
TOMORROW
starts here.
CISCO
Cisco live!

Implementing Next Gen Performance Routing – PFRv3

BRKRST-2362

Peter Thomas
Systems Engineer

#clmel

Cisco live!

Agenda

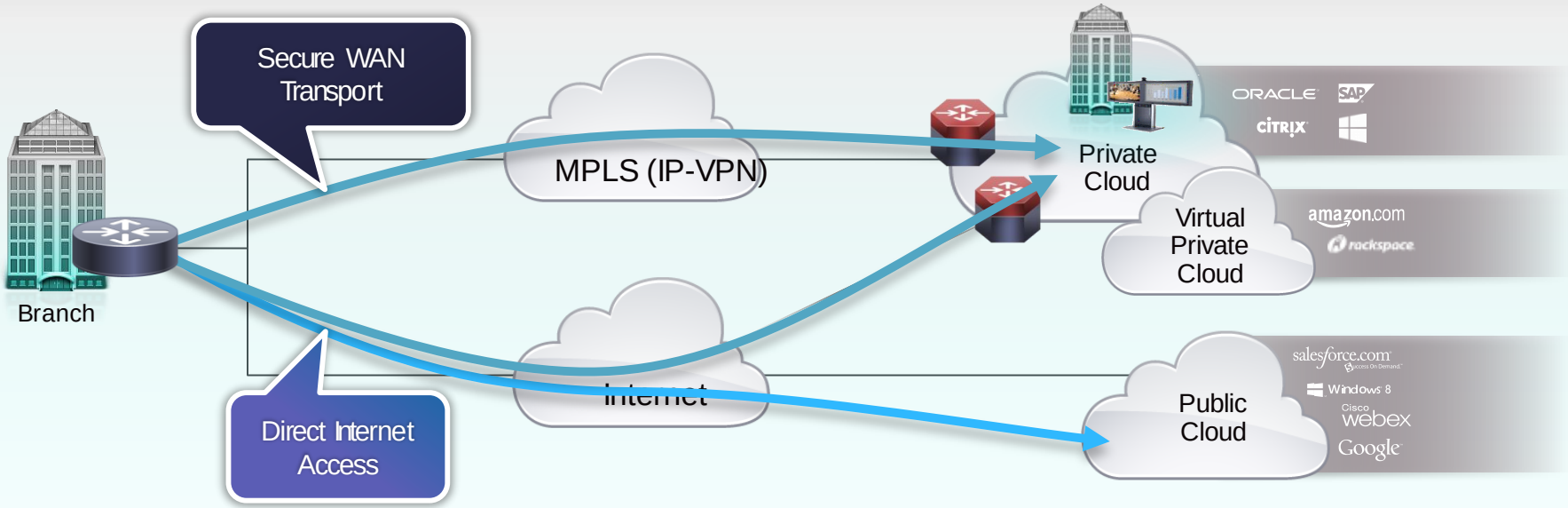
- Business Trends
- PfRv3 Principles
- Monitoring Details – The Life of a Packet
- Path Enforcement – Route Override
- Enterprise Deployment
- IWAN Management
- Key Takeaways

Business Trends

Cisco live!

Hybrid WAN: Leveraging the Internet

Secure WAN Transport and Internet Access



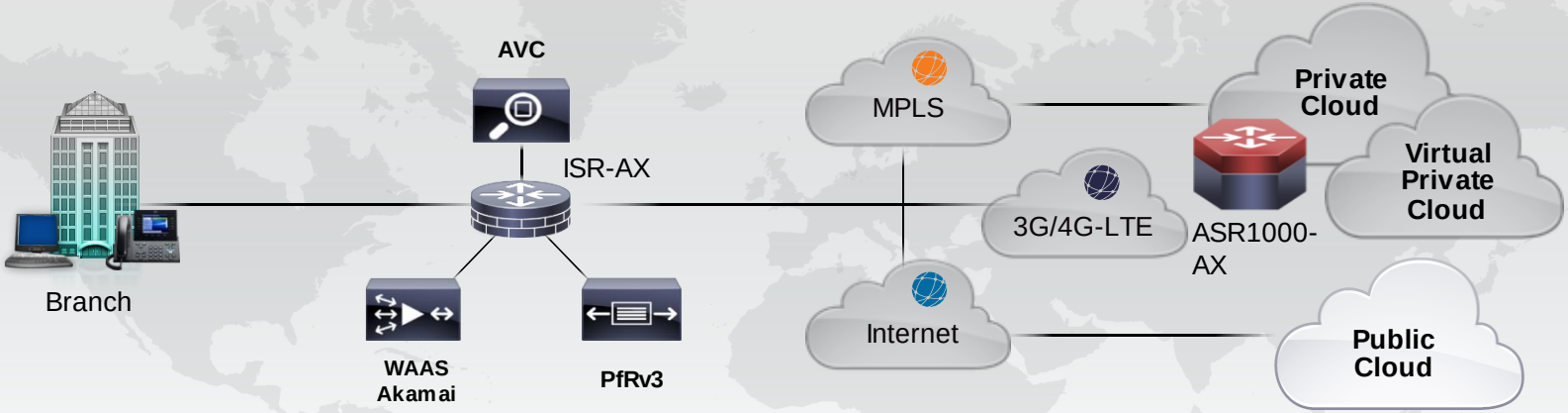
Secure WAN transport for private and virtual private cloud access

Leverage **local Internet** path for public cloud and Internet access

Increased WAN transport capacity, cost effectively!

Improve application performance (right flows to right places)

Cisco Intelligent WAN (IWAN)

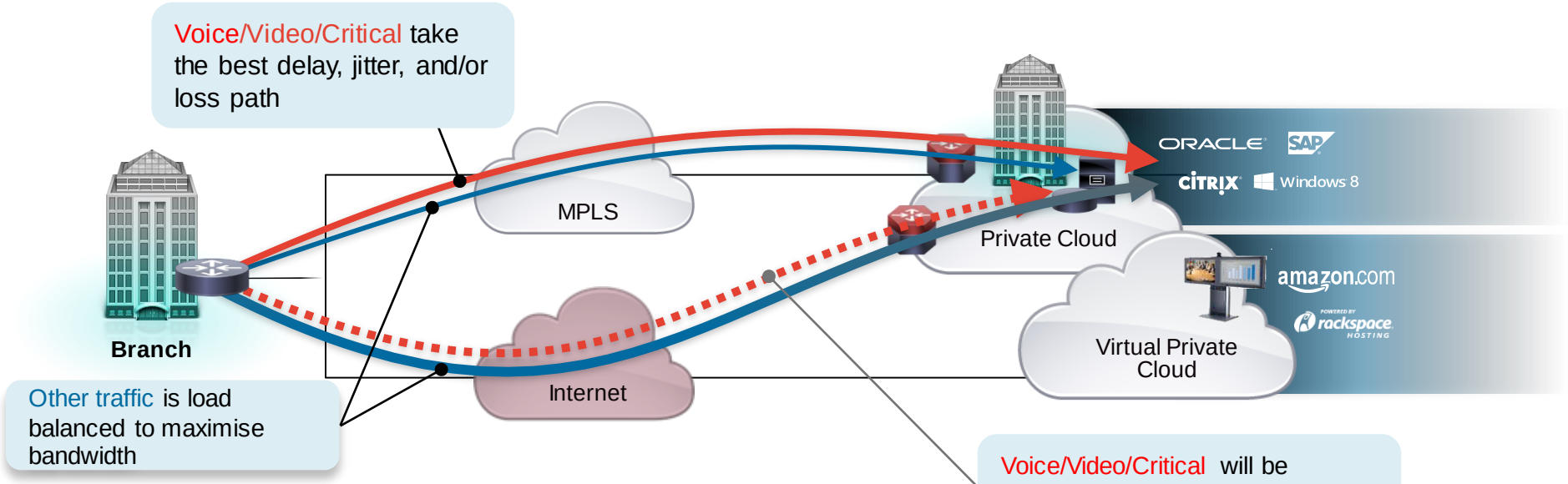


APIC **Management & Orchestration**

Transport Independence	Intelligent Path Control	Application Optimisation	Secure Connectivity
IPSec WAN Overlay	Optimal application routing	Performance monitoring	NG Strong Encryption
Consistent Operational Model	Efficient use of bandwidth	Optimisation and Caching	Threat Defence
DMVPN	**Performance Routing**	**AVC, WAAS, Akamai**	**Suite-B, CWS, ZBFW**

Intelligent Path Control with PfR

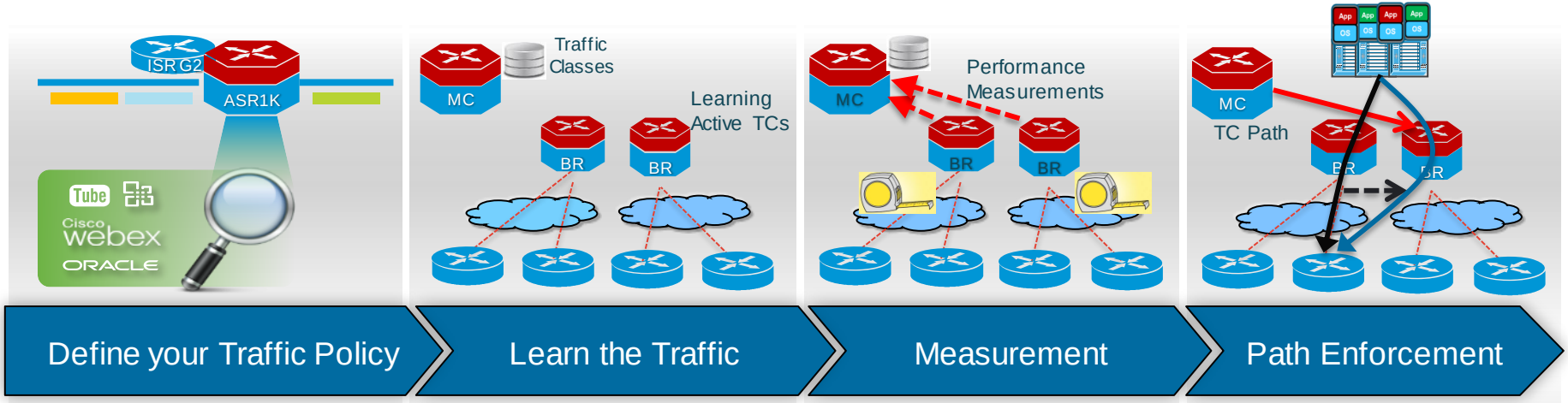
Leveraging the Internet



- PfR monitors network performance and routes applications based on application performance policies
- PfR load balances traffic based upon link utilisation levels to efficiently utilise all available WAN bandwidth

Cisco live!

PfRv3 – How it Works



Define path optimisation policies on the Hub MC

- load balancing,
- path preference, application metrics

DSCP Based Policies

Application Based Policies

Traffic flowing through the Border Routers (BRs) that match a policy are learned Traffic Classes

Unified Performance Monitor

Report the measured TC performance metrics to the Master Controller for policy compliance

Unified Performance Monitor

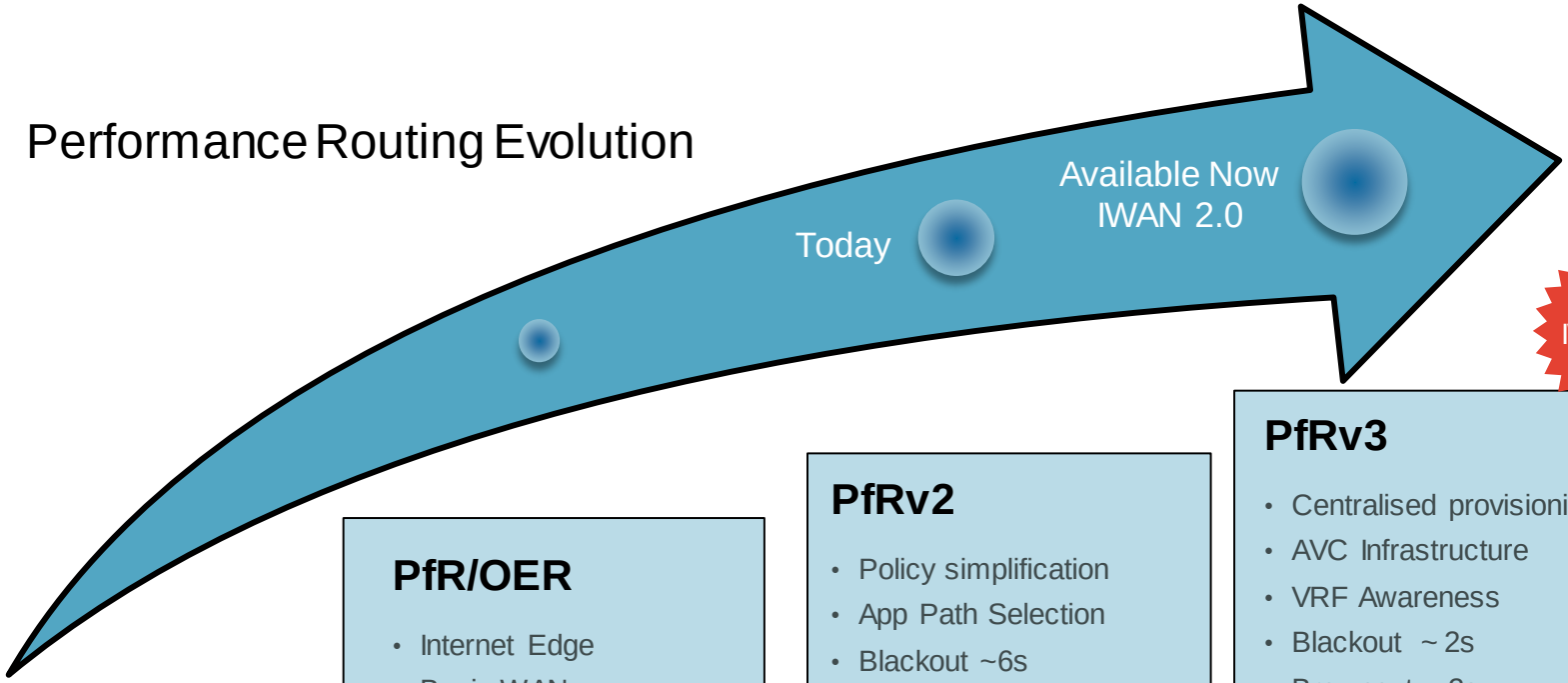
Master Controller directs BR path changes to keep traffic within policy

Route Enforcement module in feature path

Cisco live!

Intelligent Path Control

Performance Routing Evolution



IWAN 2.0

PfR/OER

- Internet Edge
- Basic WAN
- Provisioning per site per policy
- 1000s of lines of config

PfRv2

- Policy simplification
- App Path Selection
- Blackout ~6s
- Brownout ~9s
- Scale 500 sites
- 10s of lines of config

PfRv3

- Centralised provisioning
- AVC Infrastructure
- VRF Awareness
- Blackout ~ 2s
- Brownout ~ 2s
- Scale 2000 sites
- Hub config only

Configuration – Improvement and Simplification

PfRv2

- 500 sites
- ~90 lines of configuration
- All MCs

PfRv3 MC Configuration on Hub site only

```
domain <MYNAME>
 vrf <name>
  master hub
   source-interface Loopback0
   password IWAN
   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 mpls fallback inet
   class APPLICATION sequence 30
    match dscp af31 policy low-latency-data
```

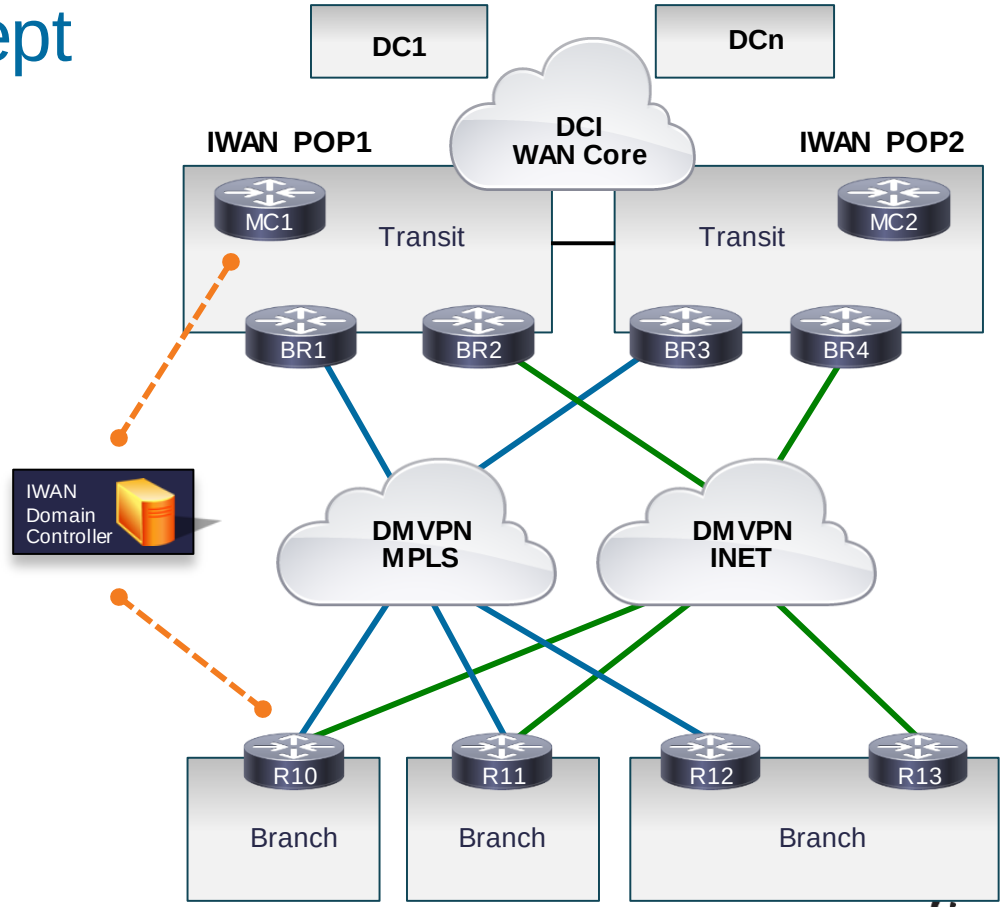
- 2000 sites
- <20 lines of configuration, all under “domain”
- On the hub only

PfRv3 Principles

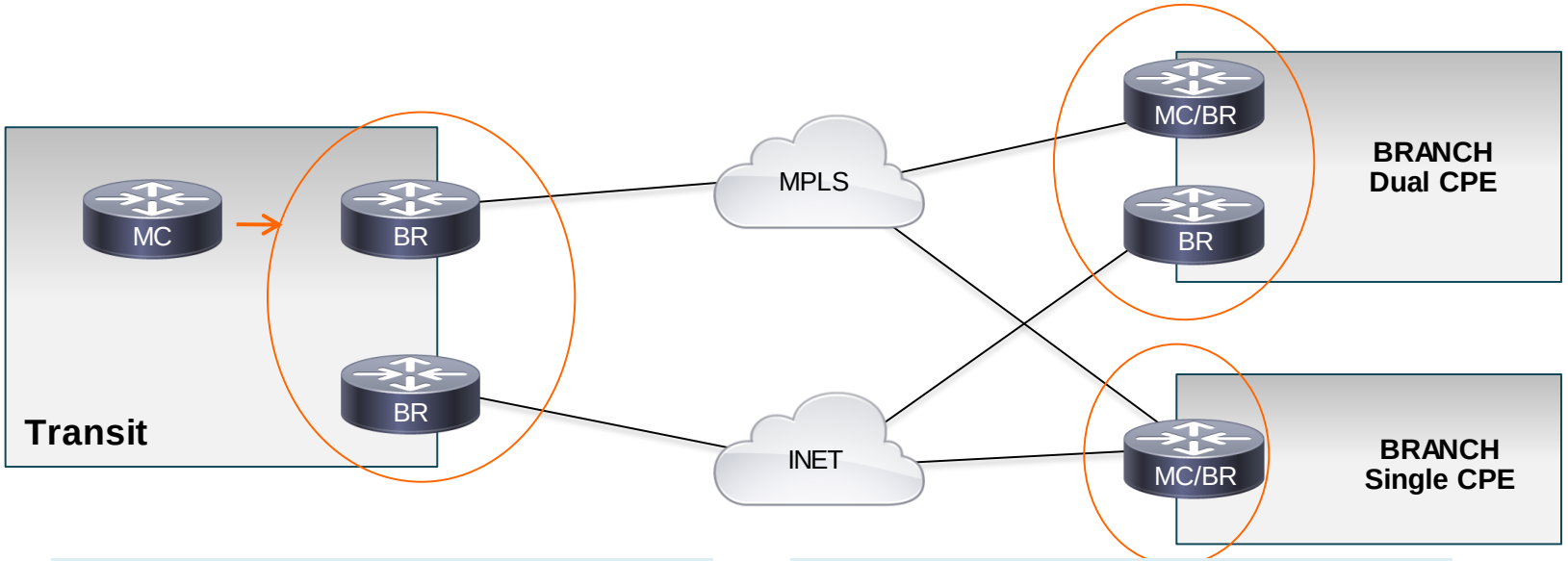
Cisco live!

IWAN Domain – Concept

- A collection of sites sharing the same set of policies
- Each site runs Performance Routing components
- They exchange services through the Enterprise Domain Peering framework
- Centralised configuration from a Domain Controller
- Overlay network per Transport for flexibility and simplification



PfRv3 Components



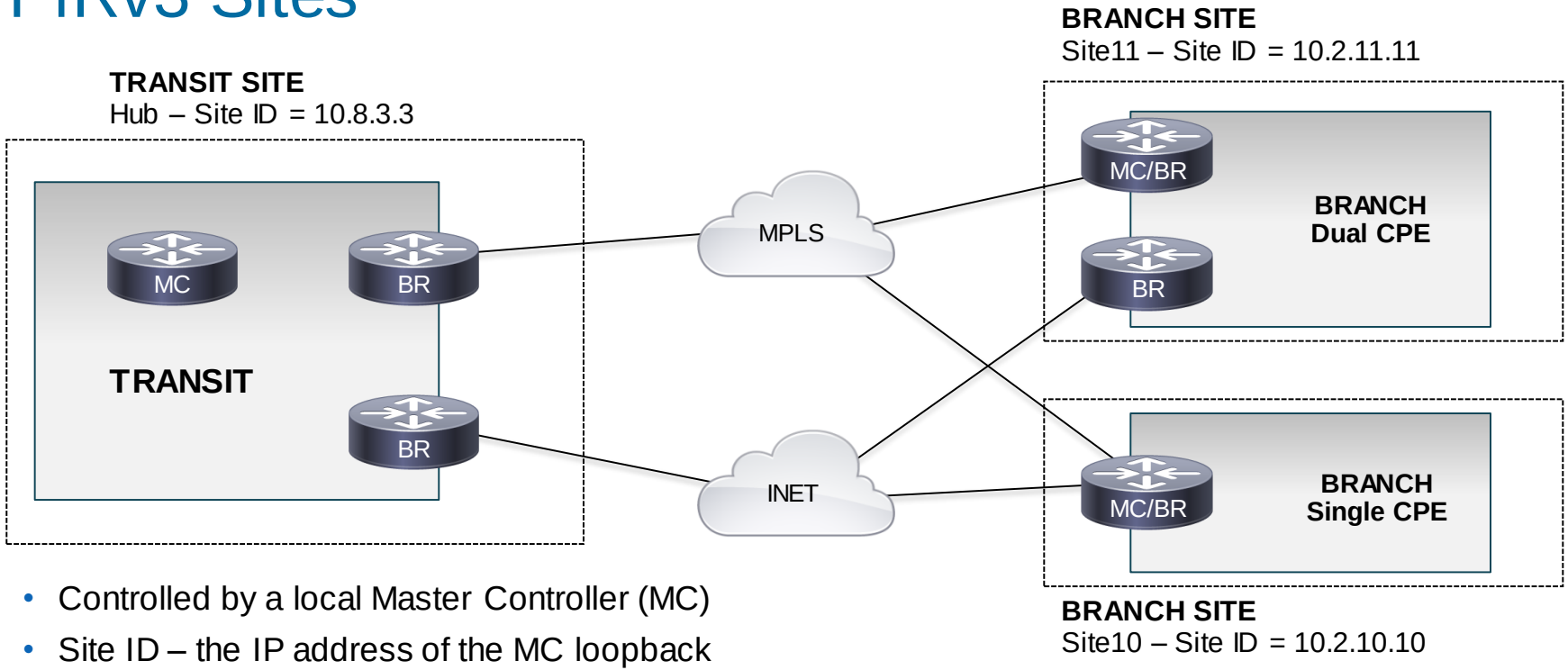
The Decision Maker: Master Controller (MC)

- Apply policy, verification, reporting
- No packet forwarding/ inspection required
- Standalone of combined with a BR
- VRF Aware

The Forwarding Path: Border Router (BR)

- Gain network visibility in forwarding path (Learn, measure)
- Enforce MC's decision (path enforcement)
- VRF aware

