Targets

- Hardware:
  - ASR 9000 as Centralized Provider Edge (C-PE) router
  - NCS 5500 and NCS 55A2 as Aggregation and Pre-Aggregation router
  - NCS 5500 as P core router
  - ASR 920, NCS 540, and NCS 5500 as Access Provider Edge (A-PE)
  - cBR-8 CMTS with 8x10GE DPIC for Remote PHY
  - Compact Remote PHY shelf with three 1x2 Remote PHY Devices (RPD)
- Software:
  - IOS-XR 6.6.3 on ASR 9000, NCS 540, NCS 5500, and NCS 55A2 routers
  - IOS-XE 16.8.1 on ASR 920
  - IOS-XE 16.10.1f on cBR-8
- Key technologies
  - Transport: End-To-End Segment-Routing
  - Network Programmability: SR- TE Inter-Domain LSPs with On-Demand Next Hop
  - Network Availability: TI-LFA/Anycast-SID
  - Services: BGP-based L2 and L3 Virtual Private Network services (EVPN and L3VPN/mVPN)
  - Network Timing: G.8275.1 and G.8275.2
  - Network Assurance: 802.1ag

Testbed Overview

Figure 1: Compass Converged SDN Transport High Level Topology

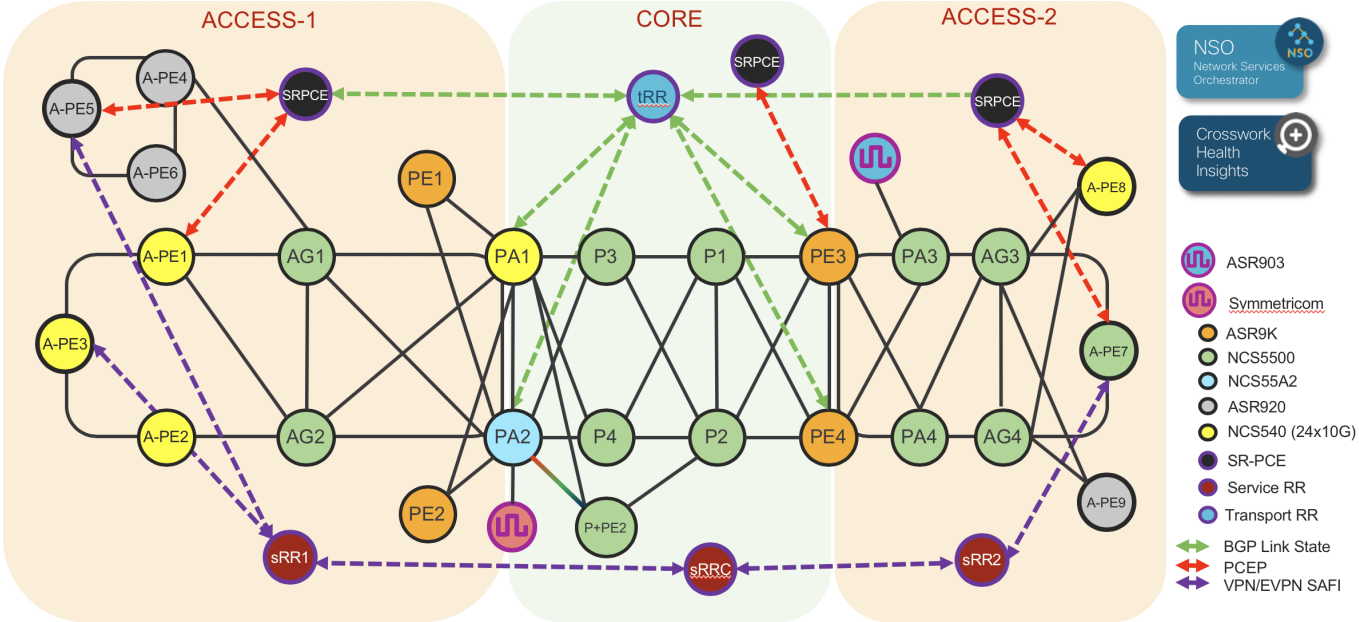


Figure 2: Testbed Physical Topology

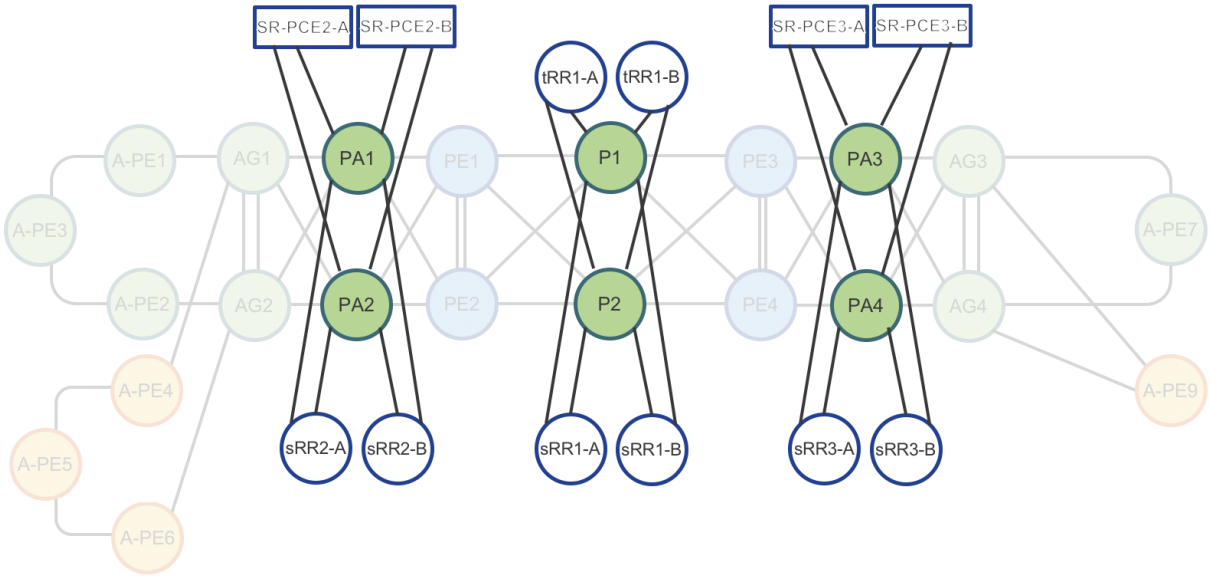


Figure 3: Testbed Route-Reflector and SR-PCE physical connectivity

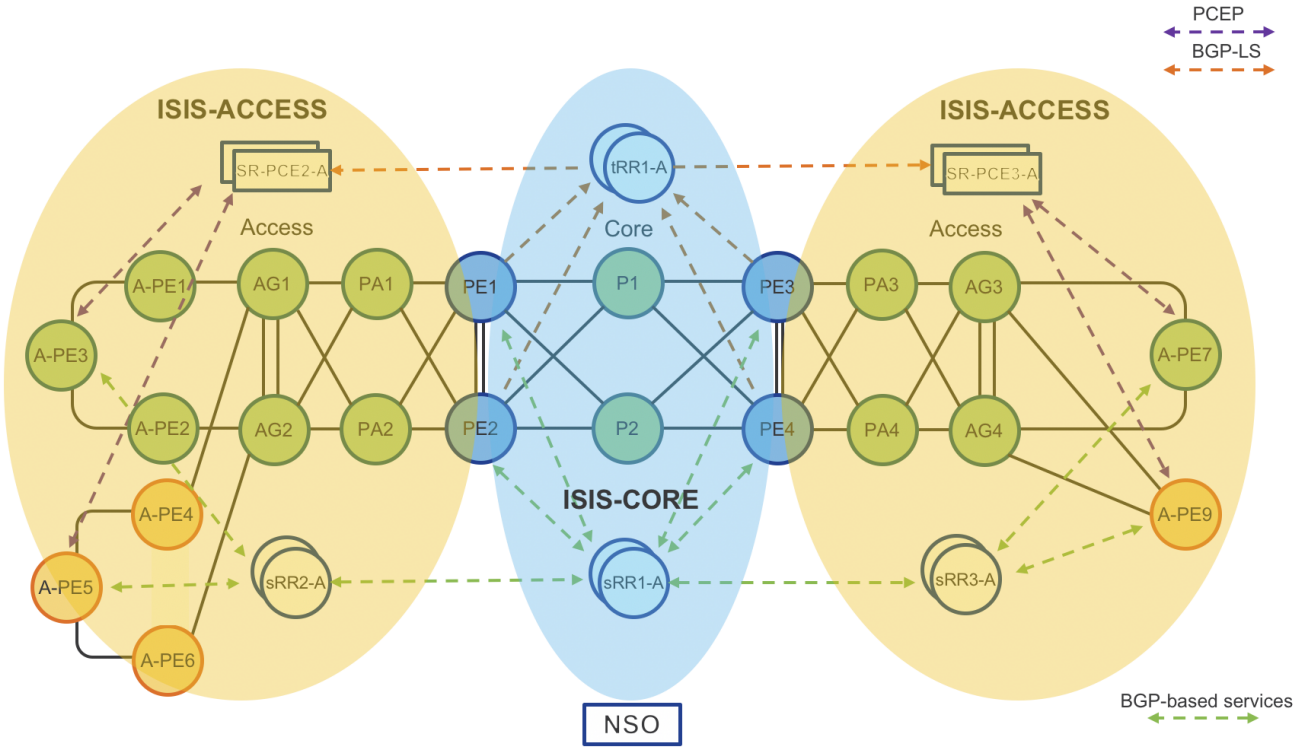


Figure 4: Testbed IGP Domains

Devices

Access PE (A-PE) Routers

- Cisco NCS5501-SE (IOS-XR) – A-PE7
- Cisco NCS540 (IOS-XR) - A-PE1, A-PE2, A-PE3, A-PE8
- Cisco ASR920 (IOS-XE) – A-PE4, A-PE5, A-PE6, A-PE9

Pre-Aggregation (PA) Routers

- Cisco NCS5501-SE (IOS-XR) – PA3, PA4

Aggregation (PA) Routers

- Cisco NCS5501-SE (IOS-XR) – AG1, AG2, AG3, AG4

High-scale Provider Edge Routers

- Cisco ASR9000 (IOS-XR) – PE1, PE2, PE3, PE4

Area Border Routers (ABRs)

- Cisco ASR9000 (IOS-XR) – PE3, PE4
- Cisco 55A2-MOD-SE - PA2
- Cisco NCS540 - PA1

Service and Transport Route Reflectors (RRs)

- Cisco IOS XRv 9000 – tRR1-A, tRR1-B, sRR1-A, sRR1-B, sRR2-A, sRR2-B, sRR3-A, sRR3-B

Segment Routing Path Computation Element (SR-PCE)

- Cisco IOS XRv 9000 – SRPCE-A1-A, SRPCE-A1-B, SRPCE-A2-A, SRPCE-A2-A, SRPCE-CORE-A, SRPCE-CORE-B

Key Resources to Allocate

- IP Addressing
    - IPv4 address plan
    - IPv6 address plan, recommend dual plane day 1
        - Plan for SRv6 in the future
- Color communities for ODN
- Segment Routing Blocks
    - SRGB (segment-routing address block)
    - Keep in mind anycast SID for ABR node pairs
    - Allocate 3 SIDs for potential future Flex-algo use
    - SRLB (segment routing local block)
        - Local significance only
        - Can be quite small and re-used on each node
- IS-IS unique instance identifiers for each domain

Role-Based Router Configuration

IOS-XR Nodes - SR-MPLS Transport

Underlay physical interface configuration with BFD

```
interface TenGigE0/0/0/10
 bfd mode ietf
 bfd address-family ipv4 timers start 180
 bfd address-family ipv4 multiplier 3
 bfd address-family ipv4 destination 10.1.2.1
 bfd address-family ipv4 fast-detect
 bfd address-family ipv4 minimum-interval 50
 mtu 9216
 ipv4 address 10.15.150.1 255.255.255.254
 ipv4 unreachables disable
 load-interval 30
 dampening
```

SRGB and SRLB Definition

It's recommended to first configure the Segment Routing Global Block (SRGB) across all nodes needing connectivity between each other. In most instances a single SRGB will be used across the entire network. In a SR MPLS deployment the SRGB and SRLB correspond to the label blocks allocated to SR. IOS-XR has a maximum configurable SRGB limit of 512,000 labels, however please consult platform-specific documentation for maximum values. The SRLB corresponds to the labels allocated for SIDs local to the node, such as Adjacency-SIDs. It is recommended to configure the same SRLB block across all nodes. The SRLB must not overlap with the SRGB. The SRGB and SRLB are configured in IOS-XR with the following configuration:

```
segment-routing
 global-block 16000 23999
 local-block 15000 15999
```

IGP protocol (ISIS) and Segment Routing MPLS configuration

Key chain global configuration for IS-IS authentication

```
key chain ISIS-KEY
 key 1
 accept-lifetime 00:00:00 january 01 2018 infinite
 key-string password 00071A150754
 send-lifetime 00:00:00 january 01 2018 infinite
 cryptographic-algorithm HMAC-MD5
```

IS-IS router configuration

All routers, except Area Border Routers (ABRs), are part of one IGP domain and L2 area (ISIS-ACCESS or ISIS-CORE). Area border routers
run two IGP IS-IS processes (ISIS-ACCESS and ISIS-CORE). Note that Loopback0 is part of both IGP processes.

```
router isis ISIS-ACCESS
 set-overload-bit on-startup 360
 is-type level-2-only
 net 49.0001.0101.0000.0110.00
 nsr
 nsf cisco
 log adjacency changes
 lsp-gen-interval maximum-wait 5000 initial-wait 5 secondary-wait 100
 lsp-refresh-interval 65000
 max-lsp-lifetime 65535
 lsp-password keychain ISIS-KEY
 address-family ipv4 unicast
  metric-style wide
  advertise link attributes
  spf-interval maximum-wait 1000 initial-wait 5 secondary-wait 100
  segment-routing mpls
  spf prefix-priority high tag 1000
  maximum-redistributed-prefixes 100 level 2
 !
 address-family ipv6 unicast
  metric-style wide
  spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  maximum-redistributed-prefixes 100 level 2
```

Note: ABR Loopback 0 on domain boundary is part of both IGP processes together with same “prefix-sid absolute” value

Note: The prefix SID can be configured as either ***absolute*** or ***index***. The ***index*** configuration is required for interop with nodes using a different SRGB.

