Empowering Your Network with SDWAN OMP:

Path Optimization and Policy Insights use cases

Waqas Daar - Customer Success Specialist SDWAN/Thousand Eyes

BRKENT-3115

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.

“If you cannot explain it simply, you don’t understand it well enough.”

Who am I?

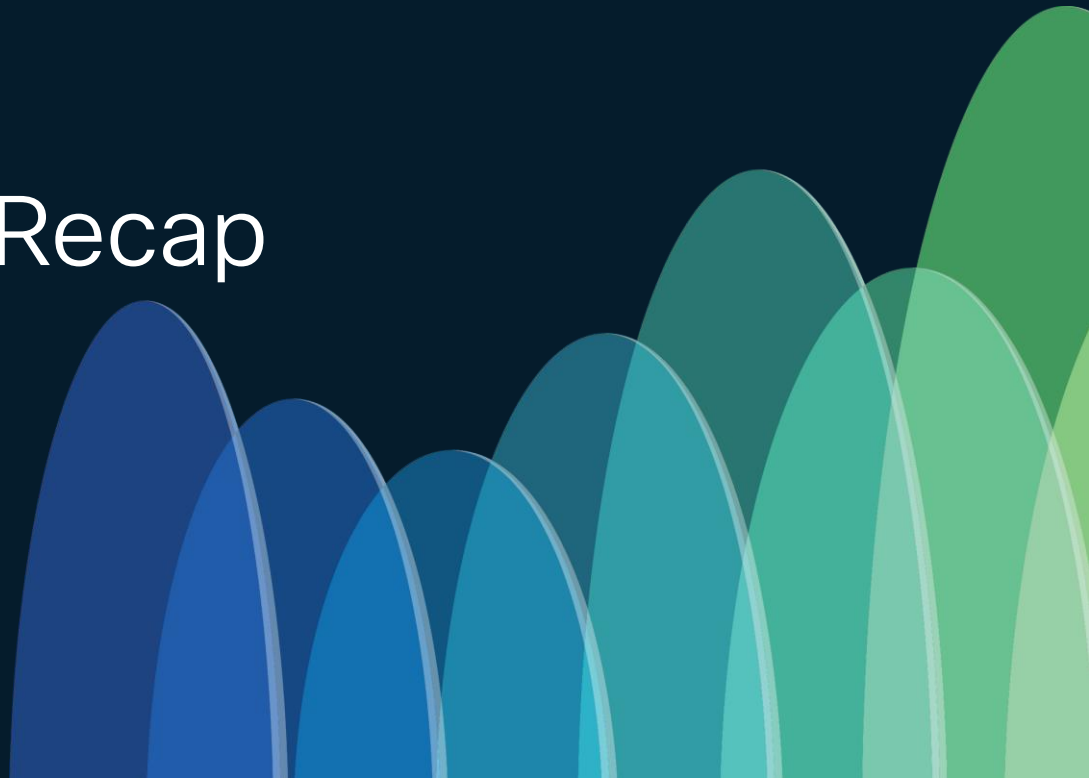
Agenda

- Part 1: SD-WAN OMP Peering Deep dive
  - Intro and OMP Quick overview
  - Demystifying OMP Peering
  - OMP Packet Insights and commonalities with BGP
  - Walkthrough of OMP Session establishment from the WAN Edge Process level
  - Navigating Through Logs During OMP Session Establishment
  - Troubleshooting OMP Peering
- Part 2: SD-WAN controller OMP deep dive
  - OMP Best path selection process
  - How OMP loop avoidance works
  - SD-WAN Controller: OMP Enhancements

Agenda

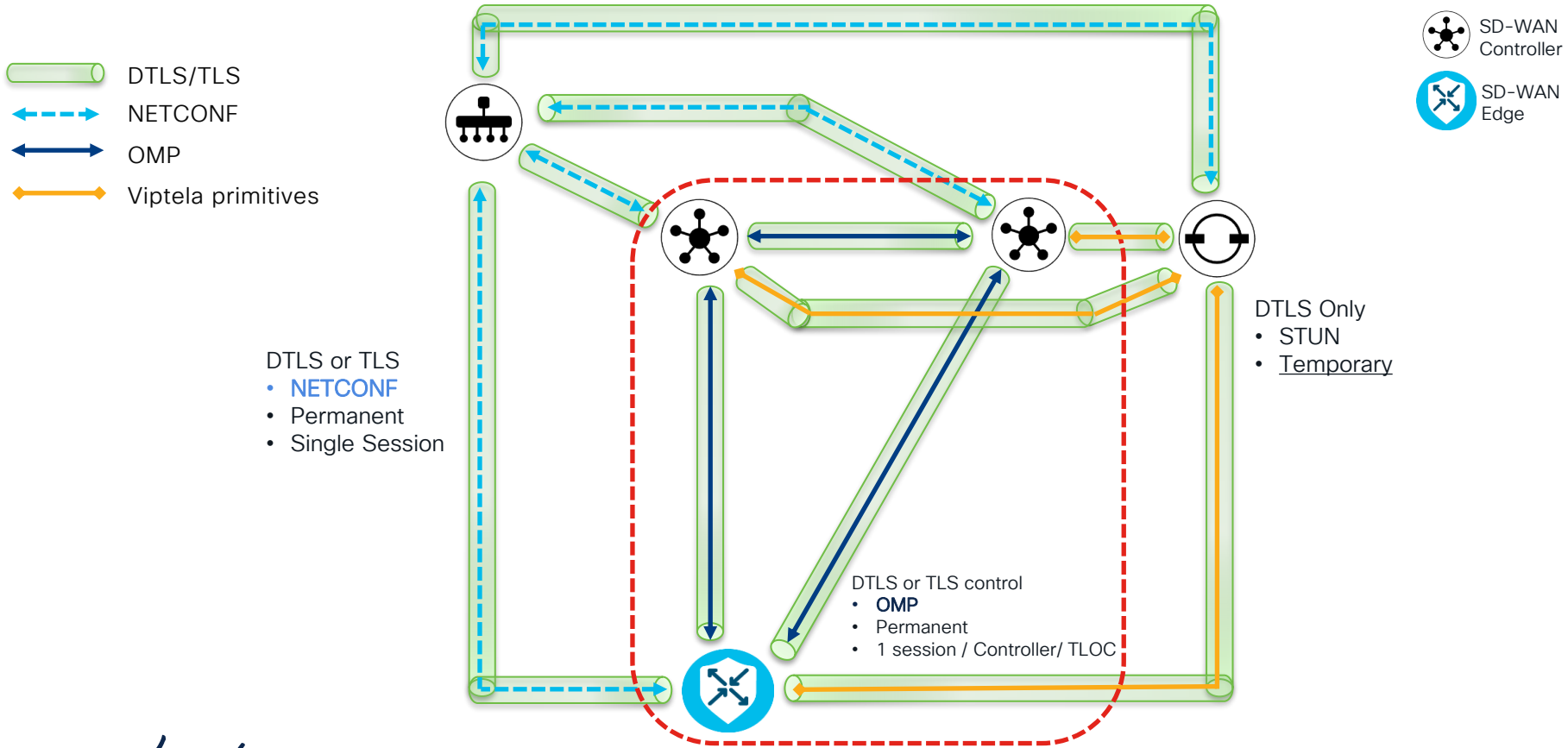
- Part 3: SD-WAN Multicast
  - How OMP build SD-WAN Multicast tree
- Part 4: SD-WAN Service Chaining and OMP
  - How OMP enables seamless service chaining

Quick SD-WAN Recap

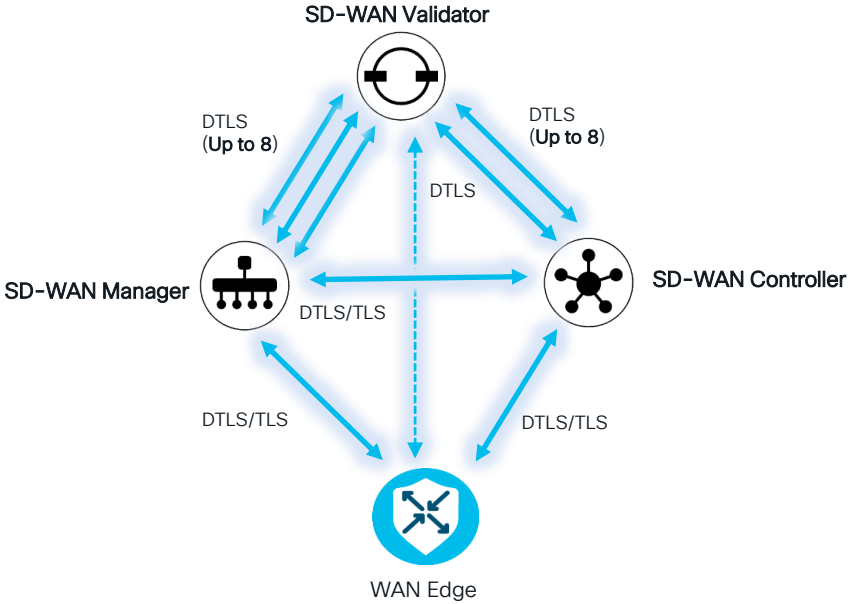


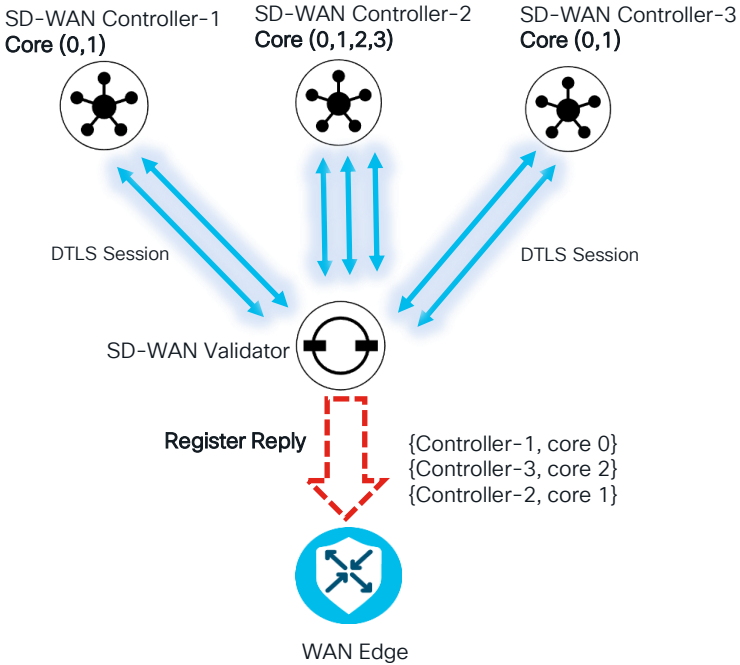
cisco Live!

Cisco SD-WAN Fabric overview



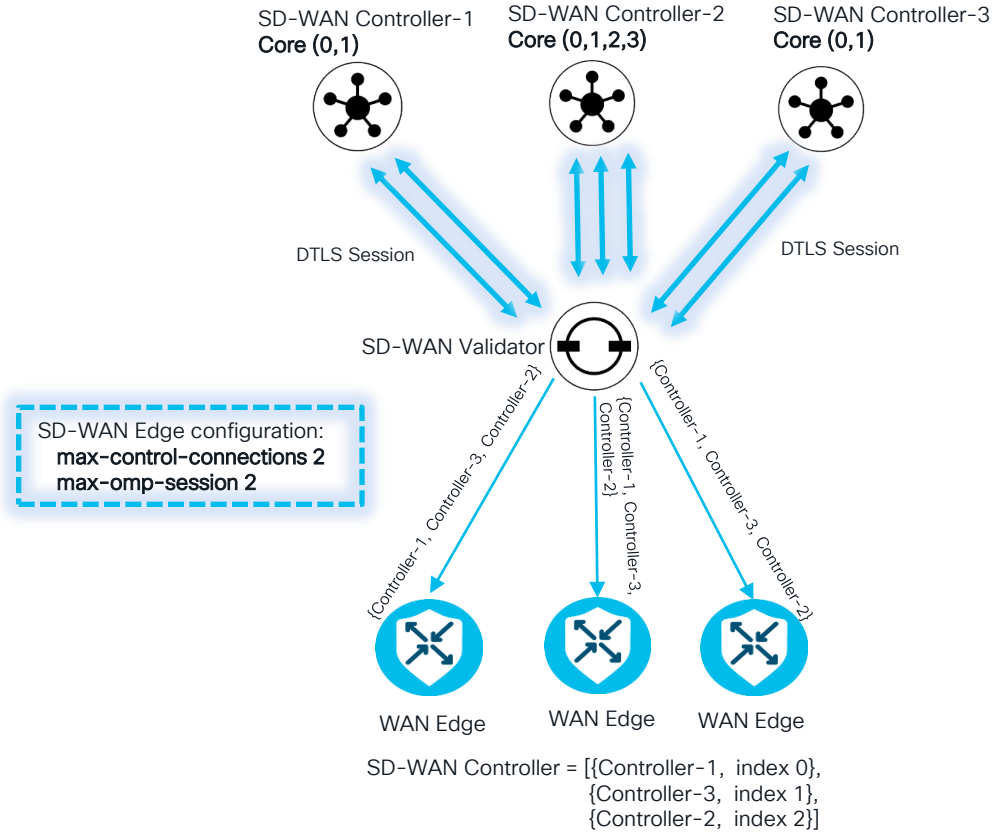
How SD-WAN Control Connections (CC) are established? 1/3



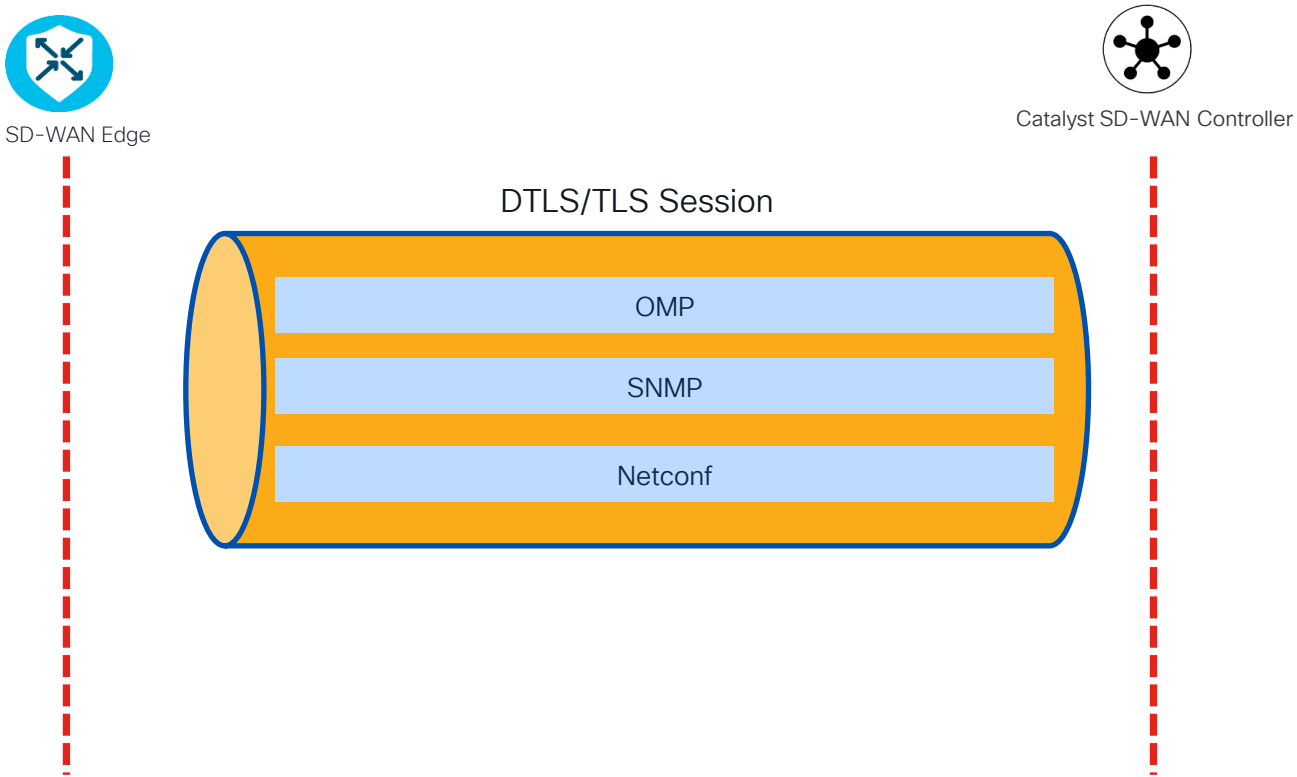


SD-WAN Controller = [{Controller-1, core 0, index 0},
{Controller-3, core 2, index 1},
{Controller-2, core 1, index 2}]

How SD-WAN Control Connections (CC) are established? 2/3

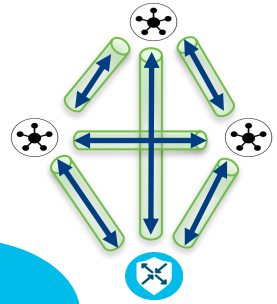


How SD-WAN Control Connections (CC) are established? 3/3



Overlay Management Protocol (OMP)

Overlay Management Protocol (OMP)



OMP is a path vector routing protocol derived from BGP.

OMP peering is established inside control connection (TLS/DTLS).
TCP as transport protocol with listening on port 17900.

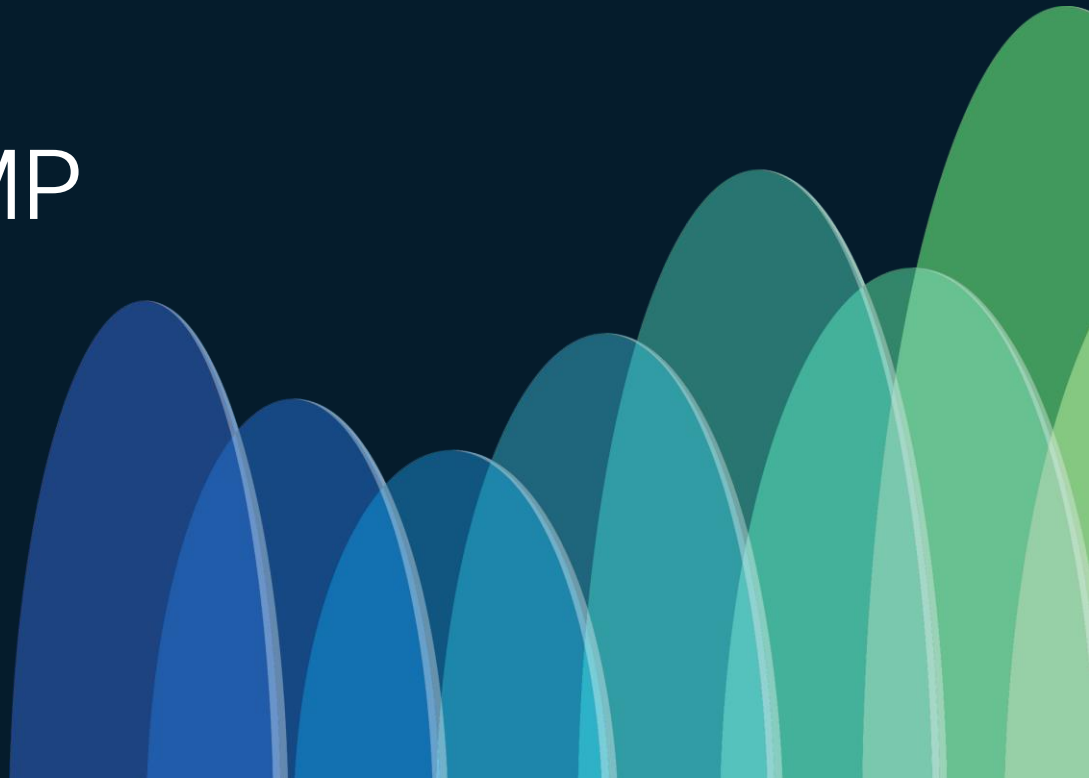
Leverages address families to advertise reachability.

OMP have a built-in loop avoidance capabilities

What information is propagated by OMP ?

vRoutes	TLOCs	Services	Policies
Service-side Routing info redistributed to Overlay + Attributes	WAN Attachments: system-ip link color encapsulation + Attributes	Services: Type of Service, Location (TLOC), Forwarding Information	Data Policy App-Route Policy VPN Membership cFlowd Template

Demystifying OMP Peering



cisco Live!

OMP Peering Overview

- OMP peering is established **between** system-IP inside the control connection (CC).
- Only a single peering session is established between a WAN Edge device and a Catalyst Controller, even in the presence of multiple DTLS/TLS connections.

- Prior to initiating the exchange of OMP packets for OMP peering establishment, a TCP connection MUST be established between peers.
- When the WAN Edge device attempts to establish OMP peering with the Catalyst controller, the WAN Edge operates in TCP active mode, while the Catalyst controller is in TCP passive mode.

- The WAN Edge device takes the initiative in actively opening a TCP connection.
- When the Catalyst controller attempts to establish a TCP connection with another Catalyst controller, the one with the lower system-IP address operates in TCP Active mode, while the other is in TCP Passive mode.

OMP Packets

- There are 7 OMP packets are exchanged to construct the overlay network, establish OMP peering, and disseminate routing, service, and policy information across the SDWAN fabric.
  - HANDSHAKE
  - HELLO
  - UPDATE
  - QUERY
  - ALERT
  - INFORM
  - POLICY

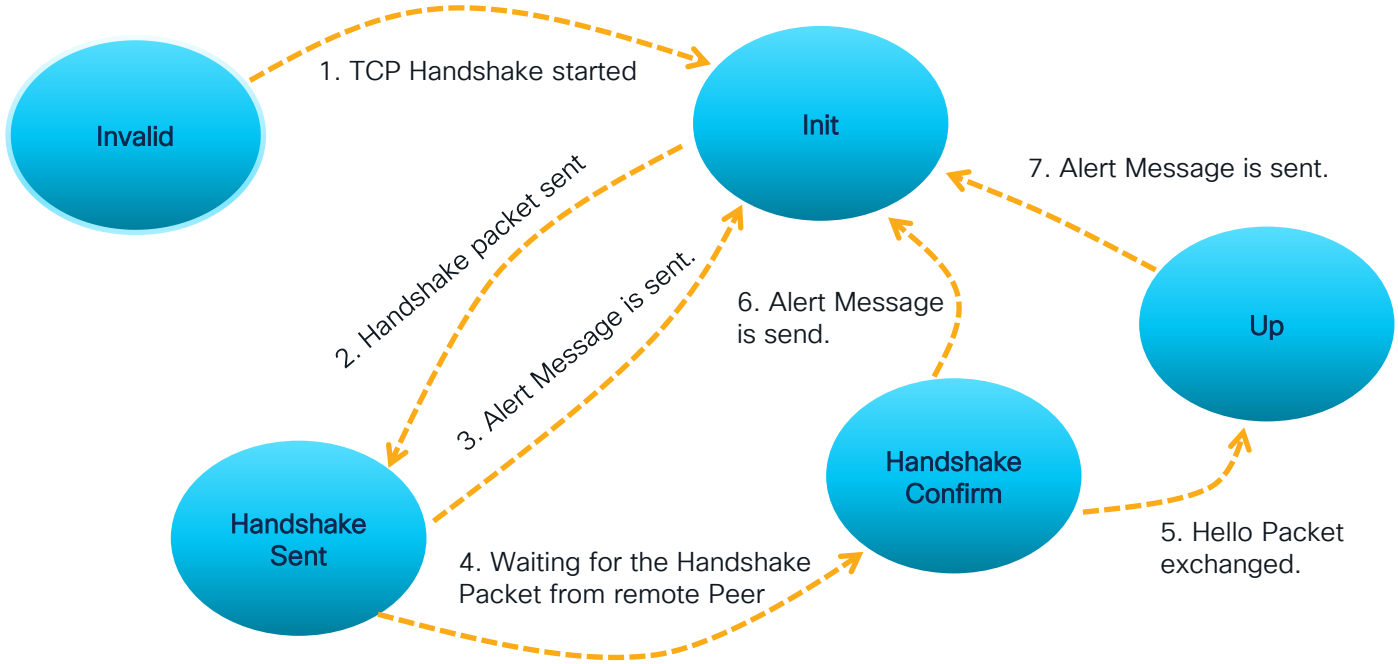
OMP Packet details

HANDSHAKE	Once the TCP session is established, the first packet which is exchange between peers is HANDSHAKE and it contains information like SITE-ID, HOLD-TIME and capability information like what it suports Multi-Protocol (MP) IPv4, MP IPv6, Multi-cast, services etc.. just like BGP OPEN message.
HELLO	OMP peers periodicly exchange HELLO packets to indicate each peer is alive and reachable.
UPDATE	This message is used to transfer routing information between peers. OMP update message is used to advertise feasible routes that share common path attributes to a peer or to withdraw multiple unfeasible routes.
QUERY	This message is used to send a request for a specific route for which an aggregate or else specific route exists. Query message is ONLY send by the WAN Edge router once it finds out that group of prefixes received is equipped with a query attribute.

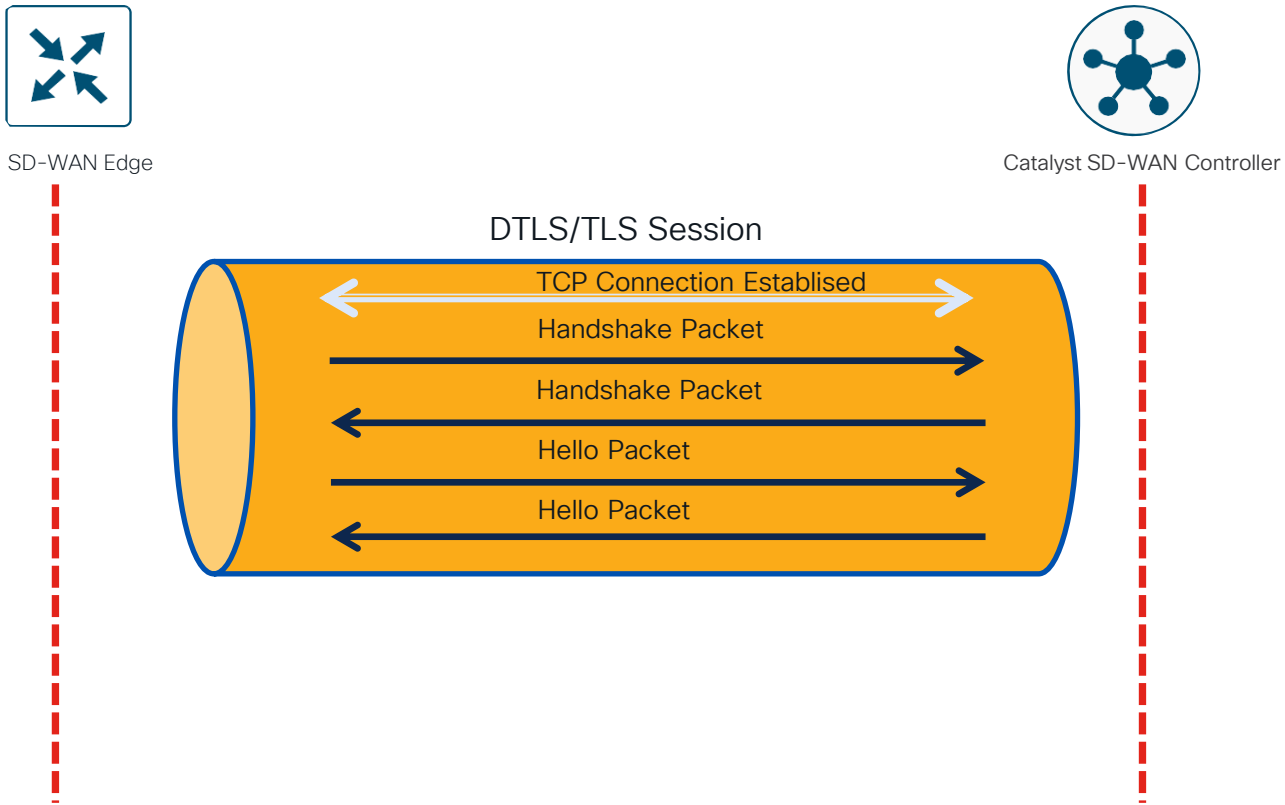
OMP Packet details

ALERT	Once the error condition has been deducted then peer used ALERT message to notify the opposite peer. The format and intention of the message is like BGP NOTIFICATION message.
INFORM	This OMP message is associated with the OMP GRACEFUL RESTART feature. For example, once OMP session went down and came back up then peer send end-of-RIB (EOR) marker, that is an OMP INFORM packet.
POLICY	This OMP message entails all the policies including control policies, centralized data policies, Application Aware Routing (AAR), cFlow template etc…

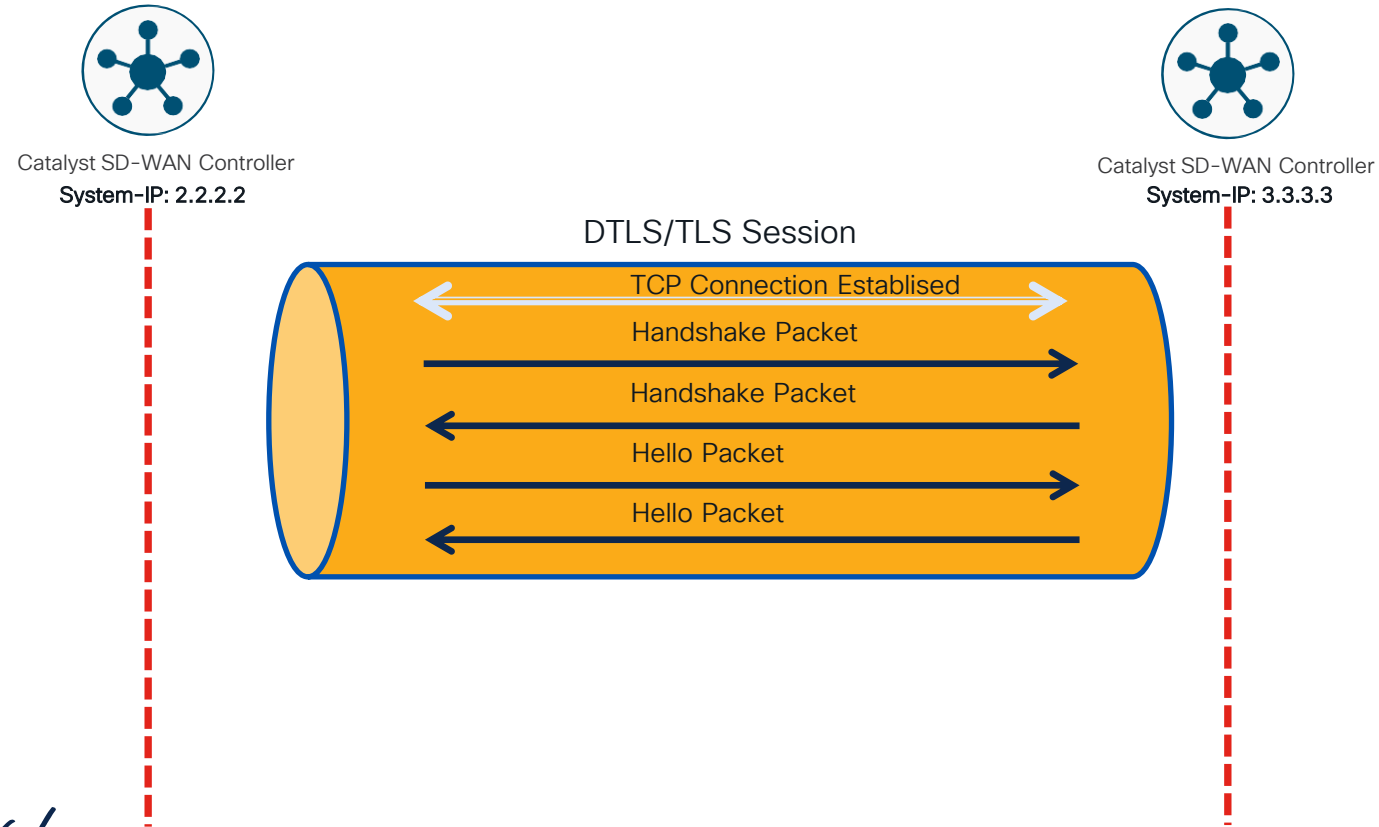
Finite State Machine for OMP Peer Establishment



How OMP peering established?



How OMP peering established?



Conditions for Establishing OMP Peer Relationship

- When Handshake packet is received from the peer, following conditions met:
  - WAN Edge and Catalyst controllers belong to same domain (**domain-id**).
  - Atleast ONE address family matches.
  - Peer capability need to matches.
- If any of the conditions are not met, an ALERT packet is sent with the appropriate error code, and the OMP peering session is terminated.
- Upon receiving a Hello packet from a peer, the peer validates the correctness of the peer address. If there is a discrepancy, an ALERT packet is sent with an error code, leading to the termination of the OMP peering session.

OMP Packet Insights and commonalities with BGP

cisco Live!