PfRv3 Sites

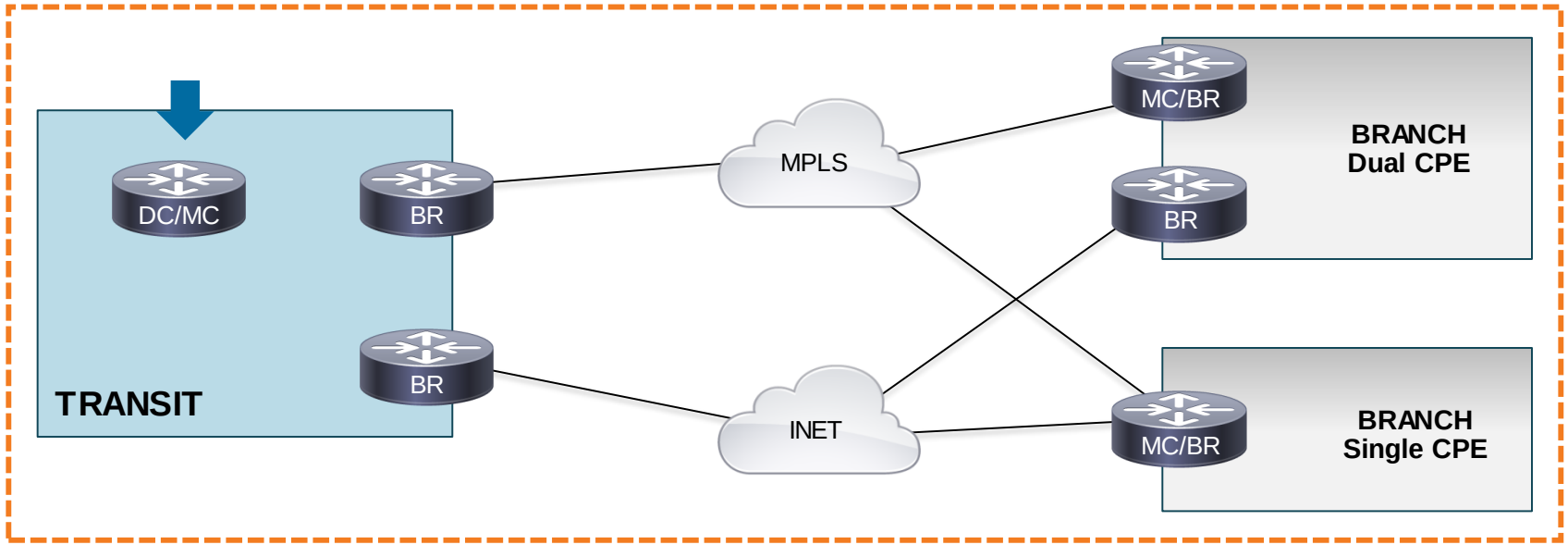


- Controlled by a local Master Controller (MC)
- Site ID – the IP address of the MC loopback
- One/Multiple BRs
- Each BR one/multiple links

Site Type

- Transit Sites – Enterprise POPs or Hubs
- Branch Sites - Stub

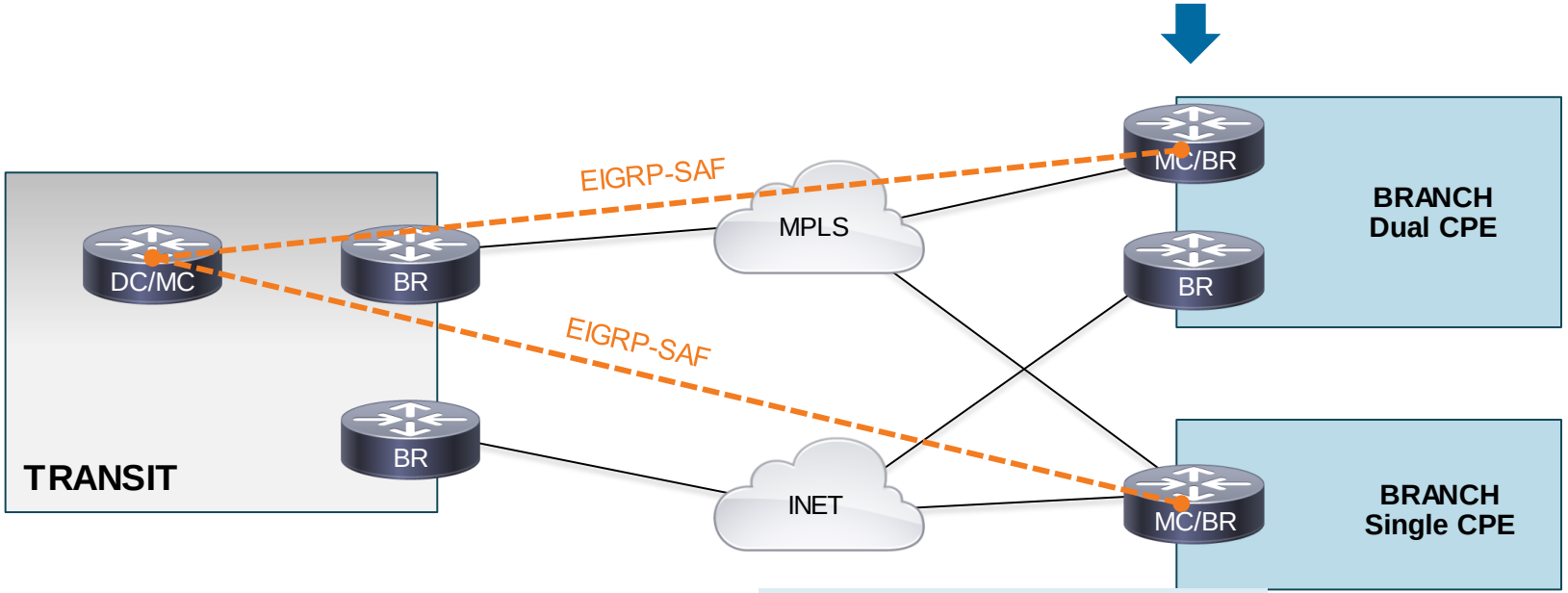
Transit Site – Hub Master Controller




```
domain IWAN
 vrf default
  master hub
   source-interface Loopback0
```

- One of the MC is assigned the Domain Controller role
- Central point of provisioning for Domain policies
- **DC + MC = Hub Master Controller**

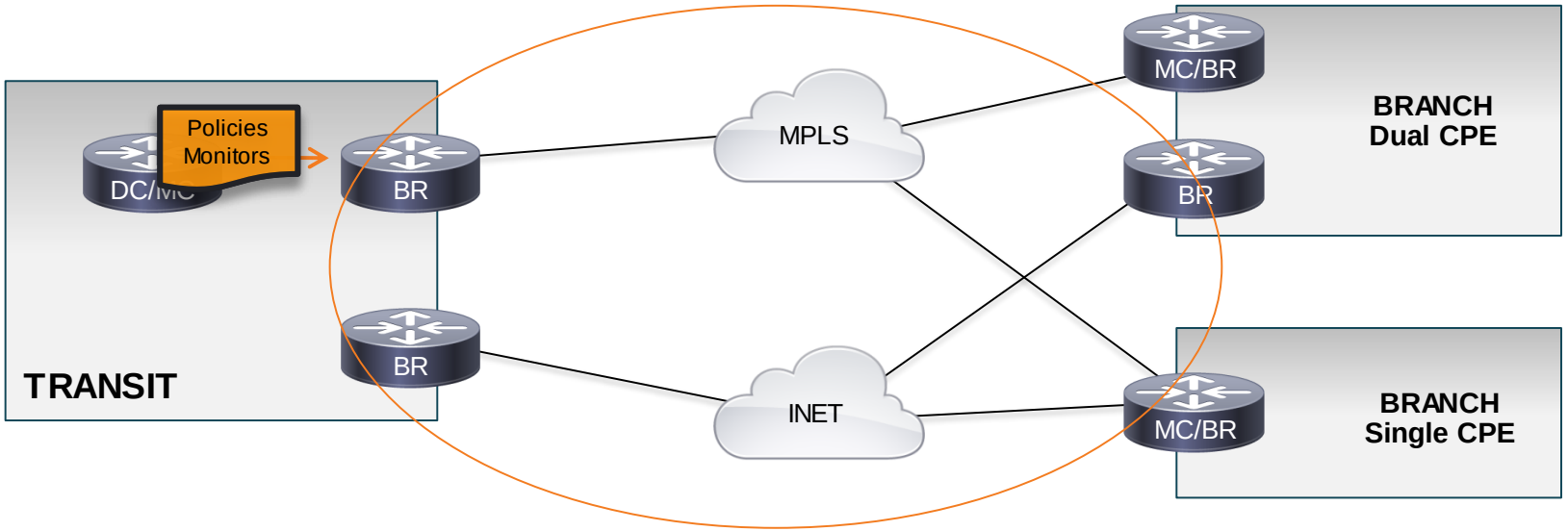
Branch Site



- Service Exchange
- Policies and Monitor configurations
- Site Prefixes

```
domain IWAN
 vrf default
  master branch
   source-interface Loopback0
   hub 10.8.3.3
  border
   source-interface Loopback0
   master local
```

Policy/Monitor Distribution



- Domain policies and monitor instances are configured on the Hub MC.
- Policies are defined per VRF
- Then distributed to branch sites using the peering infrastructure

Performance Policies - DSCP or App Based

```
domain IWAN
 vrf default
  master hub
   load-balance
   class MEDIA sequence 10
    match application telepresence-media policy real-time-video
    match application ms-lync policy real-time-video
    path-preference MPLS fallback INET
   class VOICE sequence 20
    match dscp ef policy voice
    path-preference MPLS fallback INET
   class CRITICAL sequence 30
    match dscp af31 policy low-latency-data
```

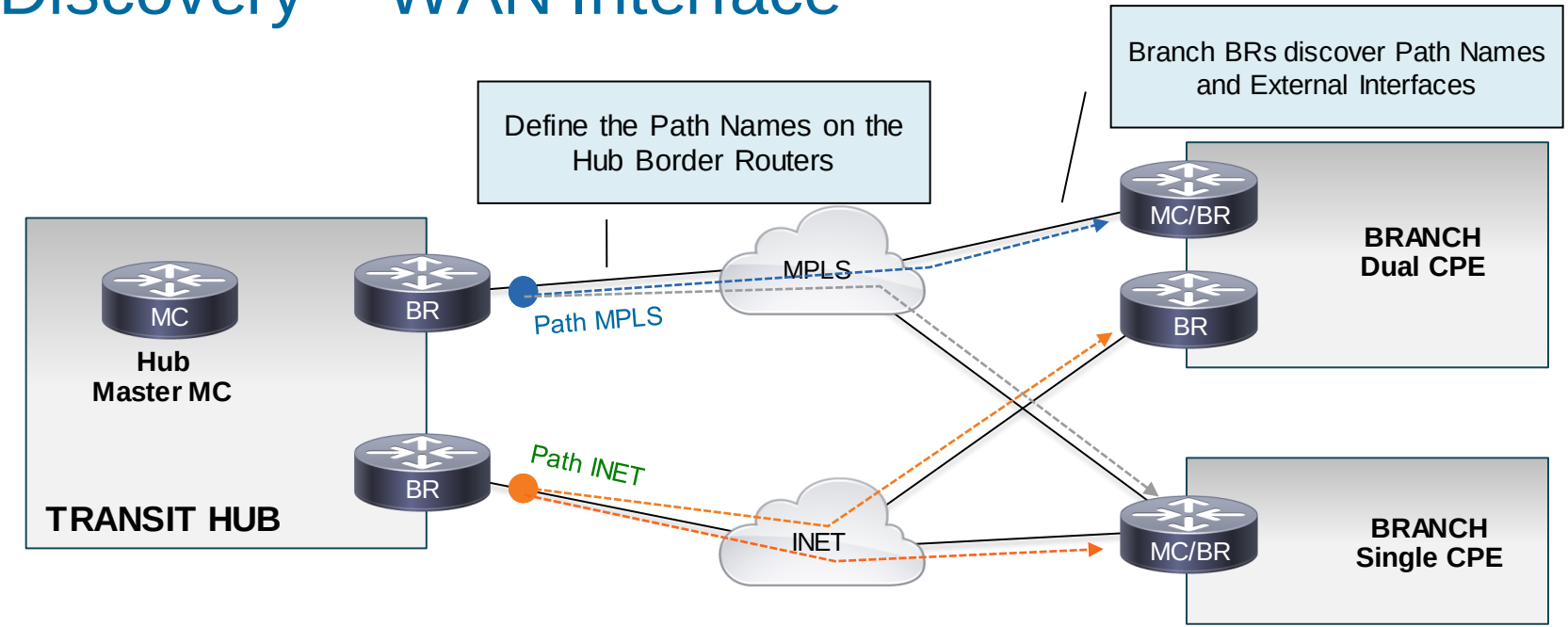
- Policies:
  - DSCP or Application Based Policies (NBAR2)
  - DSCP marking can be used with NBAR2 on the LAN interface (ingress on BR)
- Default Class is load balanced

Built-in Policy Templates

Pre-defined Template	Threshold Definition
Voice	priority 1 one-way-delay 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 (%)

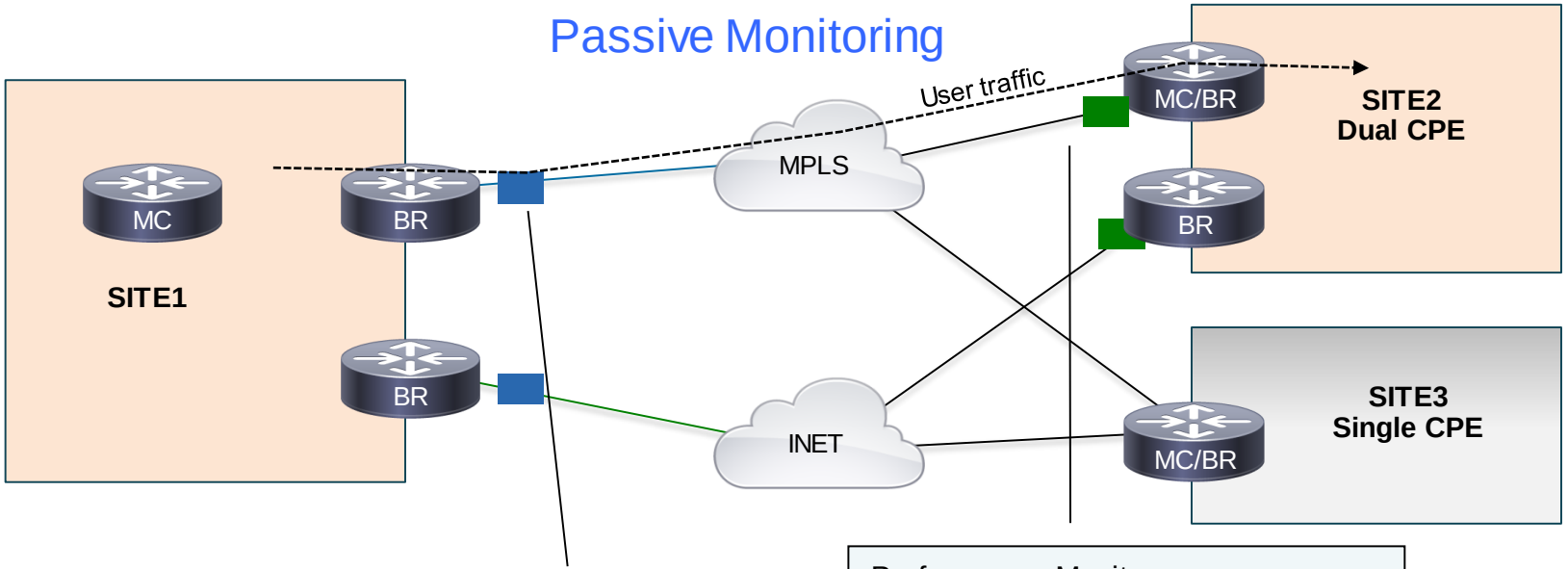
Pre-defined Template	Threshold Definition
Bulk-data	priority 1 one-way-delay threshold 300 (msec) priority 2 byte-loss-rate threshold 5 (%) priority 2 packet-loss-rate threshold 5 (%)
Best-effort	priority 1 one-way-delay threshold 500 (msec) priority 2 byte-loss-rate threshold 10 (%) priority 2 packet-loss-rate 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 (%)

Discovery – WAN Interface



- Using Smart Probes
- Hub generates Discovery packets over all available paths
- Discovery packets intercepted on spokes
- External interfaces and path names automatically discovered and added

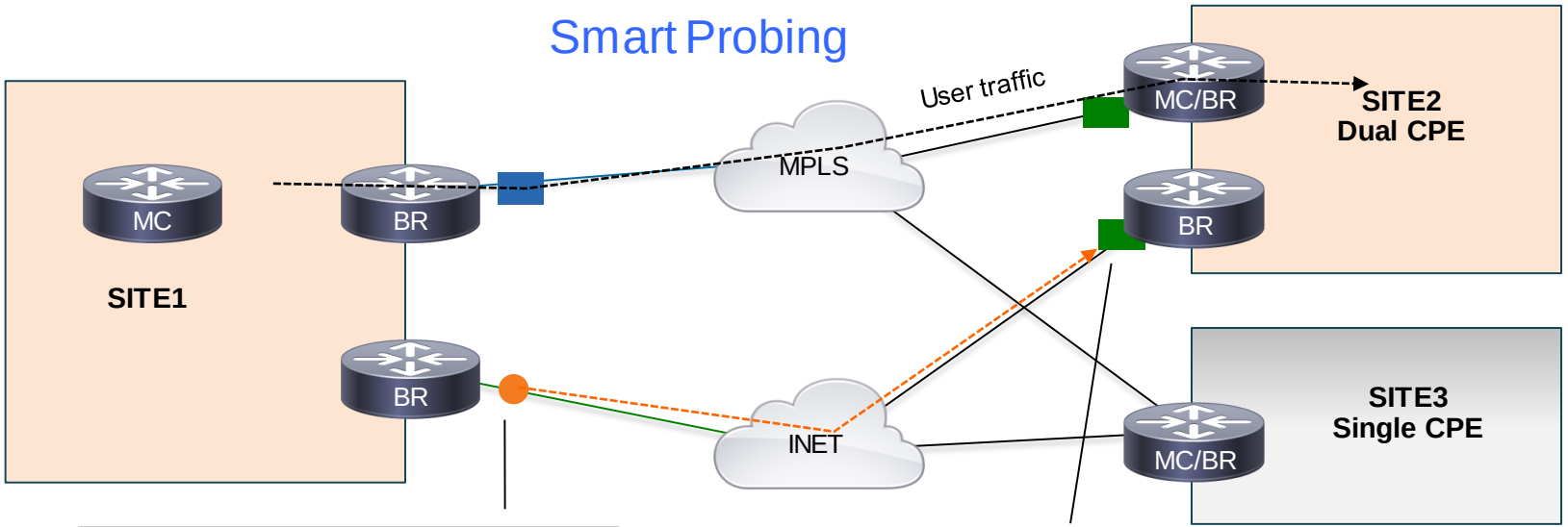
Performance Monitoring – User Traffic



Bandwidth on egress
Per Traffic Class
(dest-prefix, DSCP, AppName)

Performance Monitor
- Collect Performance Metrics
- Per Channel
  - Per DSCP
  - Per Source and Destination Site
  - Per Interface

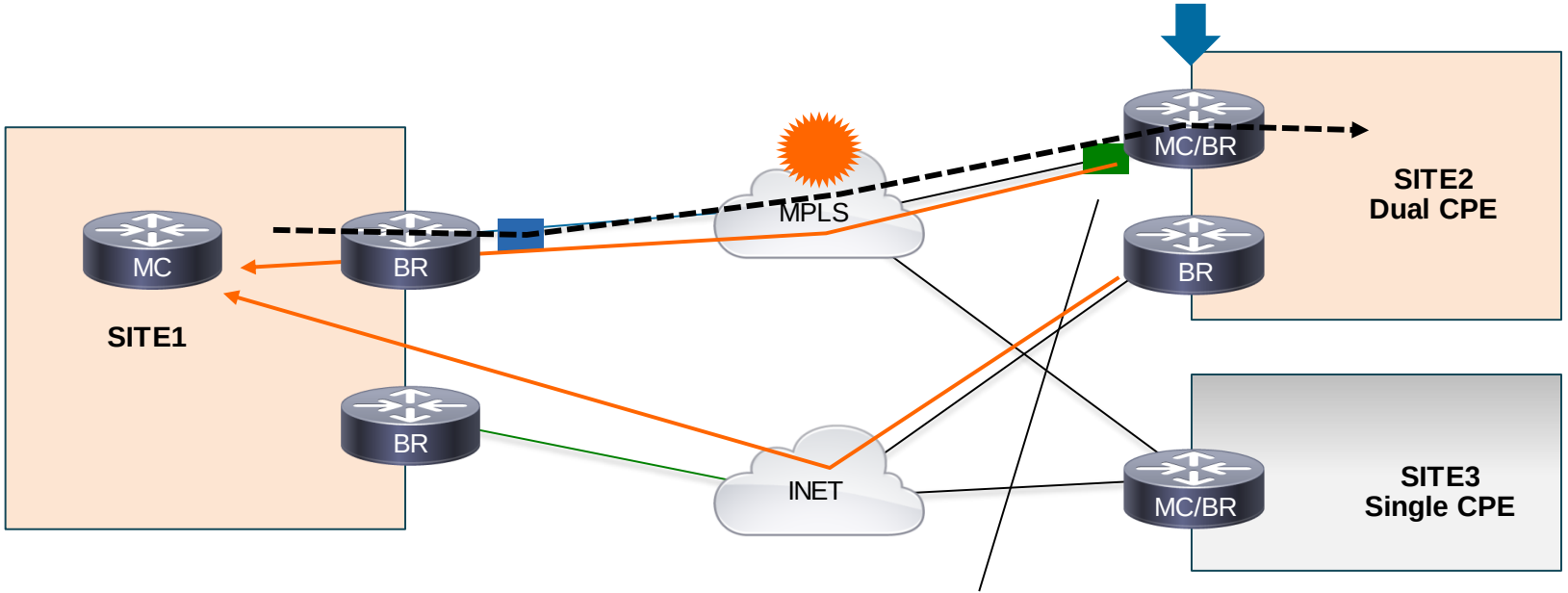
Performance Monitoring



Integrated Smart Probes
- Traffic driven – intelligent on/off
- Site to site and per DSCP

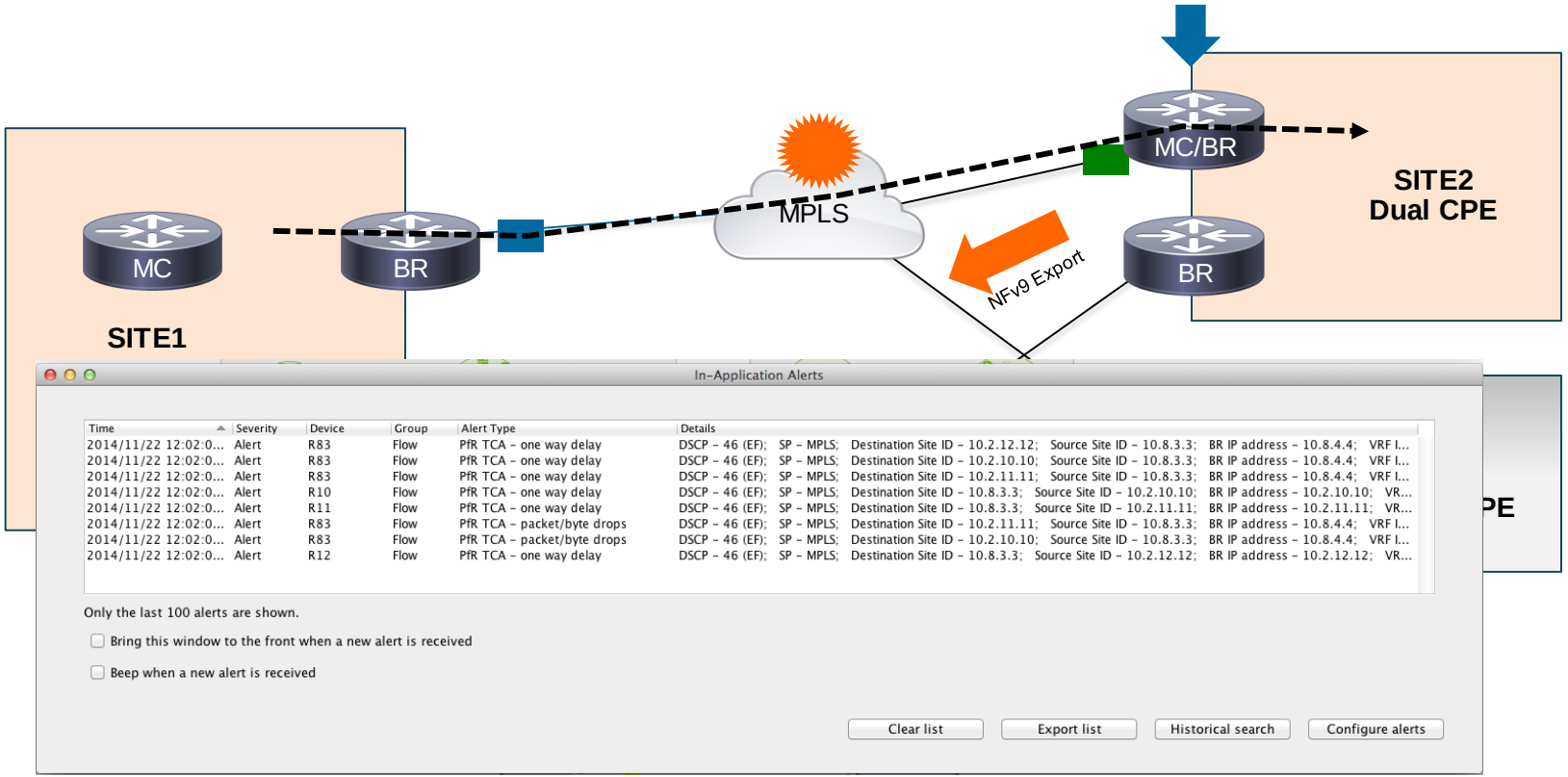
Performance Monitor
- Collect Performance Metrics
- Per Channel
  - Per DSCP
  - Per Source and Destination Site
  - Per Interface

