrowout

5.3 Check Hub Discovered sites

All sites that belong to the Domain should appear. This shows that SAF peering is correctly set up. In this workflow, we have two remote sites Branch10, Branch 11 and local hub sites connected:

```
HubMC#show derived-config | section eigrp
router eigrp #AUTOCFG# (API-generated auto-configuration, not user configurable)
 !
 service-family ipv4 autonomous-system 59501
  !
  sf-interface Loopback0
   hello-interval 120
   hold-time 600
  exit-sf-interface
  !
  topology base
  exit-sf-topology
  remote-neighbors source Loopback0 unicast-listen
 exit-service-family

HubMC#show eigrp service-family ipv4 neighbors
EIGRP-SFv4 VR(#AUTOCFG#) Service-Family Neighbors for AS(59501)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
2   10.2.10.10              Lo0                     595 01:59:20    5   100  0  11
1   10.2.11.11              Lo0                     549 02:08:36    1   100  0  16
3   10.8.1.1                Lo0                     498 02:12:11    1   100  0  4
0   10.8.2.2                Lo0                     526 02:12:42    1   100  0  7
HubBR1#
```

Notes:

- Check eigrp SAF configuration automatically enabled;
- Check EIGRP SAF peering status between local and remote sites;

```
HubMC#show domain one master discovered-sites

  *** Domain MC DISCOVERED sites ***

  Number of sites:  3
 *Traffic classes [Performance based][Load-balance based]

 Site ID: 255.255.255.255
    DSCP :default[0]-Number of traffic classes[0][0]
    DSCP :af31[26]-Number of traffic classes[0][0]
    DSCP :cs4[32]-Number of traffic classes[0][0]
    DSCP :af41[34]-Number of traffic classes[0][0]
    DSCP :cs5[40]-Number of traffic classes[0][0]
    DSCP :ef[46]-Number of traffic classes[0][0]

 Site ID: 10.2.10.10
    DSCP :default[0]-Number of traffic classes[1][1]
    DSCP :af31[26]-Number of traffic classes[0][0]
    DSCP :cs4[32]-Number of traffic classes[1][0]
    DSCP :af41[34]-Number of traffic classes[0][0]
    DSCP :cs5[40]-Number of traffic classes[0][0]
    DSCP :ef[46]-Number of traffic classes[1][0]

 Site ID: 10.2.11.11
    DSCP :default[0]-Number of traffic classes[0][0]
```

```
    DSCP :af31[26]-Number of traffic classes[0][0]
    DSCP :cs4[32]-Number of traffic classes[0][0]
    DSCP :af41[34]-Number of traffic classes[0][0]
    DSCP :cs5[40]-Number of traffic classes[0][0]
    DSCP :ef[46]-Number of traffic classes[0][0]
------------------------------------------------------------------------------
HubMC#
```

At this point the Hub BRs can generate Discovery Probes (Smart Probes) to all remote sites to help them discover their external interfaces and their path names.

5.4 Check Branch MC Status

```
Branch10#show domain one master status

  *** Domain MC Status ***

 Master VRF: Global

  Instance Type:    Branch
  Instance id:      0
  Operational status:  Up
  Configured status:  Up
  Loopback IP Address: 10.2.10.10
  Load Balancing:
   Operational Status: Up
   Max Calculated Utilization Variance: 21%
   Last load balance attempt: 00:00:07 ago
   Last Reason:  No channels yet for load balancing
   Total unbalanced bandwidth:
         External links: 5327 Kbps  Internet links: 0 Kpbs
  Route Control: Enabled
  Mitigation mode Aggressive: Disabled
  Policy threshold variance: 20
  Minimum Mask Length: 28
  Sampling: off
  Minimum Requirement: Met

  Borders:
    IP address: 10.2.10.10
    Connection status: CONNECTED (Last Updated 02:03:22 ago )
    Interfaces configured:
      Name: Tunnel100 | type: external | Service Provider: MPLS | Status: UP
          Number of default Channels: 0

      Name: Tunnel200 | type: external | Service Provider: INET | Status: UP
          Number of default Channels: 0

    Tunnel if: Tunnel0

------------------------------------------------------------------------------
Branch10#
```

Notes:

- Check that external interfaces are listed with their correct path names. That means smart probes are correctly received and decoded by local BRs. If external interfaces are not correctly discovered, that means smart probes are not correctly received:
- Check that remote MC address is reachable over all external interfaces
- Check that Smart Probes are correctly received
- Check path names are correct. If path names are not listed check that smart probes are received from the hub. Branch MC loopback address has to be announced and routable from the hub Border Routers.

To check the **smart probes packets (SMP)** are correctly received on each external interface, one can define an access-list to match SMP packets:

access-list 100 permit udp any eq 18000 any eq 19000

"show ip access-list" to check whether the counter keeps increasing, you could also use **conditional debug** or **embedded packet capture(EPC)** to capture the smart-probe packets on the external interface either on source or destination border router, please refer to section **7.4 Embedded Packet Capture (EPC).**

Check Policy is received from the hub MC: show domain <name> master policy

```
Branch10#show domain one master policy
------------------------------------------------------------------------------

  class VOICE sequence 10
    path-preference MPLS fallback INET
    class type: Dscp Based
      match dscp ef policy custom
        priority 2 packet-loss-rate threshold 5.0 percent
        priority 1 one-way-delay threshold 150 msec
        priority 2 byte-loss-rate threshold 5.0 percent
        Number of Traffic classes using this policy: 1

  class VIDEO sequence 20
    path-preference INET fallback MPLS
    class type: Dscp Based
      match dscp af41 policy custom
        priority 2 packet-loss-rate threshold 5.0 percent
        priority 1 one-way-delay threshold 150 msec
        priority 2 byte-loss-rate threshold 5.0 percent
      match dscp cs4 policy custom
        priority 2 packet-loss-rate threshold 5.0 percent
        priority 1 one-way-delay threshold 150 msec
        priority 2 byte-loss-rate threshold 5.0 percent
        Number of Traffic classes using this policy: 1

  class CRITICAL sequence 30
    path-preference MPLS fallback INET
    class type: Dscp Based
      match dscp af31 policy custom
        priority 2 packet-loss-rate threshold 10.0 percent
        priority 1 one-way-delay threshold 600 msec
        priority 2 byte-loss-rate threshold 10.0 percent

  class default
      match dscp all
```

```
--------------------------------------------------------------------------------
Branch10#
```

5.5 Check Branch BR Status

```
Branch10#show domain one border status

Thu Oct 30 05:42:00.647
------------------------------------------------------------------------------------
  ****Border Status****

Instance Status: UP
Present status last updated: 02:11:47 ago
Loopback: Configured Loopback0 UP (10.2.10.10)
Master: 10.2.10.10
Connection Status with Master: UP
MC connection info: CONNECTION SUCCESSFUL
Connected for: 02:11:41
Route-Control: Enabled
Minimum Mask length: 28
Sampling: off
Minimum Requirement: Met
External Wan interfaces:
     Name: Tunnel100 Interface Index: 14 SNMP Index: 9 SP:MPLS Status: UP
     Name: Tunnel200 Interface Index: 15 SNMP Index: 10 SP:INET Status: UP

Auto Tunnel information:

   Name:Tunnel0 if_index: 19
   Borders reachable via this tunnel:
------------------------------------------------------------------------------------
Branch10#
```

Step 1. Check that external interfaces are listed with their correct path names. That means smart probes are correctly received and decoded by local BRs.

Step 2. Check path names are correct. If path names are not listed check that smart probes are received from the hub. Branch MC loopback address has to be announced and routable from the hub Border Routers.

Step 3. Check that Minimum requirement met.

If the minimum requirement is not MET, check the SAF peering on the local master – it should correctly peer with the hub MC:

```
Branch10#show eigrp service-family ipv4 neighbors detail
EIGRP-SFv4 VR(#AUTOCFG#) Service-Family Neighbors for AS(59501)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   10.8.3.3                Lo0                     497 02:12:18    5   100  0  31
   Remote Static neighbor (static multihop)
   Version 17.0/4.0, Retrans: 0, Retries: 0, Prefixes: 6
```

```
   Topology-ids from peer - 0
Max Nbrs: 65535, Current Nbrs: 0
R10#
```

Check PfRv3 peering on the local master: show domain <name> master peering

```
Branch10#show domain one master peering
Peering state: Enabled
Origin:         Loopback0(10.2.10.10)
Peering type:      Listener, Peer(With 10.8.3.3)
Subscribed service:
     cent-policy (2) :
       Last Notification Info: 00:24:15 ago, Size: 2244, Compressed size: 488, Status:
No Error, Count: 5
     site-prefix (1) :
       Last Notification Info: 00:24:15 ago, Size: 128, Compressed size: 134, Status:
No Error, Count: 35
     service-provider (4) :
     globals (5) :
       Last Notification Info: 00:24:15 ago, Size: 325, Compressed size: 218, Status:
No Error, Count: 19

Published service:
     site-prefix (1) :
       Last Publish Info: 00:49:11 ago, Size: 160, Compressed size: 124, Status: No
Error
     globals (5) :
       Last Publish Info: 10:29:09 ago, Size: 325, Compressed size: 198, Status: No
Error
Branch10#
```

- Domain Policies are defined on the Hub MC and sent over the SAF infrastructure to all MC peers.
- Each time Domain policies are updated on the hub MC, they are refreshed and sent over to all MC peers.
- For any branch MC not receiving any update, please confirm whether MTU settings are consistently across the path which might lead to any EIGRP SAF packets get dropped unexpectedly.

Step 4. Check Monitor specification is received from the hub MC -> show domain one border pmi

Step 5. Check that performance monitors are correctly applied on the external interfaces, on ingress and egress:

```
Branch10#show domain one border pmi

****CENT PMI INFORMATION****


Ingress policy CENT-Policy-Ingress-0-4:
Ingress policy activated on:
  Tunnel200 Tunnel100


[SNIP]

------------------------------------------------------------------------
```

```
Egress policy CENT-Policy-Egress-0-3:
Egress policy activated on:
  Tunnel200 Tunnel100
------------------------------------------------------------------------
PMI[Egress-aggregate]-FLOW MONITOR[MON-Egress-aggregate-0-48-1]
  Trigger Nbar:No

------------------------------------------------------------------------
PMI[Egress-prefix-learn]-FLOW MONITOR[MON-Egress-prefix-learn-0-48-2]


With application based policy:

Branch10#show domain one border pmi

****CENT PMI INFORMATION****


Ingress policy CENT-Policy-Ingress-0-4:
Ingress policy activated on:
  Tunnel200 Tunnel100


[SNIP]

------------------------------------------------------------------------

Egress policy CENT-Policy-Egress-0-3:
Egress policy activated on:
  Tunnel200 Tunnel0 Tunnel100
------------------------------------------------------------------------
PMI[Egress-aggregate]-FLOW MONITOR[MON-Egress-aggregate-0-48-1]
  Trigger Nbar:Yes

------------------------------------------------------------------------
PMI[Egress-prefix-learn]-FLOW MONITOR[MON-Egress-prefix-learn-0-48-2]
```

Notes:

- PMI stands for Performance Monitoring Instances;
- Performance monitor definitions are received from the Hub MC;
- Policy are activated on all external interfaces on border router;
- Auto-Tunnel and NBAR get activated dynamically with application based policy only.

5.6 Check Unified Performance Monitor

PfR version 3 leverages AVC/MMA infrastructure for passive performance monitoring, includes site-prefix and traffic-class learning on WAN interface egress direction, and per DSCP performance monitoring on ingress direction. These three flow monitor are generated automatically:

```
Branch10#show flow monitor type performance-monitor
Flow Monitor type performance-monitor MON-Egress-aggregate-0-48-9:
  Description           :User defined
  Flow Record           :CENT-FLOWREC-Egress-aggregate-0-11
```

```
  Flow Exporter          :CENT_FLOW_EXP-2
  Cache type             :synchronized
        entries          :4000
        interval         :30 (seconds)
        history size     :0 (intervals)
        timeout          :1 (intervals)
        export spreading:TRUE
  Interface applied      :2

Flow Monitor type performance-monitor MON-Egress-prefix-learn-0-48-10:
  Description            :User defined
  Flow Record            :CENT-FLOWREC-Egress-prefix-learn-0-12
  Flow Exporter          :CENT_FLOW_EXP-2
  Cache type             :synchronized
        entries          :700
        interval         :30 (seconds)
        history size     :0 (intervals)
        timeout          :1 (intervals)
        export spreading:FALSE
  Interface applied      :2

Flow Monitor type performance-monitor MON-Ingress-per-DSCP-0-48-11:
  Description            :User defined
  Flow Record            :CENT-FLOWREC-Ingress-per-DSCP-0-13
  Flow Exporter          :not configured
  Cache type             :synchronized
        entries          :2000
        interval         :30 (seconds)
        history size     :0 (intervals)
        timeout          :1 (intervals)
        export spreading:FALSE
  Interface applied      :2
```

Notes:

- performance monitor cache size setting based on platform capability;
- export spreading enabled for egress monitor to avoid export storm under scale condition;
- performance monitor with a 30 sec interval by default;

You should be able to review the detail performance monitor flow definition, which is generated automatically when PfR gets configured: **show performance monitor internal flow-def-master**

```
Branch10#show performance monitor internal flow-def-master
FNF Monitor : MON-Ingress-per-DSCP-0-48-11  Name           :
MMA_DB_c_fdef_1340502592_12
  Users          : 0
  Key Fields:
  Non Key Fields:
    Name: transport packets expected counter
    Name: transport packets lost counter
    Name: transport packets lost rate
    Name: transport bytes expected
    Name: transport bytes lost
    Name: transport bytes lost rate
    Name: pfr one-way-delay samples
    Name: pfr one-way-delay sum
```

```
    Name: pfr one-way-delay
    Name: network delay sample
    Name: network delay sum
    Name: network delay average
    Name: transport rtp jitter inter arrival samples
    Name: transport rtp jitter inter arrival sum
    Name: transport rtp jitter inter arrival mean
    Name: counter bytes long
    Name: counter packets long
    Name: timestamp absolute monitoring-interval start
    Name: timestamp interval
  Name           : MMA_DB_m_fdef_1340502592_12
  Users          : 0
  Key Fields:
    Name: pfr site source id ipv4
    Name: pfr site destination id ipv4
    Name: ip dscp
    Name: interface input
    Name: policy performance-monitor classification hierarchy
  Non Key Fields:
    Name: vm (72 / 0x48)
  Name           : MMA_DB_t_fdef_1340502592_12
  Users          : 0
  Key Fields:
    Name: timestamp absolute monitoring-interval end
    Name: pfr site source id ipv4
    Name: pfr site destination id ipv4
    Name: ip dscp
    Name: interface input
    Name: policy performance-monitor classification hierarchy
  Non Key Fields:
    Name: transport packets expected counter
    Name: transport packets lost counter
    Name: transport bytes expected
    Name: transport bytes lost
    Name: pfr one-way-delay samples
    Name: pfr one-way-delay sum
    Name: network delay sample
    Name: network delay sum
    Name: transport rtp jitter inter arrival samples
    Name: transport rtp jitter inter arrival sum
    Name: counter bytes long
    Name: counter packets long
    Name: timestamp absolute monitoring-interval start
    Name: timestamp interval
    Name: vm (8 / 0x8)

FNF Monitor : MON-Egress-aggregate-0-48-9  Name          :
MMA_DB_c_fdef_2307076292_10
  Users          : 0
  Key Fields:
  Non Key Fields:
    Name: timestamp absolute monitoring-interval start
    Name: counter bytes long
    Name: counter packets long
    Name: ip protocol
    Name: pfr site destination id ipv4
    Name: pfr site source id ipv4
    Name: timestamp interval
  Name           : MMA_DB_m_fdef_2307076292_10
  Users          : 0
  Key Fields:
    Name: ipv4 destination prefix
    Name: ipv4 destination mask
    Name: pfr site destination prefix ipv4
```

```
    Name: pfr site destination prefix mask ipv4
    Name: ip dscp
    Name: interface output
  Non Key Fields:
    Name: vm (72 / 0x48)
  Name           : MMA_DB_t_fdef_2307076292_10
  Users          : 0
  Key Fields:
    Name: timestamp absolute monitoring-interval end
    Name: ipv4 destination prefix
    Name: ipv4 destination mask
    Name: pfr site destination prefix ipv4
    Name: pfr site destination prefix mask ipv4
    Name: ip dscp
    Name: interface output
  Non Key Fields:
    Name: timestamp absolute monitoring-interval start
    Name: counter bytes long
    Name: counter packets long
    Name: ip protocol
    Name: pfr site destination id ipv4
    Name: pfr site source id ipv4
    Name: timestamp interval
    Name: vm (8 / 0x8)

FNF Monitor : MON-Egress-prefix-learn-0-48-10  Name           :
MMA_DB_c_fdef_2587394358_11
  Users          : 0
  Key Fields:
  Non Key Fields:
    Name: counter bytes long
    Name: counter packets long
    Name: timestamp absolute monitoring-interval start
    Name: timestamp interval
  Name           : MMA_DB_m_fdef_2587394358_11
  Users          : 0
  Key Fields:
    Name: ipv4 source prefix
    Name: ipv4 source mask
    Name: routing vrf input
  Non Key Fields:
    Name: vm (72 / 0x48)
  Name           : MMA_DB_t_fdef_2587394358_11
  Users          : 0
  Key Fields:
    Name: timestamp absolute monitoring-interval end
    Name: ipv4 source prefix
    Name: ipv4 source mask
    Name: routing vrf input
  Non Key Fields:
    Name: counter bytes long
    Name: counter packets long
    Name: timestamp absolute monitoring-interval start
    Name: timestamp interval
    Name: vm (8 / 0x8)

Branch10#
```

Notes:

- One ingress monitor **"MON-Ingress-per-DSCP-0-48-11"** collects performance metrics per channel (per pair of site and DSCP value). Note the key fields: **pfr site source id ipv4, pfr site destination id ipv4, ip dscp** and **domain path** used to identify a channel.
- One egress performance monitor **"MON-Egress-aggregate-0-48-9"** to collect bandwidth per Traffic Class - Note the key fields: **pfr site destination prefix ipv4, mask, ip dscp, or application ID** used to identify a Traffic Class.
- One egress performance monitor "**MON-Egress-prefix-learn-0-48-10**" to catch new source prefixes and advertise them to all peers. Again note the key fields: **cef ipv4 source prefix/mask** that is used to identify new source prefixes.

Performance monitor get activated on external interface when domain path configured on hub BR or discovered on branch BR:

```
Branch10#show domain one border pmi

****CENT PMI INFORMATION****


Ingress policy CENT-Policy-Ingress-0-9:
Ingress policy activated on:
  Tunnel200 Tunnel100
------------------------------------------------------------------------
PMI[Ingress-per-DSCP]-FLOW MONITOR[MON-Ingress-per-DSCP-0-48-11]
    monitor-interval:30
    key-list:
      pfr site source id ipv4
      pfr site destination id ipv4
      ip dscp
      interface input
      policy performance-monitor classification hierarchy
    Non-key-list:
      transport packets lost rate
      transport bytes lost rate
      pfr one-way-delay
      network delay average
      transport rtp jitter inter arrival mean
      counter bytes long
      counter packets long
      timestamp absolute monitoring-interval start
    DSCP-list:
      ef-[class:CENT-Class-Ingress-DSCP-ef-0-22]
        packet-loss-rate:react_id[70]-priority[2]-threshold[5.0 percent]
        one-way-delay:react_id[71]-priority[1]-threshold[150 msec]
        network-delay-avg:react_id[72]-priority[1]-threshold[300 msec]
        byte-loss-rate:react_id[73]-priority[2]-threshold[5.0 percent]
      af41-[class:CENT-Class-Ingress-DSCP-af41-0-23]
        packet-loss-rate:react_id[74]-priority[2]-threshold[5.0 percent]
        one-way-delay:react_id[75]-priority[1]-threshold[150 msec]
        network-delay-avg:react_id[76]-priority[1]-threshold[300 msec]
        byte-loss-rate:react_id[77]-priority[2]-threshold[5.0 percent]
      cs4-[class:CENT-Class-Ingress-DSCP-cs4-0-24]
        packet-loss-rate:react_id[78]-priority[2]-threshold[5.0 percent]
        one-way-delay:react_id[79]-priority[1]-threshold[150 msec]
        network-delay-avg:react_id[80]-priority[1]-threshold[300 msec]
        byte-loss-rate:react_id[81]-priority[2]-threshold[5.0 percent]
      af31-[class:CENT-Class-Ingress-DSCP-af31-0-25]
        packet-loss-rate:react_id[82]-priority[2]-threshold[10.0 percent]
```

```
        one-way-delay:react_id[83]-priority[1]-threshold[600 msec]
        network-delay-avg:react_id[84]-priority[1]-threshold[1200 msec]
        byte-loss-rate:react_id[85]-priority[2]-threshold[10.0 percent]

    Exporter-list:None
------------------------------------------------------------------------

Egress policy CENT-Policy-Egress-0-8:
Egress policy activated on:
  Tunnel200 Tunnel100
------------------------------------------------------------------------
PMI[Egress-aggregate]-FLOW MONITOR[MON-Egress-aggregate-0-48-9]
    monitor-interval:30
    Trigger Nbar:No
    minimum-mask-length:28
    key-list:
      ipv4 destination prefix
      ipv4 destination mask
      pfr site destination prefix ipv4
      pfr site destination prefix mask ipv4
      ip dscp
      interface output
    Non-key-list:
      timestamp absolute monitoring-interval start
      counter bytes long
      counter packets long
      ip protocol
      pfr site destination id ipv4
      pfr site source id ipv4
    DSCP-list:N/A
    Class:CENT-Class-Egress-ANY-0-21

    Exporter-list:
      10.2.10.10
------------------------------------------------------------------------
PMI[Egress-prefix-learn]-FLOW MONITOR[MON-Egress-prefix-learn-0-48-10]
    monitor-interval:30
    minimum-mask-length:28
    key-list:
      ipv4 source prefix
      ipv4 source mask
      routing vrf input
    Non-key-list:
      counter bytes long
      counter packets long
      timestamp absolute monitoring-interval start
    DSCP-list:N/A
    Class:CENT-Class-Egress-ANY-0-21

    Exporter-list:
      10.2.10.10
------------------------------------------------------------------------
Branch10#
```

Notes:

- PMI stands for Performance Monitoring Instances.
- Performance monitor definitions are received from the Hub MC
- One ingress performance monitor with 2 sec interval for all critical applications, with DSCP EF, AF41/CS4, and AF31 - this monitor is called "quick" monitor.