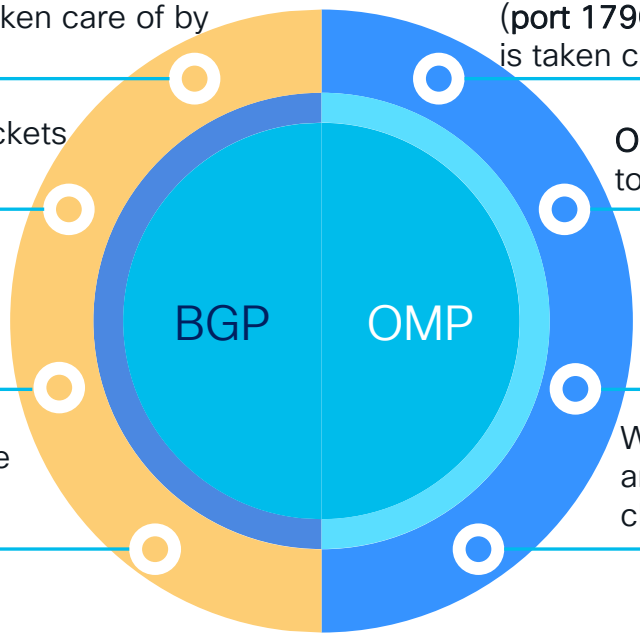
Exploring Key Similarities between BGP and OMP

BGP employs TCP as its transport protocol (**port 179**) to ensure all the transport reliability is taken care of by TCP.

BGP speakers exchange **KEEPALIVE** packets to maintain the connection keep alive.

BGP provides a mechanism to gracefully close a connection with the peer by sending a **NOTIFICATION error** message.

When **BGP** session has been established all candidate BGP routes are exchanged, then after that **only incremental updates** are sent.



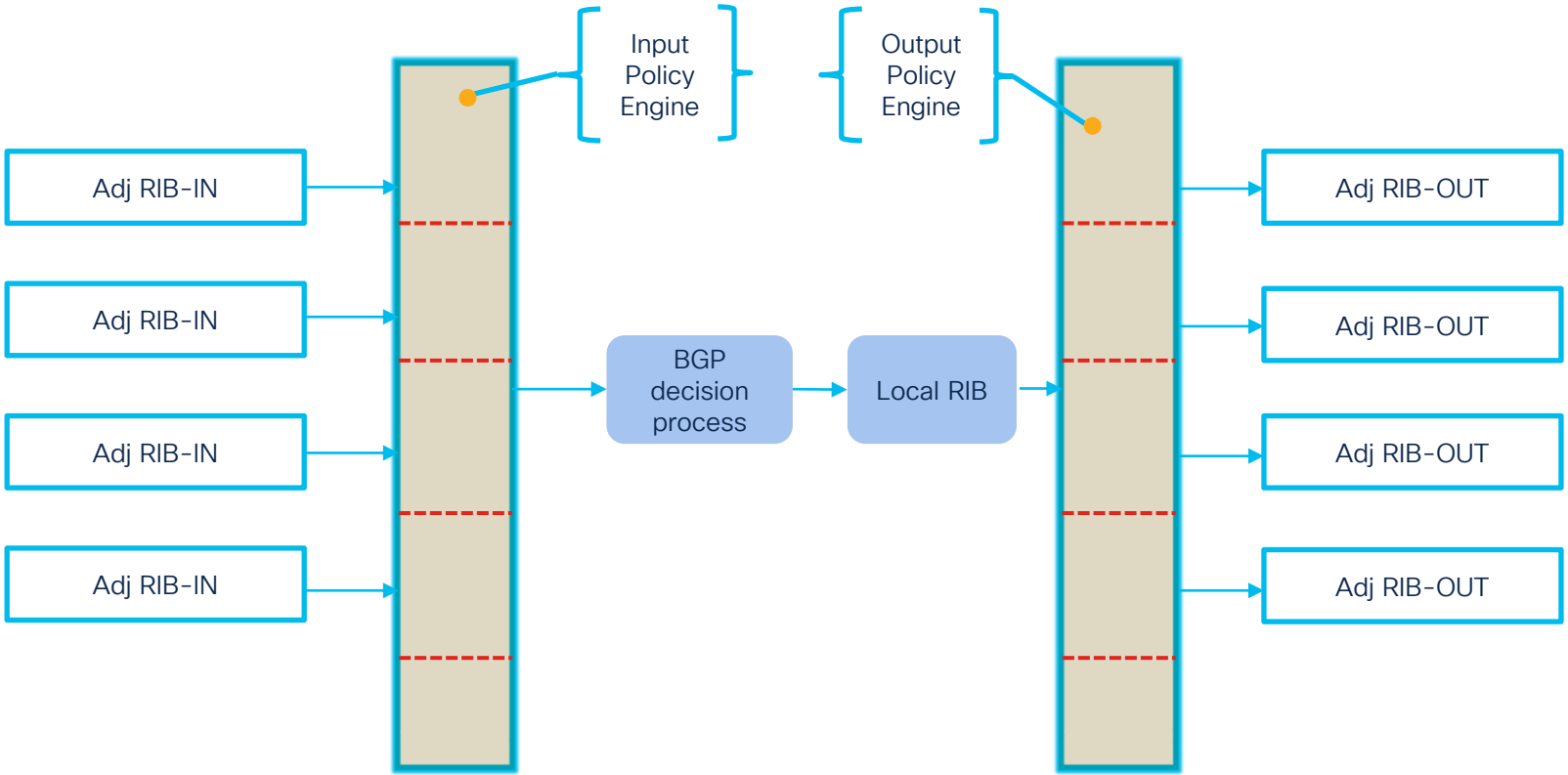
OMP also employs TCP as its transport protocol (**port 17900**) to ensure all the transport reliability is taken care by TCP.

OMP peers also exchange **HELLO packets** to maintain the peering alive.

OMP also provides a mechanism to gracefully close a connection with the peer by sending a **ALERT error** message.

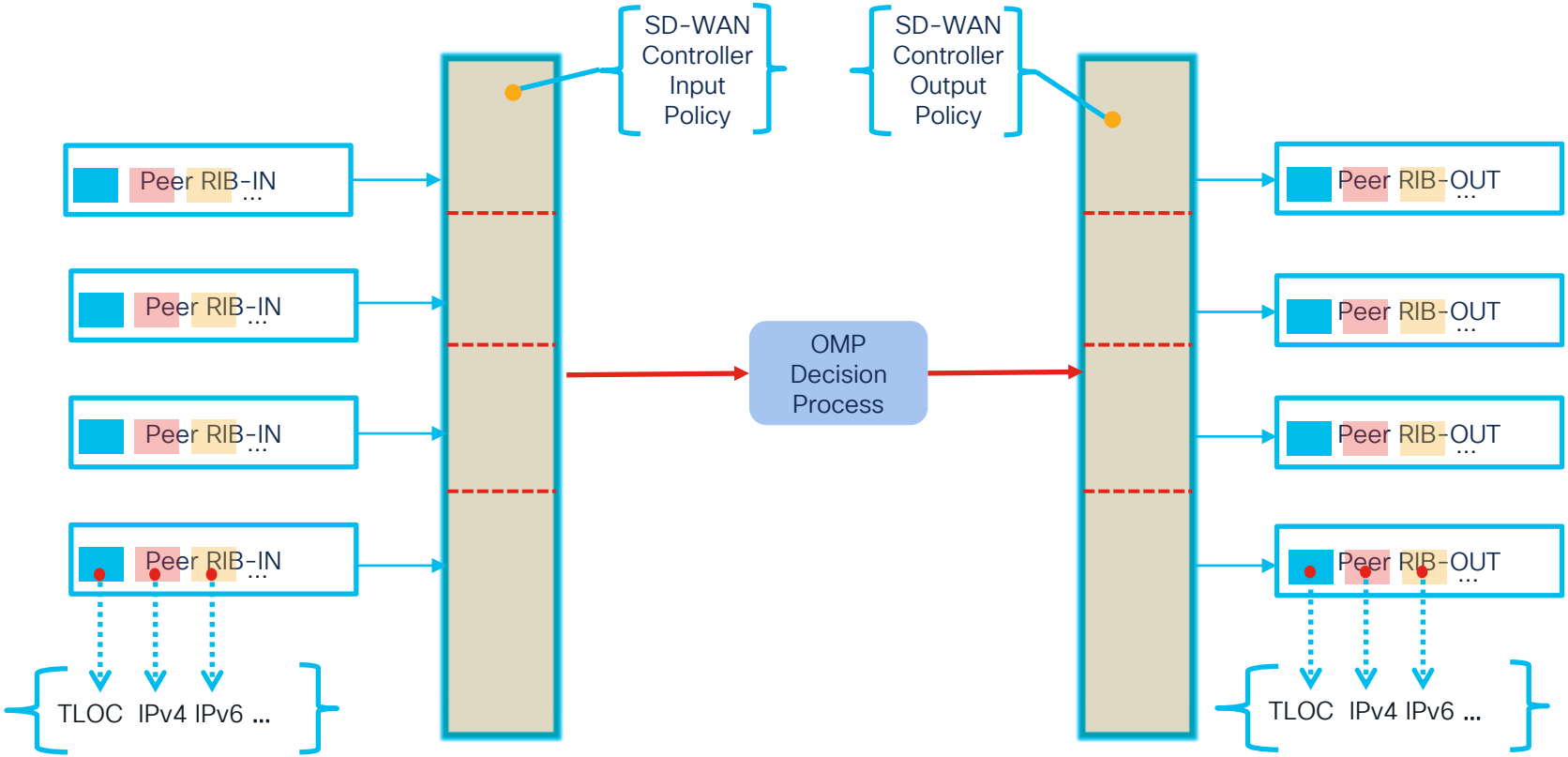
When **OMP peering** has been established and routes are exchanged then if any change **only incremental updates** are sent.

Let’s recap classic BGP Routing Process



Source: Internet Routing Architectures by Sam Halabi

SD-WAN Controller OMP Routing Process



OMP Address Families

Address Families		Key attributes
TLOC: Transport Locators	IPv4, IPv6	WAN IP Address Color Encap IP SEC keys TLOC properties
vRoute: VPN routes	IPv4, IPV6	VPN routes Route properties
mCast: Multicast Routes	IPv4, IPv6	Multicast routes Replicators information
Service		VPN: default service Firewall
Policy		Data Policy XML
Link		BFD link properties
Cloud Express		Cloud SLA properties

Key points to remember for SD-WAN Controller OMP Routing Process

SD-WAN controller have separate RIB-IN and RIB-OUT for each OMP peer.

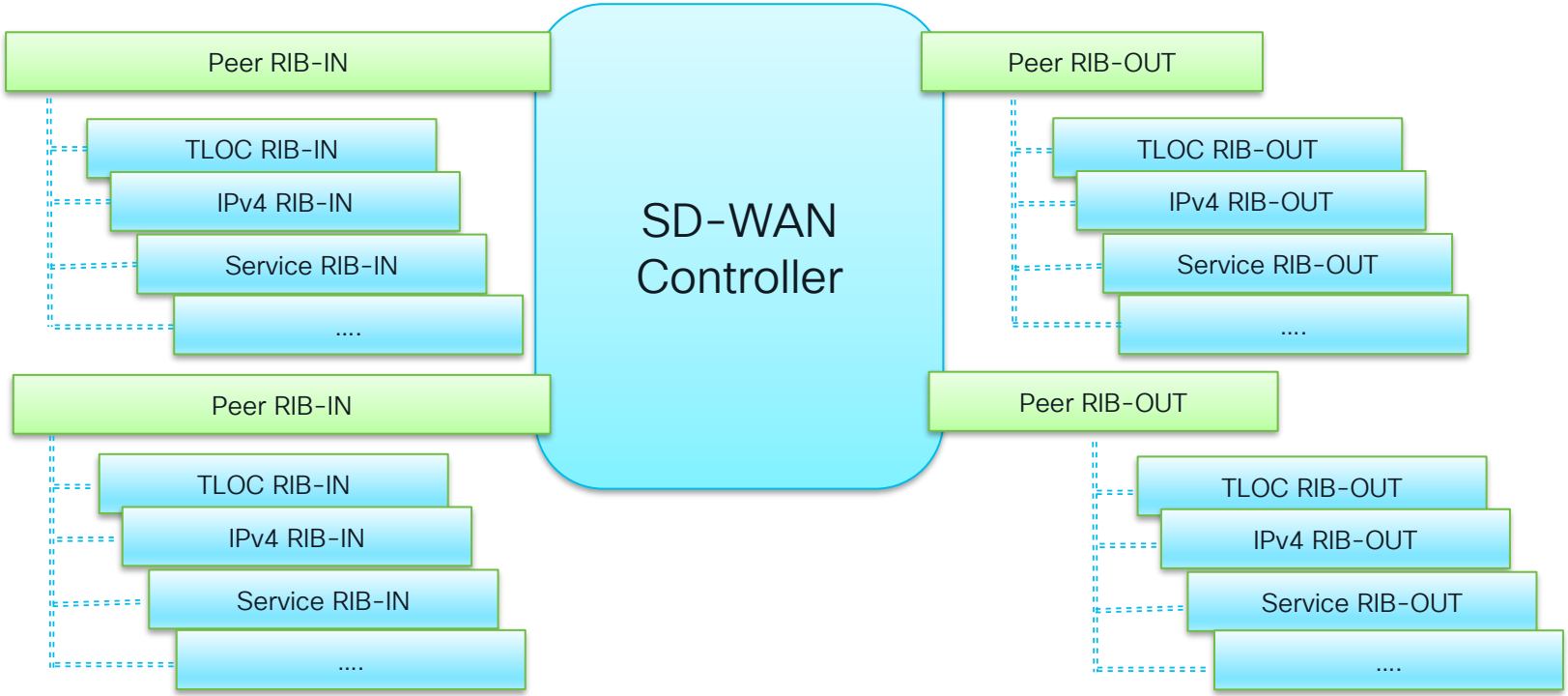
SD-WAN controller have further separate RIB-IN and RIB-OUT for each address family for example TLOC/prefix/service etc.. for each OMP peer.

From SD-WAN control policy perspective, when SD-WAN control policy is applied in IN bound direction then what ever action we perform either on TLOC/prefix/service it will be stored and shown in RIB-IN for that address-family for that peer and FLAG will be set accordingly.

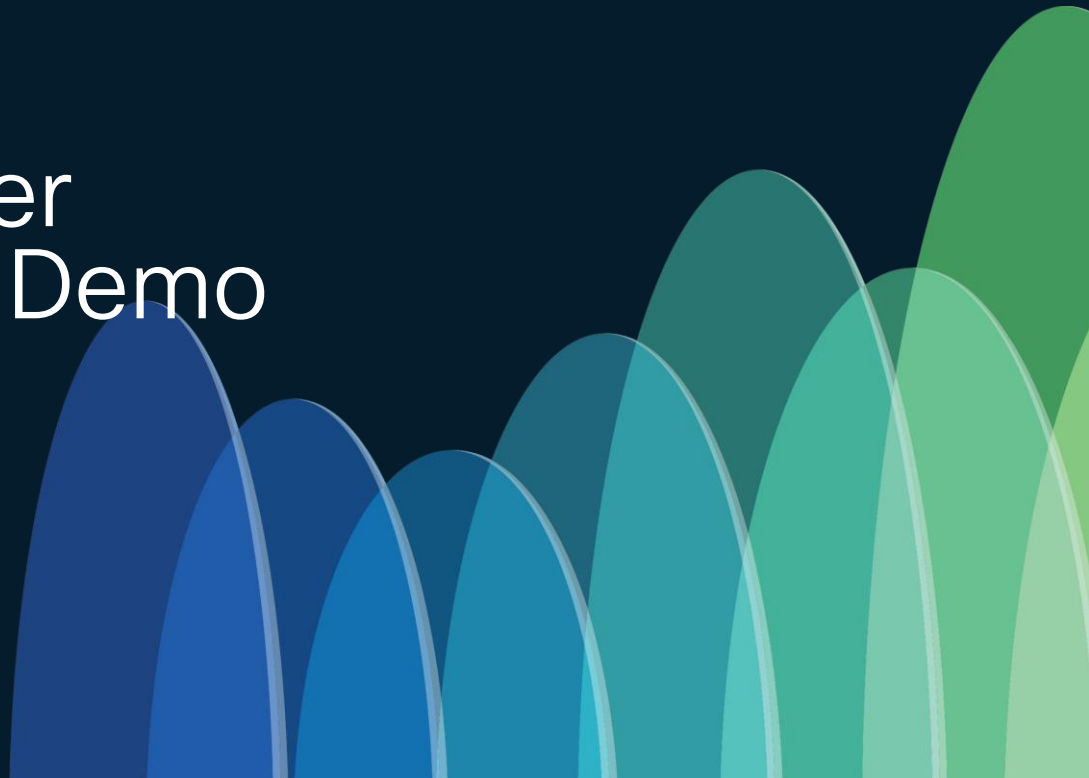
If we apply SD-WAN policy in OUT bound direction, then if action is REJECT either for TLOC/prefix/service etc.., then RIB-OUT will NOT be generated for that address family, so it will NOT be advertised to other peers.

If we apply SD-WAN control policy in OUT bound direction and change/modified either TLOC/prefix/service etc.. the attributes, then RIB-OUT will be generated as per our control policy/data policy and advertised to other peers.

SD-WAN Controller OMP Routing Process

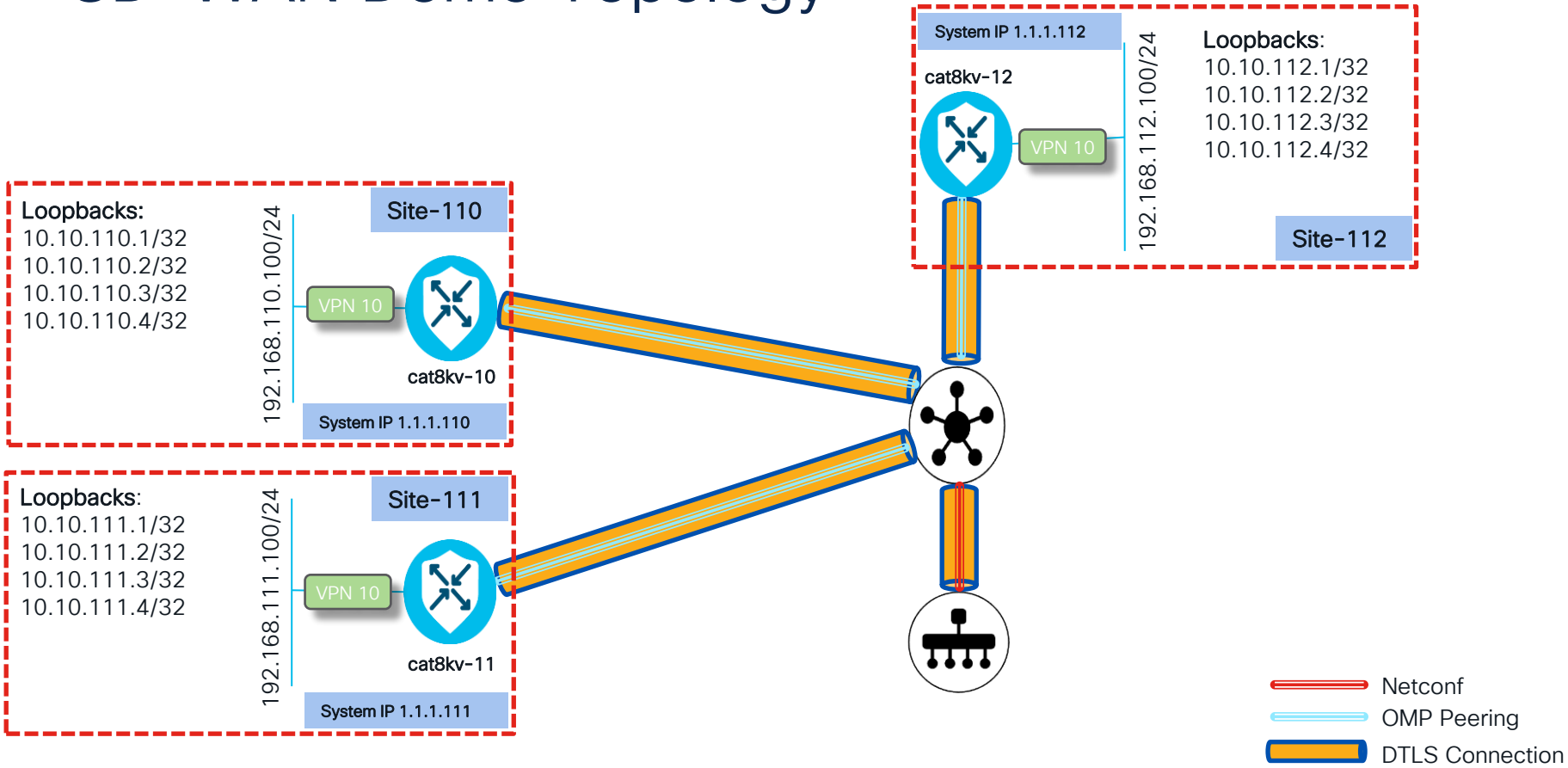


SDWAN Controller RIB-IN/RIB-OUT Demo

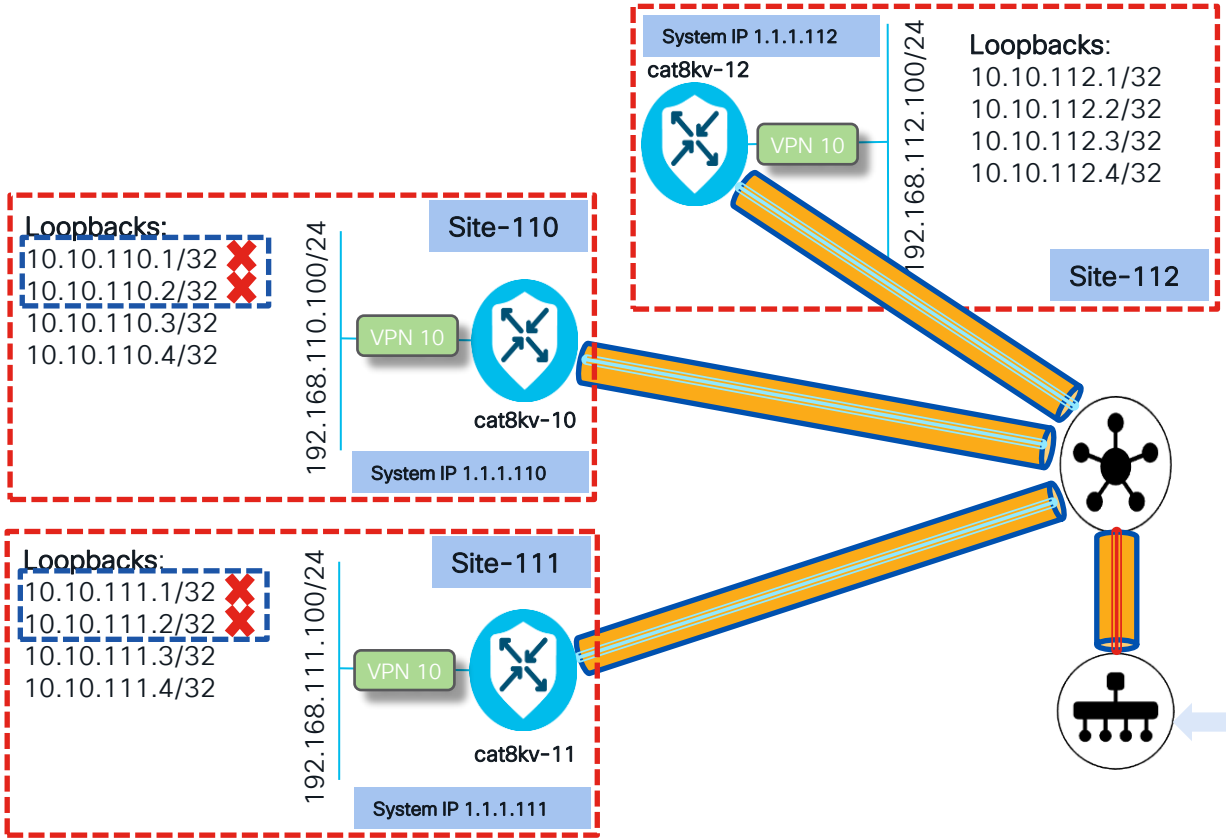


cisco Live!

SD-WAN Demo Topology



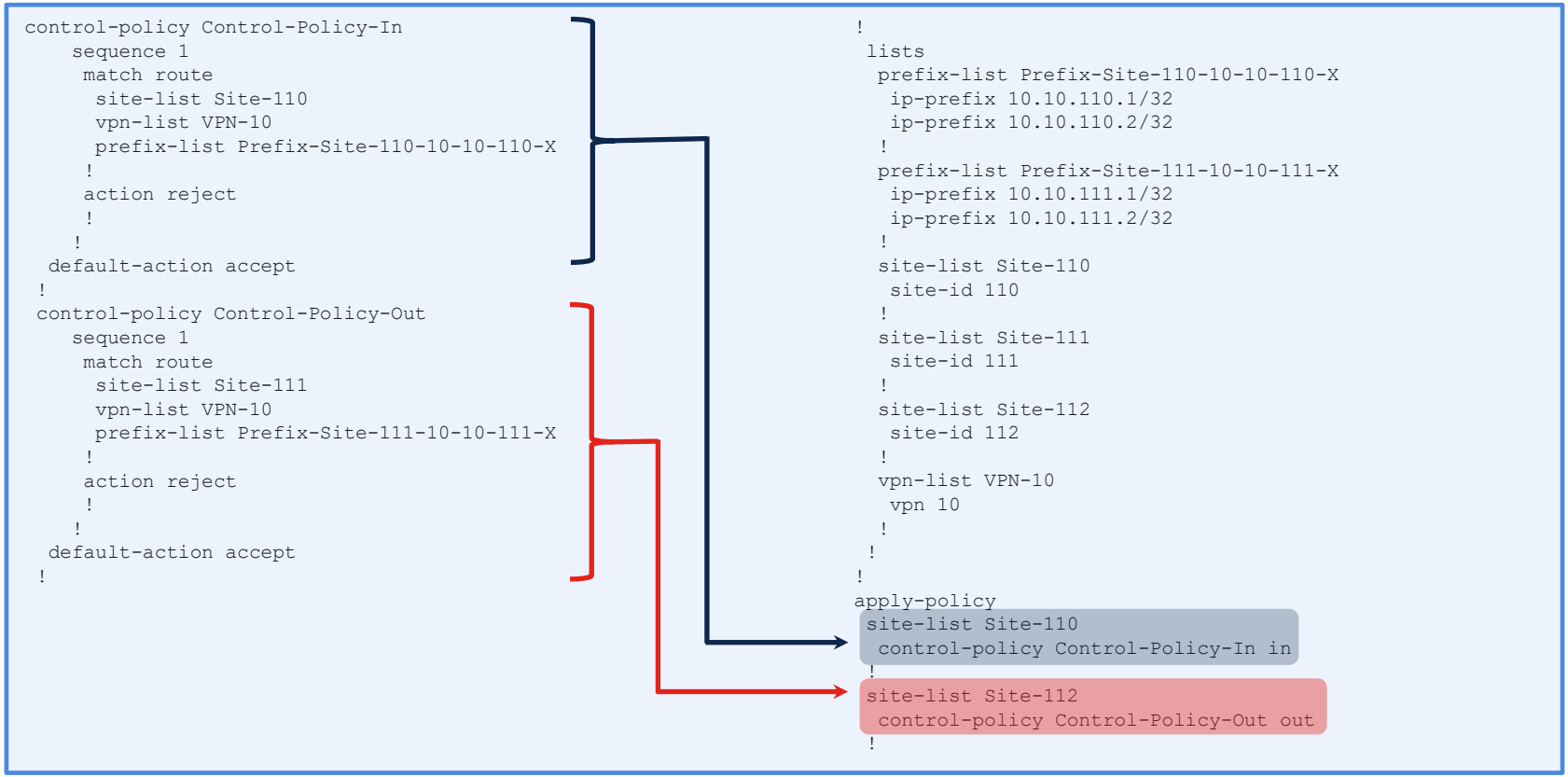
SD-WAN Demo Topology with Control Policy




```
control-policy Control-Policy-In
    sequence 1
     match route
      site-list Site-110
      vpn-list VPN-10
      prefix-list Prefix-Site-110-10-10-110-X
     !
     action reject
     !
    !
  default-action accept
 !
control-policy Control-Policy-Out
    sequence 1
    match route
     site-list Site-111
     vpn-list VPN-10
     prefix-list Prefix-Site-111-10-10-111-X
     !
     action reject
     !
    !
  default-action accept
```

Netconf
OMP Peering
DTLS Connection

Centralized Control Policy



OMP Routes state before applying control policy

```
Controller1#show omp routes vpn 10 received | tab | begin VPN
VPN     PREFIX              FROM PEER       ID     LABEL    STATUS    TYPE       TLOC IP          COLOR            ENCAP
-------------------------------------------------------------------------------------------------------------------------
10      10.10.110.1/32      1.1.1.110       66     1003     C,R       installed  1.1.1.110        mpls             ipsec
                            1.1.1.110       81     1003     C,R       installed  1.1.1.110        private1         ipsec
                            3.3.3.3         1      1003     C,R       installed  1.1.1.110        mpls             ipsec
                            3.3.3.3         2      1003     C,R       installed  1.1.1.110        private1         ipsec
10      10.10.110.2/32      1.1.1.110       66     1003     C,R       installed  1.1.1.110        mpls             ipsec
                            1.1.1.110       81     1003     C,R       installed  1.1.1.110        private1         ipsec
                            3.3.3.3         1      1003     C,R       installed  1.1.1.110        mpls             ipsec
                            3.3.3.3         2      1003     C,R       installed  1.1.1.110        private1         ipsec
10      10.10.110.3/32      1.1.1.110       66     1003     C,R       installed  1.1.1.110        mpls             ipsec
                            1.1.1.110       81     1003     C,R       installed  1.1.1.110        private1         ipsec
                            3.3.3.3         1      1003     C,R       installed  1.1.1.110        mpls             ipsec
                            3.3.3.3         2      1003     C,R       installed  1.1.1.110        private1         ipsec
10      10.10.110.4/32      1.1.1.110       66     1003     C,R       installed  1.1.1.110        mpls             ipsec
                            1.1.1.110       81     1003     C,R       installed  1.1.1.110        private1         ipsec
                            3.3.3.3         1      1003     C,R       installed  1.1.1.110        mpls             ipsec
                            3.3.3.3         2      1003     C,R       installed  1.1.1.110        private1         ipsec
10      10.10.111.1/32      1.1.1.111       66     1007     C,R       installed  1.1.1.111        mpls             ipsec
                            1.1.1.111       81     1007     C,R       installed  1.1.1.111        private1         ipsec
                            3.3.3.3         1      1007     C,R       installed  1.1.1.111        mpls             ipsec
                            3.3.3.3         2      1007     C,R       installed  1.1.1.111        private1         ipsec
10      10.10.111.2/32      1.1.1.111       66     1007     C,R       installed  1.1.1.111        mpls             ipsec
                            1.1.1.111       81     1007     C,R       installed  1.1.1.111        private1         ipsec
                            3.3.3.3         1      1007     C,R       installed  1.1.1.111        mpls             ipsec
                            3.3.3.3         2      1007     C,R       installed  1.1.1.111        private1         ipsec
10      10.10.111.3/32      1.1.1.111       66     1007     C,R       installed  1.1.1.111        mpls             ipsec
                            1.1.1.111       81     1007     C,R       installed  1.1.1.111        private1         ipsec
                            3.3.3.3         1      1007     C,R       installed  1.1.1.111        mpls             ipsec
                            3.3.3.3         2      1007     C,R       installed  1.1.1.111        private1         ipsec
10      10.10.111.4/32      1.1.1.111       66     1007     C,R       installed  1.1.1.111        mpls             ipsec
                            1.1.1.111       81     1007     C,R       installed  1.1.1.111        private1         ipsec
                            3.3.3.3         1      1007     C,R       installed  1.1.1.111        mpls             ipsec
                            3.3.3.3         2      1007     C,R       installed  1.1.1.111        private1         ipsec
```

OMP Routes state after applying Inbound control policy

```
Controller-1#show omp routes vpn 10 received | begin VPN
VPN     PREFIX              FROM PEER       ID     LABEL    STATUS    TYPE       TLOC IP         COLOR            ENCAP
10      10.10.110.1/32      1.1.1.110       66     1003     Rej,R,Inv installed  1.1.1.110       mpls             ipsec
                            1.1.1.110       81     1003     Rej,R,Inv installed  1.1.1.110       private1         ipsec
10      10.10.110.2/32      1.1.1.110       66     1003     Rej,R,Inv installed  1.1.1.110       mpls             ipsec
                            1.1.1.110       81     1003     Rej,R,Inv installed  1.1.1.110       private1         ipsec
10      10.10.110.3/32      1.1.1.110       66     1003     C,R       installed  1.1.1.110       mpls             ipsec
                            1.1.1.110       81     1003     C,R       installed  1.1.1.110       private1         ipsec
                            3.3.3.3         48     1003     C,R       installed  1.1.1.110       mpls             ipsec
                            3.3.3.3         55     1003     C,R       installed  1.1.1.110       private1         ipsec
10      10.10.110.4/32      1.1.1.110       66     1003     C,R       installed  1.1.1.110       mpls             ipsec
                            1.1.1.110       81     1003     C,R       installed  1.1.1.110       private1         ipsec
                            3.3.3.3         48     1003     C,R       installed  1.1.1.110       mpls             ipsec
                            3.3.3.3         55     1003     C,R       installed  1.1.1.110       private1         ipsec
10      10.10.111.1/32      1.1.1.111       66     1003     C,R       installed  1.1.1.111       mpls             ipsec
                            1.1.1.111       81     1003     C,R       installed  1.1.1.111       private1         ipsec
                            3.3.3.3         15     1003     C,R       installed  1.1.1.111       mpls             ipsec
                            3.3.3.3         16     1003     C,R       installed  1.1.1.111       private1         ipsec
10      10.10.111.2/32      1.1.1.111       66     1003     C,R       installed  1.1.1.111       mpls             ipsec
                            1.1.1.111       81     1003     C,R       installed  1.1.1.111       private1         ipsec
                            3.3.3.3         15     1003     C,R       installed  1.1.1.111       mpls             ipsec
                            3.3.3.3         16     1003     C,R       installed  1.1.1.111       private1         ipsec
10      10.10.111.3/32      1.1.1.111       66     1003     C,R       installed  1.1.1.111       mpls             ipsec
                            1.1.1.111       81     1003     C,R       installed  1.1.1.111       private1         ipsec
                            3.3.3.3         15     1003     C,R       installed  1.1.1.111       mpls             ipsec
                            3.3.3.3         16     1003     C,R       installed  1.1.1.111       private1         ipsec
10      10.10.111.4/32      1.1.1.111       66     1003     C,R       installed  1.1.1.111       mpls             ipsec
                            1.1.1.111       81     1003     C,R       installed  1.1.1.111       private1         ipsec
                            3.3.3.3         15     1003     C,R       installed  1.1.1.111       mpls             ipsec
                            3.3.3.3         16     1003     C,R       installed  1.1.1.111       private1         ipsec
```

