
cisco
You make possible

Cisco SD-WAN (Viptela)

Branch and Data Center Integration Design

Larry Roberts– Presenter

BRKRST-2091

cisco Live!

Barcelona | January 27-31, 2020

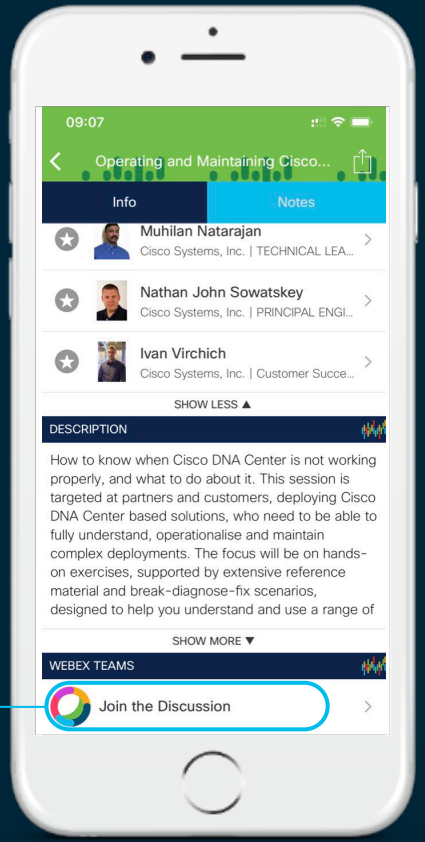
Cisco Webex Teams

Questions?

Use Cisco Webex Teams 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 Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



Agenda

- Introduction
- Data Center Integration
- Branch Integration
- Overlay/Underlay Routing
- Segmentation Design and Integration
- Conclusion

Introduction

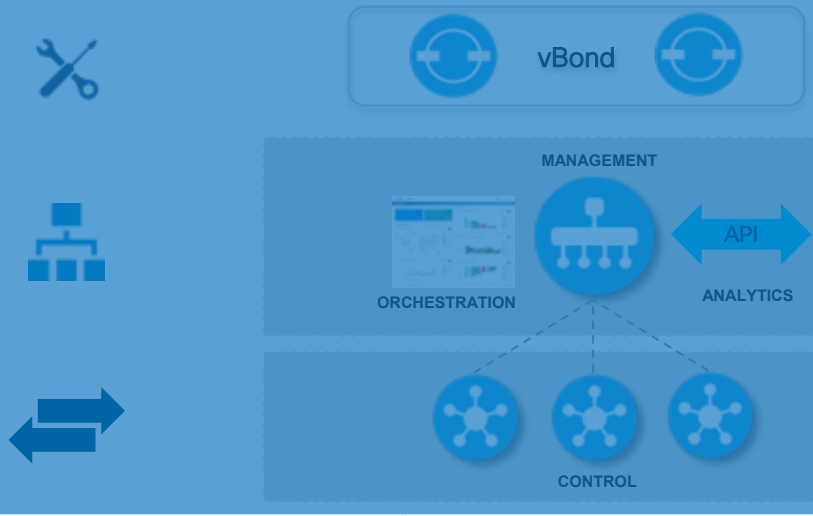
Cisco SDWAN

Orchestration Plane

Management Plane
(Multi-tenant or Dedicated)

Control Plane
(Containers or VMs)

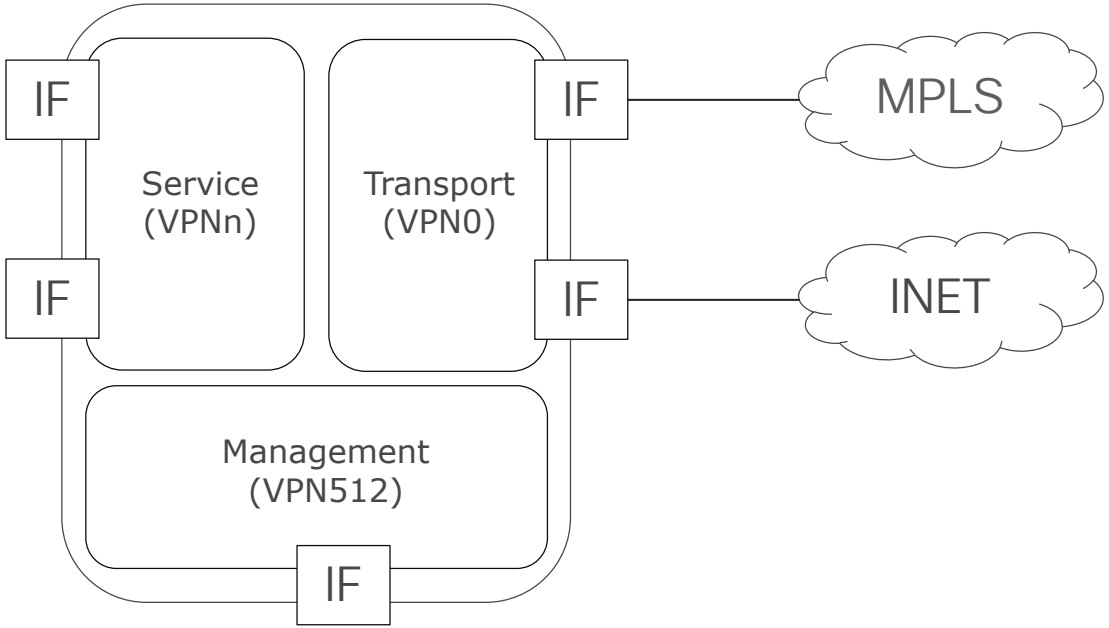
Data Plane
(Physical or Virtual)