Check service-policy stats updated correctly for each class-map on the external interfaces:

```
Branch10#show domain one border pmi policy-map interface tunnel100
 Tunnel100

  Service-policy performance-monitor input: CENT-Policy-Ingress-0-9

    Class-map: CENT-Class-Ingress-DSCP-ef-0-22 (match-any)
      7388086 packets, 3506803395 bytes
      30 second offered rate 11266000 bps, drop rate 0000 bps
      Match:  dscp ef (46)
      Total Packets classified: 0
      Total Bytes classified: 0
      Monitor AOR: disabled

    Class-map: CENT-Class-Ingress-DSCP-af41-0-23 (match-any)
      6902212 packets, 3274797427 bytes
      30 second offered rate 11291000 bps, drop rate 0000 bps
      Match:  dscp af41 (34)
      Total Packets classified: 0
      Total Bytes classified: 0
      Monitor AOR: disabled

    Class-map: CENT-Class-Ingress-DSCP-cs4-0-24 (match-any)
      7642239 packets, 3407622455 bytes
      30 second offered rate 11368000 bps, drop rate 0000 bps
      Match:  dscp cs4 (32)
      Total Packets classified: 0
      Total Bytes classified: 0
      Monitor AOR: disabled

    Class-map: CENT-Class-Ingress-DSCP-af31-0-25 (match-any)
      12345248 packets, 5860560391 bytes
      30 second offered rate 18787000 bps, drop rate 0000 bps
      Match:  dscp af31 (26)
      Total Packets classified: 0
      Total Bytes classified: 0
      Monitor AOR: disabled

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: any

  Service-policy performance-monitor output: CENT-Policy-Egress-0-8

    Class-map: CENT-Class-Egress-ANY-0-21 (match-any)
      24999229 packets, 3233800218 bytes
      30 second offered rate 10759000 bps, drop rate 0000 bps
      Match: access-group name mma-dvmc-acl#3
      Total Packets classified: 0
      Total Bytes classified: 0
      Monitor AOR: disabled

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: any
Branch10#
Branch10#show ip access-lists dynamic
Extended IP access list mma-dvmc-acl#3
    10 deny ip any 224.0.0.0 15.255.255.255
```

```
    20 deny ip any any dscp cs6
    30 permit tcp any any
    40 permit udp any neq 18000 any neq 19000
    50 permit icmp any any
```

Notes:

- Check the packets/bytes counter accounted properly;
- TCP, UDP and ICMP flows are learned and supported in this phase;
- Multicast and control-protocol packets with DSCP CS6 are not controlled by PfR;

```
Branch10#show performance monitor cache monitor MON-Egress-prefix-learn-0-48-10 detail
format record
 Monitor: MON-Egress-prefix-learn-0-48-10

 Data Collection Monitor:

  Cache type:                           Synchronized (Platform cache)
  Cache size:                                  700
  Current entries:                               1
  High Watermark:                                1

  Flows added:                                 103
  Flows aged:                                  102
  Synchronized timeout (secs):                  30

IPV4 SOURCE PREFIX:       10.1.10.0
IPV4 SOURCE MASK:         /24
IP VRF ID INPUT:          0          (DEFAULT)
counter bytes long:       26201651
counter packets long:     258674
timestamp monitor start:  16:14:30.000
```

Notes:

- Check site-prefix flow monitor cache records;
- Prefix is learned based on IPV4 SOURCE PREFIX/MASK in CEF;

```
Branch10#show performance monitor cache monitor MON-Egress-aggregate-0-48-9 detail
 Monitor: MON-Egress-aggregate-0-48-9

 Data Collection Monitor:

  Cache type:                           Synchronized (Platform cache)
  Cache size:                                 4000
  Current entries:                               7
  High Watermark:                               12

  Flows added:                                 700
  Flows aged:                                  693
  Synchronized timeout (secs):                  30

IPV4 DST PREFIX  IPV4 DST MASK  IPV4 DESTINATION SITE PREFIX  IPV4 DESTINATION SITE
PREFIX MASK  IP DSCP  INTF OUTPUT           time monitor start           bytes long
pkts long  ip prot  pfr destination site id  pfr source site id
```

```
==============  =============  ============================
================================  =======  ====================  ==================
====================  ====================  =======  ======================
==================
10.8.101.0                /28  10.8.0.0
/16  0x28     Tu200                        16:12:30.000                 88491
879        6  10.8.3.3                  10.2.10.10
10.8.101.0                /28  10.8.0.0
/16  0x20     Tu100                        16:12:30.000               4657472
45981        6  10.8.3.3                 10.2.10.10
10.8.101.0                /28  10.8.0.0
/16  0x22     Tu100                        16:12:30.000               7057760
69637        6  10.8.3.3                 10.2.10.10
10.8.101.0                /28  10.8.0.0
/16  0x0A     Tu200                        16:12:30.000                223105
2237        6  10.8.3.3                  10.2.10.10
10.8.101.0                /28  10.8.0.0
/16  0x08     Tu200                        16:12:30.000                222142
2226        6  10.8.3.3                  10.2.10.10
10.8.101.0                /28  10.8.0.0
/16  0x1A     Tu100                        16:12:30.000              11752935
115975       6  10.8.3.3                  10.2.10.10
10.8.101.0                /28  10.8.0.0
/16  0x2E     Tu100                        16:12:30.000               7044009
69518        6  10.8.3.3                 10.2.10.10
```

Notes:

- Check traffic-class flow monitor cache records;
- Traffic-class is learned based on site-prefix database with longest match of IPV4 DESTINATION SITE PREFIX /MASK;
- Internet traffic-class learned based on IPV4 Destination PREFIX/MASK and minimum-mask-length.

```
Branch10#show performance monitor cache monitor MON-Ingress-per-DSCP-0-48-11 detail
format record
 Monitor: MON-Ingress-per-DSCP-0-48-11

 Data Collection Monitor:

  Cache type:                           Synchronized (Platform cache)
  Cache size:                                 2000
  Current entries:                               8
  High Watermark:                                8

  Flows added:                                 816
  Flows aged:                                  808
  Synchronized timeout (secs):                  30

PFR SOURCE SITE ID:               10.8.3.3
PFR DESTINATION SITE ID:          10.2.10.10
IP DSCP:                          0x1A
INTERFACE INPUT:                  Tu200
POLICY PERF MON CLASS HIERARCHY:  CENT-Policy-Ingress-0-9: CENT-Class-Ingress-DSCP-
af31-0-25
trns counter packets expect:      130
trns counter packets lost:        0
trns bytes expected:              0
```

```
trns bytes lost:                    0
trns one way delay samples:         0
trns one way delay sum:             0
application network delay sample:   130
application network delay sum:      46955
rtp jitter inter arrival samples:   130
rtp jitter inter arrival sum:       83441
counter bytes long:                 9360
counter packets long:               130
timestamp monitor start:            16:14:00.000

PFR SOURCE SITE ID:                 10.8.3.3
PFR DESTINATION SITE ID:            10.2.10.10
IP DSCP:                            0x20
INTERFACE INPUT:                    Tu200
POLICY PERF MON CLASS HIERARCHY:    CENT-Policy-Ingress-0-9: CENT-Class-Ingress-DSCP-
cs4-0-24
trns counter packets expect:        131
trns counter packets lost:          0
trns bytes expected:                0
trns bytes lost:                    0
trns one way delay samples:         0
trns one way delay sum:             0
application network delay sample:   131
application network delay sum:      47315
rtp jitter inter arrival samples:   131
rtp jitter inter arrival sum:       74578
counter bytes long:                 9432
counter packets long:               131
timestamp monitor start:            16:14:00.000

[SNIP]

Branch10#
```

Notes:

- Check Per-DSCP channel performance monitor cache records, include one-way-delay, packet/byte loss, jitter metrics;
- Metrics are aggregated per channel level;
- Both smart-probe and data traffic flows are used for performance monitoring;
- Threshold control Alerts (TCA) will be generated if there is violation for pre-defined performance threshold.

6 Monitoring Operation

6.1 Monitor Site Prefix

Site-prefix is the database infrastructure for “inside” prefixes of all sites. Each local site learns site-prefix itself from egress performance monitor on external interface, and then publishes across all sites over EIGRP SAF framework. Each local site subscribes to all remote site prefix service as well, so all sites share one synchronized prefix database.

Check following table, there are four different type of prefix in this site-prefix database:

- **Local site-preifx with flag L**: Local-learned prefix, here is the site-id, learned by egress site-prefix monitor;
- **Local site-preifx with flag C**: site-prefix configured by static site-prefix list, mostly on transit site;
- **Remote site-preifx with flag S**: site-prefix learned from remote EIGRP SAF neigh ours;
- **Enterprise prefix with T**: summary prefix defines the enterprise site-prefix boundary;

Example:

```
HubMC#show domain one master site-prefix
  Change will be published between 5-60 seconds
  Next Publish 00:54:41 later
  Prefix DB Origin: 10.8.3.3
  Prefix Flag: S-From SAF; L-Learned; T-Top Level; C-Configured;

Site-id              Site-prefix          Last Updated         Flag
-------------------------------------------------------------------------------
10.2.10.10            10.1.10.0/24         00:42:07 ago         S,
10.2.10.10            10.2.10.10/32        00:42:07 ago         S,
10.2.11.11            10.2.11.11/32        00:18:25 ago         S,
10.8.3.3              10.8.3.3/32          1d05h    ago         L,
10.8.3.3              10.8.0.0/16          1d05h    ago         C,
255.255.255.255      *10.0.0.0/8           1d05h    ago         T,
-------------------------------------------------------------------------------
HubMC#

Branch10#show domain one master site-prefix
  Change will be published between 5-60 seconds
  Next Publish 00:53:12 later
  Prefix DB Origin: 10.2.10.10
  Prefix Flag: S-From SAF; L-Learned; T-Top Level; C-Configured;

Site-id              Site-prefix          Last Updated         Flag
-------------------------------------------------------------------------------
10.2.10.10            10.1.10.0/24         00:00:26 ago         L,
10.2.11.11            10.1.11.0/24         01:20:47 ago         S,
10.2.10.10            10.2.10.10/32        01:06:49 ago         L,
10.2.11.11            10.2.11.11/32        01:20:47 ago         S,
10.8.3.3              10.8.3.3/32          01:29:07 ago         S,
10.8.3.3              10.8.0.0/16          01:29:07 ago         S,C,
255.255.255.255      *10.0.0.0/8           01:29:07 ago         S,T,
-------------------------------------------------------------------------------

HubBR1#show domain one border site-prefix

  Prefix Flag: S-From SAF; L-Learned; T-Top Level; C-Configured;

Site-id              Site-prefix          Last Updated         Flag
-------------------------------------------------------------------------------
10.2.10.10            10.1.10.0/24         00:59:12 ago         S,
10.2.11.11            10.1.11.0/24         01:14:42 ago         S,
10.2.10.10            10.2.10.10/32        01:08:04 ago         S,
10.2.11.11            10.2.11.11/32        01:22:01 ago         S,
10.8.3.3              10.8.3.3/32          01:30:22 ago         S,
10.8.3.3              10.8.0.0/16          01:30:22 ago         S,C,
255.255.255.255      *10.0.0.0/8           01:30:22 ago         S,T,
-------------------------------------------------------------------------------
HubBR1#

Branch11#show domain one border site-prefix
```

```
  Change will be published between 5-60 seconds
  Prefix DB Origin: 10.2.11.11
  Prefix Flag: S-From SAF; L-Learned; T-Top Level; C-Configured;

Site-id              Site-prefix          Last Updated         Flag
------------------------------------------------------------------------------
10.2.10.10            10.1.10.0/24         01:07:46 ago         S,
10.2.11.11            10.1.11.0/24         01:21:44 ago         S,
10.2.10.10            10.2.10.10/32        01:07:46 ago         S,
10.2.11.11            10.2.11.11/32        01:21:44 ago         S,
10.8.3.3              10.8.3.3/32          01:30:04 ago         S,
10.8.3.3              10.8.0.0/16          01:14:23 ago         S,C,
255.255.255.255      *10.0.0.0/8           01:30:04 ago         S,T,
------------------------------------------------------------------------------
Branch11#
```

Notes:

- Site-prefix database is infrastructure, used for enterprise traffic-classes learning and routing-control;
- Site-prefix database is in sync across the PfRv3 domain for all master controller and border routers;
- MCs publish local site prefixes to local BR and remote branch sites every 2 hours;
- MCs subscribe and learn all remote site-prefix from EIGRP SAF service;
- MCs and BRs age out all the site prefixes at a frequency of 24 hours;

Site-prefix monitor enabled on border router automatically:

```
Branch10#show domain one border pmi | begin prefix-learn
PMI[Egress-prefix-learn]-FLOW MONITOR[MON-Egress-prefix-learn-0-48-29]
    monitor-interval:30
    minimum-mask-length:28
    key-list:
      ipv4 source prefix
      ipv4 source mask
      routing vrf input
    Non-key-list:
      counter bytes long
      counter packets long
      timestamp absolute monitoring-interval start
    DSCP-list:N/A
    Class:CENT-Class-Egress-ANY-0-51

    Exporter-list:
      10.2.10.10
------------------------------------------------------------------------------
Branch10#


Branch10#show performance monitor cache monitor MON-Egress-prefix-learn-0-48-29 detail
 Monitor: MON-Egress-prefix-learn-0-48-29

 Data Collection Monitor:

  Cache type:                           Synchronized (Platform cache)
```

```
  Cache size:                                 700
  Current entries:                              1
  High Watermark:                               1

  Flows added:                                241
  Flows aged:                                 240
  Synchronized timeout (secs):                 30

IPV4 SRC PREFIX  IPV4 SRC MASK  IP VRF ID INPUT                          bytes long
pkts long  time monitor start
===============  =============  ==============================  ====================
====================  ==================
10.1.10.0                /24  0          (DEFAULT)                        1725067
17202        07:55:30.000

Branch10#

HubBR2#show performance monitor cache monitor MON-Egress-prefix-learn-0-48-39 detail
 Monitor: MON-Egress-prefix-learn-0-48-39

 Data Collection Monitor:

HubBR2#
```

Notes:

- Local site-prefix monitor activated for site-prefix-learning-period (30 secs);
- Site Prefix learned based on ipv4 source prefix and mask in CEF table;
- Site-prefix learn based on egress traffic observed on external interface(UDP/TCP/ICMP flows); exported to the local MC;
- We must disable automatic site-prefix learning on transit site like DMVPN Hub site; any mistake for site-prefix learning could result in unexpected results like traffic looping between sites due to messed site-prefix database;

6.2 Monitor Traffic Class

Check Traffic-class learning and control. This has to be done on Master Controllers. Remember that all Master Controllers are making local path decision, there is no Centralized MC making global decisions. Start with the traffic-class summary to get a summary view of all traffic and how it is controlled as well as their current path.

Here are the possible states for a Traffic Class:

- UNCONTROLLED: No parent route is found
- CONTROLLED: found a path that meets the criteria
- OUT OF POLICY: No path meets the criteria set in the policy

Example:

```
HubMC#show domain one master traffic-classes summary
```

```
APP - APPLICATION, TC-ID - TRAFFIC-CLASS-ID, APP-ID - APPLICATION-ID
SP - SERVICE PROVIDER, PC = PRIMARY CHANNEL ID,
BC - BACKUP CHANNEL ID, BR - BORDER, EXIT - WAN INTERFACE
UC - UNCONTROLLED, PE - PICK-EXIT, CN - CONTROLLED, UK - UNKNOWN

Dst-Site-Pfx      Dst-Site-Id APP            DSCP    TC-ID APP-ID    State  SP
PC/BC       BR/EXIT

10.1.10.0/24      10.2.10.10  N/A            af11    193   N/A       CN     MPLS
59/60       10.8.2.2/Tunnel100
10.1.10.0/24      10.2.10.10  N/A            cs1     192   N/A       CN     MPLS
57/58       10.8.2.2/Tunnel100
10.1.10.0/24      10.2.10.10  N/A            cs5     191   N/A       CN     MPLS
55/NA       10.8.2.2/Tunnel100
10.1.10.0/24      10.2.10.10  N/A            ef      190   N/A       CN     MPLS
52/NA       10.8.2.2/Tunnel100
10.1.10.0/24      10.2.10.10  N/A            af41    195   N/A       CN     INET
64/63       10.8.1.1/Tunnel200
10.1.10.0/24      10.2.10.10  N/A            cs4     189   N/A       CN     INET
54/53       10.8.1.1/Tunnel200
10.1.10.0/24      10.2.10.10  N/A            af31    194   N/A       CN     MPLS
61/62       10.8.2.2/Tunnel100
 Total Traffic Classes: 7 Site: 7  Internet: 0
HubMC#
```

Notes:

- Check destination Prefix (column Dst-Site-Pfx)
- Check App Id if Application policies are used - Will N/A if DSCP based policies are used
- Check DSCP value
- Check the associated state - should be controlled (CN)
- Check the path used - this is the path for all traffic going to this prefix with this DSCP value, i.e. Traffic Class. In our example all performance based policies should go to the preferred path MPLS.
- Check the local Border Router used and the external exit used.

From there you can drill down and check individual Traffic Classes on master controller:

```
HubMC#show domain one master traffic-classes

 Dst-Site-Prefix: 10.1.10.0/24        DSCP: af11 [10] Traffic class id:193
  TC Learned:                 00:22:13 ago
  Present State:              CONTROLLED
  Current Performance Status: not monitored (default class)
  Current Service Provider:   MPLS since 00:12:10
  Previous Service Provider:  INET for 298 sec
  BW Used:                    9195 Kbps
  Present WAN interface:      Tunnel100 in Border 10.8.2.2
  Present Channel (primary):  59
  Backup Channel:             60
  Destination Site ID:        10.2.10.10
  Class-Sequence in use:      default
  Class Name:                 default
  BW Updated:                 00:00:14 ago
  Reason for Route Change:    Load Balance
```

```
------------------------------------------------------------------------------

 Dst-Site-Prefix: 10.1.10.0/24        DSCP: cs1 [8] Traffic class id:192
  TC Learned:                 00:22:14 ago
  Present State:              CONTROLLED
  Current Performance Status: not monitored (default class)
  Current Service Provider:   MPLS since 00:12:40
  Previous Service Provider:  INET for 184 sec
  BW Used:                    9251 Kbps
  Present WAN interface:      Tunnel100 in Border 10.8.2.2
  Present Channel (primary):  57
  Backup Channel:             58
  Destination Site ID:        10.2.10.10
  Class-Sequence in use:      default
  Class Name:                 default
  BW Updated:                 00:00:12 ago
  Reason for Route Change:    Load Balance
------------------------------------------------------------------------------

 Dst-Site-Prefix: 10.1.10.0/24        DSCP: cs5 [40] Traffic class id:191
  TC Learned:                 00:32:43 ago
  Present State:              CONTROLLED
  Current Performance Status: not monitored (default class)
  Current Service Provider:   MPLS since 00:32:12
  Previous Service Provider:  Unknown
  BW Used:                    3647 Kbps
  Present WAN interface:      Tunnel100 in Border 10.8.2.2
  Present Channel (primary):  55
  Backup Channel:             none
  Destination Site ID:        10.2.10.10
  Class-Sequence in use:      default
  Class Name:                 default
  BW Updated:                 00:00:10 ago
  Reason for Route Change:    Uncontrolled to Controlled Transition
------------------------------------------------------------------------------

 Dst-Site-Prefix: 10.1.10.0/24        DSCP: ef [46] Traffic class id:190
  TC Learned:                 00:37:44 ago
  Present State:              CONTROLLED
  Current Performance Status: in-policy
  Current Service Provider:   MPLS since 00:37:13
  Previous Service Provider:  Unknown
  BW Used:                    5543 Kbps
  Present WAN interface:      Tunnel100 in Border 10.8.2.2
  Present Channel (primary):  52
  Backup Channel:             none
  Destination Site ID:        10.2.10.10
  Class-Sequence in use:      10
  Class Name:                 VOICE using policy User-defined
    priority 2 packet-loss-rate threshold 5.0 percent
    priority 1 one-way-delay threshold 150 msec
    priority 2 byte-loss-rate threshold 5.0 percent
  BW Updated:                 00:00:13 ago
  Reason for Route Change:    Uncontrolled to Controlled Transition
------------------------------------------------------------------------------

 Dst-Site-Prefix: 10.1.10.0/24        DSCP: af41 [34] Traffic class id:195
  TC Learned:                 00:22:11 ago
  Present State:              CONTROLLED
  Current Performance Status: in-policy
  Current Service Provider:   INET since 00:14:07
  Previous Service Provider:  MPLS for 181 sec
  BW Used:                    5495 Kbps
  Present WAN interface:      Tunnel200 in Border 10.8.1.1
  Present Channel (primary):  64
```

```
  Backup Channel:             63
  Destination Site ID:        10.2.10.10
  Class-Sequence in use:      20
  Class Name:                 VIDEO using policy User-defined
    priority 2 packet-loss-rate threshold 5.0 percent
    priority 1 one-way-delay threshold 150 msec
    priority 2 byte-loss-rate threshold 5.0 percent
  BW Updated:                 00:00:13 ago
  Reason for Route Change:    Backup to Primary path preference transition
------------------------------------------------------------------------------

 Dst-Site-Prefix: 10.1.10.0/24        DSCP: cs4 [32] Traffic class id:189
  TC Learned:                 00:37:44 ago
  Present State:              CONTROLLED
  Current Performance Status: in-policy
  Current Service Provider:   INET since 00:13:13
  Previous Service Provider:  MPLS for 181 sec
  BW Used:                    7276 Kbps
  Present WAN interface:      Tunnel200 in Border 10.8.1.1
  Present Channel (primary):  54
  Backup Channel:             53
  Destination Site ID:        10.2.10.10
  Class-Sequence in use:      20
  Class Name:                 VIDEO using policy User-defined
    priority 2 packet-loss-rate threshold 5.0 percent
    priority 1 one-way-delay threshold 150 msec
    priority 2 byte-loss-rate threshold 5.0 percent
  BW Updated:                 00:00:14 ago
  Reason for Route Change:    Backup to Primary path preference transition
------------------------------------------------------------------------------

 Dst-Site-Prefix: 10.1.10.0/24        DSCP: af31 [26] Traffic class id:194
  TC Learned:                 00:22:12 ago
  Present State:              CONTROLLED
  Current Performance Status: in-policy
  Current Service Provider:   MPLS since 00:21:41
  Previous Service Provider:  Unknown
  BW Used:                    9247 Kbps
  Present WAN interface:      Tunnel100 in Border 10.8.2.2
  Present Channel (primary):  61
  Backup Channel:             62
  Destination Site ID:        10.2.10.10
  Class-Sequence in use:      30
  Class Name:                 CRITICAL using policy User-defined
    priority 2 packet-loss-rate threshold 10.0 percent
    priority 1 one-way-delay threshold 600 msec
    priority 2 byte-loss-rate threshold 10.0 percent
  BW Updated:                 00:00:11 ago
  Reason for Route Change:    Uncontrolled to Controlled Transition
------------------------------------------------------------------------------
 Total Traffic Classes: 7 Site: 7  Internet: 0
HubMC#
```

Notes:

- Check present state
- Check current and (if any) previous provider
- Check the Traffic Class bandwidth
- Check current WAN interface

- Check present and backup channels. Performance measurements are extracted from channels. You will not get performance directly from the traffic class itself.
- Check that TC is correctly mapped to the policy

If a specific Traffic Class has experienced performance issues, you will be able to check it in the Traffic Class report:

```
HubMC#show domain one master traffic-classes policy VIDEO

 Dst-Site-Prefix: 10.1.10.0/24        DSCP: cs4 [32] Traffic class id:200
  TC Learned:                 00:06:00 ago
  Present State:              CONTROLLED
  Current Performance Status: in-policy
  Current Service Provider:   MPLS since 00:00:30 (hold until 59 sec)
  Previous Service Provider:  INET for 117 sec
  (A fallback provider. Primary provider will be re-evaluated 00:02:30 later)
  BW Used:                    309 Kbps
  Present WAN interface:      Tunnel100 in Border 10.8.2.2
  Present Channel (primary):  76
  Backup Channel:             73
  Destination Site ID:        10.2.10.10
  Class-Sequence in use:      20
  Class Name:                 VIDEO using policy User-defined
    priority 2 packet-loss-rate threshold 5.0 percent
    priority 1 one-way-delay threshold 150 msec
    priority 2 byte-loss-rate threshold 5.0 percent
  BW Updated:                 00:00:03 ago
  Reason for Route Change:    Delay
------------------------------------------------------------------------------

 Dst-Site-Prefix: 10.1.10.0/24        DSCP: af41 [34] Traffic class id:199
  TC Learned:                 00:06:01 ago
  Present State:              CONTROLLED
  Current Performance Status: in-policy
  Current Service Provider:   MPLS since 00:00:00 (hold until 89 sec)
  Previous Service Provider:  INET for 148 sec
  (A fallback provider. Primary provider will be re-evaluated 00:03:00 later)
  BW Used:                    177 Kbps
  Present WAN interface:      Tunnel100 in Border 10.8.2.2
  Present Channel (primary):  75
  Backup Channel:             71
  Destination Site ID:        10.2.10.10
  Class-Sequence in use:      20
  Class Name:                 VIDEO using policy User-defined
    priority 2 packet-loss-rate threshold 5.0 percent
    priority 1 one-way-delay threshold 150 msec
    priority 2 byte-loss-rate threshold 5.0 percent
  BW Updated:                 00:00:01 ago
  Reason for Route Change:    Delay
------------------------------------------------------------------------------
 Total Traffic Classes: 2 Site: 2  Internet: 0
HubMC#
```

Notes:

- Check Reason for recent Path Changes
- Check Service provider re-evaluated timer for every 3 minutes;