OMP Routes state after applying Inbound control policy

```
Controller1#show omp routes vpn 10 advertised | tab | begin VPN
VPN     PREFIX              TO PEER
10      10.10.110.3/32      1.1.1.111
                            1.1.1.112
                            1.1.1.113
                            1.1.1.114
                            1.1.1.115
                            1.1.1.116
                            3.3.3.3
10      10.10.110.4/32      1.1.1.111
                            1.1.1.112
                            1.1.1.113
                            1.1.1.114
                            1.1.1.115
                            1.1.1.116
                            3.3.3.3
```

OMP Routes state after applying Inbound control policy

```
Controller-1# show support omp rib vroute 10:10.10.110.1/32
Looking up vroute 10.10.110.1/32 in 10

RIB-Entry: (0x7f131609c780) ROUTE-IPV4 Flags: (0x0) , recv-attr-count 2, adv-attr-count 0
  ri-peer-tree: 0x7f131609c7d8(2), ro-peer-tree: 0x7f131609c800(0),  ro-ri-id-tree: 0x7f131609c838(0), Scheduled: 72, Version: 1195,  ro-cache-
ri-id-tree: 0x7f13160a2090(0), ro-cache-policy-name-tree: 0x7f13160a20c0(0)   VPN-ID: 10, Prefix: 10.10.110.1/32

 Region-Info Region-ID: 65534
   RIB-IN: (0x7f13153631e0, prev: (nil), next: 0x7f131532e380), Peer: 1.1.1.110, ID: 355, updated: Mon Nov 20 12:41:32 2023
    Path-id: 66, Label: 1003 Affinity Number: 0 TLOC-pref: 0 TLOC-stale: 0 version: 1 (stale: 0) Management-Region: False
    Lost-to-peer: ::, Lost-to-path-id: 0, Loss-Reason: None(0)
    Rcv-Attr: 0x7f1313401500, Flags: (0x28) REJECT RESOLVED
    Attribute: (0x7f1313401500), ROUTE-IPV4, Length: 1184, Ref: 2
      Flags: (0x8000c25) WEIGHT TLOC SITE-ID OVERLAY-ID ORIGIN ORIGINATOR
      Region-id: 65534, Secondary-Region-id: 65535, Orig-Access-Region-id: 65534, Sub-Region-ID: 0, Pref: 0, Weight: 1, Tag: 0, Stale: 0
Version: 0, Restrict: 0, on-Demand: 0, Domain: 0, BR-Preference: 0, Affinity-Group-Number:0, MRF-Route-Originator:None , Derived Affinity-
group-number: 0      Distance: 0, Site-ID: 110, Carrier: 0, Query: 0, Gen-ID: 0x0, Border: 0 Overlay: 1 Site-Type: 0 0 0 0
      Originator: 1.1.1.110
      Origin: Protocol: ospf[4], Sub-Type: intra-area[1], Metric: 1
      TLOC: (0x7f1316366500) 1.1.1.110 : mpls : ipsec
  RIB-IN: (0x7f131532e380, prev: 0x7f13153631e0, next: (nil)), Peer: 1.1.1.110, ID: 371, updated: Mon Nov 20 12:41:32 2023
    Path-id: 81, Label: 1003 Affinity Number: 0 TLOC-pref: 0 TLOC-stale: 0 version: 1 (stale: 0) Management-Region: False
    Lost-to-peer: 1.1.1.110, Lost-to-path-id: 66, Loss-Reason: TLOC ID(10)
    Rcv-Attr: 0x7f1313453c00, Flags: (0x28) REJECT RESOLVED
    Attribute: (0x7f1313453c00), ROUTE-IPV4, Length: 1184, Ref: 2
      Flags: (0x8000c25) WEIGHT TLOC SITE-ID OVERLAY-ID ORIGIN ORIGINATOR
      Region-id: 65534, Secondary-Region-id: 65535, Orig-Access-Region-id: 65534, Sub-Region-ID: 0, Pref: 0, Weight: 1, Tag: 0, Stale: 0
Version: 0, Restrict: 0, on-Demand: 0, Domain: 0, BR-Preference: 0, Affinity-Group-Number:0, MRF-Route-Originator:None , Derived Affinity-
group-number: 0      Distance: 0, Site-ID: 110, Carrier: 0, Query: 0, Gen-ID: 0x0, Border: 0 Overlay: 1 Site-Type: 0 0 0 0
      Originator: 1.1.1.110
      Origin: Protocol: ospf[4], Sub-Type: intra-area[1], Metric: 1
      TLOC: (0x7f13163665a0) 1.1.1.110 : private1 : ipsec
```

OMP Routes state after applying Inbound control policy

```
Controller-1# show omp routes vpn 10 advertised | begin VPN
VPN     PREFIX                  TO PEER
-------------------------------------------
10      10.10.110.3/32          1.1.1.111
                                1.1.1.112
                                1.1.1.113
                                1.1.1.114
                                1.1.1.115
                                1.1.1.116
                                3.3.3.3
10      10.10.110.4/32          1.1.1.111
                                1.1.1.112
                                1.1.1.113
                                1.1.1.114
                                1.1.1.115
                                1.1.1.116
                                3.3.3.3
```

OMP Routes state after applying Inbound control policy

```
Controller1# show support omp rib vroute 10:10.10.110.3/32 | include RIB-OUT\|RIB-IN
  RIB-IN: (0x7f3b0b664d00, prev: (nil), next: 0x7f3b0b665400), Peer: 1.1.1.110, ID: 95, updated: Sun Jan 12 21:11:22 2025
  RIB-IN: (0x7f3b0b665400, prev: 0x7f3b0b664d00, next: 0x7f3b0b6cd8c0), Peer: 1.1.1.110, ID: 103, updated: Sun Jan 12 21:11:22 2025
  RIB-IN: (0x7f3b0b6cd8c0, prev: 0x7f3b0b665400, next: 0x7f3b0b6cef80), Peer: 3.3.3.3, ID: 171, updated: Sun Jan 12 14:49:04 2025
  RIB-IN: (0x7f3b0b6cef80, prev: 0x7f3b0b6cd8c0, next: (nil)), Peer: 3.3.3.3, ID: 197, updated: Sun Jan 12 14:49:04 2025
   RIB-OUT: (0x7f3b0ffa3540), RI-ID: 95, Peer: 1.1.1.111 Path-id: 1, Label: 1003, Flags: (0x1) ADV  Common (0x7f3b0a00a280) Common Ref: 7
   RIB-OUT: (0x7f3b0ffa4b00), RI-ID: 103, Peer: 1.1.1.111 Path-id: 2, Label: 1003, Flags: (0x1) ADV  Common (0x7f3b0a00a2c0) Common Ref: 7
   RIB-OUT: (0x7f3b0ffa9ab0), RI-ID: 95, Peer: 1.1.1.112 Path-id: 1, Label: 1003, Flags: (0x1) ADV  Common (0x7f3b0a00a280) Common Ref: 7
   RIB-OUT: (0x7f3b0ffad6b0), RI-ID: 103, Peer: 1.1.1.112 Path-id: 2, Label: 1003, Flags: (0x1) ADV  Common (0x7f3b0a00a2c0) Common Ref: 7
   RIB-OUT: (0x7f3b0ffad590), RI-ID: 95, Peer: 1.1.1.113 Path-id: 1, Label: 1003, Flags: (0x1) ADV  Common (0x7f3b0a00a280) Common Ref: 7
   RIB-OUT: (0x7f3b0ffa3630), RI-ID: 103, Peer: 1.1.1.113 Path-id: 2, Label: 1003, Flags: (0x1) ADV  Common (0x7f3b0a00a2c0) Common Ref: 7
   RIB-OUT: (0x7f3b0ffa7e60), RI-ID: 95, Peer: 1.1.1.114 Path-id: 1, Label: 1003, Flags: (0x1) ADV  Common (0x7f3b0a00a280) Common Ref: 7
   RIB-OUT: (0x7f3b0ffa8a90), RI-ID: 103, Peer: 1.1.1.114 Path-id: 2, Label: 1003, Flags: (0x1) ADV  Common (0x7f3b0a00a2c0) Common Ref: 7
   RIB-OUT: (0x7f3b0ffb15e0), RI-ID: 95, Peer: 1.1.1.115 Path-id: 1, Label: 1003, Flags: (0x1) ADV  Common (0x7f3b0a00a280) Common Ref: 7
   RIB-OUT: (0x7f3b0ffb2de0), RI-ID: 103, Peer: 1.1.1.115 Path-id: 2, Label: 1003, Flags: (0x1) ADV  Common (0x7f3b0a00a2c0) Common Ref: 7
   RIB-OUT: (0x7f3b0ffaa290), RI-ID: 95, Peer: 1.1.1.116 Path-id: 1, Label: 1003, Flags: (0x1) ADV  Common (0x7f3b0a00a280) Common Ref: 7
   RIB-OUT: (0x7f3b0ffa8430), RI-ID: 103, Peer: 1.1.1.116 Path-id: 2, Label: 1003, Flags: (0x1) ADV  Common (0x7f3b0a00a2c0) Common Ref: 7
   RIB-OUT: (0x7f3b0ffb0b00), RI-ID: 95, Peer: 3.3.3.3 Path-id: 1, Label: 1003, Flags: (0x1) ADV  Common (0x7f3b0a00a280) Common Ref: 7
   RIB-OUT: (0x7f3b0ffb0c20), RI-ID: 103, Peer: 3.3.3.3 Path-id: 2, Label: 1003, Flags: (0x1) ADV  Common (0x7f3b0a00a2c0) Common Ref: 7
```

OMP Routes state after applying Outbound control policy

```
Controller-1# show omp routes vpn 10 advertised | begin VPN
VPN     PREFIX              TO PEER
-----------------------------------------------
10      10.10.110.3/32      1.1.1.111
                            1.1.1.112
                            1.1.1.113
                            1.1.1.114
                            1.1.1.115
                            1.1.1.116
                            3.3.3.3
10      10.10.110.4/32      1.1.1.111
                            1.1.1.112
                            1.1.1.113
                            1.1.1.114
                            1.1.1.115
                            1.1.1.116
                            3.3.3.3
10      10.10.111.1/32      1.1.1.110
                            1.1.1.113
                            1.1.1.114
                            1.1.1.115
                            1.1.1.116
                            3.3.3.3
10      10.10.111.2/32      1.1.1.110
                            1.1.1.113
                            1.1.1.114
                            1.1.1.115
                            1.1.1.116
                            3.3.3.3
10      10.10.111.3/32      1.1.1.110
                            1.1.1.112
                            1.1.1.113
                            1.1.1.114
                            1.1.1.115
                            1.1.1.116
                            3.3.3.3
```

OMP Routes state after applying Outbound control policy

```
Controller1# show support omp rib vroute 10:10.10.111.1/32 rib-out-peer-ip 1.1.1.112 | include RIB
RIB-Entry: (0x7f3b0b66c500) ROUTE-IPV4 Flags: (0x0) , recv-attr-count 4, adv-attr-count 12, ro-path-id-counter 4
   RIB-IN: (0x7f3b0b662ae0, prev: (nil), next: 0x7f3b0b6633a0), Peer: 1.1.1.111, ID: 78, updated: Sun Jan 12 14:49:02 2025
  RIB-IN: (0x7f3b0b6633a0, prev: 0x7f3b0b662ae0, next: 0x7f3b0b6cfe60), Peer: 1.1.1.111, ID: 88, updated: Sun Jan 12 14:49:02 2025
  RIB-IN: (0x7f3b0b6cfe60, prev: 0x7f3b0b6633a0, next: 0x7f3b0b6d0e20), Peer: 3.3.3.3, ID: 214, updated: Sun Jan 12 14:49:04 2025
  RIB-IN: (0x7f3b0b6d0e20, prev: 0x7f3b0b6cfe60, next: (nil)), Peer: 3.3.3.3, ID: 232, updated: Sun Jan 12 14:49:04 2025
```

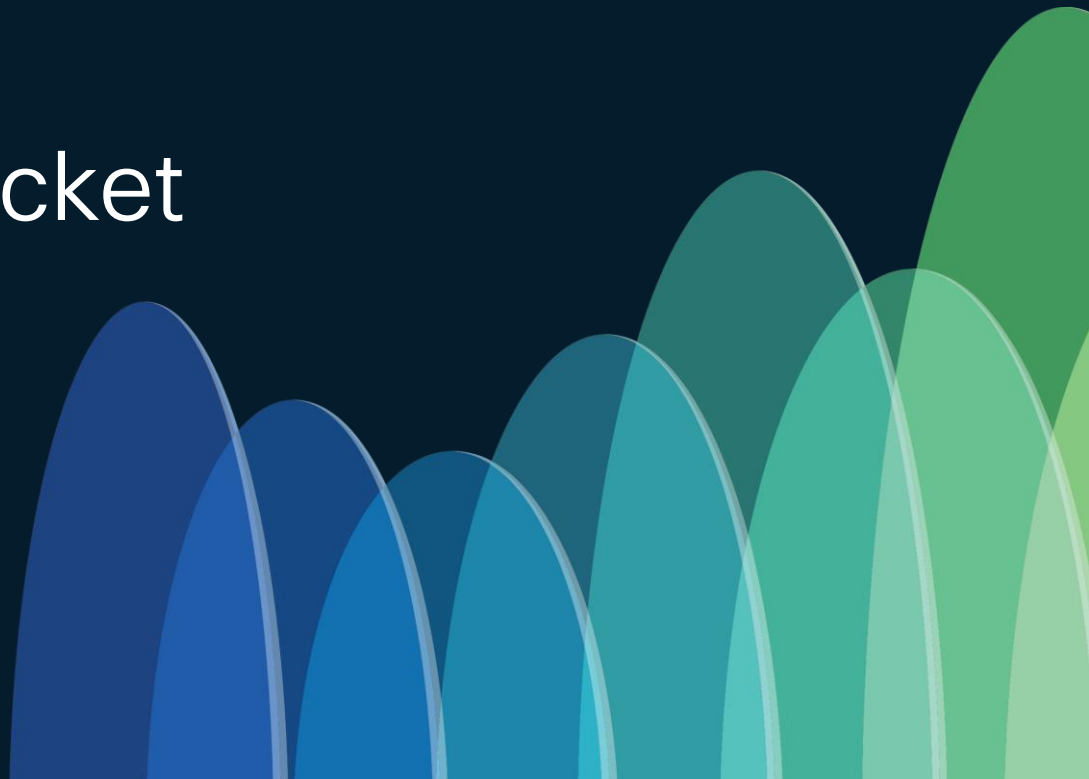
OMP Routes state after applying Outbound control policy

```
Controller-1# show omp routes vpn 10 advertised | begin VPN
VPN     PREFIX              TO PEER
-----------------------------------------
10      10.10.110.3/32      1.1.1.111
                            1.1.1.112
                            1.1.1.113
                            1.1.1.114
                            1.1.1.115
                            1.1.1.116
                            3.3.3.3
10      10.10.110.4/32      1.1.1.111
                            1.1.1.112
                            1.1.1.113
                            1.1.1.114
                            1.1.1.115
                            1.1.1.116
                            3.3.3.3
10      10.10.111.1/32      1.1.1.110
                            1.1.1.113
                            1.1.1.114
                            1.1.1.115
                            1.1.1.116
                            3.3.3.3
10      10.10.111.2/32      1.1.1.110
                            1.1.1.113
                            1.1.1.114
                            1.1.1.115
                            1.1.1.116
                            3.3.3.3
10      10.10.111.3/32      1.1.1.110
                            1.1.1.112
                            1.1.1.113
                            1.1.1.114
                            1.1.1.115
                            1.1.1.116
                            3.3.3.3
```

OMP Routes state after applying Outbound control policy

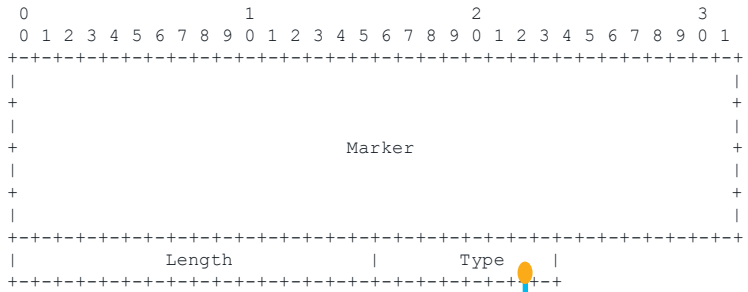
```
Controller1# show support omp rib vroute 10:10.10.111.1/32 rib-out-peer-ip 1.1.1.110 | include RIB
RIB-Entry: (0x7f3b0b66c500) ROUTE-IPV4 Flags: (0x0) , recv-attr-count 4, adv-attr-count 12, ro-path-id-counter 4
   RIB-IN: (0x7f3b0b662ae0, prev: (nil), next: 0x7f3b0b6633a0), Peer: 1.1.1.111, ID: 78, updated: Sun Jan 12 14:49:02 2025
  RIB-IN: (0x7f3b0b6633a0, prev: 0x7f3b0b662ae0, next: 0x7f3b0b6cfe60), Peer: 1.1.1.111, ID: 88, updated: Sun Jan 12 14:49:02 2025
  RIB-IN: (0x7f3b0b6cfe60, prev: 0x7f3b0b6633a0, next: 0x7f3b0b6d0e20), Peer: 3.3.3.3, ID: 214, updated: Sun Jan 12 14:49:04 2025
  RIB-IN: (0x7f3b0b6d0e20, prev: 0x7f3b0b6cfe60, next: (nil)), Peer: 3.3.3.3, ID: 232, updated: Sun Jan 12 14:49:04 2025
  RIB-OUT: (0x7f3b0ffa1110), RI-ID: 78, Peer: 1.1.1.110 Path-id: 1, Label: 1007, Flags: (0x1) ADV  Common (0x7f3b0a00a100) Common Ref: 6
  RIB-OUT: (0x7f3b0ffa79e0), RI-ID: 88, Peer: 1.1.1.110 Path-id: 2, Label: 1007, Flags: (0x1) ADV  Common (0x7f3b0a00a140) Common Ref: 6
```

OMP and BGP Packet Insights



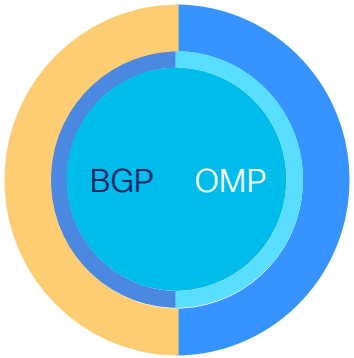
cisco Live!

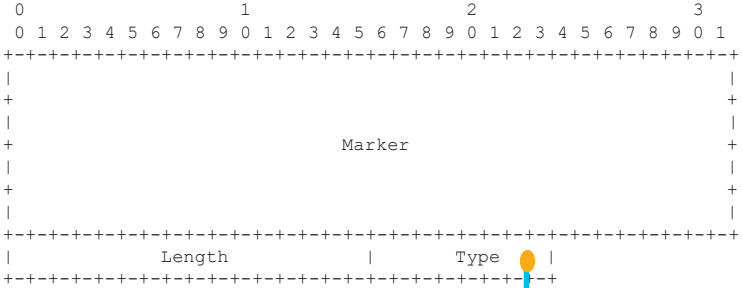
Commonalities between OMP and BGP Packets



BGP Message Header Format

- OPEN
- UPDATE
- NOTIFICATION
- KEEPALIVE

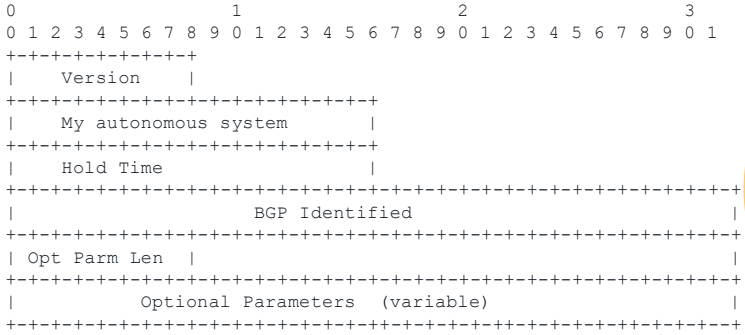




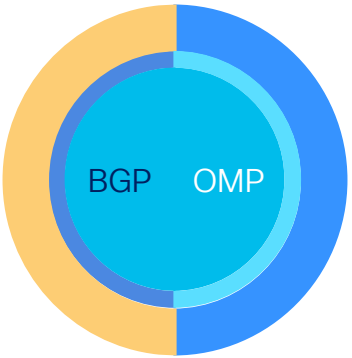
OMP Message Header Format

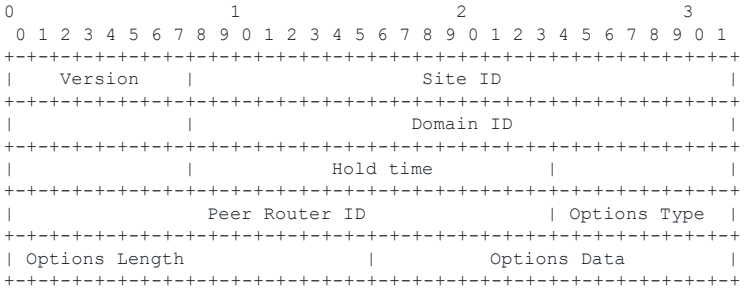
- HANDSHAKE
- UPDATE
- ALERT
- HELLO
- QUERY
- POLICY
- INFORM

Commonalities between OMP and BGP Packets



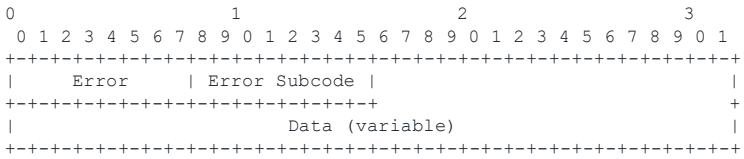
BGP Open Packet Format



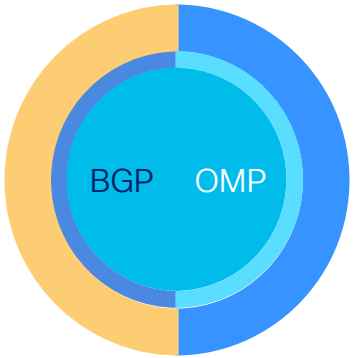


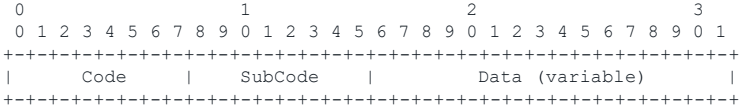
OMP Handshake Packet Format

Commonalities between OMP and BGP Packets



BGP Notification Packet Format

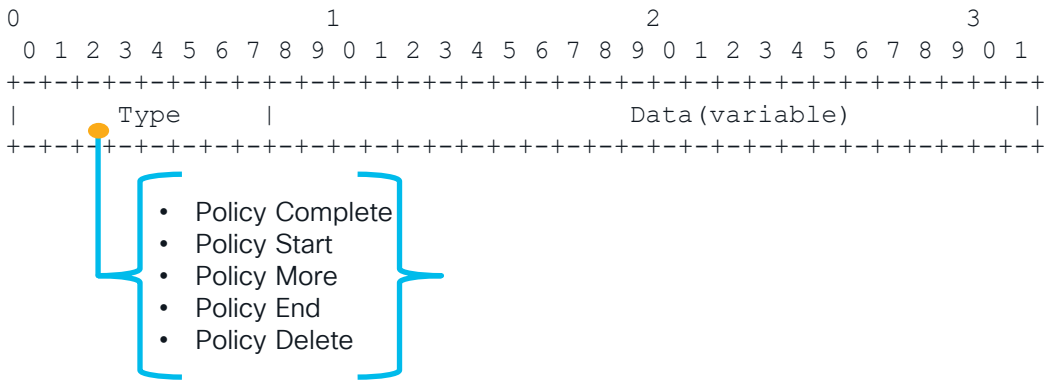




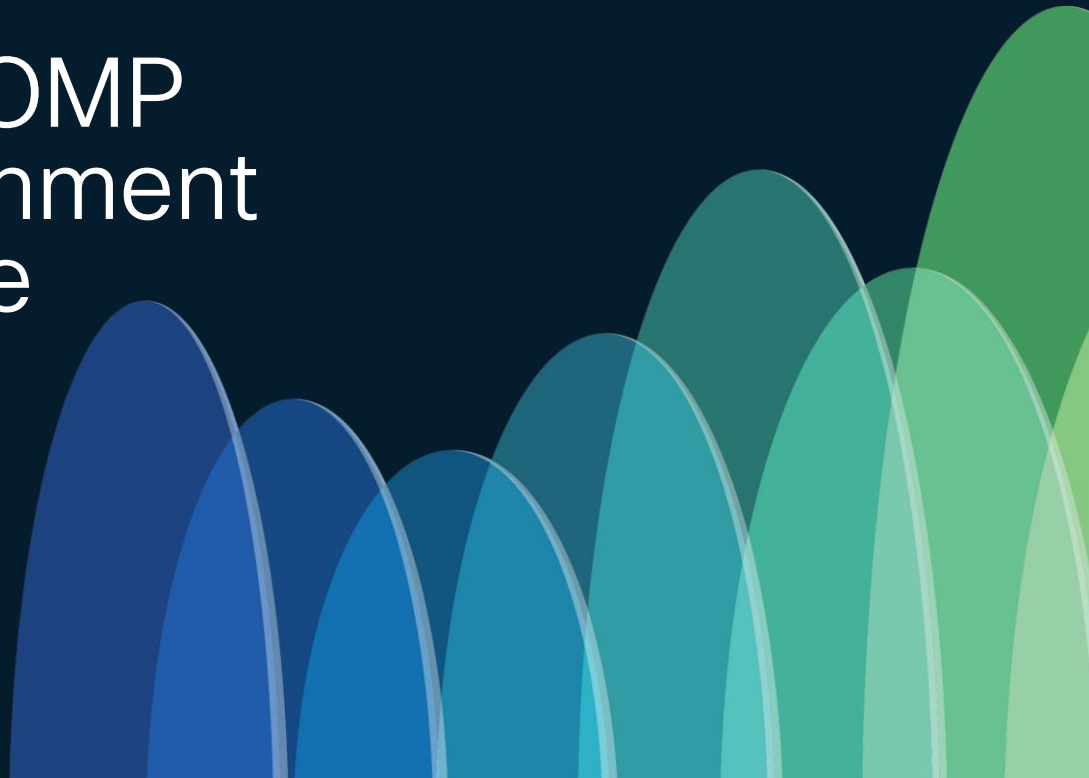
OMP Alert Packet Format

OMP Policy Packet Format

- SD-WAN policies are send in OMP Policy Packet.
- Maximum Policy packet size is 4000 bytes and if policy is huge then policy will be send in fragments.
- If policy data is less than 3980 (4000-20 TCP header) bytes, then Type field is set with Policy Complete.
- If policy data is more than 3980 bytes then it will be send in fragments with Type field is set to Policy Start, when first packet is send and with last fragment Type field is set to Policy End.

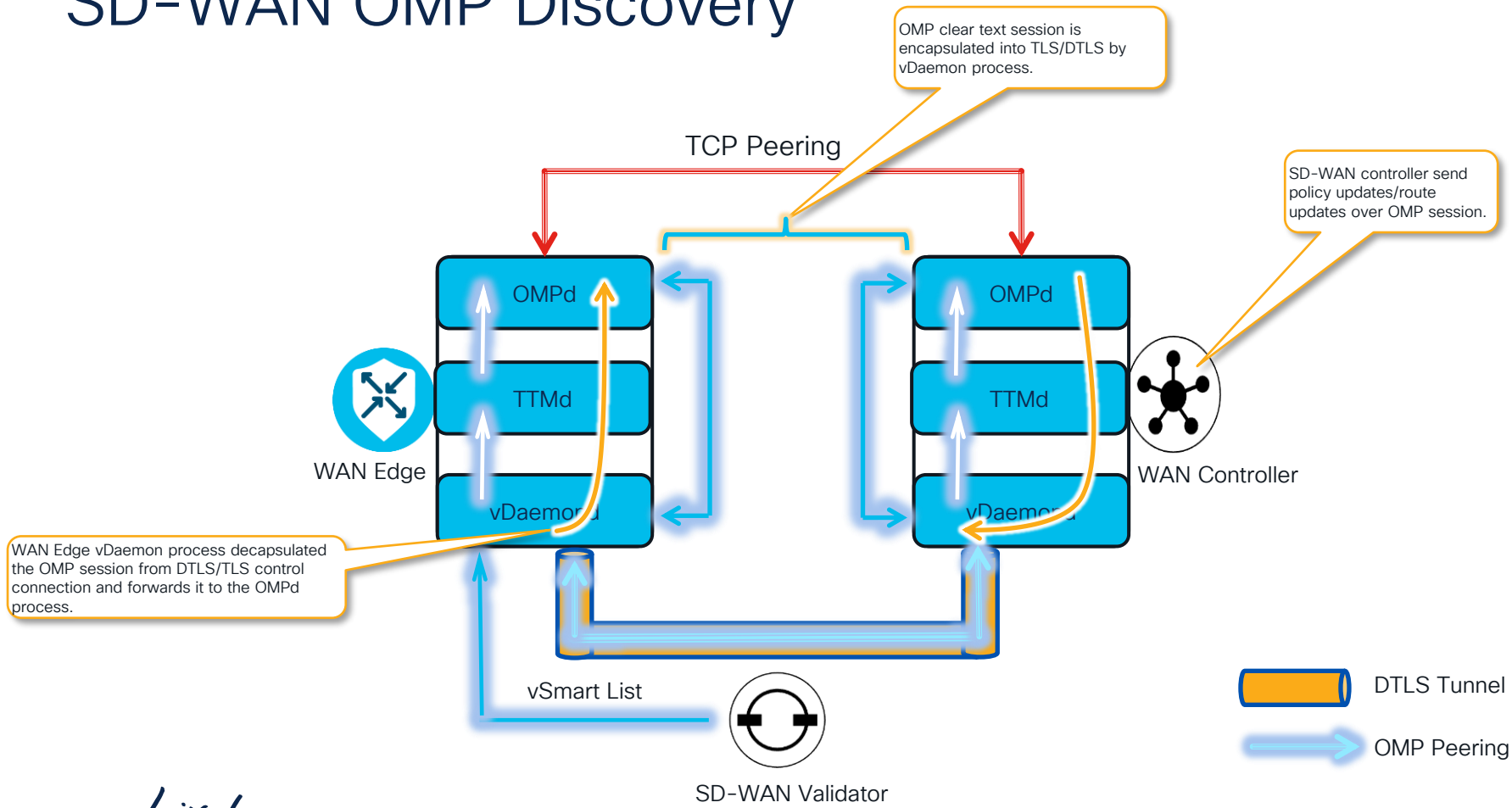


Walkthrough of OMP Session establishment at the WAN Edge Process level



cisco Live!