IS-IS Loopback and node SID configuration

```
interface Loopback0
 ipv4 address 100.0.1.50 255.255.255.255
 address-family ipv4 unicast
  prefix-sid absolute 16150
  tag 1000
```

IS-IS interface configuration with TI-LFA

It is recommended to use manual adjacency SIDs. A ***protected*** SID is eligible for backup path computation, meaning if a packet ingresses the node with the label a backup path will be provided in case of a failure. In the case of having multiple adjacencies between the same two nodes, use the same adjacency-sid on each link.

```
interface TenGigE0/0/0/10
 point-to-point
```

```
  hello-password keychain ISIS-KEY
  address-family ipv4 unicast
   fast-reroute per-prefix
   fast-reroute per-prefix ti-lfa
   adjacency-sid absolute 15002 protected
   metric 100
  !
  address-family ipv6 unicast
   fast-reroute per-prefix
   fast-reroute per-prefix ti-lfa
   metric 100
```

MPLS Segment Routing Traffic Engineering (SRTE) configuration

The following configuration is done at the global ISIS configuration level and should be performed for all IOS-XR nodes.

```
router isis ACCESS
 address-family ipv4 unicast
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
```

MPLS Segment Routing Traffic Engineering (SRTE) TE metric configuration

The TE metric is used when computing SR Policy paths with the "te" or "latency" constraint type. The TE metric is carried as a TLV within the TE opaque LSA distributed across the IGP area and to the PCE via BGP-LS.
The TE metric is used in the CST 5G Transport use case. If no TE metric is defined the local CSPF or PCE will utilize the IGP metric.

```
segment-routing
 traffic-eng
  interface TenGigE0/0/0/6
   metric 1000
```

Interface delay metric static configuration

In the absence of dynamic realtime one-way latency monitoring for physical interfaces, the interface delay can be set manually. The one-way delay measurement value is used when computing SR Policy paths with the "latency" constraint type. The configured value is advertised in the IGP using extensions defined in RFC 7810, and advertised to the PCE using BGP-LS extensions. Keep in mind the delay metric value is defined in microseconds, so if you are mixing dynamic computation with static values they should be set appropriately.

```
performance-measurement
 interface TenGigE0/0/0/10
```

```
 delay-measurement
  advertise-delay 15000
interface TenGigE0/0/0/20
 delay-measurement
  advertise-delay 10000
```

IOS-XE Nodes - SR-MPLS Transport

Segment Routing MPLS configuration

```
mpls label range 6001 32767 static 16 6000
```

segment-routing mpls ! set-attributes address-family ipv4 sr-label-preferred exit-address-family ! global-block 16000 24999 !

Prefix-SID assignment to loopback 0 configuration

```
connected-prefix-sid-map
 address-family ipv4
  100.0.1.51/32 index 151 range 1
 exit-address-family
!
```

IGP protocol (ISIS) with Segment Routing MPLS configuration

key chain ISIS-KEY key 1 key-string cisco accept-lifetime 00:00:00 Jan 1 2018 infinite send-lifetime 00:00:00 Jan 1 2018 infinite ! router isis ACCESS net 49.0001.0102.0000.0254.00 is-type level-2-only authentication mode md5 authentication key-chain ISIS-KEY metric-style wide fast-flood 10 set-overload-bit on-startup 120 max-lsp-lifetime 65535 lsp-refresh-interval 65000 spf-interval 5 50 200 prc-interval 5 50 200 lsp-gen-interval 5 5 200 log-adjacency-changes segment-routing mpls segment-routing prefix-sid-map advertise-local

TI-LFA FRR configuration

```
 fast-reroute per-prefix level-2 all
 fast-reroute ti-lfa level-2
 microloop avoidance protected
!
```

interface Loopback0 ip address 100.0.1.51 255.255.255.255 ip router isis ACCESS isis circuit-type level-2-only end

IS-IS and MPLS interface configuration

```
interface TenGigabitEthernet0/0/12
 mtu 9216
 ip address 10.117.151.1 255.255.255.254
 ip router isis ACCESS
 mpls ip
 isis circuit-type level-2-only
 isis network point-to-point
 isis metric 100
end
```

MPLS Segment Routing Traffic Engineering (SRTE)

```
router isis ACCESS
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
```

interface TenGigabitEthernet0/0/12 mpls traffic-eng tunnels

Area Border Routers (ABRs) IGP-ISIS Redistribution configuration (IOS-XR)

The ABR nodes must provide IP reachability for RRs, SR-PCEs and NSO between ISIS-ACCESS and ISIS-CORE IGP domains. This is done by IP prefix redistribution. The ABR nodes have static hold-down routes for the block of IP space used in each domain across the network, those static routes are then redistributed into the domains using the ***redistribute static*** command with a route-policy. The distance command is used to ensure redistributed routes are not preferred over local IS-IS routes on the opposite ABR. The distance command must be applied to both ABR nodes.

```
router static
address-family ipv4 unicast
  100.0.0.0/24 Null0
  100.0.1.0/24 Null0
  100.1.0.0/24 Null0
  100.1.1.0/24 Null0
prefix-set ACCESS-PCE_SvRR-LOOPBACKS
  100.0.1.0/24,
  100.1.1.0/24
end-set
prefix-set RR-LOOPBACKS
    100.0.0.0/24,
  100.1.0.0/24
end-set
```

Redistribute Core SvRR and TvRR loopback into Access domain

```
route-policy CORE-TO-ACCESS1
  if destination in RR-LOOPBACKS then
    pass
  else
    drop
  endif
end-policy
```

router isis ACCESS address-family ipv4 unicast distance 254 0.0.0.0/0 RR-LOOPBACKS redistribute static route-policy CORE-TO-ACCESS1

Redistribute Access SR-PCE and SvRR loopbacks into CORE domain

```
route-policy ACCESS1-TO-CORE
  if destination in ACCESS-PCE_SvRR-LOOPBACKS then
    pass
  else
    drop
  endif
end-policy
```

router isis CORE address-family ipv4 unicast distance 254 0.0.0.0/0 ACCESS-PCE_SvRR-LOOPBACKS redistribute static route-policy CORE-TO-ACCESS1

Multicast transport using mLDP

Overview

This portion of the implementation guide instructs the user how to configure mLDP end to end across the multi-domain network. Multicast service examples are given in the "Services" section of the implementation guide.

mLDP core configuration

In order to use mLDP across the Converged SDN Transport network LDP must first be enabled. There are two mechanisms to enable LDP on physical interfaces across the network, LDP auto-configuration or manually under the MPLS LDP configuration context. The capabilities statement will ensure LDP unicast FECs are not advertised, only mLDP FECs. Recursive forwarding is required in a multi-domain network. mLDP must be enabled on all participating A-PE, PE, AG, PA, and P routers.

LDP base configuration with defined interfaces

```
mpls ldp
 capabilities sac mldp-only
 mldp
  logging notifications
```

```
   address-family ipv4
    make-before-break delay 30
    forwarding recursive
    recursive-fec
   !
  !
  router-id 100.0.2.53
  session protection
  address-family ipv4
  !
  interface TenGigE0/0/0/6
  !
  interface TenGigE0/0/0/7
```

LDP auto-configuration

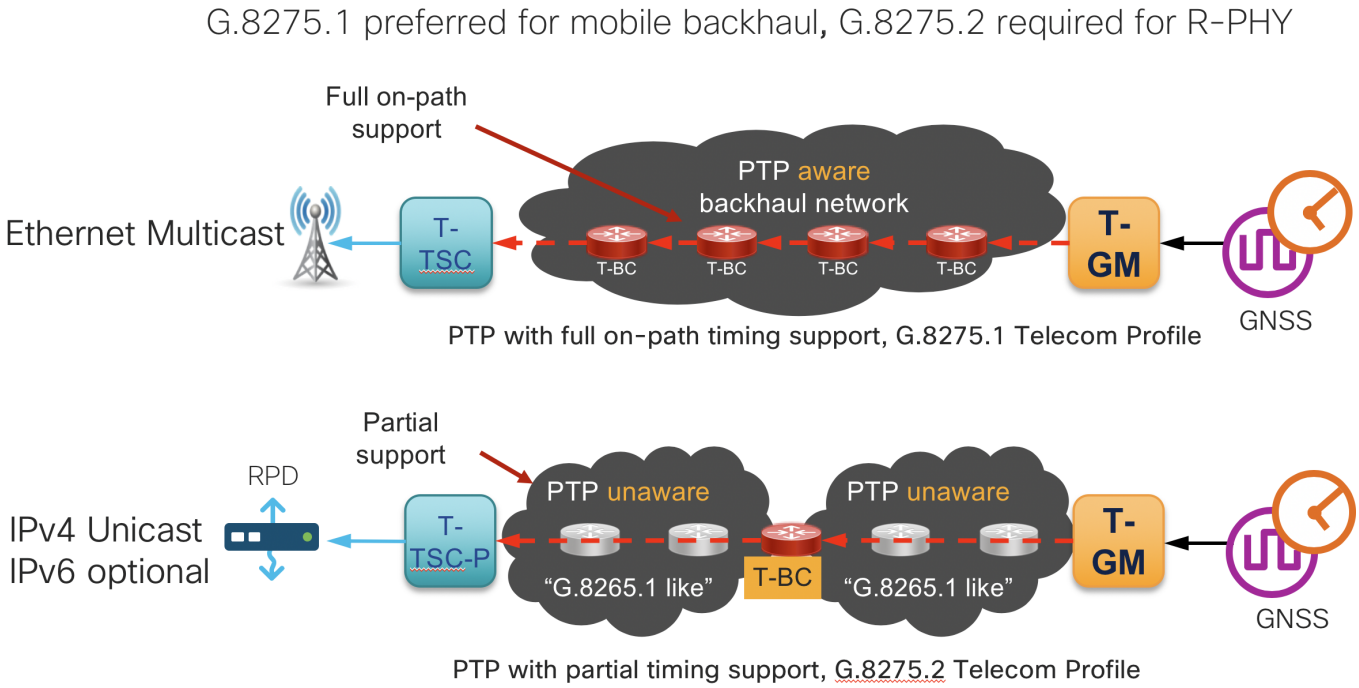
LDP can automatically be enabled on all IS-IS interfaces with the following configuration in the IS-IS configuration. It is recommended to do this only after configuring all MPLS LDP properties.

```
router isis ACCESS
  address-family ipv4 unicast
    segment-routing mpls sr-prefer
    mpls ldp auto-config
```

G.8275.1 and G.8275.2 PTP (1588v2) timing configuration

Summary

This section contains the base configurations used for both G.8275.1 and G.8275.2 timing. Please see the CST 3.0 HLD for an overview on timing in general.



Enable frequency synchronization

In order to lock the internal oscillator to a PTP source, frequency synchronization must first be enabled globally.

```
frequency synchronization
 quality itu-t option 1
 clock-interface timing-mode system
 log selection changes
!
```

Optional Synchronous Ethernet configuration (PTP hybrid mode)

If the end-to-end devices support SyncE it should be enabled. SyncE will allow much faster frequency sync and maintain integrity for long periods of time during holdover events. Using SyncE for frequency and PTP for phase is known as "Hybrid" mode. A lower priority is used on the SyncE input (50 for SyncE vs. 100 for PTP).

```
interface TenGigE0/0/0/10
 frequency synchronization
  selection input
  priority 50
 !
!
```

PTP G.8275.2 global timing configuration

As of CST 3.0, IOS-XR supports a single PTP timing profile and single clock type in the global PTP configuration. The clock domain should follow the ITU-T guidelines for specific profiles using a domain >44 for G.8275.2 clocks.

```
ptp
 clock
  domain 60
  profile g.8275.2 clock-type T-BC
  !
 frequency priority 100
 time-of-day priority 50
 log
  servo events
  best-master-clock changes
 !
```

PTP G.8275.2 interface profile definitions

It is recommended to use "profiles" defined globally which are then applied to interfaces participating in timing. This helps minimize per-interface timing configuration. It is also recommended to define different profiles for "master" and "slave" interfaces.

IPv4 G.8275.2 master profile

The master profile is assigned to interfaces for which the router is acting as a boundary clock

```
ptp
 profile g82752_master_v4
  transport ipv4
  port state master-only
  sync frequency 16
  clock operation one-step <-- 1 10 16 note the ncs series should be
configured with one-step, asr9000 two-step announce timeout interval
unicast-grant invalid-request deny delay-request frequency ! < pre>
```

IPv6 G.8275.2 master profile

The master profile is assigned to interfaces for which the router is acting as a boundary clock

```
ptp
 profile g82752_master_v6
  transport ipv6
  port state master-only
  sync frequency 16
  clock operation one-step
  announce timeout 10
  announce interval 1
  unicast-grant invalid-request deny
  delay-request frequency 16
```

```
 !
!
```

IPv4 G.8275.2 slave profile

The slave profile is assigned to interfaces for which the router is acting as a slave to another master clock

```
ptp
 profile g82752_master_v4
  transport ipv4
  port state slave-only
  sync frequency 16
  clock operation one-step <-- 1 10 16 note the ncs series should be
configured with one-step, asr9000 two-step announce timeout interval
unicast-grant invalid-request deny delay-request frequency ! < pre>
```

IPv6 G.8275.2 slave profile

The slave profile is assigned to interfaces for which the router is acting as a slave to another master clock

```
ptp
 profile g82752_master_v6
  transport ipv6
  port state slave-only
  sync frequency 16
  clock operation one-step <-- 1 10 16 note the ncs series should be
configured with one-step, asr9000 two-step announce timeout interval
unicast-grant invalid-request deny delay-request frequency ! < pre>
```

PTP G.8275.1 global timing configuration

As of CST 3.0, IOS-XR supports a single PTP timing profile and single clock type in the global PTP configuration. The clock domain should follow the ITU-T guidelines for specific profiles using a domain <44 for G.8275.1 clocks.

```
ptp
clock domain 24
  operation one-step Use one-step for NCS series, two-step for ASR 9000
  physical-layer-frequency
  frequency priority 100
  profile g.8275.1 clock-type T-BC
log
  servo events
  best-master-clock changes
```

IPv6 G.8275.1 slave profile

The slave profile is assigned to interfaces for which the router is acting as a slave to another master clock

```
ptp
 profile g82751_slave
  port state slave-only
  clock operation one-step <-- note the ncs series should be configured
with one-step, asr9000 two-step< b>
  announce timeout 10
  announce interval 1
  delay-request frequency 16
  multicast transport ethernet
 !
!
```

IPv6 G.8275.1 master profile

The master profile is assigned to interfaces for which the router is acting as a master to slave devices

```
ptp
 profile g82751_slave
  port state master-only
  clock operation one-step <-- note the ncs series should be configured
with one-step, asr9000 two-step< b>
  sync frequency 16
  announce timeout 10
  announce interval 1
  delay-request frequency 16
  multicast transport ethernet
 !
!
```

Application of PTP profile to physical interface

Note: In CST 3.0 PTP may only be enabled on physical interfaces. G.8275.1 operates at L2 andsupports PTP across Bundle member links and interfaces part of a bridge domain. G.8275.2 operates at L3 and does not support Bundle interfaces or BVI interfaces.