Performance Violation

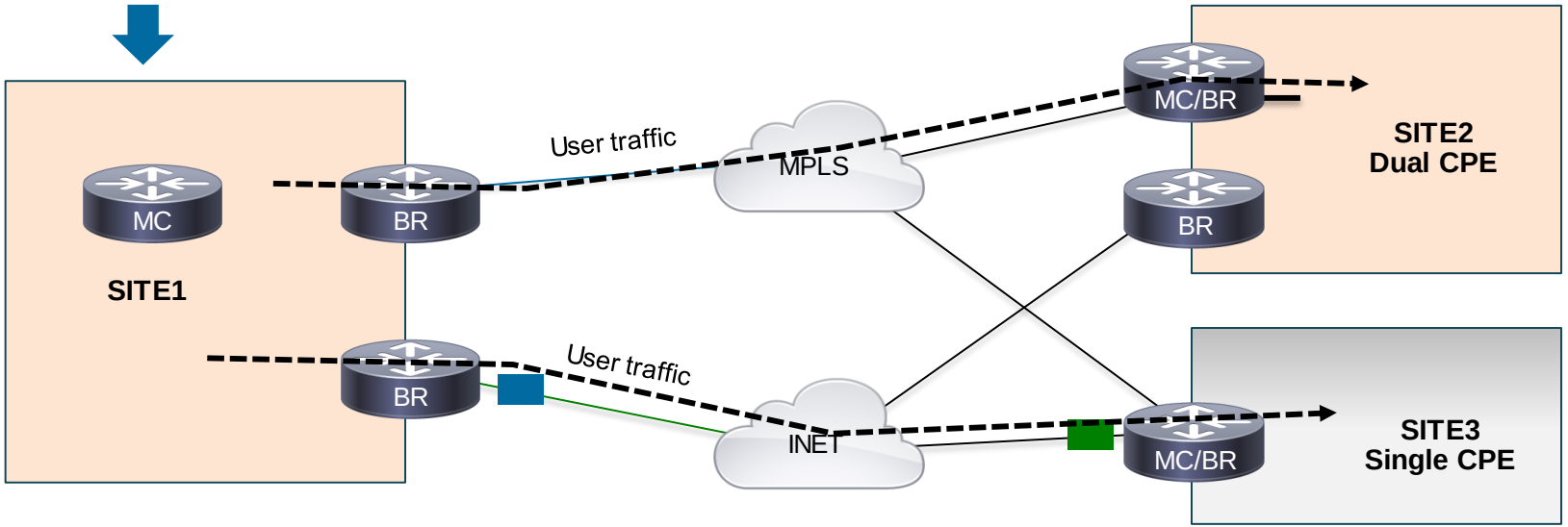


Threshold Crossing Alert (TCA)
- Sent to source site
- loss, delay, jitter, unreachable

Performance Violation – NetFlow Export



Policy Decision



- Reroute Traffic to a Secondary Path

Key Points and … Limitations

- Key Points
  - DSCP or Application (NBAR2) based policies
  - Control traffic in the global Routing Table and per VRF
  - Passive Monitoring based on user traffic
  - Leverage smart probing when needed
  - Cooperation between pair of sites
  - Exports of PfR information with NetFlow v9 to collectors
- Limitation:
  - No IPv6 support yet (Roadmap) – But infrastructure is IPv6 ready
  - NBAR2 with Asymmetric Routing is not yet supported

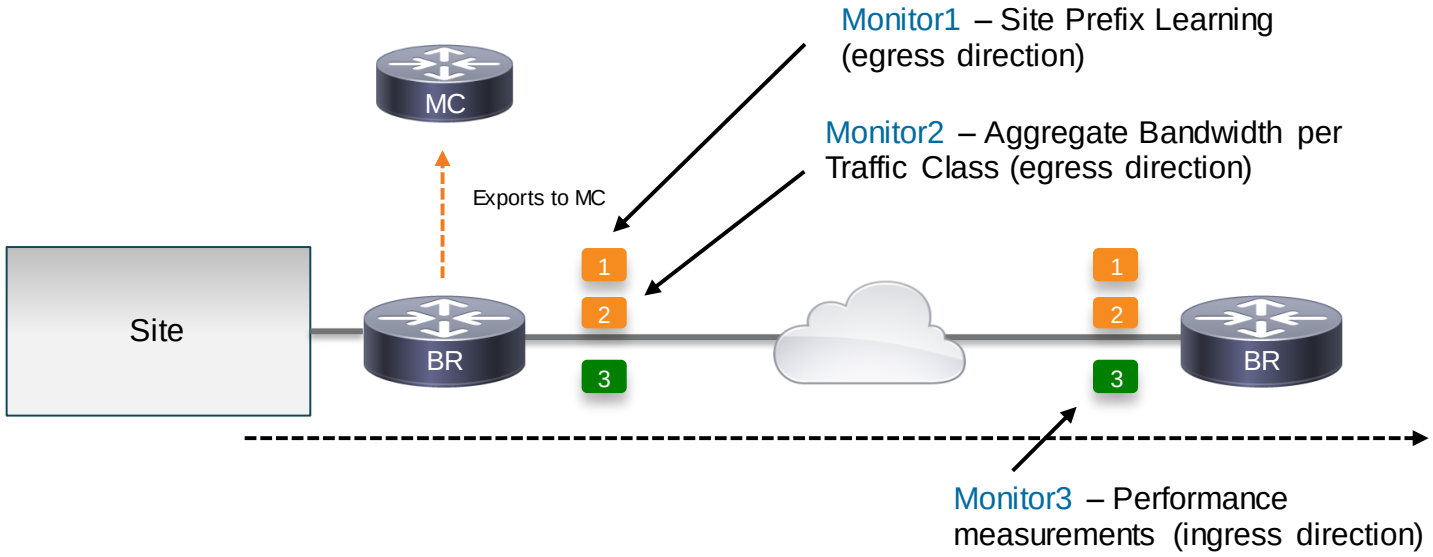
Cisco live!

Monitoring Details – The Life of a Packet

PfRv3 Monitoring

Based on Performance Monitor

- PfRv3 defines multiple Performance Monitor Instances (PMI)
- Applied on all External interfaces



Performance Monitor

Multiple Monitors with Unique Key Fields

Key Fields	Packet 1
ipv4 destination prefix	10.1.10.0
ipv4 destination mask	/24
Destination Site ID	10.2.10.10
Application Name	Skype
DSCP	AF41
Interface Output	Tunnel100

Non-Key Fields
Packets
Bytes
Timestamps

Performance Monitor Cache #1

Dest Prefix	Dest. Mask	Dest Site	App Name	DSCP	Output I/F	…	Pkts
10.1.10.0	/24	10.2.10.10	Skype	AF41	Tunnel100	…	1100

Key Fields	Packet 1
Source Prefix	10.8.0.0
Source Mask	/16
Input VRF	VRF1

Non-Key Fields
Packets
Bytes
Timestamps

Performance Monitor Cache #2

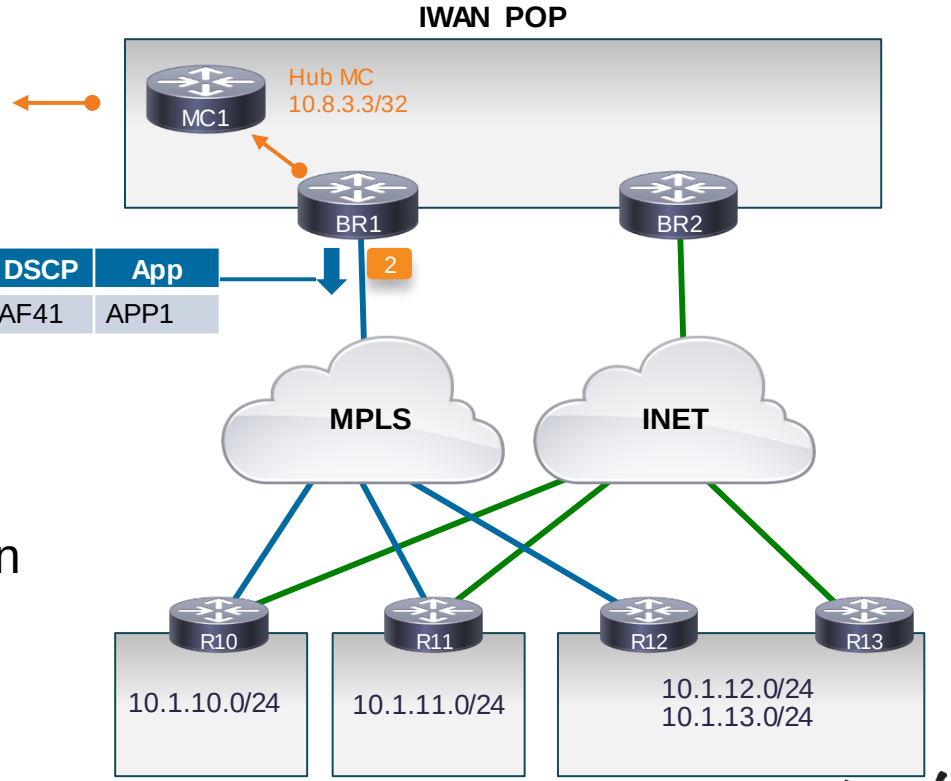
Source Prefix	Source Mask	Input VRF	…	Pkts
10.8.0.0	/16	VRF1	…	11000

Source Site – Egress Traffic

Collecting Traffic Class

MC1	Dst-Site-Pfx	App	DSCP	Dst-Site-Id	State	BW	BR	Exit
	10.1.10.0	APP1	AF41	?	UK	24	BR1	Tu10

Source	Destination	DSCP	App
10.8.1.200	10.1.10.200	AF41	APP1



- Traffic going outside a source site
  - Initially based on Routing Information
- Captured by a Performance Monitor on the external interface on egress
- BR reports to its local MC
- Monitor interval is 30 sec

Monitor2 Details

Aggregate Bandwidth Per TC

- Aggregate Bandwidth Per TC
- Bandwidth is measured egress direction.
- Using monitor #2
- Collect bandwidth per Traffic Class

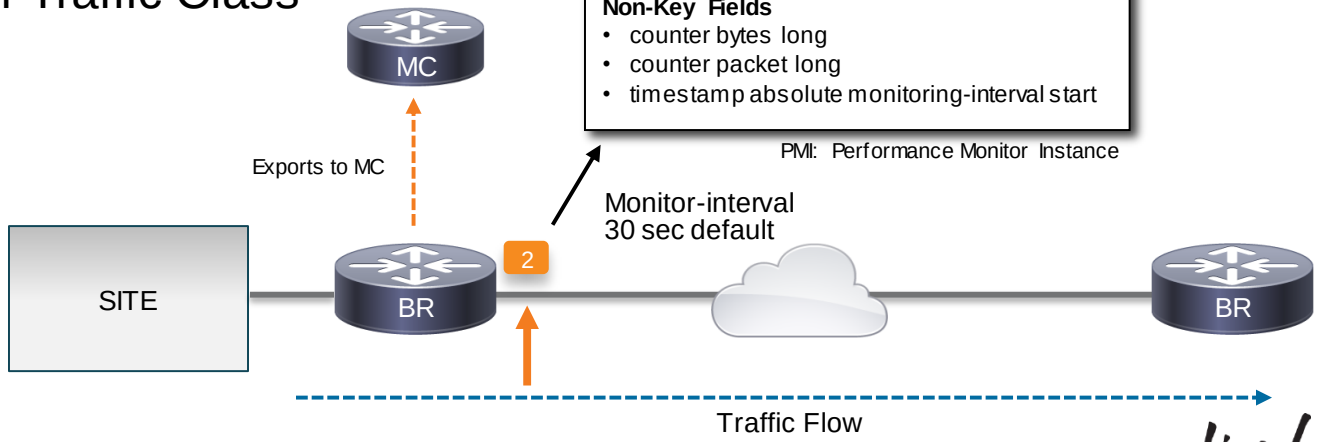
PMI: [Egress-Aggregate] - #2

Trigger NBAR: no/yes

Key Fields
- ipv4 destination prefix,
- ipv4 destination mask,
- pfr site destination prefix ipv4
- pfr site destination prefix mask ipv4
- [application id]
- ip dscp
- interface output

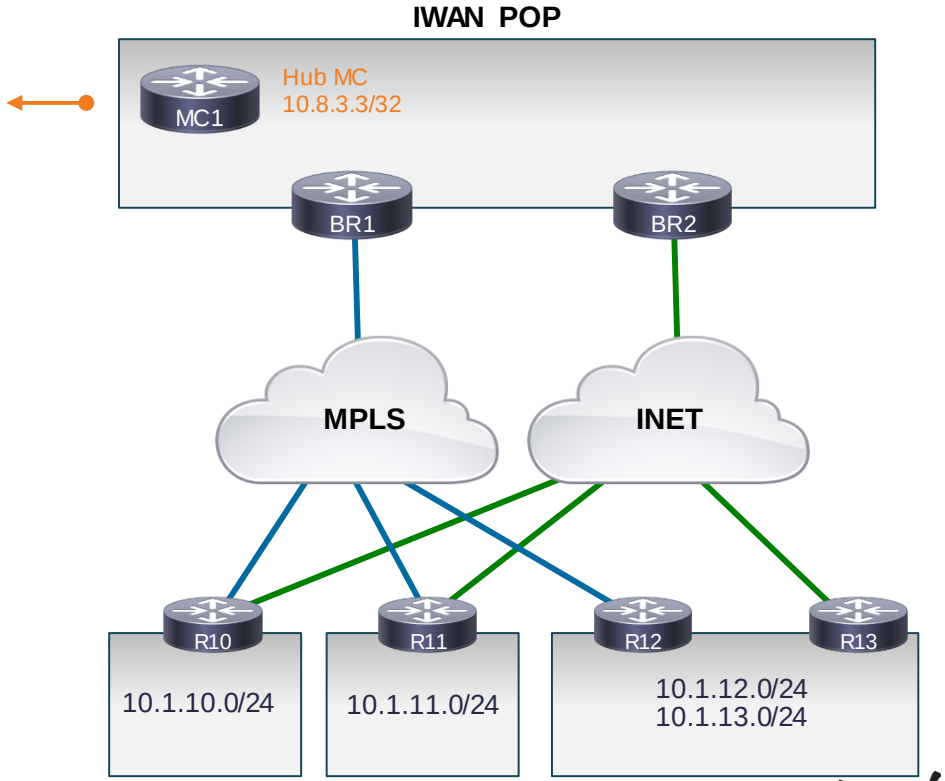
Non-Key Fields
- counter bytes long
- counter packet long
- timestamp absolute monitoring-interval start

PMI: Performance Monitor Instance



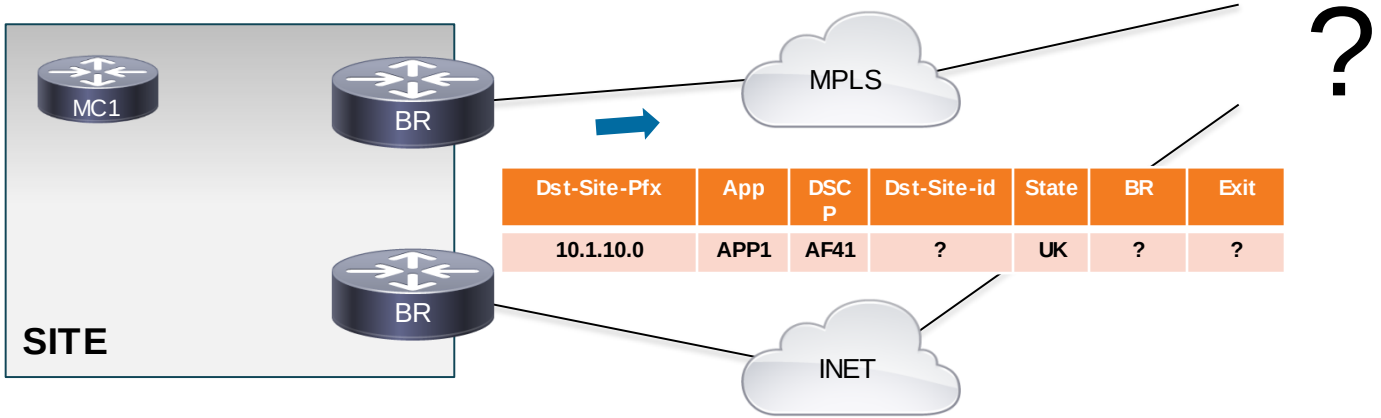
What is a Traffic Class?

Dst-Site-Pfx	App	DSCP	Dst-Site-id	State	BR	Exit
10.1.10.0	APP1	AF41	?	UK	?	?
10.1.10.0	N/A	EF	?	UK	?	?
10.1.10.0	N/A	AF31	?	UK	?	?
10.1.10.0	N/A	0	?	UK	?	?
10.1.11.0	N/A	EF	?	UK	?	?
10.1.11.0	N/A	AF31	?	UK	?	?
10.1.11.0	N/A	0	?	UK	?	?
10.1.12.0	N/A	0	?	UK	?	?
…						



- What is a Traffic Class (TC)?
  - Destination Site Prefix
  - DSCP value
  - Application Name
- Each Master Controller owns a TC Database

We Need The Destination Site ID – Why??

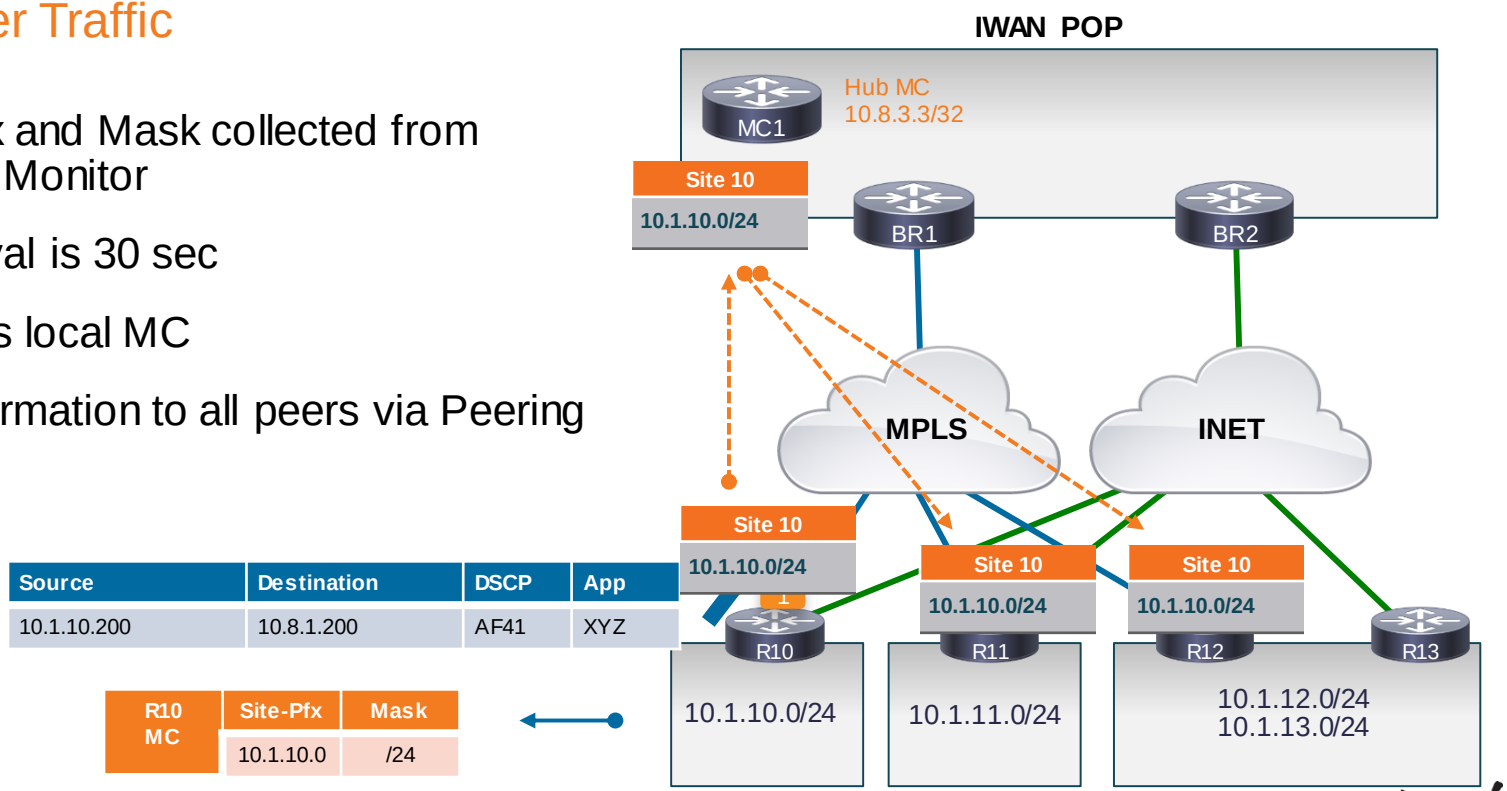


- Performance Measurement is done on the destination site
- Source site needs to get Performance Metrics from the destination site

Site Prefix Exchange – Dynamic

Based on User Traffic

- Source Prefix and Mask collected from Performance Monitor
- Monitor interval is 30 sec
- BR send to its local MC
- MC send information to all peers via Peering

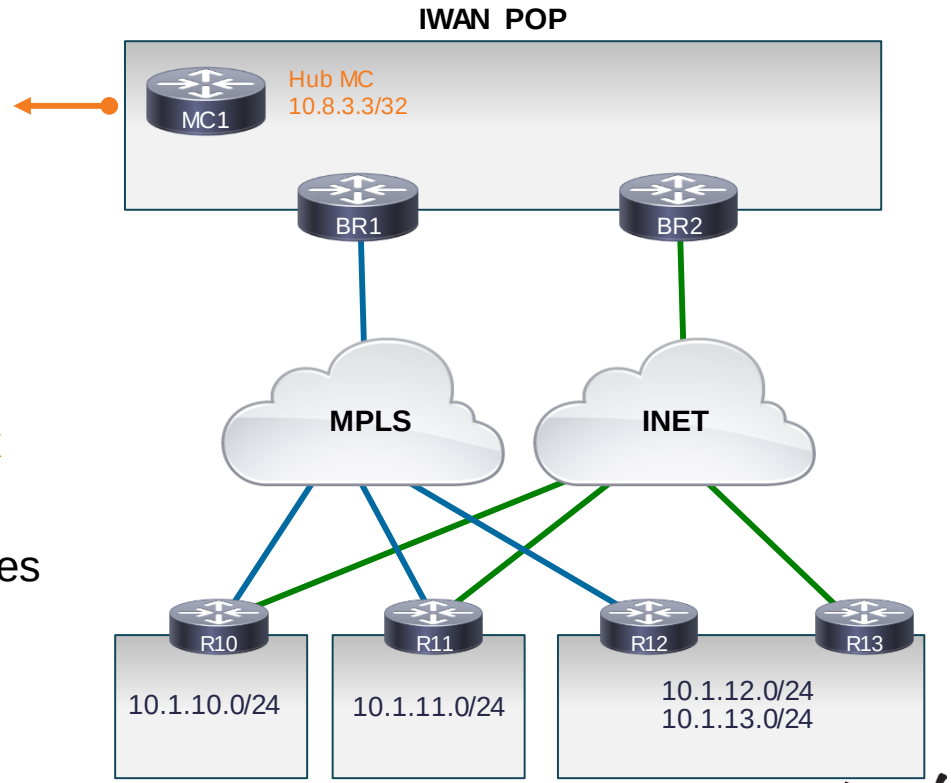


Site Prefix Exchange – Dynamic

Based on User Traffic

Site	Prefix List
Hub	10.8.0.0/16
R10	10.1.10.0/24
R11	10.1.11.0/24
R12	10.1.12.0/24
R12	10.1.13.0/24

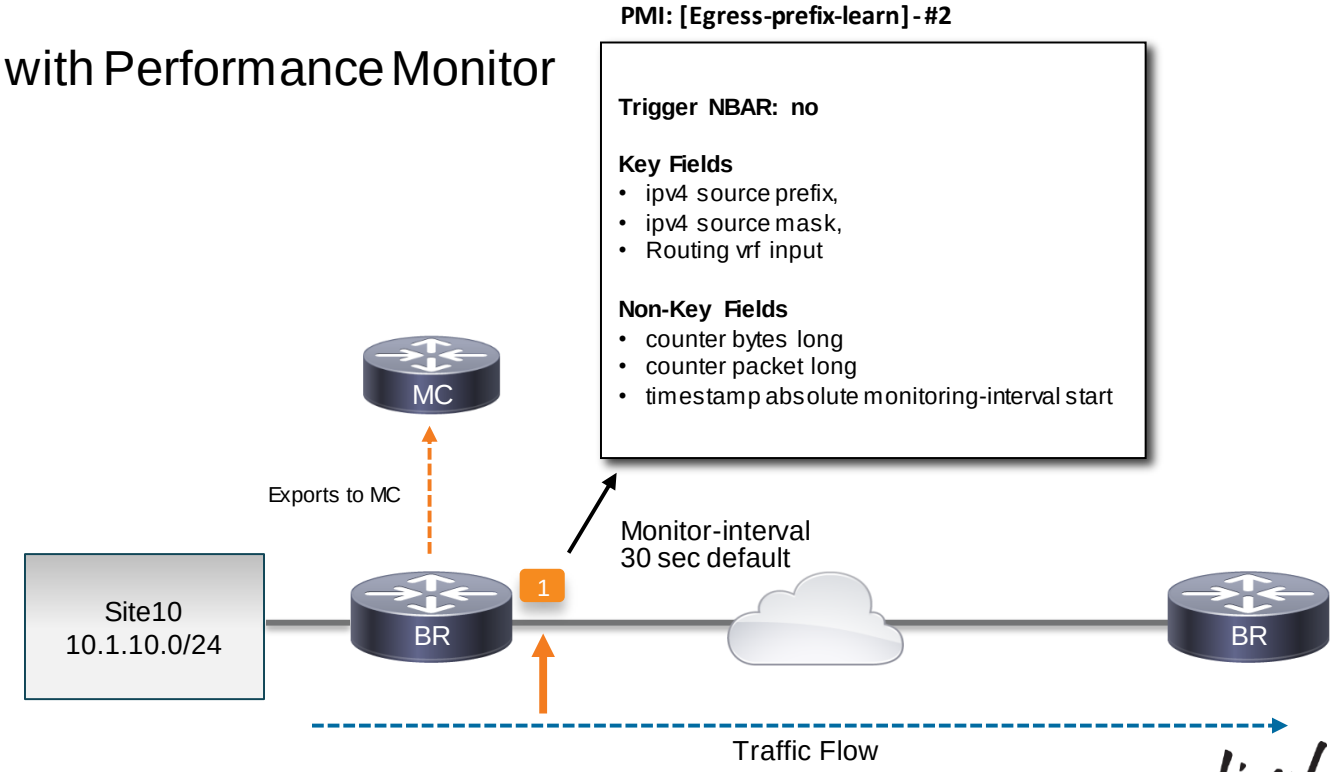
- Every MC in the domain owns a Site Prefix database
- Gives the mapping between site and prefixes



Monitor1 Details

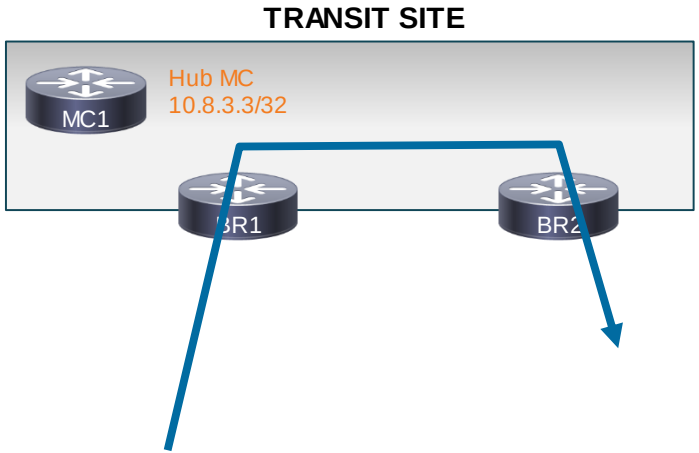
Site Prefix Learning

- Site Prefix collected with Performance Monitor
- Using monitor #1



Site Prefixes – Static Configuration

- This allows configuring site-prefix manually instead of learning.
- This configuration should be used at the site if the site is used for transit.
  - For example, Site A reaches Site B via Hub-Site, where Hub-Site is transit site. The configuration is used to prevent learning of Site A prefix as Hub-Site prefix when it is transiting from Hub.