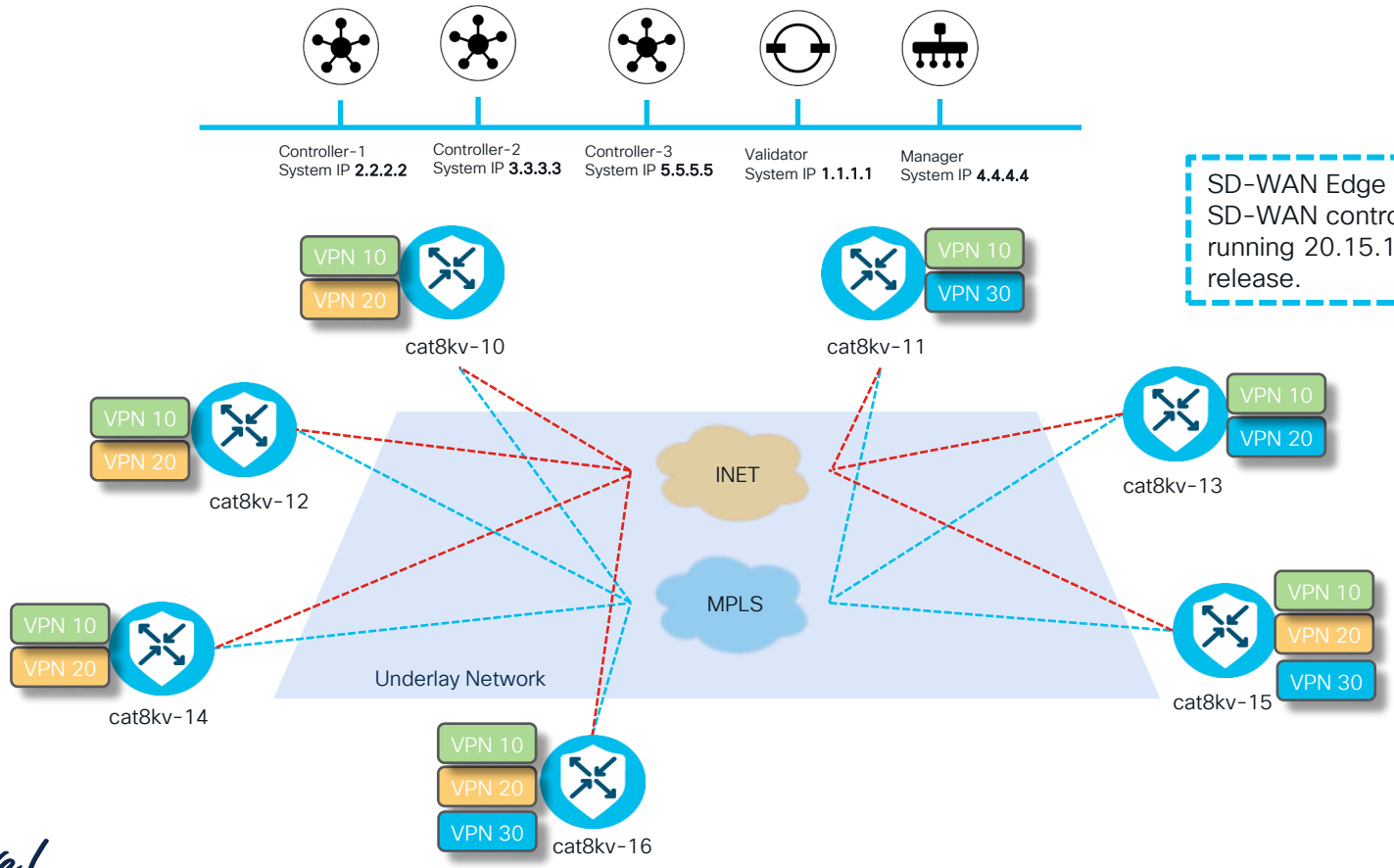
SD-WAN OMP Discovery



SDWAN OMP Peering Topology

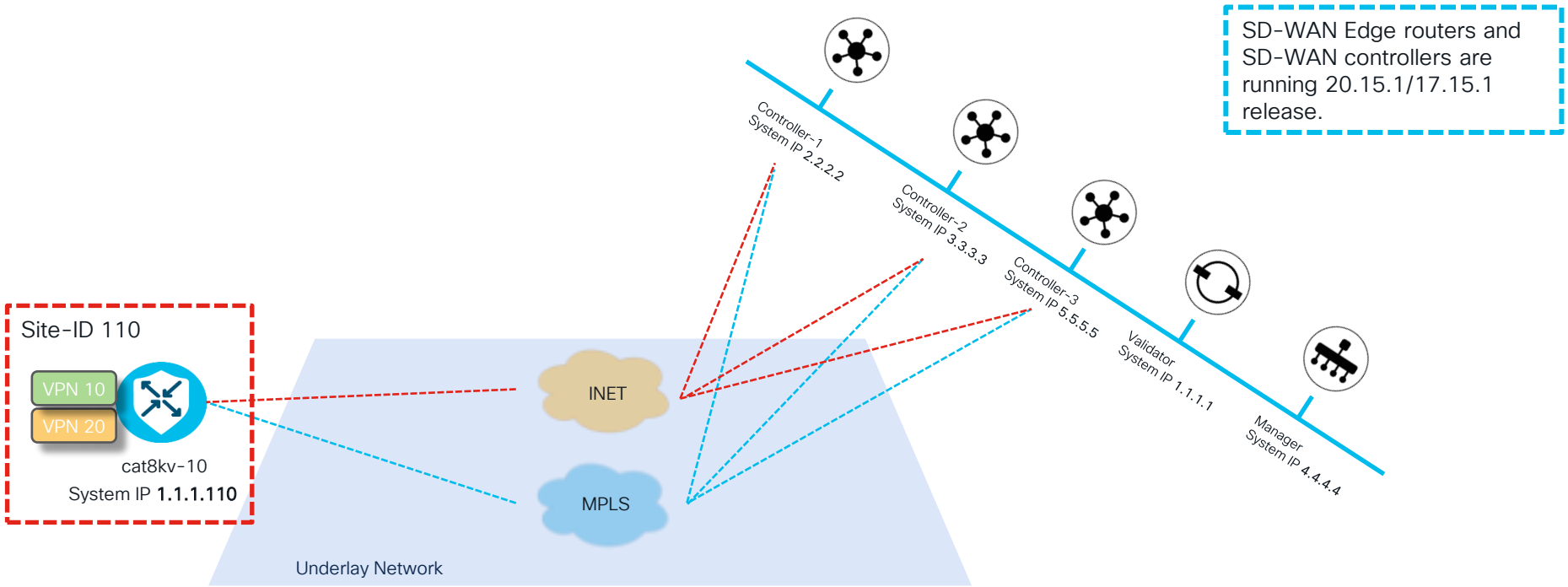
cisco Live!

A topic Catalyst SD-WAN demo topology



SD-WAN Edge routers and SD-WAN controllers are running 20.15.1/17.15.1 release.

A topic Catalyst SD-WAN demo topology



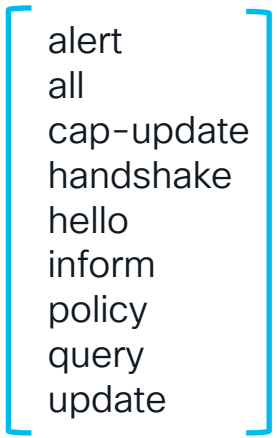
Navigating Through Logs During OMP Session Establishment

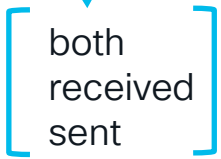
cisco Live!

How can I begin navigating through the OMP logs? 1/3

- From SD-WAN Edge perspective:
  - We can enable OMP debugging by using flags to filter peer OMP negotiation or OMP packets.
    - `[no]debug platform software sdwan omp packets "direction both peer-address <PEER-IP-ADDRESS> packet-type all"`

SD-WAN debug information does not appear in the output of the '**show debugging**' command.





How can I begin navigating through the OMP logs? 2/3

- From SD-WAN Edge perspective:
  - Starting from the 17.12 release, we need to enable traces for OMP process along with the module name and then we can view the messages exchanged between SD-WAN controller and SD-WAN Edge devices.
    - `set platform software trace ompd RP active ompd-pkt verbose`
    - `set platform software trace ompd RP active ompd-oper verbose`
    - `set platform software trace ompd RP active ompd-event verbose`
  - By default, all modules for OMP processes are set to the "Notice" level.
  - We can verify with the following command if OMP traces are enabled or not.
    - `show platform software trace level ompd rp active`
  - The following command will exhibit what flags are enabled for OMP debugging.
    - `show platform software sdwan omp debug`
  - To view the OMP debug messages:
    - `show logging process ompd internal`

Note: Once collected all the required logs/traces, set it back to "**Notice**"

How can I begin navigating through the OMP logs? 3/3

- From SD-WAN controller perspective:
  - The following debug can be enabled to view the OMP packet exchange between SD-WAN controllers and WAN-Edges.

```
Controller-1# debug omp
Possible completions:
  best-path          Debug OMP best-path calculation
  cxp                Debug OMP cloudexpress
  events             Debug OMP events
  graceful-restart   Debug OMP Graceful Restart
  identity           Debug OMP Identity
  ipcs               Debug OMP IPCs
  packets            Debug OMP packets
  policy             Debug OMP policy
```

  - All the debug logs are written by the SD-WAN controller in the following files.

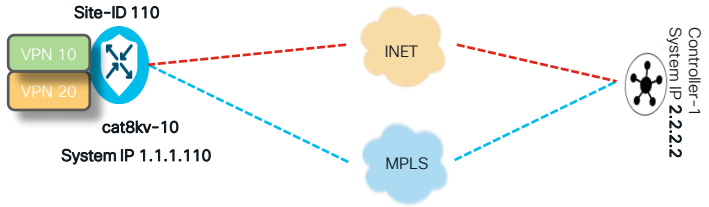
```
Controller-1# vshell
Controller-1:~$ tail -f /var/log/vdebug
```

```
Controller-1# vshell
Controller-1:~$ tail -f /var/log/tmplog/vdebug
```

Let’s enable debug and traces !!!

```
cat8kv-10#debug platform software sdwan omp packets "direction both peer-address 2.2.2.2 packet-type all"
cat8kv-10#set platform software trace ompd RP active ompd-pkt verbose
cat8kv-10#set platform software trace ompd RP active ompd-oper verbose
cat8kv-10#set platform software trace ompd RP active ompd-event verbose
```

```
cat8kv-10#show platform software trace level ompd rp active
Module Name                      Trace Level
----------------------------------------------
bcrpgc                           Informational
binos                            Notice
bipc                             Notice
btrace                           Notice
…
ompd                             Notice
ompd-bestpath                    Notice
ompd-config                      Notice
ompd-cxp                         Notice
ompd-event                       Verbose
ompd-idm                         Notice
ompd-ipc                         Notice
ompd-oper                        Verbose
ompd-pkt                         Verbose
ompd-policy                      Notice
…
vipcommon-sql                    Notice
vista                            Notice
vs_flock                         Notice
```




```
cat8kv-10#show platform software sdwan omp debug
   ================================
            DEBUG
   ================================
  Events: FALSE level: 0
  IPC: FALSE level: 0, peer_ip: 2.2.2.2
  Packets: TRUE Dir: Both
  Packet Type:  HANDSHAKE UPDATE ALERT HELLO QUERY
VSMART_CONFIG INFORM REGION-ID CAPABILITY-UPDATE
```

SD-WAN Edge debug out for OMP peering establishment 1/3

```
cat8kv-10#set logging marker OMP-PEER-DEBUGGING
cat8kv-10#show logging process ompd internal start marker OMP-PEER-DEBUGGING
Logging display requested on 2025/01/12 22:48:00 (CET) for Hostname: [cat8kv-10], Model: [C8000V], Version: [17.15.01a], SN:
[9LH68EOO2FF], MD_SN: [SSI130300YK]

Start marker [OMP-PEER-DEBUGGING] at timestamp ["2025/01/12 21:47:32.184564" UTC] found
executing cmd on chassis local ...
Start Marker: OMP-PEER-DEBUGGING
Unified Decoder Library Init .. DONE
Found 1 UTF Streams

2025/01/12 22:59:05.156791997 {smand_R0-0}{255}: Marker Msg: OMP-PEER-DEBUGGING
2025/01/12 22:59:24.420561408 {ompd_R0-0}{255}: [ompd-event] [23994]: (verbose): Peer 2.2.2.2 is Passive
2025/01/12 22:59:25.856554202 {ompd_R0-0}{255}: [vconfd] [23994]: (note): Enqueued blocking task [Set policy]
2025/01/12 22:59:25.856640162 {ompd_R0-0}{255}: [vconfd] [23994]: (note): Enqueued blocking task [Set Tag-Instances]
2025/01/12 22:59:25.856644144 {ompd_R0-0}{255}: [ompd-event] [23994]: (verbose): Connect retry timer expired for 2.2.2.2
2025/01/12 22:59:25.856644781 {ompd_R0-0}{255}: [ompd-event] [23994]: (verbose): Trying to active connect to 2.2.2.2
2025/01/12 22:59:25.858266698 {ompd_R0-0}{255}: [vconfd] [23994:24090]: (note): Blocking task [Set policy] now scheduled
2025/01/12 22:59:25.858269249 {ompd_R0-0}{255}: [ompd-event] [23994:24090]: (debug): Applying forwarding policy of size: 779
bytes
2025/01/12 22:59:25.859948642 {ompd_R0-0}{255}: [ompd-event] [23994]: (debug): Tenant 0 client port number 56087
2025/01/12 22:59:25.861364924 {ompd_R0-0}{255}: [ompd-event] [23994]: (verbose): Received active connect event 0x80
2025/01/12 22:59:25.861366558 {ompd_R0-0}{255}: [ompd-event] [23994]: (verbose): Received connect from 2.2.2.2
2025/01/12 22:59:25.861373225 {ompd_R0-0}{255}: [ompd-event] [23994]: (verbose): Peer: 2.2.2.2, fd: 70, setsockopt successful!
2025/01/12 22:59:25.861374437 {ompd_R0-0}{255}: [ompd-event] [23994]: (debug): Peer: 2.2.2.2, New Event: Connected curr state:
Init
…
<continue>
```

SD-WAN Edge debug out for OMP peering establishment 2/3

```
2025/01/12 22:59:25.861380181 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Sent HANDSHAKE message 173 bytes: peer: 2.2.2.2
2025/01/12 22:59:25.861381266 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Version: 1 Holdtime: 300 site: 110 domain: 1
2025/01/12 22:59:25.861383498 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Peer-ID: 110.1.1.1 Options-Length: 138
2025/01/12 22:59:25.861384433 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Option-Type: Capabilities(2) Option-Length: 136
2025/01/12 22:59:25.861385354 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Capability: Multi-Protocol Length: 4
2025/01/12 22:59:25.861385603 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Value:
2025/01/12 22:59:25.861386659 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): AFI: ipv4(1) SAFI: tloc(2) VERSION:0
2025/01/12 22:59:25.861386972 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Capability: Multi-Protocol Length: 4
2025/01/12 22:59:25.861387200 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Value:
2025/01/12 22:59:25.861387777 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): AFI: l2(3) SAFI: L2VPN-Status(12) VERSION:0
2025/01/12 22:59:25.861401506 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Capability: Multi-Protocol Length: 4
2025/01/12 22:59:25.861401733 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Value:
2025/01/12 22:59:25.861402039 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): AFI: ipv4(1) SAFI: vroute(1) VERSION:0
2025/01/12 22:59:25.861402254 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Capability: Multi-Protocol Length: 4
2025/01/12 22:59:25.861402457 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Value:
2025/01/12 22:59:25.861402668 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): AFI: ipv6(2) SAFI: vroute(1) VERSION:0
2025/01/12 22:59:25.861402887 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Capability: Multi-Protocol Length: 4
2025/01/12 22:59:25.861403090 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Value:
2025/01/12 22:59:25.861403442 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): AFI: ipv4(1) SAFI: multicast(4) VERSION:2
2025/01/12 22:59:25.861403665 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Capability: Multi-Protocol Length: 4
2025/01/12 22:59:25.861403870 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Value:
2025/01/12 22:59:25.861404201 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): AFI: ipv4(1) SAFI: Link(6) VERSION:0
2025/01/12 22:59:25.861414617 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Capability: Identity Length: 4 Value: vEdge
2025/01/12 22:59:25.861414899 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Capability: Graceful-Restart Length: 4 Value:
43200
2025/01/12 22:59:25.861470333 {ompd_R0-0}{255}: [errmsg] [23994]: (info): %OMPD-6-PEER_STATE_HANDSHAKE: R0/0: ompd: vSmart peer
2.2.2.2 state changed to Handshake
2025/01/12 22:59:25.861475017 {ompd_R0-0}{255}: [ompd-event] [23994]: (verbose): Peer: 2.2.2.2, New State: Handshake
```

SD-WAN Edge debug out for OMP peering establishment 3/3

```
2025/01/12 22:59:25.862722222 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Received HANDSHAKE message 155 bytes: peer:
2.2.2.2
2025/01/12 22:59:25.862723520 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Version: 1 Holdtime: 300 site: 100 domain: 1
2025/01/12 22:59:25.862726338 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Peer-ID: 2.2.2.2 Options-Length: 120
2025/01/12 22:59:25.862726979 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Option-Type: Capabilities(2) Option-Length: 118
2025/01/12 22:59:25.862727444 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Capability: Multi-Protocol Length: 4
2025/01/12 22:59:25.862727735 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Value:
2025/01/12 22:59:25.862728225 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): AFI: ipv4(1) SAFI: tloc(2) VERSION:0
2025/01/12 22:59:25.862728587 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Capability: Multi-Protocol Length: 4
2025/01/12 22:59:25.862728972 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Value:
2025/01/12 22:59:25.862729330 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): AFI: l2(3) SAFI: L2VPN-Status(12) VERSION:0
2025/01/12 22:59:25.862757162 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Capability: Multi-Protocol Length: 4
2025/01/12 22:59:25.862757366 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Value:
2025/01/12 22:59:25.862757577 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): AFI: l2(3) SAFI: vroute(1) VERSION:0
2025/01/12 22:59:25.862758136 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Capability: Identity Length: 4 Value: vSmart
2025/01/12 22:59:25.862758463 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Capability: Graceful-Restart Length: 4 Value:
43200
2025/01/12 22:59:25.862758717 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Capability: Refresh Length: 0
2025/01/12 22:59:25.862758997 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Capability: Security Length: 0
2025/01/12 22:59:25.862759245 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Capability: Overlay ID Length: 4 Value: 1
2025/01/12 22:59:25.862759543 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose):
2025/01/12 22:59:25.862767348 {ompd_R0-0}{255}: [ompd-event] [23994]: (debug): Peer: 2.2.2.2, New Event: Handshake Recv curr
state: Handshake
2025/01/12 22:59:25.862770653 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Sent HELLO message of length: 27: peer: 2.2.2.2
(in: 155, out: 0)
2025/01/12 22:59:25.863166551 {ompd_R0-0}{255}: [ompd-pkt] [23994]: (verbose): Received HELLO message of length: 19: peer:
2.2.2.2 (in: 19, out: 0)
2025/01/12 22:59:25.863808921 {ompd_R0-0}{255}: [ompd-event] [23994]: (verbose): Peer: 2.2.2.2, New State: UP
```

SD-WAN Edge OMP peering is UP !!!

```
cat8kv-10#show sdwan omp peers
R -> routes received
I -> routes installed
S -> routes sent

TENANT                              DOMAIN     OVERLAY    SITE       REGION
ID         PEER             TYPE    ID         ID         ID         ID         STATE    UPTIME           R/I/S
-------------------------------------------------------------------------------------------------------------------
0          2.2.2.2          vsmart  1          1          100        None       up       0:00:42:10       148/148/30
0          3.3.3.3          vsmart  1          1          100        None       up       32:01:59:57      148/0/30
```

- Use the following command on SD-WAN Edge device to see all the negotiated parameters , advertised TLOC's, address families etc.. with SD-WAN controller.
  - `show platform software sdwan omp peer <PEER-IP>`
- Same command is available also on SD-WAN controller.
  - `show support omp peer peer-ip <PEER-IP>`

SD-WAN Edge OMP peer output

```
cat8kv-10# show platform software sdwan omp peer 2.2.2.2
========================================
 PEERS for CONTEXT 1.1.1.110, Tenant id: 0
========================================
 Local address: 1.1.1.110
 Looking up Peer: 2.2.2.2
 Peer: 2.2.2.2 (0x6545ec5d3298), Type: vSmart, Site: 100, Region-id-set: None, Domain: 1, Overlay: 1, Legit: yes
        State: Up, version: 1, Control-Up: yes, Staging: no, flags: 0x21
        Multithreading- down: no, move-marker: no, update-gen: no, work-queue: no, needs_upd:0x0
        buffer ev: 0x0x6545ec5dede8, src_port 56087
        fd: 70
        Hello timer: Enabled (e: 49, c: 100, md: 100 lmd: 0)  Hold timer: Enabled (e: 285 v: 300 c: 300) Expiry-Alert-Send-Fail-Count: 0
        Connect retry: Disabled (e: -1 v: 2 c: 2)  Adv. timer: Enabled (e: 1 v: 1 c: 1)
        Down-pending: Disabled (e: -1 v: 1 c: 1)
    EOR interval: 300 EOR timer: Disabled (e: -1 v: 300)

    Force-Send interval: 2 Force-Send timer: Disabled (e: -1 v: 2)

        Rcv cap: Identity MP GR Refresh Security Overlay
        Neg cap: Identity MP GR Refresh Security Overlay
        Rcv afi-safi: TLOC-IPV4 STATUS-L2 SRVC-IPV4 SRVC-IPV6 SRVC-L2 ROUTE-IPV4 ROUTE-IPV6 MCAST-IPV4 (2) LINK CXP (2) IDENTITY-USER
IDENTITY-IPV4-TO-USER IDENTITY-IPV6-TO-USER IDENTITY-IPV4-TO-SGT IDENTITY-IPV6-TO-SGT ROUTE-L2
        Neg afi-safi: TLOC-IPV4 STATUS-L2 SRVC-IPV4 SRVC-IPV6 SRVC-L2 ROUTE-IPV4 ROUTE-IPV6 MCAST-IPV4 (2) LINK CXP (2) IDENTITY-USER
IDENTITY-IPV4-TO-USER IDENTITY-IPV6-TO-USER IDENTITY-IPV4-TO-SGT IDENTITY-IPV6-TO-SGT ROUTE-L2
        GR-enabled: Enabled, My GR interval: 43200 GR timer: Disabled (e: -1 v: 43200 c: 43200)
        Enter gr: 1, Exit gr: 1, GR mode: FALSE
        site-pol: None route-pol-in: None route-pol-out: None data-pol-in: None
           data-pol-out: None pfr-pol: None mem-pol: None cflowd:None
        UP time: Sun Jan 12 22:59:25 2025
<snip>
```

SD-WAN Edge OMP peer output

```
Needs Update gen: 0x0

        TLOC-IPV4:
           EOR - TX: 1 RX: 1
           Browse-Done: 1 Force-Send: 0
           received: 12 installed: 12 sent: 2
           ri-cleanup: 48 ro-cleanup: 8 ri-reeval: 0 reeval: 0
           marker-reset: 0 routes-browse: 1955 ri-browsed: 1955 te-changed: 0
           ctx-rib-version: 2857 peer-ro-version: 2857
        ROUTE-IPV4:
           EOR - TX: 1 RX: 1
           Browse-Done: 1 Force-Send: 0
           received: 82 installed: 82 sent: 20
           ri-cleanup: 288 ro-cleanup: 64 ri-reeval: 0 reeval: 0
           marker-reset: 0 routes-browse: 3264 ri-browsed: 12317 te-changed: 0
           ctx-rib-version: 9169 peer-ro-version: 9169

            Updates pending: No, Withdraws pending: No
        ROUTE-IPV6:
           EOR - TX: 1 RX: 1
           Browse-Done: 1 Force-Send: 0
           received: 66 installed: 66 sent: 4
           ri-cleanup: 216 ro-cleanup: 28 ri-reeval: 0 reeval: 0
           marker-reset: 0 routes-browse: 39003 ri-browsed: 86485 te-changed: 0
           ctx-rib-version: 129135 peer-ro-version: 129135

            Updates pending: No, Withdraws pending: No
<snip>
```

How can we see the OMP policy packets?

- Following debugs needs to be enable on SD-WAN controller to see the OMP policy packet exchanged, while pushing SD-WAN policies.
  - `debug omp events level high`
  - `debug omp policy level high`
  - `debug omp policy direction both`
  - `debug omp packets packet-type policy direction both`
- The following traces must be enabled on WAN edge to see the exchange of OMP policy packets while SD-WAN policies are being pushed.
  - `set platform software trace ompd RP active ompd-policy verbose`
  - `set platform software trace ompd RP active ompd-pkt verbose`
  - `set platform software trace ompd Rp active ompd-event verbose`
- We can verify with the following command if OMP traces are enabled or not.
  - `show platform software trace level ompd rp active`

How to read OMP policy packet logs on controller 1/3?

```
Controller1# vshell
Controller1:~$ tail -f /var/log/vdebug
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_pkt_encode_policy[701]: Peer 1.1.1.110, total fragments: 4, pol_size: 14085
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_pkt_encode_policy[734]: Peer 1.1.1.110, type: START Current fragments: 1,
frag_len: 1 cfg_sub_type = 3979
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_debug_pkt_policy[1621]: Sent POLICY message 4000 bytes: peer: 1.1.1.110
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_debug_pkt_policy[1636]:    length: 4000, pol_sub_type: STARTcfg_sub_type = POLICY
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_debug_pkt_policy[1640]:  Forwarding (data + pfr): <data-policy>
  <name>_ALL-VPN_Data-Policy-QoS-Demo</name>
  <vpn-list>
    <name>ALL-VPN</name>
    <sequence>
      <seq-value>1</seq-value>
      <match>
        <source-data-prefix-list>Data-Prefix-Trex-Site-201</source-data-prefix-list>
        <destination-data-prefix-list>Data-Prefix-Trex-Site-200</destination-data-prefix-list>
        <source-port>63000</source-port>
        <destination-port>53000</destination-port>
      </match>
      <action>
        <action-value>accept</action-value>
        <count>DP-Port-63000_-1125422396</count>
        <log/>
        <set>
          <forwarding-class>REAL-TIME</forwarding-class>
        </set>
      </action>
…
<continue>
```

How to read OMP policy packet logs on controller 2/3?

```
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_debug_pkt_policy[1641]:
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_pkt_encode_policy[734]: Peer 1.1.1.110, type: MORE Current fragments: 2,
frag_len: 1 cfg_sub_type = 3979
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_debug_pkt_policy[1621]: Sent POLICY message 4000 bytes: peer: 1.1.1.110
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_debug_pkt_policy[1636]:    length: 4000, pol_sub_type: MOREcfg_sub_type = POLICY
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_debug_pkt_policy[1640]:  Forwarding (data + pfr): lass>
</action>
    </sequence>
    <sequence>
      <seq-value>21</seq-value>
      <match>
        <source-data-prefix-list>Data-Prefix-Trex-Site-201</source-data-prefix-list>
        <destination-data-prefix-list>Data-Prefix-Trex-Site-200</destination-data-prefix-list>
        <source-port>6200</source-port>
        <destination-port>5200</destination-port>
        <protocol>17</protocol>
      </match>
…
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_debug_pkt_policy[1641]:
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_pkt_encode_policy[734]: Peer 1.1.1.110, type: MORE Current fragments: 3,
frag_len: 1 cfg_sub_type = 3979
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_debug_pkt_policy[1621]: Sent POLICY message 4000 bytes: peer: 1.1.1.110
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_debug_pkt_policy[1636]:    length: 4000, pol_sub_type: MOREcfg_sub_type = POLICY
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_debug_pkt_policy[1640]:  Forwarding (data + pfr): <color>
    <color-name>private1</color-name>
    <dscp>8</dscp>
  </color>
</app-probe-class>
…
<continue>
```

How to read OMP policy packet logs on controller 3/3?

```
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_debug_pkt_policy[1641]:
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_pkt_encode_policy[734]: Peer 1.1.1.110, type: END Current fragments: 4, frag_len:
1 cfg_sub_type = 2148
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_debug_pkt_policy[1621]: Sent POLICY message 2169 bytes: peer: 1.1.1.110
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_debug_pkt_policy[1636]:    length: 2169, pol_sub_type: ENDcfg_sub_type = POLICY
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_debug_pkt_policy[1640]:  Forwarding (data + pfr): sh</name>
  </app>
  <app>
    <name>live_storage</name>
  </app>
  <app>
…
 <app>
    <name>yammer</name>
  </app>
</app-list>
</lists>ame>google_groups</n
Jan  5 22:51:15 Controller1 OMPD[2113]: omp_debug_pkt_policy[1641]:
```

How to read OMP policy packet logs on WAN-Edge?

```
cat8kv-10#show logging process ompd internal
…
2025/01/05 23:45:34.296078349 {ompd_R0-0}{255}: [ompd-pkt] [22843]: (verbose): Received POLICY message 4000 bytes: peer: 2.2.2.2
2025/01/05 23:45:34.296081770 {ompd_R0-0}{255}: [ompd-pkt] [22843]: (verbose): length: 4000, type: START
2025/01/05 23:45:34.296085881 {ompd_R0-0}{255}: [ompd-pkt] [22843]: (verbose):  Forwarding (data + pfr): <data-policy>
  <name>_ALL-VPN_Data-Policy-QoS-Demo</name>
  <vpn-list>
…
2025/01/05 23:45:34.296156109 {ompd_R0-0}{255}: [ompd-event] [22843]: (verbose): Partial message for peer 2.2.2.2, bailing
2025/01/05 23:45:34.296175046 {ompd_R0-0}{255}: [ompd-pkt] [22843]: (verbose): Received POLICY message 4000 bytes: peer: 2.2.2.2
2025/01/05 23:45:34.296175829 {ompd_R0-0}{255}: [ompd-pkt] [22843]: (verbose): length: 4000, type: MORE
2025/01/05 23:45:34.296178825 {ompd_R0-0}{255}: [ompd-pkt] [22843]: (verbose):  Forwarding (data + pfr): lass>
      </action>
    </sequence>
    <sequence>
…
2025/01/05 23:45:34.305498345 {ompd_R0-0}{255}: [ompd-event] [22843]: (verbose): Partial message for peer 2.2.2.2, bailing
2025/01/05 23:45:34.306100223 {ompd_R0-0}{255}: [ompd-pkt] [22843]: (verbose): Received POLICY message 4000 bytes: peer: 2.2.2.2
2025/01/05 23:45:34.306102732 {ompd_R0-0}{255}: [ompd-pkt] [22843]: (verbose): length: 4000, type: MORE
2025/01/05 23:45:34.306107332 {ompd_R0-0}{255}: [ompd-pkt] [22843]: (verbose):  Forwarding (data + pfr): <color>
    <color-name>private1</color-name>
    <dscp>8</dscp>
…
2025/01/05 23:45:34.306125175 {ompd_R0-0}{255}: [ompd-pkt] [22843]: (verbose):
2025/01/05 23:45:34.306149702 {ompd_R0-0}{255}: [ompd-pkt] [22843]: (verbose): Received POLICY message 2169 bytes: peer: 2.2.2.2
2025/01/05 23:45:34.306150713 {ompd_R0-0}{255}: [ompd-pkt] [22843]: (verbose): length: 2169, type: END
2025/01/05 23:45:34.306154298 {ompd_R0-0}{255}: [ompd-pkt] [22843]: (verbose):  Forwarding (data + pfr): sh</name>
  </app>
  <app>
..
2025/01/05 23:45:34.306163615 {ompd_R0-0}{255}: [ompd-pkt] [22843]: (verbose):
```

How can we verify if policy is being applied correctly?

```
Controller1#show support omp peer peer-ip 1.1.1.112

================================
            PEERS for CONTEXT 2.2.2.2
================================
 Local address: 2.2.2.2
 Looking up Peer: 1.1.1.112
 Peer: 1.1.1.112 (0x7fd8cd031800), Type: vEdge, Site: 112, Region-id-set: None, Domain: 1, Overlay: 1, Legit: yesa
        State: Up, version: 1, Control-Up: yes, Staging: no, flags: 0x21, Peer ID: 4
        CAP: TLOC color supported bitmap: 0x20004, TLOC color supported list: mpls private1
        CAP: BR: no, TGW: no MGW: no MGMT-REGION: no
        Multithreading- down: no, move-marker: no, update-gen: no, work-queue: no, needs_upd: 0x0
        buffer ev: 0x0x7fd949672400
        fd: 29
        Hello timer: Enabled (e: 73, c: 100, md: 100 lmd: 0)  Hold timer: Enabled (e: 225 v: 300 c: 300) Expiry-Alert-Send-Fail-Count: 0
        Connect retry: Disabled (e: -1 v: 2 c: 2)  Adv. timer: Enabled (e: 1 v: 1 c: 1)
        Down-pending: Disabled (e: -1 v: 1 c: 1)
    EOR interval: 300 EOR timer: Disabled (e: -1 v: 300)

    Force-Send interval: 2 Force-Send timer: Disabled (e: -1 v: 2)

        Rcv cap: Identity MP GR Refresh Security Overlay Network-Identity VSmart-Configuation
        Neg cap: Identity MP GR Refresh Security Overlay Network-Identity VSmart-Configuation
        Rcv afi-safi: TLOC-IPV4 SRVC-IPV4 SRVC-IPV6 ROUTE-IPV4 ROUTE-IPV6 MCAST-IPV4 (2) LINK CXP (2) IDENTITY-USER IDENTITY-IPV4-TO-USER
IDENTITY-IPV6-TO-USER IDENTITY-IPV4-TO-SGT IDENTITY-IPV6-TO-SGT
        Neg afi-safi: TLOC-IPV4 SRVC-IPV4 SRVC-IPV6 ROUTE-IPV4 ROUTE-IPV6 MCAST-IPV4 (2) LINK CXP (2) IDENTITY-USER IDENTITY-IPV4-TO-USER
IDENTITY-IPV6-TO-USER IDENTITY-IPV4-TO-SGT IDENTITY-IPV6-TO-SGT
        GR-enabled: Enabled, My GR interval: 43200 GR timer: Disabled (e: -1 v: 43200 c: 43200)
        Enter gr: 0, Exit gr: 0, GR mode: FALSE
        site-pol: SPOKE-SITES route-pol-in: None route-pol-out: CiscoLive-Active-Backup-Hub-Demo data-pol-in: None
           data-pol-out: None pfr-pol: None mem-pol: None cflowd:None
```

How can we verify if policy is being applied correctly?

```
Controller1# show omp peers 1.1.1.112 detail

peer                     1.1.1.112
type                     vedge
domain-id                1
site-id                  112
overlay-id               1
region-id                None
state                    up
version                  1
legit                    yes
control-up               yes
staging                  no
upcount                  1
downcount                0
last-uptime              2025-01-12T14:49:02+00:00
last-downtime            0000-00-00T00:00:00+00:00
uptime                   0:09:39:41
hold-time                300
site-policy              SPOKE-SITES
policy-out               CiscoLive-Active-Backup-Hub-Demo
graceful-restart         supported
graceful-restart-interval 43200
network-identity         supported
identity-gr              not-supported
identity-gr-interval
refresh                  supported
hello-sent               15520
hello-received           15542
handshake-sent           4
handshake-received       4
alert-sent               3
alert-received           0
inform-sent              42
inform-received          42
update-sent              1680
update-received          162
policy-sent
policy-received
```

Control policy applied.