G.8275.2 interface configuration

This example is of a slave device using a master of 2405:10:23:253::0.

```
interface TenGigE0/0/0/6
 ptp
  profile g82752_slave_v6
```

```
  master ipv6 2405:10:23:253::
  !
 !
```

G.8275.1 interface configuration

```
interface TenGigE0/0/0/6
 ptp
  profile g82751_slave
  !
 !
```

Segment Routing Path Computation Element (SR-PCE) configuration

```
router static
 address-family ipv4 unicast
  0.0.0.0/1 Null0
```

router bgp 100 nsr bgp router-id 100.0.0.100 bgp graceful-restart graceful-reset bgp graceful-restart ibgp policy out enforce-modifications address-family link-state link-state ! neighbor-group TvRR remote-as 100 update-source Loopback0 address-family link-state link-state ! ! neighbor 100.0.0.10 use neighbor-group TvRR ! neighbor 100.1.0.10 use neighbor-group TvRR ! ! pce address ipv4 100.100.100.1 rest user rest_user password encrypted 00141215174C04140B ! authentication basic ! state-sync ipv4 100.100.100.2 peer-filter ipv4 access-list pe-routers !

BGP - Services (sRR) and Transport (tRR) route reflector configuration

Services Route Reflector (sRR) configuration

In the CST validation a sRR is used to reflect all service routes. In a production network each service could be allocated its own sRR based on resiliency and scale demands.

```
router static
 address-family ipv4 unicast
  0.0.0.0/1 Null0
```

router bgp 100 nsr bgp router-id 100.0.0.200 bgp graceful-restart ibgp policy out enforce-modifications address-family vpnv4 unicast nexthop trigger-delay critical 10 additional-paths receive additional-paths send ! address-family vpnv6 unicast nexthop trigger-delay critical 10 additional-paths receive additional-paths send retain route-target all ! address-family l2vpn evpn additional-paths receive additional-paths send ! address-family ipv4 mvpn nexthop trigger-delay critical 10 soft-reconfiguration inbound always ! address-family ipv6 mvpn nexthop trigger-delay critical 10 soft-reconfiguration inbound always ! neighbor-group SvRR-Client remote-as 100 bfd fast-detect

bfd minimum-interval 3 update-source Loopback0 address-family l2vpn evpn route-reflector-client ! address-family vpnv4 unicast route-reflector-client ! address-family vpnv6 unicast route-reflector-client ! address-family ipv4 mvpn route-reflector-client ! address-family ipv6 mvpn route-reflector-client ! ! neighbor 100.0.0.1 use neighbor-group SvRR-Client ! !

Transport Route Reflector (tRR) configuration

```
router static
 address-family ipv4 unicast
  0.0.0.0/1 Null0
```

router bgp 100 nsr bgp router-id 100.0.0.10 bgp graceful-restart ibgp policy out enforce-modifications address-family link-state link-state additional-paths receive additional-paths send ! neighbor-group RRC remote-as 100 update-source Loopback0 address-family link-state link-state route-reflector-client ! ! neighbor 100.0.0.1 use neighbor-group RRC ! neighbor 100.0.0.2 use neighbor-group RRC !

BGP – Provider Edge Routers (A-PEx and PEx) to service RR

Each PE router is configured with BGP sessions to service route-reflectors for advertising VPN service routes across the inter-domain network.

IOS-XR configuration

```
router bgp 100
 nsr
 bgp router-id 100.0.1.50
 bgp graceful-restart graceful-reset
 bgp graceful-restart
 ibgp policy out enforce-modifications
 address-family vpnv4 unicast
 !
 address-family vpnv6 unicast
 !
 address-family ipv4 mvpn
 !
 address-family ipv6 mvpn
 !
 address-family l2vpn evpn
 !
 neighbor-group SvRR
  remote-as 100
  bfd fast-detect
  bfd minimum-interval 3
  update-source Loopback0
  address-family vpnv4 unicast
  soft-reconfiguration inbound always
  !
  address-family vpnv6 unicast
```

```
  soft-reconfiguration inbound always
  !
  address-family ipv4 mvpn
  soft-reconfiguration inbound always
  !
  address-family ipv6 mvpn
  soft-reconfiguration inbound always
  !
  address-family l2vpn evpn
  soft-reconfiguration inbound always
  !
 !
 neighbor 100.0.1.201
  use neighbor-group SvRR
  !
!
```

IOS-XE configuration

```
router bgp 100
 bgp router-id 100.0.1.51
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor SvRR peer-group
 neighbor SvRR remote-as 100
 neighbor SvRR update-source Loopback0
 neighbor 100.0.1.201 peer-group SvRR
 !
 address-family ipv4
 exit-address-family
 !
 address-family vpnv4
  neighbor SvRR send-community both
  neighbor SvRR next-hop-self
  neighbor 100.0.1.201 activate
 exit-address-family
 !
 address-family l2vpn evpn
  neighbor SvRR send-community both
  neighbor SvRR next-hop-self
  neighbor 100.0.1.201 activate
 exit-address-family
 !
```

BGP-LU co-existence bgp configuration

CST 3.0 introduced co-existence between services using BGP-LU and SR endpoints.

Boundary node configuration

The following configuration is necessary on all domain boundary nodes. Note the *ibgp policy out enforce-modifications* command is required to change the next-hop on reflected IBGP routes.

```
router bgp 100
 ibgp policy out enforce-modifications
 neighbor-group BGP-LU-PE
  remote-as 100
  update-source Loopback0
  address-family ipv4 labeled-unicast
   soft-reconfiguration inbound always
   route-reflector-client
   next-hop-self
  !
 !
 neighbor-group BGP-LU-PE
  remote-as 100
  update-source Loopback0
  address-family ipv4 labeled-unicast
   soft-reconfiguration inbound always
   route-reflector-client
   next-hop-self
  !
 !
 neighbor 100.0.2.53
  use neighbor-group BGP-LU-PE
 !
 neighbor 100.0.2.52
  use neighbor-group BGP-LU-PE
 !
 neighbor 100.0.0.1
  use neighbor-group BGP-LU-BORDER
 !
 neighbor 100.0.0.2
  use neighbor-group BGP-LU-BORDER
 !
!
```

PE node configuration

The following configuration is necessary on all domain PE nodes participating in BGP-LU services.

```
neighbor-group BGP-LU-BORDER
  remote-as 100
  update-source Loopback0
  address-family ipv4 labeled-unicast
  !
 !
neighbor 100.0.0.3
  use neighbor-group BGP-LU-BORDER
```

```
 !
neighbor 100.0.0.4
  use neighbor-group BGP-LU-BORDER
 !
```

Area Border Routers (ABRs) IGP topology distribution

Next network diagram: “BGP-LS Topology Distribution” shows how Area Border Routers (ABRs) distribute IGP network topology from ISIS ACCESS and ISIS CORE to Transport Route-Reflectors (tRRs). tRRs then reflect topology to Segment Routing Path Computation Element (SR-PCEs). Each SR-PCE has full visibility of the entire inter-domain network.

Note: Each IS-IS process in the network requires a unique instance-id to identify itself to the PCE.

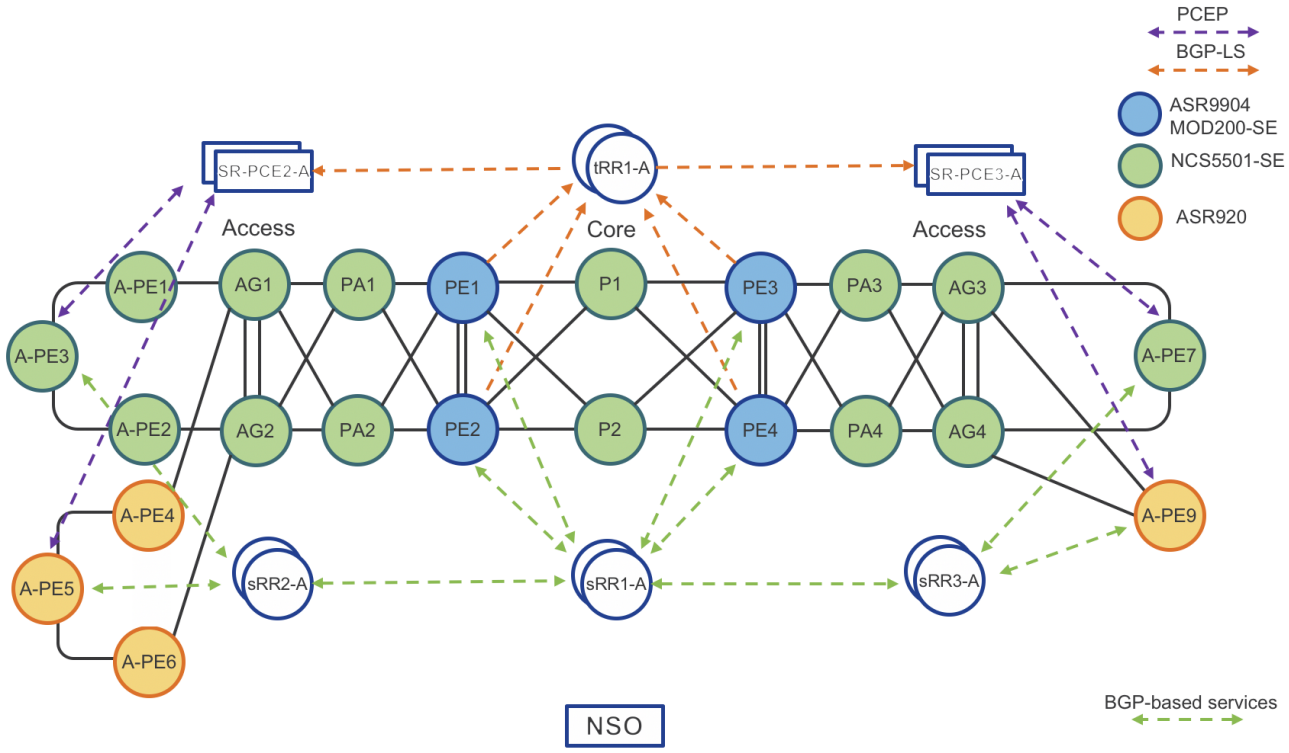


Figure 5: BGP-LS Topology Distribution

```
router isis ACCESS
 **distribute link-state instance-id 101**
 net 49.0001.0101.0000.0001.00
 address-family ipv4 unicast
  mpls traffic-eng router-id Loopback0
  !
!
router isis CORE
 **distribute link-state instance-id 100**
 net 49.0001.0100.0000.0001.00
 address-family ipv4 unicast
  mpls traffic-eng router-id Loopback0
  !
```

```
!
router bgp 100
 **address-family link-state link-state**
 !
 neighbor-group TvRR
  remote-as 100
  update-source Loopback0
  address-family link-state link-state
  !
  neighbor 100.0.0.10
  use neighbor-group TvRR
 !
 neighbor 100.1.0.10
  use neighbor-group TvRR
 !
```

Segment Routing Traffic Engineering (SRTE) and Services Integration

This section shows how to integrate Traffic Engineering (SRTE) with services. ODN is configured by first defining a global ODN color associated with specific SR Policy constraints. The color and BGP next-hop address on the service route will be used to dynamically instantiate a SR Policy to the remote VPN endpoint.

On Demand Next-Hop (ODN) configuration – IOS-XR

```
segment-routing
 traffic-eng
  logging
   policy status
  !
  on-demand color 100
   dynamic
    pce
    !
    metric
     type igp
    !
   !
  !
  pcc
   source-address ipv4 100.0.1.50
   pce address ipv4 100.0.1.101
   !
   pce address ipv4 100.1.1.101
   !
  !
```

extcommunity-set opaque BLUE 100 end-set

route-policy ODN_EVPN set extcommunity color BLUE end-policy

router bgp 100 address-family l2vpn evpn route-policy ODN_EVPN out ! !