Source	Destination	DSCP	App
10.1.10.200	10.1.11.200	AF41	AppXY

```
domain IWAN
 vrf default
  master hub
   source-interface Loopback0
   site-prefixes prefix-list DC1_PREFIX
!
ip prefix-list DC1_PREFIX seq 10 permit 10.8.0.0/16
!
```

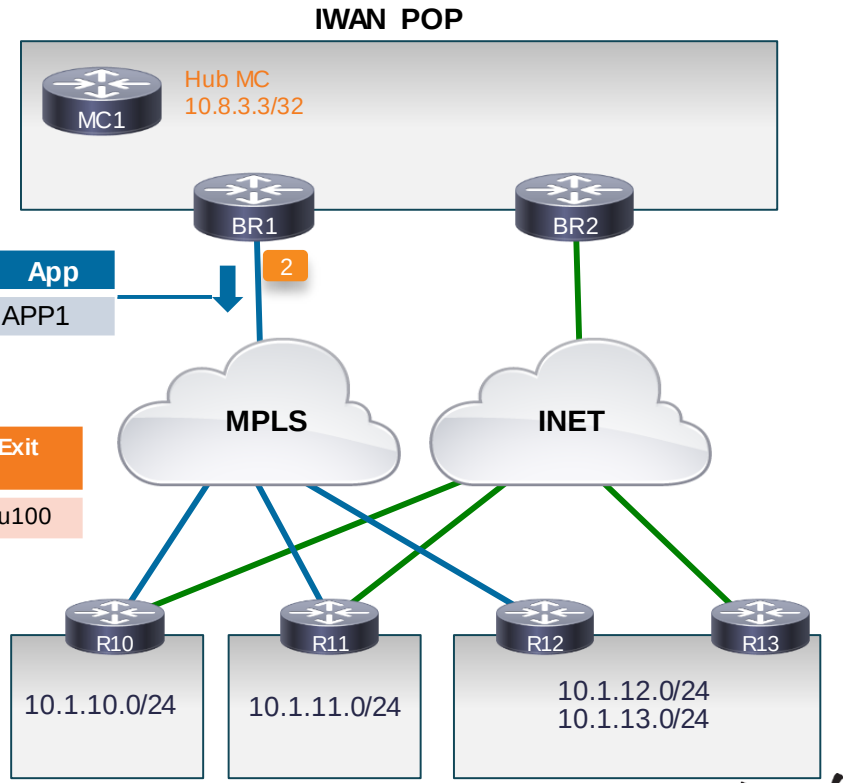
Source Site – Egress Traffic

Traffic Class Controlled

MC1	Site	Prefix List
	Hub	10.8.0.0/16
	R10	10.1.10.0/24
	R11	10.1.11.0/24
	R12	10.1.12.0/24
	R12	10.1.13.0/24

Source	Destination	DSCP	App
10.8.1.200	10.1.10.200	AF41	APP1

MC1	Dst-Site-Pfx	App	DSCP	Dst-Site-id	State	BW	BR	Exit
	10.1.10.0	APP1	AF41	**R10**	**CN**	24	BR1	Tu100

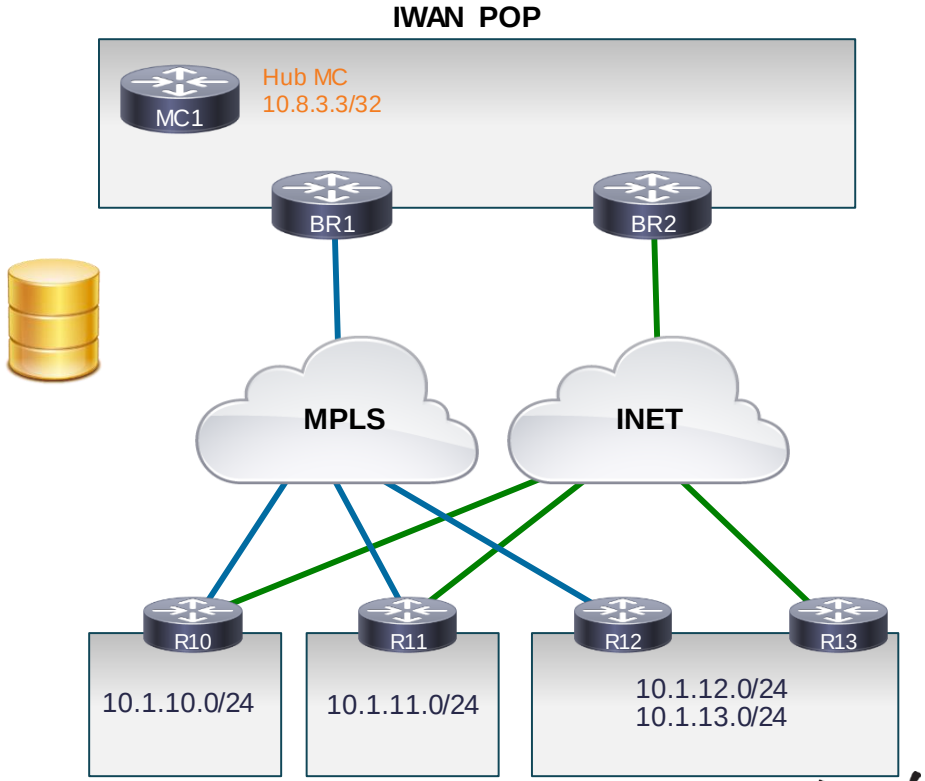


- Now the MC has the destination site information
- Traffic Class is controlled

Source Site – Traffic Class Database

Dst-Site-Pfx	Dst-Site-id	App	DSCP	State	BR	Exit
10.1.10.0	R10	APP1	AF41	CN	BR1	Tu100
10.1.10.0	R10	N/A	EF	CN	BR1	Tu100
10.1.10.0	R10	N/A	AF31	CN	BR1	Tu100
10.1.10.0	R10	N/A	0	CN	BR2	Tu200
10.1.11.0	R11	N/A	EF	CN	BR1	Tu100
10.1.11.0	R11	N/A	AF31	CN	BR1	Tu100
10.1.11.0	R11	N/A	0	CN	BR2	Tu200
10.1.12.0	R12	N/A	0	CN	BR2	Tu200

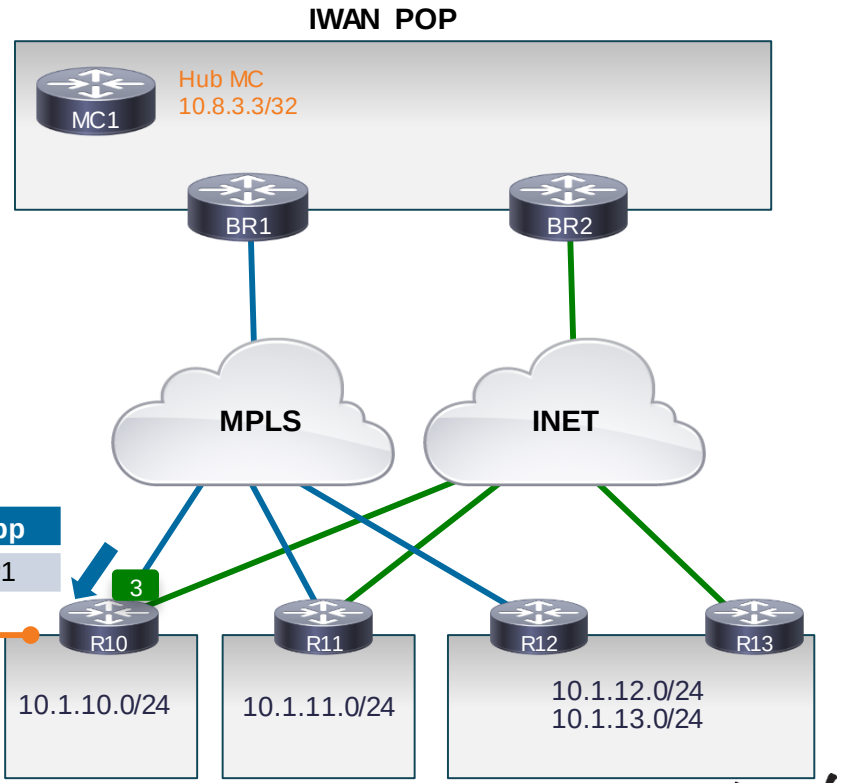
- Same process for all traffic to between all sites.
- Traffic Class database contains bandwidth, destination sites, BR and external path used



Destination Site – Ingress Traffic

Channel Performance

- Traffic flow captured on the destination site
- Performance Monitor collects Performance Metrics
- **Per Channel**
- Default Monitor interval is 30 sec



Source	Destination	DSCP	App
10.8.1.200	10.1.10.200	AF41	APP1

R10 MC	Channel	Dst-Site-id	Path	DSCP	BW	Delay	Jitter	Loss
	5	Hub	Tu1	AF41	24	51	2	1

What is a Channel?

Between Sites

- A Channel is a unique combination of:
  - Interface
  - Peer-Site id
  - DSCP
- Created
  - Based on real traffic observed on the BRs
  - Added every time there is a new DSCP or a new interface or a new site added to the prefix database.
  - Smart Probe is received
- On all exits (Present Channel, Backup Channel)

Monitor3 Details

Ingress Performance Monitor

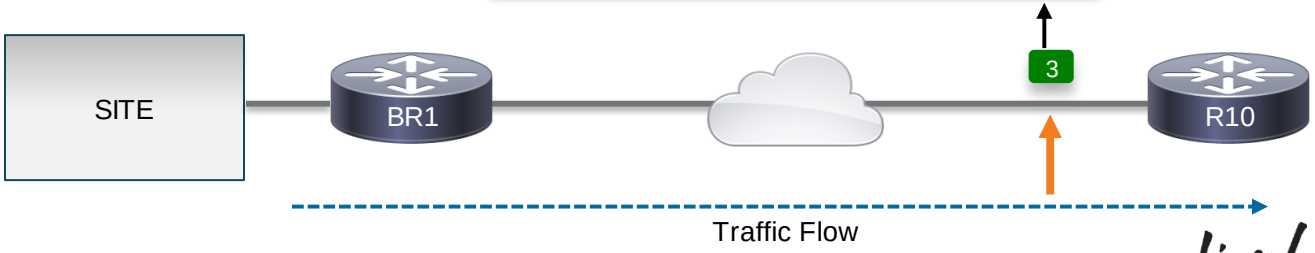
- Performance is measured ingress direction:
  - Actual Traffic
  - Smart Probes if no traffic
- Using monitor #3
- Monitors performance metrics per DSCP and per Site
- Export only when there is a performance issue (performance threshold crossed)

PMI [Ingress-per-DSCP] - #3

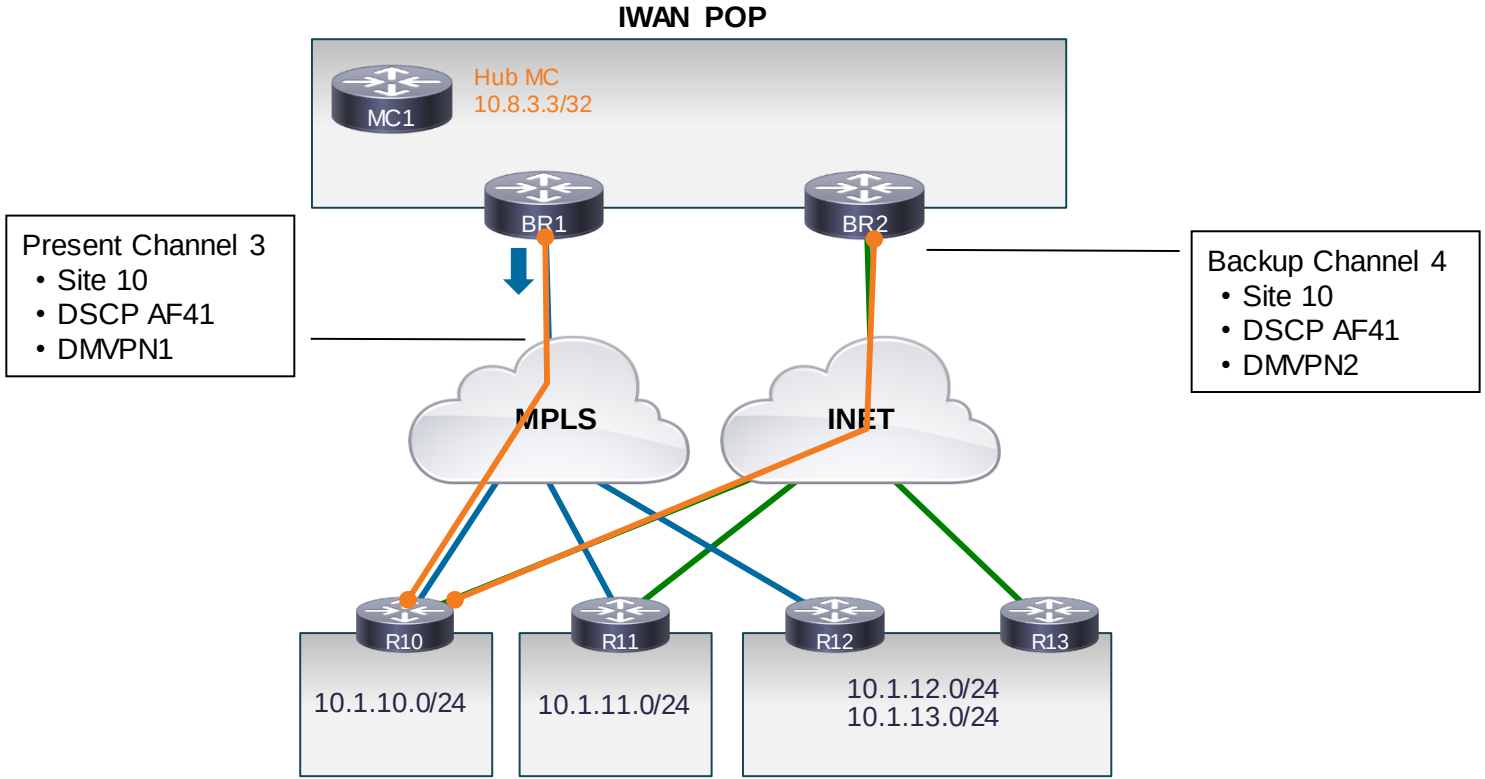
Key Fields
- pfr site source id ipv4
- pfr site destination id ipv4
- ip dscp
- Interface input
- policy performance-monitor classification hierarchy

Non-Key Fields
- 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

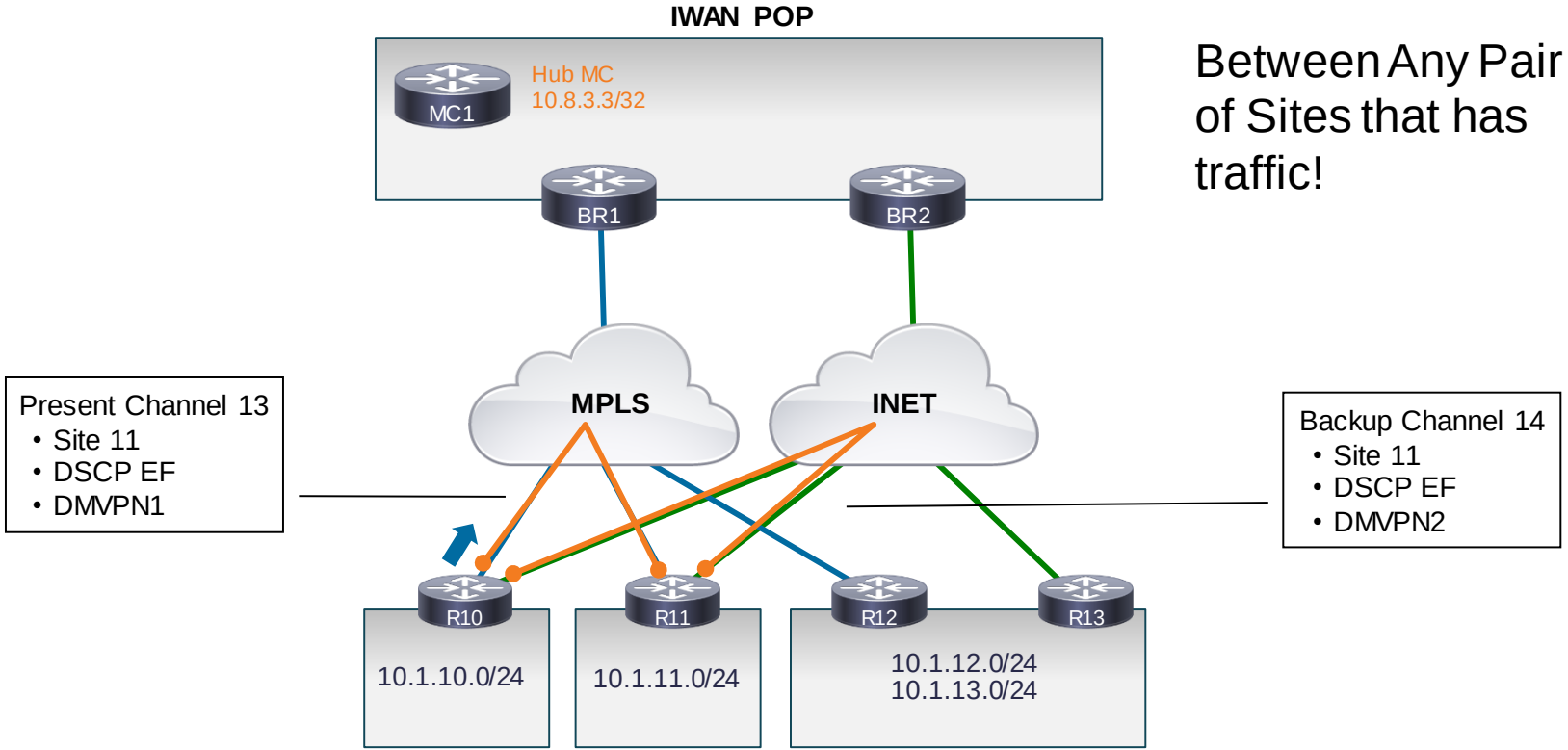
Monitor-interval
30 sec default



Channel Details



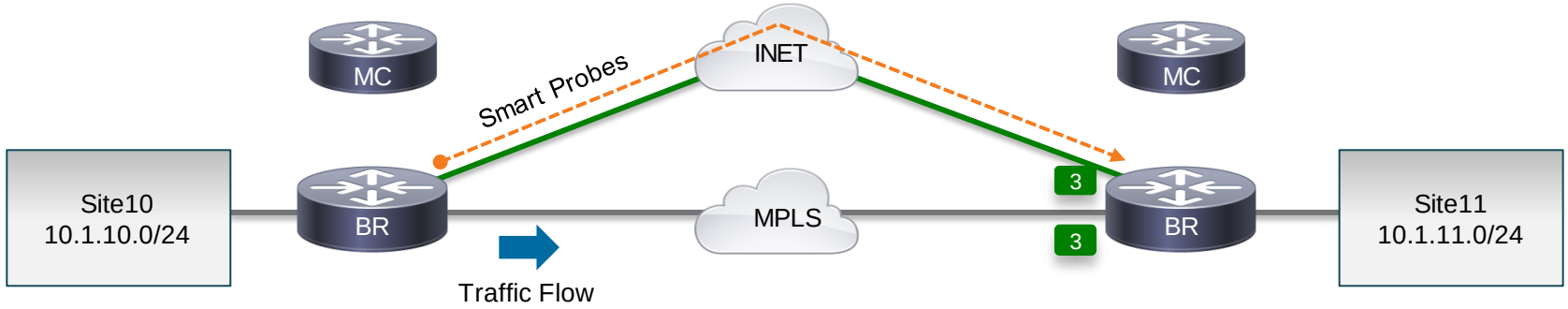
Channel Details



Between Any Pair of Sites that has traffic!

Smart Probing

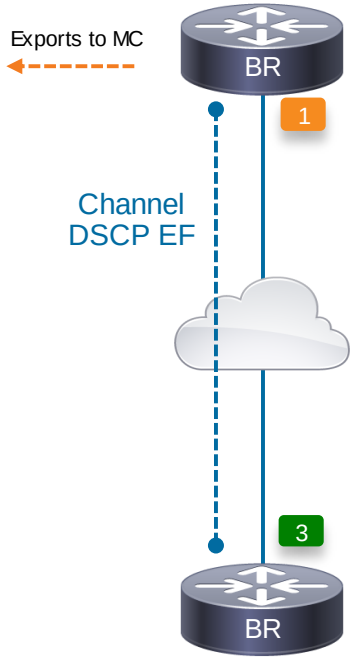
Help for Measurement Over Channels



- Without actual traffic
  - BR sends 10 probes spaced 20ms apart in the first 500ms and another similar 10 probes in the next 500ms, thus achieving 20pps for channels without traffic.
- With actual traffic
  - Lower frequency when real traffic is observed over the channel
  - Probes sent every 1/3 of [Monitor Interval], ie every 10 sec by default
- Measured by Unified Performance Monitoring just like other data traffic

Channel Unreachable

- PfRv3 considers a channel reachable as long as the site receives a PACKET on that channel
- A channel is declared unreachable in both direction if
  - There is NO traffic on the Channel, probes are our only way of detecting unreachability. So if no probe is received within 1 sec, we detect unreachability.
  - When there IS traffic on the channel, if we don't see any packet for more than a second on a channel we detect unreachability.
- A channel is put to reachable if following happens
  - Traffic is received from the remote side.
  - Unreachable TCA not received for two monitor intervals



Unreachable

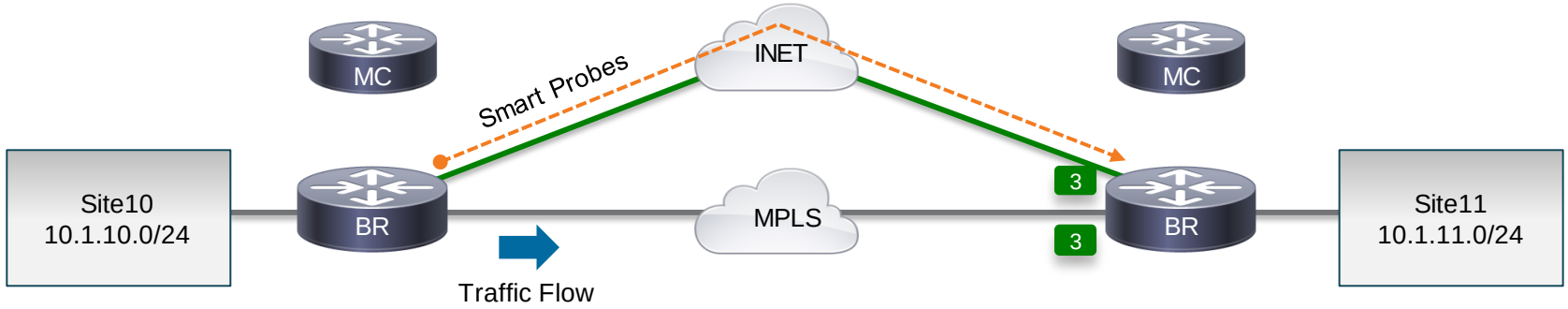
Channel State Examples

```
R84#sh domain IWAN border channels

 Channel id: 1
  Channel create time: 12:52:35 ago
  Site id : 255.255.255.255
  DSCP : default[0]
  Service provider : MPLS
  Number of Probes sent : 0
  Number of Probes received : 0
  Last Probe sent : 12:52:35 ago
  Last Probe received : - ago
  Channel state : Initiated and open
  Channel next_hop : 0.0.0.0
  RX Reachability : Initial State
  TX Reachability : Reachable
  Channel is sampling 0 flows
  Supports Zero-SLA: Yes
  Muted by Zero-SLA: No
  Probe freq with traffic : 1 in 10000 ms
```

```
R84#sh domain IWAN border channels

  Channel id: 3
  Channel create time: 12:50:55 ago
  Site id : 10.2.11.11
  DSCP : default[0]
  Service provider : MPLS
  Number of Probes sent : 843019
  Number of Probes received : 838980
  Last Probe sent : 00:00:00 ago
  Last Probe received : 00:00:00 ago
  Channel state : Initiated and open
  Channel next_hop : 10.0.100.11
  RX Reachability : Reachable
  TX Reachability : Reachable
  Channel is sampling 0 flows
  Supports Zero-SLA: Yes
  Muted by Zero-SLA: No
  Probe freq with traffic : 1 in 10000 ms
```


Cisco live!