vManage
vSmart
vBond
vBond
Edge

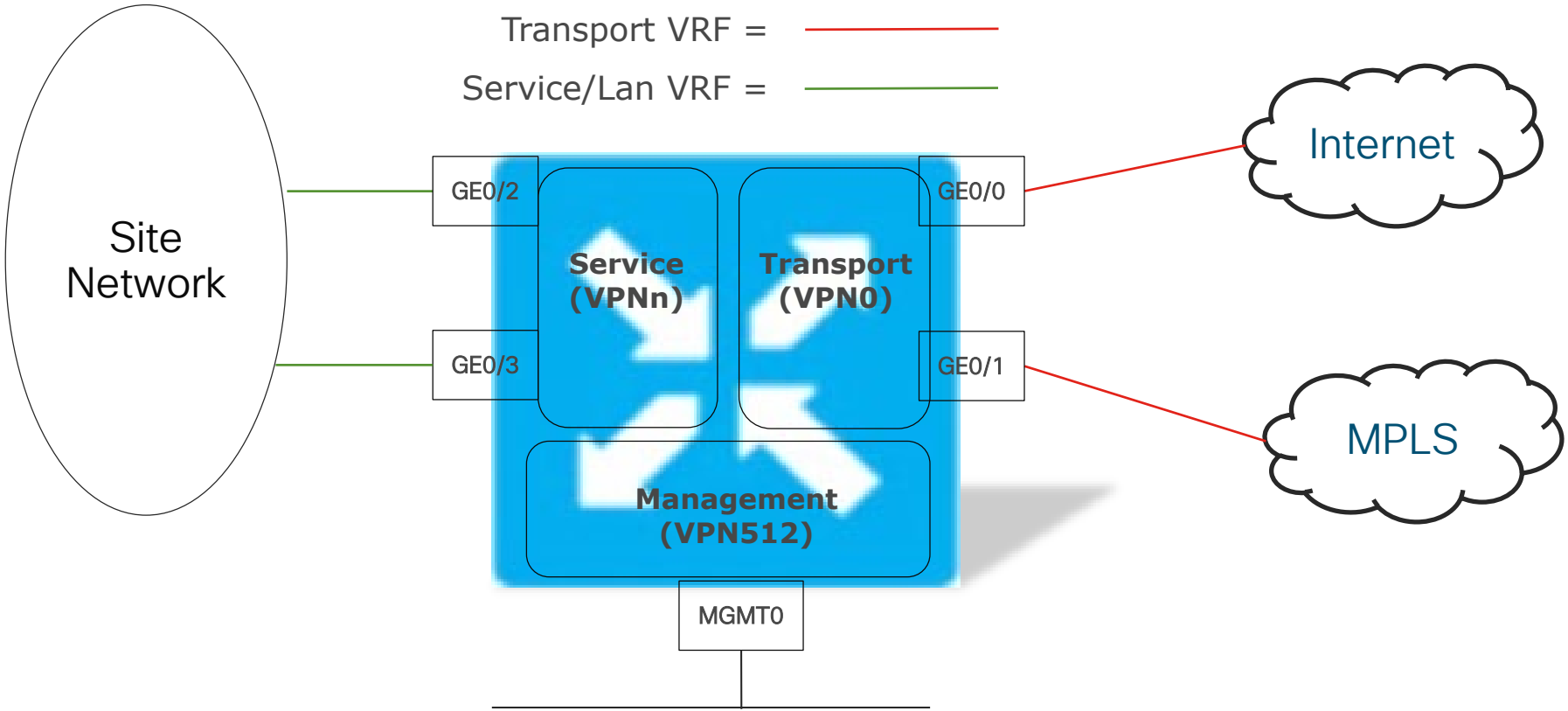
Today's Focus

Cisco SD-WAN VPNs

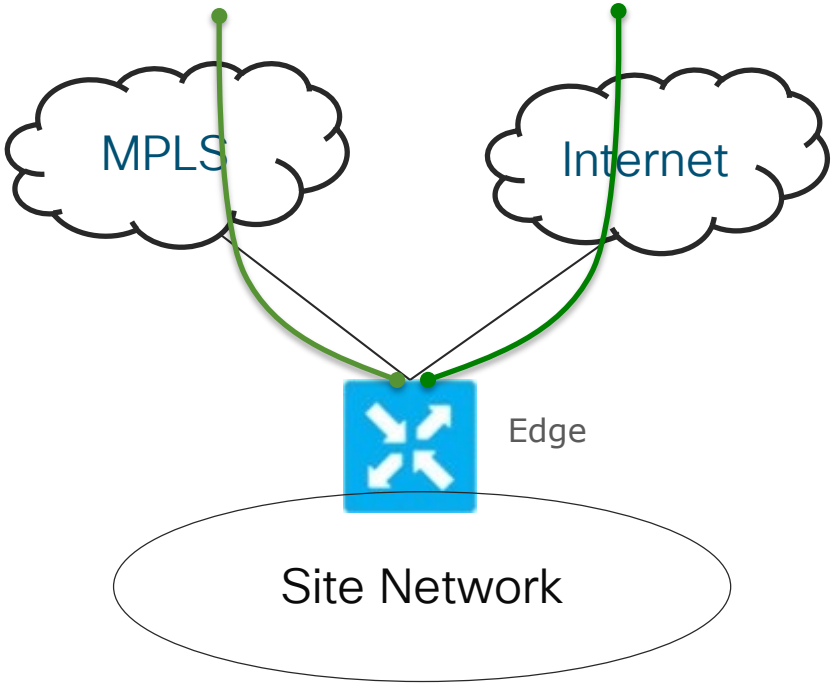


- VPN = VRF
- VPNs are isolated from each other, each VPN has its own forwarding table
- Edge router allocates label to each of it's service VPNs and advertises it as route attribute in OMP updates
  - Labels are used to identify VPN in the incoming packets
- Service VPN can be any number except 0 or 512 as those are reserved for Transport and Management

SD-WAN VPNs Cont.

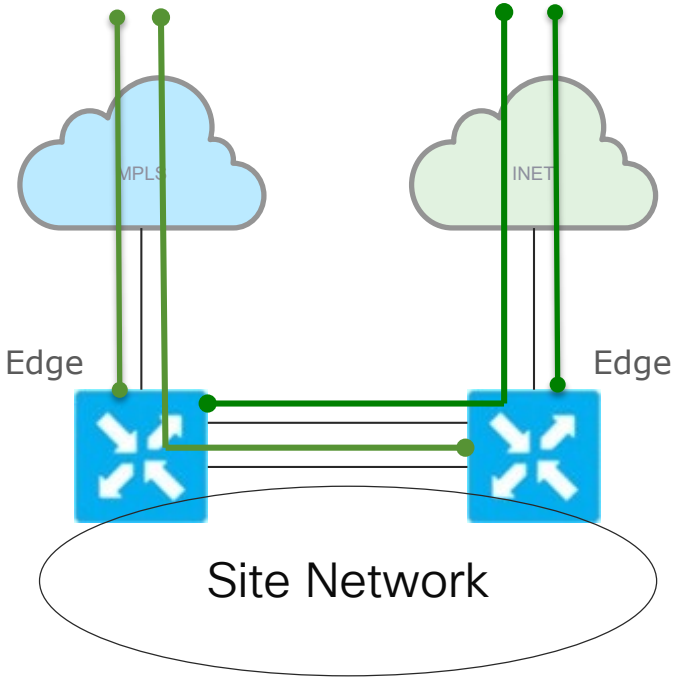


Transport Connectivity



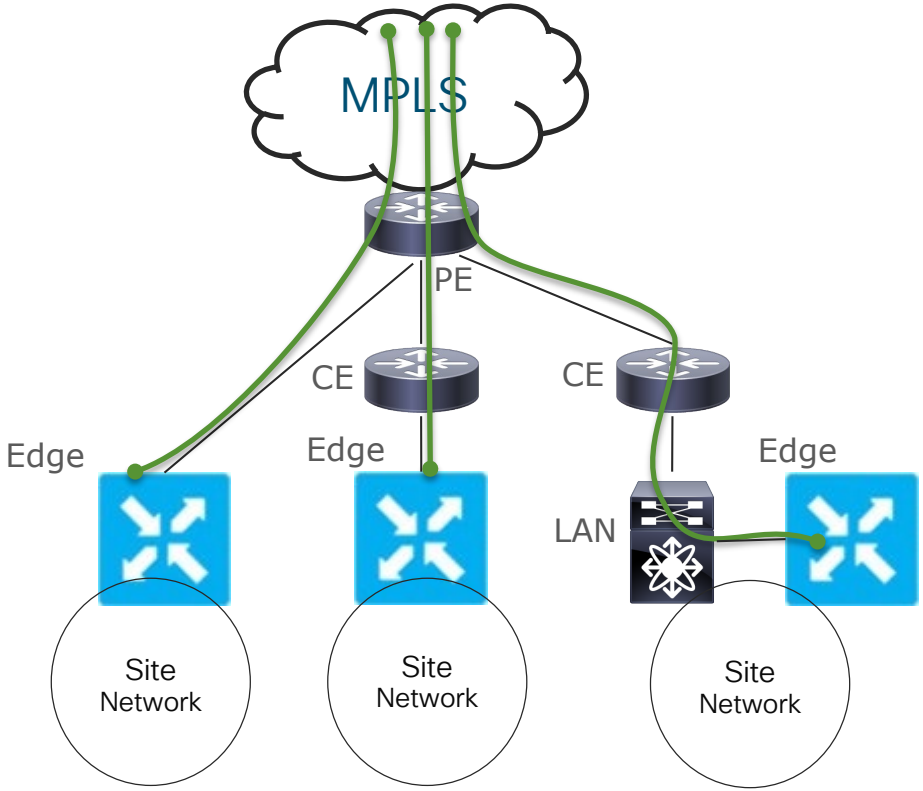
- Edge routers are connected to all transports
- When a transport goes down, Edge routers detect the condition and bring down the tunnels built across the failed transport
  - BFD times out across tunnels
- Edge router still draws the traffic for the prefixes available through the SD-WAN fabric