Only incremented when centralized Data policy applied.

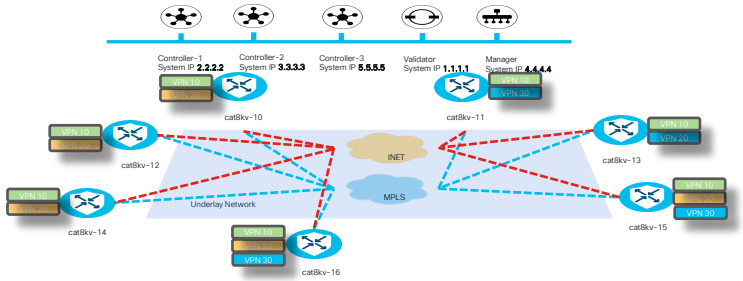
How to read OMP summary output?

```
cat8kv-10#show sdwan omp summary
oper-state                UP
admin-state               UP
personality               vedge
device-role               Edge-Router
omp-uptime                0:00:34:34
routes-received           320
routes-installed          100
routes-sent               60
tlocs-received            38
tlocs-installed           12
tlocs-sent                6
services-received         4
services-installed        0
services-sent             12
mcast-routes-received     0
mcast-routes-installed    0
mcast-routes-sent         0
hello-sent                78
hello-received            63
handshake-sent            3
handshake-received        3
alert-sent                0
alert-received            0
inform-sent               39
inform-received           39
update-sent               63
update-received           255
policy-sent               0
policy-received           12
total-packets-sent        183
total-packets-received    375
vsmart-peers              3
```

Hello-sent 78 +
Handshake-sent 3 +
Alert-sent. 0 +
Inform-sent. 39 +
Update-sent 63 +
Policy-sent. 0 = **183 packets.**

We have total 7 WAN-Edges with 2 TLOCs each, so total 6 X 2 = **12 TLOCS installed.**

We have 2 TLOCs (private1, internet) as we have 3 OMP peering so total **3 X 2 = 6 TLOC-send**.



We have **3 OMP peering** and our policy is send in **4 fragments** from 3 SD-WAN controllers. So, **total policy packet received is 12**.

How can we verify if policy is being applied correctly?

```
Controller1#show support policy route-policy

================================
  ROUTE POLICIES
================================

route-policy CiscoLive-Active-Backup-Hub-Demo
seq-num 187
users-count 5
action srvc/srvc-chain/tloc/tloc-list/affinity counts: 0/0/0/1/0
Policy TLOC-Interest Database:
   TLOC:1.1.1.110 : mpls : ipsec Ref-Count: 1
   TLOC:1.1.1.110 : private1 : ipsec Ref-Count: 1
   TLOC:1.1.1.111 : mpls : ipsec Ref-Count: 1
   TLOC:1.1.1.111 : private1 : ipsec Ref-Count: 1

    sequence: 1
        match tloc [SITE-LIST  (0x1) ]
            site-list: SPOKE-SITES (0x7fd8ccfb3680)
        action: reject
        set: [ (0x0) ]
    sequence: 11
        match tloc [SITE-LIST  (0x1) ]
            site-list: DC-LIST (0x7fd94962af00)
        action: accept
        set: [ (0x0) ]
    sequence: 21
        match route [SITE-LIST PFX-LIST  (0x11) ]
            site-list: SPOKE-SITES (0x7fd8ccfb3680)
            IPv4 prefix-list: _AnyIpv4PrefixList (0x7fd8cd00a480)
        action: accept
        set: [TLOC-LIST  (0x20) ]
            tloc-list: HUB-TLOCS [none]
    default-action: reject, fetch_xml: 1

  Users:
  1.1.1.112, type: route, dir: out, policy: CiscoLive-Active-Backup-Hub-Demo (0x7fd8cd01ae00), ctx: 0x7fd8cd031800, cb: 0x55fbf77bc4ac, change: no
  1.1.1.113, type: route, dir: out, policy: CiscoLive-Active-Backup-Hub-Demo (0x7fd8cd01ae00), ctx: 0x7fd8cd034000, cb: 0x55fbf77bc4ac, change: no
  1.1.1.114, type: route, dir: out, policy: CiscoLive-Active-Backup-Hub-Demo (0x7fd8cd01ae00), ctx: 0x7fd9493a0800, cb: 0x55fbf77bc4ac, change: no
  1.1.1.115, type: route, dir: out, policy: CiscoLive-Active-Backup-Hub-Demo (0x7fd8cd01ae00), ctx: 0x7fd9496a7800, cb: 0x55fbf77bc4ac, change: no
  1.1.1.116, type: route, dir: out, policy: CiscoLive-Active-Backup-Hub-Demo (0x7fd8cd01ae00), ctx: 0x7fd94939e000, cb: 0x55fbf77bc4ac, change: no
```

My OMP Peering is down, where to start?

cisco Live!

What steps should be taken if OMP peering fails to establish?

- Check if Control Connection (**CC**) is up between SD-WAN Edge and SD-WAN controller?
- If NOT, then we need to troubleshoot first, why CC is not coming up?

- If CC is UP but still OMP peering is not coming UP, then verify that **system-ip** is **NOT** overlapping in SD-WAN overlay.

- OMPd process crashed that cause OMP peering failed to establish.
- We can check the status if OMPd process crash/rebooted with the following commands
  - On SD-WAN Controller:
    - `show system status`
    - `show support omp peer peer-ip <PEER-IP>`
  - On SD-WAN Router:
    - `show platform software sdwan omp peer <PEER-IP>`
    - `show sdwan crash`
- Memory consumption/leakage can also cause OMP peering issue and can be seen with the following commands:
    - `[SD-WAN Edge] show platform software process memory r0 all sorted | include ompd`
    - `[SD-WAN Controller] show support omp memory-statistics`

Interesting SHOW commands for OMP debugging !!!

- SD-WAN Controller
  - `show omp peers`
  - `show omp peers <PEER-IP> detail`
  - `show omp summary`
  - `show support omp context`
  - `show support omp daemon`
  - `show support policy route-policy`
  - `show support omp peer peer-ip <PEER-IP>`
  - `show support omp rib vroute <VPN-ID:Prefix/Length>`
  - `show support omp memory-statistics`
  - `show support omp label-db`
- SD-WAN Edge
  - `show sdwan omp summary`
  - `show sdwan omp peers`
  - `show platform software sdwan omp omp daemon`
  - `show platform software sdwan omp peer`
  - `show platform software sdwan omp peer-ip <PEER-IP>`
  - `show platform software sdwan omp rib vroute vpn <VPN> <Prefix/Length>`
  - `show platform software sdwan omp rib tloc <TLOC-IP> <COLOR> <Encap>`
  - `show platform software sdwan omp memory`

What is OMP Graceful Restart?

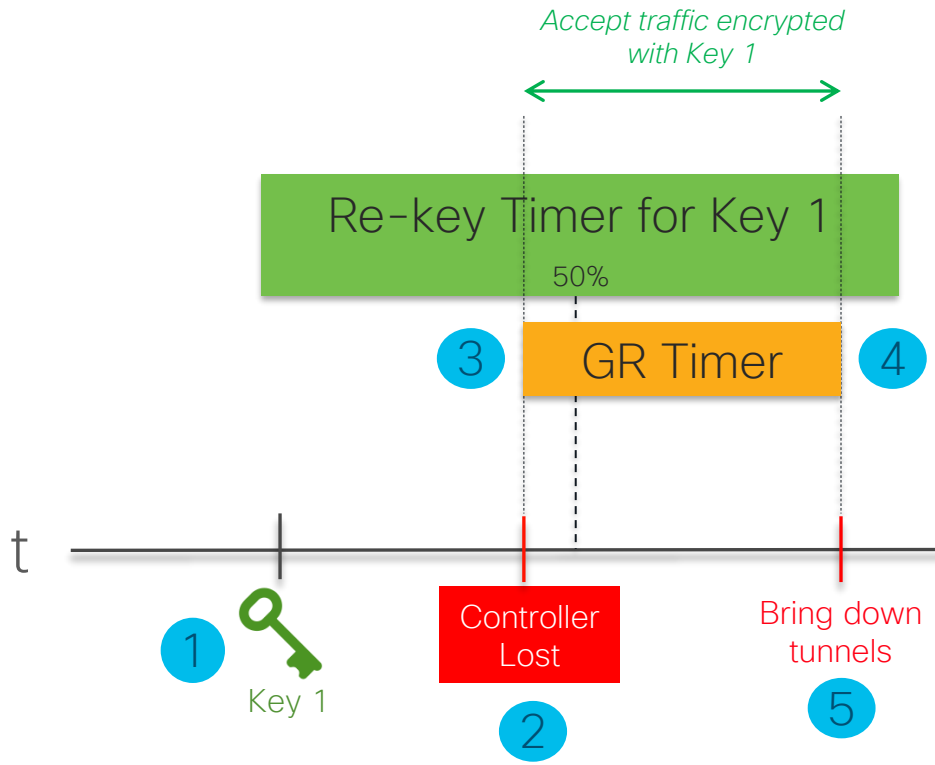
OMP graceful restart allows OMP peers to continue operating if one of the peers becomes unavailable.

WAN Edge router and a SD-WAN controller cache the OMP information that they learn from their peer.

OMP graceful restart timer tells the OMP peer how long to retain the cached advertised routes.

Loss During First 50% of IPSec Re-Key Timer

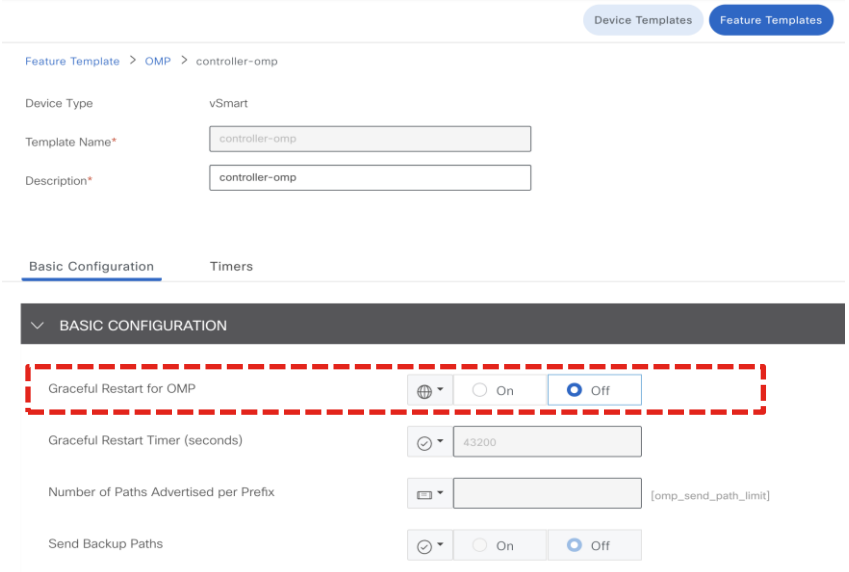
Re-key timer twice or more OMP Graceful Restart timer



1. Encryption key received
2. Controllers are lost
3. GR is triggered
4. GR expires
5. Tunnels go down

There is a valid encryption key for the entire duration of GR

OMP Graceful Restart – Off



- Graceful Restart for OMP = Off at all SD-WAN Controllers means Graceful Restart is disabled on all SD-WAN Edges.
- OMP Routing Table and BFD Session are lost immediately when SD-WAN Edges loses all OMP peers.

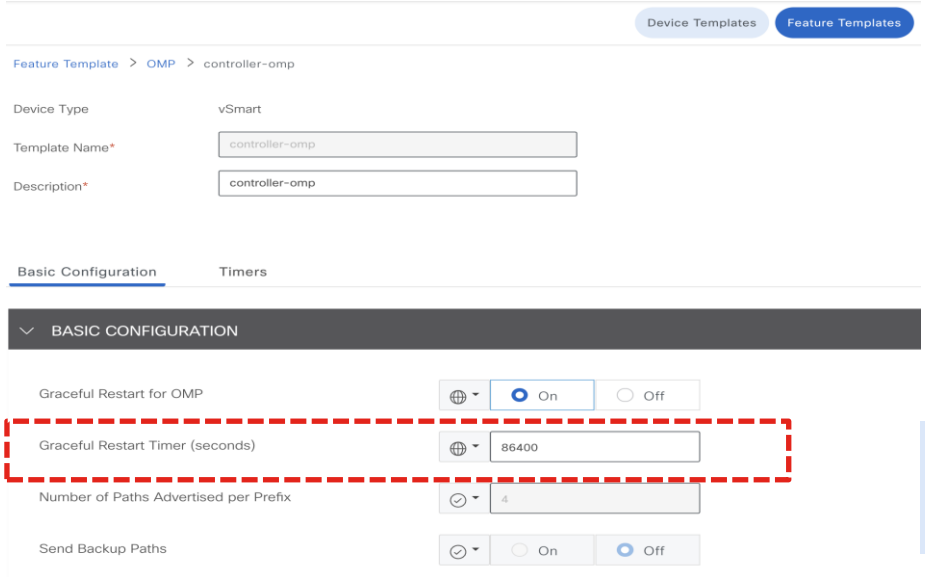
```
Controller1# show running-config omp
omp
 no shutdown
 filter-route
  no outbound affinity-group-preference
  no outbound tloc-color
 exit
 no graceful-restart
 outbound-policy-caching
!
```

```
Controller2# show running-config omp
omp
 no shutdown
 filter-route
  no outbound affinity-group-preference
  no outbound tloc-color
 exit
 no graceful-restart
 outbound-policy-caching
!
```

```
cat8kv-10#show sdwan omp peers detail | include graceful|peer|state|type
peer                    2.2.2.2
type                    vsmart
state                   up
graceful-restart        not-supported
graceful-restart-interval
peer                    3.3.3.3
type                    vsmart
state                   up
graceful-restart        not-supported
graceful-restart-interval
peer                    5.5.5.5
type                    vsmart
state                   up
graceful-restart        not-supported
graceful-restart-interval
```

```
cat8kv-10# !! -- #### shutdown Controller1, Controller2 and Controller3 #### -- !!
Site400-cE1#
2025/02/07 10:30:15.988025744 {iosrp_R0-0}{255}: [iosrp] [17261]: (info):  *Dec 21
10:30:15.988: %Cisco-SDWAN-cat8kv-10-OMPD-6-INFO-1400002: Notification: 2025/02/07
10:30:15 omp-number-of-vsmarts-change severity-level:major host-name:"cat8kv-10"
system-ip:1.1.1.110 tenant-name:"[Default]" tenant-global-id:0 number-of-vsmarts:0
cat8kv-10#show sdwan bfd sessions
cat8kv-10#
```

OMP Graceful Restart Timer



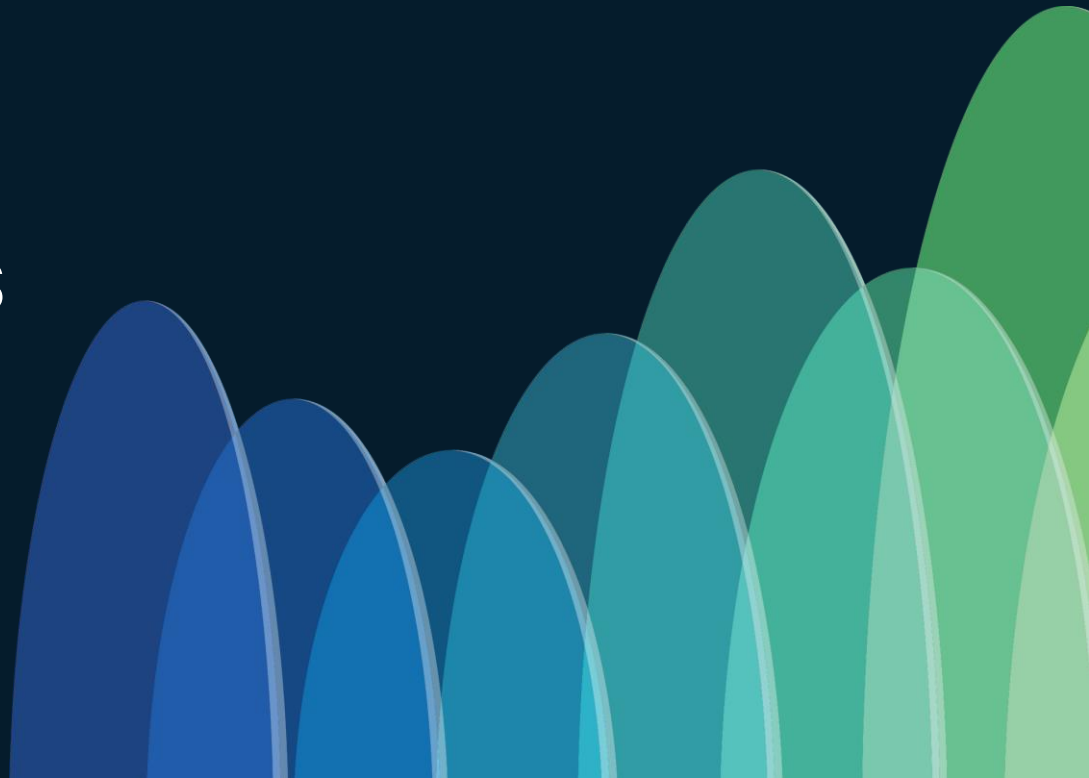
- Graceful Restart timer configured on SD-WAN controllers is applied to SD-WAN Edge, and conversely.
- If any change to an OMP graceful restart configuration is made, the OMP session between the Cisco SD-WAN controllers and the device is flapped.

```
Controller1# show running-config omp
omp
 no shutdown
 filter-route
  no outbound affinity-group-preference
  no outbound tloc-color
 exit
 graceful-restart
 outbound-policy-caching
 timers
  graceful-restart-timer 86400
 exit
!
```

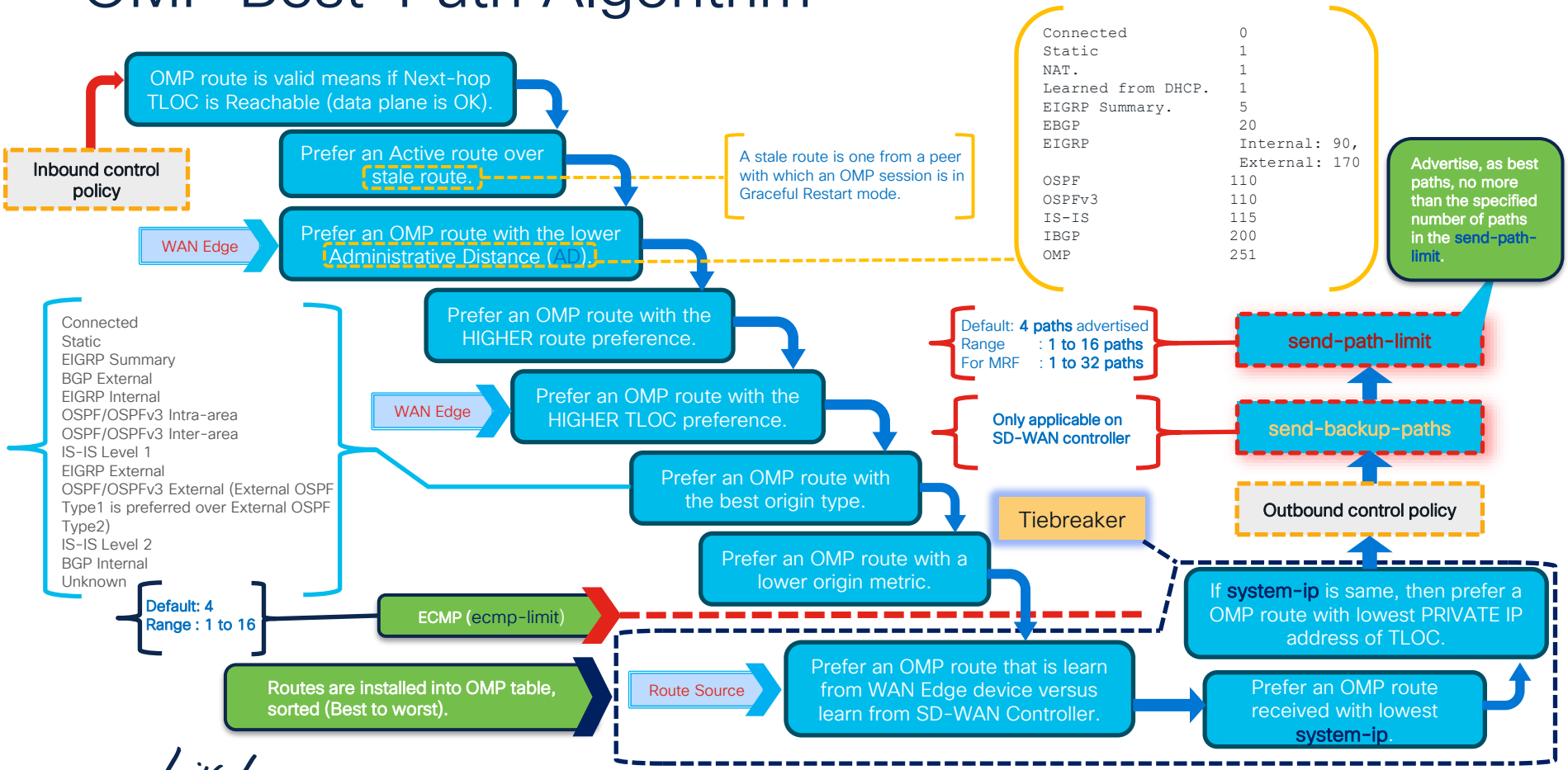
```
Controller1#show omp peers 1.1.1.110 detail | include peer\|state\|graceful
peer                    1.1.1.110
state                   up
graceful-restart        supported
graceful-restart-interval 43200
```

```
cat8kv-10#show sdwan omp peers detail | include peer|state|graceful
peer                    2.2.2.2
state                   up
graceful-restart        supported
graceful-restart-interval 86400
peer                    3.3.3.3
state                   up
graceful-restart        supported
graceful-restart-interval 86400
```

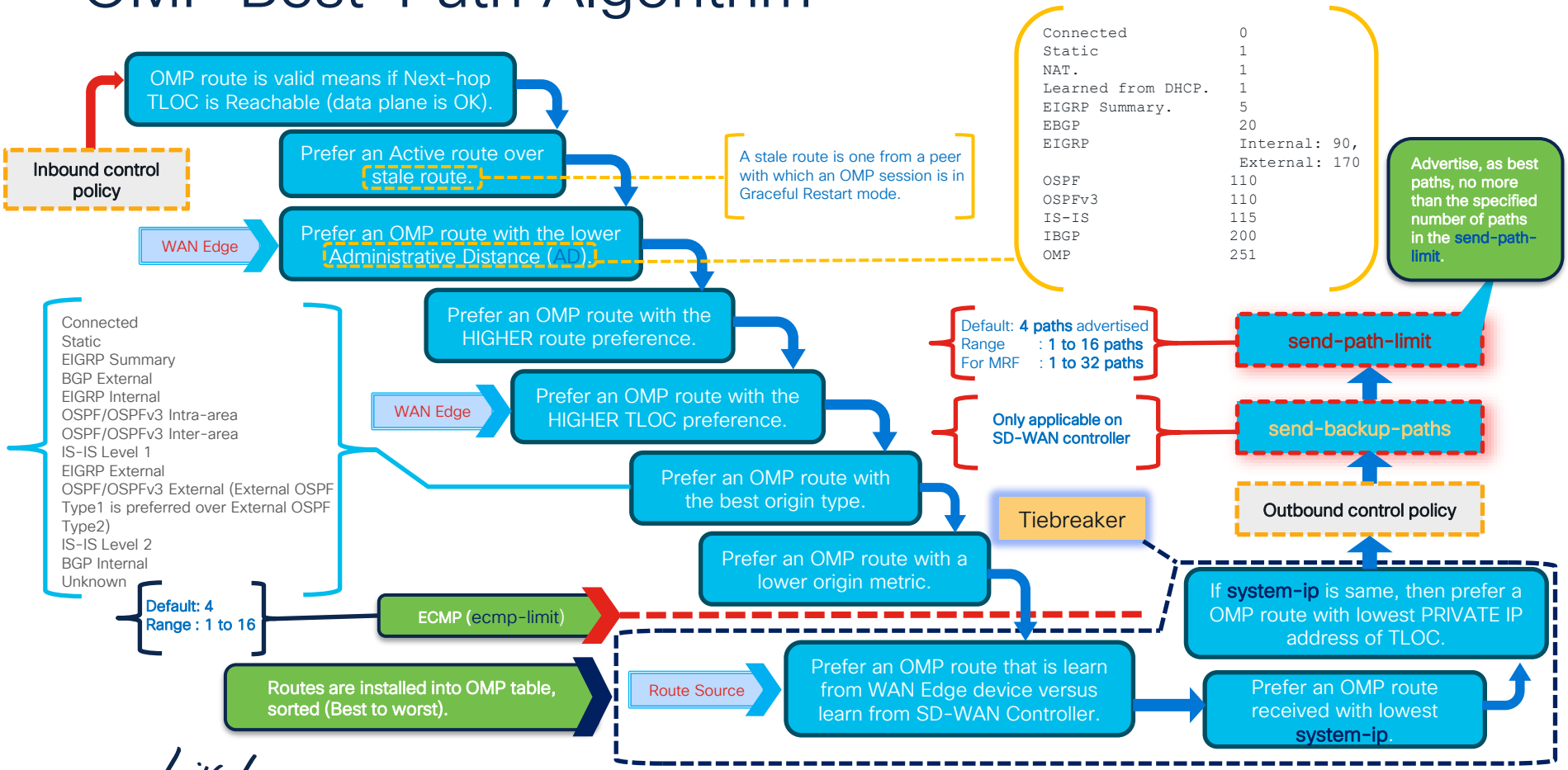
OMP Best Path selection process



OMP Best-Path Algorithm



OMP Best-Path Algorithm



OMP Best-Path Algorithm with Multi Region Fabric(MRF)

OMP route is valid means if Next-hop TLOC is Reachable (data plane is OK).

Inbound control policy

Prefer an Active route over stale route.

WAN Edge

Prefer an OMP route with the lower Administrative Distance (AD).

Compare region-path-length. **Prefer lower**. If region-path-length-ignore is configured, then OMP skip this step.

Yes

MRF

Prefer an OMP route with the HIGHER route preference.

No

Prefer access region paths [intra-region] over core region paths [inter-region].

Prefer a direct path over a transport gateway path. (depend upon user-configuration)

WAN Edge

Prefer an OMP route with the HIGHER TLOC preference.

Prefer paths from the router's own subregion.

Prefer an OMP route with the best origin type.

Prefer a path with a higher border router preference value.

Tiebreaker

Prefer an OMP route with a lower origin metric.

Prefer a path with lower derived affinity value.

WAN Edge

Compare the affinity in the paths based on the affinity preference list configuration on WAN Edge.

WAN Edge

Route Source

Prefer an OMP route that is learn from WAN Edge device versus learn from SD-WAN Controller.

Prefer an OMP route received with lowest **system-ip**.

If **system-ip** is same, then prefer a OMP route with lowest PRIVATE IP address of TLOC.

Outbound control policy

send-backup-paths

send-path-limit

How does OMP ensure loop avoidance?

- OMP loop avoidance is based on originator System-IP.
- Native built-in loop prevention mechanisims when OMP interacts with OSPF, EIGRP, RIP and BGP.

OSPF

- OSPF uses "Down Bit" (RFC 4577). When redistributed form OMP into OSPF on WAN Edge, it is set.
- When LSA distributed through sevice side network gets to the other WAN Edge, as DN bit is set so route is not installed into RIB on WAN Edge as SDWAN-Dnbit flag is set.

EIGRP

- EIGRP uses "**External Protocol**" ID field. It is set to a value of "**OMP-Agent**".
- When the other WAN Edge on the same site receives such update, it installs the route into the EIGRP topology table, sets "**SDWAN-Down**" flag and then install into the RIB with **Administrative Distance (AD)** to **252**. This, in turn, makes OMP the preferred route because it has an **AD** of **251**.

RIP

- RIP uses "**OMP-ROUTE-TAG**" with value **44270,** which is **not configurable**.
- When the other WAN Edge on the same site receives RIP update, it is not get installed because of "**OMP-ROUTE-TAG**" tag. This route will get installed with **AD** of **252**, ONLY when OMP route gets withdrawn, thus avoiding routing loop.

How does OMP ensure loop avoidance?

- OMP loop avoidance is based on originator System-IP.
- Native built-in loop prevention mechanisims when OMP interacts with OSPF, EIGRP, RIP and BGP.

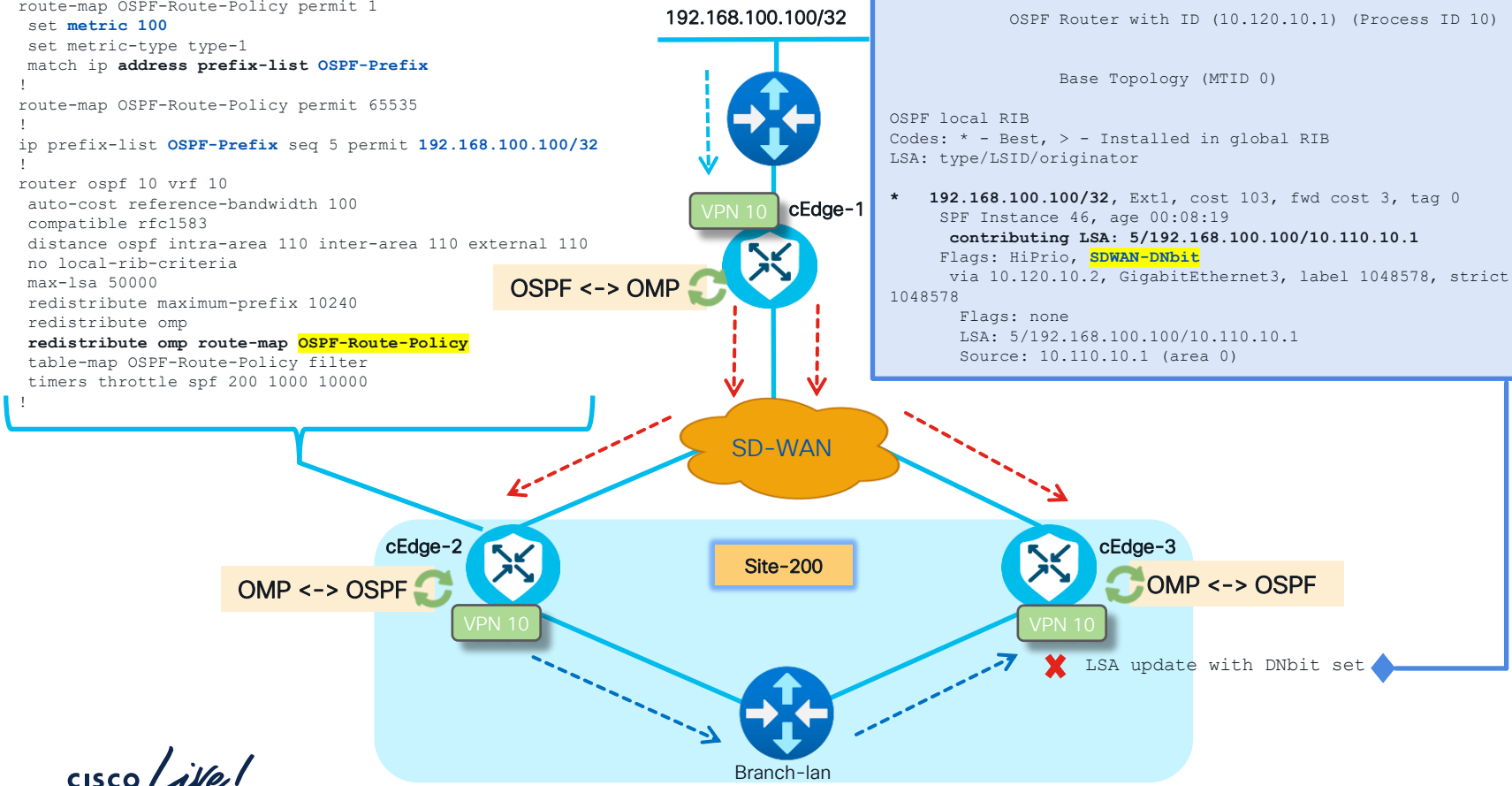
BGP

- BGP uses **SoO**, extended community which value is set to the OMP **site ID**.
- When the other WAN Edge receives the BGP update from the service-side network and there **SoO** community matches its **own site ID**, then route will **not be installed into RIB**.
- BGP peers at site must send **BGP extended communities** and have the **same site ID**.