Smart Probing – Zero SLA Support



- No SLA on the secondary path, but still probing all channels (DSCPs)
  - 10 DSCP => 10 Smart Probes over the secondary path
- Waste of bandwidth, especially for metered interfaces (4G/LTE)

Zero-SLA

Principles

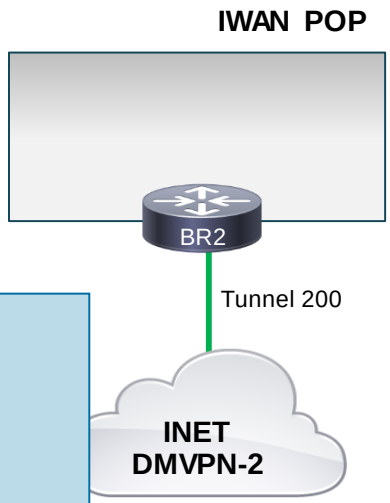
- Zero-sla added on the WAN interface path configuration option.
- PfR will only probe the default channel (DSCP 0).
  - It will mute all other smart-probes besides the default channel.
  - The default channel runs as DSCP 0, TCA and ODE are DSCP CS6.
  - Extrapolate metrics on this to all other DSCPs on this channel
- Site Capability Exchange:
  - Site-capability exchange: allow for backwards compatibility and coexistence with legacy sites until they are upgraded.
  - The site-capability is fully extensible so that additional domain configuration features can be added, not just PfRv3 capabilities.

Zero SLA Configuration

```
interface Tunnel200
 description --- INET ---
 domain IWAN path INET zero-sla
!
```

```
R83#sh domain IWAN master site-capability
 Device Capability

 ------------------------------------------------------------
|       Capability          |     Major     |     Minor      |
 ------------------------------------------------------------
|     Domain                |     2         |      0         |
 ------------------------------------------------------------
|     Zero-SLA              |     1         |      0         |
 ------------------------------------------------------------
Site id  :10.2.10.10
```

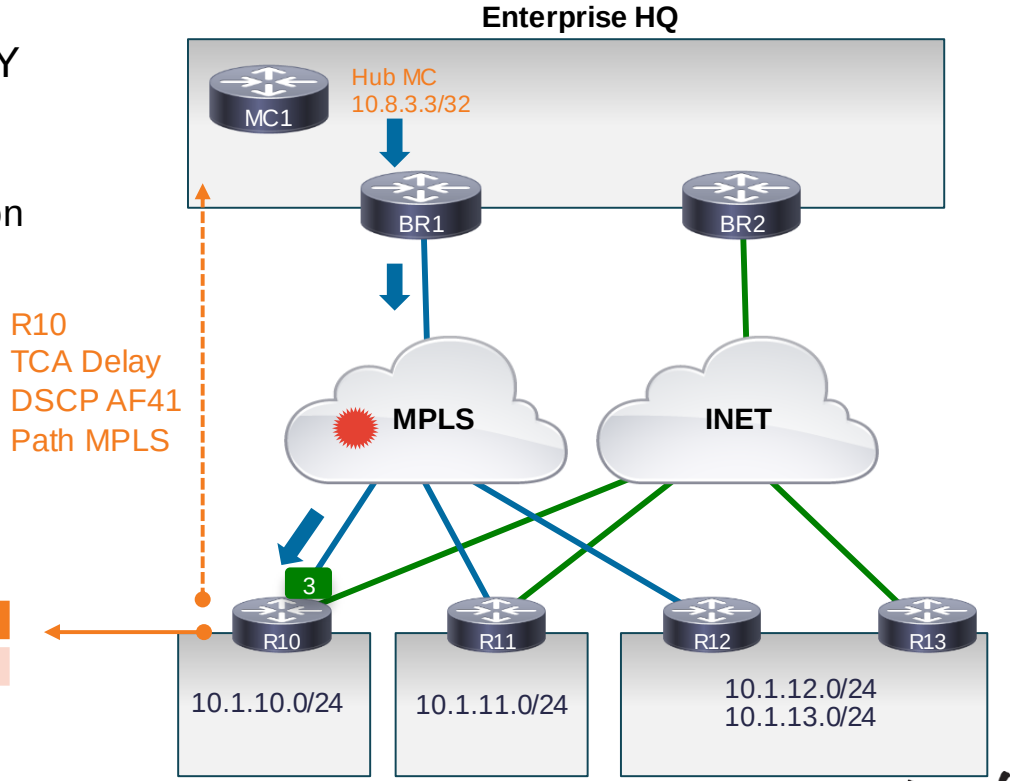
```
Borders:
   IP address: 10.8.4.4
   Version: 2
   Connection status: CONNECTED (Last Updated 1d00h ago )
   Interfaces configured:
     Name: Tunnel100 | type: external | Service Provider: MPLS | Status: UP | Zero-SLA: NO
         Number of default Channels: 0

   Tunnel if: Tunnel0

   IP address: 10.8.5.5
   Version: 2
   Connection status: CONNECTED (Last Updated 00:04:59 ago )
   Interfaces configured:
     Name: Tunnel200 | type: external | Service Provider: INET | Status: UP | Zero-SLA: YES
         Number of default Channels: 0

   Tunnel if: Tunnel0
```



Path Enforcement – Route Override

Performance Violation

- Performance notification exported ONLY when there is a violation on a specific channel
  - Generated from ingress monitor attached on BRs to the source site MC
  - Based on Monitor interval (30 sec default, configurable)
  - Via all available external interfaces.

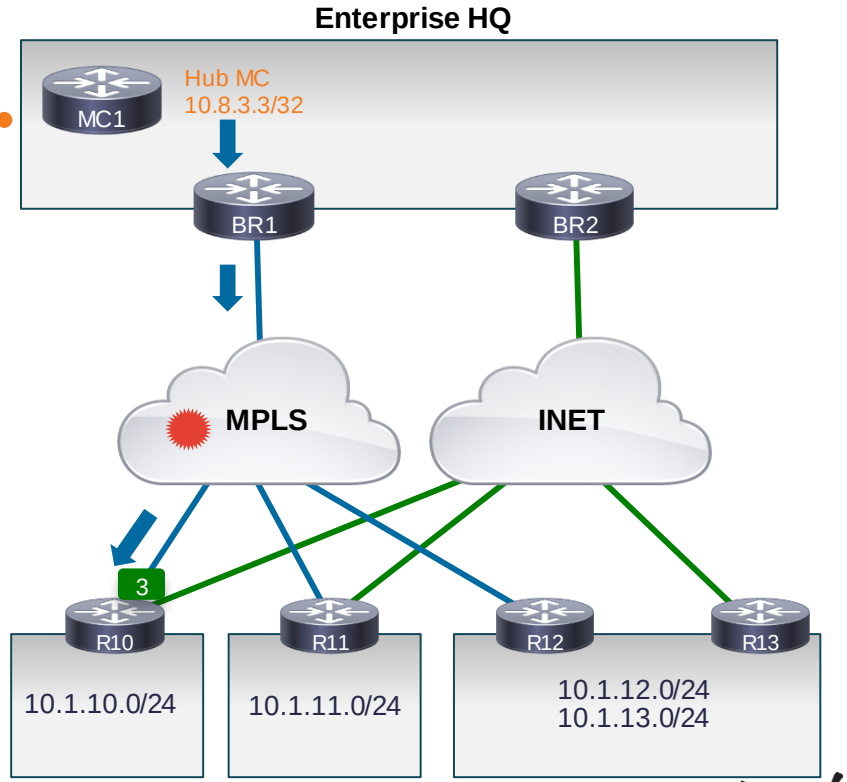


R10	Channel	Dst-Site-id	DSCP	Path	BW	Delay	Jitter	Loss
	5	Hub	AF41	Tu1	24	250	2	1

Performance Violation – Detected on Dst Site

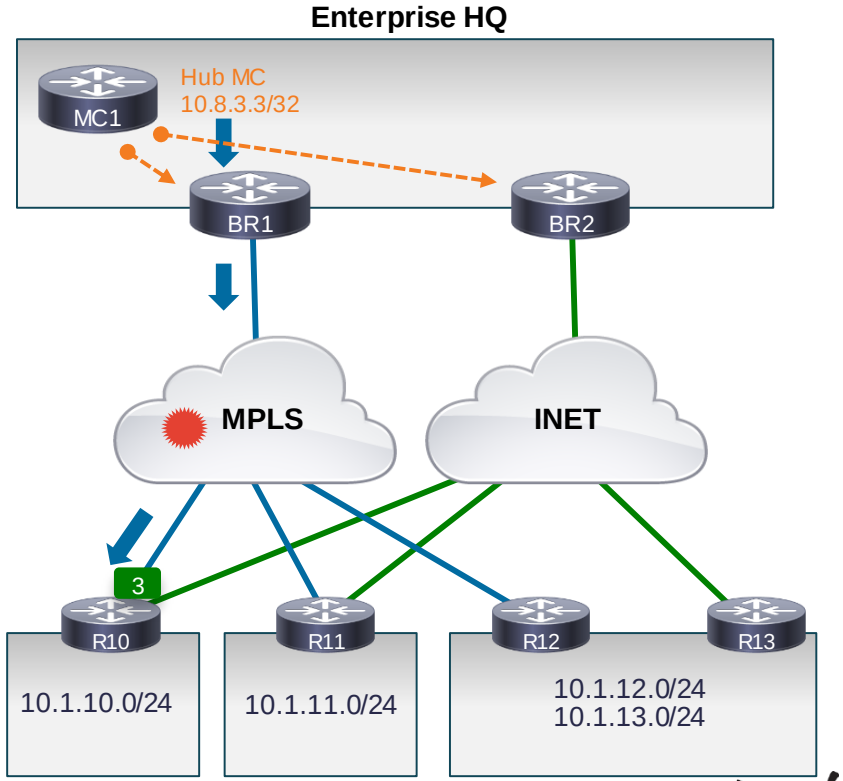
Dst-Site-Pfx	Dst-Site-id	App	DSCP	State	BR	Exit
10.1.10.0	R10	APP1	AF41	CN	BR1	Tu1
10.1.10.0	R10	N/A	AF41	CN	BR1	Tu1
10.1.10.0	R10	N/A	AF31	CN	BR1	Tu1
10.1.10.0	R10	N/A	0	CN	BR2	Tu2
10.1.11.0	R11	N/A	EF	CN	BR1	Tu1
10.1.11.0	R11	N/A	AF31	CN	BR1	Tu1
10.1.11.0	R11	N/A	0	CN	BR2	Tu2
10.1.12.0	R12	N/A	0	CN	BR2	Tu2

R10
TCA Delay
DSCP EF
Path MPLS



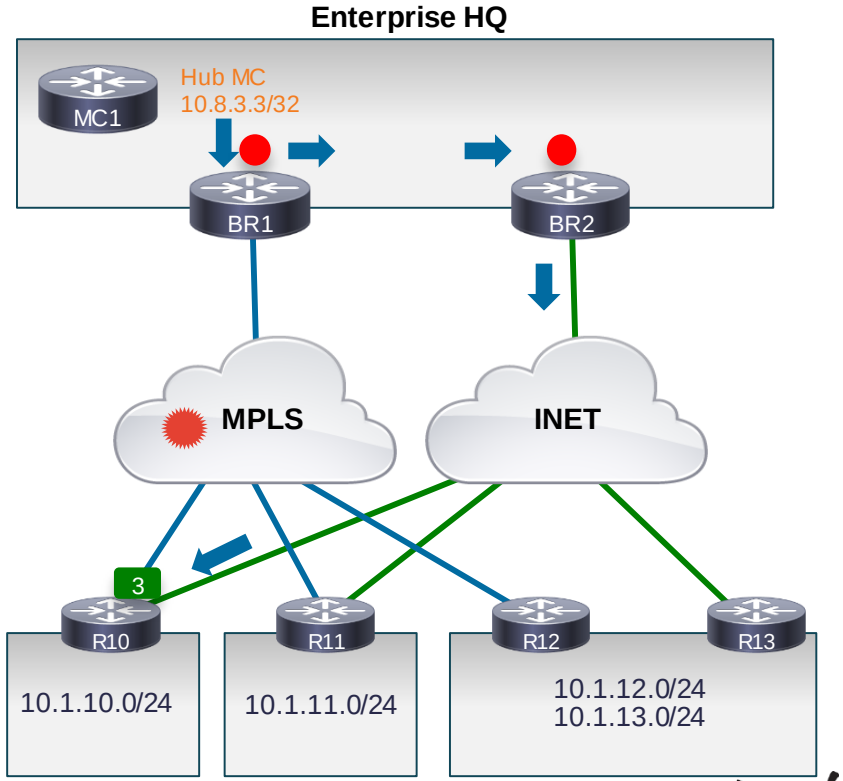
Policy Decision – Reroute TC

- MC computes a new path for each impacted TC
- MC tells the BRs to enforce the new path



Reroute TC – Path Enforcement

- Dataplane forwarding
- Activated on all but external interfaces
- Lookup per packet - output-if/next hop retrieved
  - Packet Forwarded
  - If no entry – Uses FIB entry
- TC flows redirected to the new path over the auto mGRE tunnels between the BRs
- No change in the routing table

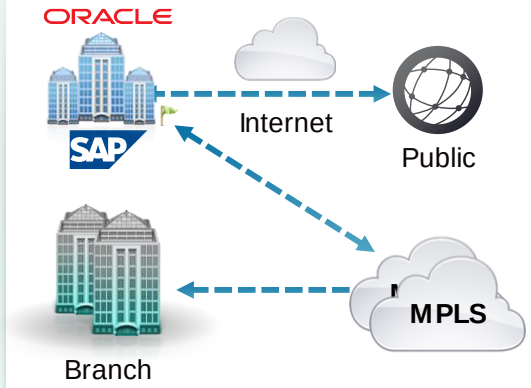


Enterprise Deployment

Cisco live!

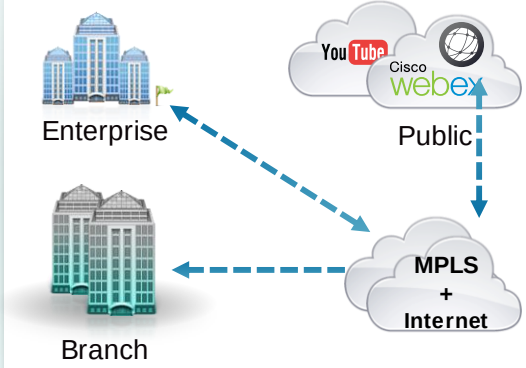
Intelligent WAN Deployment Models

Dual MPLS



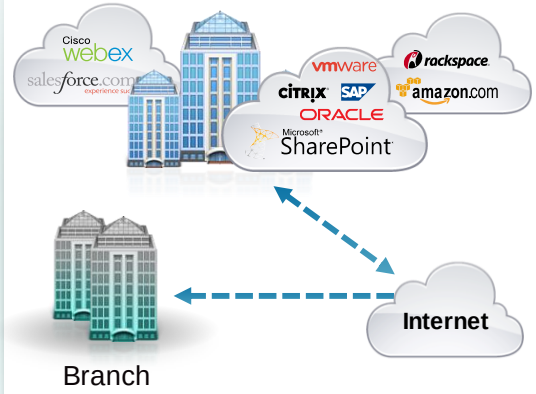
- Highest SLA guarantees
- Tightly coupled to SP
- Expensive

Hybrid



- More BW for key applications
- Balanced SLA guarantees
- Moderately priced

Dual Internet



- Best price/performance
- Most SP flexibility
- Enterprise responsible for SLAs

Consistent VPN Overlay Enables Security Across Transition

Hybrid WAN Designs

Traditional and IWAN

Active/Standby WAN Paths

Primary With Backup

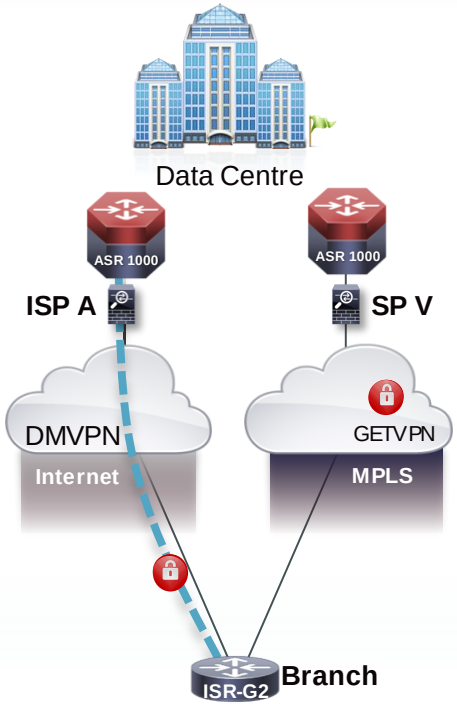
Two Ipsec Technologies

GETVPN/MPLS
DMVPN/Internet

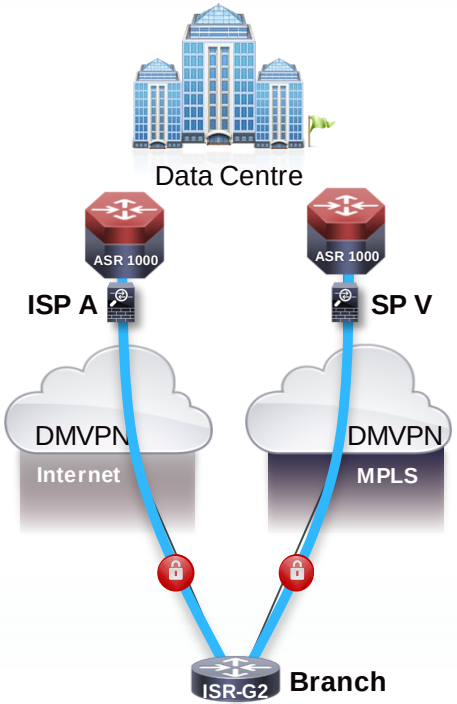
Two WAN Routing Domains

MPLS: eBGP or Static
Internet: iBGP, EIGRP or OSPF
Route Redistribution
Route Filtering Loop Prevention

TRADITIONAL HYBRID



IWAN HYBRID



Active/Active WAN Paths

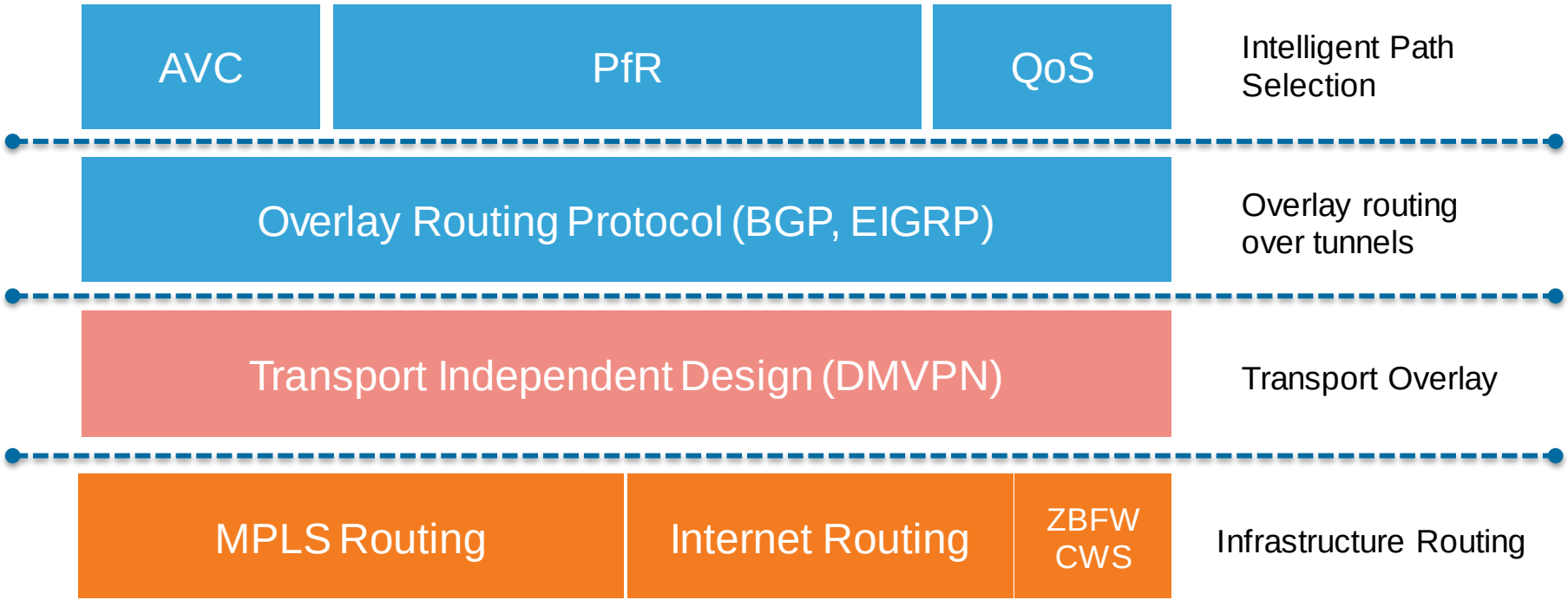
One IPsec Overlay

DMVPN

One WAN Routing Domain

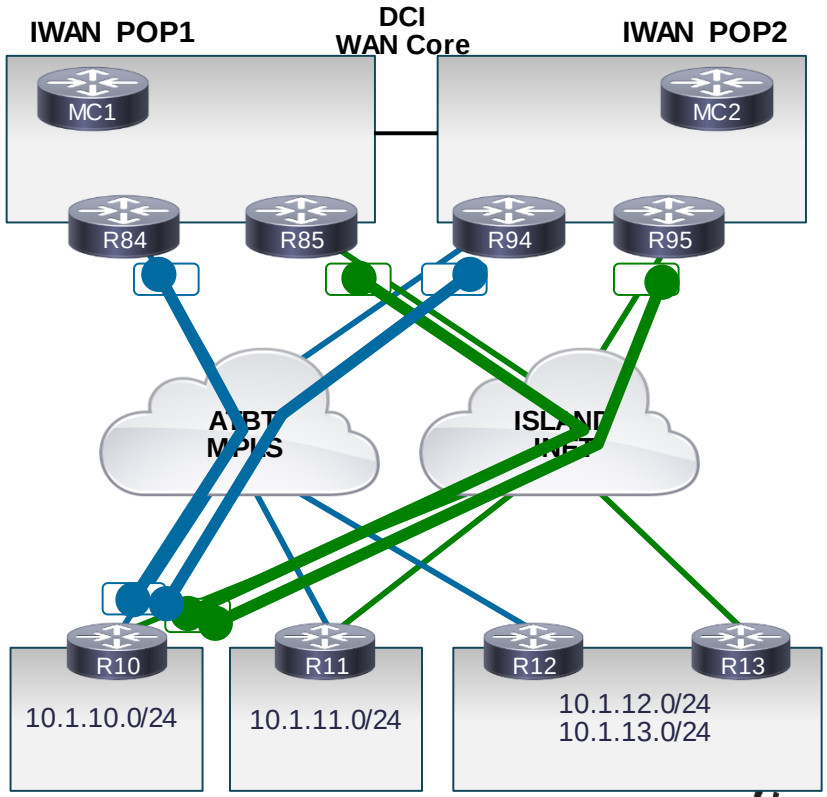
iBGP, EIGRP, or OSPF

IWAN Layers



IWAN Deployment – DMVPN

- IWAN Prescriptive Design – Transport Independent Design based on DMVPN
  - Branch spoke sites establish an IPsec tunnel to and register with the hub site
  - Data traffic flows over the DMVPN tunnels
  - WAN interface IP address used for the tunnel source address (in a Front VRF)
  - One tunnel per user VRF
- Over the Top Routing
  - BGP or EIGRP are typically used for scalability
  - IP routing exchanges prefix information for each site
- Per-tunnel QOS is applied to prevent hub site oversubscription to spoke sites