On Demand Next-Hop (ODN) configuration – IOS-XE

```
mpls traffic-eng tunnels
mpls traffic-eng pcc peer 100.0.1.101 source 100.0.1.51
mpls traffic-eng pcc peer 100.0.1.111 source 100.0.1.51
mpls traffic-eng pcc report-all
mpls traffic-eng auto-tunnel p2p config unnumbered-interface Loopback0
mpls traffic-eng auto-tunnel p2p tunnel-num min 1000 max 5000
!
mpls traffic-eng lsp attributes L3VPN-SRTE
 path-selection metric igp
 pce
!
ip community-list 1 permit 9999
!
route-map L3VPN-ODN-TE-INIT permit 10
 match community 1
 set attribute-set L3VPN-SRTE
!
route-map L3VPN-SR-ODN-Mark-Comm permit 10
 match ip address L3VPN-ODN-Prefixes
 set community 9999
 !
!
router bgp 100
 address-family vpnv4
  neighbor SvRR send-community both
  neighbor SvRR route-map L3VPN-ODN-TE-INIT in
  neighbor SvRR route-map L3VPN-SR-ODN-Mark-Comm out
```

SR-PCE configuration – IOS-XR

```
segment-routing
 traffic-eng
  pcc
   source-address ipv4 100.0.1.50
   pce address ipv4 100.0.1.101
   !
   pce address ipv4 100.1.1.101
   !
  !
```

SR-PCE configuration – IOS-XE

mpls traffic-eng tunnels mpls traffic-eng pcc peer 100.0.1.101 source 100.0.1.51 mpls traffic-eng pcc peer 100.0.1.111 source 100.0.1.51 mpls traffic-eng pcc report-all

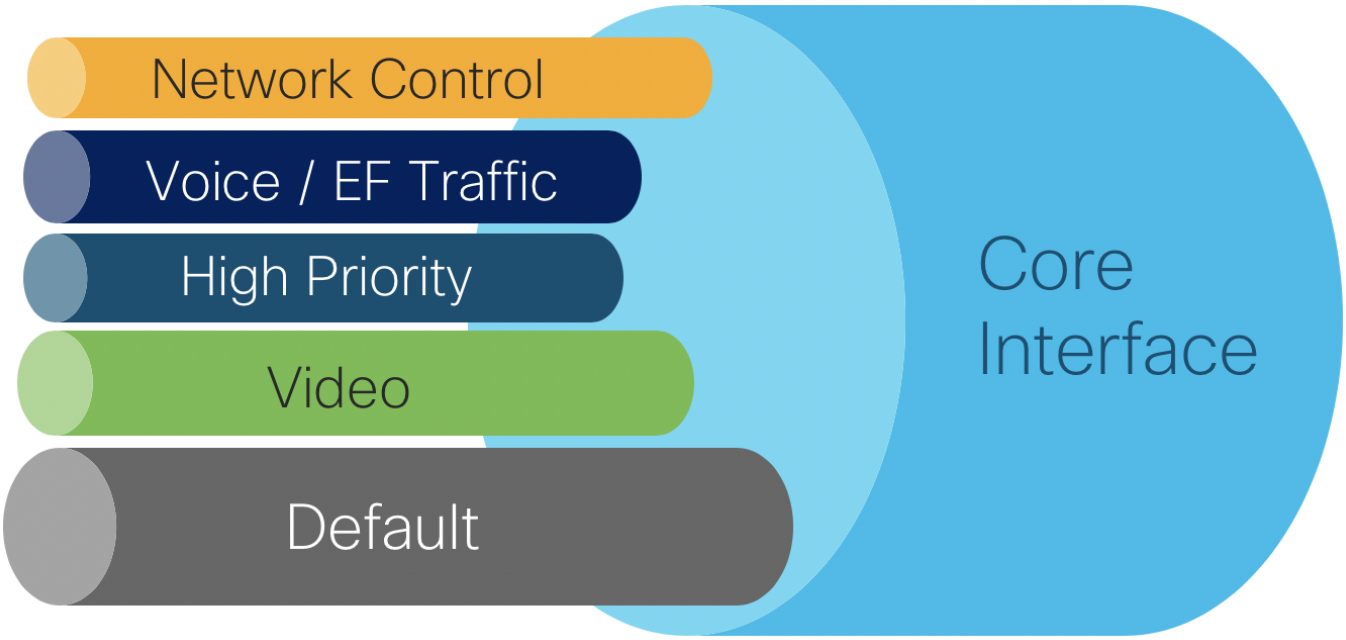
QoS Implementation

Summary

Please see the CST 3.0 HLD for in-depth information on design choices.

Core QoS configuration

The core QoS policies defined for CST 3.0 utilize priority levels, with no bandwidth guarantees per traffic class. In a production network it is recommended to analyze traffic flows and determine an appropriate BW guarantee per traffic class. The core QoS uses four classes. Note the "video" class uses priority level 6 since only levels 6 and 7 are supported for high priority multicast.



Traffic Type	Priority Level	Core EXP Marking
Network Control	1	6
Voice	2	5
High Priority	3	4
Video	6	2
Default	0	0

Class maps used in QoS policies

Class maps are used within a policy map to match packet criteria or internal QoS markings like traffic-class or qos-group

```
class-map match-any match-ef-exp5
 description High priority, EF
 match dscp 46
 match mpls experimental topmost 5
 end-class-map
!
class-map match-any match-cs5-exp4
 description Second highest priority
 match dscp 40
 match mpls experimental topmost 4
 end-class-map
!
class-map match-any match-video-cs4-exp2
 description Video
 match dscp 32
 match mpls experimental topmost 2
 end-class-map
!
class-map match-any match-cs6-exp6
 description Highest priority control-plane traffic
 match dscp cs6
 match mpls experimental topmost 6
 end-class-map
!
class-map match-any match-qos-group-1
 match qos-group 1
 end-class-map
!
class-map match-any match-qos-group-2
 match qos-group 2
 end-class-map
!
class-map match-any match-qos-group-3
 match qos-group 3
 end-class-map
!
class-map match-any match-qos-group-6
 match qos-group 3
 end-class-map
!
class-map match-any match-traffic-class-1
 description "Match highest priority traffic-class 1"
 match traffic-class 1
 end-class-map
!
class-map match-any match-traffic-class-2
 description "Match high priority traffic-class 2"
 match traffic-class 2
 end-class-map
!
class-map match-any match-traffic-class-3
```

```
 description "Match medium traffic-class 3"
 match traffic-class 3
 end-class-map
!
class-map match-any match-traffic-class-6
 description "Match video traffic-class 6"
 match traffic-class 6
 end-class-map
```

Core ingress classifier policy

```
policy-map core-ingress-classifier
 class match-cs6-exp6
  set traffic-class 1
 !
 class match-ef-exp5
  set traffic-class 2
 !
 class match-cs5-exp4
  set traffic-class 3
 !
 class match-video-cs4-exp2
  set traffic-class 6
 !
 class class-default
  set mpls experimental topmost 0
  set traffic-class 0
  set dscp 0
 !
 end-policy-map
!
```

Core egress queueing map

```
policy-map core-egress-queuing
 class match-traffic-class-2
  priority level 2
  queue-limit 100 us
 !
 class match-traffic-class-3
  priority level 3
  queue-limit 500 us
 !
 class match-traffic-class-6
  priority level 6
  queue-limit 500 us
 !
```

```
 class match-traffic-class-1
  priority level 1
  queue-limit 500 us
 !
 class class-default
  queue-limit 250 ms
 !
 end-policy-map
!
```

Core egress MPLS EXP marking map

The following policy must be applied for CIN PE devices with MPLS-based VPN services.

```
policy-map core-egress-exp-marking
 class match-qos-group-1
  set mpls experimental imposition 6
 !
 class match-qos-group-2
  set mpls experimental imposition 5
 !
 class match-qos-group-3
  set mpls experimental imposition 4
 !
 class match-qos-group-6
  set mpls experimental imposition 2
 !
 class class-default
  set mpls experimental imposition 0
 !
 end-policy-map
!
```

H-QoS configuration

Enabling H-QoS on NCS 540 and NCS 5500

Enabling H-QoS on the NCS platforms requires the following global command and requires a reload of the device.

```
hw-module profile qos hqos-enable
```

Example H-QoS policy for 5G services

The following H-QoS policy represents an example QoS policy reserving 5Gbps on a sub-interface. On ingress each child class is policed to a certain percentage of the 5Gbps policer. In the egress queuing policy, shaping is

used with guaranteed each class a certain amount of egress bandwidth, with high priority traffic being serviced in a low-latency queue (LLQ).

Class maps used in ingress H-QoS policies

```
class-map match-any edge-hqos-2-in
 match dscp 46
 end-class-map
!
class-map match-any edge-hqos-3-in
 match dscp 40
 end-class-map
!
class-map match-any edge-hqos-6-in
 match dscp 32
 end-class-map
```

Parent ingress QoS policy

```
policy-map hqos-ingress-parent-5g
 class class-default
  service-policy hqos-ingress-child-policer
  police rate 5 gbps
  !
 !
 end-policy-map
```

H-QoS ingress child policies

```
policy-map hqos-ingress-child-policer
 class edge-hqos-2-in
  set traffic-class 2
  police rate percent 10
  !
 !
 class edge-hqos-3-in
  set traffic-class 3
  police rate percent 30
  !
 !
 class edge-hqos-6-in
  set traffic-class 6
  police rate percent 30
  !
 !
 class class-default
```

```
  set traffic-class 0
  set dscp 0
  police rate percent 100
  !
 !
 end-policy-map
```

Egress H-QoS parent policy (Priority levels)

```
policy-map hqos-egress-parent-4g-priority
 class class-default
  service-policy hqos-egress-child-priority
  shape average 4 gbps
 !
 end-policy-map
!
```

Egress H-QoS child using priority only

In this policy all classes can access 100% of the bandwidth, queues are services based on priority level. The lower priority level has preference.

```
policy-map hqos-egress-child-priority
 class match-traffic-class-2
  shape average percent 100
  priority level 2
 !
 class match-traffic-class-3
  shape average percent 100
  priority level 3
 !
 class match-traffic-class-6
  priority level 4
  shape average percent 100
 !
 class class-default
 !
 end-policy-map
```

Egress H-QoS child using reserved bandwidth

In this policy each class is reserved a certain percentage of bandwidth. Each class may utilize up to 100% of the bandwidth, if traffic exceeds the guaranteed bandwidth it is eligible for drop.

```
policy-map hqos-egress-child-bw
 class match-traffic-class-2
  bandwidth remaining percent 30
 !
 class match-traffic-class-3
  bandwidth remaining percent 30
 !
 class match-traffic-class-6
  bandwidth remaining percent 30
 !
 class class-default
  bandwidth remaining percent 10
 !
 end-policy-map
```

Egress H-QoS child using shaping

In this policy each class is shaped to a defined amount and cannot exceed the defined bandwidth.

```
policy-map hqos-egress-child-shaping
 class match-traffic-class-2
  shape average percent 30
 !
 class match-traffic-class-3
  shape average percent 30
 !
 class match-traffic-class-6
  shape average percent 30
 !
 class class-default
  shape average percent 10
 !
 end-policy-map
!
```

Services

End-To-End VPN Services

Service	Technology	Access Platform
L3VPN	MP-BGP VPNv4 ODN	ASR920
L2VPN P2P	EVPN-VPWS ODN • Single-Homed	NCS5501-SE
	Legacy EoMPLS (StaticPW) Preferred Path	NCS5501-SE ASR920

Figure 6: End-To-End Services Table

L3VPN MP-BGP VPNv4 On-Demand Next-Hop

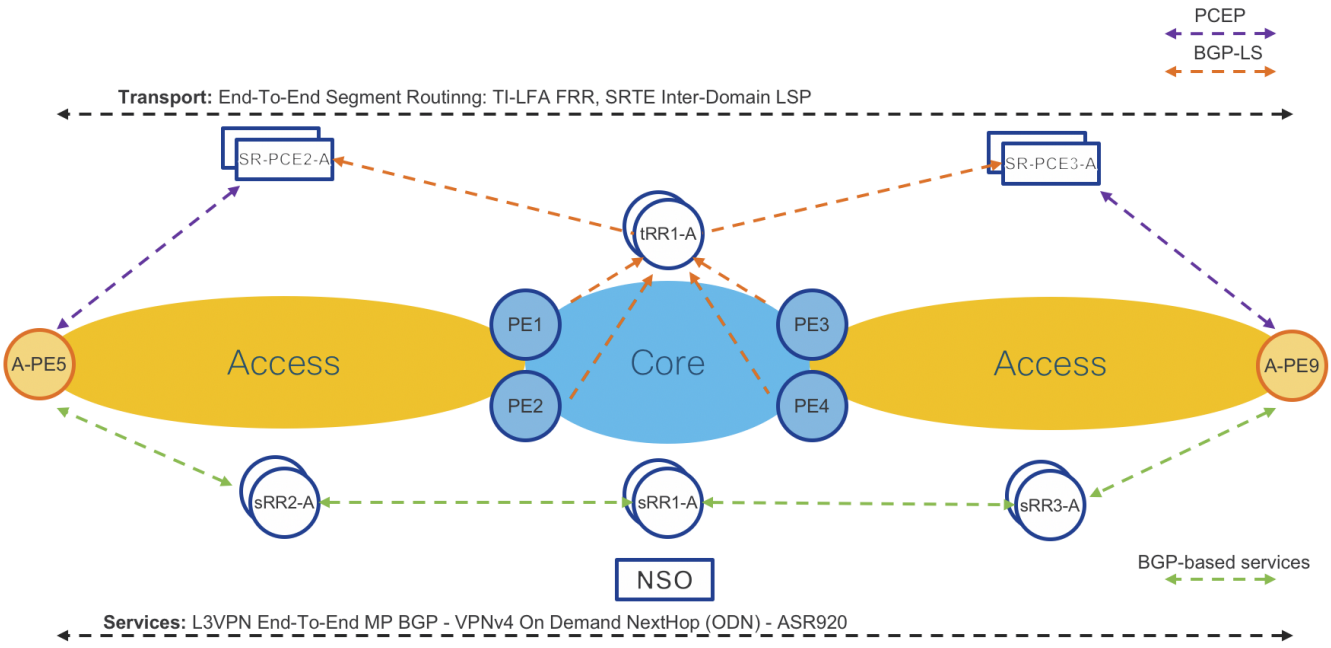


Figure 7: L3VPN MP-BGP VPNv4 On-Demand Next-Hop Control Plane

Access Routers: Cisco ASR920 IOS-XE and NCS540 IOS-XR

1. **Operator:** New VPNv4 instance via CLI or NSO
2. **Access Router:** Advertises/receives VPNv4 routes to/from Services Route-Reflector (sRR)
3. **Access Router**: Request SR-PCE to provide path (shortest IGP metric) to remote access router
4. **SR-PCE:** Computes and provides the path to remote router(s)
5. **Access Router:** Programs Segment Routing Traffic Engineering (SRTE) Policy to reach remote access router

Please refer to "**On Demand Next-Hop (ODN)**" sections for initial ODN configuration.