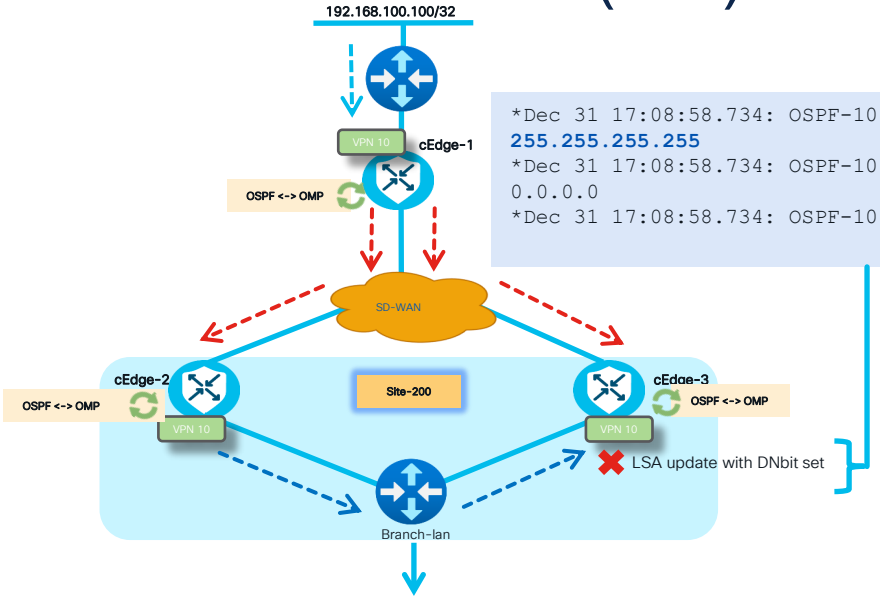
How Down-bit (DN) works? 1/2

```
route-map OSPF-Route-Policy permit 1
 set metric 100
 set metric-type type-1
 match ip address prefix-list OSPF-Prefix
!
route-map OSPF-Route-Policy permit 65535
!
ip prefix-list OSPF-Prefix seq 5 permit 192.168.100.100/32
!
router ospf 10 vrf 10
 auto-cost reference-bandwidth 100
 compatible rfc1583
 distance ospf intra-area 110 inter-area 110 external 110
 no local-rib-criteria
 max-lsa 50000
 redistribute maximum-prefix 10240
 redistribute omp
 redistribute omp route-map OSPF-Route-Policy
 table-map OSPF-Route-Policy filter
 timers throttle spf 200 1000 10000
!
```

```
cEdge-3#show ip ospf rib 192.168.100.100 255.255.255.255

            OSPF Router with ID (10.120.10.1) (Process ID 10)


                    Base Topology (MTID 0)

OSPF local RIB
Codes: * - Best, > - Installed in global RIB
LSA: type/LSID/originator

*   192.168.100.100/32, Ext1, cost 103, fwd cost 3, tag 0
     SPF Instance 46, age 00:08:19
      contributing LSA: 5/192.168.100.100/10.110.10.1
     Flags: HiPrio, SDWAN-DNbit
      via 10.120.10.2, GigabitEthernet3, label 1048578, strict label
1048578
       Flags: none
       LSA: 5/192.168.100.100/10.110.10.1
       Source: 10.110.10.1 (area 0)
```



How Down-bit (DN) works? 2/2



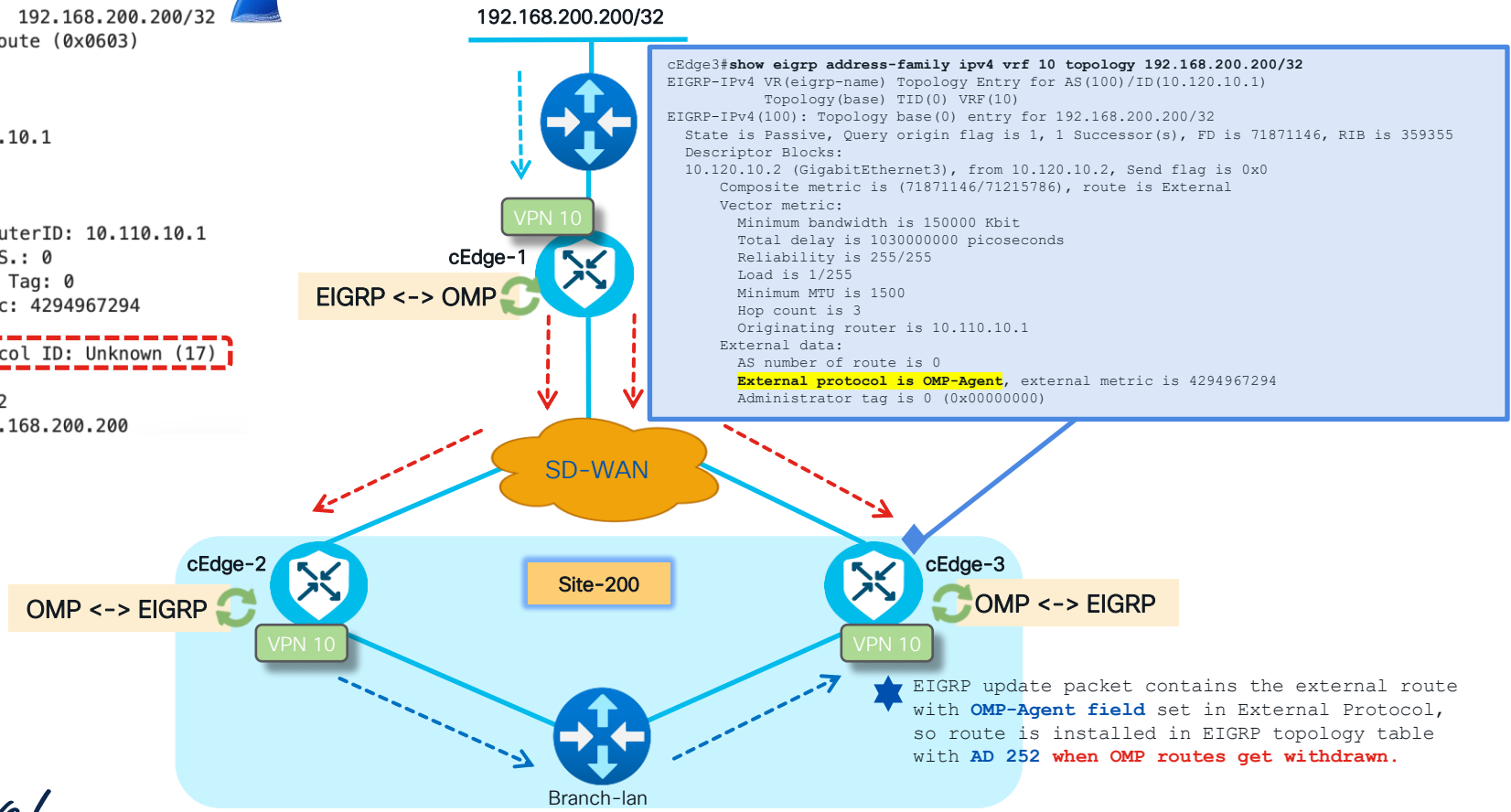

```
*Dec 31 17:08:58.734: OSPF-10 EXTER: Start processing AS External LSA 5/192.168.100.100/10.110.10.1, mask
255.255.255.255
*Dec 31 17:08:58.734: OSPF-10 EXTER:  age 885, seq 0x80000028, lsa_metric 100, metric-type 1, fw-addr
0.0.0.0
*Dec 31 17:08:58.734: OSPF-10 EXTER: Downward bit with SDWAN, ignoring the LSA
```

```
Branch-Lan#show ip route 192.168.100.100 255.255.255.255
Routing entry for 192.168.100.100/32
  Known via "ospf 10", distance 110, metric 101, type extern 1
  Last update from 10.110.10.1 on GigabitEthernet0/3, 03:35:49 ago
  Routing Descriptor Blocks:
  * 10.110.10.1, from 10.110.10.1, 03:35:49 ago, via GigabitEthernet0/3
      Route metric is 101, traffic share count is 1
```

```
LSA-type 5 (AS-External-LSA (ASBR)), len 36
    .000 0000 1110 0101 = LS Age (seconds): 229
    0... .... .... .... = Do Not Age Flag: 0
  Options: 0xa0, DN, (DC) Demand Circuits
    1... .... = DN: Set
    .0.. .... = (O) Opaque: Not set
    ..1. .... = (DC) Demand Circuits: Supported
    ...0 .... = (L) LLS Data block: Not Present
    .... 0... = (N) NSSA: Not supported
    .... .0.. = (MC) Multicast: Not capable
    .... ..0. = (E) External Routing: Not capable
    .... ...0 = (MT) Multi-Topology Routing: No
  LS Type: AS-External-LSA (ASBR) (5)
  Link State ID: 192.168.100.100
  Advertising Router: 10.110.10.1
  Sequence Number: 0x80000028
  Checksum: 0xa9c9
  Length: 36
  Netmask: 255.255.255.255
  0... .... = External Type: Type 1 (metric is specified in the same units as interface cost)
  .000 0000 = TOS: 0
  Metric: 100
  Forwarding Address: 0.0.0.0
  External Route Tag: 0
```

How loop avoidance works in EIGRP 1/2?

```
External Route  =   192.168.200.200/32
  Type: External Route (0x0603)
  Length: 65
  Topology: 0
  AFI: IPv4 (1)
  RouterID: 10.110.10.1
> Wide Metric
  NextHop: 0.0.0.0
v External Data
    Originating RouterID: 10.110.10.1
    Originating A.S.: 0
    Administrative Tag: 0
    External Metric: 4294967294
    Reserved: 0
    External Protocol ID: Unknown (17)
  > External Flags
  Prefix Length: 32
  Destination: 192.168.200.200
```

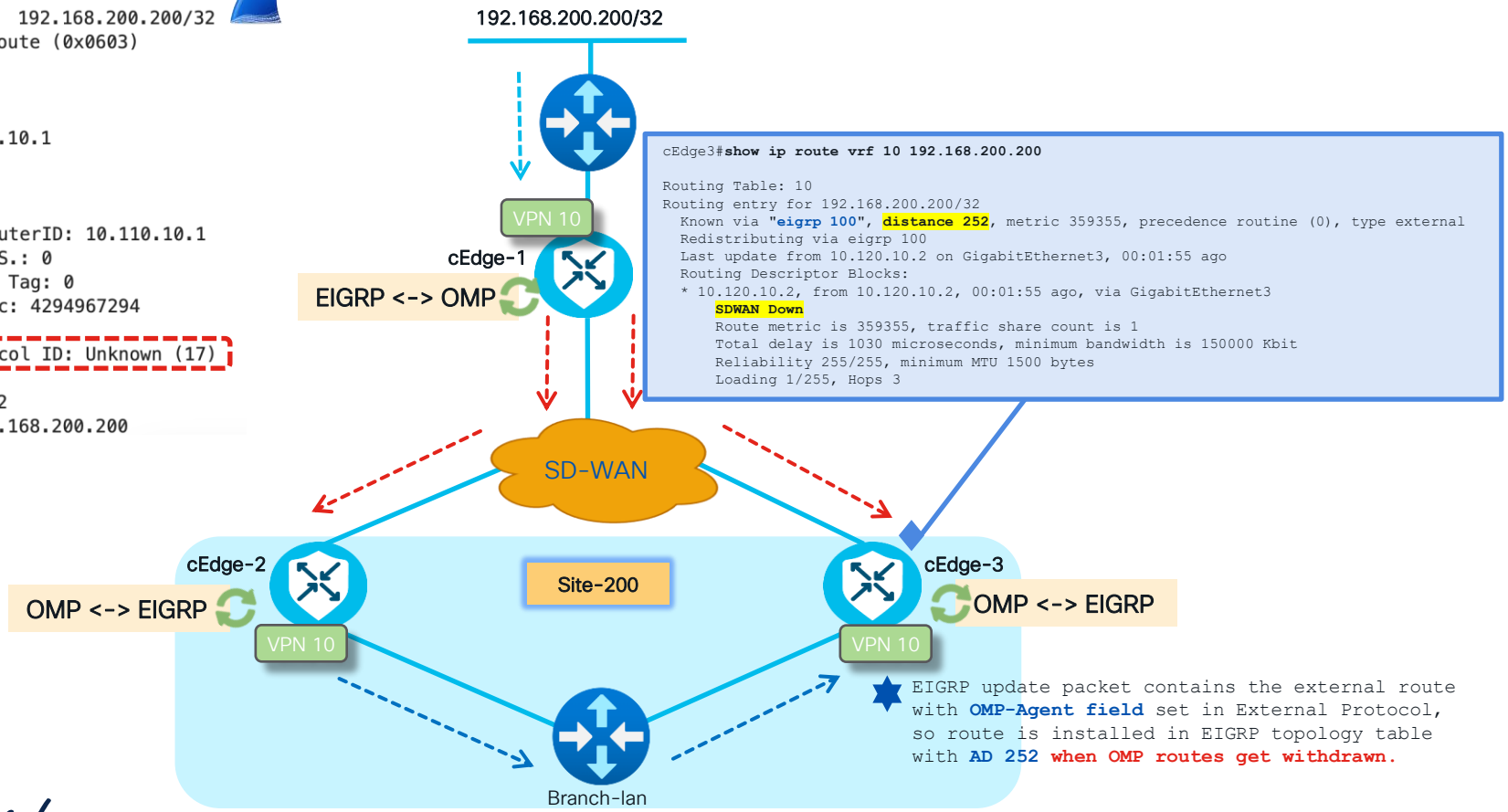



```
cEdge3#show eigrp address-family ipv4 vrf 10 topology 192.168.200.200/32
EIGRP-IPv4 VR(eigrp-name) Topology Entry for AS(100)/ID(10.120.10.1)
          Topology(base) TID(0) VRF(10)
EIGRP-IPv4(100): Topology base(0) entry for 192.168.200.200/32
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 71871146, RIB is 359355
  Descriptor Blocks:
  10.120.10.2 (GigabitEthernet3), from 10.120.10.2, Send flag is 0x0
      Composite metric is (71871146/71215786), route is External
      Vector metric:
        Minimum bandwidth is 150000 Kbit
        Total delay is 1030000000 picoseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 3
        Originating router is 10.110.10.1
      External data:
        AS number of route is 0
        External protocol is OMP-Agent, external metric is 4294967294
        Administrator tag is 0 (0x00000000)
```

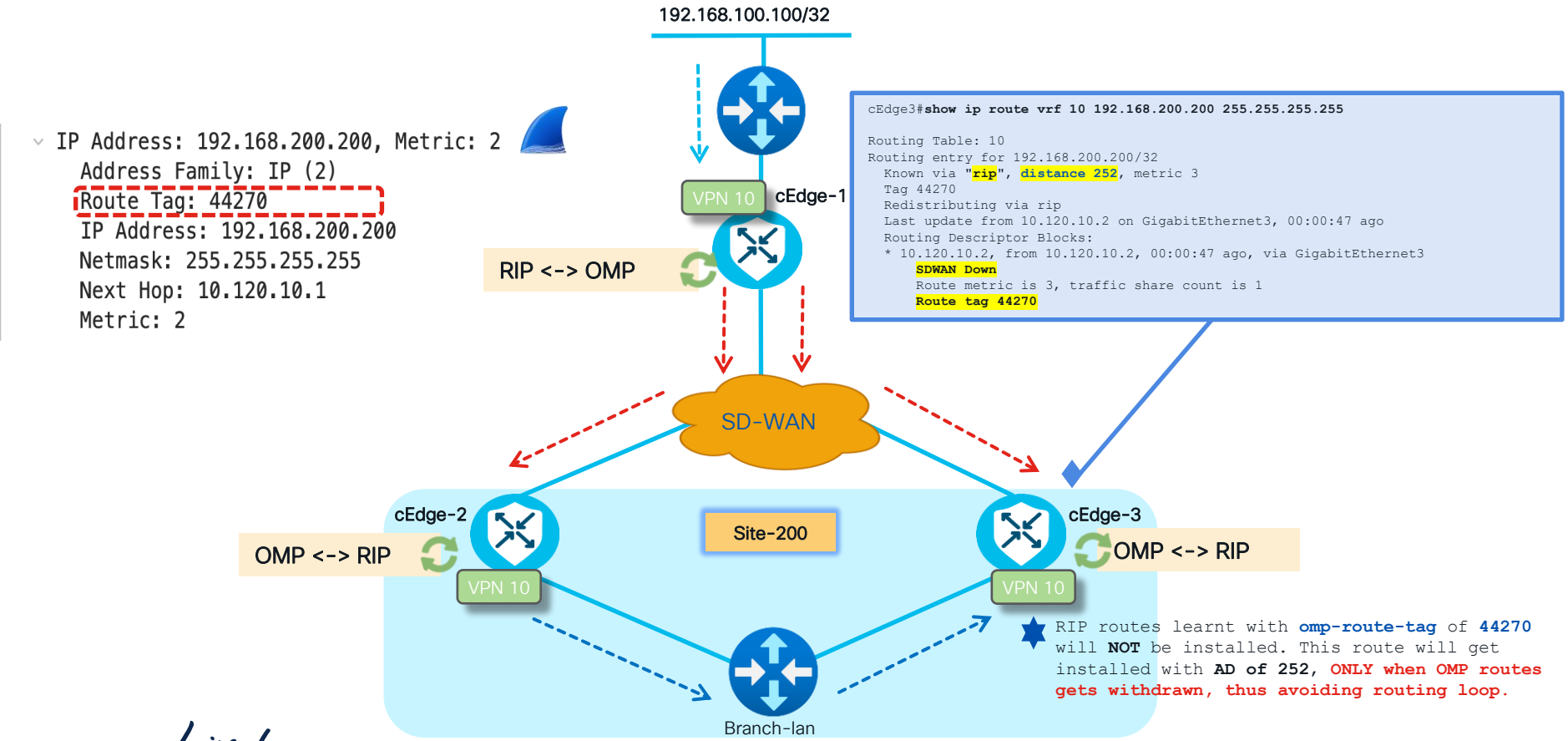
EIGRP update packet contains the external route with **OMP-Agent field** set in External Protocol, so route is installed in EIGRP topology table with **AD 252 when OMP routes get withdrawn.**

How loop avoidance works in EIGRP 2/2?

```
External Route  =   192.168.200.200/32
  Type: External Route (0x0603)
  Length: 65
  Topology: 0
  AFI: IPv4 (1)
  RouterID: 10.110.10.1
> Wide Metric
  NextHop: 0.0.0.0
v External Data
    Originating RouterID: 10.110.10.1
    Originating A.S.: 0
    Administrative Tag: 0
    External Metric: 4294967294
    Reserved: 0
    External Protocol ID: Unknown (17)
  > External Flags
  Prefix Length: 32
  Destination: 192.168.200.200
```



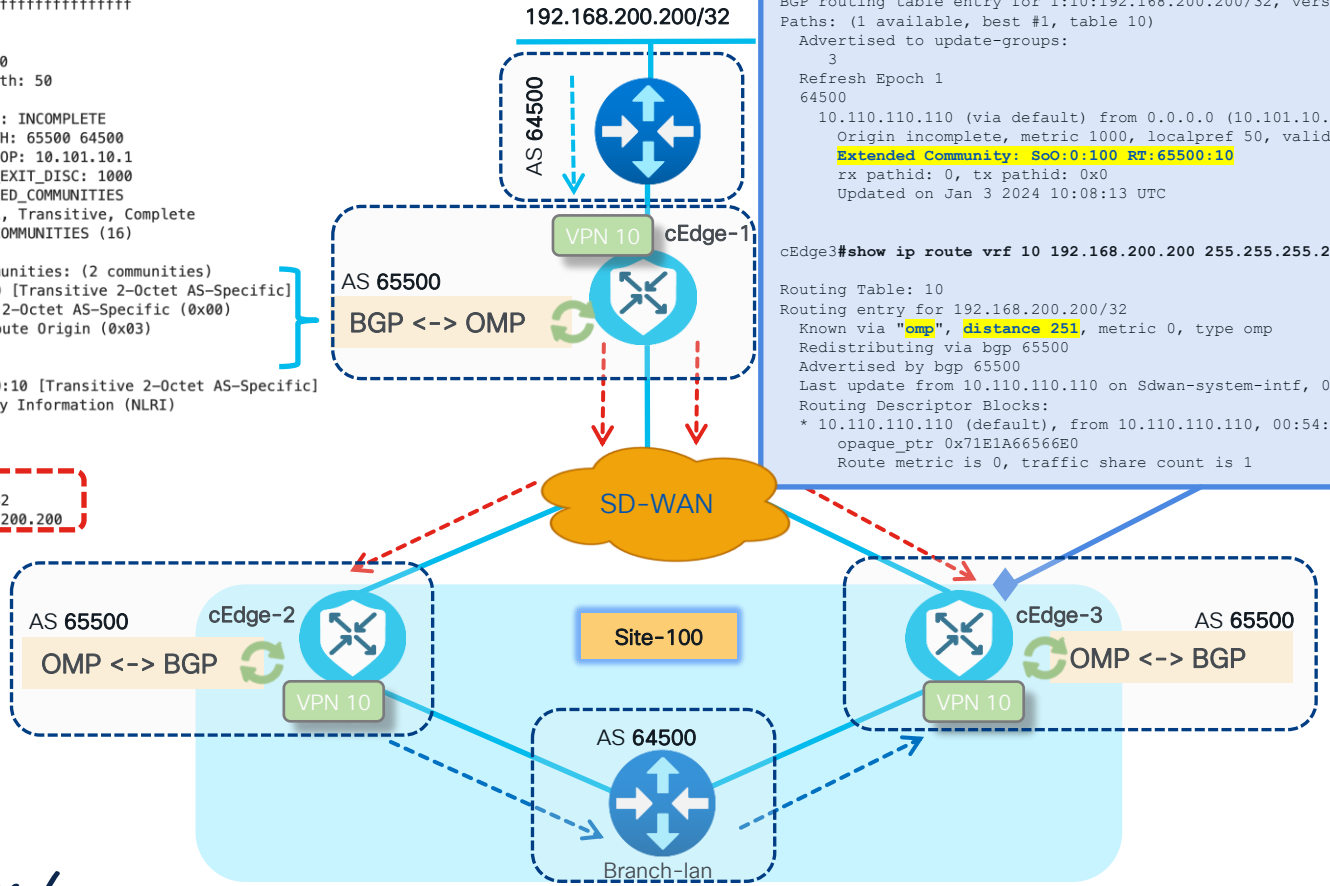
How loop avoidance works in RIP?



How loop avoidance works in BGP 1/2?

```
Border Gateway Protocol - UPDATE Message
  Marker: ffffffffffffffffffffffffffffffff
  Length: 92
  Type: UPDATE Message (2)
  Withdrawn Routes Length: 0
  Total Path Attribute Length: 50
  Path attributes
    Path Attribute - ORIGIN: INCOMPLETE
    Path Attribute - AS_PATH: 65500 64500
    Path Attribute - NEXT_HOP: 10.101.10.1
    Path Attribute - MULTI_EXIT_DISC: 1000
    Path Attribute - EXTENDED_COMMUNITIES
      Flags: 0xc0, Optional, Transitive, Complete
      Type Code: EXTENDED_COMMUNITIES (16)
      Length: 16
      Carried extended communities: (2 communities)
        Route Origin: 0:100 [Transitive 2-Octet AS-Specific]
          Type: Transitive 2-Octet AS-Specific (0x00)
          Subtype (AS2): Route Origin (0x03)
          2-Octet AS: 0
          4-Octet AN: 100
        Route Target: 65500:10 [Transitive 2-Octet AS-Specific]
  Network Layer Reachability Information (NLRI)
    10.0.100.0/24
    10.110.10.101/32
    10.110.10.102/32
    192.168.200.200/32
      NLRI prefix length: 32
      NLRI prefix: 192.168.200.200
```

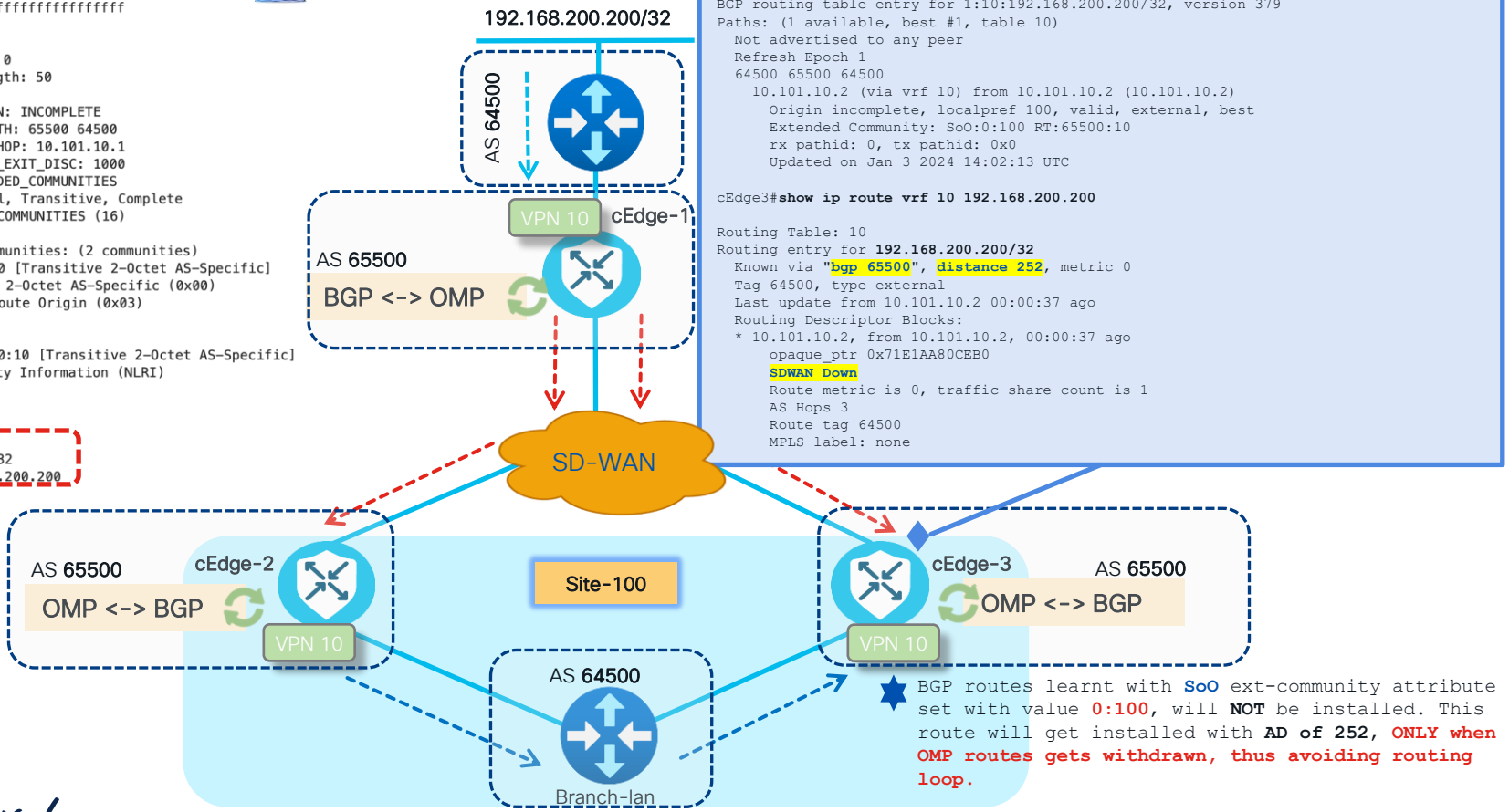
```
cEdge3#show bgp vpnv4 unicast vrf 10 192.168.200.200 255.255.255.255
BGP routing table entry for 1:10:192.168.200.200/32, version 265
Paths: (1 available, best #1, table 10)
  Advertised to update-groups:
     3
  Refresh Epoch 1
  64500
    10.110.110.110 (via default) from 0.0.0.0 (10.101.10.1)
      Origin incomplete, metric 1000, localpref 50, valid, sourced, best
      Extended Community: SoO:0:100 RT:65500:10
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 3 2024 10:08:13 UTC


cEdge3#show ip route vrf 10 192.168.200.200 255.255.255.255

Routing Table: 10
Routing entry for 192.168.200.200/32
  Known via "omp", distance 251, metric 0, type omp
  Redistributing via bgp 65500
  Advertised by bgp 65500
  Last update from 10.110.110.110 on Sdwan-system-intf, 00:54:37 ago
  Routing Descriptor Blocks:
  * 10.110.110.110 (default), from 10.110.110.110, 00:54:37 ago, via Sdwan-system-intf
      opaque_ptr 0x71E1A66566E0
      Route metric is 0, traffic share count is 1
```



How loop avoidance works in BGP 2/2?

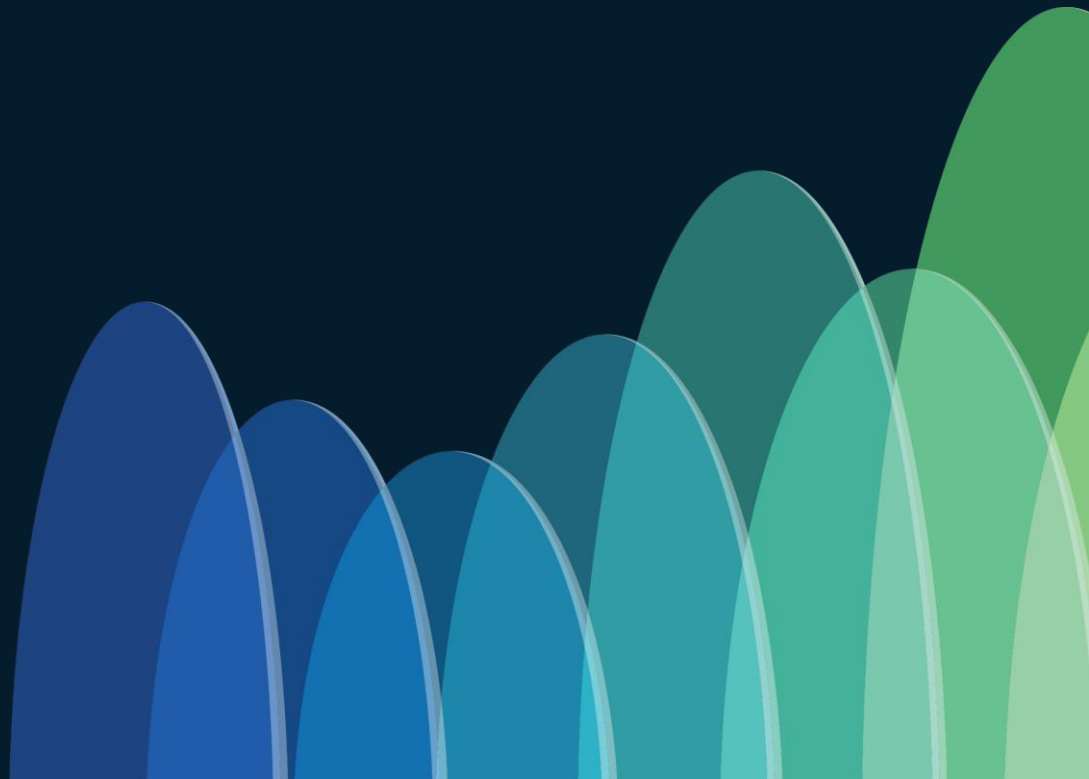
```
Border Gateway Protocol - UPDATE Message
  Marker: ffffffffffffffffffffffffffffffff
  Length: 92
  Type: UPDATE Message (2)
  Withdrawn Routes Length: 0
  Total Path Attribute Length: 50
  Path attributes
    Path Attribute - ORIGIN: INCOMPLETE
    Path Attribute - AS_PATH: 65500 64500
    Path Attribute - NEXT_HOP: 10.101.10.1
    Path Attribute - MULTI_EXIT_DISC: 1000
    Path Attribute - EXTENDED_COMMUNITIES
      Flags: 0xc0, Optional, Transitive, Complete
      Type Code: EXTENDED_COMMUNITIES (16)
      Length: 16
      Carried extended communities: (2 communities)
        Route Origin: 0:100 [Transitive 2-Octet AS-Specific]
          Type: Transitive 2-Octet AS-Specific (0x00)
          Subtype (AS2): Route Origin (0x03)
          2-Octet AS: 0
          4-Octet AN: 100
        Route Target: 65500:10 [Transitive 2-Octet AS-Specific]
  Network Layer Reachability Information (NLRI)
    10.0.100.0/24
    10.110.10.101/32
    10.110.10.102/32
    192.168.200.200/32
      NLRI prefix length: 32
      NLRI prefix: 192.168.200.200
```

```
cEdge3#show bgp vpnv4 unicast vrf 10 192.168.200.200
BGP routing table entry for 1:10:192.168.200.200/32, version 379
Paths: (1 available, best #1, table 10)
  Not advertised to any peer
  Refresh Epoch 1
  64500 65500 64500
    10.101.10.2 (via vrf 10) from 10.101.10.2 (10.101.10.2)
      Origin incomplete, localpref 100, valid, external, best
      Extended Community: SoO:0:100 RT:65500:10
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 3 2024 14:02:13 UTC

cEdge3#show ip route vrf 10 192.168.200.200

Routing Table: 10
Routing entry for 192.168.200.200/32
  Known via "bgp 65500", distance 252, metric 0
  Tag 64500, type external
  Last update from 10.101.10.2 00:00:37 ago
  Routing Descriptor Blocks:
  * 10.101.10.2, from 10.101.10.2, 00:00:37 ago
      opaque_ptr 0x71E1AA80CEB0
      SDWAN Down
      Route metric is 0, traffic share count is 1
      AS Hops 3
      Route tag 64500
      MPLS label: none
```



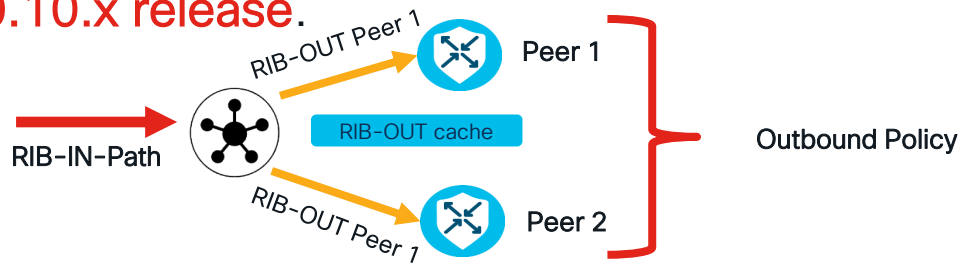
BGP routes learnt with **SoO** ext-community attribute set with value **0:100**, will **NOT** be installed. This route will get installed with **AD of 252**, **ONLY when OMP routes gets withdrawn, thus avoiding routing loop.**

How OMP Enhancements Benefit You?