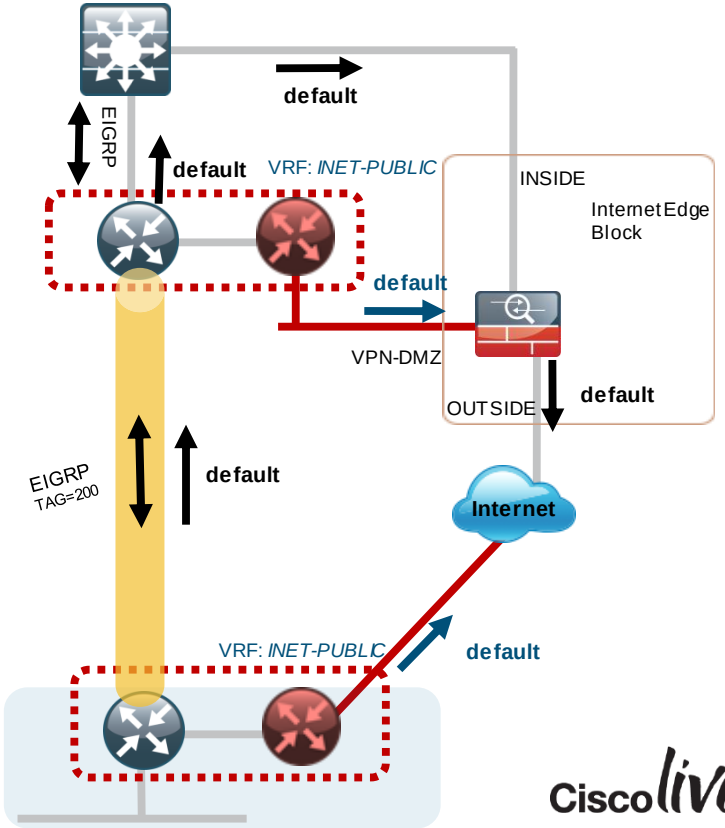


http://docwiki.cisco.com/wiki/PfR3:Solutions:IWAN

Best Practice: VRF-Aware DMVPN

Keeping the Default Routes in Separate VRFs with Front Door VRF

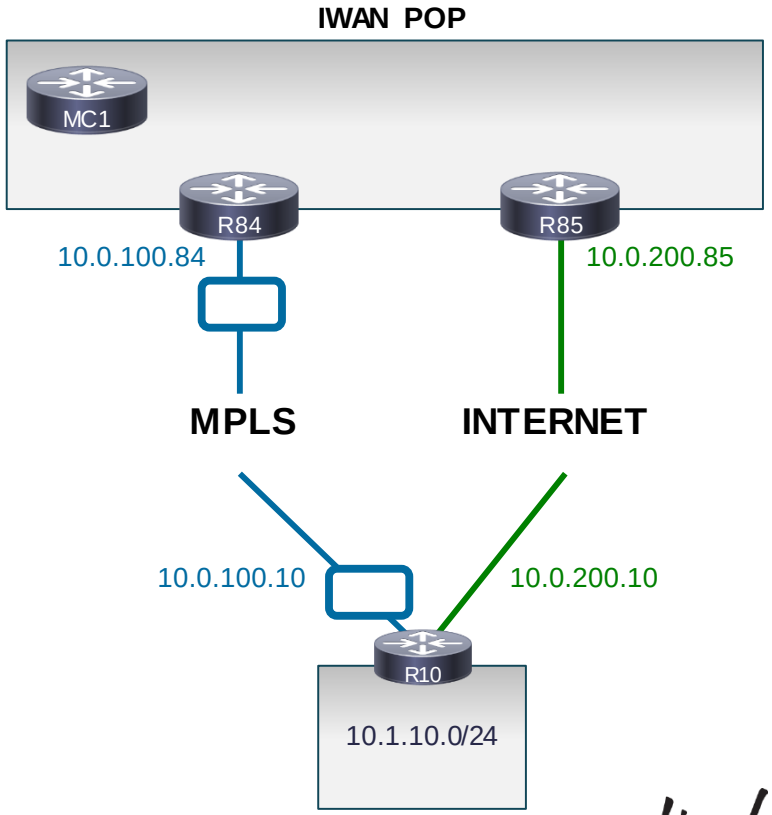
- Enable F-VRF DMVPN on the Spokes
- Allow the ISP learned Default Route in the VRF INET-PUBLIC and use for tunnel establishment
- Global VRF contains Default Route learned via tunnel. User data traffic follows Tunnel to INSIDE interface on firewall
- Allows for consistent implementation of corporate security policy for all users



DMVPN Configuration – F-VRF

```
vrf definition IWAN-TRANSPORT-1
 !
 address-family ipv4
 exit-address-family
!
```

Front-door VRF definition for MPLS Transport



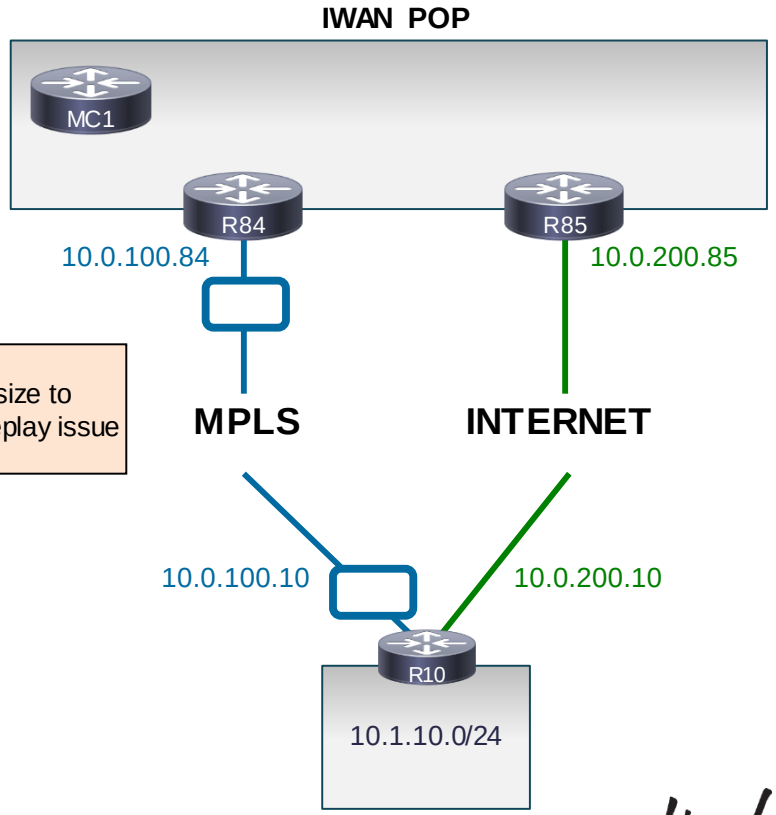
DMVPN Configuration – IPSec

```
!
! <removed IKEv2 proposal, will use smart default)
!
!
crypto ikev2 keyring DMVPN-KEYRING-1
 peer ANY
  address 0.0.0.0 0.0.0.0
  pre-shared-key c1sco123
 !
!
crypto ikev2 profile FVRF-IKEv2-IWAN-TRANSPORT-1
 match fvrf IWAN-TRANSPORT-1
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local DMVPN-KEYRING-1
!
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-PROFILE-1
 set transform-set AES256/SHA/TRANSPORT
 set ikev2-profile FVRF-IKEv2-IWAN-TRANSPORT-1
```

Maximise window size to eliminate future anti-replay issue

```
crypto ikev2 dpd 40 5 on-demand
```

! **Set DPD timers for Branch Configs ONLY!**



DMVPN Hub Configuration – Interfaces & Routing

MPLS TRANSPORT – R84

```
interface GigabitEthernet0/0/3
 description MPLS-TRANSPORT
 vrf forwarding IWAN-TRANSPORT-1
 ip address 172.16.84.4 255.255.255.0
!
interface Tunnel100
 bandwidth 1000
 ip address 10.0.100.84 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 100
 ip nhrp holdtime 600
 ip nhrp redirect
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/0/3
 tunnel mode gre multipoint
 tunnel key 101
 tunnel vrf IWAN-TRANSPORT-1
 tunnel protection ipsec profile DMVPN-PROFILE-1
!
ip route vrf IWAN-TRANSPORT-1 0.0.0.0 0.0.0.0 172.16.84.8
```

Put Transport Interface into MPLS Front-door VRF

Instantiate DMVPN Tunnel

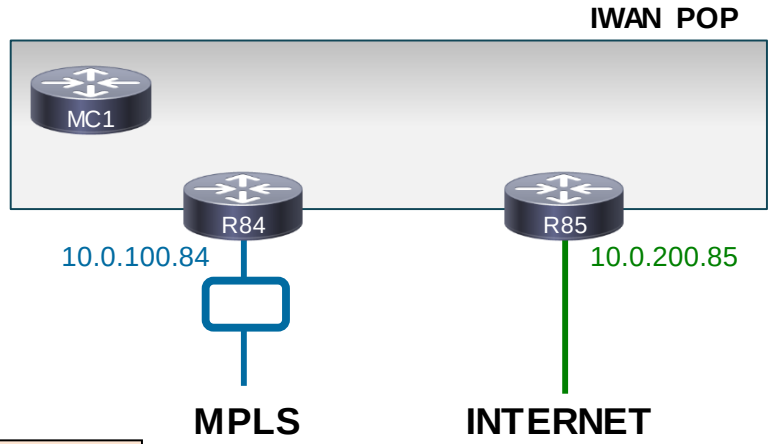
DMVPN Network ID: MPLS

Set DMVPN Ph3

Map to Physical Interface

Tunnel endpoint is in Front-door VRF

Default route for Tunnel endpoints



DMVPN Spoke Configuration – Interfaces & Routing

```
!
Interface GigabitEthernet0/1
 vrf forwarding IWAN-TRANSPORT-1
 ip address 10.0.100.10 255.255.255.0
!
interface Tunnel100
 ip address 10.0.100.10 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip pim dr-priority 0
 ip pim sparse-mode
 ip nhrp authentication cisco123
 ip nhrp network-id 100
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.100.84 nbma 172.16.84.4 multicast
 ip nhrp nhs 10.0.100.94 nbma 172.16.94.4 multicast
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 if-state nhrp
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel key 101
 tunnel vrf IWAN-TRANSPORT-1
 tunnel protection ipsec profile DMVPN-PROFILE-1
!
ip route vrf IWAN-TRANSPORT-1 0.0.0.0 0.0.0.0 172.16.101.8
```

Put Transport Interface into MPLS Front-door VRF

Instantiate DMVPN Tunnel

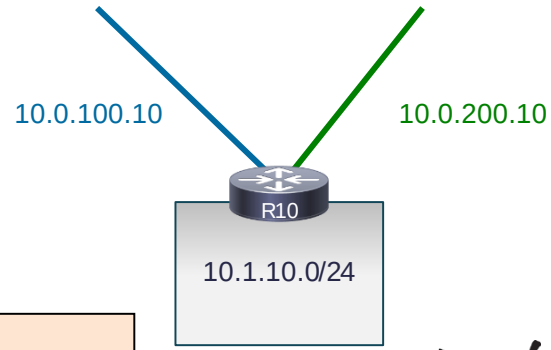
DMVPN Network ID: MPLS

Multiple DMVPN Hub for Resiliency

Set DMVPN Ph3

Tunnel endpoint is in Front-door VRF

Default route for Tunnel endpoints



IWAN Routing Protocols

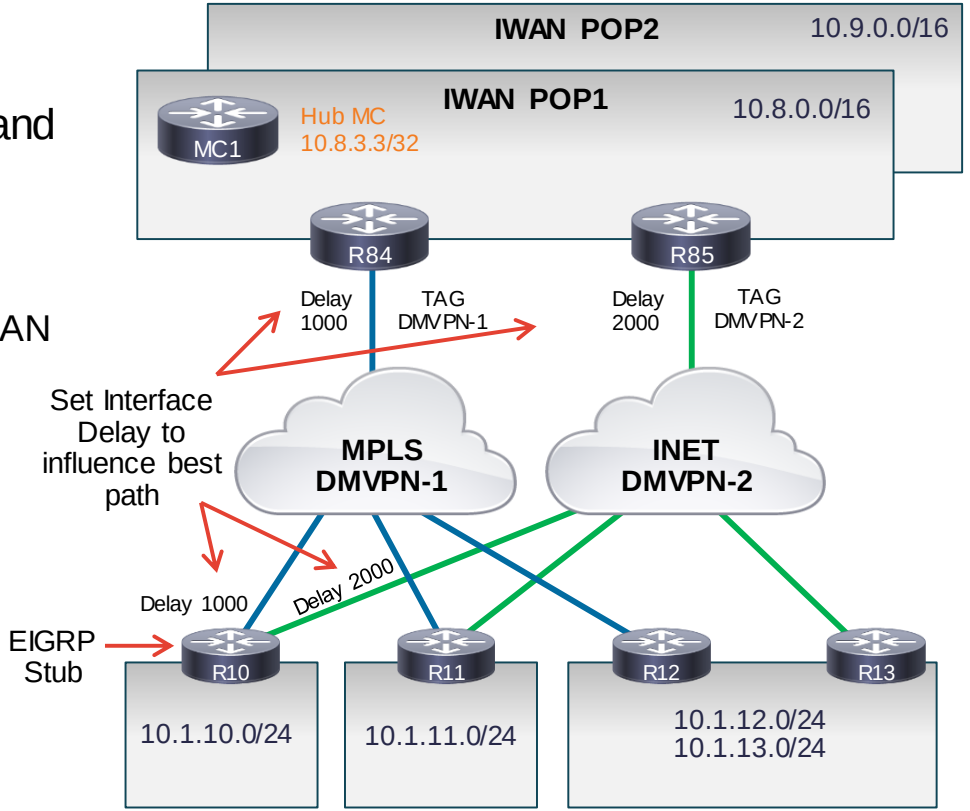
Which protocol should I use?

- IWAN Profiles are based upon BGP and EIGRP for scalability and optimal Intelligent Path Control
- Scalability:
  - BGP (Path Vector) and EIGRP (Advanced Distance Vector) provide best scale over large hub-and-spoke topologies like DMVPN
  - OSPF (Link State) maintains a lot of network state which cannot be subdivided easily in large DMVPN networks
- Intelligent Path Control:
  - PfR can be used with any routing protocols by relying on the routing table (RIB).
    - Requires all valid WAN paths be ECMP so that each valid path is in the RIB.
  - For BGP and EIGRP, PfR can look into protocol's topology information to determine both best paths and secondary paths thus, ECMP is not required.

EIGRP IWAN Design Overview

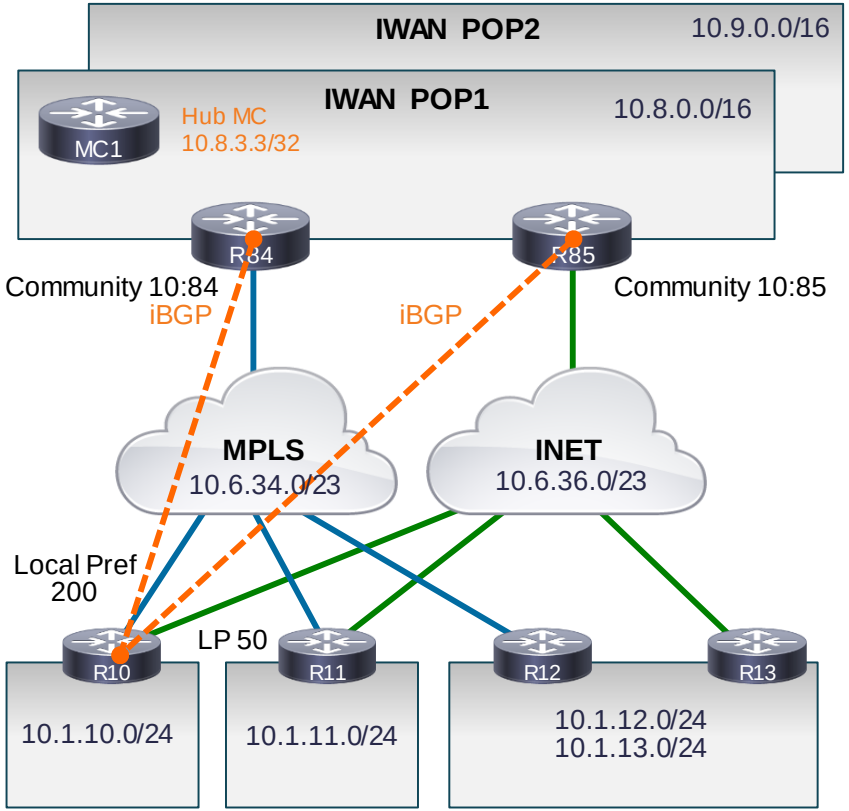
Principles

- Single EIGRP process for Branch, WAN and POP/hub sites
- Extend Hello/Hold timers for WAN
- Adjust tunnel interface "delay" to ensure WAN path preference
  - MPLS primary, INET secondary
- Hubs
  - Route tag filtering to prevent routing loops across DMVPNs
  - Branch prefix summary route for spoke-to-spoke tunnels
- Spokes
  - EIGRP Stub for scalability



IWAN Deployment – BGP

- A single iBGP routing domain is used
- Extend Hello/Hold timers for WAN
- Hub:
  - DMVPN hub routers function as BGP route-reflectors for the spokes
  - BGP dynamic peer feature configured on the route-reflectors
  - Summary route to spokes
  - Set Community for site local prefixes
- Spokes:
  - peer to a redundant pair of route-reflectors in each DMVPN cloud
  - Inbound route-map to set local-preference based on community
  - Ensure that preferred path is MPLS



PfRv3 and Parent Routes

- Make sure that all Border Routers have a route over each external path to the destination sites
  - PfR will NOT be able to effectively control traffic otherwise.
- PfRv3 always checks for a parent route before being able to control a Traffic Class. Parent route check is done as follows:
  - Check to see if there is an NHRP shortcut route
  - If not – Check in the order of BGP, EIGRP, Static and RIB
  - If at any point, an NHRP short cut route appears, PfRv3 would pick that up and relinquish using the parent route from one of the routing protocols.
- PfR3 currently supports only one next-hop per multipoint interface. Routing has to be done such that only one next-hop per destination prefix is in the routing table per DMVPN tunnel interface.

Transit Site – Hub MC

MC1

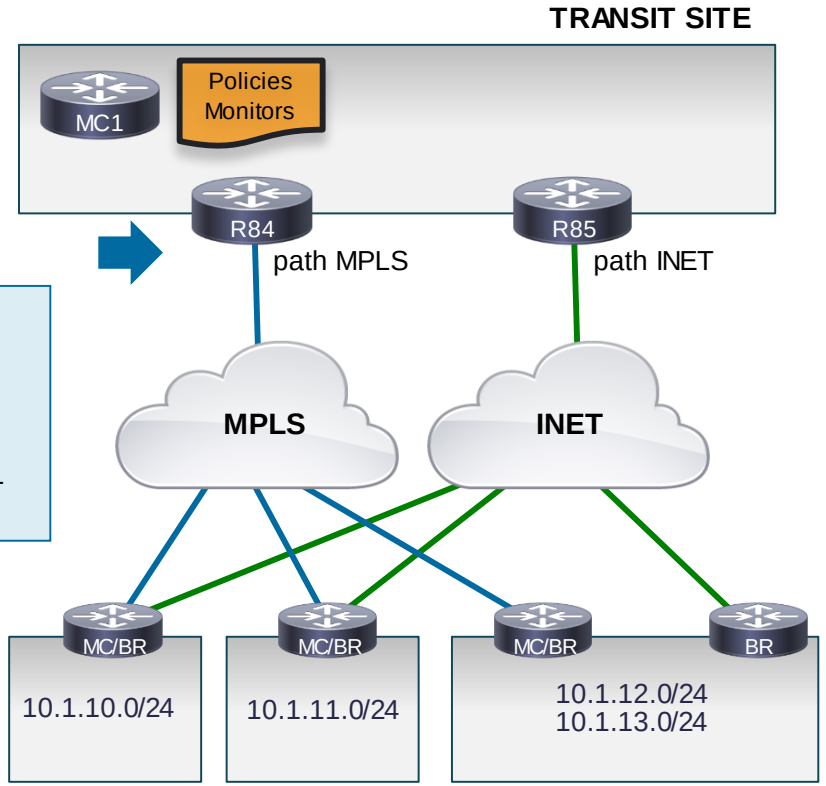
```
domain IWAN
 vrf default
  master hub
   source-interface Loopback0
   enterprise-prefix prefix-list ENTERPRISE_PREFIX
   site-prefixes prefix-list DC1_PREFIX
```

BR1

```
domain IWAN
 vrf default
   border
    master 10.8.3.3
    source-interface Loopback0
!
interface Tunnel100
 description -- Primary Path --
 domain IWAN path MPLS
```

BR2

```
domain IWAN
 vrf default
   border
    master 10.8.3.3
    source-interface Loopback0
!
interface Tunnel200
 description - Secondary Path --
 domain IWAN path INET
```



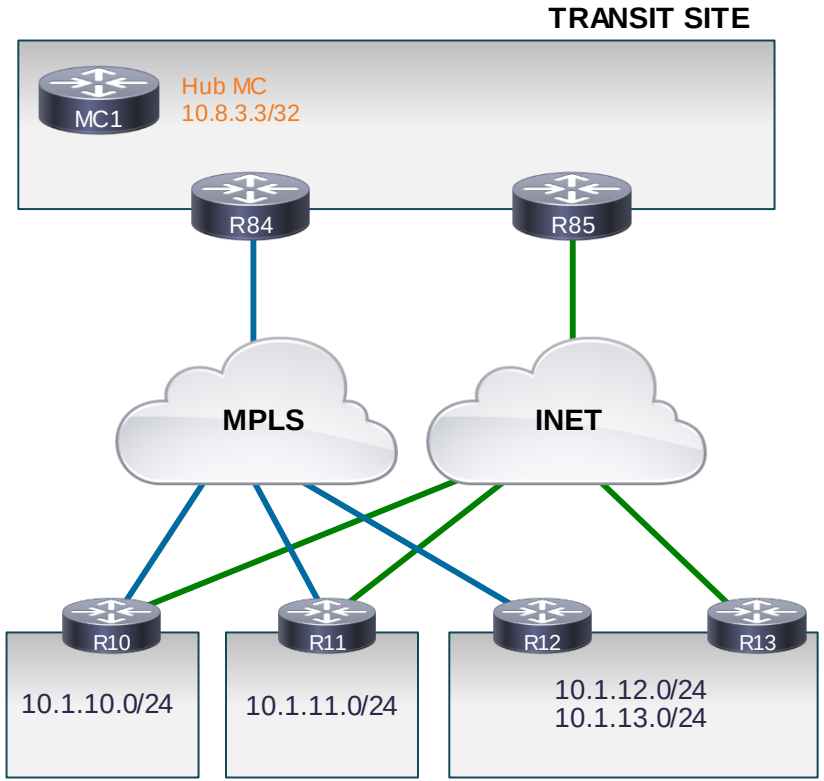
- IWAN POP is the central hub for the Enterprise Domain
  - MC1 – Hub MC
  - BR1 – Hub BR, DMVPN Hub for MPLS
  - BR2 – Hub BR, DMVPN Hub for INET

Single CPE Branch Sites

R10
R11

```
domain IWAN
 vrf default
  master branch
   source-interface Loopback0
   hub 10.8.3.3
  border
   master local
   source-interface Loopback0
```

- Stub Site
- Combination of MC and BR on the same CPE



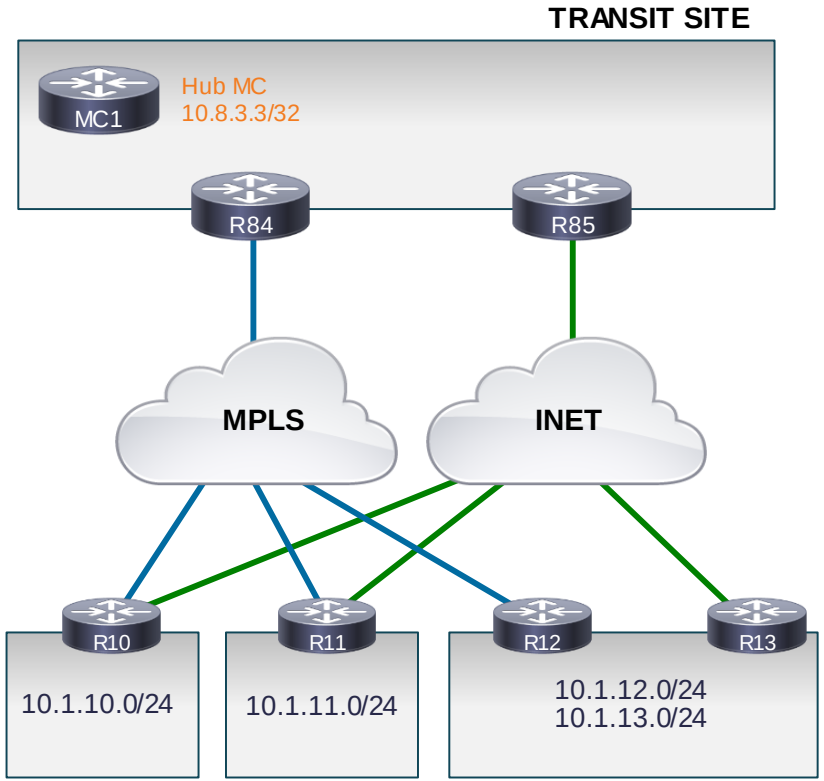
Dual CPE Branch Sites

R12

```
domain IWAN
 vrf default
  master branch
   source-interface Loopback0
   hub 10.8.3.3
  border
   master local
   source-interface Loopback0
```

R13

```
domain IWAN
 vrf default
  border
   master 10.2.12.12
   source-interface Loopback0
```



- Stub Site
- One of the BR is also the MC

Enterprise Domain

Policy – DSCP or App Based

```
domain IWAN
 vrf default
  master hub
   load-balance
   class VOICE sequence 10
    match dscp ef policy voice
    path-preference MPLS fallback INET
   class VIDEO sequence 20
    match dscp af41 policy voice
    path-preference MPLS fallback INET
   class CRITICAL sequence 30
    match dscp af31 policy low-latency-data
```

MC1

- When load balancing is enabled, PfRv3 adds a “default class for match all DSCP (lowest priority compared to all the other classes)” and we influence this traffic.
- When load balancing is disabled, PfRv3 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

Cisco live!