Access Router Service Provisioning (IOS-XR)

ODN route-policy configuration

```
extcommunity-set opaque ODN-GREEN
  100
end-set
```

route-policy ODN-L3VPN-OUT set extcommunity color ODN-GREEN pass end-policy

VRF definition configuration

```
vrf ODN-L3VPN
 rd 100:1
 address-family ipv4 unicast
  import route-target
   100:1
  !
  export route-target
  export route-policy ODN-L3VPN-OUT
   100:1
  !
 !
 address-family ipv6 unicast
  import route-target
   100:1
  !
  export route-target
  export route-policy ODN-L3VPN-OUT
   100:1
  !
 !
```

VRF Interface configuration

```
interface TenGigE0/0/0/23.2000
 mtu 9216
 vrf ODN-L3VPN
 ipv4 address 172.106.1.1 255.255.255.0
 encapsulation dot1q 2000
```

BGP VRF configuration with static/connected only

```
router bgp 100
 vrf VRF-MLDP
  rd auto
  address-family ipv4 unicast
```

```
   redistribute connected
   redistribute static
  !
  address-family ipv6 unicast
   redistribute connected
   redistribute static
  !
```

Access Router Service Provisioning (IOS-XE)

VRF definition configuration

```
vrf definition L3VPN-SRODN-1
 rd 100:100
 route-target export 100:100
 route-target import 100:100
 address-family ipv4
 exit-address-family
```

VRF Interface configuration

```
interface GigabitEthernet0/0/2
 mtu 9216
 vrf forwarding L3VPN-SRODN-1
 ip address 10.5.1.1 255.255.255.0
 negotiation auto
end
```

**BGP VRF configuration Static & BGP neighbor **

Static routing configuration

```
router bgp 100
 address-family ipv4 vrf L3VPN-SRODN-1
  redistribute connected
 exit-address-family
```

BGP neighbor configuration

```
router bgp 100
 neighbor Customer-1 peer-group
 neighbor Customer-1 remote-as 200
 neighbor 10.10.10.1 peer-group Customer-1
 address-family ipv4 vrf L3VPN-SRODN-2
```

```
    neighbor 10.10.10.1 activate
  exit-address-family
```

L2VPN Single-Homed EVPN-VPWS On-Demand Next-Hop

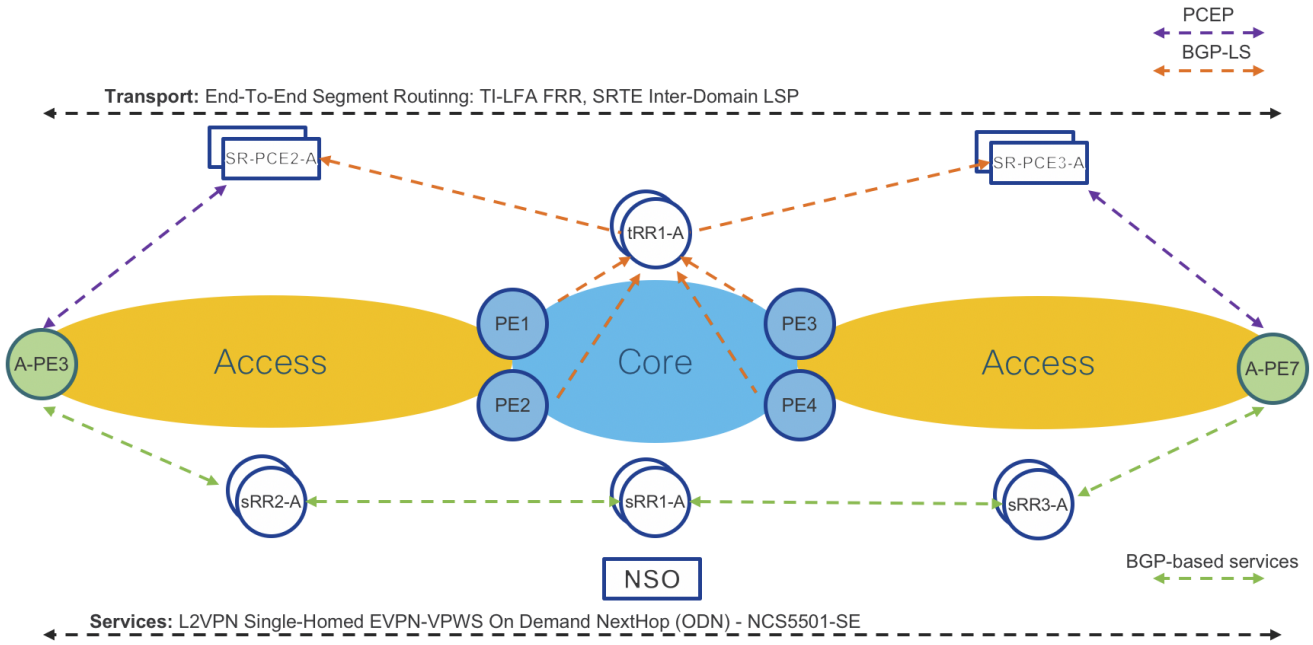


Figure 8: L2VPN Single-Homed EVPN-VPWS On-Demand Next-Hop Control Plane

Access Routers: Cisco NCS5501-SE IOS-XR

1. **Operator:** New EVPN-VPWS instance via CLI or NSO
2. **Access Router:** Advertises/receives EVPN-VPWS instance to/from Services Route-Reflector (sRR)
3. **Access Router**: Request SR-PCE to provide path (shortest IGP metric) to remote access router
4. **SR-PCE:** Computes and provides the path to remote router(s)
5. **Access Router:** Programs Segment Routing Traffic Engineering (SRTE) Policy to reach remote access router

Note: Please refer to **On Demand Next-Hop (ODN) – IOS-XR** section for initial ODN configuration. The correct EVPN L2VPN routes must be advertised with a specific color ext-community to trigger dynamic SR Policy instantiation.

Access Router Service Provisioning (IOS-XR):

Port based service configuration

```
l2vpn
xconnect group evpn_vpws
 p2p odn-1
```

```
  interface TenGigE0/0/0/5
   neighbor evpn evi 1000 target 1 source 1
```

interface TenGigE0/0/0/5 l2transport

VLAN Based service configuration

```
l2vpn
 xconnect group evpn_vpws
 p2p odn-1
  neighbor evpn evi 1000 target 1 source 1
  !
!
interface TenGigE0/0/0/5.1 l2transport
 encapsulation dot1q 1
 rewrite ingress tag pop 1 symmetric
!
```

L2VPN Static Pseudowire (PW) – Preferred Path (PCEP)

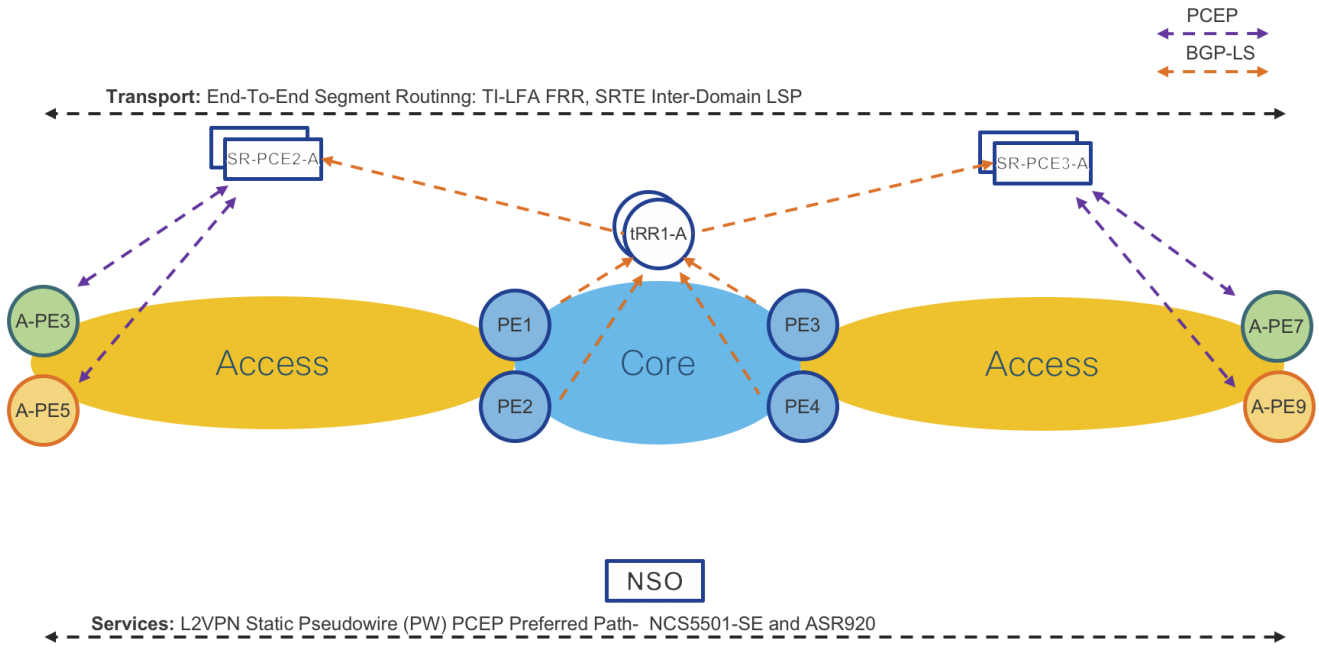


Figure 9: L2VPN Static Pseudowire (PW) – Preferred Path (PCEP) Control Plane

Access Routers: Cisco NCS5501-SE IOS-XR or Cisco ASR920 IOS-XE

1. **Operator:** New Static Pseudowire (PW) instance via CLI or NSO
2. **Access Router**: Request SR-PCE to provide path (shortest IGP metric) to remote access router
3. **SR-PCE:** Computes and provides the path to remote router(s)

4. **Access Router:** Programs Segment Routing Traffic Engineering (SRTE) Policy to reach remote access router

Access Router Service Provisioning (IOS-XR):

Note: EVPN VPWS dual homing is not supported when using an SR-TE preferred path.

Note: In IOS-XR 6.6.3 the SR Policy used as the preferred path must be referenced by its generated name and not the configured policy name. This requires first issuing the command

Define SR Policy

```
 traffic-eng
  policy GREEN-PE3-1
   color 1001 end-point ipv4 100.0.1.50
   candidate-paths
    preference 1
     dynamic
      pcep
      !
      metric
       type igp
```

Determine auto-configured policy name The auto-configured policy name will be persistant and must be used as a reference in the L2VPN preferred-path configuration.

```
RP/0/RP0/CPU0:A-PE8#show segment-routing traffic-eng policy candidate-path
name GREEN-PE3-1

SR-TE policy database
Color: 1001, End-point: 100.0.1.50
  Name: srte_c_1001_ep_100.0.1.50
```

Port Based Service configuration

```
interface TenGigE0/0/0/15
  l2transport
  !
!
l2vpn
 pw-class static-pw-class-PE3
  encapsulation mpls
   control-word
   preferred-path sr-te policy srte_c_1001_ep_100.0.1.50
   !
  !
 !
```

```
 p2p Static-PW-to-PE3-1
  interface TenGigE0/0/0/15
   neighbor ipv4 100.0.0.3 pw-id 1000
    mpls static label local 1000 remote 1000 pw-class static-pw-class-PE3
```

VLAN Based Service configuration

```
interface TenGigE0/0/0/5.1001 l2transport
 encapsulation dot1q 1001
 rewrite ingress tag pop 1 symmetric
 !
!
l2vpn
 pw-class static-pw-class-PE3
  encapsulation mpls
   control-word
   preferred-path sr-te policy srte_c_1001_ep_100.0.1.50
  p2p Static-PW-to-PE7-2
   interface TenGigE0/0/0/5.1001
    neighbor ipv4 100.0.0.3 pw-id 1001
     mpls static label local 1001 remote 1001 pw-class static-pw-class-PE3
```

Access Router Service Provisioning (IOS-XE):

Port Based service with Static OAM configuration

```
interface GigabitEthernet0/0/1
 mtu 9216
 no ip address
 negotiation auto
 no keepalive
 service instance 10 ethernet
  encapsulation default
  xconnect 100.0.2.54 100 encapsulation mpls manual pw-class mpls
   mpls label 100 100
   no mpls control-word
 !
 pseudowire-static-oam class static-oam
  timeout refresh send 10
  ttl 255
  !
 !
!
pseudowire-class mpls
 encapsulation mpls
 no control-word
 protocol none
 preferred-path interface Tunnel1
```

```
  status protocol notification static static-oam
 !
```

VLAN Based Service configuration

```
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 service instance 1 ethernet Static-VPWS-EVC
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  xconnect 100.0.2.54 100 encapsulation mpls manual pw-class mpls
   mpls label 100 100
   no mpls control-word
   !
  !
!
pseudowire-class mpls
 encapsulation mpls
 no control-word
 protocol none
 preferred-path interface Tunnel1
```

Ethernet CFM for L2VPN service assurance

Ethernet Connectivity Fault Management is an Ethernet OAM component used to validate end-to-end connectivity between service endpoints. Ethernet CFM is defined by two standards, 802.1ag and Y.1731. Within an SP network, Maintenance Domains are created based on service scope. Domains are typically separated by operator boundaries and may be nested but cannot overlap. Within each service, maintenance points can be created to verify bi-directional end to end connectivity. These are known as MEPs (Maintenance End-Point) and MIPs (Maintenance Intermediate Points). These maintenance points process CFM messages. A MEP is configured at service endpoints and has directionality where an "up" MEP faces the core of the network and a "down" MEP faces a CE device or NNI port. MIPs are optional and are created dynamically. Detailed information on Ethernet CFM configuration and operation can be found at https://www.cisco.com/c/en/us/td/docs/routers/ncs5500/software/interfaces/configuration/guide/b-interfaces-hardware-component-cg-ncs5500-66x/b-interfaces-hardware-component-cg-ncs5500-66x_chapter_0101.html

Maintenance Domain configuration

A Maintenance Domain is defined by a unique name and associated level. The level can be 0-7. The numerical identifier usually corresponds to the scope of the MD, where 7 is associated with CE endpoints, 6 associated with PE devices connected to a CE. Additional levels may be required based on the topology and service boundaries which occur along the end-to-end service. In this example we only a single domain and utilize level 0 for all MEPs.

```
ethernet cfm
 domain EVPN-VPWS-PE3-PE8 level 0
```

MEP configuration for EVPN-VPWS services

For L2VPN xconnect services, each service must have a MEP created on the end PE device. There are two components to defining a MEP, first defining the Ethernet CFM "service" and then defining the MEP on the physical or logical interface participating in the L2VPN xconnect service. In the following configuration the xconnect group "EVPN-VPWS-ODN-PE3" and P2P EVPN VPWS service odn-8 are already defined. The Ethernet CFM service of "odn-8" does NOT have to match the xconnect service name. The MEP crosscheck defines a remote MEP to listen for Continuity Check messages from. It does not have to be the same as the local MEP defined on the physical sub-interface (103), but for P2P services it is best practice to make them identical. This configuration will send Ethernet CFM Continuity Check (CC) messages every 1 minute to verify end to end reachability.