OMP Enhancements: What's New and How It Helps

- SD-WAN controller **RIB-OUT policy caching** in 20.10.x release.

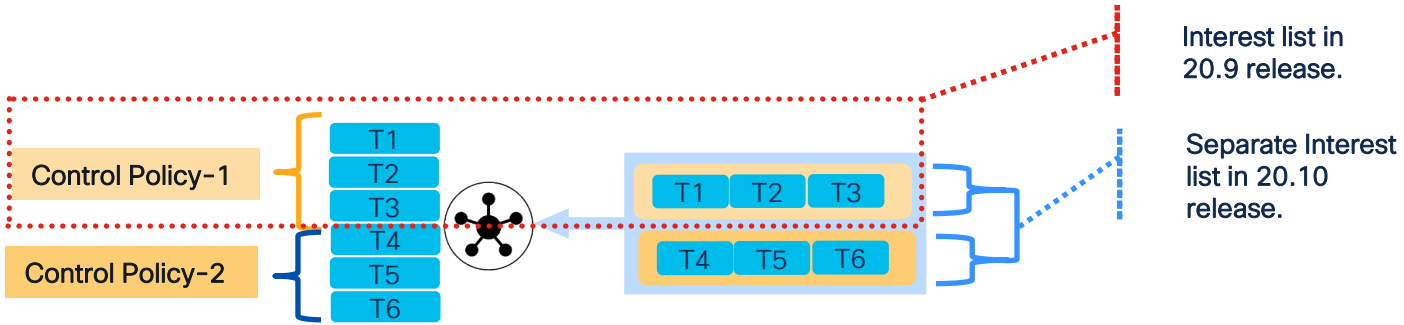



```
Controller1# show running-config omp
omp
 no shutdown
 send-path-limit    16
 filter-route
  no outbound affinity-group-preference
  no outbound tloc-color
 exit
 graceful-restart
 outbound-policy-caching
!
```

```
Controller1# show support omp rib vroute 10:192.168.110.0/24 detail | begin RIB-CACHE-ENTRY
  RIB-CACHE-ENTRY: (0x7f3b0a033c00), Policy-name: CL-Demo-Route-Policy, Policy-seq-num: 193, RI-ID: 282, attr:
0x7f3b0a02d400
    Attribute: (0x7f3b0a02d400), ROUTE-IPV4, Length: 1200, Ref: 3
      Flags: (0x8000c2d) TAG WEIGHT TLOC SITE-ID OVERLAY-ID ORIGIN ORIGINATOR
      Region-id: 65534, Secondary-Region-id: 65535, Orig-Access-Region-id: 65534, Sub-Region-ID: 0, Pref: 0,
Weight: 1, Tag: 200, Stale: 0 Version: 0, Restrict: 0, on-Demand: 0, Domain: 0, BR-Preference: 0, Affinity-Group-
Number:0, MRF-Route-Originator:None , Derived Affinity-group-number: 0
      Distance: 0, Site-ID: 110, Carrier: 0, Query: 0, Gen-ID: 0x0, Border: 0 Overlay: 1 Site-Type: 0 0 0 0
      Originator: 1.1.1.110
      Origin: Protocol: connected[1], Sub-Type: none[0], Metric: 0
      TLOC: ((nil)) 1.1.1.110 : mpls : ipsec
 ....
```

OMP Enhancements: What's New and How It Helps

- SD-WAN controller **TLOC flapping Resistence.**
  - Starting with release 20.9.x, Cisco Catalyst SD-WAN Controllers improve efficiency by maintaining an interest list of TLOCs that are employed in all control policies.
    - Cisco SD-WAN Controller disregards flapping of TLOCs not included in the interest list.
  - Release 20.10.x further optimizes performance by creating separate TLOC interest lists for each control policy, limiting the impact of flapping.

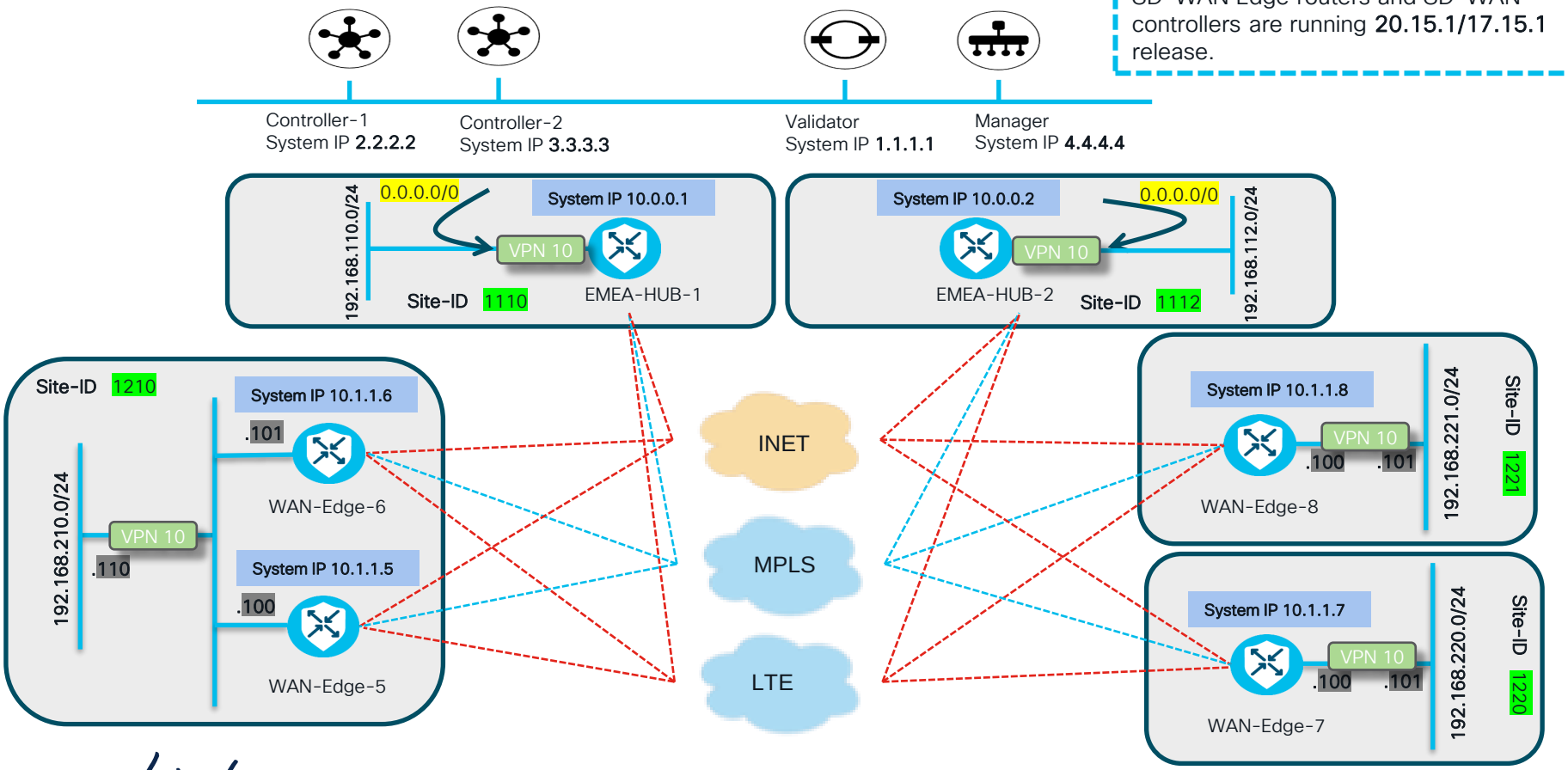


SD-WAN Hub and Spoke Topology

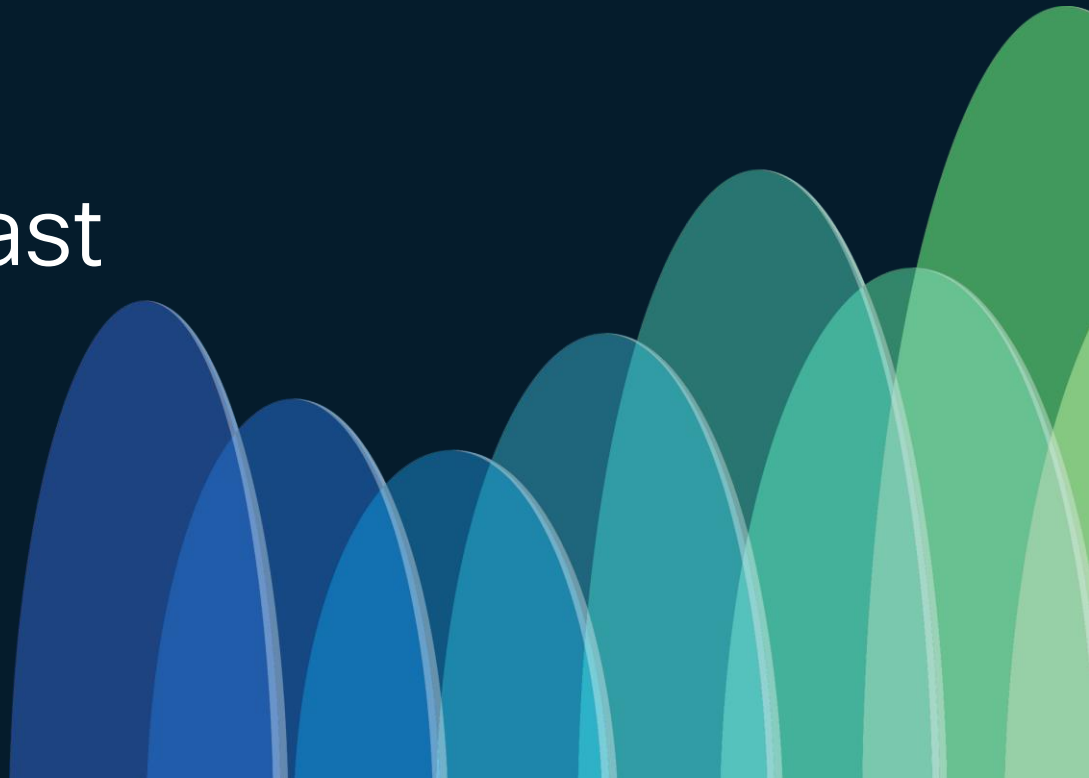
cisco Live!

Demo Topology

SD-WAN Edge routers and SD-WAN controllers are running **20.15.1/17.15.1** release.



SD-WAN Multicast



cisco Live!

Multicast Terminologies

RP - Rendezvous Point (Root of the tree)

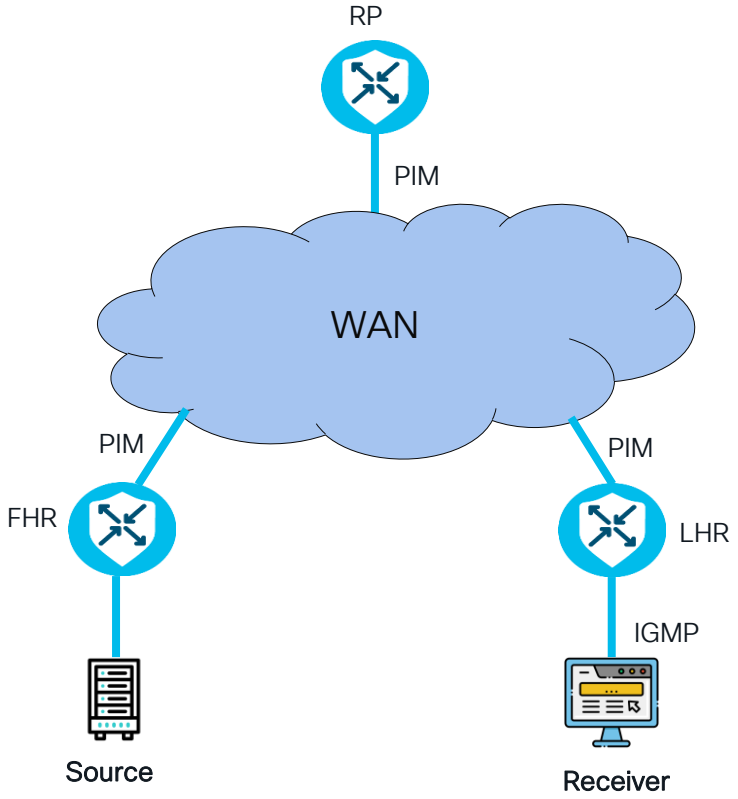
FHR - First Hop Router (Source)

LHR - Last Hop Router (Receiver)

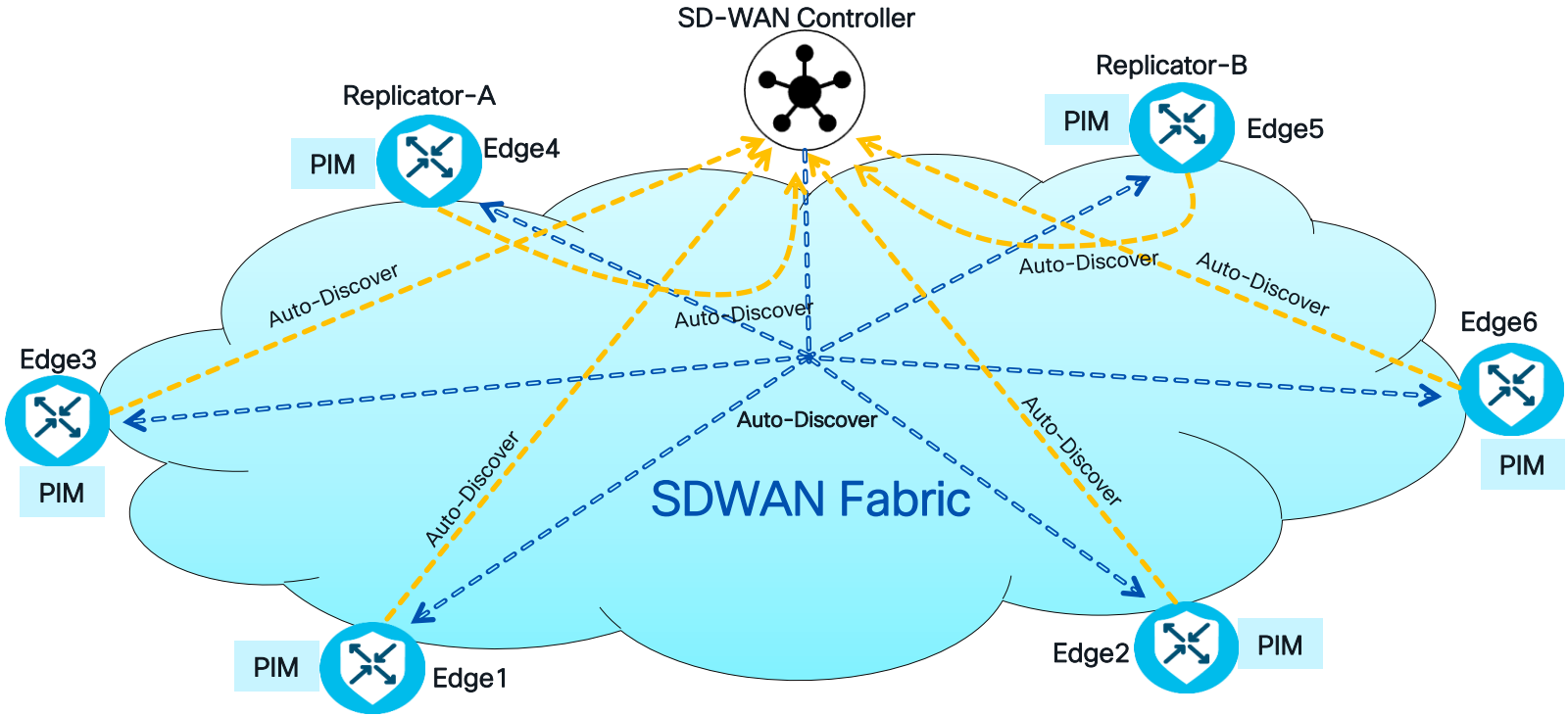
IGMP - Internet Group Management Protocol

PIM - Protocol Independent Multicast

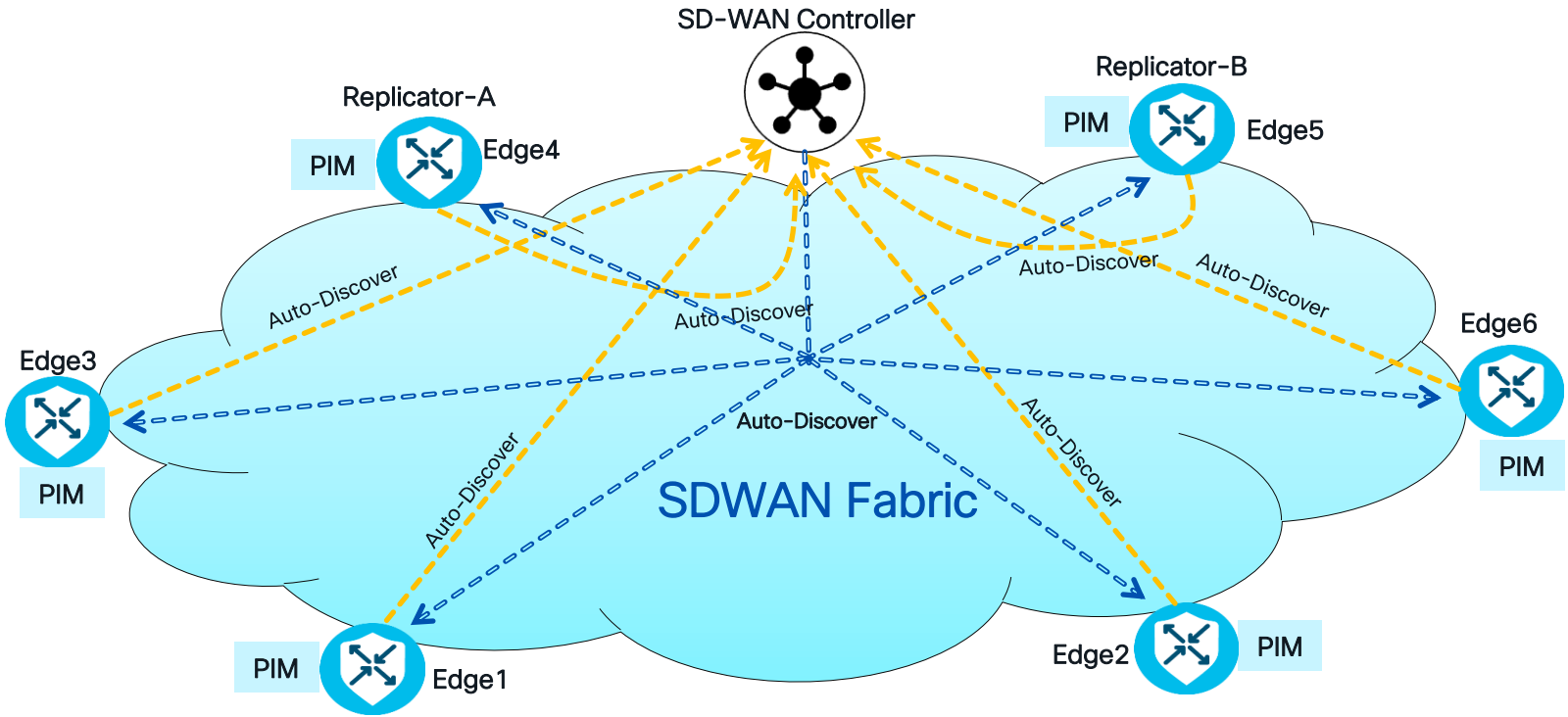
ASM - Any Source Multicast



OMP Multicast Auto-Discovery

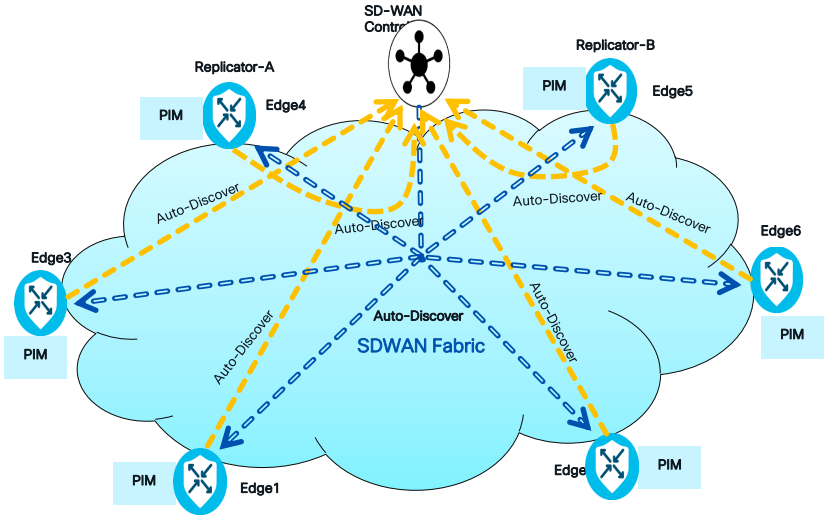


OMP Multicast Auto-Discovery



OMP Multicast Auto-Discovery

- OMP Multicast Auto-discovery packet contains:
  - List of WAN Edge devices are configured as multicast capable
  - List of devices are configured as replicator
  - Replicator capacity, GPS location etc.
- The multicast Autodiscover routes indicate whether the router has PIM enabled and whether it is a replicator.



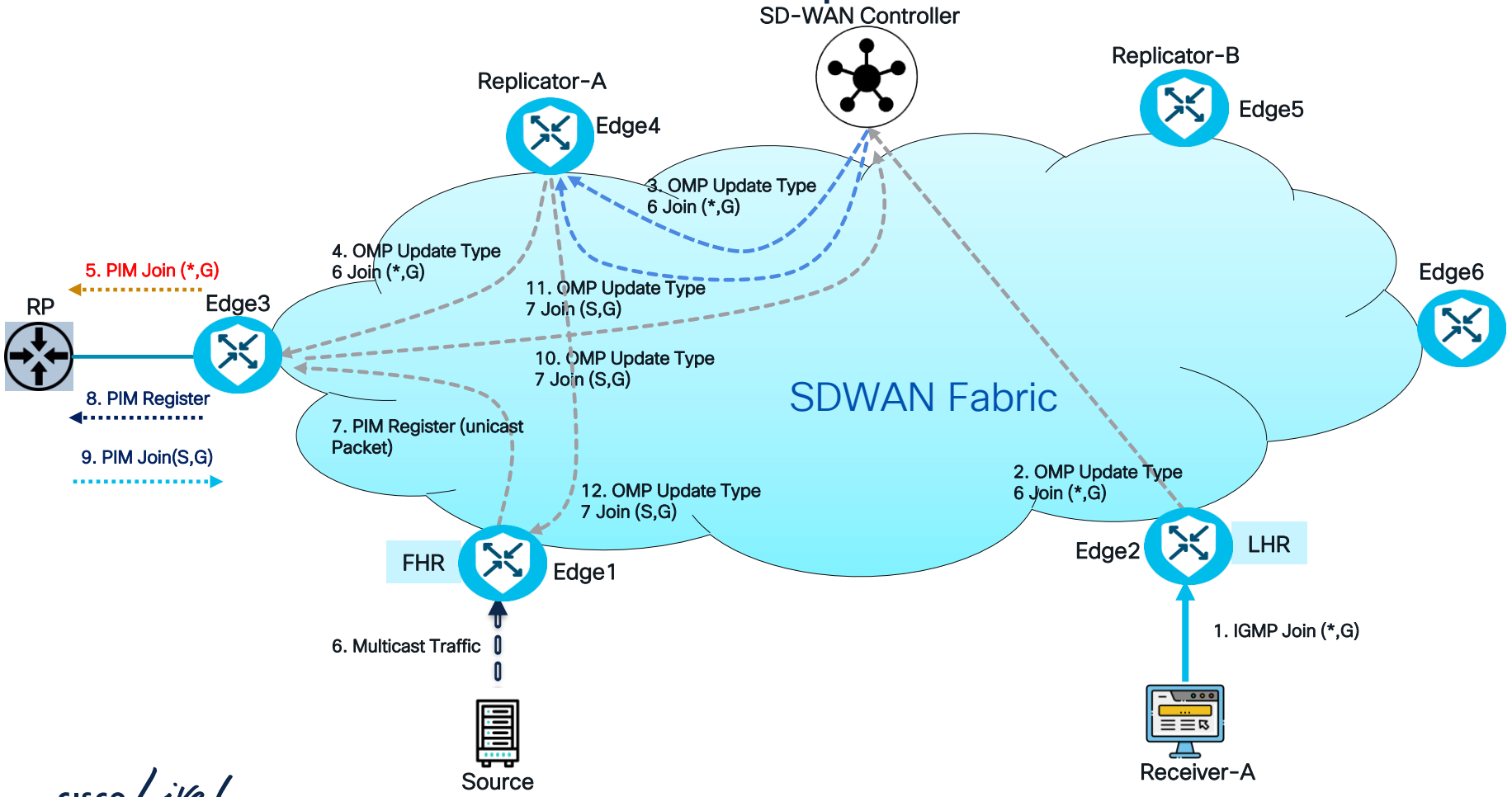
SD-WAN Multicast control packet flow - ASM

- Source register itself to an RP
- Receiver sends the (*,G) join
- First Join gets forwarded to the SD-WAN controller as an OMP packet and then forwarded to the replicator
- Replicator forwards (*,G) to the RP
- RP forwards it to the source
- Stream is forwarded to the receiver through the replicator. Stream NEVER goes to SD-WAN controller.
- Once receiver has the source information, it will then join using (S,G)
- First (S,G) join gets forwarded as an OMP control packet to the SD-WAN controller and then to replicator
- Replicator then forward the (S,G) to the source.

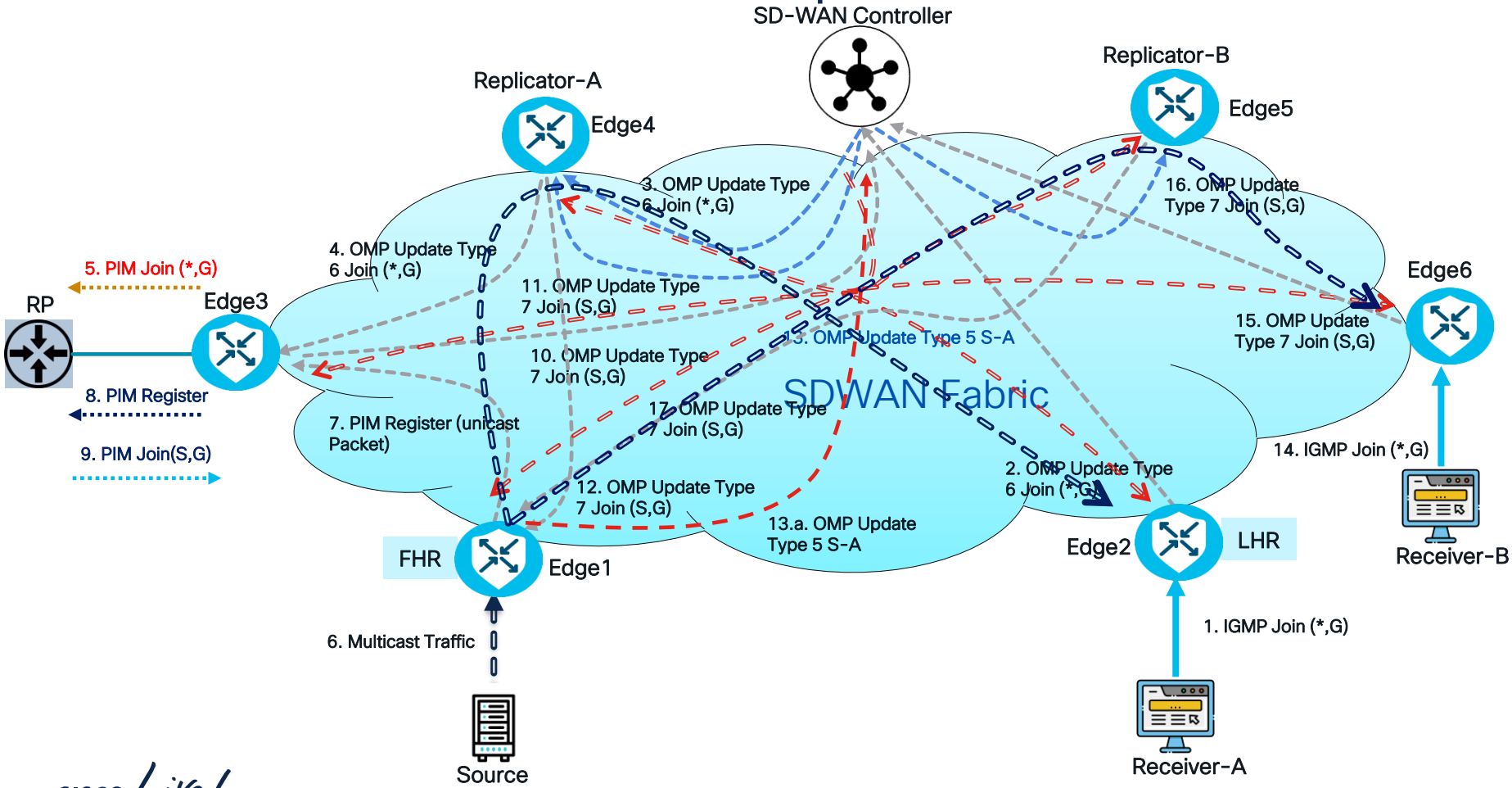
OMP Multicast Message

Route Type	OMP Overlay Multicast Route Type
5	Source Active
6	Shared Tree Join
7	Source Tree Join

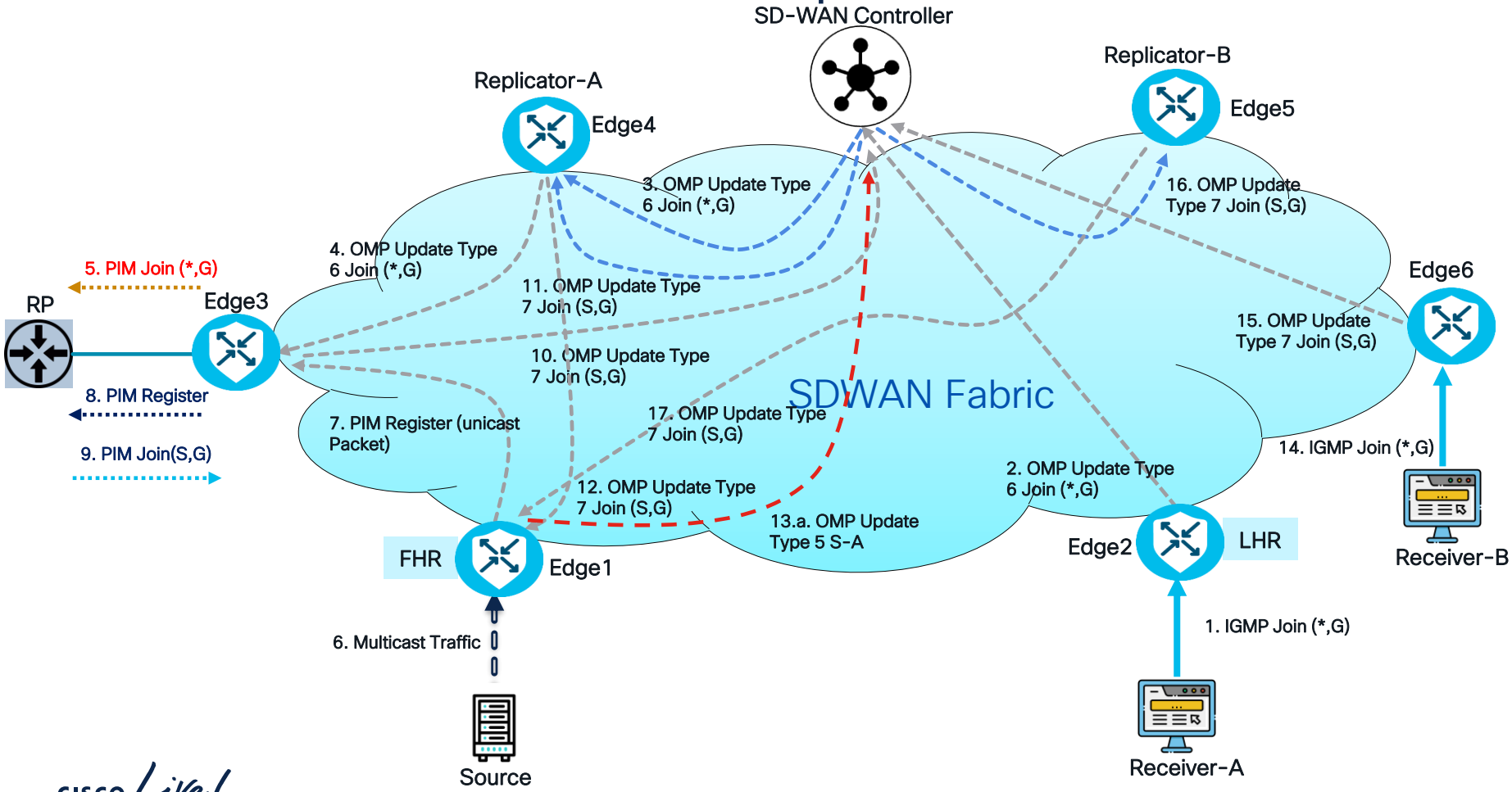
SD-WAN Multicast control packet flow – ASM 1/3



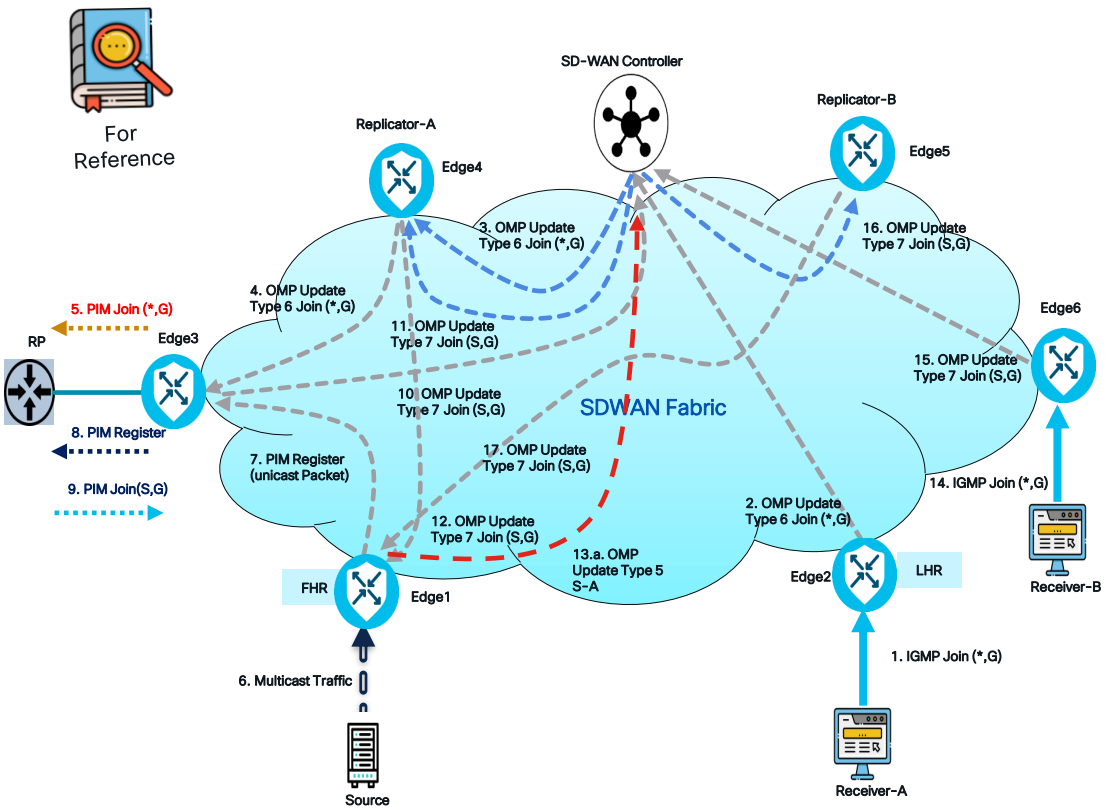
SD-WAN Multicast control packet flow – ASM 2/3



SD-WAN Multicast control packet flow – ASM 2/3



SD-WAN Multicast control packet flow - ASM 3/3



- IGMP join from Receiver is sent to LHR
- Type 6 (*,G) OMP join from LHR is sent to SD-WAN controller and SD-WAN controller forwards it to Replicator.
- Type 6 (*,G) OMP join from Replicator is sent to RP.
- Source streams the traffic to FHR.
- FHR sends PIM Registration message to RP.
- Type 7 (S,G) join from RP is sent to SD-WAN controller and then SD-WAN controller send it to Replicator.
- Type 7 (S,G) join from Replicator to is sent to FHR.
- Type 5 (S,A) message is sent from FHR to SD-WAN controller and SD-WAN controller sends to all the WAN Edges including LHR, RP and Replicator.
- Type 7 (S,G) join from LHR is sent to Replicator
- FHR transmits the traffic to the Replicator, which subsequently forwards it to LHR, and ultimately, the receiver obtains the Multicast stream.