All traffic-classes are synced to border router which perform routing-control based on traffic-class database: show domain <name> border traffic-classes

```
HubBR2#show domain one border traffic-classes

 Src-Site-Prefix: ANY Dst-Site-Prefix: 10.1.10.0/24
  DSCP: cs5 [40] Traffic class id: 202
  TC Learned: 00:09:54 ago
  Present State: CONTROLLED
  Destination Site ID: 10.2.10.10
  If_index: 13
  Primary chan id: 72
  Primary chan Presence: LOCAL CHANNEL
  Primary interface: Tunnel200
  Primary Nexthop: 10.0.200.10 (BGP)
  Backup chan id: 78
  Backup chan Presence: NEIGHBOR_CHANNEL via border 10.8.2.2
  Backup interface: Tunnel0
-------------------------------------------------------------------------------

 Src-Site-Prefix: ANY Dst-Site-Prefix: 10.1.10.0/24
  DSCP: ef [46] Traffic class id: 201
  TC Learned: 00:09:55 ago
  Present State: CONTROLLED
  Destination Site ID: 10.2.10.10
  If_index: 14
  Primary chan id: 77
  Primary chan Presence: NEIGHBOR_CHANNEL via border 10.8.2.2
  Primary interface: Tunnel0
  Backup Channel not available
-------------------------------------------------------------------------------

 Src-Site-Prefix: ANY Dst-Site-Prefix: 10.1.10.0/24
  DSCP: cs4 [32] Traffic class id: 200
  TC Learned: 00:09:55 ago
  Present State: CONTROLLED
  Destination Site ID: 10.2.10.10
  If_index: 14
  Primary chan id: 76
  Primary chan Presence: NEIGHBOR_CHANNEL via border 10.8.2.2
  Primary interface: Tunnel0
  Backup chan id: 73
  Backup chan Presence: LOCAL CHANNEL
  Backup interface: Tunnel200
-------------------------------------------------------------------------------

 Src-Site-Prefix: ANY Dst-Site-Prefix: 10.1.10.0/24
  DSCP: af41 [34] Traffic class id: 199
  TC Learned: 00:09:56 ago
  Present State: CONTROLLED
  Destination Site ID: 10.2.10.10
  If_index: 14
  Primary chan id: 75
  Primary chan Presence: NEIGHBOR_CHANNEL via border 10.8.2.2
  Primary interface: Tunnel0
  Backup chan id: 71
  Backup chan Presence: LOCAL CHANNEL
  Backup interface: Tunnel200
-------------------------------------------------------------------------------

 Src-Site-Prefix: ANY Dst-Site-Prefix: 10.1.10.0/24
```

```
  DSCP: af11 [10] Traffic class id: 198
  TC Learned: 00:09:57 ago
  Present State: CONTROLLED
  Destination Site ID: 10.2.10.10
  If_index: 13
  Primary chan id: 70
  Primary chan Presence: LOCAL CHANNEL
  Primary interface: Tunnel200
  Primary Nexthop: 10.0.200.10 (BGP)
  Backup chan id: 69
  Backup chan Presence: NEIGHBOR_CHANNEL via border 10.8.2.2
  Backup interface: Tunnel0
------------------------------------------------------------------------------

 Src-Site-Prefix: ANY Dst-Site-Prefix: 10.1.10.0/24
  DSCP: cs1 [8] Traffic class id: 197
  TC Learned: 00:09:58 ago
  Present State: CONTROLLED
  Destination Site ID: 10.2.10.10
  If_index: 13
  Primary chan id: 68
  Primary chan Presence: LOCAL CHANNEL
  Primary interface: Tunnel200
  Primary Nexthop: 10.0.200.10 (BGP)
  Backup chan id: 67
  Backup chan Presence: NEIGHBOR_CHANNEL via border 10.8.2.2
  Backup interface: Tunnel0
------------------------------------------------------------------------------

 Src-Site-Prefix: ANY Dst-Site-Prefix: 10.1.10.0/24
  DSCP: af31 [26] Traffic class id: 196
  TC Learned: 00:09:58 ago
  Present State: CONTROLLED
  Destination Site ID: 10.2.10.10
  If_index: 14
  Primary chan id: 65
  Primary chan Presence: NEIGHBOR_CHANNEL via border 10.8.2.2
  Primary interface: Tunnel0
  Backup chan id: 66
  Backup chan Presence: LOCAL CHANNEL
  Backup interface: Tunnel200
------------------------------------------------------------------------------
HubBR2#
```

Notes:

- Check Present State, Primary and Backup channel for CONTROLLED TC
- Backup channel and interface is used for fast failover;
- Part of traffic-classes controlled to second border router over PFR auto-tunnel interface;

You could be able to check traffic-class rerouted over auto-tunnel interface to Hub BR1 for following example:

```
HubBR2#show interfaces tunnel0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Description: PFR auto-tunnel for VRF default
  Interface is unnumbered. Using address of Loopback0 (10.8.1.1)
```

```
  MTU 9972 bytes, BW 10000 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 255/255, rxload 13/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 10.8.1.1 (Loopback0)
   Tunnel Subblocks:
      src-track:
         Tunnel0 source tracking subblock associated with Loopback0
          Set of tunnels with source Loopback0, 1 member (includes iterators), on
interface <OK>
  Tunnel protocol/transport multi-GRE/IP
    Key 0x296C167, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1472 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 10:37:12
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 519000 bits/sec, 139 packets/sec
  5 minute output rate 20908000 bits/sec, 5753 packets/sec
     18497647 packets input, 6987200490 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     19871488 packets output, 9071014654 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
HubBR2#
```

You could be able to check traffic-class entries on IOS-XE platform database:

- show platform software pfrv3 rp active route-control traffic-class
- show platform software pfrv3 fp active route-control traffic-class
- show platform hardware qfp active feature pfrv3 client route-control traffic-class

```
HubBR2#show platform software pfrv3 rp active route-control traffic-class
CENT routing control traffic class:

Total number of CENT RC TC: 7

TC ID : 196
  Vrf id = 0
  Src prefix = 0.0.0.0/0, Dst prefix = 10.1.10.0/24
  Policy sequence = 30
  Dscp = 26, Application ID = 0
  Match type = Dscp, Protocol = 0
  Src port = 0, Dst port = 0
  Primary action
    Channel ID = 65, Adj ID = 65
  Backup action
    Channel ID = 66, Adj ID = 0

TC ID : 197
```

```
  Vrf id = 0
  Src prefix = 0.0.0.0/0, Dst prefix = 10.1.10.0/24
  Policy sequence = 4294967295
  Dscp = 8, Application ID = 0
  Match type = Dscp, Protocol = 0
  Src port = 0, Dst port = 0
  Primary action
    Channel ID = 68, Adj ID = 0
  Backup action
    Channel ID = 67, Adj ID = 65

[SNIP]


HubBR2#show platform software pfrv3 fp active route-control traffic-class
CENT routing control traffic class :

Total number of CENT RC TC: 7

TC ID : 196
  Vrf id = 0
  Src prefix = 0.0.0.0/0, Dst prefix = 10.1.10.0/24
  Policy sequence = 30
  Dscp = 26, Application ID = 0
  Match type = Dscp, Protocol = 0
  Src port = 0, Dst port = 0
  Primary action
    Channel ID = 65, Adj ID = 65
  Backup action
    Channel ID = 66, Adj ID = 0

TC ID : 197
  Vrf id = 0
  Src prefix = 0.0.0.0/0, Dst prefix = 10.1.10.0/24
  Policy sequence = 4294967295
  Dscp = 8, Application ID = 0
  Match type = Dscp, Protocol = 0
  Src port = 0, Dst port = 0
  Primary action
    Channel ID = 68, Adj ID = 0
  Backup action
    Channel ID = 67, Adj ID = 65

[SNIP]


HubBR2#show platform hardware qfp active feature pfrv3 client route-control traffic-
class detail
CENT QFP CLIENT ROUTING_CONTROL INFO

Num of TC: 7

TC ID: 196
  tbl id: 0, src pfx: 0.0.0.0/0, dst pfx: 10.1.10.0/24
  policy seq:    30
  TC match type: DSCP
    DSCP: 26
  actions:
    primary:
      chan id: 65, adj id: 65
    backup:
      chan id: 66, adj id: 0

TC ID: 197
  tbl id: 0, src pfx: 0.0.0.0/0, dst pfx: 10.1.10.0/24
```

```
  policy seq:    4294967295
  TC match type: DSCP
    DSCP: 8
  actions:
    primary:
      chan id: 68, adj id: 0
    backup:
      chan id: 67, adj id: 65

[SNIP]

HubBR2#
```

Notes:

- Traffic-classes database stored on fman-rp/fman-fp, and CPP Client on IOS-XE platform;
- These databases are in sync between master controller, border router PI/PD;
- Traffic-classes could be DSCP or application based, primary and backup channel is used for routing-control and fast-failover;

PfR routing-control is enabled automatically on ingress direction for LAN interfaces, and check whether CENT Routing-Control features get enabled properly, for example LAN interface **GigabitEthernet2 on hub BR2**:

```
HubBR2#show platform software interface rp active name GigabitEthernet2
HubBR2#show platform software interface rp active name GigabitEthernet2
Name: GigabitEthernet2, ID: 9, QFP ID: 0, Schedules: 4096
Type: PORT, State: enabled, SNMP ID: 4, MTU: 1500
Flow control ID: 65535
bandwidth: 1000000, encap: ARPA
IP Address: 10.8.25.5
Flags: ipv4
vNet Name: , vNet Tag: 0, vNet Extra Information: 0
CENT RC: enabled
CENT SMP INGRESS: enabled

HubBR2#show platform software interface fp active name GigabitEthernet2
Name: GigabitEthernet2, ID: 9, QFP ID: 9, Schedules: 4096
Type: PORT, State: enabled, SNMP ID: 4, MTU: 1500
TX channel ID: 0, RX channel ID: 0, AOM state: created
Flow control ID: 65535
bandwidth: 1000000, encap: ARPA
IP Address: 10.8.25.5
IPV6 Address: ::
Flags: ipv4
ICMP Flags: unreachables, redirects, no-info-reply, no-mask-reply
ICMP6 Flags: unreachables, redirects
FRR linkdown ID: 65535
vNet Tag: 0, vNet Extra Information: 0
AOM dependency sanity check: PASS
AOM Obj ID: 32
CENT RC: enabled
CENT SMP INGRESS: enabled
```

```
HubBR2#show platform hardware qfp active interface if-name GigabitEthernet2
General interface information
  Interface Name: GigabitEthernet2
  Interface state: VALID
  Platform interface handle: 9
  QFP interface handle: 9
  Rx uidb: 1020
  Tx uidb: 65527
  Channel: 33
Interface Relationships

BGPPA/QPPB interface configuration information
  Ingress: BGPPA/QPPB not configured. flags: 0000
  Egress : BGPPA not configured. flags: 0000

ipv4_input enabled.
ipv4_output enabled.
layer2_input enabled.
layer2_output enabled.
ess_ac_input enabled.

Features Bound to Interface:
 2 GIC FIA state
51 PUNT INJECT DB
41 VNIC Path
42 ethernet
 1 IFM
33 icmp_svr
35 ipfrag_svr
36 ipreass_svr
 8 FIA Activations ref-count
Protocol 0 - ipv4_input
FIA handle - CP:0x2d04a00  DP:0xe74c6a80
  IPV4_INPUT_DST_LOOKUP_ISSUE (M)
  IPV4_INPUT_ARL_SANITY (M)
  IPV4_INPUT_DST_LOOKUP_CONSUME (M)
  IPV4_INPUT_FOR_US_MARTIAN (M)
  IPV4_INPUT_STILE_LEGACY
  IPV4_INPUT_CENT_SMP_PROCESS
  IPV4_INPUT_CENT_RC_PROCESS
  IPV4_INPUT_LOOKUP_PROCESS (M)
  IPV4_INPUT_IPOPTIONS_PROCESS (M)
  IPV4_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 1 - ipv4_output
FIA handle - CP:0x2d04970  DP:0xe74c7300
  IPV4_VFR_REFRAG (M)
  IPV4_OUTPUT_L2_REWRITE (M)
  IPV4_OUTPUT_STILE_LEGACY
  IPV4_OUTPUT_FRAG (M)
  IPV4_OUTPUT_DROP_POLICY (M)
  MARMOT_SPA_D_TRANSMIT_PKT
  DEF_IF_DROP_FIA (M)
Protocol 8 - layer2_input
FIA handle - CP:0x2d05978  DP:0xe74b80c0
  LAYER2_INPUT_SIA (M)
  LAYER2_INPUT_LOOKUP_PROCESS (M)
  LAYER2_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 9 - layer2_output
FIA handle - CP:0x2d052b8  DP:0xe74be6c0
  LAYER2_OUTPUT_SERVICEWIRE (M)
  LAYER2_OUTPUT_DROP_POLICY (M)
  MARMOT_SPA_D_TRANSMIT_PKT
  DEF_IF_DROP_FIA (M)
Protocol 14 - ess_ac_input
FIA handle - CP:0x2d05270  DP:0xe74beb00
```

```
  PPPOE_GET_SESSION
  ESS_ENTER_SWITCHING
  PPPOE_HANDLE_UNCLASSIFIED_SESSION
  DEF_IF_DROP_FIA (M)

QfpEth Physical Information
  DPS Addr: 0x00000000034b18f0
  Submap Table Addr: 0x00000000
  VLAN Ethertype: 0x8100
  QOS Mode: Per Link
  VLAN AutoSense: No
```

Notes:

- Check CENT RC and CENT SMP INGRESS status should be "enabled" on LAN interface;
- IPV4_INPUT_CENT_SMP_PROCESS is used for WAN interface discovery or channel stats accounting;
- IPV4_INPUT_STILE_LEGACY is enabled by NBAR2 for application classification, this is only available when application based policy configured;
- PFRv3 routing-control feature logic runs in IPV4_INPUT_CENT_RC_PROCESS ;

On wan interface, there are PfR related features like SMP ingress/egress and MMA/FME/FNF feature enabled automatically, for example WAN interface Tunnel100 on Hub BR1:

```
HubBR1#show platform software interface rp active name Tunnel100
Name: Tunnel100, ID: 14, QFP ID: 0, Schedules: 0
Type: TUNNEL, State: enabled, SNMP ID: 9, MTU: 9976
IP Address: 10.0.100.84
TCP Adjust Mss Enabled: 1360
Flags: ipv4
ICMP Flags: unreachables, no-redirects, no-info-reply, no-mask-reply
vNet Name: , vNet Tag: 0, vNet Extra Information: 0
Tunnel Source: 172.16.84.4, Tunnel Destination: 0.0.0.0
Tunnel TTL: 255, Tunnel TOS: 0, Flags: KEY
Tunnel Mode: IPv4 multi-point GRE, VRF: 0, Tunnel VRF: 0
Tunnel IPv6 PMTU: 0, Tunnel APP_ID: TUN_APP_CLI, Tunnel APP_DATA: 0
VLAN ID: 0, virtual mac: 0000.0000.0000
Tunnel lport: 0, Tunnel rport: 0
Tunnel entropy: FALSE
IPSec: attached
CENT SMP INGRESS: enabled
CENT SMP EGRESS: enabled
CENT COLOR: MPLS


HubBR1#show platform software interface fp active name Tunnel100
Name: Tunnel100, ID: 14, QFP ID: 13, Schedules: 0
Type: TUNNEL, State: enabled, SNMP ID: 9, MTU: 9976
IP Address: 10.0.100.84
IPV6 Address: ::
TCP Adjust Mss Enabled: 1360
Flags: ipv4
ICMP Flags: unreachables, no-redirects, no-info-reply, no-mask-reply
ICMP6 Flags: unreachables, redirects
FRR linkdown ID: 65535
```

```
vNet Tag: 0, vNet Extra Information: 0
AOM dependency sanity check: PASS
AOM Obj ID: 5587
Tunnel Source: 172.16.84.4, Tunnel Destination: 0.0.0.0
Tunnel TTL: 255, Tunnel TOS: 0, Flags: KEY
Tunnel Mode: IPv4 multi-point GRE, VRF: 0, Tunnel VRF: 0
Tunnel IPv6 PMTU: 0, Tunnel APP_ID: TUN_APP_CLI, Tunnel APP_DATA: 0
VLAN ID: 0, virtual mac: 0000.0000.0000
Tunnel lport: 0, Tunnel rport: 0
Tunnel entropy: FALSE
IPSec: attached
CENT SMP INGRESS: enabled
CENT SMP EGRESS: enabled
CENT COLOR: MPLS

HubBR1#show platform hardware qfp active interface if-name Tunnel100
General interface information
  Interface Name: Tunnel100
  Interface state: VALID
  Platform interface handle: 14
  QFP interface handle: 13
  Rx uidb: 65529
  Tx uidb: 65523
  Channel: 0
Interface Relationships

BGPPA/QPPB interface configuration information
  Ingress: BGPPA/QPPB not configured. flags: 0000
  Egress : BGPPA not configured. flags: 0000

ipv4_input enabled.
ipv4_output enabled.
layer2_input enabled.
layer2_output enabled.

Features Bound to Interface:
 2 GIC FIA state
51 PUNT INJECT DB
28 CPP TUNNEL
33 icmp_svr
35 ipfrag_svr
36 ipreass_svr
13 CPP IPSEC
Protocol 0 - ipv4_input
FIA handle - CP:0x1e83f00  DP:0xe7566e00
  IPV4_INPUT_DST_LOOKUP_ISSUE (M)
  IPV4_INPUT_ARL_SANITY (M)
  IPV4_INPUT_SRC_LOOKUP_ISSUE
  IPV4_INPUT_DST_LOOKUP_CONSUME (M)
  IPV4_INPUT_SRC_LOOKUP_CONSUME
  IPV4_INPUT_FOR_US_MARTIAN (M)
  IPV4_INPUT_STILE_LEGACY
  IPV4_INGRESS_MMA_LOOKUP
  IPV4_INPUT_FME_PROCESS
  INPUT_FNF_AOR_FIRST
  IPV4_INPUT_FNF_FIRST
  IPV4_INPUT_CENT_SMP_PROCESS
  IPV4_INPUT_TCP_ADJUST_MSS
  IPV4_INPUT_LOOKUP_PROCESS (M)
  INPUT_FNF_AOR_FINAL
  IPV4_INPUT_FNF_FINAL
  INPUT_FNF_AOR_RELEASE
  IPV4_INPUT_IPOPTIONS_PROCESS (M)
  IPV4_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 1 - ipv4_output
```

```
FIA handle - CP:0x1e83de0  DP:0xe7567f00
  IPV4_OUTPUT_TCP_ADJUST_MSS
  MC_OUTPUT_GEN_RECYCLE (D)
  IPV4_VFR_REFRAG (M)
  IPV4_OUTPUT_SRC_LOOKUP_ISSUE
  IPV4_OUTPUT_L2_REWRITE (M)
  IPV4_OUTPUT_SRC_LOOKUP_CONSUME
  IPV4_OUTPUT_CENT_SMP_PROCESS
  IPV4_OUTPUT_FRAG (M)
  IPV4_EGRESS_MMA_LOOKUP
  TUNNEL_OUTPUT_FNF_AOR
  IPV4_TUNNEL_OUTPUT_FNF_FINAL
  TUNNEL_OUTPUT_FNF_AOR_RELEASE
  IPV4_TUNNEL_OUTPUT_FINAL
  IPV4_OUTPUT_TUNNEL_PROTECTION_ENCRYPT
  IPV4_TUNNEL_GOTO_OUTPUT
  IPV4_OUTPUT_DROP_POLICY (M)
  OUTPUT_FNF_AOR
  IPV4_OUTPUT_FNF_FINAL
  OUTPUT_FNF_AOR_RELEASE
  DEF_IF_DROP_FIA (M)
Protocol 8 - layer2_input
FIA handle - CP:0x1e84968  DP:0xe755d0c0
  LAYER2_INPUT_SIA (M)
  LAYER2_INPUT_LOOKUP_PROCESS (M)
  LAYER2_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 9 - layer2_output
FIA handle - CP:0x1e83be8  DP:0xe7569cc0
  MC_OUTPUT_GEN_RECYCLE (D)
  LAYER2_OUTPUT_SERVICEWIRE (M)
  IPV4_OUTPUT_L2_REWRITE
  IPV4_TUNNEL_OUTPUT_FINAL
  IPV4_OUTPUT_TUNNEL_PROTECTION_ENCRYPT
  IPV4_TUNNEL_GOTO_OUTPUT
  LAYER2_OUTPUT_DROP_POLICY (M)
  DEF_IF_DROP_FIA (M)

HubBR1#
```

Notes:

- CENT SMP INGRESS is responsible for ingress channel accounting and smart-probes
- CENT SMP EGRESS is responsible for egress channel accounting and smart-probes
- MMA/FME/FNF is programmed to enable performance monitoring for prefix/traffic-classes learning, and channel performance monitoring;

6.3 Monitor Channels

NORMAL SITUATION

Let's assume the active channel for TC branch10/DSCP EF is 89, the backup channel was 91 you can check the channel performance of the active channel:

```
HubMC#show domain one master channels dscp ef
   Legend: * (Value obtained from Network delay:)
```

```
Channel Id: 89  Dst Site-Id: 10.2.10.10  Link Name: MPLS  DSCP: ef [46] TCs: 1
  Channel Created: 00:01:15 ago
  Provisional State: Initiated and open
  Operational state: Available
  Interface Id: 14
  Estimated Channel Egress Bandwidth: 5380 Kbps
  Immitigable Events Summary:
   Total Performance Count: 0, Total BW Count: 0
   TCA Statitics:
      Received 0 ; Processed 0 ; Unreach_rcvd:0
```

Notes:

- Channel is a unique combination of Dst Site-Id, Path name, and DSCP;
- Channel is created when there is a new DSCP(from real traffic) or a new interface(new service provider) or a new site added
- Channel declare as RX unreachable when no traffic over channel over 1 second monitor interval Channel is deleted if idle for 5 minutes when all traffic-classes on channel get aging out
- Performance is measured per channel on remote site, and feedback to source site in case of performance violation;
- Source MC receives TCA and ODE , then make a policy decision when there is policy violated;

Note that you do not have any performance metrics. This is because no performance issues were discovered hence no TCA received on the central site, thus no TCA/ODE received on the channel.

You can get the performance metrics from the backup channel. Remember that performance measurement is done on the remote site on ingress based on a performance monitor applied to all external interfaces.

```
HubMC#show domain one master channels | beg Id: 91
Channel Id: 91  Dst Site-Id: 10.2.10.10  Link Name: INET  DSCP: ef [46] TCs: 0
  Channel Created: 00:01:15 ago
  Provisional State: Initiated and open
  Operational state: Available
  Interface Id: 13
  Estimated Channel Egress Bandwidth: 8 Kbps
  Immitigable Events Summary:
   Total Performance Count: 0, Total BW Count: 0
   TCA Statitics:
      Received 0 ; Processed 0 ; Unreach_rcvd:0

[SNIP]
```

Note that you do not have any performance metrics either. Same reason here, this is because no performance issues were discovered hence no TCA received on the central site.

```
Branch10#show domain one border exporter statistics
show on-demand exporter(default vrf)

On-demand exporter statistics:
Border: 10.2.10.10
```

```
 Process ID: SEND=176, RECV=523

 Interface: Tunnel200 (index=15, service provider=INET)
  Bandwidth: Ingress=23464 Kbit/sec, Capacity=50000 Kbit/sec
             Egress =7609 Kbit/sec, Capacity=50000 Kbit/sec

   Total sent BW packets:              0
   Total sent BW templates:            0, Last sent: not yet sent

 Interface: Tunnel100 (index=14, service provider=MPLS)
  Bandwidth: Ingress=30285 Kbit/sec, Capacity=50000 Kbit/sec
             Egress =3757 Kbit/sec, Capacity=50000 Kbit/sec

   Total sent BW packets:              0
   Total sent BW templates:            0, Last sent: not yet sent

 Global Stats:
   Table ID lookup count: 0
   Table ID Channel found count: 0
   Table ID Next hop found count: 0
Branch10#
```

Notes:

- exporter statistics is clear and no TCA and ODE exported to remote site;

You can check the per-channel performance metrics in detail on the remote border router : show performance monitor history;

```
Branch10#show performance monitor history

Codes: *    - field is not configurable under flow record
       NA - field is not applicable for configured parameters
       UR - field is unreportable for configured parameters

Match: pfr site source id ipv4 = 10.8.3.3, pfr site destination id ipv4 = 10.2.10.10,
ip dscp = 0x20, interface input = Tu200, policy performance-monitor classification
hierarchy = CENT-Policy-Ingress-0-9: CENT-Class-Ingress-DSCP-cs4-0-24,
 Monitor: MON-Ingress-per-DSCP-0-48-11

 start time                                          16:43:30
                                                     ====================
 *history bucket number                            : 1
 transport packets expected counter                : 36953
 transport packets lost counter                    : 0
 transport packets lost rate                 ( % ) : 0.00
 transport bytes expected                          : 1223104
 transport bytes lost                              : 0
 transport bytes lost rate                         : 0.00
 pfr one-way-delay samples                         : 0
 pfr one-way-delay sum                             : 0
 pfr one-way-delay                                 : NA
 network delay sample                              : 3
 network delay sum                                 : 11
 network delay average                             : 3
 transport rtp jitter inter arrival samples        : 36903
 transport rtp jitter inter arrival sum            : 44276934
 transport rtp jitter inter arrival mean           : 1199
```

```
 counter bytes long                                    : 27281243
 counter packets long                                  : 69331
 timestamp absolute monitoring-interval start          : 16:43:30.000

Match: pfr site source id ipv4 = 10.8.3.3, pfr site destination id ipv4 = 10.2.10.10,
ip dscp = 0x2E, interface input = Tu200, policy performance-monitor classification
hierarchy = CENT-Policy-Ingress-0-9: CENT-Class-Ingress-DSCP-ef-0-22,
 Monitor: MON-Ingress-per-DSCP-0-48-11

 start time                                              16:43:30
                                                         ====================
 *history bucket number                                : 1
 transport packets expected counter                    : 593
 transport packets lost counter                        : 0
 transport packets lost rate                    ( % ) : 0.00
 transport bytes expected                              : 0
 transport bytes lost                                  : 0
 transport bytes lost rate                             : 0.00
 pfr one-way-delay samples                             : 0
 pfr one-way-delay sum                                 : 0
 pfr one-way-delay                                     : NA
 network delay sample                                  : 593
 network delay sum                                     : 1881
 network delay average                                 : 3
 transport rtp jitter inter arrival samples            : 593
 transport rtp jitter inter arrival sum                : 514268
 transport rtp jitter inter arrival mean               : 867
 counter bytes long                                    : 42696
 counter packets long                                  : 593
 timestamp absolute monitoring-interval start          : 16:43:30.000
```

Notes:

- Destination site calculates delay metric based on the timestamp the smart-probe only;
- one-way-delay is half of round-trip time between two sites(network-delay-avg);
- Jitter and packet loss metrics are measured based on RTP flows, either by data traffic or smart-probe RTP traffic when channel is idle;
- Byte loss metrics measured by per TCP data flows;
- All Jitter, Packet/Byte Loss metrics are measured per flow level by FME/MMA, but aggregated per channel

DELAY INCREASE

Let's assume we have a performance issue due to delay on the second path INET with 180 ms one-way-delay.