Transport Redundancy – TLOC Extension



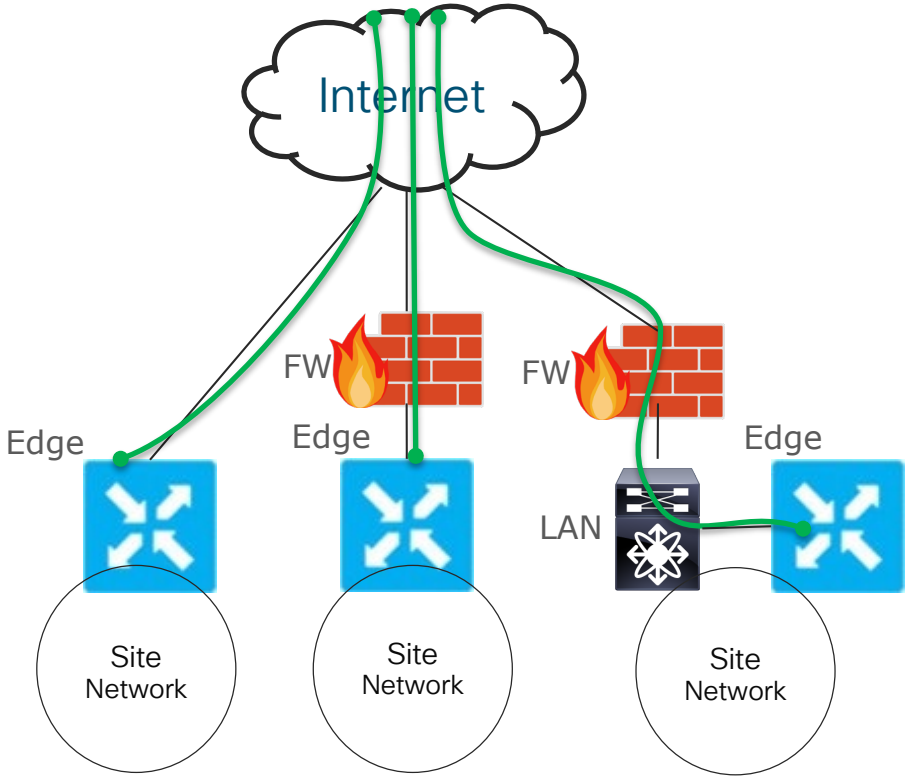
- Edge routers are connected only to their respective transports
- Edge routers build IPSec tunnels across directly connected transport and across the transport connected to the neighboring Edge router
  - Neighboring Edge router acts as an underlay router for tunnels initiated from the other Edge
- If one of the Edge routers fails, second Edge router takes over forwarding the traffic in and out of site
  - Only transport connected to the remaining Edge router can be used

MPLS Transport Connection Points



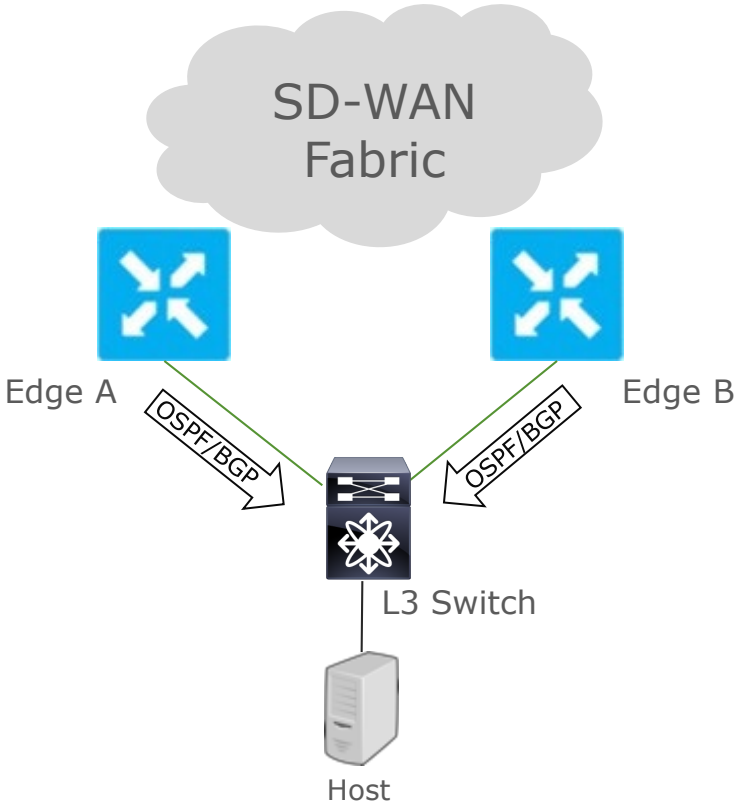
- Direct Connectivity from Edge to PE is used in CE replacement designs
- Edge sitting behind CE is typically used when TDM connectivity is required or when using the CE as a backup or alternative path to the SD-WAN overlay
- Edge connecting to the LAN for transport connectivity is used when CE is still required but no ports are available for direct physical connectivity

Internet Transport Connection Points



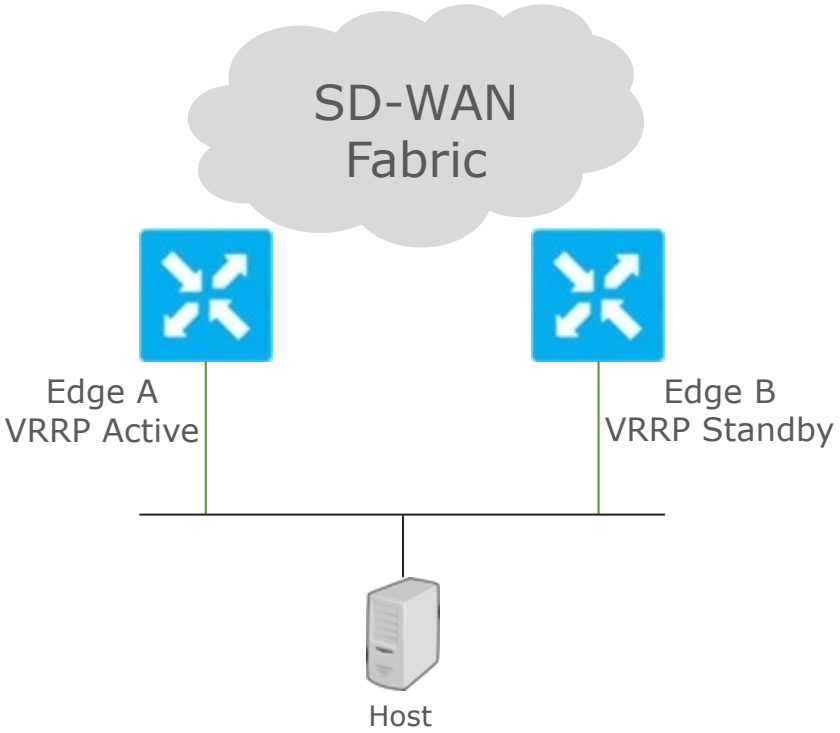
- Direct Connectivity from Edge to Internet is used mostly in the branch when no FW is present or needed. Can also be used in the DC if allowed by security teams.
- Edge sitting behind FW is typically used in the DC. Can be used in the Branch if FW is required by security.
- Edge connecting to the LAN for transport connectivity is used when FW is still required but no direct connection to FW is available.

Site Redundancy – Layer 3 LAN



- Redundant pair of Edge routers operate in active/active mode
- Edge routers are one or more Layer 3 hops away from the hosts
- Standard OSPF or BGP routing protocols are running between the redundant pair Edge routers and the LAN Switch. EIGRP is also available on XE-SDWAN platforms.
- Bi-directional redistribution between OMP and OSPF/BGP and vice versa on the Edge routers
- Site router performs equal cost multipathing for remote destinations across SD-WAN Fabric
  - Can manipulate OSPF/BGP to prefer one Edge router over the other

Site Redundancy – Layer 2 LAN



- Edge routers are Layer 2 adjacent to the hosts
  - Default gateway for the hosts
- Virtual Router Redundancy Protocol (VRRP) runs between the two redundant Edge routers
- VRRP Active Edge responds to ARP requests for the virtual IP with its physical interface MAC address
- In case of failover, new VRRP Active Edge router sends out gratuitous ARP to update ARP table on the hosts and mac address table on the intermediate L2 switches