SD-WAN Multicast Key points 1/2

- The significance of replicator selection lies solely from the perspective of the LHR (receivers' point of view).
- When multiple replicators are involved, there is no synchronous mechanism in place. In the event that a replicator becomes inactive for a specific stream, the receiver will be required to re-join the tree using an alternative replicator.
- In scenarios where there are no receivers for the multicast traffic, a PIM Register unicast message will be sent to RP. However, since there are no receivers at that point, the RP will respond by transmitting a PIM Register STOP message back to the source.
- Enabling the "spt-mode" helps minimize the exchange of control plane packets for SDWAN multicast, while still allowing multicast data traffic to be replicated through the chosen replicator.
- It is crucial to ensure that "spt-mode" is enabled on every WAN edge router within the SDWAN fabric.

SD-WAN Multicast Key points 2/2

- Data policy interworking with SDWAN overlay multicast is NOT officially tested before and not supported.

```
data-prefix-list Unicast_IPv4
   ip-prefix 0.0.0.0/1
   ip-prefix 128.0.0.0/2
   ip-prefix 192.0.0.0/3
  !
data-policy _VPN_1_AS-Set-local-tloc-policy_v2
```

Limitations of Multicast Configuration

Multicast overlay routing does not support the following features:

- MSDP/Anycast-RP on Cisco SD-WAN routers
- IPv6 overlay and IPv6 underlay
- Dynamic BFD tunnel for multicast
- Multicast with asymmetric unicast routing
- Multicast overlay working does not support Data Policy. In case data policy is configured, then only required traffic is matched and not multicast traffic.

```
      destination-data-prefix-list Unicast_IPv4 ← MATCH ONLY Unicast Traffic
     !
     action accept
      count all_traffic_counter_1526348700
      set
       local-tloc-list
        color mpls
        encap ipsec
      !
     !
    !
  default-action accept
```

SD-WAN Multicast Key points 2/2

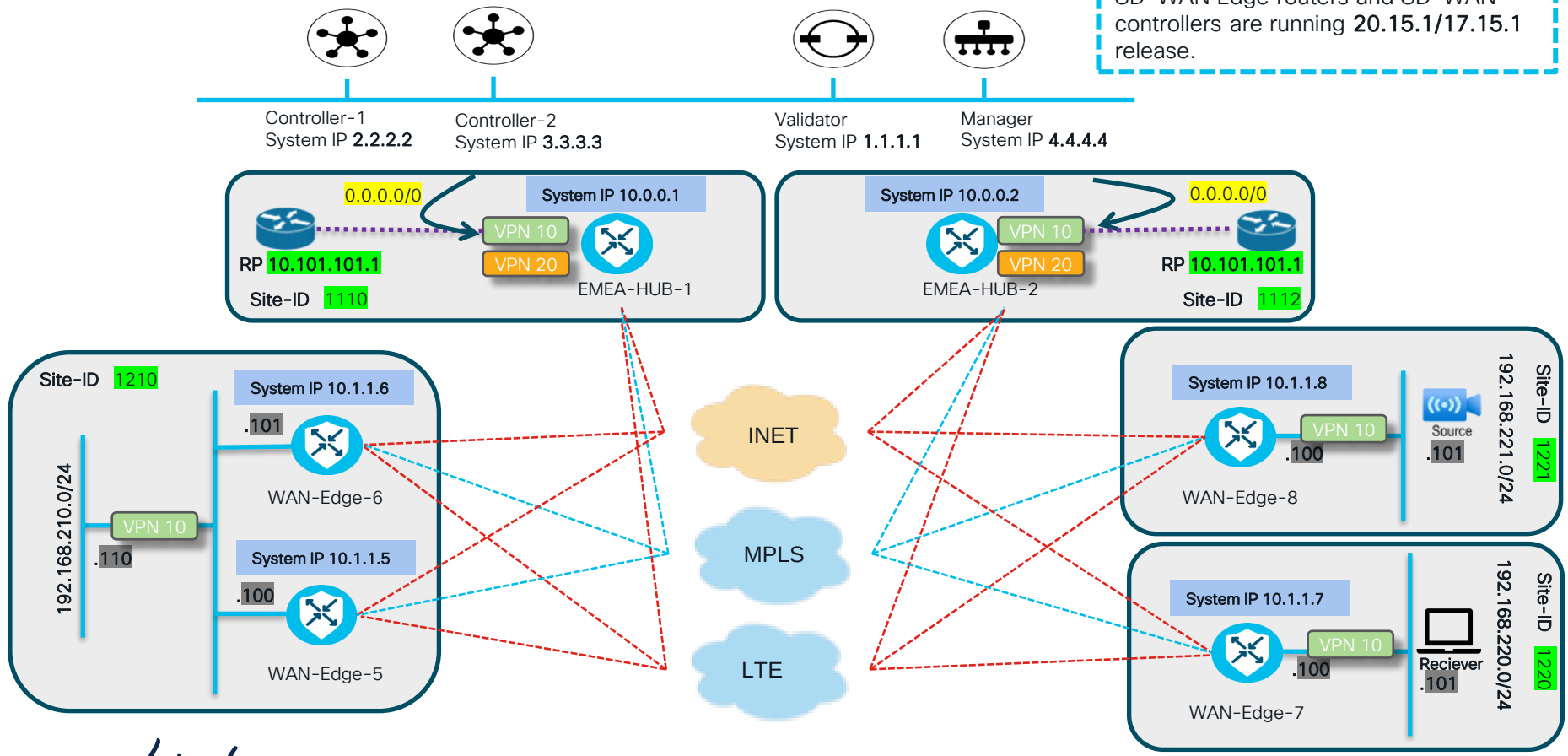
- Data policy interworking with SDWAN overlay multicast is NOT officially tested before and not supported.
- Even localized QoS policy, it might count on data policy to set different forwarding class.
- While configuring data policy or localized QoS policy, we need to make sure ONLY unicast traffic is matched.
- Support for **Hub and Spoke** topology begins with the 17.15.1/20.15.1 software release.
  - Following configuration must be performed on spoke sites using **CLI-Add-on**.

```
!
multicast
 address-family ipv4 vrf <vrf-id>
  spoke
 !
```

```
data-prefix-list Unicast_IPv4
   ip-prefix 0.0.0.0/1
   ip-prefix 128.0.0.0/2
   ip-prefix 192.0.0.0/3
  !
data-policy _VPN_1_AS-Set-local-tloc-policy_v2
  vpn-list VPN_1
    sequence 1
     match
      source-ip 0.0.0.0/0
      dscp 10
      destination-data-prefix-list Unicast_IPv4 ← MATCH ONLY Unicast Traffic
     !
     action accept
      count dscp10_counter_1526348700
      set
       local-tloc-list
        color public-internet
        encap ipsec
      !
     !
    !
    sequence 11
     match
      source-ip 0.0.0.0/0
      destination-data-prefix-list Unicast_IPv4 ← MATCH ONLY Unicast Traffic
     !
     action accept
      count all_traffic_counter_1526348700
      set
       local-tloc-list
        color mpls
        encap ipsec
      !
     !
    !
  default-action accept
```

Demo Topology

SD-WAN Edge routers and SD-WAN controllers are running **20.15.1/17.15.1** release.

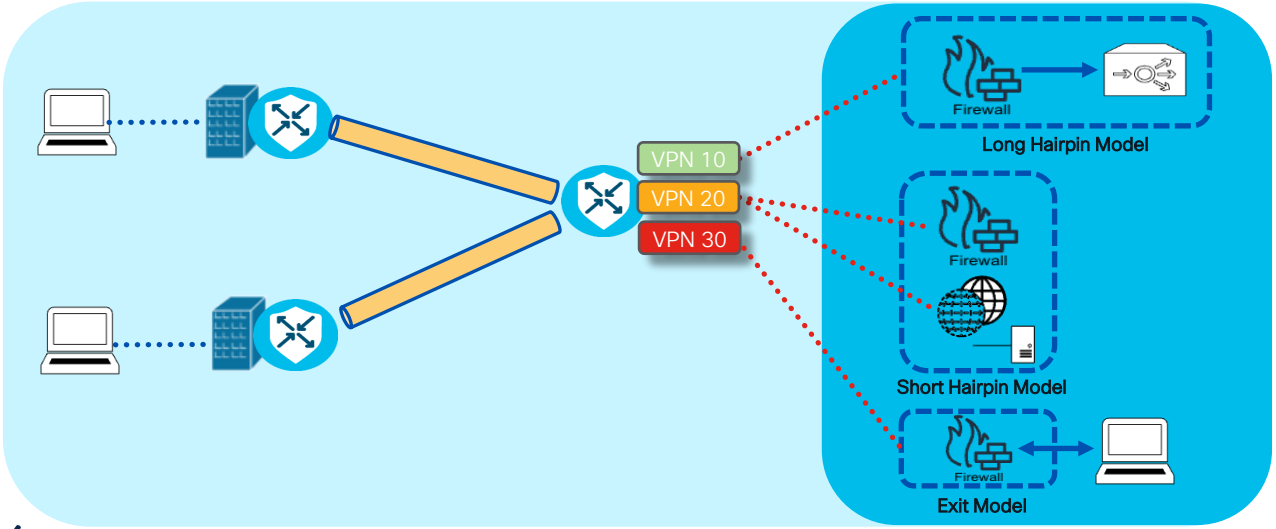


How OMP Enables Seamless Service Chaining?

What is Service Chaining?

In Cisco SD-WAN, a **service chain** is used to define the sequence of network services (like firewalls, load balancers, etc.) that traffic must pass through before reaching its destination.

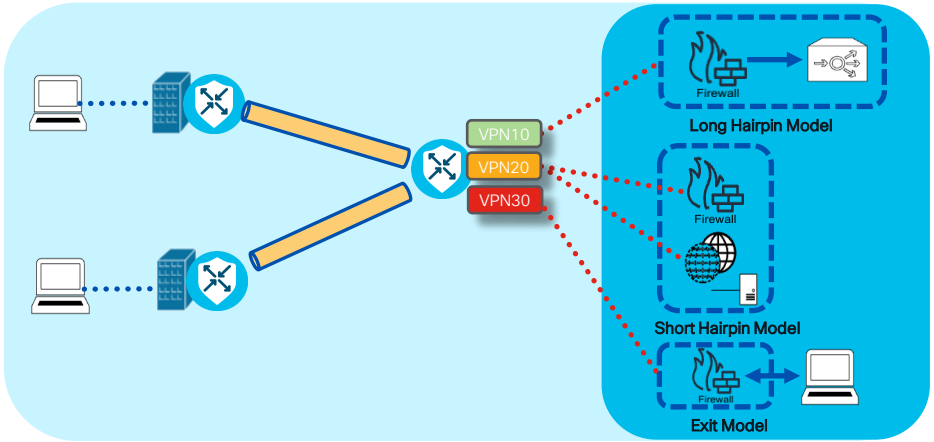
- The short hairpin serves as the base model.
- Long & Exit are cases of short hairpin.
- Service Chain can be in any device in any topology: **full mesh**, **hub-spoke**, **MRF**.
- Max **16 Service Chain** types.
- Max **4 services** in a **Service Chain**(SC).



What is Service Chaining?

In Cisco SD-WAN, a **service chain** is used to define the sequence of network services (like firewalls, load balancers, etc.) that traffic must pass through before reaching its destination.

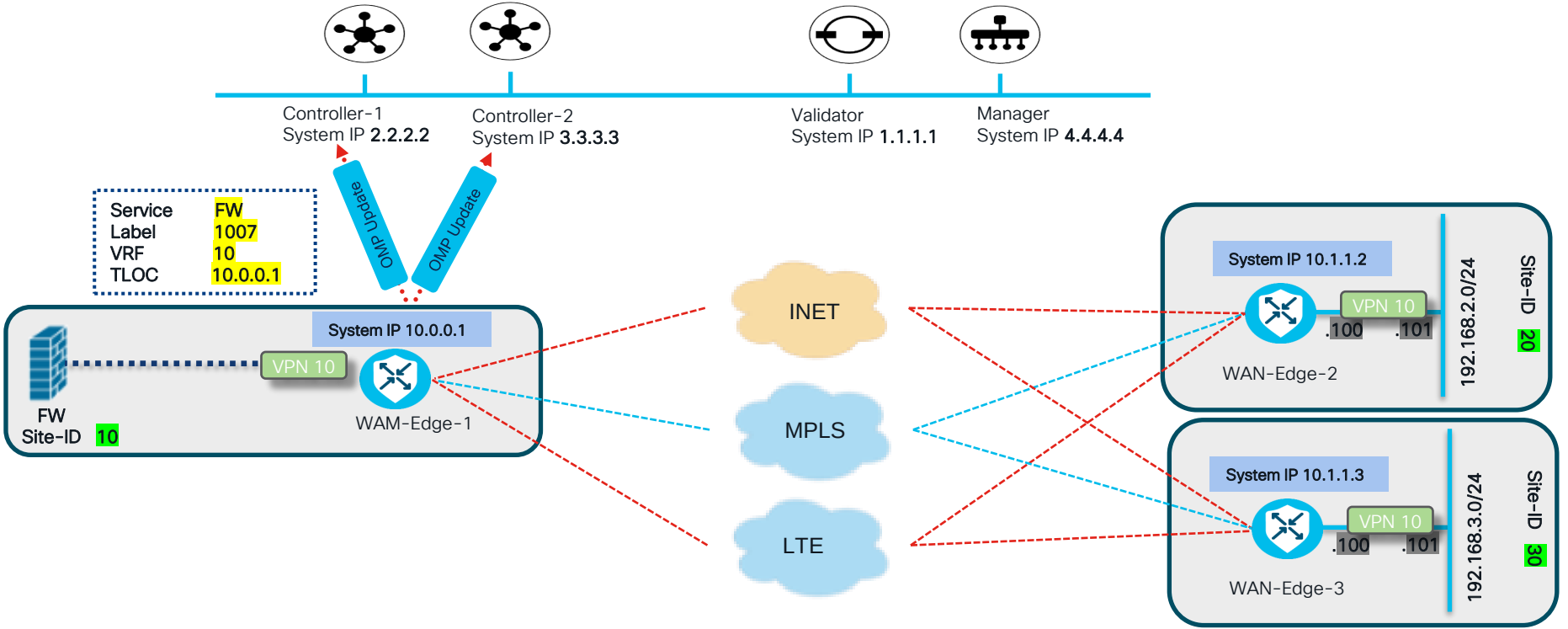
- The short hairpin serves as the base model.
- Long & Exit are cases of short hairpin.
- Service Chain can be in any device in any topology: **full mesh**, **hub-spoke**, **MRF**.
- Max **16 Service Chain** types.
- Max **4 services** in a **Service Chain**(SC).



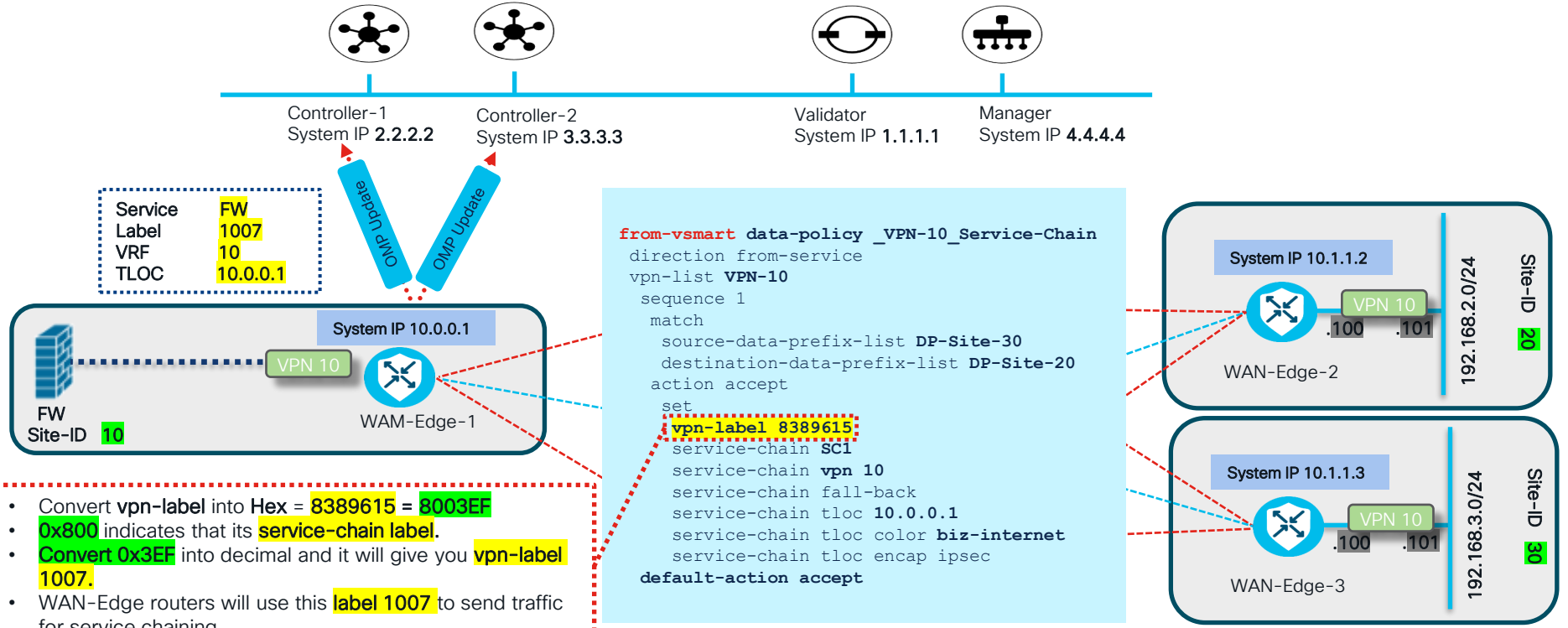
Traffic Steering to a SC "**set service-chain <>**" action in:

- Centralized **Control Policy**
- Centralized **Data Policy**
  - Co-located
  - Remote
- **Interface ACL**
  - Always **co-located.**

How Does OMP Relay Service Chaining Information?



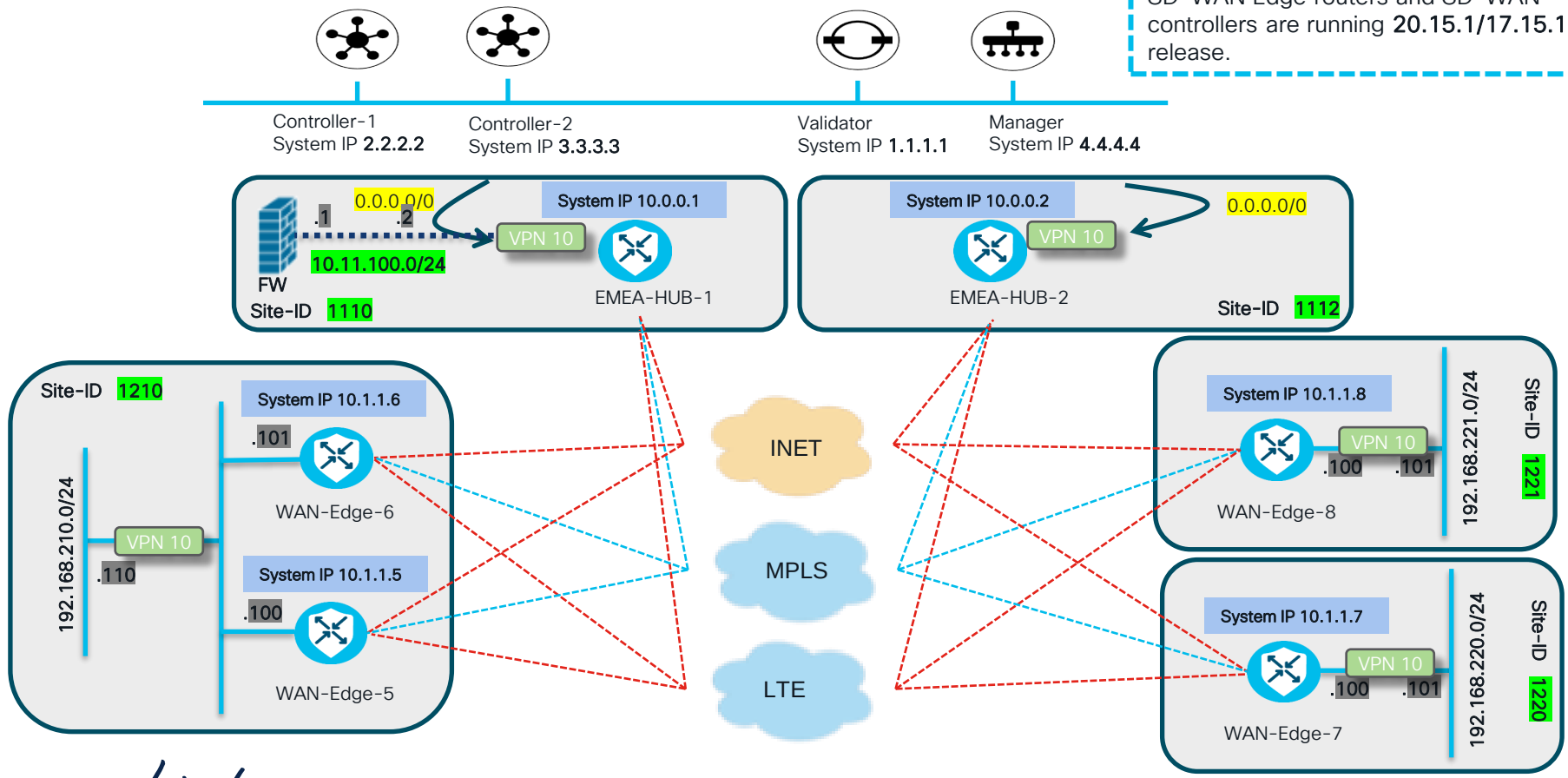
How Does OMP Relay Service Chaining Information?



- Convert **vpn-label** into **Hex** = 8389615 = 8003EF
- 0x800 indicates that its **service-chain label**.
- Convert 0x3EF into decimal and it will give you **vpn-label** 1007.
- WAN-Edge routers will use this **label 1007** to send traffic for service chaining.

Demo Topology

SD-WAN Edge routers and SD-WAN controllers are running **20.15.1/17.15.1** release.



Quiz Time

SD-WAN

Learn how to confidently deploy and operate Cisco's SD-WAN solution in a new or existing network. These sessions provide a journey from the foundation to latest Cisco SD-WAN innovations focusing on design, innovations, and integrations with Cloud, SASE, and Assurance/Analytics.

Monday-Thursday

START

LABENT-2547
Troubleshooting Cisco SD-WAN Control Plane

LABENT-2544
Troubleshooting Cisco SD-WAN Data Plane

LABENT-2490
Understanding SD-WAN Overlay Management Protocol

LABENT-2570
Unified Security Policy in Cisco SD-WAN

LABENT-2581
Adaptive QoS in Cisco SD-WAN

Monday, February 5 | 8:30 a.m.
TECENT-3377
Deep dive into Cisco SD-WAN - how it works

Monday, February 5 | 8:45 a.m.
TECENT-2208
Implementing SD-WAN Branch on-prem/ SASE Security

Monday, February 5 | 2:00 p.m.
TECENT-2376
From Zero to SD-WAN Hero: Planning, Designing and Implementing Cisco SD-WAN

Tuesday, February 6 | 8:00 a.m.
BRKENT-2108
Cisco SD-WAN: Start Here

Tuesday, February 6 | 8:00 a.m.
BRKENT-2524
Multicloud Security Unleashed: Bridging the Gap Between SD-WAN, Clouds, Firewall Service Insertion, Valtix and Secure Internet Gateways

Tuesday, February 6 | 9:30 a.m.
BRKENT-2660
Customer Case Studies: Lessons learned from Cisco's SD-WAN Design Council

Tuesday, February 6 | 2:00 p.m.
BRKENT-2043
Harnessing the Capabilities of the Cisco Catalyst SD-WAN Policy Framework: Architecture, Building Blocks, and Case Studies.

Wednesday, February 7 | 8:45 a.m.
BRKENT-3797
Advanced SD-WAN Policies Troubleshooting

Wednesday, February 7 | 1:45 p.m.
BRKENT-2283
4 steps to unify Multi-Cloud Connectivity and Design with Cisco SD-WAN principles

Thursday, February 8 | 10:30 a.m.
BRKTRS-3050
Cisco SD-WAN - Hidden Complexity Revealed - How Cisco TAC Addresses Really Tricky Problems?

Thursday, February 8 | 10:30 a.m.
BRKENT-2006
Optimizing and Orchestrating End Users' Connections to Public and Private Clouds in a SASE World

FINISH

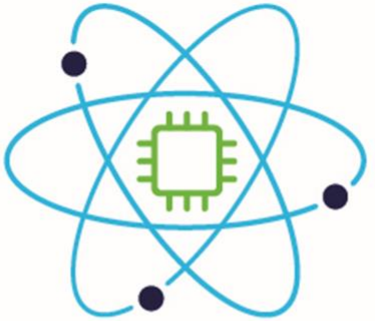
If you are unable to attend a live session, you can watch it in the On-demand library.

Become a power user

Cisco Live Amsterdam Exclusive:
Save 25% on CML-Personal and CML-Personal Plus.

Visit the Learning & Certification booth to learn more.

cisco Live!



Powered by
Cisco Modeling Labs

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

Continue your education

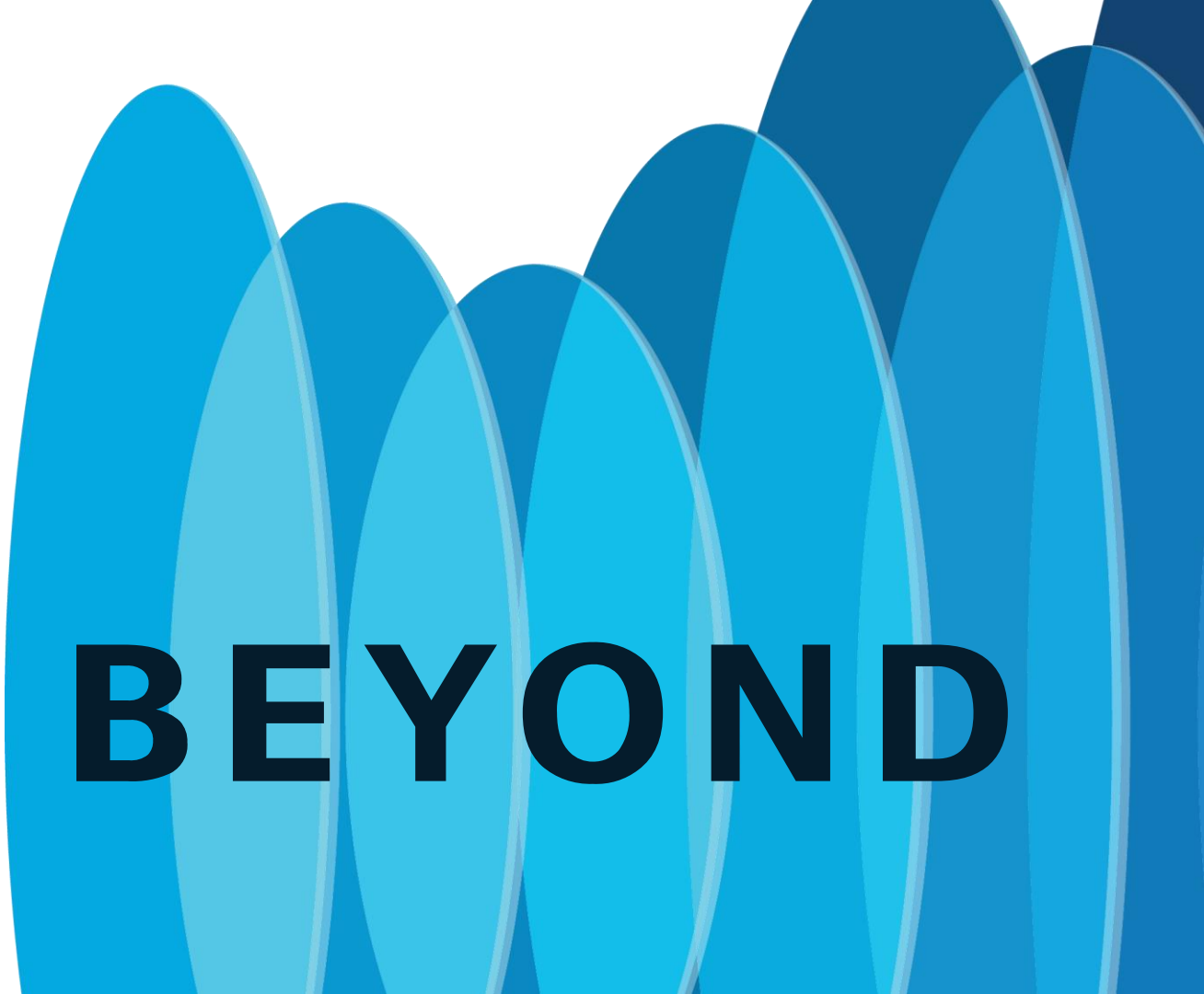
- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at: **BRKENT-3115 Webex Space.**

Thank you

cisco Live!

cisco Live!



GO BEYOND