Let's check what happens on the primary channel #91 for TC to branch10 with DSCP EF:

```
HubMC#show domain one master channels dscp ef
   Legend: * (Value obtained from Network delay:)

Channel Id: 87  Dst Site-Id: 10.2.10.10  Link Name: MPLS  DSCP: ef [46] TCs: 1
  Channel Created: 01:10:18 ago
  Provisional State: Initiated and open
```

```
  Operational state: Available
  Interface Id: 14
  Estimated Channel Egress Bandwidth: 10013 Kbps
  Immitigable Events Summary:
   Total Performance Count: 0, Total BW Count: 0
  ODE Stats Bucket Number: 1
   Last Updated  : 00:00:21 ago
    Packet Count  : 88859
    Byte Count    : 38451203
    One Way Delay : 1 msec*
    Loss Rate Pkts: 0.0 %
    Loss Rate Byte: 0.0 %
    Jitter Mean   : 199 usec
    Unreachable   : FALSE
  ODE Stats Bucket Number: 2
   Last Updated  : 00:00:51 ago
    Packet Count  : 88908
    Byte Count    : 38459895
    One Way Delay : 1 msec*
    Loss Rate Pkts: 0.0 %
    Loss Rate Byte: 0.0 %
    Jitter Mean   : 293 usec
    Unreachable   : FALSE
   TCA Statitics:
      Received 0 ; Processed 0 ; Unreach_rcvd:0


Channel Id: 91  Dst Site-Id: 10.2.10.10  Link Name: INET  DSCP: ef [46] TCs: 0
  Channel Created: 01:10:19 ago
  Provisional State: Initiated and open
  Operational state: Available
  Interface Id: 13
  Estimated Channel Egress Bandwidth: 49 Kbps
  Immitigable Events Summary:
   Total Performance Count: 0, Total BW Count: 0
  ODE Stats Bucket Number: 1
   Last Updated  : 00:00:21 ago
    Packet Count  : 603
    Byte Count    : 43416
    One Way Delay : 180 msec*
    Loss Rate Pkts: 0.0 %
    Loss Rate Byte: 0.0 %
    Jitter Mean   : 547 usec
    Unreachable   : FALSE
  ODE Stats Bucket Number: 2
   Last Updated  : 00:00:51 ago
    Packet Count  : 603
    Byte Count    : 43416
    One Way Delay : 180 msec*
    Loss Rate Pkts: 0.0 %
    Loss Rate Byte: 0.0 %
    Jitter Mean   : 535 usec
    Unreachable   : FALSE
   TCA Statitics:
      Received 131 ; Processed:131 ; Unreach_rcvd:0
  Latest TCA Bucket
   Last Updated  : 00:00:21 ago
    One Way Delay : 180 msec*
    Loss Rate Pkts: NA
    Loss Rate Byte: NA
    Jitter Mean   : NA
    Unreachability: FALSE

 [SNIP]
```

Notes:

- Latest TCA Bucket reports "**One Way Delay : 180 msec***" for channel #91 that corresponds to branch10 with DSCP EF;
- The traffic-class get moved to backup channel #87 as soon when TCA reported on the primary channel;
- Destination border router exports ODE metrics together TCA for impacted channels; on source MC, ODE received are listed so that you can now check the performance metrics
- The channel #91 TCA get clear after two monitor intervals (60s) without new TCA reported;

TCA network-delay get incremented by 3 in one monitor interval after we inject bidirectional one-way-delay 180ms over INET service provider cloud**:**

```
Branch10#show domain one border exporter statistics
show on-demand exporter(default vrf)

On-demand exporter statistics:
Border: 10.2.10.10
 Process ID: SEND=176, RECV=523

 Interface: Tunnel200 (index=15, service provider=INET)
  Bandwidth: Ingress=4471 Kbit/sec, Capacity=50000 Kbit/sec
             Egress =409 Kbit/sec, Capacity=50000 Kbit/sec

   Total sent BW packets:              10
   Total sent BW templates:            1, Last sent: 4 min 31 sec ago

  Destination-site: 10.8.3.3:
   Total sent TCA network-delay        3
   Total sent ODE                      3
   Total sent TCA templates:           1, Last sent: 0 min 2 sec ago

 Interface: Tunnel100 (index=14, service provider=MPLS)
  Bandwidth: Ingress=44080 Kbit/sec, Capacity=50000 Kbit/sec
             Egress =9966 Kbit/sec, Capacity=50000 Kbit/sec

   Total sent BW packets:              10
   Total sent BW templates:            1, Last sent: 4 min 31 sec ago

  Destination-site: 10.8.3.3:
   Total sent ODE                      3
   Total sent TCA templates:           1, Last sent: 0 min 2 sec ago

  Number of TCA via other interfaces   3 sent, 0 err, 0 no nexthop

 Global Stats:
   Table ID lookup count: 12
   Table ID Channel found count: 12
   Table ID Next hop found count: 12
Branch10#
```

Notes:

- exporter statistics shows that INET network-delay TCA exported to hub site 10.8.3.3 for service provider path INET;
- ODE exported to hub site 10.8.3.3 for service provider path MPLS as well;

```
Branch10#show performance monitor history

Codes: *    - field is not configurable under flow record
       NA - field is not applicable for configured parameters
       UR - field is unreportable for configured parameters

Match: pfr site source id ipv4 = 10.8.3.3, pfr site destination id ipv4 = 10.2.10.10,
ip dscp = 0x20, interface input = Tu200, policy performance-monitor classification
hierarchy = CENT-Policy-Ingress-0-9: CENT-Class-Ingress-DSCP-cs4-0-24,
 Monitor: MON-Ingress-per-DSCP-0-48-11

 start time                                              16:46:30
                                                         ====================
 *history bucket number                                : 1
 transport packets expected counter                    : 36011
 transport packets lost counter                        : 0
 transport packets lost rate                    ( % ) : 0.00
 transport bytes expected                              : 398132
 transport bytes lost                                  : 0
 transport bytes lost rate                             : 0.00
 pfr one-way-delay samples                             : 0
 pfr one-way-delay sum                                 : 0
 pfr one-way-delay                                     : NA
 network delay sample                                  : 3
 network delay sum                                     : 1090
 network delay average                                 : 363
 transport rtp jitter inter arrival samples            : 35961
 transport rtp jitter inter arrival sum                : 26620988
 transport rtp jitter inter arrival mean               : 740
 counter bytes long                                    : 13462166
 counter packets long                                  : 37193
 timestamp absolute monitoring-interval start          : 16:46:30.000


Codes: *    - field is not configurable under flow record
       NA - field is not applicable for configured parameters
       UR - field is unreportable for configured parameters

Match: pfr site source id ipv4 = 10.8.3.3, pfr site destination id ipv4 = 10.2.10.10,
ip dscp = 0x2E, interface input = Tu200, policy performance-monitor classification
hierarchy = CENT-Policy-Ingress-0-9: CENT-Class-Ingress-DSCP-ef-0-22,
 Monitor: MON-Ingress-per-DSCP-0-48-11

 start time                                              16:46:30
                                                         ====================
 *history bucket number                                : 1
 transport packets expected counter                    : 603
 transport packets lost counter                        : 0
 transport packets lost rate                    ( % ) : 0.00
 transport bytes expected                              : 0
 transport bytes lost                                  : 0
 transport bytes lost rate                             : 0.00
 pfr one-way-delay samples                             : 0
 pfr one-way-delay sum                                 : 0
 pfr one-way-delay                                     : NA
 network delay sample                                  : 603
 network delay sum                                     : 217560
```

```
 network delay average                                : 360
 transport rtp jitter inter arrival samples           : 603
 transport rtp jitter inter arrival sum               : 319853
 transport rtp jitter inter arrival mean              : 530
 counter bytes long                                   : 43416
 counter packets long                                 : 603
 timestamp absolute monitoring-interval start         : 16:46:30.000
```

Notes:

- exporter statistics reports TCA and ODE exported to remote site;
- one-way-delay is 180ms with network delay average 360 while policy threshold is 150ms**;**
- Packet/byte lost is based on loss percentage; while jitter metrics is measured based on RTP flows per ns

Beside the ingress performance measurement on border router, all of the channels synced to local border router maintain channel TX/RX reachability status: show domain <name> border channels

```
HubBR2#show domain one border channels
Border Smart Probe Stats:

Channel id: 21
  Channel dscp: 0
  Channel site: 255.255.255.255
  Channel interface: Tunnel200
  Channel operation state: Initiated_n_open
  Channel RX state: reachable
  Channel TX state: reachable
  Channel next hop: 0.0.0.0
  Channel recv_probes: 0
  Channel send_probes: 0
  Channel recv_packets: 0
  Channel send_packets: 0
  Channel recv_bytes: 0
  Channel send_bytes 0
  Last Probe Received: N/A
  Last Probe Sent: N/A

Channel id: 23
  Channel dscp: 0
  Channel site: 10.2.11.11
  Channel interface: Tunnel200
  Channel operation state: Initiated_n_open
  Channel RX state: reachable
  Channel TX state: reachable
  Channel next hop: 10.0.200.11
  Channel recv_probes: 980116
  Channel send_probes: 979593
  Channel recv_packets: 0
  Channel send_packets: 0
  Channel recv_bytes: 0
  Channel send_bytes 0
  Last Probe Received: 263 ms Ago
  Last Probe Sent: 74 ms Ago

Channel id: 25
  Channel dscp: 0
```

```
  Channel site: 10.2.10.10
  Channel interface: Tunnel200
  Channel operation state: Initiated_n_open
  Channel RX state: reachable
  Channel TX state: reachable
  Channel next hop: 10.0.200.10
  Channel recv_probes: 851302
  Channel send_probes: 948804
  Channel recv_packets: 0
  Channel send_packets: 610454
  Channel recv_bytes: 0
  Channel send_bytes 41510872
  Last Probe Received: 129 ms Ago
  Last Probe Sent: 259 ms Ago

Channel id: 88
  Channel dscp: 32
  Channel site: 10.2.10.10
  Channel interface: Tunnel200
  Channel operation state: Initiated_n_open
  Channel RX state: reachable
  Channel TX state: reachable
  Channel next hop: 10.0.200.10
  Channel recv_probes: 9149
  Channel send_probes: 8848
  Channel recv_packets: 386704
  Channel send_packets: 1175118
  Channel recv_bytes: 55527581
  Channel send_bytes 494292492
  Last Probe Received: 582 ms Ago
  Last Probe Sent: 7542 ms Ago

Channel id: 91
  Channel dscp: 46
  Channel site: 10.2.10.10
  Channel interface: Tunnel200
  Channel operation state: Initiated_n_open
  Channel RX state: reachable
  Channel TX state: reachable
  Channel next hop: 10.0.200.10
  Channel recv_probes: 16099
  Channel send_probes: 19038
  Channel recv_packets: 0
  Channel send_packets: 22484
  Channel recv_bytes: 0
  Channel send_bytes 10338531
  Last Probe Received: 225 ms Ago
  Last Probe Sent: 24 ms Ago
```

Notes:

- Smart Probe and Data packets counted per channel;
- Smart-probe is RTP stream per DSCP sent over UDP with src port 18000 and dst port 19000 by default;
- Smart Probes sent over all channels periodically, 10 packets per 500ms if channel is idle and 1 packet per 10s if real traffic exists;

Channel Parent-Route and Next-hop Lookup

Traffic-classes get controlled over the channel, and next-hop for channel is determined based on the existing routing protocols over between peering sites, for example EIGRP, BGP, STATIC, NHRP and RIB Tables:

```
HubBR2#show domain one border parent-route
Border Parent Route Details:

Prot: BGP, Network: 10.2.10.10/32, Gateway: 10.0.200.10, Interface: Tunnel200, Ref
count: 8
Prot: BGP, Network: 10.2.11.11/32, Gateway: 10.0.200.11, Interface: Tunnel200, Ref
count: 1

HubBR2#show domain one border channels parent-route
Border Channel Parent Route Details:

Channel id: 21, Dscp: defa [0], Site-Id: 255.255.255.255, Path: INET, Interface:
Tunnel200
  Nexthop: 0.0.0.0
  Protocol: None

Channel id: 23, Dscp: defa [0], Site-Id: 10.2.11.11, Path: INET, Interface: Tunnel200
  Nexthop: 10.0.200.11
  Protocol: BGP

Channel id: 25, Dscp: defa [0], Site-Id: 10.2.10.10, Path: INET, Interface: Tunnel200
  Nexthop: 10.0.200.10
  Protocol: BGP

Channel id: 88, Dscp: cs4  [20], Site-Id: 10.2.10.10, Path: INET, Interface: Tunnel200
  Nexthop: 10.0.200.10
  Protocol: BGP

Channel id: 91, Dscp: ef   [2E], Site-Id: 10.2.10.10, Path: INET, Interface: Tunnel200
  Nexthop: 10.0.200.10
  Protocol: BGP

Channel id: 92, Dscp: af11 [A], Site-Id: 10.2.10.10, Path: INET, Interface: Tunnel200
  Nexthop: 10.0.200.10
  Protocol: BGP

HubBR2#

HubBR2#show domain one border channels dscp ef
Border Smart Probe Stats:

Channel id: 91
  Channel dscp: 46
  Channel site: 10.2.10.10
  Channel interface: Tunnel200
  Channel operation state: Initiated_n_open
  Channel RX state: reachable
  Channel TX state: reachable
  Channel next hop: 10.0.200.10
  Channel recv_probes: 26535
  Channel send_probes: 30203
  Channel recv_packets: 0
  Channel send_packets: 22484
  Channel recv_bytes: 0
  Channel send_bytes 10338531
  Last Probe Received: 4 ms Ago
  Last Probe Sent: 253 ms Ago

HubBR2#
```

Notes:

- Perform parent lookup in Routing Tables before creating any channel for a given site-id on the border router;
- Channel next-hop will be “0.0.0.0” and not-available if parent-route lookup failed;
- Channel is “Initiated_n_open” if there is active traffic-classes over the channel, otherwise “Discovered_n_open” state;
- Check last Probe Sent /Received timestamp for fast and low rate SMPs;

Let us review the detailed channel status on the border router:

```
HubBR2#show domain one border channels
Border Smart Probe Stats:

Channel id: 93
  Channel dscp: 0
  Channel site: 255.255.255.255
  Channel interface: Tunnel200
  Channel operation state: Initiated_n_open
  Channel RX state: reachable
  Channel TX state: reachable
  Channel next hop: 0.0.0.0
  Channel recv_probes: 0
  Channel send_probes: 0
  Channel recv_packets: 0
  Channel send_packets: 0
  Channel recv_bytes: 0
  Channel send_bytes 0
  Last Probe Received: N/A
  Last Probe Sent: N/A

Channel id: 23
  Channel dscp: 0
  Channel site: 10.2.10.10
  Channel interface: Tunnel200
  Channel operation state: Initiated_n_open
  Channel RX state: reachable
  Channel TX state: reachable
  Channel next hop: 10.0.200.10
  Channel recv_probes: 1846194
  Channel send_probes: 2600488
  Channel recv_packets: 0
  Channel send_packets: 0
  Channel recv_bytes: 0
  Channel send_bytes 0
  Last Probe Received: 27 ms Ago
  Last Probe Sent: 152 ms Ago

Channel id: 91
  Channel dscp: 46
  Channel site: 10.2.10.10
  Channel interface: Tunnel200
  Channel operation state: Initiated_n_open
  Channel RX state: reachable
  Channel TX state: reachable
  Channel next hop: 10.0.200.10
  Channel recv_probes: 1843666
  Channel send_probes: 2597208
```

```
  Channel recv_packets: 201887
  Channel send_packets: 243503
  Channel recv_bytes: 29002876
  Channel send_bytes 112020160
  Last Probe Received: 15 ms Ago
  Last Probe Sent: 126 ms Ago

Channel id: 92
  Channel dscp: 10
  Channel site: 10.2.10.10
  Channel interface: Tunnel200
  Channel operation state: Initiated_n_open
  Channel RX state: reachable
  Channel TX state: reachable
  Channel next hop: 10.0.200.10
  Channel recv_probes: 1803863
  Channel send_probes: 2594827
  Channel recv_packets: 6677835
  Channel send_packets: 307136
  Channel recv_bytes: 959117414
  Channel send_bytes 120332489
  Last Probe Received: 8810 ms Ago
  Last Probe Sent: 121 ms Ago

HubBR2#show domain one border neighbor-channels
 Channel id: 20; Channel exit state: UP; Belonging to Border: 10.8.1.1; Reachability:
Reachable

 Channel id: 22; Channel exit state: UP; Belonging to Border: 10.8.1.1; Reachability:
Reachable

 Channel id: 24; Channel exit state: UP; Belonging to Border: 10.8.1.1; Reachability:
Reachable

 Channel id: 79; Channel exit state: UP; Belonging to Border: 10.8.1.1; Reachability:
Reachable

 Channel id: 80; Channel exit state: UP; Belonging to Border: 10.8.1.1; Reachability:
Reachable

 Channel id: 81; Channel exit state: UP; Belonging to Border: 10.8.1.1; Reachability:
Reachable

 Channel id: 82; Channel exit state: UP; Belonging to Border: 10.8.1.1; Reachability:
Reachable

 Channel id: 89; Channel exit state: UP; Belonging to Border: 10.8.1.1; Reachability:
Reachable

 Channel id: 90; Channel exit state: UP; Belonging to Border: 10.8.1.1; Reachability:
Reachable

HubBR2#show platform software pfrv3 rp active channel local
CENT local channel :

Total number of CENT local channel: 10

Channel id : 21
  Vrf id = 0, Site id = 255.255.255.255
  Dscp = 0, IF handle = 13, Tx state = reachable
  Next hop = 0.0.0.0, Channel status = Initiated open

Channel id : 23
  Vrf id = 0, Site id = 10.2.11.11
  Dscp = 0, IF handle = 13, Tx state = reachable
```

```
  Next hop = 10.0.200.11, Channel status = Initiated open

[SNIP]

Channel id : 88
  Vrf id = 0, Site id = 10.2.10.10
  Dscp = 32, IF handle = 13, Tx state = reachable
  Next hop = 10.0.200.10, Channel status = Initiated open

Channel id : 91
  Vrf id = 0, Site id = 10.2.10.10
  Dscp = 46, IF handle = 13, Tx state = reachable
  Next hop = 10.0.200.10, Channel status = Initiated open

Channel id : 92
  Vrf id = 0, Site id = 10.2.10.10
  Dscp = 10, IF handle = 13, Tx state = reachable
  Next hop = 10.0.200.10, Channel status = Initiated open


HubBR2#show platform software pfrv3 fp active channel local
CENT local channel :

Total number of CENT local channel: 10

Channel id : 21
  Vrf id = 0, Site id = 255.255.255.255
  Dscp = 0, IF handle = 13, Tx state = reachable
  Next hop = 0.0.0.0, Channel status = Initiated open

Channel id : 23
  Vrf id = 0, Site id = 10.2.11.11
  Dscp = 0, IF handle = 13, Tx state = reachable
  Next hop = 10.0.200.11, Channel status = Initiated open


Channel id : 88
  Vrf id = 0, Site id = 10.2.10.10
  Dscp = 32, IF handle = 13, Tx state = reachable
  Next hop = 10.0.200.10, Channel status = Initiated open

Channel id : 91
  Vrf id = 0, Site id = 10.2.10.10
  Dscp = 46, IF handle = 13, Tx state = reachable
  Next hop = 10.0.200.10, Channel status = Initiated open

Channel id : 92
  Vrf id = 0, Site id = 10.2.10.10
  Dscp = 10, IF handle = 13, Tx state = reachable
  Next hop = 10.0.200.10, Channel status = Initiated open


HubBR2#show platform hardware qfp active feature pfrv3 client channel
CENT QFP CLIENT CHANNEL INFO

Num of channels: 10

Chan ID     Tbl ID      Site ID          DSCP  If hdl      State              rx state
tx state
-------------------------------------------------------------------------------------
----------------------
21          0           255.255.255.255  0     11          Initiated_n_open
reachable           reachable
23          0           10.2.11.11       0     11          Initiated_n_open
reachable           reachable
```

```
25          0           10.2.10.10       0     11          Initiated_n_open
reachable           reachable
84          0           10.2.10.10       26    11          Initiated_n_open
reachable           reachable
85          0           10.2.10.10       34    11          Initiated_n_open
reachable           reachable
86          0           10.2.10.10       40    11          Initiated_n_open
reachable           reachable
87          0           10.2.10.10       8     11          Initiated_n_open
reachable           reachable
88          0           10.2.10.10       32    11          Initiated_n_open
reachable           reachable
91          0           10.2.10.10       46    11          Initiated_n_open
reachable           reachable
92          0           10.2.10.10       10    11          Initiated_n_open
reachable           reachable

HubBR2#show platform hardware qfp active feature pfrv3 client neighbor-channel
CENT QFP Client neighbor channel info


nb-chan ID  State   TX state
------------------------------
20          up      reachable
22          up      reachable
24          up      reachable
79          up      reachable
80          up      reachable
81          up      reachable
82          up      reachable
83          up      reachable
89          up      reachable
90          up      reachable
```

Notes:

- Local and neighbor channel status should be TX/RX reachable in normal state;
- Channel declare as RX unreachable when no traffic over channel over 1s monitor interval;
- Unreachable TCA will feedback to local and remote master controller;
- If three is unreachable detected, traffic-classed get controlled over backup channel immediately for fast failover;

If channel RX unreachable detected, you could check that “sent TCA unreach”counter keep increasing for each 30s interval: show domain <name> border exporter statistics

```
HubBR2#show domain one border exporter statistics
show on-demand exporter(default vrf)

On-demand exporter statistics:
Border: 10.8.1.1
 Process ID: SEND=125, RECV=278

 Interface: Tunnel200 (index=13, service provider=INET)
  Bandwidth: Ingress=3430 Kbit/sec, Capacity=50000 Kbit/sec
             Egress =14899 Kbit/sec, Capacity=50000 Kbit/sec

   Total sent BW packets:              1
```

```
    Total sent BW templates:            1, Last sent: 0 min 7 sec ago

  Destination-site: 10.8.3.3:
    Total sent TCA unreach              8
    Total sent TCA templates:           1, Last sent: 0 min 3 sec ago

  Destination-site: 10.2.10.10:
    Total sent TCA unreach              8
    Total sent ODE                      4
    Total sent TCA templates:           1, Last sent: 0 min 3 sec ago

 Other border: 10.8.2.2

 Global Stats:
   Table ID lookup count: 0
   Table ID Channel found count: 0
   Table ID Next hop found count: 0
HubBR2#
```

You could check that Channel TX/RX status transit to “unreachable” as well: show domain <name> border channels

```
HubBR2#show domain one border channels
Border Smart Probe Stats:

Channel id: 23
  Channel dscp: 0
  Channel site: 10.2.11.11
  Channel interface: Tunnel200
  Channel operation state: Initiated_n_open
  Channel RX state: reachable
  Channel TX state: reachable
  Channel next hop: 10.0.200.11
  Channel recv_probes: 996579
  Channel send_probes: 996055
  Channel recv_packets: 0
  Channel send_packets: 0
  Channel recv_bytes: 0
  Channel send_bytes 0
  Last Probe Received: 8 ms Ago
  Last Probe Sent: 116 ms Ago

Channel id: 88
  Channel dscp: 32
  Channel site: 10.2.10.10
  Channel interface: Tunnel200
  Channel operation state: Initiated_n_open
  Channel RX state: unreachable
  Channel TX state: unreachable
  Channel next hop: 10.0.200.10
  Channel recv_probes: 23591
  Channel send_probes: 25311
  Channel recv_packets: 386704
  Channel send_packets: 1175118
  Channel recv_bytes: 55527581
  Channel send_bytes 494292492
  Last Probe Received: 45238 ms Ago
  Last Probe Sent: 4 ms Ago

Channel id: 91
```

```
  Channel dscp: 46
  Channel site: 10.2.10.10
  Channel interface: Tunnel200
  Channel operation state: Initiated_n_open
  Channel RX state: unreachable
  Channel TX state: unreachable
  Channel next hop: 10.0.200.10
  Channel recv_probes: 30541
  Channel send_probes: 35500
  Channel recv_packets: 0
  Channel send_packets: 22484
  Channel recv_bytes: 0
  Channel send_bytes 10338531
  Last Probe Received: 45216 ms Ago
  Last Probe Sent: 64 ms Ago
```