Policy – Monitor Intervals

```
domain IWAN
 vrf default
  master hub
   monitor-interval 2 dscp ef
   monitor-interval 2 dscp af41
   monitor-interval 2 dscp cs4
   monitor-interval 2 dscp af31
```

MC1

Monitoring Interval Fast
Reaction Time 2 sec

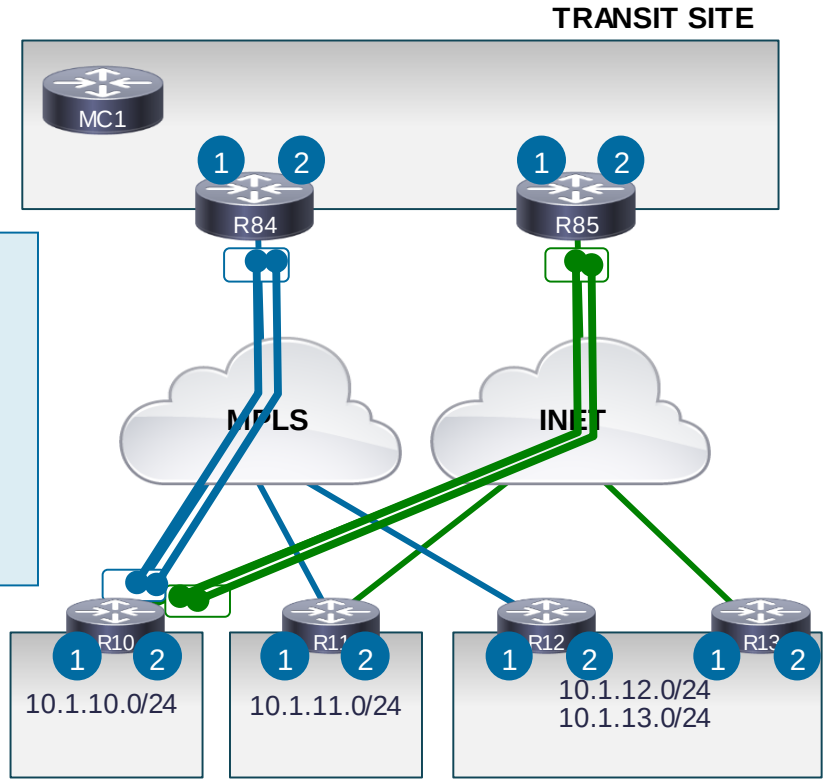
- Advanced commands
  - Carefully choose monitor interval for critical applications

Cisco live!

Deploying With User VRFs

```
vrf definition TEST1
 !
 address-family ipv4
 exit-address-family
!
vrf definition TEST2
 !
 address-family ipv4
 exit-address-family
!
```

```
interface Tunnel 101
 vrf forwarding TEST1
 tunnel key 101
 tunnel vrf IWAN-TRANSPORT-1
!
interface Tunnel 102
 vrf forwarding TEST2
 tunnel key 102
 tunnel vrf IWAN-TRANSPORT-1
```

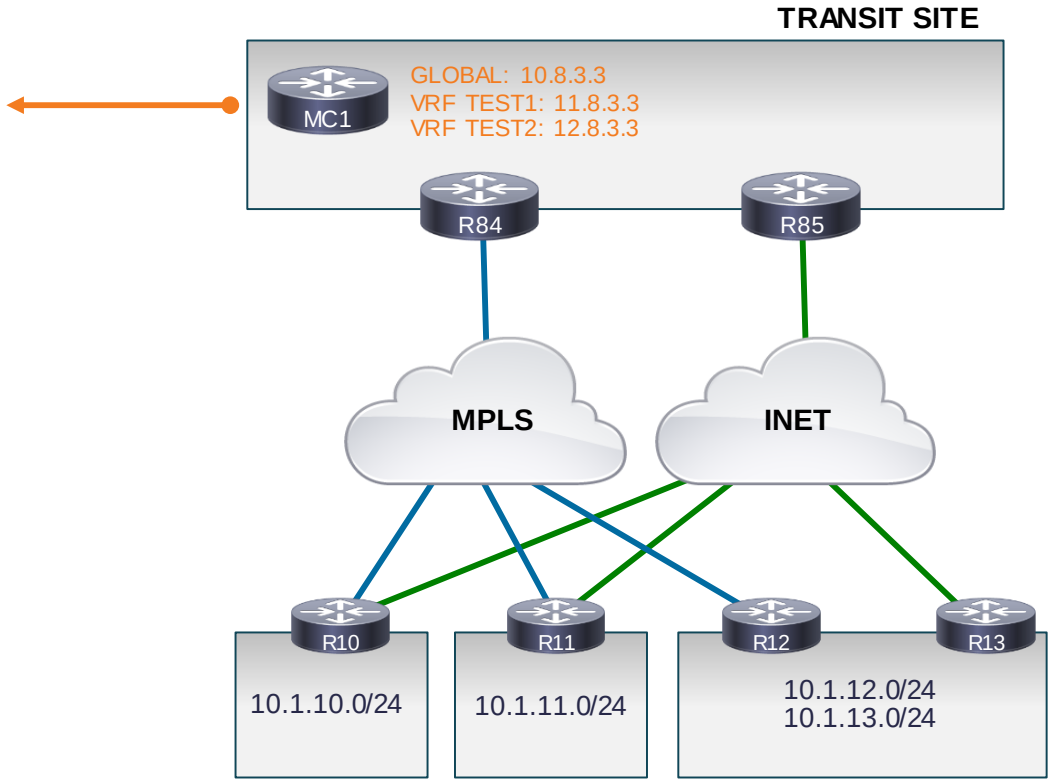


- DMVPN Tunnel per VRF
- Over the top routing per VRF
- SAF Peering per VRF

Deploying With VRF – Hub MC

```
interface Loopback1
 vrf forwarding TEST1
!
interface Loopback2
 vrf forwarding TEST2
```

```
domain IWAN
 vrf TEST1
  master hub
   source-interface Loopback1
 !
 vrf TEST2
  master hub
   source-interface Loopback2
```



Deploying With VRF – Hub MC Policies

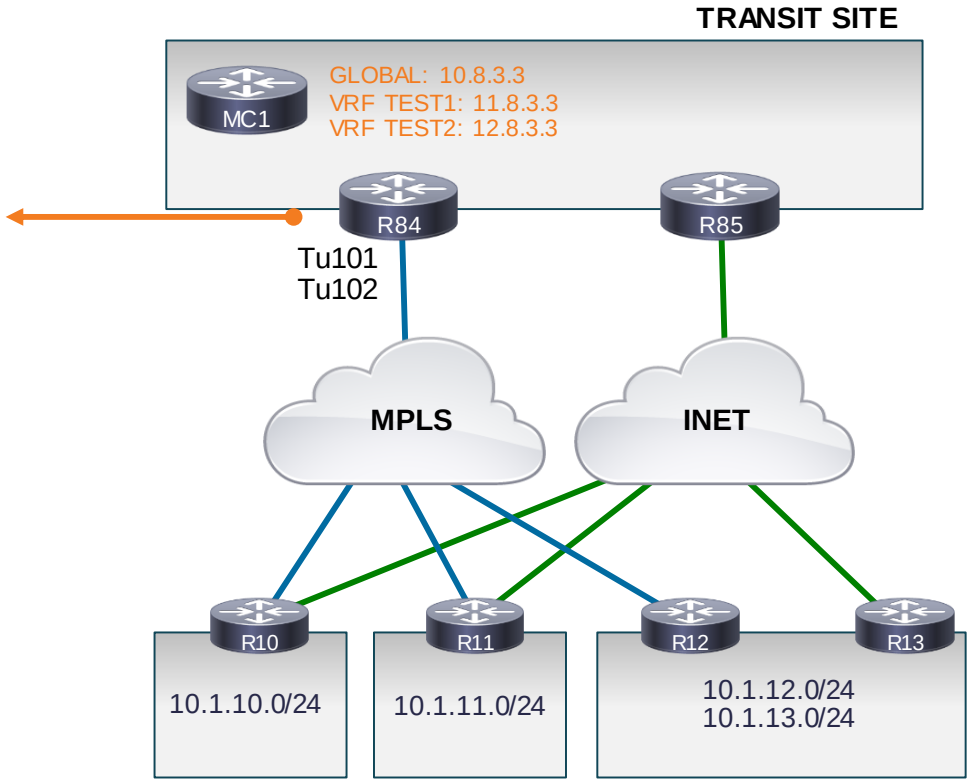
```
domain IWAN
 vrf TEST1
  master hub
   load-balance
   class VOICE sequence 10
    match dscp ef policy voice
    path-preference MPLS fallback INET
   class VIDEO sequence 20
    match dscp af41 policy voice
    path-preference MPLS fallback INET
   class CRITICAL sequence 30
    match dscp af31 policy low-latency-
data
```

```
[Cont'd]
 vrf TEST2
  master hub
   load-balance
   class VOICE sequence 10
    match dscp ef policy voice
    path-preference MPLS fallback INET
   class CRITICAL sequence 30
    match dscp af31 policy low-latency-
data
```


Cisco live!

Deploying With VRF – Hub BR

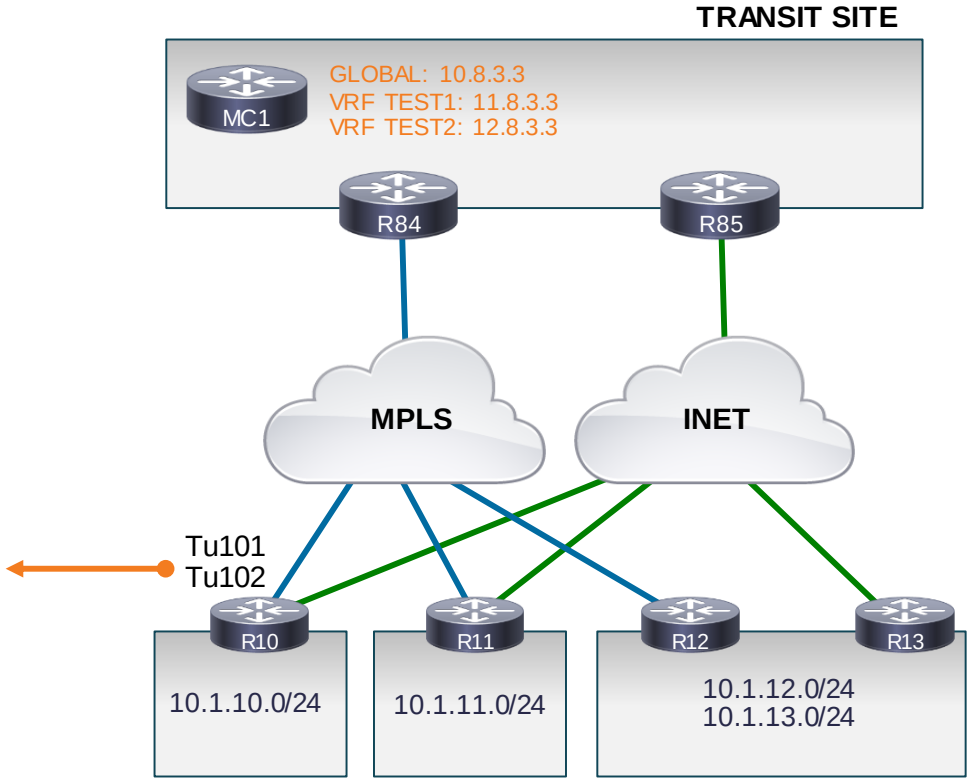
```
domain IWAN
 vrf TEST1
   border
    master 11.8.3.3
    source-interface Loopback1
!
 vrf TEST2
   border
    master 12.8.3.3
    source-interface Loopback2
!
interface Tunnel101
 description -- Primary Path -
 vrf forwarding TEST1
 domain IWAN path MPLS
!
interface Tunnel102
 description -- Primary Path -
 vrf forwarding TEST2
 domain IWAN path MPLS
```



Deploying With VRF – Branch MC/BR

R10

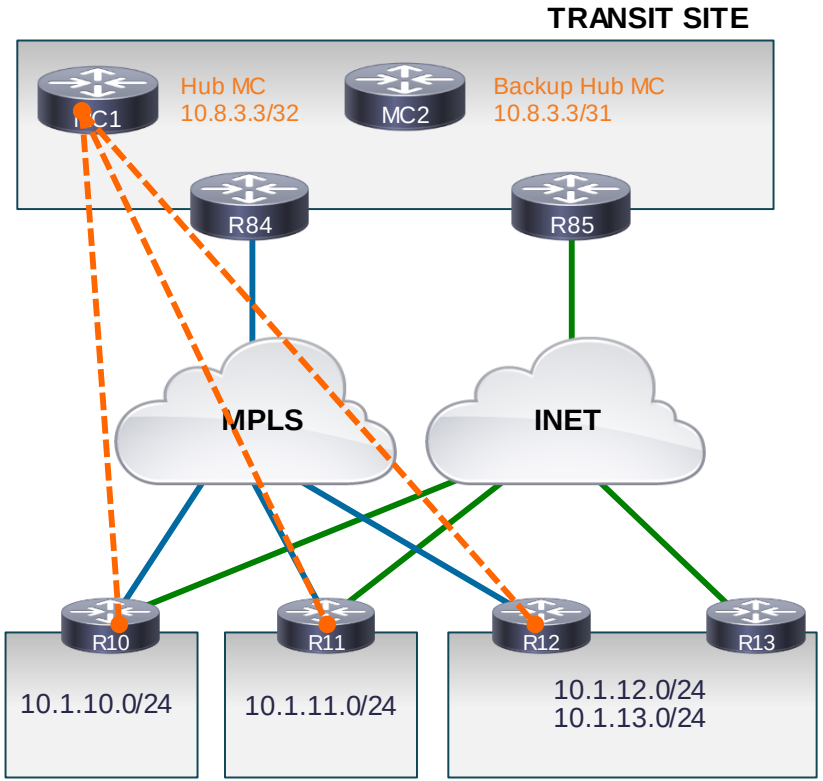
```
domain IWAN
 vrf TEST1
  master branch
   source-interface Loopback1
   hub 11.8.3.3
  border
   master local
   source-interface Loopback1
 !
vrf TEST2
  master branch
   source-interface Loopback2
   hub 12.8.3.3
  border
   master local
   source-interface Loopback2
```



Redundant MC – Anycast IP

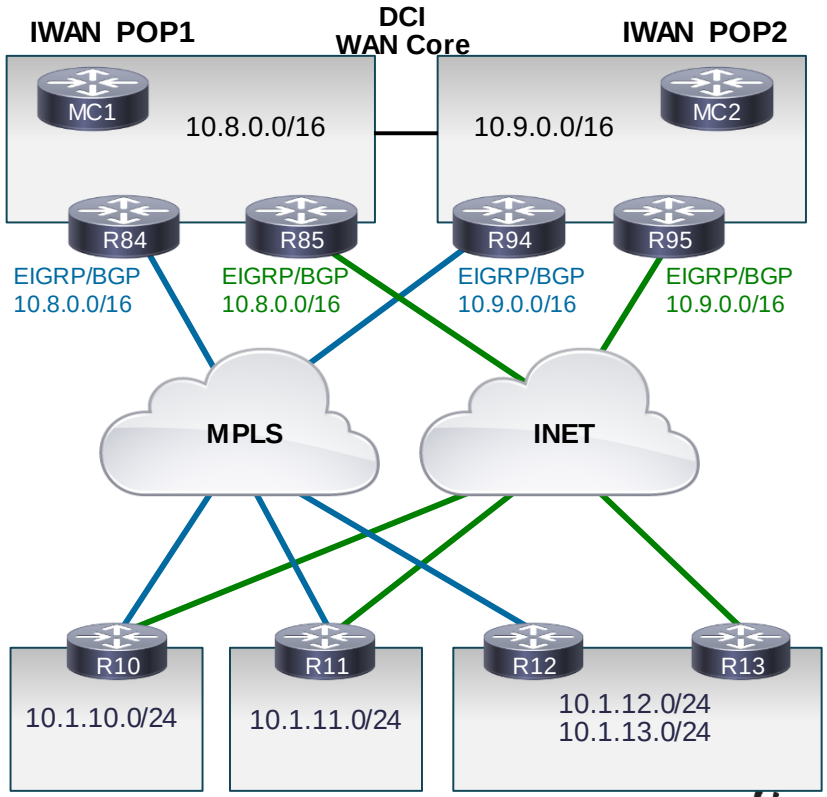
In IWAN POP

- What happens when a MC fails?
  - Traffic forwarded based on routing information – ie no drop
- What happens when the Hub MC fails?
  - Branch MCs keep their configuration and policies
  - Continue to optimise traffic
- A backup MC can be defined on the hub.
- Using the same IP address as the primary
- Routing Protocol is used to make sure BRs and branch MC connect to the primary
- Stateless redundancy
  - Backup MC will re-learn the traffic



Dual POPs – Different Prefixes

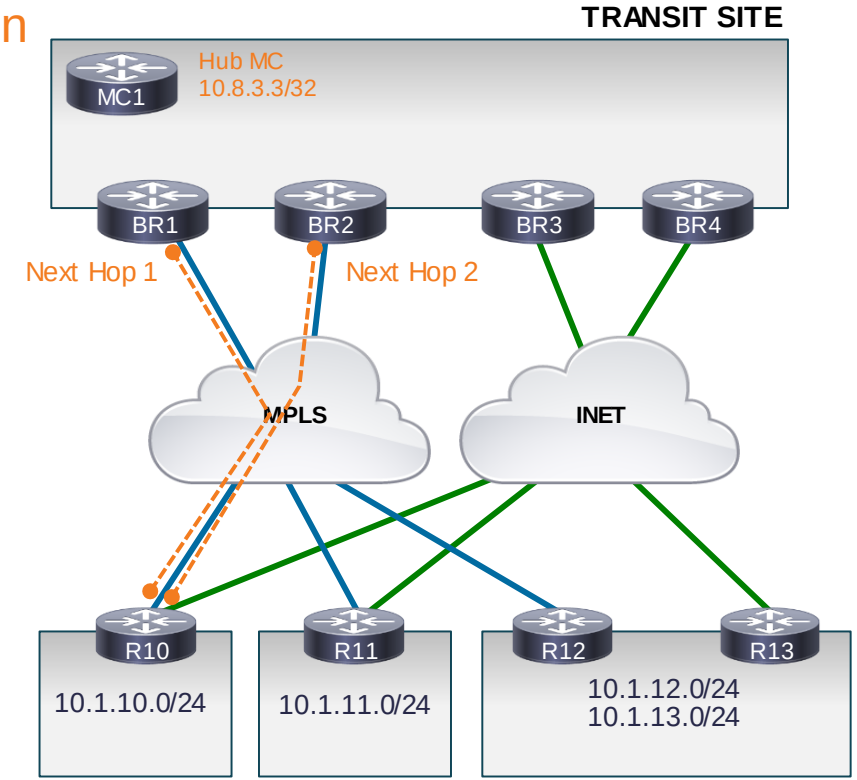
- Requirements:
  - Separate data centres/POPs
  - Separate prefix advertised from each data centres to spokes
- POP2 Hub MC
  - Configured as Branch



Horizontal Scaling Architecture

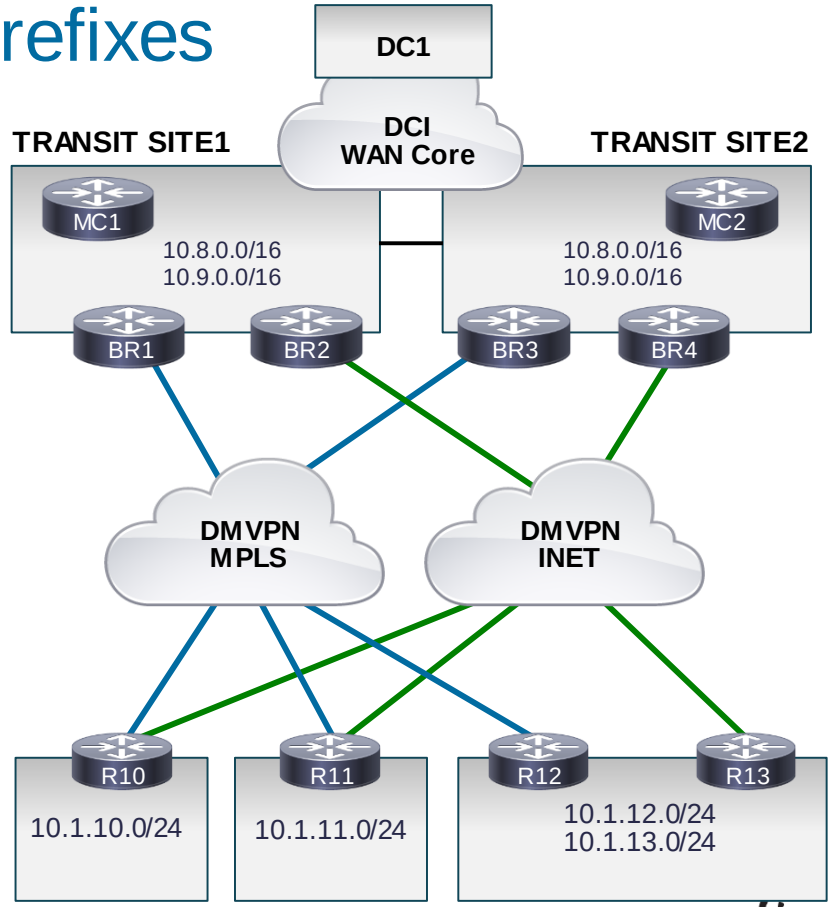
PfRv3 Multiple DMVPN Next Hop Limitation

- Limitations:
  - PfRv3 manages traffic between Tunnel Interfaces, not multiple tunnels within a single Tunnel Interface
  - Spokes have multiple next hops on the same DMVPN tunnel Interface
  - Channel definition:
    - local site id + remote site id + DSCP + colour(SP)
    - No differentiation for multiple channels within a colour(SP)
- Solution: PfRv3 DMVPN Multiple Next Hop support
  - Need to add sub-colour to differentiate channels
  - New channel definition
    - local site id + remote site id + DSCP + colour(SP) + SP tag
  - BR1 with tag 1, BR2 with tag 2
- Targeted for April CY15 XE 3.15 / 15.5(2)T releases



Multiple POPs – Common Prefixes

- Requirements:
  - 2 (or more) Transit Sites advertise the very same set of prefixes
  - Data centre may not be collocated with the Transit Sites
  - DCs/DMZs are reachable across the WAN Core for each Transit Site
  - Branches can access any DC or DMZ across either POP(hub). And, DC/DMZs can reach any branch across multiple Transit Sites (hubs).
  - Multiple BRs per DMVPN per site may be required for crypto and bandwidth horizontal scaling
- Targeted for April CY15 XE 3.15 / 15.5(2)T releases



Monitoring Operations

```
R83#sh 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

10.1.13.0/24   10.2.13.13  N/A    ef      11    N/A       CN     MPLS    25/27      10.8.4.4/Tunnel100
10.1.12.0/24   10.2.12.12  N/A    ef      9     N/A       CN     MPLS    20/19      10.8.4.4/Tunnel100

10.1.11.0/24   10.2.11.11  N/A    af31    6     N/A       CN     MPLS    24/22      10.8.4.4/Tunnel100

10.1.13.0/24   10.2.13.13  N/A    af31    8     N/A       CN     MPLS    26/28      10.8.4.4/Tunnel100
10.1.12.0/24   10.2.12.12  N/A    af31    4     N/A       CN     MPLS    11/12      10.8.4.4/Tunnel100
10.1.11.0/24   10.2.11.11  N/A    default 5     N/A       CN     INET    8/NA       10.8.5.5/Tunnel200

[SNIP]

Total Traf
R83#
```

Traffic Class – Site11 - Critical

TC Id

Controlled

Path Information - Channels

Check Traffic Classes Details

```
R83#sh domain one master traffic-classes

Dst-Site-Prefix: 10.1.10.0/24          DSCP: ef [46] Traffic class id:25
 TC Learned:                    00:12:44 ago
 Present State:                 CONTROLLED
 Current Performance Status:    in-policy

 Current Service Provider:      INET since 00:06:01
 Previous Service Provider:     INET for 181 sec
 (A fallback provider. Primary provider will be re-evaluated 00:00:01 later)
 BW Used:                       24 Kbps
 Present WAN interface:         Tunnel200 in Border 10.8.5.5

Present Channel (primary):      84
 Backup Channel:                85
 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:                    00:00:14 ago
 Reason for Route Change:       Delay
```

Check Traffic Class Voice for site 10

Active Path used

Check Channels used (Primary and Backup)

Policies and reason for last change

Check Channel After TCA

```
MC1#sh domain IWAN master channels | beg 107
Channel Id: 107  Dst Site-Id: 10.2.11.11  Link Name: MPLS  DSCP: ef [46] TCs: 1
  Channel Created: 00:15:03 ago
  Provisional State: Initiated and open
  Operational state: Available
  Interface Id: 11
  Estimated Channel Egress Bandwidth: 0 Kbps
  Immitigable Events Summary:
   Total Performance Count: 0, Total BW Count: 0
  ODE Stats Bucket Number: 1
   Last Updated  : 00:05:45 ago
    Packet Count  : 2
    Byte Count    : 116
    One Way Delay : 254 msec*
    Loss Rate Pkts: 0.66 %
    Loss Rate Byte: 0.0 %
    Jitter Mean   : 38000 usec
    Unreachable   : FALSE
```

On Demand Export (ODE)

Threshold Crossing Alert (TCA)

```
[SNIP]

TCA Statistics:
  Received:1 ; Processed:1 ; Unreach_rcvd:0
  Latest TCA Bucket
   Last Updated  : 00:05:45 ago
    One Way Delay : 266 msec
    Loss Rate Pkts: NA
    Loss Rate Byte: NA
    Jitter Mean   : NA
    Unreachability: FALSE
```

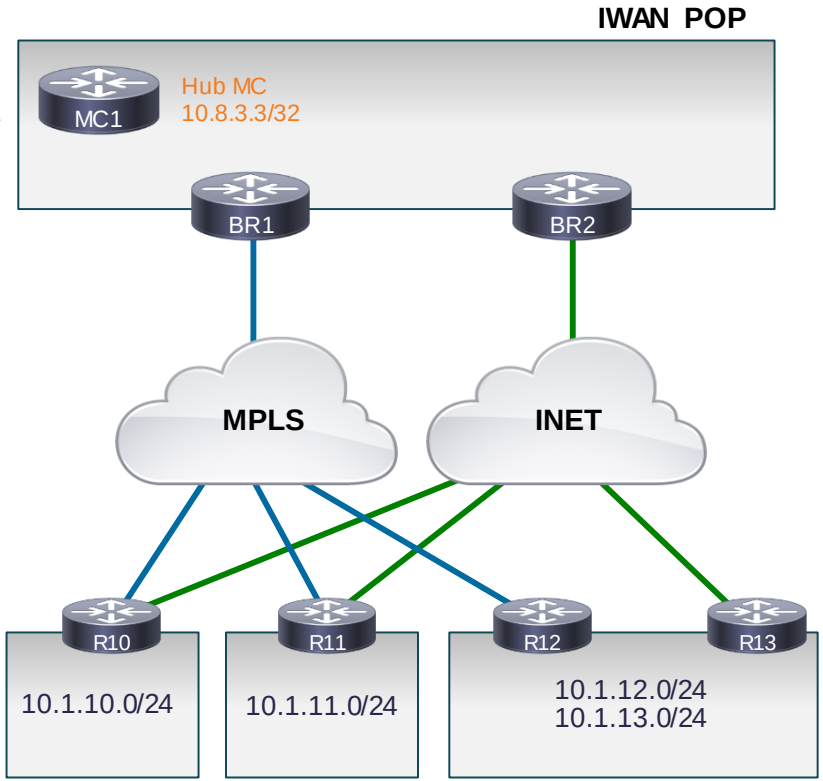
PfRv3 Management

Cisco live!