L2VPN configuration

```
l2vpn
 xconnect group EVPN-VPWS-ODN-PE3
  p2p odn-8
   interface TenGigE0/0/0/23.8
   neighbor evpn evi 1318 target 8 source 8
   !
  !
 !
!
```

Physical sub-interface configuration

```
interface TenGigE0/0/0/23.8 l2transport
 encapsulation dot1q 8
 rewrite ingress tag pop 1 symmetric
 ethernet cfm
  mep domain EVPN-VPWS-PE3-PE8 service odn-8 mep-id 103
  !
 !
!
```

Ethernet CFM service configuration

```
ethernet cfm
 domain EVPN-VPWS-PE3-PE8
  service odn-8 xconnect group EVPN-VPWS-ODN-PE3 p2p odn-8
   mip auto-create all
```

```
    continuity-check interval 1m
    mep crosscheck
     mep-id 103
    !
    log crosscheck errors
    log continuity-check errors
    log continuity-check mep changes
   !
  !
 !
```

Multicast NG-MVPN Profile 14 using mLDP and ODN L3VPN

In ths service example we will implement multicast delivery across the CST network using mLDP transport for multicast and SR-MPLS for unicast traffic. L3VPN SR paths will be dynamically created using ODN. Multicast profile 14 is the "Partitioned MDT - MLDP P2MP - BGP-AD - BGP C-Mcast Signaling" Using this profile each mVPN will use a dedicated P2MP tree, endpoints will be auto-discovered using NG-MVPN BGP NLRI, and customer multicast state such as source streams, PIM, and IGMP membership data will be signaled using BGP. Profile 14 is the recommended profile for high scale and utilizing label-switched multicast (LSM) across the core.

Multicast core configuration

The multicast "core" includes transit endpoints participating in mLDP only. See the mLDP core configuration section for details on end-to-end mLDP configuration.

Unicast L3VPN PE configuration

In order to complete an RPF check for SSM sources, unicast L3VPN configuration is required. Additionally the VRF must be defined under the BGP configuration with the NG-MVPN address families configured. In our use case we are utilizing ODN for creating the paths between L3VPN endpoints with a route-policy attached to the mVPN VRF to set a specific color on advertised routes.

ODN opaque ext-community set

```
extcommunity-set opaque MLDP
  1000
end-set
```

ODN route-policy

```
route-policy ODN-MVPN
  set extcommunity color MLDP
  pass
end-policy
```

Global L3VPN VRF definition

```
vrf VRF-MLDP
 address-family ipv4 unicast
  import route-target
   100:38
  !
  export route-policy ODN-MVPN
  export route-target
   100:38
  !
 !
 address-family ipv6 unicast
  import route-target
   100:38
  !
  export route-policy ODN-MVPN
  export route-target
   100:38
  !
 !
!
```

BGP configuration

```
router bgp 100
 vrf VRF-MLDP
  rd auto
  address-family ipv4 unicast
   redistribute connected
   redistribute static
  !
  address-family ipv6 unicast
   redistribute connected
   redistribute static
  !
  address-family ipv4 mvpn
  !
  address-family ipv6 mvpn
  !
 !
!
```

Multicast PE configuration

The multicast "edge" includes all endpoints connected to native multicast sources or receivers.

Define RPF policy

```
route-policy mldp-partitioned-p2mp
  set core-tree mldp-partitioned-p2mp
end-policy
!
```

Enable Multicast and define mVPN VRF

```
multicast-routing
 address-family ipv4
  interface Loopback0
   enable
  !
 !
 vrf VRF-MLDP
  address-family ipv4
   mdt source Loopback0
   rate-per-route
   interface all enable
   accounting per-prefix
   bgp auto-discovery mldp
   !
   mdt partitioned mldp ipv4 p2mp
   mdt data 100
  !
 !
!
```

Enable PIM for mVPN VRF In this instance there is an interface TenGigE0/0/0/23.2000 which is using PIM within the VRF

```
router pim
 address-family ipv4
  rp-address 100.0.1.50
 !
 vrf VRF-MLDP
  address-family ipv4
   rpf topology route-policy mldp-partitioned-p2mp
   mdt c-multicast-routing bgp
   !
   interface TenGigE0/0/0/23.2000
    enable
   !
  !
```

Enable IGMP for mVPN VRF interface To discover listeners for a specific group, enable IGMP on interfaces within the VRF. These interested receivers will be advertised via BGP to establish end to end P2MP trees from the

source.

```
router igmp
 vrf VRF-MLDP
  interface TenGigE0/0/0/23.2001
  !
  version 3
 !
!
```

End-To-End VPN Services Data Plane

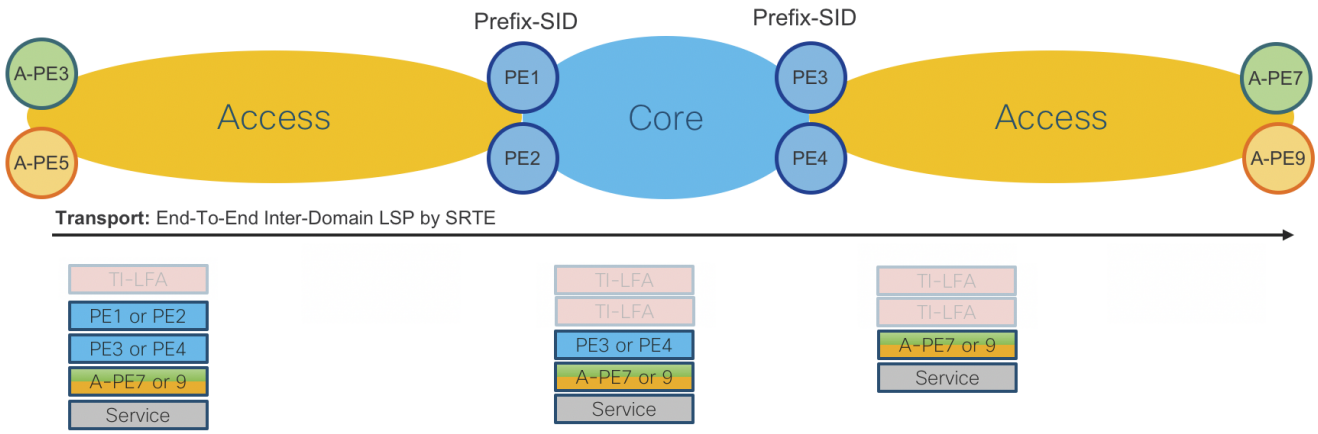


Figure 10: End-To-End Services Data Plane

Hierarchical Services

Service	Technology in Access	Technology in Core	Access Platform
L3VPN	EVPN-VPWS • Single-Homed	MP-BGP VPNv4/6 PWHE	NCS5501-SE ASR920
	Anycast StaticPW PE ABRs Anycast-SID required	MP-BGP VPNv4 Anycast IRB EVPN multichassis CP required	NCS5501-SE ASR920
L2/L3VPN Multipoint	Anycast-Static-PW PE ABRs Anycast-SID required	EVPN • Multi-Homed • All-Active Anycast IRB (optional)	NCS5501-SE ASR920

Figure 11: Hierarchical Services Table

L3VPN – Single-Homed EVPN-VPWS, MP-BGP VPNv4/6 with Pseudowire-Headend (PWHE)

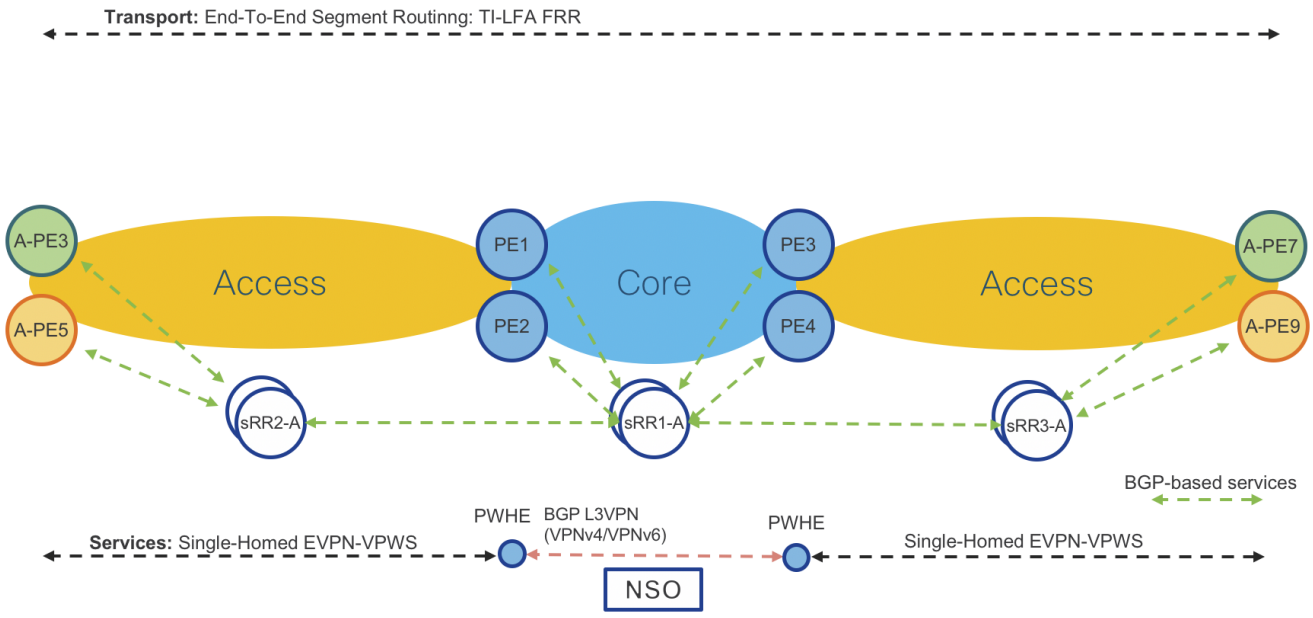


Figure 12: L3VPN – Single-Homed EVPN-VPWS, MP-BGP VPNv4/6 with Pseudowire-Headend (PWHE) Control Plane

Access Routers: Cisco NCS5501-SE IOS-XR or Cisco ASR920 IOS-XE

1. **Operator:** New EVPN-VPWS instance via CLI or NSO
2. **Access Router:** Path to PE Router is known via ACCESS-ISIS IGP.

Provider Edge Routers: Cisco ASR9000 IOS-XR

1. **Operator:** New EVPN-VPWS instance via CLI or NSO
2. **Provider Edge Router:** Path to Access Router is known via ACCESS-ISIS IGP.
3. **Operator:** New L3VPN instance (VPNv4/6) together with Pseudowire-Headend (PWHE) via CLI or NSO
4. **Provider Edge Router:** Path to remote PE is known via CORE-ISIS IGP.

Access Router Service Provisioning (IOS-XR):

VLAN based service configuration

```
l2vpn
 xconnect group evpn-vpws-l3vpn-PE1
  p2p L3VPN-VRF1
   interface TenGigE0/0/0/5.501
   neighbor evpn evi 13 target 501 source 501
   !
  !
 !
interface TenGigE0/0/0/5.501 l2transport
 encapsulation dot1q 501
 rewrite ingress tag pop 1 symmetric
```

Port based service configuration

```
l2vpn
 xconnect group evpn-vpws-l3vpn-PE1
 p2p odn-1
  interface TenGigE0/0/0/5
   neighbor evpn evi 13 target 502 source 502
   !
  !
 !
!
interface TenGigE0/0/0/5
  l2transport
```

Access Router Service Provisioning (IOS-XE):

VLAN based service configuration

```
l2vpn evpn instance 14 point-to-point
 vpws context evpn-pe4-pe1
  service target 501 source 501
  member GigabitEthernet0/0/1 service-instance 501
 !
interface GigabitEthernet0/0/1
 service instance 501 ethernet
  encapsulation dot1q 501
  rewrite ingress tag pop 1 symmetric
 !
```

Port based service configuration

```
l2vpn evpn instance 14 point-to-point
 vpws context evpn-pe4-pe1
  service target 501 source 501
  member GigabitEthernet0/0/1 service-instance 501
 !
interface GigabitEthernet0/0/1
 service instance 501 ethernet
  encapsulation default
```

Provider Edge Router Service Provisioning (IOS-XR):

VRF configuration

```
vrf L3VPN-ODNTE-VRF1
 address-family ipv4 unicast
  import route-target
   100:501
  !
  export route-target
   100:501
  !
 !
 address-family ipv6 unicast
  import route-target
   100:501
  !
  export route-target
   100:501
  !
 !
```

BGP configuration

```
router bgp 100
 vrf L3VPN-ODNTE-VRF1
  rd 100:501
  address-family ipv4 unicast
   redistribute connected
  !
  address-family ipv6 unicast
   redistribute connected
  !
 !
```

PWHE configuration

```
interface PW-Ether1
 vrf L3VPN-ODNTE-VRF1
 ipv4 address 10.13.1.1 255.255.255.0
 ipv6 address 1000:10:13::1/126
 attach generic-interface-list PWHE
!
```

EVPN VPWS configuration towards Access PE

```
l2vpn
 xconnect group evpn-vpws-l3vpn-A-PE3
  p2p L3VPN-ODNTE-VRF1
```

```
    interface PW-Ether1
    neighbor evpn evi 13 target 501 source 501
    !
```