You could check the channel status on master controller with latest unreachable TCA and ODE exports:
show domain <name> master channels service-provider <PATH>

```
HubMC#show domain one master channels link-name INET
   Legend: * (Value obtained from Network delay:)


Channel Id: 25  Dst Site-Id: 10.2.10.10  Link Name: INET  DSCP: default [0] TCs: 0
  Channel Created: 13:39:27 ago
  Provisional State: Initiated and open
  Operational state: Available but unreachable
  Interface Id: 13
  Estimated Channel Egress Bandwidth: 0 Kbps
  Immitigable Events Summary:
   Total Performance Count: 0, Total BW Count: 0
  ODE Stats Bucket Number: 1
   Last Updated  : 00:00:01 ago
    Packet Count  : 0
    Byte Count    : 0
    One Way Delay  : N/A
    Loss Rate Pkts : N/A
    Loss Rate Bytes: N/A
    Jitter Mean    : N/A
    Unreachable   : TRUE
  ODE Stats Bucket Number: 2
   Last Updated  : 00:00:57 ago
    Packet Count  : 0
    Byte Count    : 0
    One Way Delay  : N/A
    Loss Rate Pkts : N/A
    Loss Rate Bytes: N/A
    Jitter Mean    : N/A
    Unreachable   : TRUE
   TCA Statitics:
      Received:4 ; Processed:1 ; Unreach_rcvd:4
  Latest TCA Bucket
   Last Updated  : 00:00:01 ago

Channel Id: 91  Dst Site-Id: 10.2.10.10  Link Name: INET  DSCP: ef [46] TCs: 0
  Channel Created: 00:32:21 ago
  Provisional State: Initiated and open
  Operational state: Available but unreachable
  Interface Id: 13
  Estimated Channel Egress Bandwidth: 149 Kbps
  Immitigable Events Summary:
   Total Performance Count: 0, Total BW Count: 0
```

```
   ODE Stats Bucket Number: 1
    Last Updated  : 00:00:02 ago
     Packet Count  : 603
     Byte Count    : 43416
     One Way Delay  : N/A
     Loss Rate Pkts : N/A
     Loss Rate Bytes: N/A
     Jitter Mean    : N/A
     Unreachable   : TRUE
   ODE Stats Bucket Number: 2
    Last Updated  : 00:00:02 ago
     Packet Count  : 0
     Byte Count    : 0
     One Way Delay  : N/A
     Loss Rate Pkts : N/A
     Loss Rate Bytes: N/A
     Jitter Mean    : N/A
     Unreachable   : TRUE
    TCA Statitics:
       Received:42 ; Processed:40 ; Unreach_rcvd:2
   Latest TCA Bucket
    Last Updated  : 00:00:02 ago
     Local unreachable TCA received


Channel Id: 88  Dst Site-Id: 10.2.10.10  Link Name: INET  DSCP: cs4 [32] TCs: 0
   Channel Created: 00:32:21 ago
   Provisional State: Initiated and open
   Operational state: Available but unreachable
   Interface Id: 13
   Estimated Channel Egress Bandwidth: 364 Kbps
   Immitigable Events Summary:
    Total Performance Count: 0, Total BW Count: 0
   ODE Stats Bucket Number: 1
    Last Updated  : 00:00:02 ago
     Packet Count  : 604
     Byte Count    : 43488
     One Way Delay  : N/A
     Loss Rate Pkts : N/A
     Loss Rate Bytes: N/A
     Jitter Mean    : N/A
     Unreachable   : TRUE
   ODE Stats Bucket Number: 2
    Last Updated  : 00:00:02 ago
     Packet Count  : 0
     Byte Count    : 0
     One Way Delay  : N/A
     Loss Rate Pkts : N/A
     Loss Rate Bytes: N/A
     Jitter Mean    : N/A
     Unreachable   : TRUE
    TCA Statitics:
       Received:42 ; Processed:40 ; Unreach_rcvd:2
   Latest TCA Bucket
    Last Updated  : 00:00:02 ago
     Local unreachable TCA received


HubMC#show domain one master channels dscp EF
    Legend: * (Value obtained from Network delay:)

Channel Id: 89  Dst Site-Id: 10.2.10.10  Link Name: MPLS  DSCP: ef [46] TCs: 1
   Channel Created: 00:34:49 ago
   Provisional State: Initiated and open
   Operational state: Available
```

```
  Interface Id: 14
  Estimated Channel Egress Bandwidth: 5652 Kbps
  Immitigable Events Summary:
   Total Performance Count: 0, Total BW Count: 0
  ODE Stats Bucket Number: 1
   Last Updated  : 00:02:30 ago
    Packet Count  : 31540
    Byte Count    : 13543122
    One Way Delay : 0 msec*
    Loss Rate Pkts: 0.0 %
    Loss Rate Byte: 0.0 %
    Jitter Mean   : 266 usec
    Unreachable   : FALSE
  ODE Stats Bucket Number: 2
   Last Updated  : 00:05:30 ago
    Packet Count  : 58054
    Byte Count    : 25080440
    One Way Delay : 1 msec*
    Loss Rate Pkts: 0.0 %
    Loss Rate Byte: 0.0 %
    Jitter Mean   : 0 usec
    Unreachable   : FALSE
   TCA Statitics:
      Received:0 ; Processed:0 ; Unreach_rcvd:0


Channel Id: 91  Dst Site-Id: 10.2.10.10  Link Name: INET  DSCP: ef [46] TCs: 0
  Channel Created: 00:34:49 ago
  Provisional State: Initiated and open
  Operational state: Available but unreachable
  Interface Id: 13
  Estimated Channel Egress Bandwidth: 149 Kbps
  Immitigable Events Summary:
   Total Performance Count: 0, Total BW Count: 0
  ODE Stats Bucket Number: 1
   Last Updated  : 00:00:26 ago
    Packet Count  : 0
    Byte Count    : 0
    One Way Delay  : N/A
    Loss Rate Pkts : N/A
    Loss Rate Bytes: N/A
    Jitter Mean    : N/A
    Unreachable   : TRUE
  ODE Stats Bucket Number: 2
   Last Updated  : 00:00:58 ago
    Packet Count  : 0
    Byte Count    : 0
    One Way Delay  : N/A
    Loss Rate Pkts : N/A
    Loss Rate Bytes: N/A
    Jitter Mean    : N/A
    Unreachable   : TRUE
   TCA Statitics:
      Received:42 ; Processed:40 ; Unreach_rcvd:2
  Latest TCA Bucket
   Last Updated  : 00:00:26 ago
    Local unreachable TCA received


HubMC#
```

7 IOS-XE Troubleshooting

In this section, you could be able to get IOS-XE specific troubleshooting tips on how to isolate PfR platform related issues for PfR version 3.

7.1 Platform CLI

Check PfR instance status and path information downloaded correctly into hardware:

```
Branch10#show platform hardware qfp active feature pfrv3 client global cent-instance
detail
CENT QFP CLIENT GLOBAL INFO

Number of Instances: 1

Instance
  hash val:  5
  tbl id:    0
  symmetry:  Off
  discovery: On
  discovery_probe: Off
  probe info:
    probe src: 10.2.10.10, src port: 18000, dst port: 19000
    unreach time: 1000, probe period: 500
    dscp bitmap: 0000000000000000, interval: 10000
    mml: 28
  exmem info:
    PPE addr: 0xe80b4830

Branch10#show platform hardware qfp active feature pfrv3 client global color detail
CENT QFP CLIENT GLOBAL INFO

Number of Colors: 2

Color info
  if_h: 14
  color: INET
  exmem info:
    PPE addr: 0xead925a0

Color info
  if_h: 13
  color: MPLS
  exmem info:
    PPE addr: 0xead92590
```

Check PFR global datapath stats like Routing Control, Smart Probe, and CFT(common-flow-table).

```
Branch10#show platform hardware qfp active feature pfrv3 datapath global
CENT QFP Datapath global information

CENT FDB:
  Channel hash:
    table address: 0xe94b5000    table size: 32768
  RC flow hash:
```

```
    table address: 0xe94f5000    table size: 32768
  Instance hash:
    table address: 0xe80b4420    table size: 16
  debug mode:  0x0000
  spdb epoch:  2048
  timer wheel: 0xe85e8810        0x0     0x0     0x0
               0x0       0x0     0x0     0x0
  timer flags: 0x0003    number of timer wheeels: 1

Global stats:
  Routing Control:
    cft unsupported:        950290
    cft no feat obj:        593990140
    cache spdb miss:        0
    cache flow miss:        60904998
    cache hit:              1736369427
    channel local:          2387565130
    channel neighbor:       0
    auto-tunnel rcvd:       0
    auto-tunnel cache:      0
  Smart Probe:
    channel disc:           308
    channel reach:          8
    channel unreach:        49
    channel inital->reach:  143
    channel all unreach:    5
    interface disc:         34
    interface color change: 0
    transit smart probe:    0
    drop no route:          0
    drop no uidb_sb:        0
    drop pkt init:          0
    drop min interval:      0
    drop err site-id:       0
    drop no channel disc:   169
    drop no interface disc: 0
    drop no color change:   0
  CFT:
    FO alloc:               593990150
    FO alloc err:           0
    FO dealloc:             593985878
    FO dealloc err:         0
  Proxy:
    Message init:           3
    Message deinit:         2
    Message channel add:    146
    Message channel modify: 62
    Message channel delete: 130
Branch10#
```

Check CFT(common-flow-table) and relative Feacute Objects(FO) get enabled properly, CENT and FME FO is enabled automatically with DSCP based policy, STILE(NBAR2) and FNF are enabled dynamically with application based policy:

```
Branch10#show platform hardware qfp active infrastructure cft status brief
================================== CFT 1/1 ==================================
    CFT id: 0
    CFT name: GLOBAL_CFT
    General Parameters:
        Max flows: 500000
```

```
        Number of buckets in CFT hash table: 2135282
    Features Registered (total:4):
         Feature id         Feature Name
        ------------       ---------------
         0                  CENT
         1                  FME
         2                  STILE
         3                  FNF
    Feature Objects (total:4):
         FO id          FO Name
        -------        ---------
         0              CENT FO
         1              FME FO
         2              STILE FO
         3              FNF FO
    Statistics:
        Total number of packets seen                              : 6355472630
        Total number of TCP packets seen                          : 6012374900
        Total number of UDP packets seen                          : 343097730
        Total number of ICMP packets seen                         : 0
        Total number of unsupported-L4-protocol packets seen      : 279627576
        Total number of flows added                               : 712101475
        Total number of flows removed                             : 712095280
        Total number of currently allocated flows                 : 6224
        Total number of TCP flows                                 : 711875877
        Total number of UDP flows                                 : 225598
        Total number of ICMP flows                                : 0
    Memory:
        Total CFT memory allocated - QFP 0: 11531352 bytes
        Total CFT initial memory allocated - QFP 0: 9076920 bytes
        Memory Elements in QFP 0 (total:15):
             Element id         Allocated bytes         Number of Objects
Owner         Element Name
            ------------       -----------------       -------------------       -----
---      --------------
             0                  1140048                 6224
GLOBAL_CFT    CFT IPv4 FC
             1                  0                       0
GLOBAL_CFT    CFT IPv6 FC
             2                  0                       0
GLOBAL_CFT    CFT IPv4 Extra Key
             3                  0                       0
GLOBAL_CFT    CFT IPv6 Extra Key
             4                  229424                  4376                      CENT
CENT FO Chunk
             5                  810144                  4417                      FME
FME Chunk 0
             6                  2000                    24                        FME
FME Chunk 1
             7                  0                       0                         FME
FME Chunk 2
             8                  976                     4                         FME
FME Chunk 3
             9                  219552                  1949
STILE         STILE Chunk 0
             10                 38784                   160
STILE         STILE Chunk 1
             11                 3120                    15
STILE         STILE Chunk 2
             12                 3312                    63                        FNF
FNF Chunk 0
             13                 7072                    63                        FNF
FNF Chunk 1
             14                 0                       0                         FNF
FNF Chunk 2
```

```
    IPC statistics:
        Control-plane to data-plane IPC messages successfully sent: 18
        Control-plane to data-plane IPC messages failed to be sent: 0
        Data-plane to control-plane IPC messages successfully sent: 18

Branch10#
```

PfR version 3 dynamically enable AVC components like CFT/FME/FNF/NABR2, together with CENT itself, which could consume QFP DRAM memory depending on the number of active flows in the chassis. DRAM on QFP usage can be found on the following command:

```
Branch10#show platform hardware qfp active infrastructure exmem statistics
QFP exmem statistics

Type: Name: DRAM, QFP: 0
  Total: 268435456
  InUse: 71523328
  Free: 196912128
  Lowest free water mark: 193837056
Type: Name: IRAM, QFP: 0
  Total: 2097152
  InUse: 109568
  Free: 1987584
  Lowest free water mark: 1987584
Type: Name: SRAM, QFP: 0
  Total: 0
  InUse: 0
  Free: 0
  Lowest free water mark: 0
Type: Name: DP_TEXT, QFP: 0
  Total: 0
  InUse: 0
  Free: 0
  Lowest free water mark: 0
Type: Name: DP_DATA, QFP: 0
  Total: 0
  InUse: 0
  Free: 0
  Lowest free water mark: 0
Type: Name: DP_RODATA, QFP: 0
  Total: 0
  InUse: 0
  Free: 0
  Lowest free water mark: 0
Type: Name: DP_BSS, QFP: 0
  Total: 0
  InUse: 0
  Free: 0
  Lowest free water mark: 0


Branch10#show platform hardware qfp active infrastructure exmem statistics user
Type: Name: IRAM, QFP: 0
  Allocations  Bytes-Alloc  Bytes-Total  User-Name
  ------------------------------------------------------------------------------
  1            108800       109568       CPP_FIA
Type: Name: GLOBAL, QFP: 0
  Allocations  Bytes-Alloc  Bytes-Total  User-Name
  ------------------------------------------------------------------------------
  7            20976        25600        P/I
```

```
  1            4384         5120         DPSS
  1            16384        16384        FHS
  1            4384         5120         EPC
  1            512          1024         FME
  39           395992       434176       MMA
  1            4384         5120         SBC
  9            9152776      9159680      CFT
  22           7254160      7274496      CVLA
  10           279152       284672       CEF

  [SNIP]

  1            147456       147456       CENT chan
  1            32768        32768        CENT rc flow
  1            256          1024         cent color chunk
  1            32768        32768        cent policy chunk
  1            384          1024         CENT inst
  1            16384        16384        CPP_FNF_UIDB_DP_CHUNK
  1            16896        17408        FME PARAMETERS OBJECTS
Type: Name: GLOBAL, QFP: 0
  Allocations  Bytes-Alloc  Bytes-Total  User-Name
  ------------------------------------------------------------------------------
  2            262144       262144       QoS 32
  2            524288       524288       QoS 64
  2            1048576      1048576      QoS 128
  2            524288       524288       QoS 256
  687          12477600     12491776     CPR STILE EXMEM GRAPH


Branch10#show platform hardware qfp active infrastructure cvla client handles
Handles for cpp 0:
---------------------
Entity name: FNF_AOR
Handle: 0xe95b5000
Number of allocations: 0
Memory allocated: 0

Entity name: NBAR_CVLA_ENTITY
Handle: 0xe95cf000
Number of allocations: 0
Memory allocated: 0

Entity name: FNF Chunk 2
Handle: 0xe95b9000
Number of allocations: 0
Memory allocated: 0

Entity name: FNF Chunk 1
Handle: 0xe95b8000
Number of allocations: 67
Memory allocated: 7552

Entity name: FNF Chunk 0
Handle: 0xe95b6000
Number of allocations: 67
Memory allocated: 3648

Entity name: STILE Chunk 2
Handle: 0xe9605000
Number of allocations: 18
Memory allocated: 3744

Entity name: STILE Chunk 1
Handle: 0xe9604000
Number of allocations: 139
```

```
Memory allocated: 34592

Entity name: STILE Chunk 0
Handle: 0xe9603000
Number of allocations: 1868
Memory allocated: 210880

Entity name: FME Chunk 3
Handle: 0xead96000
Number of allocations: 4
Memory allocated: 976

Entity name: FME Chunk 2
Handle: 0xead95000
Number of allocations: 0
Memory allocated: 0

Entity name: FME Chunk 1
Handle: 0xead94000
Number of allocations: 24
Memory allocated: 2000

Entity name: FME Chunk 0
Handle: 0xead93000
Number of allocations: 4144
Memory allocated: 739840

Entity name: CFT IPv6 Extra Key_0
Handle: 0xe862d000
Number of allocations: 0
Memory allocated: 0

Entity name: CFT IPv4 Extra Key_0
Handle: 0xe862c000
Number of allocations: 0
Memory allocated: 0

Entity name: CFT IPv6 FC_0
Handle: 0xe862b000
Number of allocations: 0
Memory allocated: 0

Entity name: CFT IPv4 FC_0
Handle: 0xe862a000
Number of allocations: 5902
Memory allocated: 1053328

Entity name: CENT FO Chunk
Handle: 0xe8629000
Number of allocations: 4124
Memory allocated: 219120

---------------------

Branch10#
```

Check IOS-XE Forwarding-manager Asynchronous Object Manager Statistics, no error and pending objects:

```
Branch10#show platform software object-manager fp active statistics
Forwarding Manager Asynchronous Object Manager Statistics
```

```
Object update: Pending-issue: 0, Pending-acknowledgement: 0
Batch begin:   Pending-issue: 0, Pending-acknowledgement: 0
Batch end:     Pending-issue: 0, Pending-acknowledgement: 0
Command:       Pending-acknowledgement: 0
Stale-objects: 0
Error-objects: 0

Branch10#show platform software object-manager fp active error-object
Branch10#
Branch10#show platform software object-manager fp active pending-issue-update
Branch10#
Branch10#show platform software object-manager fp active pending-ack-update
Branch10#
```

Check three FNF(Flexible-Netflow) monitors get installed and work properly in datapath:

```
Branch10#show platform hardware qfp active feature fnf client monitor all
QFP Client FNF Monitors

Name                              Oid
--------------------------------  ----------
MON-Ingress-per-DSCP-0-48-11      2000012
MON-Egress-aggregate-0-48-16      2000017
MON-Egress-prefix-learn-0-48-17   2000018

Branch10#
Branch10#show platform hardware qfp active feature fnf client flowdef all
QFP Client FNF FLOW_DEFs

Name                              Oid
--------------------------------  ----------
mma_monitor_pd_fdef_0x4FE67240_0xC  2000012
mma_monitor_pd_fdef_0x4585D112_0x11  2000017
mma_monitor_pd_fdef_0x9A388131_0x12  2000018

Branch10#
Branch10#show platform hardware qfp active feature fnf client exporter all
QFP Client FNF Exporters

Name                              Oid
--------------------------------  ----------
CENT_FLOW_EXP-5                   2000006

Branch10#
Branch10#show platform hardware qfp active feature fnf client interface all
QFP Client FNF Interfaces

Name                              QFP Id      Direction
------------------------------------------------------
Tunnel100                         13          Ingress
Tunnel200                         14          Ingress
Tunnel100                         13          Egress
Tunnel200                         14          Egress
Tunnel0                           16          Egress

Branch10#
Branch10#show platform hardware qfp active feature fnf datapath aor
 CFT:  ConfigAddress 0x8aeae2c0, Instance 0x8252a720, Feat ID 3, FlowObj ID 3, Flags
0x00000001
 CVLA: handle 0xe95b5000 epoch 0x1
```

```
 Statistics:                                          Success              Fail
   Flow Object (chunk ID 12)
        Alloc                                        63903210                 0
        Attach                                       63903210                 0
        Detach                                       63902837                 0
        Free                                         63903149                 0
   Flow Object elements:
   Main Metrics (chunk ID 13)
        Alloc                                        63903210                 0
        Free                                         63903149                 0
   MMA Metrics (chunk ID 14)
        Alloc                                               0                 0
        Free                                                0                 0
   Extracted Field AOR root objects
        Alloc                                               0                 0
        Free                                                0
   Extracted Field objects
        Alloc                                               0                 0
        Free                                                0

 Flow Object Termination Event from CFT                   312
        Flow Object Detach                                  0
        Flow Object Free                                  312
 EOTE Flow Object Free:
        Ager                                                0
        Config                                              0
 Errors:
        NULL Flow object                                    0
        NULL Main Metric                                    0
        NULL MMA Metric                                     0
        CFT not configured                                  0
        CFT search failure                                  0
        Zero RefCount                                       0
        CVLA epoch errors                                   0
        CVLA handle errors                                  0
        NBAR SB fail                                    31453
 Packets:                                           Unresolved          Resolved
        INPUT_FNF_AOR_FIRST                                 0                 0
        INPUT_FNF_AOR_FINAL                                 0                 0
        INPUT_FNF_AOR_FIRST_WAAS                            0                 0
        INPUT_FNF_AOR_FINAL_WAAS                            0                 0
        OUTPUT_FNF_AOR                              127858147         134964462
        OUTPUT_FNF_AOR_WAAS                                 0                 0
        INPUT_FNF_AOR_DROP                                  0                 0
        FNF_AOR_RELEASE                              63902843
 FNF AOR Monitor:
        Skip                                        127858147
        Run                                         134964462

Branch10#
```

Check MMA monitors get installed and work properly in datapath:

```
Branch10#show platform hardware qfp active feature mma client db monitor all
Monitors in the DB:
-------------------
MMA Monitor id:     1340502592
FNF Monitor oid:    2000012
FNF Monitor Name:   MON-Ingress-per-DSCP-0-48-11
Punt indication:    TRUE
punt exmem block:
```

```
   CPP num: 0      ppe address: 0xe95b6940

MMA Monitor id:     2587394353
FNF Monitor oid:    2000018
FNF Monitor Name:   MON-Egress-prefix-learn-0-48-17
Punt indication:    TRUE
punt exmem block:
   CPP num: 0      ppe address: 0xe862bc80

MMA Monitor id:     1166397714
FNF Monitor oid:    2000017
FNF Monitor Name:   MON-Egress-aggregate-0-48-16
Punt indication:    TRUE
punt exmem block:
   CPP num: 0      ppe address: 0xe8628810


Branch10#show platform hardware qfp active feature mma client db class-action all
Class actions in the DB:
-----------------------
Class group id:   11064832
Class group name: CENT-Policy-Ingress-0-9
Class id:         807614884

Class group id:   11064832
Class group name: CENT-Policy-Ingress-0-9
Class id:         1968189332

Class group id:   11064832
Class group name: CENT-Policy-Ingress-0-9
Class id:         1812905690

Class group id:   11064832
Class group name: CENT-Policy-Ingress-0-9
Class id:         525874308

Class group id:   14952096
Class group name: CENT-Policy-Egress-0-12
Class id:         340355238

Class group id:   11064832
Class group name: CENT-Policy-Ingress-0-9
Class id:         368863262

Class group id:   11064832
Class group name: CENT-Policy-Ingress-0-9
Class id:         1020219285

Class group id:   11064832
Class group name: CENT-Policy-Ingress-0-9
Class id:         541121671


Branch10#show platform hardware qfp active feature mma punt datapath hsl stats
MMA Export Statistics
---------------------
Total records logged into MMA: 144113
Total records sent towards HSL: 144113
Total packets exported via HSL: 13670
Total record allocation failures: 0
Total records dropped by MMA: 0
Total packets dropped by HSL before export: 0

MMA HSL Statistics
------------------
```

```
Total records exported : 144113
Total packets exported: 13670
Total bytes exported: 11703760
Total dropped records: 0
Total dropped packets (includes Punt drops): 0
Total dropped bytes: 0
Successful template refreshes: 57
Template timer expired: 0
Unsuccessful template refreshes: 0
Number of data templates: 0
Number of option templates: 0
Branch10#
```

7.2 Conditional Debug

Conditional Debugging allows users to define conditions to match all packets from an interface or limit matching based on an IPv4/IPv6 address or IPv4/IPv6 ACL together with feature level conditions. PfR, CFT, FME, IPsec support Conditional Debugging in Datapath:

debug platform condition interface GigabitEthernet0/0/0 ingress
debug platform condition interface Tunnel100 both
debug platform condition feature pfrv3 dataplane submode routing-control level <info|verbose>
debug platform condition feature pfrv3 dataplane submode smart-probe level <info|verbose>
debug platform condition feature pfrv3 dataplane submode all level <info|verbose>
debug platform condition start
debug platform condition stop