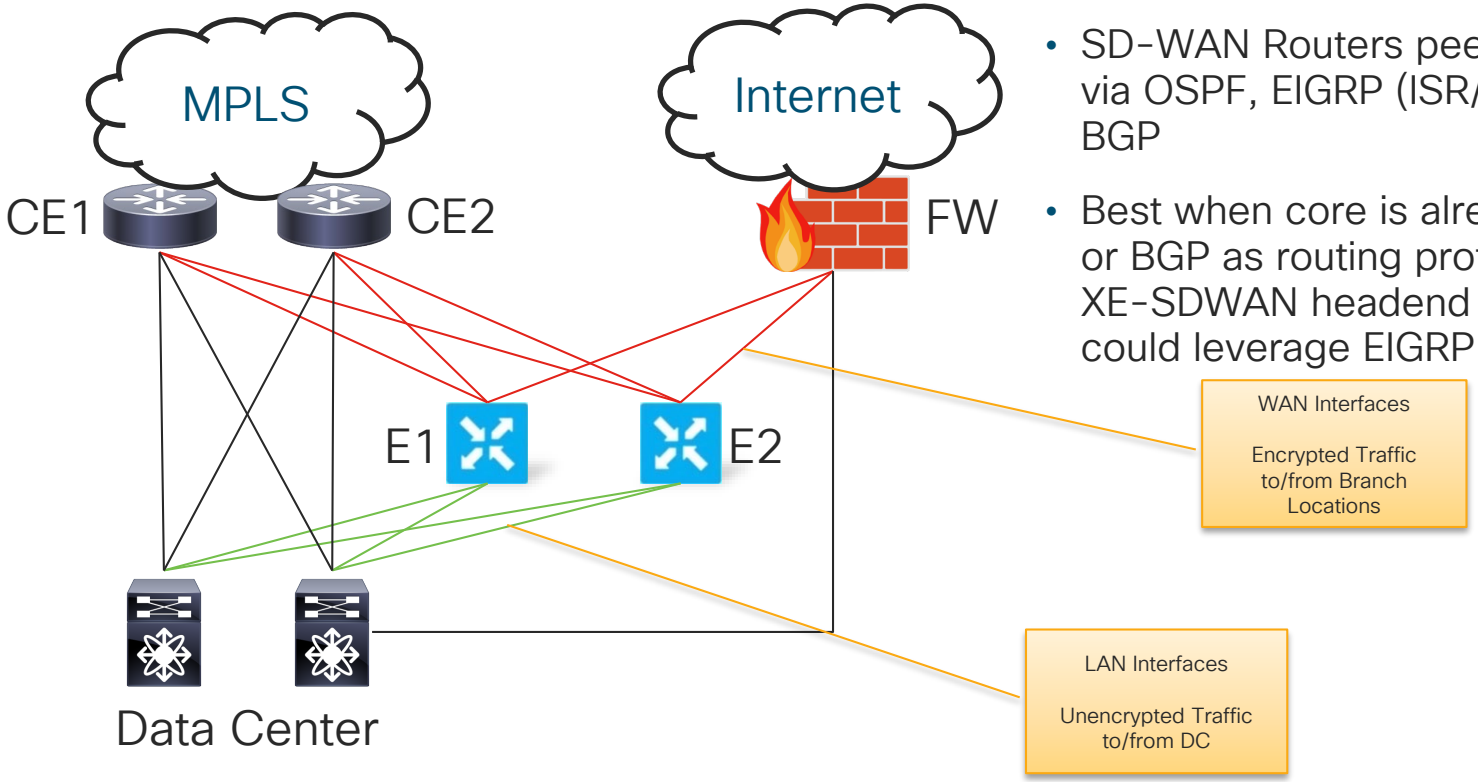
Data Center Design

Data Center Design Principles

- Do not impact normal traffic flows to/from Data Center for sites which have not converted to SD-WAN
- Integration should be transparent to the business
- Leverage BGP when possible OSPF/EIGRP when necessary
- Integrate routing with the Core or WAN Services Block if possible
- Integrate routing with Customer Edge when necessary

Layer 3 to Data Center LAN

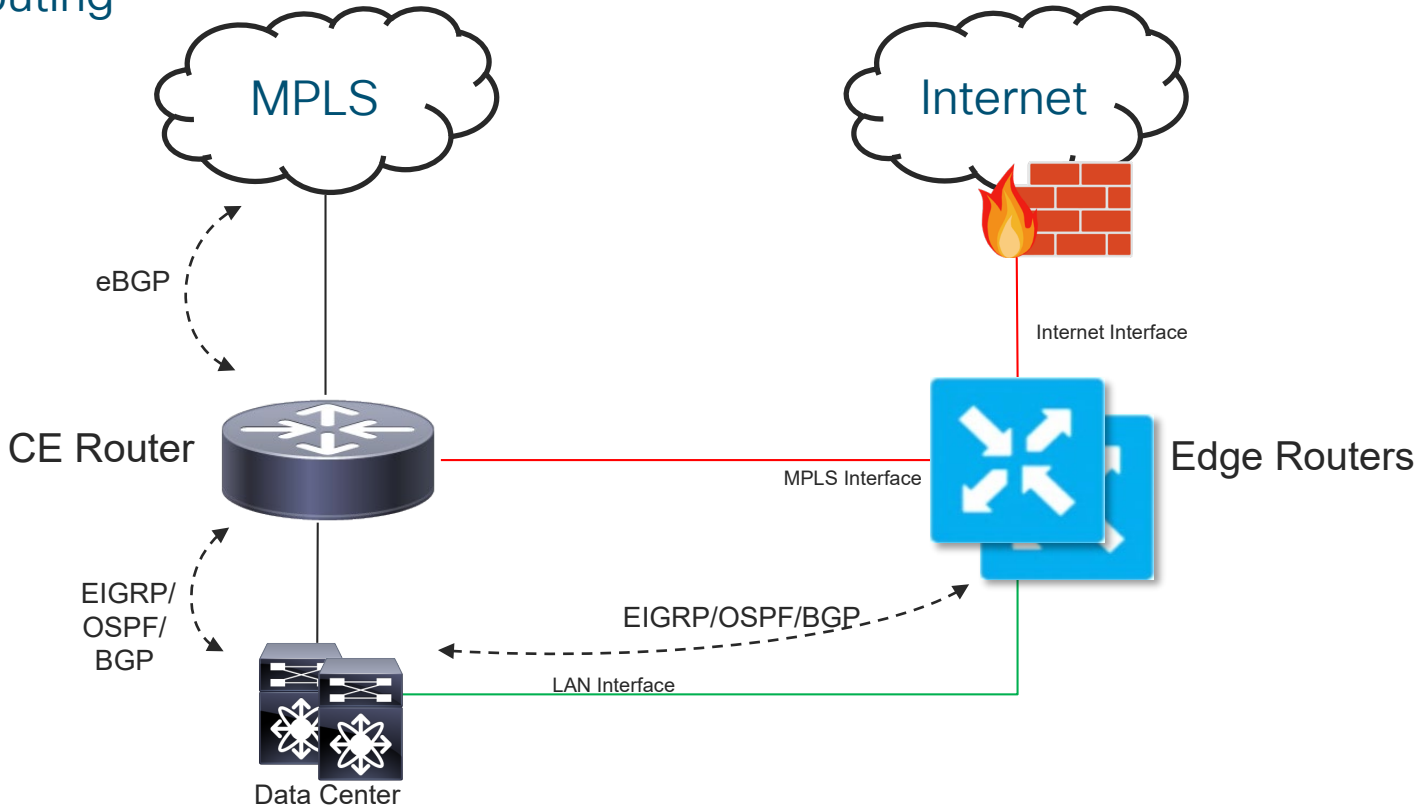
Overview



- SD-WAN Routers peer with DC Core via OSPF, EIGRP (ISR/ASR only), or BGP
- Best when core is already using OSPF or BGP as routing protocols. If using XE-SDWAN headend platform you could leverage EIGRP as well.