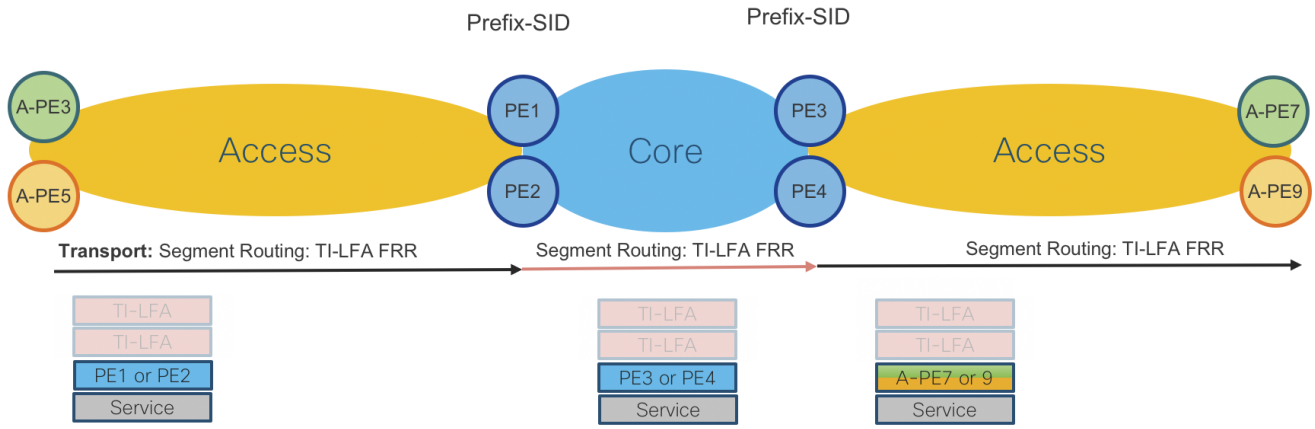


Figure 13: L3VPN – Single-Homed EVPN-VPWS, MP-BGP VPNv4/6 with Pseudowire-Headend (PWHE) Data Plane

L3VPN – Anycast Static Pseudowire (PW), MP-BGP VPNv4 with Anycast IRB

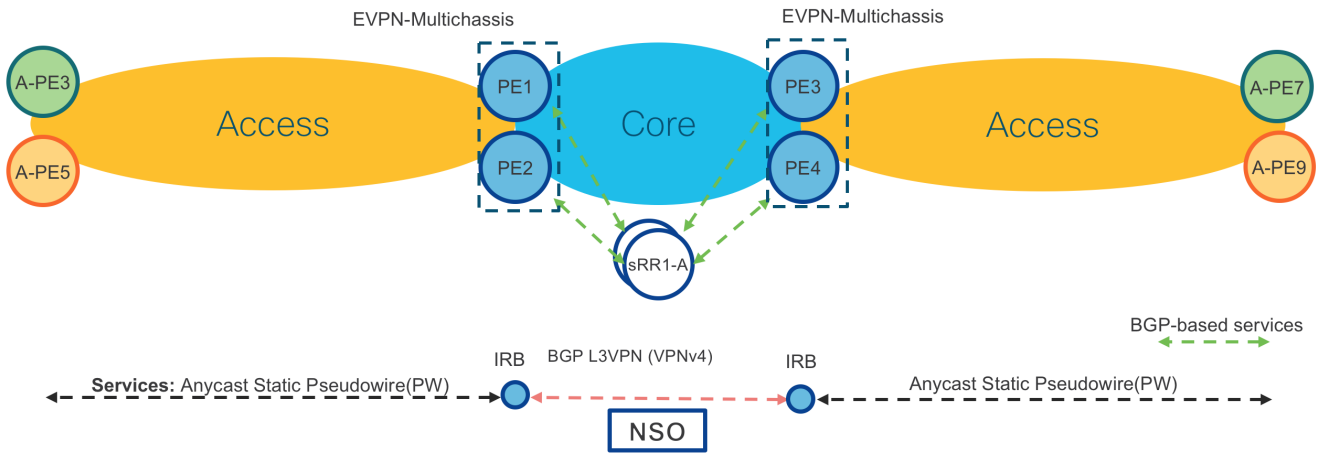


Figure 14: L3VPN – Anycast Static Pseudowire (PW), MP-BGP VPNv4 with Anycast IRB Control Plane

Access Routers: Cisco NCS5501-SE IOS-XR or Cisco ASR920 IOS-XE

3. **Operator:** New Static Pseudowire (PW) instance via CLI or NSO
4. **Access Router:** Path to PE Router is known via ACCESS-ISIS IGP.

Provider Edge Routers: Cisco ASR9000 IOS-XR (Same on both PE routers in same location PE1/2 and PE3/4)

5. **Operator:** New Static Pseudowire (PW) instance via CLI or NSO
6. **Provider Edge Routers:** Path to Access Router is known via ACCESS-ISIS IGP.

7. **Operator:** New L3VPN instance (VPNv4/6) together with Anycast IRB via CLI or NSO
8. **Provider Edge Routers:** Path to remote PEs is known via CORE-ISIS IGP.

Access Router Service Provisioning (IOS-XR):

VLAN based service configuration

```
l2vpn
 xconnect group Static-VPWS-PE12-H-L3VPN-AnyCast
  p2p L3VPN-VRF1
   interface TenGigE0/0/0/2.1
   neighbor ipv4 100.100.100.12 pw-id 5001
    mpls static label local 5001 remote 5001
    pw-class static-pw-h-l3vpn-class
   !
  !
interface TenGigE0/0/0/2.1 l2transport
 encapsulation dot1q 1
 rewrite ingress tag pop 1 symmetric
 !
!
l2vpn
 pw-class static-pw-h-l3vpn-class
  encapsulation mpls
   control-word
  !
```

Port based service configuration

```
l2vpn
 xconnect group Static-VPWS-PE12-H-L3VPN-AnyCast
  p2p L3VPN-VRF1
   interface TenGigE0/0/0/2
   neighbor ipv4 100.100.100.12 pw-id 5001
    mpls static label local 5001 remote 5001
    pw-class static-pw-h-l3vpn-class
   !
  !
interface TenGigE0/0/0/2
 l2transport
 !
!
l2vpn
 pw-class static-pw-h-l3vpn-class
  encapsulation mpls
   control-word
  !
```

Access Router Service Provisioning (IOS-XE):

VLAN based service configuration

```
interface GigabitEthernet0/0/5
 no ip address
 media-type auto-select
 negotiation auto
 service instance 1 ethernet
  encapsulation dot1q 1
  rewrite ingress tag pop 1 symmetric
  xconnect 100.100.100.12 4001 encapsulation mpls manual
   mpls label 4001 4001
   mpls control-word
 !
```

Port based service configuration

```
interface GigabitEthernet0/0/5
 no ip address
 media-type auto-select
 negotiation auto
 service instance 1 ethernet
  encapsulation default
  xconnect 100.100.100.12 4001 encapsulation mpls manual
   mpls label 4001 4001
   mpls control-word
 !
```

Provider Edge Routers Service Provisioning (IOS-XR):

```
cef adjacency route override rib
```

AnyCast Loopback configuration

```
interface Loopback100
 description Anycast
 ipv4 address 100.100.100.12 255.255.255.255
!
router isis ACCESS
 interface Loopback100
 address-family ipv4 unicast
  prefix-sid index 1012 n-flag-clear
```

L2VPN configuration

```
l2vpn
 bridge group Static-VPWS-H-L3VPN-IRB
  bridge-domain VRF1
   neighbor 100.0.1.50 pw-id 5001
    mpls static label local 5001 remote 5001
    pw-class static-pw-h-l3vpn-class
   !
   neighbor 100.0.1.51 pw-id 4001
    mpls static label local 4001 remote 4001
    pw-class static-pw-h-l3vpn-class
   !
   routed interface BVI1
    split-horizon group core
   !
   evi 12001
   !
  !
```

EVPN configuration

```
evpn
 evi 12001
 !
  advertise-mac
 !
 virtual neighbor 100.0.1.50 pw-id 5001
  ethernet-segment
   identifier type 0 12.00.00.00.00.00.50.00.01
```

Anycast IRB configuration

```
interface BVI1
 host-routing
 vrf L3VPN-AnyCast-ODNTE-VRF1
 ipv4 address 12.0.1.1 255.255.255.0
 mac-address 12.0.1
 load-interval 30
```

VRF configuration

```
vrf L3VPN-AnyCast-ODNTE-VRF1
 address-family ipv4 unicast
  import route-target
```

```
    100:10001
   !
   export route-target
    100:10001
   !
  !
 !
```

BGP configuration

```
router bgp 100
 vrf L3VPN-AnyCast-ODNTE-VRF1
  rd auto
  address-family ipv4 unicast
   redistribute connected
  !
 !
```

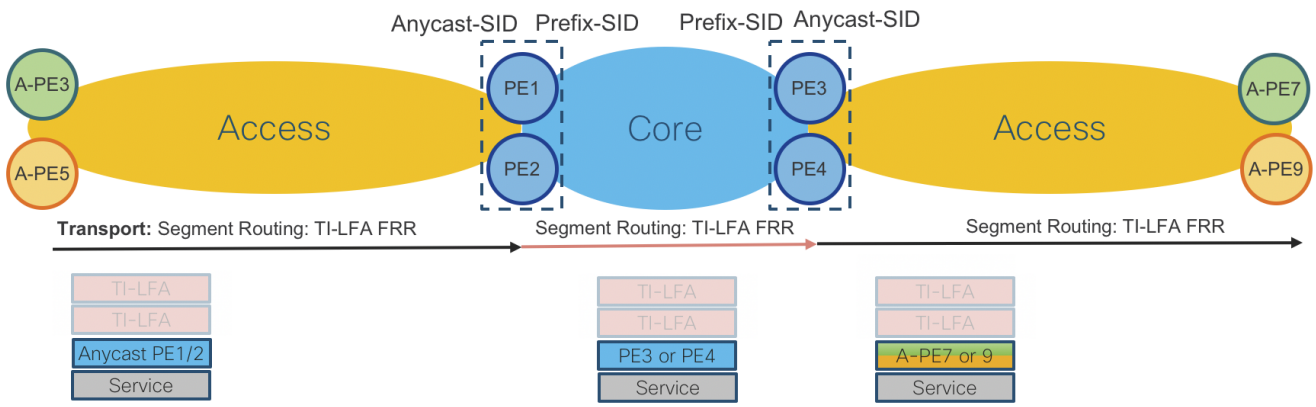


Figure 15: L3VPN – Anycast Static Pseudowire (PW), MP-BGP VPNv4/6 with Anycast IRB Datal Plane

L2/L3VPN – Anycast Static Pseudowire (PW), Multipoint EVPN with Anycast IRB

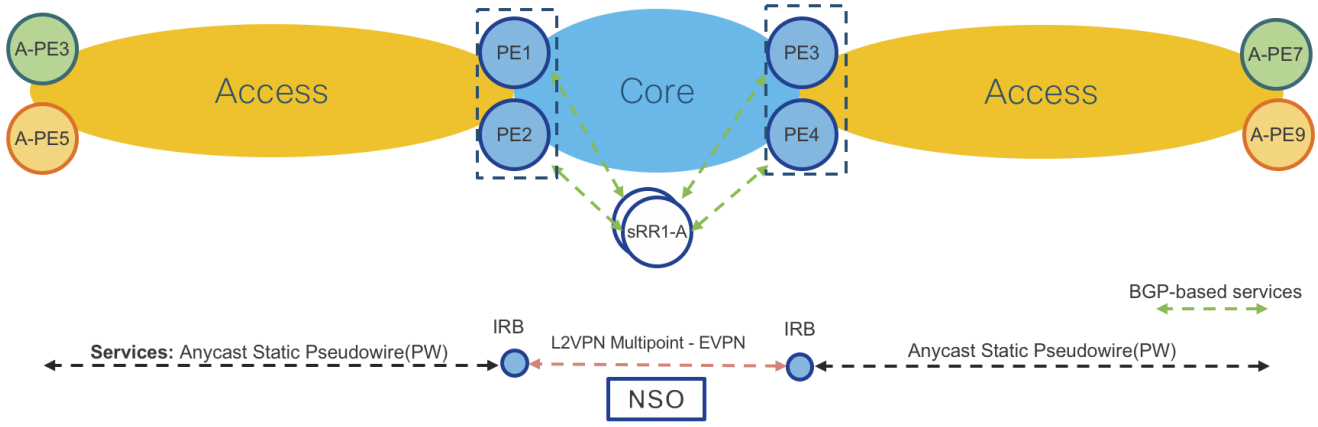


Figure 16: L2/L3VPN – Anycast Static Pseudowire (PW), Multipoint EVPN with Anycast IRB Control Plane

Access Routers: Cisco NCS5501-SE IOS-XR or Cisco ASR920 IOS-XE

5. **Operator:** New Static Pseudowire (PW) instance via CLI or NSO
6. **Access Router:** Path to PE Router is known via ACCESS-ISIS IGP.

Provider Edge Routers: Cisco ASR9000 IOS-XR (Same on both PE routers in same location PE1/2 and PE3/4)

7. **Operator:** New Static Pseudowire (PW) instance via CLI or NSO
8. **Provider Edge Routers:** Path to Access Router is known via ACCESS-ISIS IGP.
9. **Operator:** New L2VPN Multipoint EVPN instance together with Anycast IRB via CLI or NSO (Anycast IRB is optional when L2 and L3 is required in same service instance)
10. **Provider Edge Routers:** Path to remote PEs is known via CORE-ISIS IGP.

Please note that provisioning on Access and Provider Edge routers is same as in "L3VPN – Anycast Static Pseudowire (PW), MP-BGP VPNv4/6 with Anycast IRB". In this use case there is BGP EVPN instead of MP-BGP VPNv4/6 in the core.