Conditional Debug on wan interface Tunnel100 both direction with dataplane submode smart-probe level verbose:

```
Branch10#debug platform condition interface Tunnel100 both
Branch10#debug platform condition feature pfrv3 dataplane submode smart-probe level
verbose
Branch10#debug platform condition start
Branch10#
Branch10#show platform conditions

Conditional Debug Global State: Start

Conditions
Direction
------------------------------------------------------------------------------------
--------|---------
Tunnel100
both
GigabitEthernet5.100
ingress
```

```
Feature Condition        Type                    Value
----------------------|-----------------------|-------------------------------



Feature      Type           Submode
Level
------------|-------------|-------------------------------------------------------------
-----------------------------------|----------
PfRv3          dataplane     SMP
verbose

Branch10#
Branch10#debug platform condition stop
Branch10#
Branch10#test platform software trace slot fp active cpp-control-process rotate
  Rotated file from: /tmp/fp/trace/stage/cpp_cp_F0-0.log.19425.20141102003007, Bytes:
99746, Messages: 524

Branch10#more bootflash:/tracelogs/cpp_cp_F0-0.log.19425.20141102003007
11/02 00:29:06.573 : btrace continued for process ID 19425 with 159 modules

11/02 00:29:06.576 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000248581978947724 :SMP:[10.1.10.4] 35995 => [10.8.101.3] 80 6 (0): channel 0x92
found, mark as tx touched
11/02 00:29:06.576 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000248581978992572 :SMP:[10.1.10.4] 35995 => [10.8.101.3] 80 6 (0): Packet Out:
vrf 0, src 10.1.10.4, dst 10.8.101.3, dscp 0x1a
11/02 00:29:06.576 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000248581978995096 :SMP:[10.1.10.4] 35995 => [10.8.101.3] 80 6 (0): channel 0x92
found, mark as tx touched
11/02 00:29:06.576 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000248581984745026 :SMP:[10.1.10.3] 36042 => [10.8.101.6] 80 6 (0): Packet Out:
vrf 0, src 10.1.10.3, dst 10.8.101.6, dscp 0xa
11/02 00:29:06.576 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000248581984748008 :SMP:[10.1.10.3] 36042 => [10.8.101.6] 80 6 (0): channel 0x87
found, mark as tx touched
11/02 00:29:06.576 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000248581984813885 :SMP:[10.1.10.4] 36078 => [10.8.101.6] 80 6 (0): Packet Out:
vrf 0, src 10.1.10.4, dst 10.8.101.6, dscp 0x1a
11/02 00:29:06.576 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000248581984816746 :SMP:[10.1.10.4] 36078 => [10.8.101.6] 80 6 (0): channel 0x92
found, mark as tx touched
11/02 00:29:06.577 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000248581984879710 :SMP:[10.1.10.6] 36076 => [10.8.101.4] 80 6 (0): Packet Out:
vrf 0, src 10.1.10.6, dst 10.8.101.4, dscp 0x2e
```

Conditional Debug on LAN interface GigabitEthernet5.100 ingress direction with dataplane submode **routing-control** level verbose:

```
Branch10#debug platform condition interface GigabitEthernet5.100 ingress
Branch10#debug platform condition feature pfrv3 dataplane submode routing-control
level verbose
Branch10#debug platform condition start
Branch10#
Branch10#show platform conditions

Conditional Debug Global State: Start
```

```
Conditions
Direction
-------------------------------------------------------------------------------
--------|---------
Tunnel100
both
GigabitEthernet5.100
ingress



Feature Condition        Type                    Value
-----------------------|-----------------------|--------------------------------



Feature      Type           Submode
Level
------------|-------------|-------------------------------------------------------
-----------------------------------|----------
PfRv3          dataplane     RC
verbose

Branch10#
Branch10#debug platform condition stop
Branch10#
Branch10#test platform software trace slot fp active cpp-control-process rotate
  Rotated file from: /tmp/fp/trace/stage/cpp_cp_F0-0.log.19425.20141102003345, Bytes:
1030291, Messages: 5787

Branch10#
Branch10#more bootflash:/tracelogs/cpp_cp_F0-0.log.19425.20141102003345
11/02 00:33:26.483 : btrace continued for process ID 19425 with 159 modules

11/02 00:33:26.485 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000248841977688674 :RC:[10.1.10.5] 45244 => [10.8.101.11] 80 6 (0): PACKET: vrf
0, src 10.1.10.5, dst 10.8.101.11, dscp 22, app 3000050
11/02 00:33:26.485 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000248841977691516 :RC:[10.1.10.5] 45244 => [10.8.101.11] 80 6 (0): get cft fid
0xea06eea0 and cent fo 0xea05ec80
11/02 00:33:26.485 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000248841977693372 :RC:[10.1.10.5] 45244 => [10.8.101.11] 80 6 (0): FO spdb
caches: slen 0, dlen 16
11/02 00:33:26.485 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000248841977694700 :RC:[10.1.10.5] 45244 => [10.8.101.11] 80 6 (0): flow key: 0,
0.0.0.0/0 -> 10.8.0.0/16
11/02 00:33:26.485 [cpp-dp-PfRv3]: (info): QFP:0.0 Thread:000 TS:00000248841977696486
:RC:[10.1.10.5] 45244 => [10.8.101.11] 80 6 (0): policy seq 10 miss match
11/02 00:33:26.485 [cpp-dp-PfRv3]: (info): QFP:0.0 Thread:000 TS:00000248841977697637
:RC:[10.1.10.5] 45244 => [10.8.101.11] 80 6 (0): policy seq 20 hits dscp 22
11/02 00:33:26.486 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000248841977698894 :RC:[10.1.10.5] 45244 => [10.8.101.11] 80 6 (0): process
action: adjacency 0, channel 0xead9fb60
11/02 00:33:26.486 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000248841977700416 :RC:[10.1.10.5] 45244 => [10.8.101.11] 80 6 (0): channel 141
uidb 65527 state up, routing by 10.0.200.85
11/02 00:33:26.486 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000248841977703047 :RC:[10.1.10.5] 45244 => [10.8.101.11] 80 6 (0): find
oce_chain_p 0xe86355a0 for vrf 0 next-hop 10.0.200.85
11/02 00:33:26.486 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000248841977705213 :RC:[10.1.10.5] 45244 => [10.8.101.11] 80 6 (0): primary
action take effect
```

```
11/02 00:33:26.486 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000248841977943901 :RC:[10.1.10.11] 45242 => [10.8.101.9] 80 6 (0): PACKET: vrf
0, src 10.1.10.11, dst 10.8.101.9, dscp 28, app 3000050
```

Conditional Debug with ipv4 access-list on LAN and WAN interface for selective packets with both routing-control and smart-probe on:

```
Branch10#show running-config | section access-list
ip access-list extended RC
 permit tcp host 10.1.10.2 any
ip access-list extended SMP
 permit udp any eq 18000 any eq 19000
!

Branch10#debug platform condition interface gigabitEthernet 5.100 ipv4 access-list RC
ingress
Branch10#debug platform condition interface tunnel100 ipv4 access-list SMP both
Branch10#debug platform condition feature pfrv3 dataplane submode all level verbose
Branch10#debug platform condition start
Branch10#
Branch10#show platform conditions

Conditional Debug Global State: Start

Conditions
Direction
------------------------------------------------------------------------------------
--------|---------
Tunnel100                              & IPV4 ACL [SMP]
both
GigabitEthernet5.100                   & IPV4 ACL [RC]
ingress



Feature Condition        Type                    Value
-----------------------|-----------------------|--------------------------------



Feature      Type           Submode
Level
------------|-------------|-------------------------------------------------------
-----------------------------------|----------
CENT          dataplane     RC SMP
verbose

Branch10#debug platform condition stop
Branch10#
Branch10#test platform software trace slot fp active cpp-control-process rotate
  Rotated file from: /tmp/fp/trace/stage/cpp_cp_F0-0.log.19425.20141102015646, Bytes:
1039673, Messages: 5824

Branch10#
Branch10#more bootflash:/tracelogs/cpp_cp_F0-0.log.19425.20141102015646
11/02 00:45:26.265 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000249561773691125 :RC:[10.1.10.2] 6691 => [10.8.101.6] 80 6 (0): PACKET: vrf 0,
src 10.1.10.2, dst 10.8.101.6, dscp 8, app 3000050
```

```
11/02 00:45:26.265 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000249561773694907 :RC:[10.1.10.2] 6691 => [10.8.101.6] 80 6 (0): get cft fid
0xea0ee6c0 and cent fo 0xea3792d0
11/02 00:45:26.265 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000249561773697511 :RC:[10.1.10.2] 6691 => [10.8.101.6] 80 6 (0): FO spdb caches:
slen 0, dlen 16
11/02 00:45:26.265 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000249561773699317 :RC:[10.1.10.2] 6691 => [10.8.101.6] 80 6 (0): flow key: 0,
0.0.0.0/0 -> 10.8.0.0/16
11/02 00:45:26.265 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000249561773701901 :RC:[10.1.10.2] 6691 => [10.8.101.6] 80 6 (0): FO flow caches
282f: policy 0xe8aed080
11/02 00:45:26.265 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000249561773704169 :RC:[10.1.10.2] 6691 => [10.8.101.6] 80 6 (0): process action:
adjacency 0, channel 0xead9fd10
11/02 00:45:26.265 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000249561773705797 :RC:[10.1.10.2] 6691 => [10.8.101.6] 80 6 (0): channel 133
uidb 65527 state up, routing by 10.0.200.85
11/02 00:45:26.265 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000249561773708701 :RC:[10.1.10.2] 6691 => [10.8.101.6] 80 6 (0): find
oce_chain_p 0xe86355a0 for vrf 0 next-hop 10.0.200.85
11/02 00:45:26.265 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000249561773710424 :RC:[10.1.10.2] 6691 => [10.8.101.6] 80 6 (0): primary action
take effect
11/02 00:45:26.265 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000249561773714516 :SMP:[10.1.10.2] 6691 => [10.8.101.6] 80 6 (0): Packet Out:
vrf 0, src 10.1.10.2, dst 10.8.101.6, dscp 0x8
11/02 00:45:26.269 [cpp-dp-PfRv3]: (verbose): QFP:0.0 Thread:000
TS:00000249561773716854 :SMP:[10.1.10.2] 6691 => [10.8.101.6] 80 6 (0): channel 0x85
found, mark as tx touched
```

7.3 Packet Trace

Packet Trace provides a mechanism for users to capture and analyze packets as they traverse through the router like packet accounting, feature details, ingress and egress packet copy, and feature invocation array (FIA) chain information, including PfR Routing-control/CFT/NBAR2/FNF, etc:

debug platform condition interface GigabitEthernet2 ingress
debug platform condition interface tunnel100 both
debug platform packet-trace packet 1024 fia-trace data-size 2048
debug platform packet-trace enable
debug platform condition start
debug platform condition stop
show platform packet-trace summary

```
HubBR1#debug platform condition interface GigabitEthernet2 ingress
HubBR1#debug platform condition interface tunnel100 both
HubBR1#debug platform packet-trace packet 1024 fia-trace data-size 2048
HubBR1#debug platform packet-trace enable
HubBR1#debug platform condition start
HubBR1#debug platform condition stop

Branch10#show platform packet-trace statistics
Packets Summary
```

```
  Matched  23811
  Traced   1024
Packets Received
  Ingress  23811
  Inject   0
Packets Processed
  Forward  21979
  Punt     0
  Drop     0
  Consume  1832


HubBR1#show platform packet-trace summary
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, *06:34:06.649 CST Sun Dec 28 2014
Pkt   Input            Output           State  Reason
0     Tu100            Gi2              FWD
1     Tu100            Gi2              FWD
2     Tu100            Gi2              FWD
3     Tu100            Gi2              FWD

76    Gi2              Gi2              FWD
77    Gi2              Gi2              FWD
78    Gi2              Gi2              FWD
79    Gi2              Gi2              FWD
80    Gi2              Gi2              FWD
81   internal0/0/recycle:0  Gi3              FWD

1000  Gi2              Gi2              FWD
1001  Gi2              Gi2              FWD
1002  Gi2              Gi2              FWD
1003  Gi2              Gi2              FWD
1004  Gi2              Gi2              FWD
1005  Gi2              Gi2              FWD
1006  Gi2              Gi2              FWD
1007  Gi2              Gi2              FWD
1008  Gi2              Gi2              FWD
1009  Gi2              Gi2              FWD
1010  internal0/0/recycle:0  Gi3              FWD
1011  Gi2              Gi2              FWD


PfRv3 Smart-Probe RTP packets send over WAN interface:

HubBR1#show platform packet-trace packet 81
Packet: 81          CBUG ID: 81
Summary
  Input     : internal0/0/recycle:0
  Output    : GigabitEthernet3
  State     : FWD
  Timestamp
    Start   : 329500971307254 ns (11/01/2014 16:57:30.514637 UTC)
    Stop    : 329500971356600 ns (11/01/2014 16:57:30.514687 UTC)
Path Trace
  Feature: IPV4
    Source      : 10.8.3.3
    Destination : 10.2.11.11
    Protocol    : 17 (UDP)
      SrcPort : 18000
      DstPort : 19000
  Feature: FIA_TRACE
    Entry      : 0x8088e170 - IPV4_OUTPUT_TCP_ADJUST_MSS
    Lapsed time: 6160 ns
  Feature: FIA_TRACE
    Entry      : 0x8050fe40 - MC_OUTPUT_GEN_RECYCLE
```

```
    Lapsed time: 4160 ns
  Feature: FIA_TRACE
    Entry      : 0x80ace3b0 - IPV4_VFR_REFRAG
    Lapsed time: 3600 ns
  Feature: FIA_TRACE
    Entry      : 0x80abbf00 - IPV4_OUTPUT_SRC_LOOKUP_ISSUE
    Lapsed time: 12280 ns
  Feature: FIA_TRACE
    Entry      : 0x80912b70 - IPV6_OUTPUT_L2_REWRITE
    Lapsed time: 15940 ns
  Feature: FIA_TRACE
    Entry      : 0x80ab4180 - IPV4_INPUT_SRC_LOOKUP_CONSUME
    Lapsed time: 1520 ns
  Feature: CFT
    API                    : cft_handle_pkt
    packet capabilities    : 0x0000008c
    input vrf_idx          : 0
    calling feature        : STILE
    direction              : Output
    triplet.vrf_idx        : 0
    triplet.network_start  : 0x01004270
    triplet.triplet_flags  : 0x00000000
    triplet.counter        : 0
    cft_bucket_number      : 831382
    cft_l3_payload_size    : 52
    cft_pkt_ind_flags      : 0x00000202
    cft_pkt_ind_valid      : 0x00009bff
    tuple.src_ip           : 10.8.3.3
    tuple.dst_ip           : 10.2.11.11
    tuple.src_port         : 18000
    tuple.dst_port         : 19000
    tuple.vrfid            : 0
    tuple.l4_protocol      : UDP
    tuple.l3_protocol      : IPV4
    pkt_sb_state           : 0
    pkt_sb.num_flows       : 1
    pkt_sb.tuple_epoch     : 0
    returned cft_error     : 0
    returned fid           : 0xe9dd4d20
  Feature: NBAR
    Packet number in flow: 3
    Classification state: Final
    Classification name: rtp
    Classification ID: [CANA-L7:61]
    Number of matched sub-classifications: 0
    Number of extracted fields: 0
    Is PA (split) packet: False
  Feature: FIA_TRACE
    Entry      : 0x80843470 - IPV4_OUTPUT_STILE_LEGACY
    Lapsed time: 106360 ns
  Feature: FIA_TRACE
    Entry      : 0x80255df0 - IPV4_OUTPUT_CENT_SMP_PROCESS
    Lapsed time: 1480 ns
  Feature: FIA_TRACE
    Entry      : 0x80a8b820 - IPV4_OUTPUT_FRAG
    Lapsed time: 1920 ns
  Feature: FIA_TRACE
    Entry      : 0x8055e8c0 - IPV4_EGRESS_MMA_LOOKUP_CLRT
    Lapsed time: 86400 ns
  Feature: FIA_TRACE
    Entry      : 0x803655d0 - TUNNEL_OUTPUT_FNF_AOR
    Lapsed time: 4320 ns
  Feature: FIA_TRACE
    Entry      : 0x8033d420 - IPV4_OUTPUT_FNF_FINAL
    Lapsed time: 9240 ns
```

```
  Feature: FIA_TRACE
    Entry      : 0x80366080 - OUTPUT_FNF_AOR_RELEASE_CLRT
    Lapsed time: 2180 ns
  Feature: FIA_TRACE
    Entry      : 0x808c4090 - IPV4_TUNNEL_OUTPUT_FINAL
    Lapsed time: 22780 ns
  Feature: FIA_TRACE
    Entry      : 0x808c4d10 - IPV4_OUTPUT_TUNNEL_PROTECTION_ENCRYPT
    Lapsed time: 3040 ns
  Feature: IPSec
    Result    : IPSEC_RESULT_SA
    Action    : ENCRYPT
    SA Handle : 6
    Peer Addr : 172.16.111.11
    Local Addr: 172.16.84.4
  Feature: FIA_TRACE
    Entry      : 0x804cbd30 - IPV4_OUTPUT_IPSEC_CLASSIFY
    Lapsed time: 45820 ns
  Feature: FIA_TRACE
    Entry      : 0x804cde50 - IPV4_OUTPUT_IPSEC_DOUBLE_ACL
    Lapsed time: 1460 ns
  Feature: FIA_TRACE
    Entry      : 0x804cdde0 - IPV4_IPSEC_FEATURE_RETURN
    Lapsed time: 2380 ns
  Feature: FIA_TRACE
    Entry      : 0x80c33d30 - IPV4_OUTPUT_IPSEC_INLINE_FRAG_CHK
    Lapsed time: 2680 ns
  Feature: FIA_TRACE
    Entry      : 0x80c34ed0 - IPV4_OUTPUT_IPSEC_INLINE_PROCESS
    Lapsed time: 170220 ns
  Feature: FIA_TRACE
    Entry      : 0x804cdc60 - IPV4_OUTPUT_IPSEC_TUNNEL_RERUN_JUMP
    Lapsed time: 1800 ns
  Feature: FIA_TRACE
    Entry      : 0x804cf270 - IPV4_OUTPUT_IPSEC_POST_PROCESS
    Lapsed time: 9280 ns
  Feature: FIA_TRACE
    Entry      : 0x804cdde0 - IPV4_IPSEC_FEATURE_RETURN
    Lapsed time: 900 ns
  Feature: FIA_TRACE
    Entry      : 0x804cdde0 - IPV4_IPSEC_FEATURE_RETURN
    Lapsed time: 1040 ns
  Feature: FIA_TRACE
    Entry      : 0x808c2f00 - IPV4_TUNNEL_GOTO_OUTPUT
    Lapsed time: 11840 ns
  Feature: FIA_TRACE
    Entry      : 0x808c2d20 - IPV4_TUNNEL_FW_CHECK
    Lapsed time: 5060 ns
  Feature: FIA_TRACE
    Entry      : 0x80ac9d10 - IPV4_INPUT_DST_LOOKUP_ISSUE
    Lapsed time: 8160 ns
  Feature: FIA_TRACE
    Entry      : 0x80a74ea0 - IPV4_INPUT_ARL
    Lapsed time: 1920 ns
  Feature: FIA_TRACE
    Entry      : 0x80ab9f50 - IPV4_OUTPUT_DST_LOOKUP_CONSUME
    Lapsed time: 1700 ns
  Feature: FIA_TRACE
    Entry      : 0x808c2dc0 - IPV4_TUNNEL_ENCAP_FOR_US
    Lapsed time: 2740 ns
  Feature: FIA_TRACE
    Entry      : 0x80aa8d00 - IPV4_OUTPUT_LOOKUP_PROCESS
    Lapsed time: 9160 ns
  Feature: FIA_TRACE
    Entry      : 0x80a7abf0 - IPV4_TUNNEL_ENCAP_GOTO_OUTPUT_FEATURE
```

```
    Lapsed time: 4240 ns
  Feature: FIA_TRACE
    Entry      : 0x80ace3d0 - IPV4_MC_INPUT_VFR_REFRAG
    Lapsed time: 880 ns
  Feature: FIA_TRACE
    Entry      : 0x80912c60 - IPV6_OUTPUT_L2_REWRITE
    Lapsed time: 5220 ns
  Feature: CFT
    API                   : cft_handle_pkt
    packet capabilities   : 0x0000008c
    input vrf_idx         : 0
    calling feature       : STILE
    direction             : Output
    triplet.vrf_idx       : 0
    triplet.network_start : 0x010041d8
    triplet.triplet_flags : 0x00000000
    triplet.counter       : 0
    cft_bucket_number     : 0
    cft_l3_payload_size   : 132
    cft_pkt_ind_flags     : 0x00000000
    cft_pkt_ind_valid     : 0x00000931
    tuple.src_ip          : 172.16.84.4
    tuple.dst_ip          : 172.16.111.11
    tuple.src_port        : 0
    tuple.dst_port        : 0
    tuple.vrfid           : 0
    tuple.l4_protocol     : 50
    tuple.l3_protocol     : IPV4
    pkt_sb_state          : 0
    pkt_sb.num_flows      : 1
    pkt_sb.tuple_epoch    : 0
    returned cft_error    : 14
    returned fid          : 0x00000000
  Feature: NBAR
    Packet number in flow: 3
    Classification state: Final
    Classification name: ipsec
    Classification ID: [CANA-L7:9]
    Number of matched sub-classifications: 0
    Number of extracted fields: 0
    Is PA (split) packet: False
  Feature: FIA_TRACE
    Entry      : 0x808431a0 - IPV4_OUTPUT_STILE_CLR_TXT
    Lapsed time: 74380 ns
  Feature: FIA_TRACE
    Entry      : 0x80a8b860 - IPV4_OUTPUT_FRAG
    Lapsed time: 8080 ns
  Feature: FIA_TRACE
    Entry      : 0x809101a0 - L2_REWRITE_AFTER_FRAG_WITHOUT_CLIP
    Lapsed time: 5500 ns
  Feature: FIA_TRACE
    Entry      : 0x80b15550 - IPV4_OUTPUT_DROP_POLICY
    Lapsed time: 5980 ns
  Feature: FIA_TRACE
    Entry      : 0x80c38700 - MARMOT_SPA_D_TRANSMIT_PKT
    Lapsed time: 35020 ns


PfRv3 controlled packets send over local WAN interface:

HubBR1#
HubBR1#show platform packet-trace packet 1015
Packet: 1015        CBUG ID: 1015
Summary
  Input     : GigabitEthernet2
```

```
  Output    : GigabitEthernet3
  State     : FWD
  Timestamp
    Start   : 329501042996259 ns (11/01/2014 16:57:30.586327 UTC)
    Stop    : 329501043066837 ns (11/01/2014 16:57:30.586397 UTC)
Path Trace
  Feature: IPV4
    Source      : 10.8.101.8
    Destination : 10.1.10.4
    Protocol    : 6 (TCP)
      SrcPort : 80
      DstPort : 46782
  Feature: FIA_TRACE
    Entry      : 0x809e42f0 - DEBUG_COND_INPUT_PKT
    Lapsed time: 1180 ns
  Feature: FIA_TRACE
    Entry      : 0x80abac20 - IPV4_INPUT_DST_LOOKUP_CONSUME
    Lapsed time: 1200 ns
  Feature: FIA_TRACE
    Entry      : 0x800f87d0 - IPV4_INPUT_FOR_US_MARTIAN
    Lapsed time: 1220 ns
  Feature: CFT
    API                   : cft_handle_pkt
    packet capabilities   : 0x0000008c
    input vrf_idx         : 0
    calling feature       : CENT
    direction             : Input
    triplet.vrf_idx       : 0
    triplet.network_start : 0x0100410e
    triplet.triplet_flags : 0x00000000
    triplet.counter       : 0
    cft_bucket_number     : 1553462
    cft_l3_payload_size   : 1380
    cft_pkt_ind_flags     : 0x00000100
    cft_pkt_ind_valid     : 0x00009bff
    tuple.src_ip          : 10.8.101.8
    tuple.dst_ip          : 10.1.10.4
    tuple.src_port        : 80
    tuple.dst_port        : 46782
    tuple.vrfid           : 0
    tuple.l4_protocol     : TCP
    tuple.l3_protocol     : IPV4
    pkt_sb_state          : 0
    pkt_sb.num_flows      : 1
    pkt_sb.tuple_epoch    : 0
    returned cft_error    : 0
    returned fid          : 0xe9a111f0
  Feature: NBAR
    Packet number in flow: 4
    Classification state: Final
    Classification name: http
    Classification ID: [IANA-L4:80]
    Number of matched sub-classifications: 0
    Number of extracted fields: 0
    Is PA (split) packet: False
  Feature: FIA_TRACE
    Entry      : 0x80843530 - IPV4_INPUT_STILE_LEGACY
    Lapsed time: 85700 ns
  Feature: FIA_TRACE
    Entry      : 0x80255e90 - IPV4_INPUT_CENT_SMP_PROCESS
    Lapsed time: 11120 ns
  Feature: PfRv3
    Local Channel id : 120
    Peer Site id     : 10.2.10.10
    Dscp             : 26
```

```
    Interface         : Tunnel100
    Destination Prefix: 10.1.10.0/24
    App id            : 218103809
    Next hop          : 10.0.100.10
 Feature: FIA_TRACE
    Entry      : 0x80256fb0 - IPV4_INPUT_CENT_RC_PROCESS
    Lapsed time: 42300 ns
  Feature: FIA_TRACE
    Entry      : 0x80aa8d00 - IPV4_OUTPUT_LOOKUP_PROCESS
    Lapsed time: 4940 ns
  Feature: FIA_TRACE
    Entry      : 0x80acc860 - IPV4_INPUT_IPOPTIONS_PROCESS
    Lapsed time: 1060 ns
  Feature: FIA_TRACE
    Entry      : 0x800b7390 - MPLS_INPUT_GOTO_OUTPUT_FEATURE
    Lapsed time: 3100 ns
  Feature: FIA_TRACE
    Entry      : 0x809e0820 - CBUG_OUTPUT_FIA
    Lapsed time: 1660 ns
  Feature: FIA_TRACE
    Entry      : 0x8088e1c0 - IPV4_INPUT_TCP_ADJUST_MSS
    Lapsed time: 4080 ns
  Feature: FIA_TRACE
    Entry      : 0x8050fe40 - MC_OUTPUT_GEN_RECYCLE
    Lapsed time: 3460 ns
  Feature: FIA_TRACE
    Entry      : 0x80ace3d0 - IPV4_MC_INPUT_VFR_REFRAG
    Lapsed time: 1140 ns
  Feature: FIA_TRACE
    Entry      : 0x80abad80 - IPV4_OUTPUT_SRC_LOOKUP_ISSUE
    Lapsed time: 3500 ns
  Feature: FIA_TRACE
    Entry      : 0x80912c60 - IPV6_OUTPUT_L2_REWRITE
    Lapsed time: 9660 ns
  Feature: FIA_TRACE
    Entry      : 0x80ab40e0 - IPV4_INPUT_SRC_LOOKUP_CONSUME
    Lapsed time: 1560 ns
  Feature: NBAR
    Packet number in flow: 4
    Classification state: Final
    Classification name: http
    Classification ID: [IANA-L4:80]
    Number of matched sub-classifications: 0
    Number of extracted fields: 0
    Is PA (split) packet: False
  Feature: FIA_TRACE
    Entry      : 0x808431a0 - IPV4_OUTPUT_STILE_CLR_TXT
    Lapsed time: 11600 ns
  Feature: FIA_TRACE
    Entry      : 0x80255710 - IPV4_OUTPUT_CENT_SMP_PROCESS
    Lapsed time: 25460 ns
  Feature: FIA_TRACE
    Entry      : 0x80a8b860 - IPV4_OUTPUT_FRAG
    Lapsed time: 960 ns
  Feature: FIA_TRACE
    Entry      : 0x8055e8e0 - IPV4_EGRESS_MMA_LOOKUP
    Lapsed time: 49020 ns
  Feature: FIA_TRACE
    Entry      : 0x80365250 - OUTPUT_FNF_AOR_CLRT
    Lapsed time: 16620 ns
  Feature: FIA_TRACE
    Entry      : 0x8033d5c0 - IPV4_TUNNEL_OUTPUT_FNF_FINAL
    Lapsed time: 105820 ns
  Feature: FIA_TRACE
    Entry      : 0x803660c0 - OUTPUT_FNF_AOR_RELEASE_CLRT
```

```
    Lapsed time: 2680 ns
  Feature: FIA_TRACE
    Entry      : 0x808c3090 - IPV4_TUNNEL_OUTPUT_FINAL
    Lapsed time: 10840 ns
  Feature: FIA_TRACE
    Entry      : 0x808c4d30 - IPV4_OUTPUT_TUNNEL_PROTECTION_ENCRYPT
    Lapsed time: 2980 ns
  Feature: IPSec
    Result    : IPSEC_RESULT_SA
    Action    : ENCRYPT
    SA Handle : 4
    Peer Addr : 172.16.101.10
    Local Addr: 172.16.84.4
  Feature: FIA_TRACE
    Entry      : 0x804cbd30 - IPV4_OUTPUT_IPSEC_CLASSIFY
    Lapsed time: 35800 ns
  Feature: FIA_TRACE
    Entry      : 0x804cde50 - IPV4_OUTPUT_IPSEC_DOUBLE_ACL
    Lapsed time: 1440 ns
  Feature: FIA_TRACE
    Entry      : 0x804cdde0 - IPV4_IPSEC_FEATURE_RETURN
    Lapsed time: 1220 ns
  Feature: FIA_TRACE
    Entry      : 0x80c33d30 - IPV4_OUTPUT_IPSEC_INLINE_FRAG_CHK
    Lapsed time: 2640 ns
  Feature: FIA_TRACE
    Entry      : 0x80c34ed0 - IPV4_OUTPUT_IPSEC_INLINE_PROCESS
    Lapsed time: 444440 ns
  Feature: FIA_TRACE
    Entry      : 0x804cdc60 - IPV4_OUTPUT_IPSEC_TUNNEL_RERUN_JUMP
    Lapsed time: 880 ns
  Feature: FIA_TRACE
    Entry      : 0x804cf270 - IPV4_OUTPUT_IPSEC_POST_PROCESS
    Lapsed time: 5460 ns
  Feature: FIA_TRACE
    Entry      : 0x804cdde0 - IPV4_IPSEC_FEATURE_RETURN
    Lapsed time: 520 ns
  Feature: FIA_TRACE
    Entry      : 0x804cdde0 - IPV4_IPSEC_FEATURE_RETURN
    Lapsed time: 600 ns
  Feature: FIA_TRACE
    Entry      : 0x808c2e30 - IPV4_TUNNEL_GOTO_OUTPUT
    Lapsed time: 3760 ns
  Feature: FIA_TRACE
    Entry      : 0x808c2d20 - IPV4_TUNNEL_FW_CHECK
    Lapsed time: 4300 ns
  Feature: FIA_TRACE
    Entry      : 0x80ac9d10 - IPV4_INPUT_DST_LOOKUP_ISSUE
    Lapsed time: 4220 ns
  Feature: FIA_TRACE
    Entry      : 0x80a74ea0 - IPV4_INPUT_ARL
    Lapsed time: 2820 ns
  Feature: FIA_TRACE
    Entry      : 0x80ab9f50 - IPV4_OUTPUT_DST_LOOKUP_CONSUME
    Lapsed time: 1260 ns
  Feature: FIA_TRACE
    Entry      : 0x808c2dc0 - IPV4_TUNNEL_ENCAP_FOR_US
    Lapsed time: 2040 ns
  Feature: FIA_TRACE
    Entry      : 0x80aa8d00 - IPV4_OUTPUT_LOOKUP_PROCESS
    Lapsed time: 5260 ns
  Feature: FIA_TRACE
    Entry      : 0x80a7abf0 - IPV4_TUNNEL_ENCAP_GOTO_OUTPUT_FEATURE
    Lapsed time: 3980 ns
  Feature: FIA_TRACE
```

```
    Entry      : 0x80ace3d0 - IPV4_MC_INPUT_VFR_REFRAG
    Lapsed time: 460 ns
  Feature: FIA_TRACE
    Entry      : 0x80912c60 - IPV6_OUTPUT_L2_REWRITE
    Lapsed time: 3340 ns
  Feature: CFT
    API                   : cft_handle_pkt
    packet capabilities   : 0x0000008c
    input vrf_idx         : 0
    calling feature       : STILE
    direction             : Output
    triplet.vrf_idx       : 0
    triplet.network_start : 0x01004078
    triplet.triplet_flags : 0x00000000
    triplet.counter       : 0
    cft_bucket_number     : 0
    cft_l3_payload_size   : 1460
    cft_pkt_ind_flags     : 0x00000000
    cft_pkt_ind_valid     : 0x00000931
    tuple.src_ip          : 172.16.84.4
    tuple.dst_ip          : 172.16.101.10
    tuple.src_port        : 0
    tuple.dst_port        : 0
    tuple.vrfid           : 0
    tuple.l4_protocol     : 50
    tuple.l3_protocol     : IPV4
    pkt_sb_state          : 0
    pkt_sb.num_flows      : 1
    pkt_sb.tuple_epoch    : 0
    returned cft_error    : 14
    returned fid          : 0x00000000
  Feature: NBAR
    Packet number in flow: 4
    Classification state: Final
    Classification name: ipsec
    Classification ID: [CANA-L7:9]
    Number of matched sub-classifications: 0
    Number of extracted fields: 0
    Is PA (split) packet: False
  Feature: FIA_TRACE
    Entry      : 0x808431a0 - IPV4_OUTPUT_STILE_CLR_TXT
    Lapsed time: 58540 ns
  Feature: FIA_TRACE
    Entry      : 0x80a8b860 - IPV4_OUTPUT_FRAG
    Lapsed time: 4540 ns
  Feature: FIA_TRACE
    Entry      : 0x809101a0 - L2_REWRITE_AFTER_FRAG_WITHOUT_CLIP
    Lapsed time: 4020 ns
  Feature: FIA_TRACE
    Entry      : 0x80b15550 - IPV4_OUTPUT_DROP_POLICY
    Lapsed time: 4740 ns
  Feature: FIA_TRACE
    Entry      : 0x80c38700 - MARMOT_SPA_D_TRANSMIT_PKT
    Lapsed time: 32020 ns
```