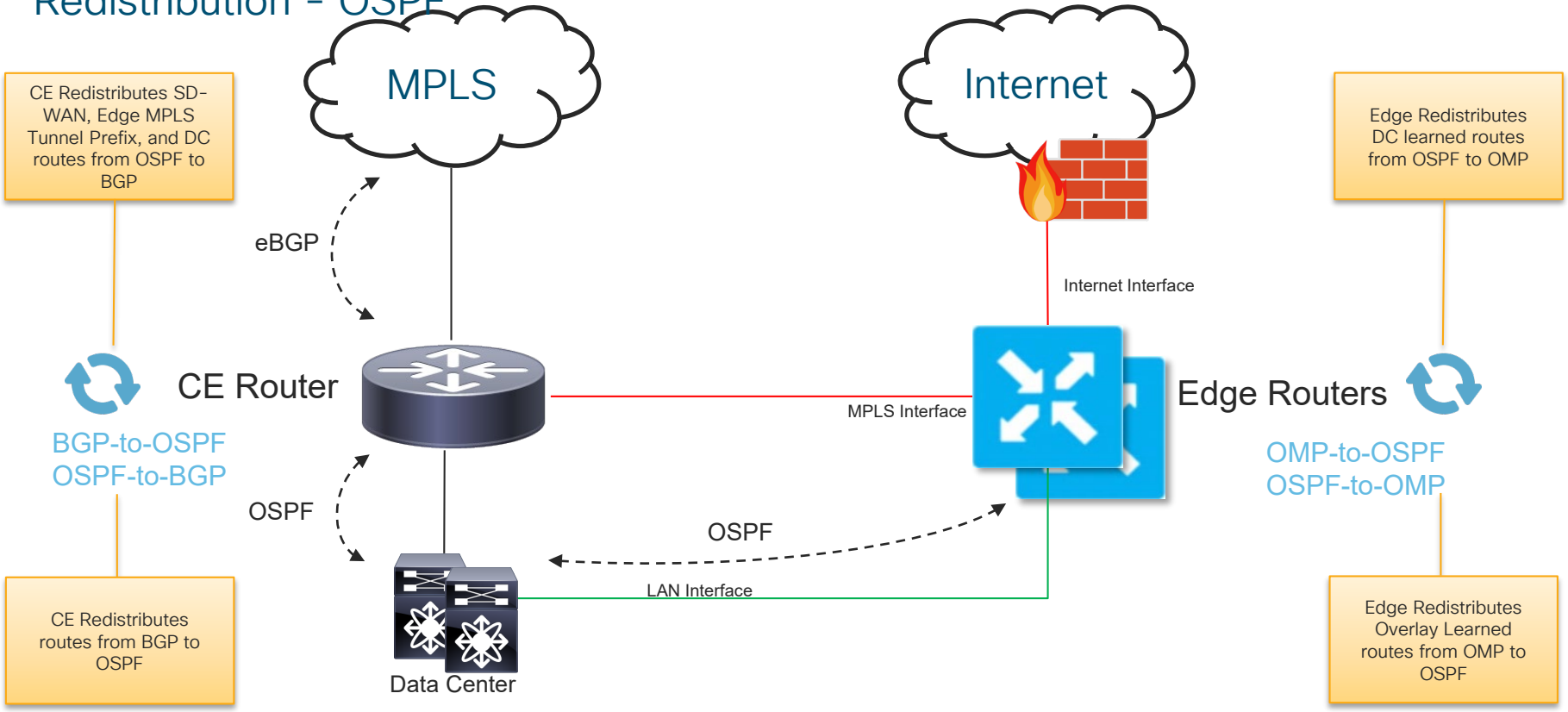
Layer 3 to Data Center

LAN Routing



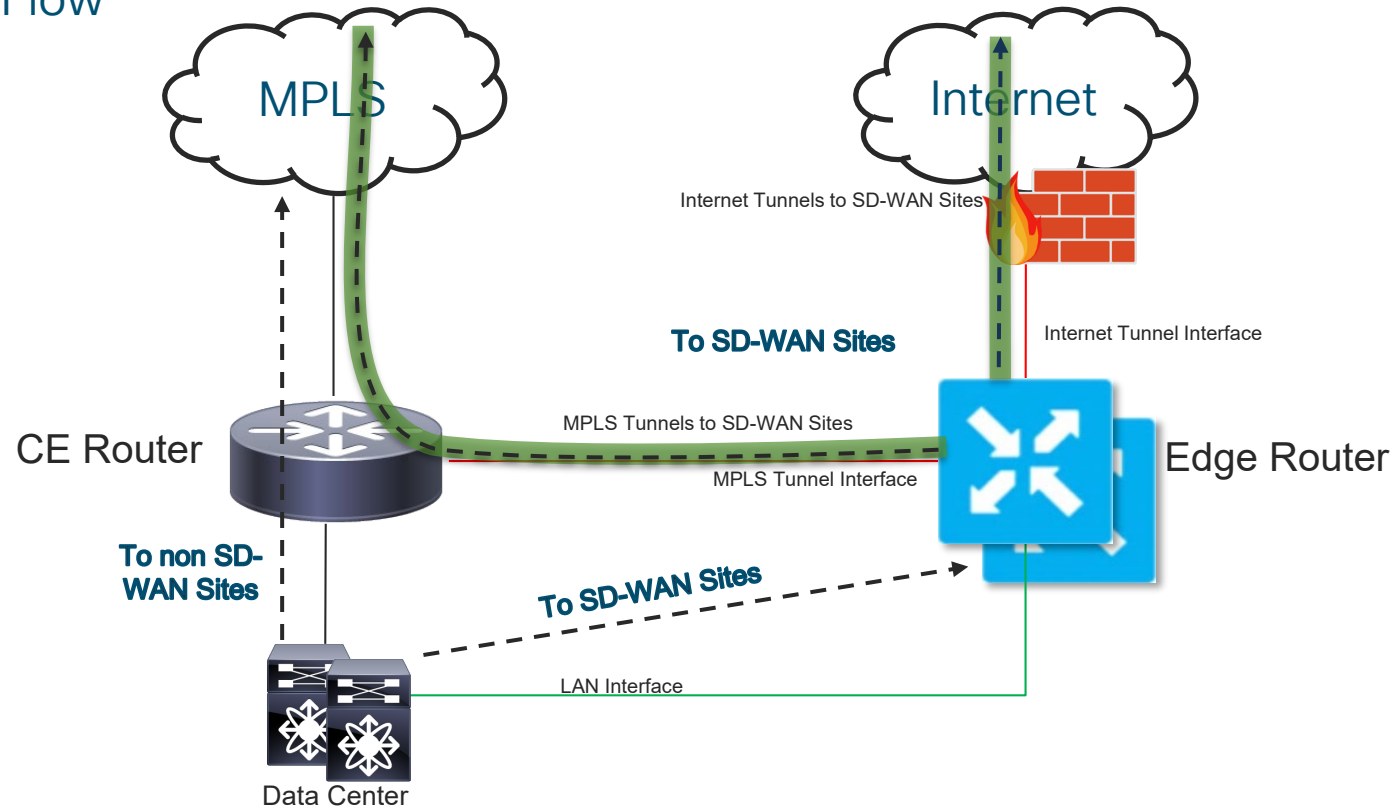
Layer 3 to Data Center LAN

Redistribution – OSPF



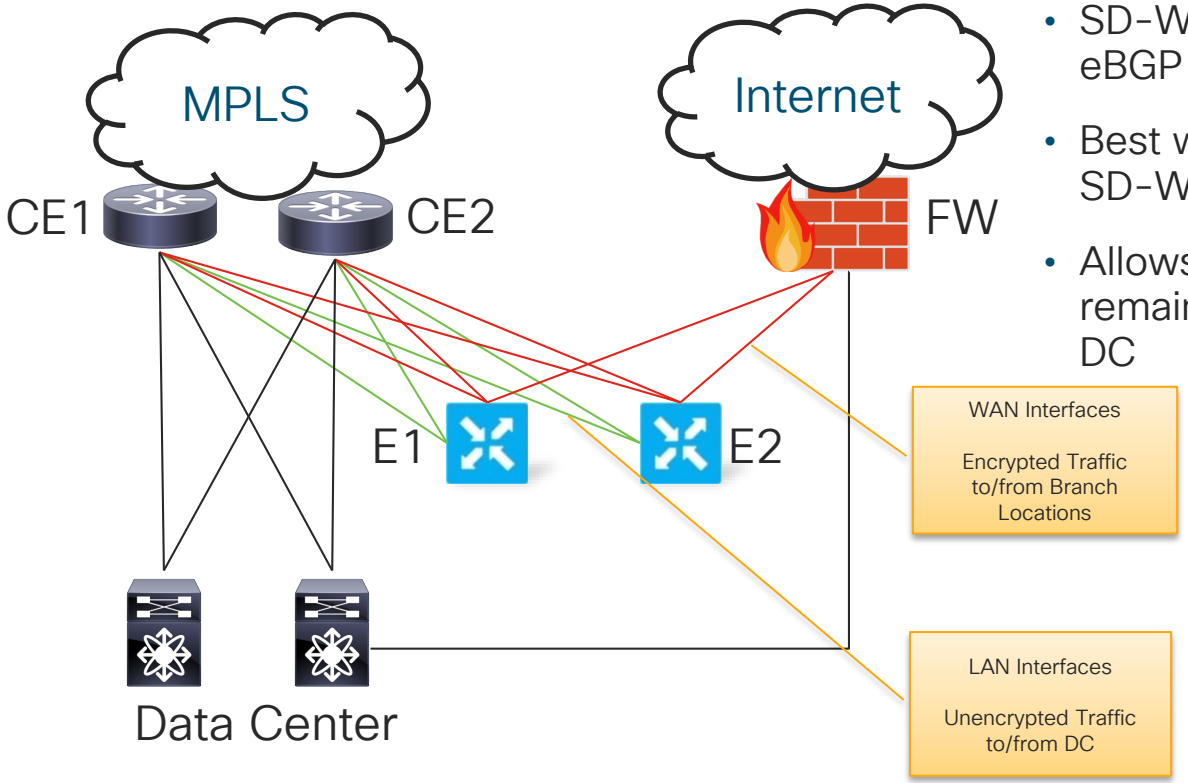
Layer 3 to Data Center LAN

Traffic Flow