Access Router Service Provisioning (IOS-XR):

VLAN based service configuration

```
l2vpn
 xconnect group Static-VPWS-PE12-H-L3VPN-AnyCast
  p2p L3VPN-VRF1
   interface TenGigE0/0/0/2.1
   neighbor ipv4 100.100.100.12 pw-id 5001
    mpls static label local 5001 remote 5001
    pw-class static-pw-h-l3vpn-class
   !
  !
interface TenGigE0/0/0/2.1 l2transport
 encapsulation dot1q 1
 rewrite ingress tag pop 1 symmetric
!
l2vpn
 pw-class static-pw-h-l3vpn-class
  encapsulation mpls
   control-word
  !
```

Port based service configuration

```
l2vpn
 xconnect group Static-VPWS-PE12-H-L3VPN-AnyCast
  p2p L3VPN-VRF1
   interface TenGigE0/0/0/2
   neighbor ipv4 100.100.100.12 pw-id 5001
    mpls static label local 5001 remote 5001
    pw-class static-pw-h-l3vpn-class
   !
  !
!
interface TenGigE0/0/0/2
 l2transport
!
l2vpn
 pw-class static-pw-h-l3vpn-class
  encapsulation mpls
   control-word
```

Access Router Service Provisioning (IOS-XE):

VLAN based service configuration

```
interface GigabitEthernet0/0/5
 no ip address
 media-type auto-select
 negotiation auto
 service instance 1 ethernet
  encapsulation dot1q 1
  rewrite ingress tag pop 1 symmetric
  xconnect 100.100.100.12 4001 encapsulation mpls manual
   mpls label 4001 4001
   mpls control-word
 !
```

Port based service configuration

```
interface GigabitEthernet0/0/5
 no ip address
 media-type auto-select
 negotiation auto
 service instance 1 ethernet
  encapsulation default
  xconnect 100.100.100.12 4001 encapsulation mpls manual
   mpls label 4001 4001
   mpls control-word
 !
```

Provider Edge Routers Service Provisioning (IOS-XR):

```
cef adjacency route override rib
```

AnyCast Loopback configuration

```
interface Loopback100
 description Anycast
 ipv4 address 100.100.100.12 255.255.255.255
!
router isis ACCESS
 interface Loopback100
  address-family ipv4 unicast
   prefix-sid index 1012
```

L2VPN Configuration

```
l2vpn
 bridge group Static-VPWS-H-L3VPN-IRB
  bridge-domain VRF1
   neighbor 100.0.1.50 pw-id 5001
    mpls static label local 5001 remote 5001
    pw-class static-pw-h-l3vpn-class
   !
   neighbor 100.0.1.51 pw-id 4001
    mpls static label local 4001 remote 4001
    pw-class static-pw-h-l3vpn-class
   !
   routed interface BVI1
    split-horizon group core
   !
   evi 12001
   !
  !
```

EVPN configuration

```
evpn
 evi 12001
  !
  advertise-mac
  !
 !
 virtual neighbor 100.0.1.50 pw-id 5001
```

```
  ethernet-segment
   identifier type 0 12.00.00.00.00.00.50.00.01
```

Anycast IRB configuration

```
interface BVI1
 host-routing
 vrf L3VPN-AnyCast-ODNTE-VRF1
 ipv4 address 12.0.1.1 255.255.255.0
 mac-address 12.0.1
 load-interval 30
!
```

VRF configuration

```
vrf L3VPN-AnyCast-ODNTE-VRF1
 address-family ipv4 unicast
  import route-target
   100:10001
  !
  export route-target
   100:10001
  !
 !
!
```

BGP configuration

```
router bgp 100
 vrf L3VPN-AnyCast-ODNTE-VRF1
  rd auto
  address-family ipv4 unicast
   redistribute connected
  !
 !
```

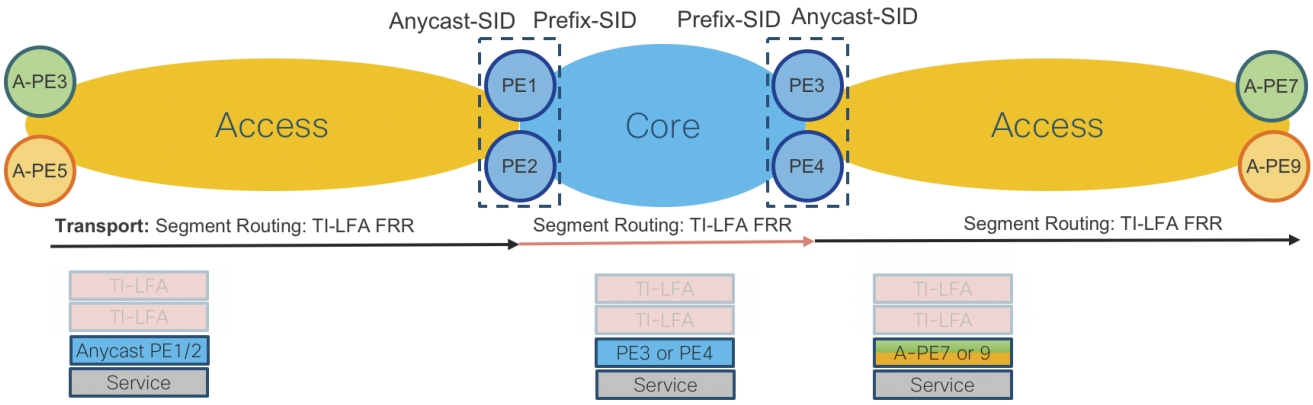


Figure 17: L2/L3VPN – Anycast Static Pseudowire (PW), Multipoint EVPN with Anycast IRB Data Plane

Remote PHY CIN Implementation

Summary

Detail can be found in the CST 3.0 high-level design guide for design decisions, this section will provide sample configurations.

Sample QoS Policies

The following are usable policies but policies should be tailored for specific network deployments.

Class maps

Class maps are used within a policy map to match packet criteria for further treatment

```
class-map match-any match-ef-exp5
 description High priority, EF
 match dscp 46
 match mpls experimental topmost 5
 end-class-map
!
class-map match-any match-cs5-exp4
 description Second highest priority
 match dscp 40
 match mpls experimental topmost 4
 end-class-map
!
class-map match-any match-video-cs4-exp2
 description Video
 match dscp 32
 match mpls experimental topmost 2
 end-class-map
!
class-map match-any match-cs6-exp6
 description Highest priority control-plane traffic
 match dscp cs6
```

```
 match mpls experimental topmost 6
 end-class-map
!
class-map match-any match-qos-group-1
 match qos-group 1
 end-class-map
!
class-map match-any match-qos-group-2
 match qos-group 2
 end-class-map
!
class-map match-any match-qos-group-3
 match qos-group 3
 end-class-map
!
class-map match-any match-qos-group-6
 match qos-group 3
 end-class-map
!
class-map match-any match-traffic-class-1
 description "Match highest priority traffic-class 1"
 match traffic-class 1
 end-class-map
!
class-map match-any match-traffic-class-2
 description "Match high priority traffic-class 2"
 match traffic-class 2
 end-class-map
!
class-map match-any match-traffic-class-3
 description "Match medium traffic-class 3"
 match traffic-class 3
 end-class-map
!
class-map match-any match-traffic-class-6
 description "Match video traffic-class 6"
 match traffic-class 6
 end-class-map
```

RPD and DPIC interface policy maps

These are applied to all interfaces connected to cBR-8 DPIC and RPD devices.

Note: Egress queueing maps are not supported on L3 BVI interfaces

RPD/DPIC ingress classifier policy map

```
policy-map rpd-dpic-ingress-classifier
 class match-cs6-exp6
  set traffic-class 1
```

```
  set qos-group 1
 !
 class match-ef-exp5
  set traffic-class 2
  set qos-group 2
 !
 class match-cs5-exp4
  set traffic-class 3
  set qos-group 3
 !
 class match-video-cs4-exp2
  set traffic-class 6
  set qos-group 6
 !
 class class-default
  set traffic-class 0
  set dscp 0
  set qos-group 0
 !
 end-policy-map
!
```

RPD/DPIC egress queueing policy map

```
policy-map rpd-dpic-egress-queuing
 class match-traffic-class-1
  priority level 1
  queue-limit 500 us
 !
 class match-traffic-class-2
  priority level 2
  queue-limit 100 us
 !
 class match-traffic-class-3
  priority level 3
  queue-limit 500 us
 !
 class match-traffic-class-6
  priority level 6
  queue-limit 500 us
 !
 class class-default
  queue-limit 250 ms
 !
 end-policy-map
!
```

Core QoS

Please see the general QoS section for core-facing QoS configuration

Multicast configuration

Global multicast configuration - Native multicast

On CIN aggregation nodes all interfaces should have multicast enabled.

```
multicast-routing
 address-family ipv4
  interface all enable
 !
 address-family ipv6
  interface all enable
   enable
 !
```

PIM configuration - Native multicast

PIM should be enabled for IPv4/IPv6 on all core facing interfaces

```
router pim
 address-family ipv4
  interface Loopback0
   enable
  !
  interface TenGigE0/0/0/6
   enable
  !
  interface TenGigE0/0/0/7
   enable
  !
 !
```

IGMPv3/MLDv2 configuration - Native multicast

Interfaces connected to RPD and DPIC interfaces should have IGMPv3 and MLDv2 enabled

```
router igmp
 interface BVI100
  version 3
 !
 interface TenGigE0/0/0/25
  version 3
 !
!
```

```
router mld
 interface BVI100
  version 2
 interface TenGigE0/0/0/25
  version 3
 !
 !
```

IGMPv3 / MLDv2 snooping profile configuration (BVI aggregation)

In order to limit L2 multicast replication for specific groups to only interfaces with interested receivers, IGMP and MLD snooping must be enabled.

```
igmp snooping profile igmp-snoop-1
!
mld snooping profile mld-snoop-1
!
```

RPD DHCPv4/v6 relay configuration

In order for RPDs to self-provision DHCP relay must be enabled on all RPD-facing L3 interfaces. In IOS-XR the DHCP relay configuration is done in its own configuration context without any configuration on the interface itself.

```
dhcp ipv4
 profile rpd-dhcpv4 relay
  helper-address vrf default 4.4.9.100
  helper-address vrf default 10.0.2.3
 !
 interface BVI100 relay profile rpd-dhcpv4
 interface TenGigE0/0/0/15 relay profile rpd-dhcpv4
!
dhcp ipv6
 profile rpd-dhcpv6 relay
  helper-address vrf default 2001:10:0:2::3
  iana-route-add
  source-interface BVI100
 !
 interface BVI100 relay profile rpd-dhcpv6
 interface TenGigE0/0/0/15 relay profile rpd-dhcpv6
!
```

cBR-8 DPIC interface configuration without Link HA

Without link HA the DPIC port is configured as a normal physical interface

```
interface TenGigE0/0/0/25
 description .. Connected to cbr8 port te1/1/0
 service-policy input rpd-dpic-ingress-classifier
 service-policy output rpd-dpic-egress-queuing
 ipv4 address 4.4.9.101 255.255.255.0
 ipv6 address 2001:4:4:9::101/64
 carrier-delay up 0 down 0
 load-interval 30
```

cBR-8 DPIC interface configuration with Link HA

When using Link HA faster convergence is achieved when each DPIC interface is placed into a BVI with a statically assigned MAC address. Each DPIC interface is placed into a separate bridge-domain with a unique BVI L3 interface. The same MAC address should be utilized on all BVI interfaces. Convergence using BVI interfaces is <50ms, L3 physical interfaces is 1-2s.

Even DPIC port CIN interface configuration

```
interface TenGigE0/0/0/25
 description "Connected to cBR8 port Te1/1/0"
 lldp
 !
 carrier-delay up 0 down 0
 load-interval 30
 l2transport
 !
!
l2vpn
 bridge group cbr8
  bridge-domain port-ha-0
   interface TenGigE0/0/0/25
   !
   routed interface BVI500
   !
  !
 !
 interface BVI500
 description "BVI for cBR8 port HA, requires static MAC"
 service-policy input rpd-dpic-ingress-classifier
 ipv4 address 4.4.9.101 255.255.255.0
 ipv6 address 2001:4:4:9::101/64
 mac-address 8a.9698.64
 load-interval 30
!
```

Odd DPIC port CIN interface configuration

```
interface TenGigE0/0/0/26
 description "Connected to cBR8 port Te1/1/1"
 lldp
 !
 carrier-delay up 0 down 0
 load-interval 30
 l2transport
 !
!
l2vpn
 bridge group cbr8
  bridge-domain port-ha-1
   interface TenGigE0/0/0/26
   !
   routed interface BVI501
   !
  !
 !
 interface BVI501
 description "BVI for cBR8 port HA, requires static MAC"
 service-policy input rpd-dpic-ingress-classifier
 ipv4 address 4.4.9.101 255.255.255.0
 ipv6 address 2001:4:4:9::101/64
 mac-address 8a.9698.64
 load-interval 30
!
```

cBR-8 Digital PIC Interface Configuration

```
interface TenGigE0/0/0/25
 description .. Connected to cbr8 port te1/1/0
 service-policy input rpd-dpic-ingress-classifier
 service-policy output rpd-dpic-egress-queuing
 ipv4 address 4.4.9.101 255.255.255.0
 ipv6 address 2001:4:4:9::101/64
 carrier-delay up 0 down 0
 load-interval 30
```

RPD interface configuration

P2P L3

```
interface TeGigE0/0/0/15
 description To RPD-1
 service-policy input rpd-dpic-ingress-classifier
 ipv4 address 192.168.2.0 255.255.255.254
```

```
 ipv6 address 2001:192:168:2::0/127
 ipv6 enable
 !
```

BVI

```
l2vpn
 bridge group rpd
  bridge-domain rpd-1
   mld snooping profile mld-snoop-1
   igmp snooping profile igmp-snoop-1
   interface TenGigE0/0/0/15
   !
   interface TenGigE0/0/0/16
   !
   interface TenGigE0/0/0/17
   !
   routed interface BVI100
   !
   !
  !
 !
!
interface BVI100
 description ... to downstream RPD hosts
 service-policy input rpd-dpic-ingress-classifier
 ipv4 address 192.168.2.1 255.255.255.0
 ipv6 address 2001:192:168:2::1/64
 ipv6 enable
 !
```

RPD/DPIC agg device IS-IS configuration

The standard IS-IS configuration should be used on all core interfaces with the addition of specifying all DPIC and RPD connected as IS-IS passive interfaces. Using passive interfaces is preferred over redistributing connected routes. This configuration is needed for reachability between DPIC and RPDs across the CIN network.

```
router isis ACCESS
 interface TenGigE0/0/0/25
  passive
  address-family ipv4 unicast
  !
  address-family ipv6 unicast
```