PfRv3 Smart-Probe RTP packets send to neighour BR over Auto-Tunnel interface:

```
HubBR1#
HubBR1#show platform packet-trace pa 1008

HubBR1#show platform packet-trace packet 1008
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, *06:54:11.582 CST Sun Dec 28 2014
Packet: 1008        CBUG ID: 13502393
```

```
Summary
  Input     : GigabitEthernet2
  Output    : GigabitEthernet2
  State     : FWD
  Timestamp
    Start   : 10510401601048 ns (12/27/2014 22:53:49.842386 UTC)
    Stop    : 10510401632067 ns (12/27/2014 22:53:49.842417 UTC)
Path Trace
  Feature: IPV4
    Source      : 10.8.101.224
    Destination : 10.1.10.2
    Protocol    : 6 (TCP)
      SrcPort : 80
      DstPort : 47916
  Feature: FIA_TRACE
    Entry      : 0x809e4f70 - DEBUG_COND_INPUT_PKT
    Lapsed time: 4533 ns
  Feature: FIA_TRACE
    Entry      : 0x80abb8a0 - IPV4_INPUT_DST_LOOKUP_CONSUME
    Lapsed time: 1946 ns
  Feature: FIA_TRACE
    Entry      : 0x800f8960 - IPV4_INPUT_FOR_US_MARTIAN
    Lapsed time: 1813 ns
  Feature: FIA_TRACE
    Entry      : 0x80256280 - IPV4_INPUT_CENT_SMP_PROCESS
    Lapsed time: 20053 ns
  Feature: CFT
    API                   : cft_handle_pkt
    packet capabilities   : 0x00000080
    input vrf_idx         : 0
    calling feature       : CENT
    direction             : Input
    triplet.vrf_idx       : 0
    triplet.network_start : 0x0100410e
    triplet.triplet_flags : 0x00000000
    triplet.counter       : 0
    cft_bucket_number     : 549667
    cft_l3_payload_size   : 36
    cft_pkt_ind_flags     : 0x00000000
    cft_pkt_ind_valid     : 0x000019f7
    tuple.src_ip          : 10.8.101.224
    tuple.dst_ip          : 10.1.10.2
    tuple.src_port        : 80
    tuple.dst_port        : 47916
    tuple.vrfid           : 0
    tuple.l4_protocol     : TCP
    tuple.l3_protocol     : IPV4
    pkt_sb_state          : 0
    pkt_sb.num_flows      : 0
    pkt_sb.tuple_epoch    : 0
    returned cft_error    : 12
    returned fid          : 0x00000000
  Feature: PfRv3
    Neighbor Channel id : 17
    Peer Site id        : 10.2.10.10
    Dscp                : 32
    Destnation Prefix: 10.1.10.0/24
    App id              : 218103809
    Neighbor BR         : 10.8.2.2
  Feature: CFT
    API                   : cft_handle_pkt
    packet capabilities   : 0x00000084
    input vrf_idx         : 0
    calling feature       : CENT
    direction             : Input
```

```
    triplet.vrf_idx       : 0
    triplet.network_start : 0x0100410e
    triplet.triplet_flags : 0x00000000
    triplet.counter       : 0
    cft_bucket_number     : 549667
    cft_l3_payload_size   : 36
    cft_pkt_ind_flags     : 0x00000103
    cft_pkt_ind_valid     : 0x0000dbff
    tuple.src_ip          : 10.8.101.224
    tuple.dst_ip          : 10.1.10.2
    tuple.src_port        : 80
    tuple.dst_port        : 47916
    tuple.vrfid           : 0
    tuple.l4_protocol     : TCP
    tuple.l3_protocol     : IPV4
    pkt_sb_state          : 0
    pkt_sb.num_flows      : 1
    pkt_sb.tuple_epoch    : 0
    returned cft_error    : 0
    returned fid          : 0xede64b10
  Feature: FIA_TRACE
    Entry      : 0x802573a0 - IPV4_INPUT_CENT_RC_PROCESS
    Lapsed time: 254133 ns
  Feature: FIA_TRACE
    Entry      : 0x80aa9980 - IPV4_INPUT_LOOKUP_PROCESS
    Lapsed time: 7413 ns
  Feature: FIA_TRACE
    Entry      : 0x80acd4e0 - IPV4_INPUT_IPOPTIONS_PROCESS
    Lapsed time: 1973 ns
  Feature: FIA_TRACE
    Entry      : 0x800b7390 - LAYER2_INPUT_GOTO_OUTPUT_FEATURE
    Lapsed time: 3546 ns
  Feature: FIA_TRACE
    Entry      : 0x80510bf0 - MC_OUTPUT_GEN_RECYCLE
    Lapsed time: 6106 ns
  Feature: FIA_TRACE
    Entry      : 0x80acf050 - IPV4_VFR_REFRAG
    Lapsed time: 1360 ns
  Feature: FIA_TRACE
    Entry      : 0x809138e0 - IPV4_INPUT_L2_REWRITE
    Lapsed time: 13093 ns
  Feature: FIA_TRACE
    Entry      : 0x80a8c4e0 - IPV4_OUTPUT_FRAG
    Lapsed time: 1386 ns
  Feature: FIA_TRACE
    Entry      : 0x80365d50 - OUTPUT_FNF_AOR_CLRT
    Lapsed time: 3760 ns
  Feature: FIA_TRACE
    Entry      : 0x8033dfe0 - IPV4_TUNNEL_OUTPUT_FNF_FINAL
    Lapsed time: 3466 ns
  Feature: FIA_TRACE
    Entry      : 0x80366bc0 - OUTPUT_FNF_AOR_RELEASE
    Lapsed time: 2080 ns
  Feature: FIA_TRACE
    Entry      : 0x808c3d00 - IPV4_TUNNEL_OUTPUT_FINAL
    Lapsed time: 16106 ns
  Feature: FIA_TRACE
    Entry      : 0x808c3aa0 - IPV4_TUNNEL_GOTO_OUTPUT
    Lapsed time: 4000 ns
  Feature: FIA_TRACE
    Entry      : 0x808c3990 - IPV4_TUNNEL_FW_CHECK
    Lapsed time: 5413 ns
  Feature: FIA_TRACE
    Entry      : 0x80aca990 - IPV4_INPUT_DST_LOOKUP_ISSUE
    Lapsed time: 2000 ns
```

```
  Feature: FIA_TRACE
    Entry      : 0x80a75b20 - IPV4_INPUT_ARL
    Lapsed time: 2933 ns
  Feature: FIA_TRACE
    Entry      : 0x80ababd0 - IPV4_INTERNAL_DST_LOOKUP_CONSUME
    Lapsed time: 826 ns
  Feature: FIA_TRACE
    Entry      : 0x808c3a30 - IPV4_TUNNEL_ENCAP_FOR_US
    Lapsed time: 2213 ns
  Feature: FIA_TRACE
    Entry      : 0x80aa9980 - IPV4_INPUT_LOOKUP_PROCESS
    Lapsed time: 2293 ns
  Feature: FIA_TRACE
    Entry      : 0x80a7b870 - IPV4_TUNNEL_ENCAP_GOTO_OUTPUT_FEATURE
    Lapsed time: 4773 ns
  Feature: FIA_TRACE
    Entry      : 0x80acf050 - IPV4_VFR_REFRAG
    Lapsed time: 586 ns
  Feature: FIA_TRACE
    Entry      : 0x809138e0 - IPV4_INPUT_L2_REWRITE
    Lapsed time: 3333 ns
  Feature: FIA_TRACE
    Entry      : 0x80a8c4e0 - IPV4_OUTPUT_FRAG
    Lapsed time: 426 ns
  Feature: FIA_TRACE
    Entry      : 0x80b173a0 - IPV4_OUTPUT_DROP_POLICY
    Lapsed time: 11280 ns
  Feature: FIA_TRACE
    Entry      : 0x80c3a580 - MARMOT_SPA_D_TRANSMIT_PKT
    Lapsed time: 38000 ns

HubBR1#
```

7.4 Embedded Packet Capture (EPC)

Embedded Packet Capture (EPC) is supported on ASR1000 since release IOS-XE 3.7.0S, and it provides a flexiable way to capture packets from ingress or egress interface that are processed by QFP. The capture packets could be exported and decoded by Wireshark directly:

monitor capture epc interface tunnel 100 both access-list SMP buffer size 100 limit pps 1000
show monitor capture epc parameter
monitor capture epc start
monitor capture epc stop
show monitor capture epc buffer brief
monitor capture epc export ftp://mgcusr:mgcusr@10.74.48.151/SMP.pcap

```
Branch10#show running-config | section SMP
ip access-list extended SMP
 permit udp any eq 18000 any eq 19000
!
Branch10#monitor capture epc interface tunnel 100 both access-list SMP buffer size 100
limit pps 1000
Branch10#monitor capture epc start
*Nov  2 01:05:49.891 CST: %BUFCAP-6-ENABLE: Capture Point epc enabled.?
```

```
Status Information for Capture epc
  Target Type:
   Interface: Tunnel100, Direction: both
   Status : Active
  Filter Details:
   Access-list: SMP
  Buffer Details:
   Buffer Type: LINEAR (default)
   Buffer Size (in MB): 100
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)

Branch10#monitor capture epc stop
*Nov  2 01:05:58.595 CST: %BUFCAP-6-DISABLE: Capture Point epc disabled.
Branch10#show monitor capture epc buffer brief
 ----------------------------------------------------------
 #   size   timestamp     source             destination   protocol
 ----------------------------------------------------------
   0   86    0.000000   10.8.3.3         ->  10.2.10.10       UDP
   1   86    0.001999   10.2.10.10       ->  10.8.3.3         UDP
   2   86    0.008987   10.2.10.10       ->  10.8.3.3         UDP
   3   86    0.008987   10.2.10.10       ->  10.8.3.3         UDP
   4   86    0.008987   10.8.3.3         ->  10.2.10.10       UDP
   5   86    0.011993   10.8.3.3         ->  10.2.10.10       UDP
   6   86    0.020995   10.8.3.3         ->  10.2.10.10       UDP
   7   86    0.028991   10.8.3.3         ->  10.2.10.10       UDP
   8   86    0.031997   10.8.3.3         ->  10.2.10.10       UDP
   9   86    0.035994   10.2.10.10       ->  10.8.3.3         UDP
  10   86    0.038985   10.8.3.3         ->  10.2.10.10       UDP
  11   86    0.039992   10.2.10.10       ->  10.8.3.3         UDP
  12   86    0.048994   10.2.10.10       ->  10.8.3.3         UDP
  13   86    0.048994   10.2.10.10       ->  10.8.3.3         UDP
  14   86    0.051984   10.8.3.3         ->  10.2.10.10       UDP

Branch10#monitor capture epc export ftp://mgcusr:mgcusr@10.74.48.151/SMP.pcap
Writing SMP.pcap
Exported Successfully

Then you could get the wireshark captures from ftp server and check whether packets
sent properly.
```

8 Configuration Sample

8.1 Example configuration on Hub MC

```
HubMC#show running-config
Building configuration...

Current configuration : 5137 bytes
!
! Last configuration change at 02:37:06 CST Mon Nov 3 2014
! NVRAM config last updated at 02:35:51 CST Mon Nov 3 2014
!
version 15.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
no platform punt-keepalive disable-kernel-core
platform console serial
!
hostname HubMC
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
!
no logging console
!
no aaa new-model
clock timezone CST 8 0
!
!
!
no ip domain lookup
!
!
!
subscriber templating
!
multilink bundle-name authenticated
!
domain one
 vrf default
  master hub
   source-interface Loopback0
   site-prefixes prefix-list DC1_PREFIX
   monitor-interval 2 dscp cs5
   monitor-interval 2 dscp ef
   load-balance
   enterprise-prefix  prefix-list ENTERPRISE_PREFIX
   class VOICE sequence 10
    match dscp ef policy custom
     priority 2 loss threshold 5
     priority 1 one-way-delay threshold 150
     path-preference MPLS fallback INET
   class VIDEO sequence 20
    match dscp af41 policy custom
```

```
     priority 2 loss threshold 5
     priority 1 one-way-delay threshold 150
     match dscp cs4 policy custom
     priority 2 loss threshold 5
     priority 1 one-way-delay threshold 150
     path-preference INET fallback MPLS
   class CRITICAL sequence 30
    match dscp af31 policy custom
     priority 2 loss threshold 10
     priority 1 one-way-delay threshold 600
     path-preference MPLS fallback INET
!
!
license udi pid CSR1000V sn 90KU0SDCWNB
license boot level ax
spanning-tree extend system-id
!
!
redundancy
 mode none
!
!
!
!
!
!
ip ftp source-interface GigabitEthernet1
ip ftp username mgcusr
ip ftp password mgcusr
ip tftp source-interface GigabitEthernet1
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.8.3.3 255.255.255.255
!
interface GigabitEthernet1
 vrf forwarding Mgmt-intf
 ip address 10.124.19.208 255.255.255.0
 negotiation auto
!
interface GigabitEthernet2
 no ip address
 load-interval 30
 speed 1000
 no negotiation auto
!
interface GigabitEthernet2.100
 encapsulation dot1Q 100
 ip address 10.8.101.1 255.255.255.0
!
interface GigabitEthernet2.101
 encapsulation dot1Q 101
 ip address 10.8.102.1 255.255.255.0
!
interface GigabitEthernet2.102
 encapsulation dot1Q 102
 ip address 10.8.103.1 255.255.255.0
!
interface GigabitEthernet2.103
 encapsulation dot1Q 103
```

```
 ip address 10.8.104.1 255.255.255.0
!
interface GigabitEthernet3
 description --INTERNAL--
 ip address 10.8.24.2 255.255.255.0
 speed 1000
 no negotiation auto
!
interface GigabitEthernet4
 description --INTERNAL--
 ip address 10.8.25.2 255.255.255.0
 speed 1000
 no negotiation auto
!
!
router eigrp 100
 network 10.8.3.3 0.0.0.0
 network 10.8.24.0 0.0.0.255
 network 10.8.25.0 0.0.0.255
 redistribute connected
!
!
virtual-service csr_mgmt
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.124.19.1
!
!
ip prefix-list DC1_PREFIX seq 10 permit 10.8.0.0/16
!
ip prefix-list ENTERPRISE_PREFIX seq 10 permit 10.0.0.0/8
no service-routing capabilities-manager
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 no login
line vty 5 15
 exec-timeout 0 0
 privilege level 15
 no login
!
ntp logging
ntp source Loopback0
ntp master 3
!
end
```