Layer 3 Integration with CE Router

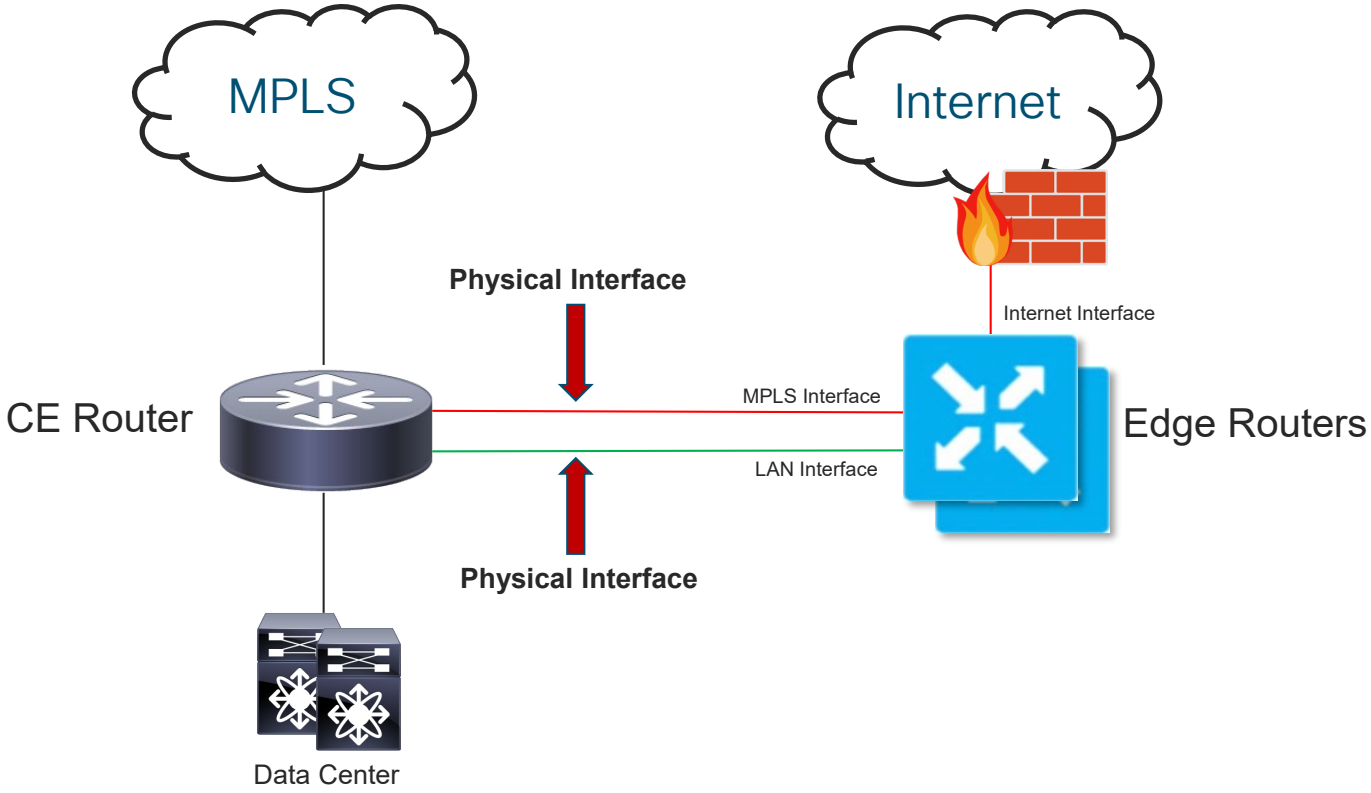
Overview



- SD-WAN Routers peer with the CE via eBGP
- Best when DC LAN is using EIGRP and SD-WAN Headend is vEdge platform
- Allows route-redistribution point to remain on CE only. Simplifies routing in DC