PfRv3 Exporter Configuration

```
domain IWAN
 vrf default
  master hub
   collector 10.151.1.95 port 2055
```

MC1



- Enable exporter on the Hub MC
  - Collector IP address
  - Default UDP port 9995
- Distributed through SAF to all MCs and BRs in the domain

PfRv3 NetFlow Export

List of Templates

- Exports from MC
  - TCA record
  - Route Change record
  - Immitigable Event Summary
- Bandwidth
  - Exports from BRs
  - Egress Measurement Template
  - Ingress Measurement Template
- All records available at:
  - http://docwiki.cisco.com/wiki/PfRv3:Reporting

Cisco live!

Cisco IWAN Management

On-Prem Management

Prime Infrastructure 2.2

End-to-End Assurance of Application Experience

- **Single-pane view of IWAN**
- IWAN deployment workflows
- Plug and Play
- DMVPN, QoS, AVC deployment and monitoring
- PfR v3 in Q1 2015
- License includes IWAN App and APIC-EM controller!

Specialised Management

LiveAction
Simplifying the Network

Application Aware Network Performance Management

- **Integrates with Cisco AVC and PfR**
- Monitor and analyse application traffic
- End-to-end flow visualisation
- Flow & App-based Troubleshooting
- Fix and Verify in Realtime

Cloud-Based Management

glue™ NETWORKS

Automates Deployment and Lifecycle Management

- **Eliminates manual building of WANs**
- Automated SD-WAN orchestration
- Centralised hybrid WAN management
- Quick config updates and IOS upgrades
- Leverages onePK and REST APIs

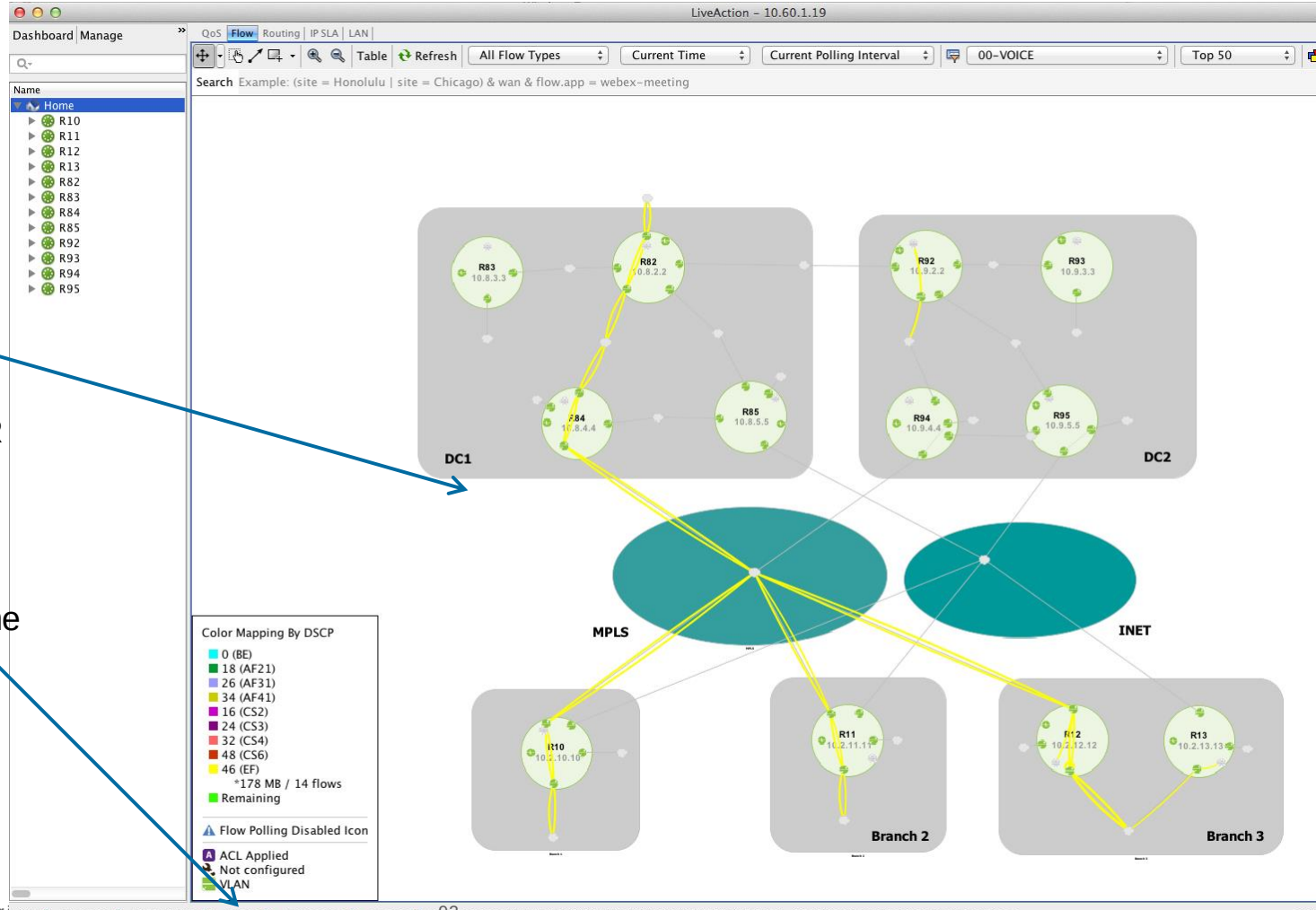
LiveAction 4.1

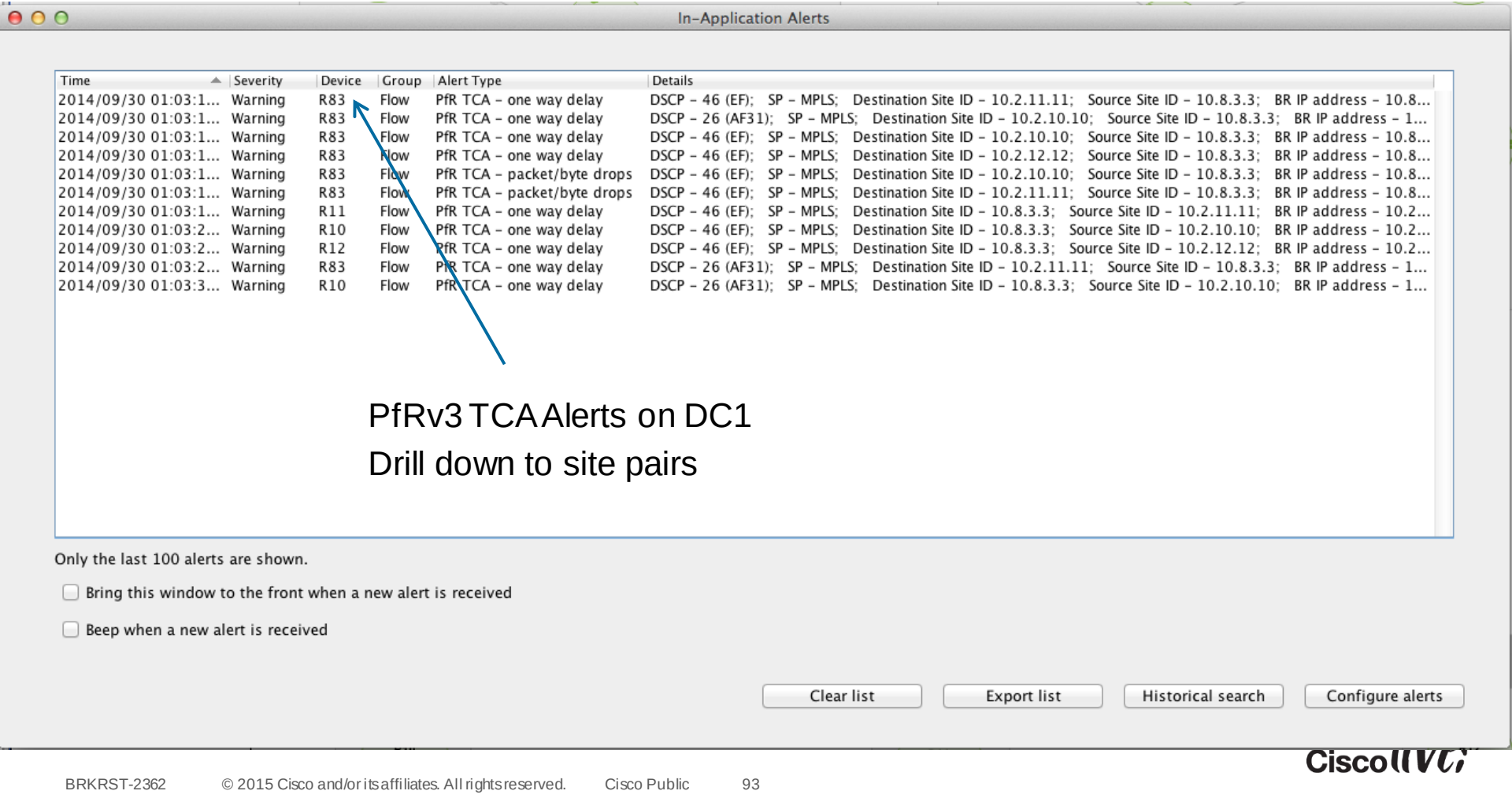
1. Alert Workflow

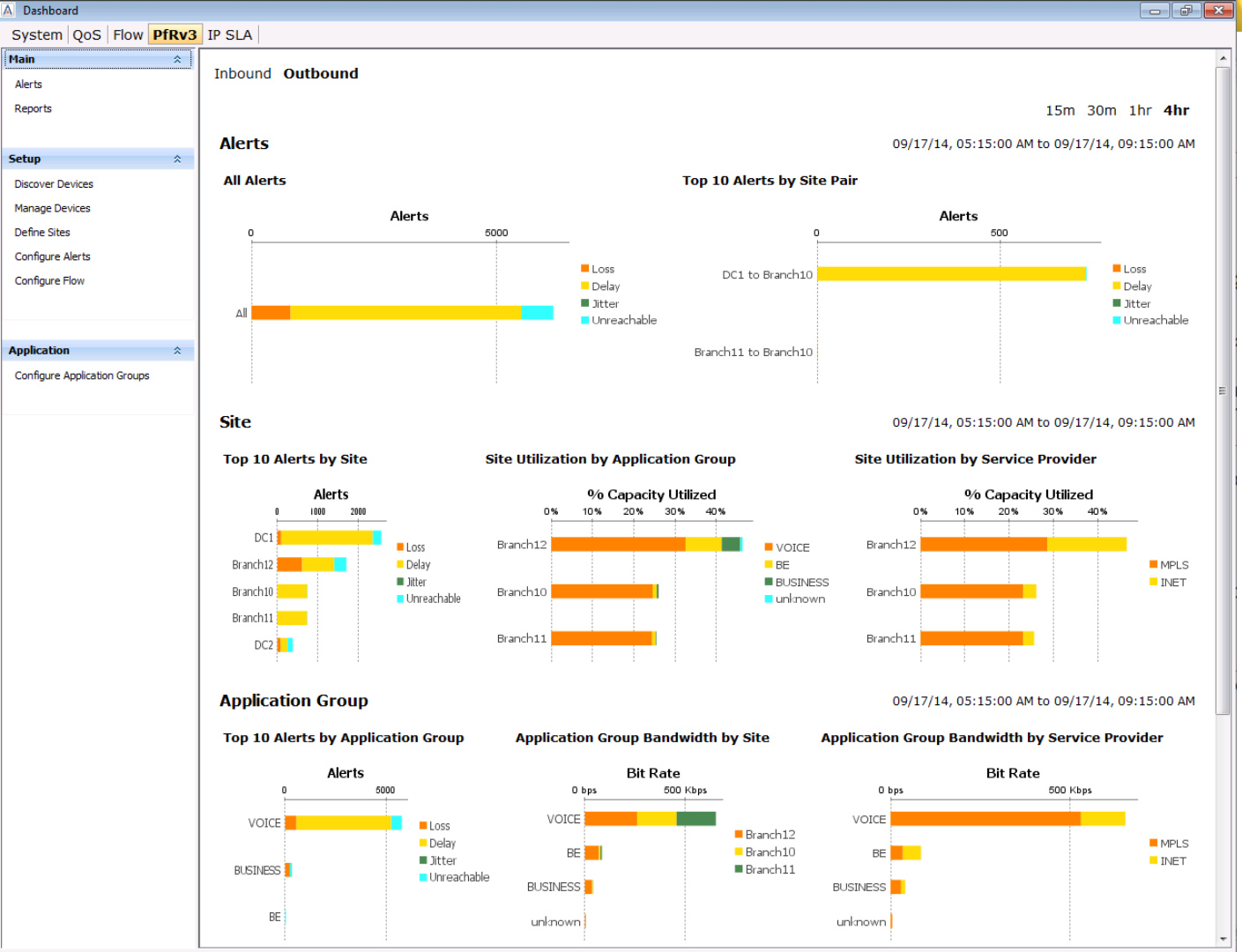
1. PfR path change visualisation

2. Alert and report on PfR Out of Policy events

3. Click on Alerts to get the details







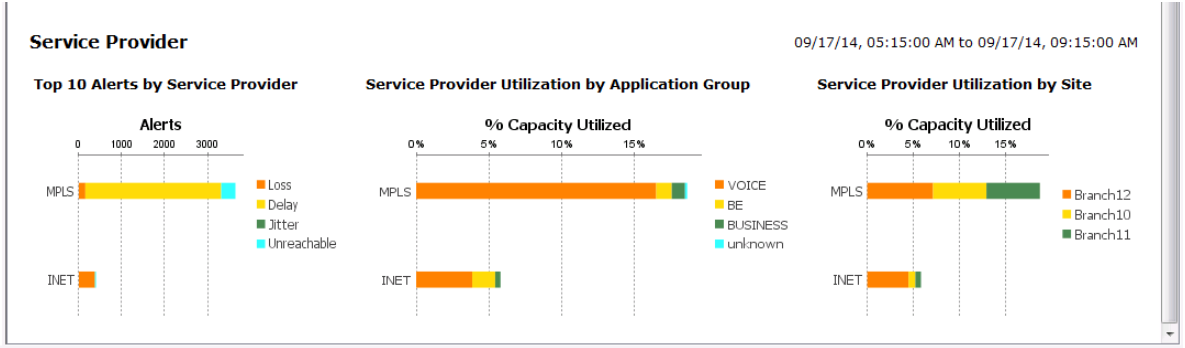
2. PfRv3 Dashboard

All Alerts

Alerts / performance by Site

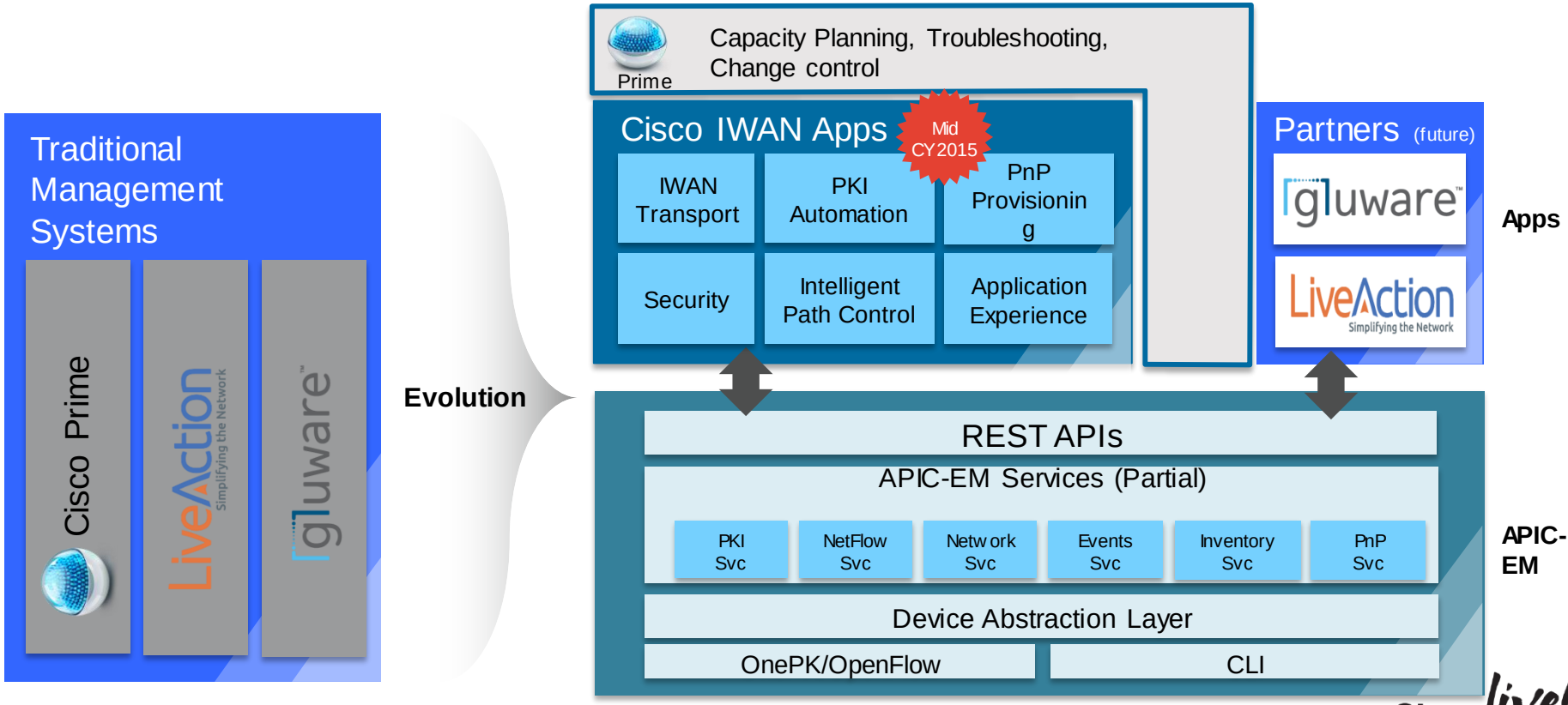
Alerts / performance by Application Group

Cisco live!



Alerts / performance by Service Provider

IWAN Automation and Orchestration Evolution



Key Takeaways

Performance Routing – IOS and IOS-XE Releases

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 ~ 2 sec Brownout ~ 2 sec Scale 2000 sites

Performance Routing – Platform Support

Cisco ISR G2 family

3900-AX
2900-AX
1900-AX
890

MC
BR

Cisco ISR 4000

4400
4300

MC
BR

Cisco ASR-1000

MC
BR

Cisco CSR-1000

MC
BR*

* BR support coming

Key Takeaways

- IWAN Intelligent Path Control pillar is based upon Performance Routing (PfR)
  - Maximises WAN bandwidth utilisation
  - Protects applications from performance degradation
  - Enables the Internet as a viable WAN transport
  - Provides multisite coordination to simplify network wide provisioning.
  - Application-based policy driven framework and is tightly integrated with existing AVC components.
  - Smart and Scalable multi-sites solution to enforce application SLAs while optimising network resources utilisation.
- PfRv3 is the 3rd generation Multi-Site aware Bandwidth and Path Control/Optimisation solution for WAN/Cloud based applications.
  - Available now on ASR1k, 4451-X, ISR-G2, and CSR

More Information

- Cisco.com IWAN/PfR Page:
  - http://www.cisco.com/go/iwan
  - http://www.cisco.com/go/pfr
- PfRv3 Home Page
  - http://docwiki.cisco.com/wiki/PfRv3:Home
- Leverage dcloud.cisco.com virtual labs
- LiveAction:
  - 1 year free license for Cisco employees
  - The New LiveAction 4.1: http://liveaction.com/new-liveaction-4-1/
  - Download LiveAction v4.1.2: http://liveaction.com/download/links/
  - LiveAction PfRv3 Demo: http://player.vimeo.com/video/103767237
  - LiveAction 4.1 IWAN Webinar, October 2nd 2014: http://liveaction.com/webinars/oct-02-2014/?elq=d49b1ff6a68b43a7a4f8e81baa8bc801&elqCampaignId=172

Call to Action

- Visit the World of Solutions for
  - Cisco Campus
  - Meet the Expert
  - Technical Solution Clinics
- Walk-in Self Paced Labs
- DevNet zone related labs and sessions
- Recommended Reading: for reading material and further resources for this session, please visit www.pearson-books.com/CLMilan2015

Cisco live!


Q & A

Complete Your Online Session Evaluation

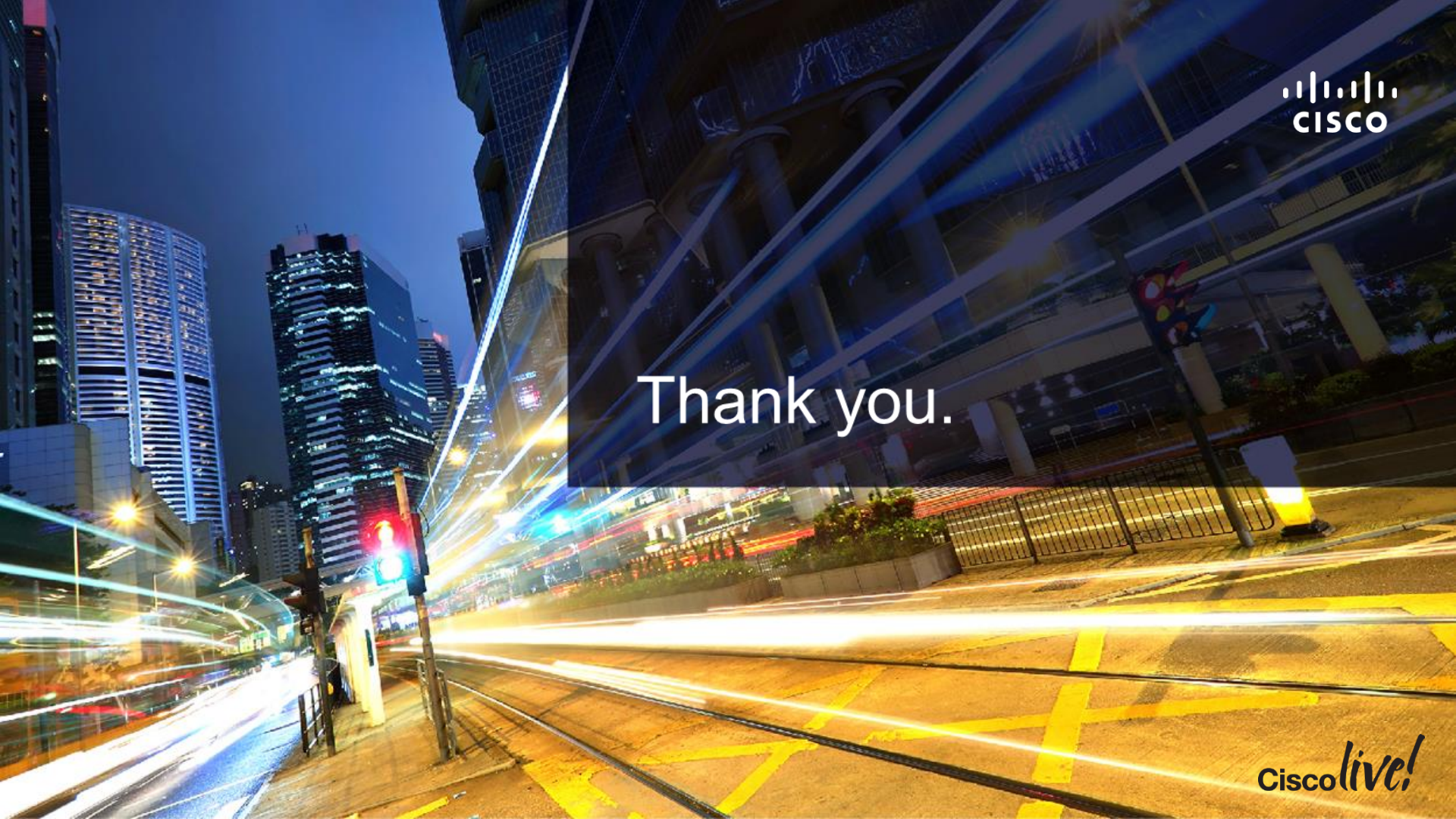
Give us your feedback and receive a Cisco Live 2015 T-Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com


Thank you.


CISCO