8.2 Example configuration on Hub BR1

```
HubBR1#show running-config
Building configuration...
```

```
Current configuration : 5312 bytes
!
! Last configuration change at 02:31:02 CST Mon Nov 3 2014
! NVRAM config last updated at 02:31:02 CST Mon Nov 3 2014
!
version 15.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
no platform punt-keepalive disable-kernel-core
platform console serial
!
hostname HubBR1
!
boot-start-marker
boot-end-marker
!
!
vrf definition INET1
 rd 65512:1
 !
 address-family ipv4
 exit-address-family
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
!
no logging console
!
no aaa new-model
clock timezone CST 8 0
!
!
!
!
no ip domain lookup
!
!
!
!
!
subscriber templating
!
multilink bundle-name authenticated
!
domain one
 vrf default
  border
   source-interface Loopback0
   master 10.8.3.3
!
!
license udi pid CSR1000V sn 952V3LWQECD
license boot level ax
spanning-tree extend system-id
!
!
redundancy
 mode none
!
!
!
```

```
!
!
!
ip ftp source-interface GigabitEthernet1
ip ftp username mgcusr
ip ftp password mgcusr
ip tftp source-interface GigabitEthernet1
!
crypto keyring DMVPN-KEYRING1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
!
!
!
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
crypto isakmp performance
crypto isakmp profile ISAKMP-INET1
   keyring DMVPN-KEYRING1
   match identity address 0.0.0.0
!
crypto ipsec security-association replay disable
crypto ipsec security-association replay window-size 1024
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE1
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile ISAKMP-INET1
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.8.1.1 255.255.255.255
!
interface Tunnel100
 bandwidth 100000
 ip address 10.0.100.84 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp holdtime 600
 ip nhrp redirect
 ip tcp adjust-mss 1360
 load-interval 30
 tunnel source GigabitEthernet3
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile DMVPN-PROFILE1
 domain one path MPLS
!
interface GigabitEthernet1
 vrf forwarding Mgmt-intf
 ip address 10.124.19.210 255.255.255.0
```

```
 negotiation auto
!
interface GigabitEthernet2
 description --INTERNAL--
 ip address 10.8.24.4 255.255.255.0
 speed 1000
 no negotiation auto
!
interface GigabitEthernet3
 description --MPLS--
 ip address 172.16.84.4 255.255.255.0
 load-interval 30
 speed 1000
 no negotiation auto
!
interface GigabitEthernet4
 no ip address
 load-interval 30
 speed 1000
 no negotiation auto
!
interface GigabitEthernet5
 ip address 101.1.4.1 255.255.255.0
 speed 1000
 no negotiation auto
!
interface GigabitEthernet6
 no ip address
 speed 1000
 no negotiation auto
!
!
router eigrp 100
 network 10.8.2.2 0.0.0.0
 network 10.8.24.0 0.0.0.255
 redistribute bgp 10 metric 100000 1 255 255 1500
 distance eigrp 90 210
!
router ospf 100
 router-id 10.8.1.1
 network 172.16.84.4 0.0.0.0 area 0
!
router bgp 10
 bgp router-id 10.8.1.1
 bgp log-neighbor-changes
 bgp listen range 10.0.100.0/24 peer-group MPLS-SPOKES
 neighbor MPLS-SPOKES peer-group
 neighbor MPLS-SPOKES remote-as 10
 neighbor MPLS-SPOKES timers 20 60
 !
 address-family ipv4
  bgp redistribute-internal
  network 10.8.1.1 mask 255.255.255.255
  network 10.8.3.3 mask 255.255.255.255
  network 10.8.101.0 mask 255.255.255.0
  network 10.8.102.0 mask 255.255.255.0
  network 10.8.103.0 mask 255.255.255.0
  network 10.8.104.0 mask 255.255.255.0
  aggregate-address 10.8.0.0 255.255.0.0 summary-only
  neighbor MPLS-SPOKES activate
  neighbor MPLS-SPOKES send-community
  neighbor MPLS-SPOKES next-hop-self all
  neighbor MPLS-SPOKES default-originate
  neighbor MPLS-SPOKES route-map MPLS-DC1-IN in
  neighbor MPLS-SPOKES route-map MPLS-DC1-OUT out
```

```
  distance bgp 20 109 109
 exit-address-family
!
!
virtual-service csr_mgmt
!
ip forward-protocol nd
!
ip bgp-community new-format
ip community-list standard MPLS-DMVPN permit 10:100
ip community-list standard INET-DMVPN permit 10:200
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.124.19.1
!
!
ip prefix-list DC1-LOCAL-ROUTES seq 10 permit 0.0.0.0/0
ip prefix-list DC1-LOCAL-ROUTES seq 20 permit 10.8.0.0/16 le 32
no service-routing capabilities-manager
!
route-map MPLS-DC1-IN deny 10
 match ip address prefix-list DC1-LOCAL-ROUTES
!
route-map MPLS-DC1-IN permit 20
 set community 10:100
!
route-map TO-PEER permit 10
 match ip address prefix-list DC1-LOCAL-ROUTES
 set ip next-hop self
 set community no-advertise
!
route-map site_prefixes permit 10
 match ip address prefix-list site_prefixes
!
route-map MPLS-DC1-OUT permit 10
 match ip address prefix-list DC1-LOCAL-ROUTES
 set community 10:100
!
route-map MPLS-DC1-OUT permit 20
 description readvertise routes learned from MPLS DMVPN cloud
 match community MPLS-DMVPN
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 no login
line vty 5 15
 exec-timeout 0 0
 privilege level 15
 no login
!
ntp source Loopback0
ntp server 10.8.3.3
!
end
```

8.3 Example configuration on Hub BR2

```
HubBR2#show running-config
Building configuration...

Current configuration : 5254 bytes
!
! Last configuration change at 02:30:54 CST Mon Nov 3 2014
! NVRAM config last updated at 02:25:26 CST Mon Nov 3 2014
!
version 15.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
no platform punt-keepalive disable-kernel-core
platform console serial
!
hostname HubBR2
!
boot-start-marker
boot-end-marker
!
!
vrf definition INET2
 rd 65512:2
 !
 address-family ipv4
 exit-address-family
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
!
no logging console
!
no aaa new-model
clock timezone CST 8 0
!
!
!
!
!
!
!
no ip domain lookup
!
!
!
!
subscriber templating
!
multilink bundle-name authenticated
!
domain one
 vrf default
  border
   source-interface Loopback0
   master 10.8.3.3
!
!
license udi pid CSR1000V sn 94EFH1HPLI9
license boot level ax
spanning-tree extend system-id
```

```
!
!
redundancy
 mode none
!
!
!
!
!
!
ip ftp source-interface GigabitEthernet1
ip ftp username mgcusr
ip ftp password mgcusr
ip tftp source-interface GigabitEthernet1
!
crypto keyring DMVPN-KEYRING2 vrf INET2
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
!
!
!
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
crypto isakmp invalid-spi-recovery
crypto isakmp performance
crypto isakmp profile ISAKMP-INET2
   keyring DMVPN-KEYRING2
   match identity address 0.0.0.0 INET2
!
crypto ipsec security-association replay disable
crypto ipsec security-association replay window-size 1024
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE2
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile ISAKMP-INET2
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.8.2.2 255.255.255.255
!
interface Tunnel200
 bandwidth 50000
 ip address 10.0.200.85 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 2
 ip nhrp holdtime 600
 ip nhrp redirect
 ip tcp adjust-mss 1360
 load-interval 30
 delay 1000
```

```
 tunnel source GigabitEthernet4
 tunnel mode gre multipoint
 tunnel key 200
 tunnel vrf INET2
 tunnel protection ipsec profile DMVPN-PROFILE2
 domain one path INET
!
interface GigabitEthernet1
 vrf forwarding Mgmt-intf
 ip address 10.124.19.209 255.255.255.0
 negotiation auto
!
interface GigabitEthernet2
 description --INTERNAL--
 ip address 10.8.25.5 255.255.255.0
 speed 1000
 no negotiation auto
!
interface GigabitEthernet3
 ip address 101.1.4.2 255.255.255.0
 speed 1000
 no negotiation auto
!
interface GigabitEthernet4
 description --INET--
 vrf forwarding INET2
 ip address 172.16.85.5 255.255.255.0
 load-interval 30
 speed 1000
 no negotiation auto
!
!
router eigrp 100
 network 10.8.1.1 0.0.0.0
 network 10.8.25.0 0.0.0.255
 redistribute bgp 10 metric 100000 1 255 255 1500
 distance eigrp 90 210
!
router ospf 100 vrf INET2
 router-id 10.8.2.2
 network 172.16.85.5 0.0.0.0 area 0
!
router bgp 10
 bgp router-id 10.8.2.2
 bgp log-neighbor-changes
 bgp listen range 10.0.200.0/24 peer-group INET-SPOKES
 neighbor INET-SPOKES peer-group
 neighbor INET-SPOKES remote-as 10
 neighbor INET-SPOKES timers 20 60
 !
 address-family ipv4
  bgp redistribute-internal
  network 10.8.2.2 mask 255.255.255.255
  network 10.8.3.3 mask 255.255.255.255
  network 10.8.101.0 mask 255.255.255.0
  network 10.8.102.0 mask 255.255.255.0
  network 10.8.103.0 mask 255.255.255.0
  network 10.8.104.0 mask 255.255.255.0
  aggregate-address 10.8.0.0 255.255.0.0 summary-only
  neighbor INET-SPOKES activate
  neighbor INET-SPOKES send-community
  neighbor INET-SPOKES next-hop-self all
  neighbor INET-SPOKES default-originate
  neighbor INET-SPOKES route-map INET-DC1-IN in
  neighbor INET-SPOKES route-map INET-DC1-OUT out
```

```
  distance bgp 20 109 109
 exit-address-family
!
!
virtual-service csr_mgmt
!
ip forward-protocol nd
!
ip bgp-community new-format
ip community-list standard MPLS-DMVPN permit 10:100
ip community-list standard INET-DMVPN permit 10:200
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.124.19.1
!
!
ip prefix-list DC1-LOCAL-ROUTES seq 10 permit 0.0.0.0/0
ip prefix-list DC1-LOCAL-ROUTES seq 20 permit 10.8.0.0/16 le 32
no service-routing capabilities-manager
!
route-map INET-DC1-IN deny 10
 match ip address prefix-list DC1-LOCAL-ROUTES
!
route-map INET-DC1-IN permit 20
 set community 10:200
!
route-map TO-PEER permit 10
 match ip address prefix-list DC1-LOCAL-ROUTES
 set ip next-hop self
 set community no-advertise
!
route-map site_prefixes permit 10
 match ip address prefix-list site_prefixes
!
route-map INET-DC1-OUT permit 10
 match ip address prefix-list DC1-LOCAL-ROUTES
 set community 10:200
!
route-map INET-DC1-OUT permit 20
 description readvertise routes learned from INTERNET DMVPN cloud
 match community INET-DMVPN
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 no login
line vty 5 15
 exec-timeout 0 0
 privilege level 15
 no login
!
ntp source Loopback0
ntp server 10.8.3.3
!
end
```

8.4 Example configuration on Branch10(R10)

```
Branch10#show running-config
Building configuration...

Current configuration : 8517 bytes
!
! Last configuration change at 02:29:54 CST Mon Nov 3 2014
!
version 15.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
no platform punt-keepalive disable-kernel-core
platform shell
platform console serial
!
hostname Branch10
!
boot-start-marker
boot-end-marker
!
!
vrf definition INET2
 rd 65512:2
 !
 address-family ipv4
 exit-address-family
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
!
no logging console
!
no aaa new-model
clock timezone CST 8 0
!
!
!
!
!
!
!
!
!
!
!
!
!


no ip domain lookup

!
!
!
!
!
!
!
```

```
!
!
!
subscriber templating
!
multilink bundle-name authenticated
!
domain one
 vrf default
  border
   source-interface Loopback0
   master local
  master branch
   source-interface Loopback0
   hub 10.8.3.3
!
!
license udi pid CSR1000V sn 92WYKUIJKRO
license boot level ax
spanning-tree extend system-id
!
!
redundancy
 mode none
!
!
!
!
!
!
ip ftp source-interface GigabitEthernet1
ip ftp username mgcusr
ip ftp password mgcusr
ip tftp source-interface GigabitEthernet1
!
!
crypto keyring DMVPN-KEYRING1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
crypto keyring DMVPN-KEYRING2 vrf INET2
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
!
!
!
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
crypto isakmp invalid-spi-recovery
crypto isakmp keepalive 40 5
crypto isakmp profile ISAKMP-INET1
   keyring DMVPN-KEYRING1
   match identity address 0.0.0.0
crypto isakmp profile ISAKMP-INET2
   keyring DMVPN-KEYRING2
   match identity address 0.0.0.0 INET2
!
crypto ipsec security-association idle-time 60
crypto ipsec security-association replay window-size 512
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE1
 set transform-set AES256/SHA/TRANSPORT
```

```
 set isakmp-profile ISAKMP-INET1
!
crypto ipsec profile DMVPN-PROFILE2
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile ISAKMP-INET2
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.2.10.10 255.255.255.255
!
interface Tunnel100
 bandwidth 100000
 ip address 10.0.100.10 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map 10.0.100.84 172.16.84.4
 ip nhrp map multicast 172.16.84.4
 ip nhrp network-id 1
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.100.84
 ip nhrp registration timeout 60
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 load-interval 30
 delay 1000
 tunnel source GigabitEthernet2
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile DMVPN-PROFILE1
!
interface Tunnel200
 bandwidth 50000
 ip address 10.0.200.10 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map 10.0.200.85 172.16.85.5
 ip nhrp map multicast 172.16.85.5
 ip nhrp network-id 2
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.200.85
 ip nhrp registration timeout 60
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 load-interval 30
 delay 1000
 tunnel source GigabitEthernet3
 tunnel mode gre multipoint
 tunnel key 200
 tunnel vrf INET2
 tunnel protection ipsec profile DMVPN-PROFILE2
!
interface GigabitEthernet1
 vrf forwarding Mgmt-intf
 ip address 10.124.19.212 255.255.255.0
 negotiation auto
!
```

```
interface GigabitEthernet2
 description --MPLS--
 ip address 172.16.101.10 255.255.255.0
 speed 1000
 no negotiation auto
!
interface GigabitEthernet3
 description --INET--
 vrf forwarding INET2
 ip address 172.16.102.10 255.255.255.0
 load-interval 30
 speed 1000
 no negotiation auto
!
interface GigabitEthernet4
 no ip address
 speed 1000
 no negotiation auto
!
interface GigabitEthernet5
 no ip address
 speed 1000
 no negotiation auto
!
interface GigabitEthernet5.100
 encapsulation dot1Q 100
 ip address 10.1.10.1 255.255.255.0
!
router ospf 200 vrf INET2
 network 172.16.102.10 0.0.0.0 area 0
!
router ospf 100
 router-id 10.2.10.10
 network 101.7.7.2 0.0.0.0 area 0
 network 172.16.101.10 0.0.0.0 area 0
!
router bgp 10
 bgp router-id 10.2.10.10
 bgp log-neighbor-changes
 neighbor MPLS-HUB peer-group
 neighbor MPLS-HUB remote-as 10
 neighbor MPLS-HUB timers 20 60
 neighbor INET-HUB peer-group
 neighbor INET-HUB remote-as 10
 neighbor INET-HUB timers 20 60
 neighbor 10.0.100.84 peer-group MPLS-HUB
 neighbor 10.0.200.85 peer-group INET-HUB
 !
 address-family ipv4
  network 10.1.10.0 mask 255.255.255.0
  network 10.2.10.10 mask 255.255.255.255
  neighbor MPLS-HUB send-community
  neighbor MPLS-HUB route-map MPLS-SPOKE-IN in
  neighbor MPLS-HUB route-map MPLS-SPOKE-OUT out
  neighbor INET-HUB send-community
  neighbor INET-HUB route-map INET-SPOKE-IN in
  neighbor INET-HUB route-map INET-SPOKE-OUT out
  neighbor 10.0.100.84 activate
  neighbor 10.0.100.84 soft-reconfiguration inbound
  neighbor 10.0.200.85 activate
  neighbor 10.0.200.85 soft-reconfiguration inbound
 exit-address-family
!
!
virtual-service csr_mgmt
```

```
!
ip forward-protocol nd
!
ip bgp-community new-format
ip community-list standard MPLS-HUB1 permit 10:100
ip community-list standard MPLS-HUB2 permit 10:101
ip community-list standard INET-HUB1 permit 10:200
ip community-list standard INET-HUB2 permit 10:201
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.124.19.1
!
ip access-list extended RC
 permit tcp host 10.1.10.2 any
ip access-list extended SMP
 permit udp any eq 18000 any eq 19000
!
!
ip prefix-list INET-DMVPN seq 5 permit 0.0.0.0/0
ip prefix-list INET-DMVPN seq 10 permit 10.8.0.0/16
!
ip prefix-list MPLS-DMVPN seq 5 permit 0.0.0.0/0
ip prefix-list MPLS-DMVPN seq 10 permit 10.8.0.0/16
no service-routing capabilities-manager
!
route-map MPLS-SPOKE-OUT deny 10
 match ip address prefix-list INET-DMVPN
!
route-map MPLS-SPOKE-OUT permit 20
!
route-map INET-SPOKE-OUT deny 10
 match ip address prefix-list MPLS-DMVPN
!
route-map INET-SPOKE-OUT permit 20
!
route-map MPLS-SPOKE-IN permit 5
 match ip address prefix-list MPLS-DMVPN
 set local-preference 201
!
route-map MPLS-SPOKE-IN permit 10
 match community MPLS-HUB1
 set local-preference 201
!
route-map MPLS-SPOKE-IN permit 20
 match community MPLS-HUB2
 set local-preference 200
!
route-map INET-SPOKE-IN permit 5
 match ip address prefix-list MPLS-DMVPN
 set local-preference 151
!
route-map INET-SPOKE-IN permit 30
 match community INET-HUB1
 set local-preference 151
!
route-map INET-SPOKE-IN permit 40
 match community INET-HUB2
 set local-preference 150
!
!
!
control-plane
!
!
line con 0
```

```
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 no login
line vty 5 15
 exec-timeout 0 0
 privilege level 15
 no login
!
ntp source Loopback0
ntp server 10.8.3.3
!
end
```

8.5 Example configuration on Branch11(R11)

```
Branch11#show running-config
Building configuration...

Current configuration : 6929 bytes
!
! Last configuration change at 02:30:33 CST Mon Nov 3 2014
! NVRAM config last updated at 02:30:34 CST Mon Nov 3 2014
!
version 15.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
no platform punt-keepalive disable-kernel-core
platform shell
platform console serial
!
hostname Branch11
!
boot-start-marker
boot-end-marker
!
!
vrf definition INET2
 rd 65512:2
 !
 address-family ipv4
 exit-address-family
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
!
no logging console
!
no aaa new-model
clock timezone CST 8 0
!
!
!
!
!
!
!
!
```

```
!
!
!
!
!
!
!


no ip domain lookup

!
!
!
!
!
!
!
!
!
subscriber templating
!
multilink bundle-name authenticated
!
domain one
 vrf default
  border
   source-interface Loopback0
   master local
  master branch
   source-interface Loopback0
   hub 10.8.3.3
!
!
license udi pid CSR1000V sn 9YRYPG7XWOA
license boot level ax
spanning-tree extend system-id
!
!
redundancy
 mode none
!
!
!
!
!
!
ip ftp source-interface GigabitEthernet1
ip ftp username mgcusr
ip ftp password mgcusr
ip tftp source-interface GigabitEthernet1
!
crypto keyring DMVPN-KEYRING1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
crypto keyring DMVPN-KEYRING2 vrf INET2
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
!
!
!
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
```

```
crypto isakmp invalid-spi-recovery
crypto isakmp keepalive 40 5
crypto isakmp profile ISAKMP-INET1
   keyring DMVPN-KEYRING1
   match identity address 0.0.0.0
crypto isakmp profile ISAKMP-INET2
   keyring DMVPN-KEYRING2
   match identity address 0.0.0.0 INET2
!
crypto ipsec security-association idle-time 60
crypto ipsec security-association replay window-size 512
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE1
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile ISAKMP-INET1
!
crypto ipsec profile DMVPN-PROFILE2
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile ISAKMP-INET2
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.2.11.11 255.255.255.255
!
interface Tunnel100
 bandwidth 100000
 ip address 10.0.100.11 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map 10.0.100.84 172.16.84.4
 ip nhrp map multicast 172.16.84.4
 ip nhrp network-id 1
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.100.84
 ip nhrp registration timeout 60
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 load-interval 30
 delay 1000
 tunnel source GigabitEthernet3
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile DMVPN-PROFILE1
!
interface Tunnel200
 bandwidth 50000
 ip address 10.0.200.11 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map 10.0.200.85 172.16.85.5
 ip nhrp map multicast 172.16.85.5
 ip nhrp network-id 2
 ip nhrp holdtime 600
```

```
 ip nhrp nhs 10.0.200.85
 ip nhrp registration timeout 60
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 load-interval 30
 delay 1000
 tunnel source GigabitEthernet6
 tunnel mode gre multipoint
 tunnel key 200
 tunnel vrf INET2
 tunnel protection ipsec profile DMVPN-PROFILE2
!
interface GigabitEthernet1
 vrf forwarding Mgmt-intf
 ip address 10.124.19.213 255.255.255.0
 negotiation auto
!
interface GigabitEthernet2
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet3
 description --MPLS--
 ip address 172.16.111.11 255.255.255.0
 load-interval 30
 negotiation auto
!
interface GigabitEthernet4
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet5
 no ip address
 negotiation auto
!
interface GigabitEthernet5.200
 encapsulation dot1Q 200
 ip address 10.1.11.1 255.255.255.0
!
interface GigabitEthernet6
 description --INET--
 vrf forwarding INET2
 ip address 172.16.112.11 255.255.255.0
 negotiation auto
!
router ospf 200 vrf INET2
 network 172.16.112.11 0.0.0.0 area 0
!
router ospf 100
 router-id 10.2.11.11
 network 101.7.8.2 0.0.0.0 area 0
 network 172.16.111.11 0.0.0.0 area 0
!
router bgp 10
 bgp router-id 10.2.11.11
 bgp log-neighbor-changes
 neighbor MPLS-HUB peer-group
 neighbor MPLS-HUB remote-as 10
 neighbor MPLS-HUB timers 20 60
 neighbor INET-HUB peer-group
 neighbor INET-HUB remote-as 10
 neighbor INET-HUB timers 20 60
 neighbor 10.0.100.84 peer-group MPLS-HUB
```

```
 neighbor 10.0.200.85 peer-group INET-HUB
 !
 address-family ipv4
  network 10.1.11.0 mask 255.255.255.0
  network 10.2.11.11 mask 255.255.255.255
  neighbor MPLS-HUB send-community
  neighbor MPLS-HUB route-map MPLS-SPOKE-IN in
  neighbor MPLS-HUB route-map MPLS-SPOKE-OUT out
  neighbor INET-HUB send-community
  neighbor INET-HUB route-map INET-SPOKE-IN in
  neighbor INET-HUB route-map INET-SPOKE-OUT out
  neighbor 10.0.100.84 activate
  neighbor 10.0.100.84 soft-reconfiguration inbound
  neighbor 10.0.200.85 activate
  neighbor 10.0.200.85 soft-reconfiguration inbound
 exit-address-family
!
!
virtual-service csr_mgmt
!
ip forward-protocol nd
!
ip bgp-community new-format
ip community-list standard MPLS-HUB1 permit 10:100
ip community-list standard MPLS-HUB2 permit 10:101
ip community-list standard INET-HUB1 permit 10:200
ip community-list standard INET-HUB2 permit 10:201
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.124.19.1
!
!
ip prefix-list INET-DMVPN seq 5 permit 0.0.0.0/0
ip prefix-list INET-DMVPN seq 10 permit 10.8.0.0/16
!
ip prefix-list MPLS-DMVPN seq 5 permit 0.0.0.0/0
ip prefix-list MPLS-DMVPN seq 10 permit 10.8.0.0/16
no service-routing capabilities-manager
!
route-map MPLS-SPOKE-OUT deny 10
 match ip address prefix-list INET-DMVPN
!
route-map MPLS-SPOKE-OUT permit 20
!
route-map INET-SPOKE-OUT deny 10
 match ip address prefix-list MPLS-DMVPN
!
route-map INET-SPOKE-OUT permit 20
!
route-map MPLS-SPOKE-IN permit 5
 match ip address prefix-list MPLS-DMVPN
 set local-preference 201
!
route-map MPLS-SPOKE-IN permit 10
 match community MPLS-HUB1
 set local-preference 201
!
route-map MPLS-SPOKE-IN permit 20
 match community MPLS-HUB2
 set local-preference 200
!
route-map site_prefixes permit 10
 match ip address prefix-list site_prefixes
!
route-map INET-SPOKE-IN permit 5
```

```
 match ip address prefix-list MPLS-DMVPN
 set local-preference 151
!
route-map INET-SPOKE-IN permit 30
 match community INET-HUB1
 set local-preference 151
!
route-map INET-SPOKE-IN permit 40
 match community INET-HUB2
 set local-preference 150
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 no login
line vty 5 15
 exec-timeout 0 0
 privilege level 15
 no login
!
ntp source Loopback0
ntp server 10.8.3.3
!
end
```