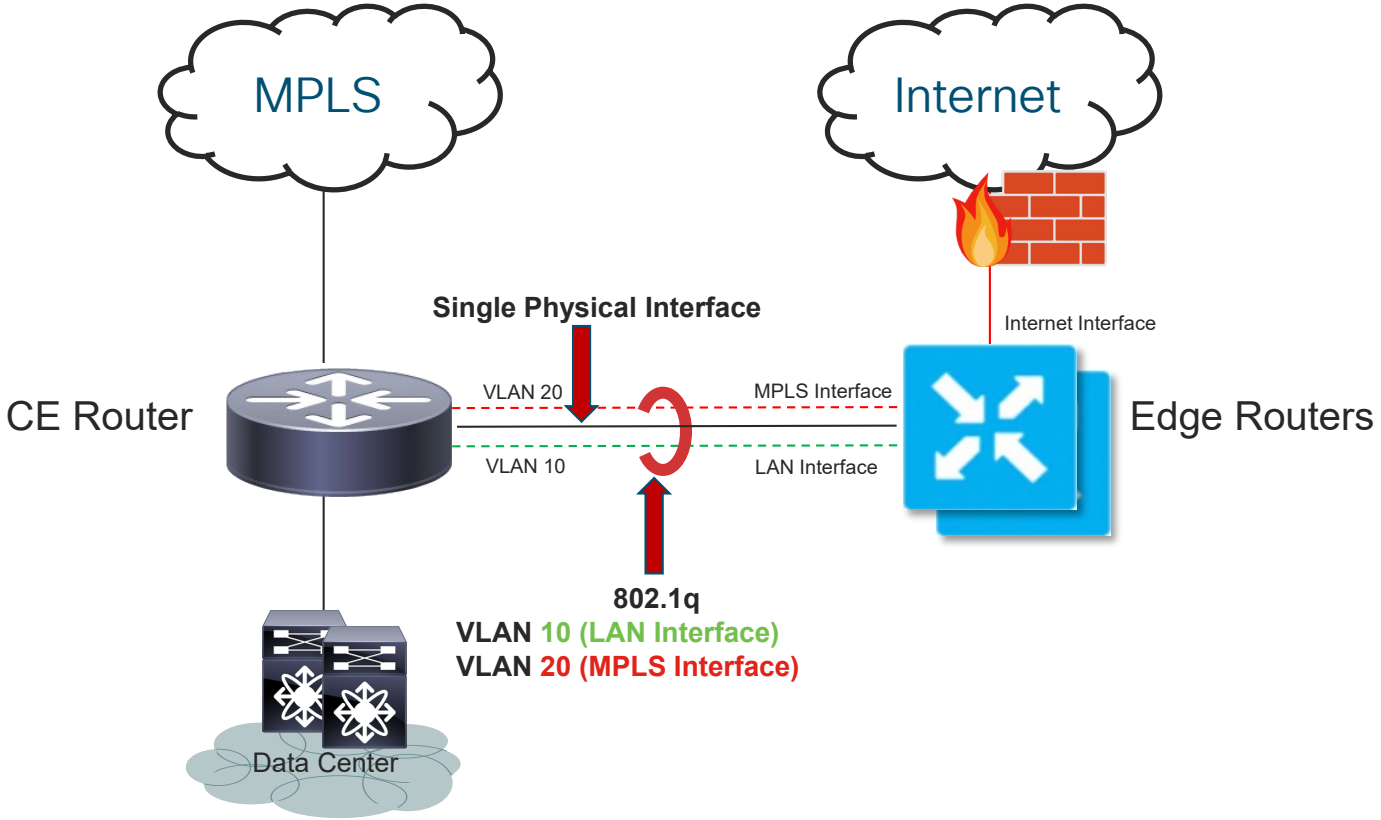
Layer 3 Integration with CE Router

Two Physical Ports



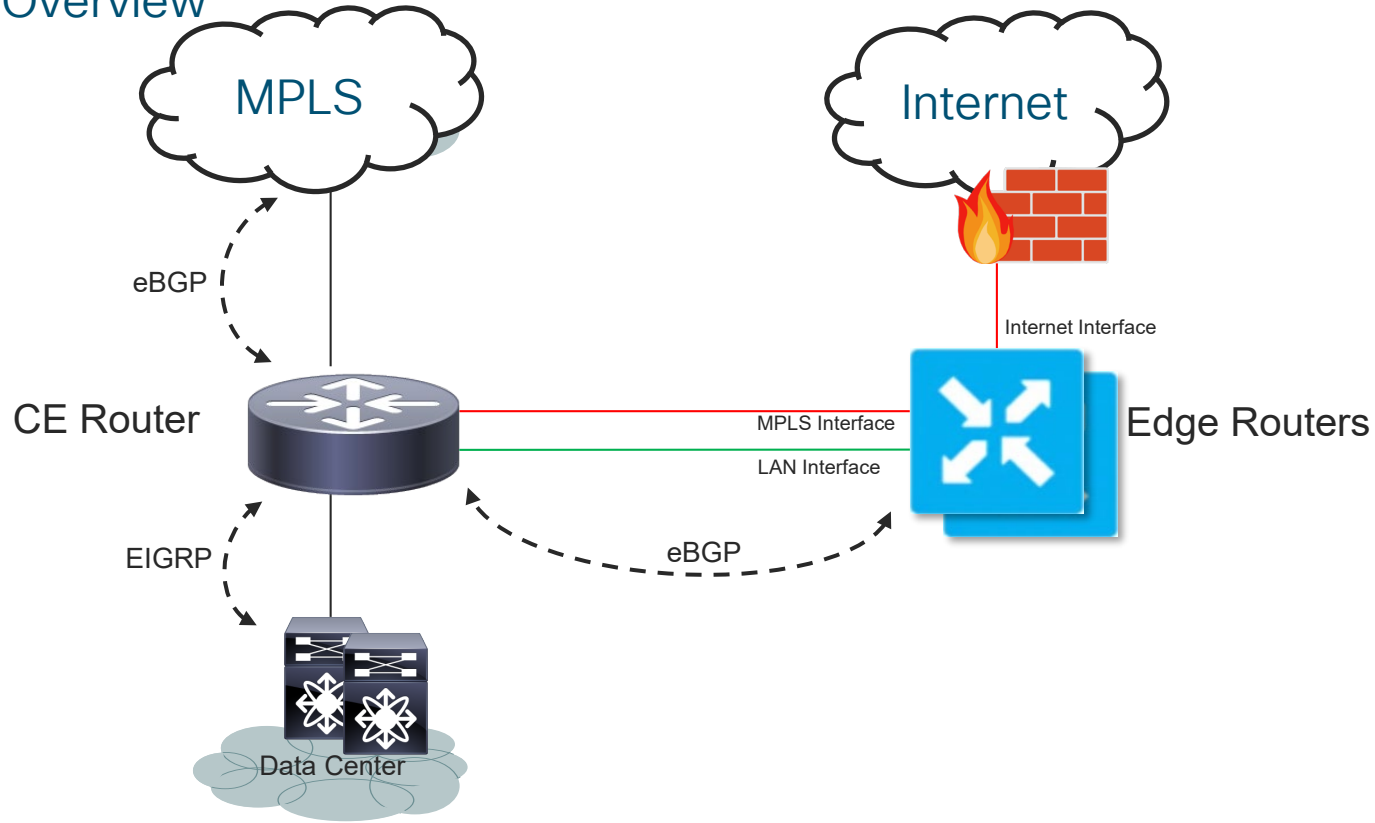
Layer 3 Integration with CE Router

One Physical Trunk Port



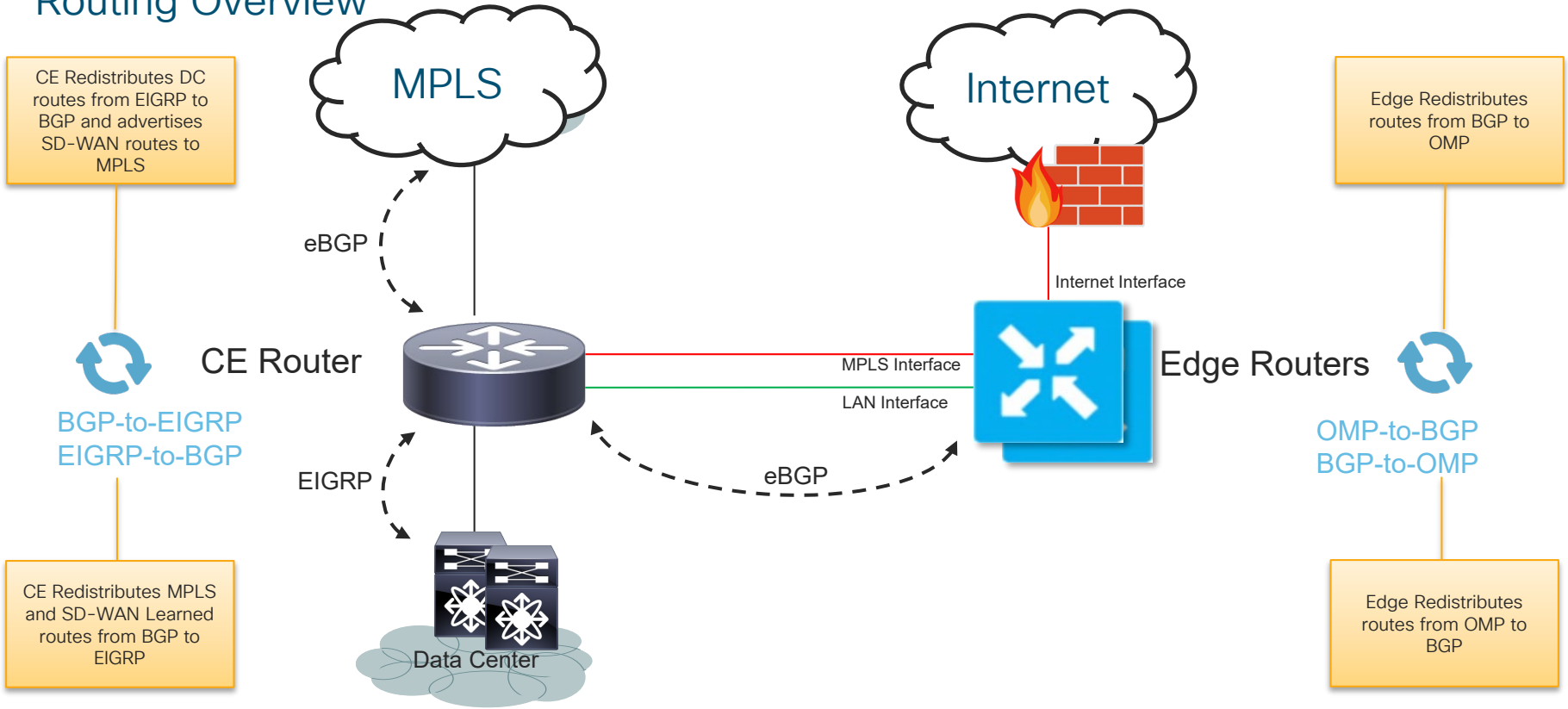
Layer 3 Integration with CE Router

Routing Overview



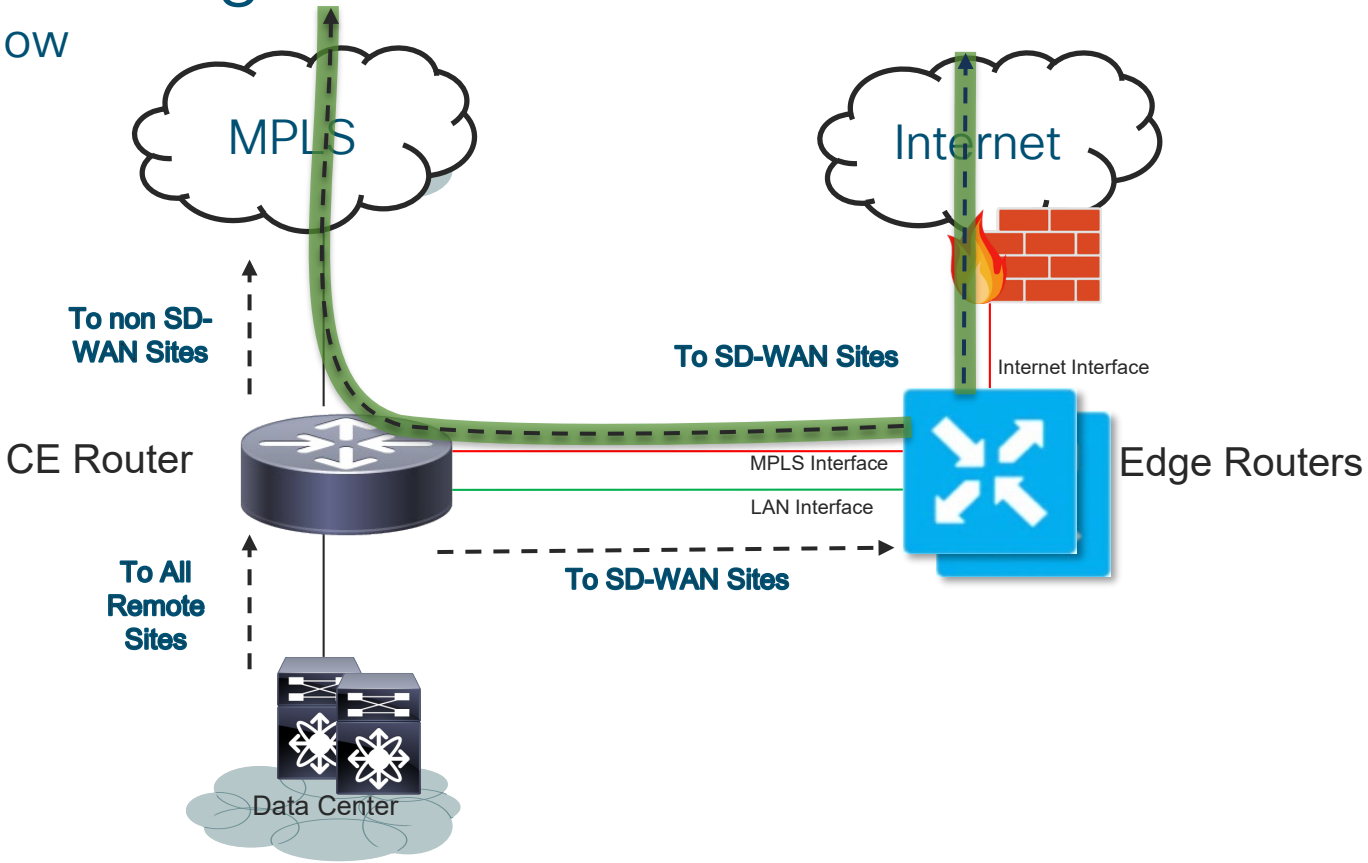
Layer 3 Integration with CE Router

Routing Overview



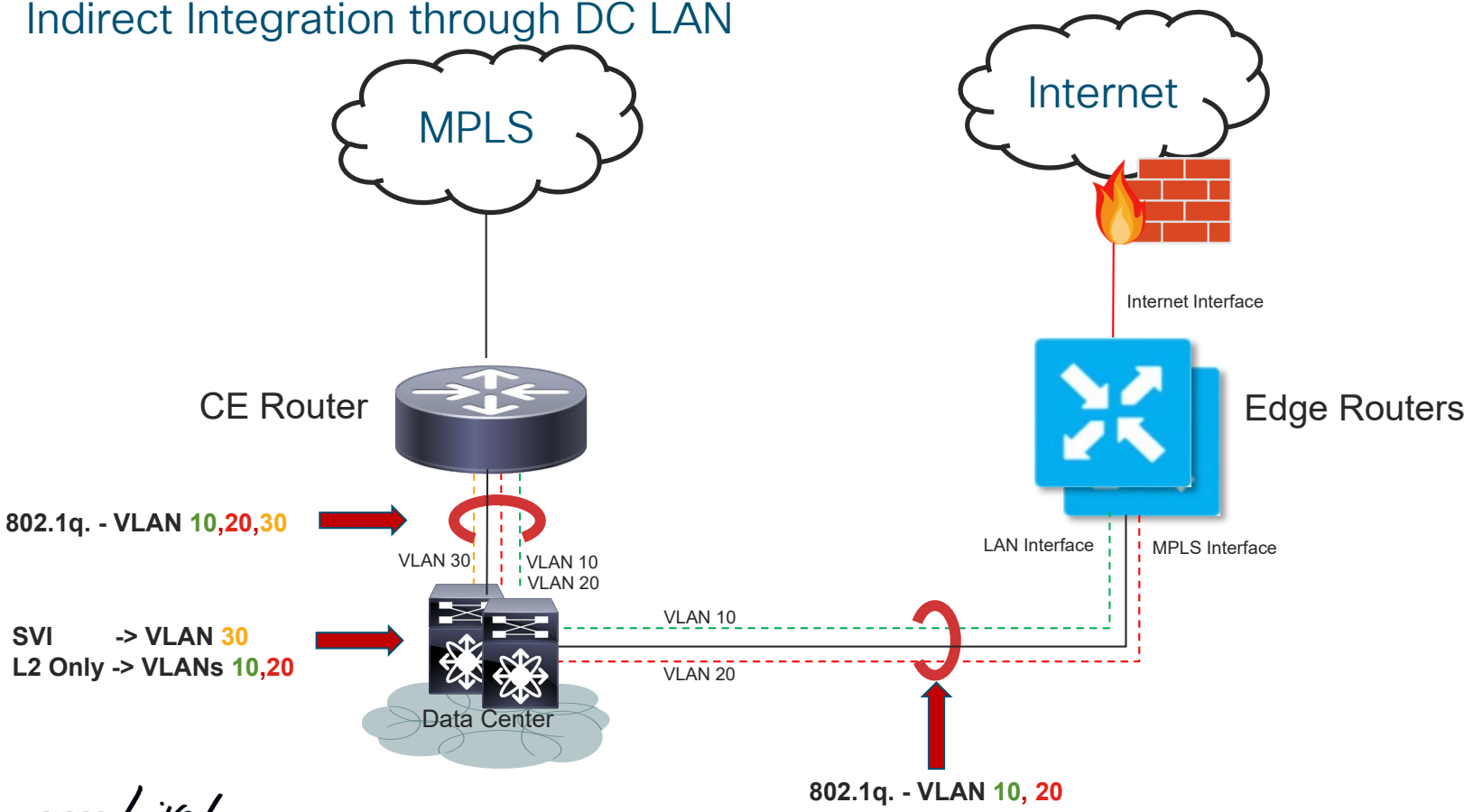
Layer 3 Integration with CE Router

Traffic Flow



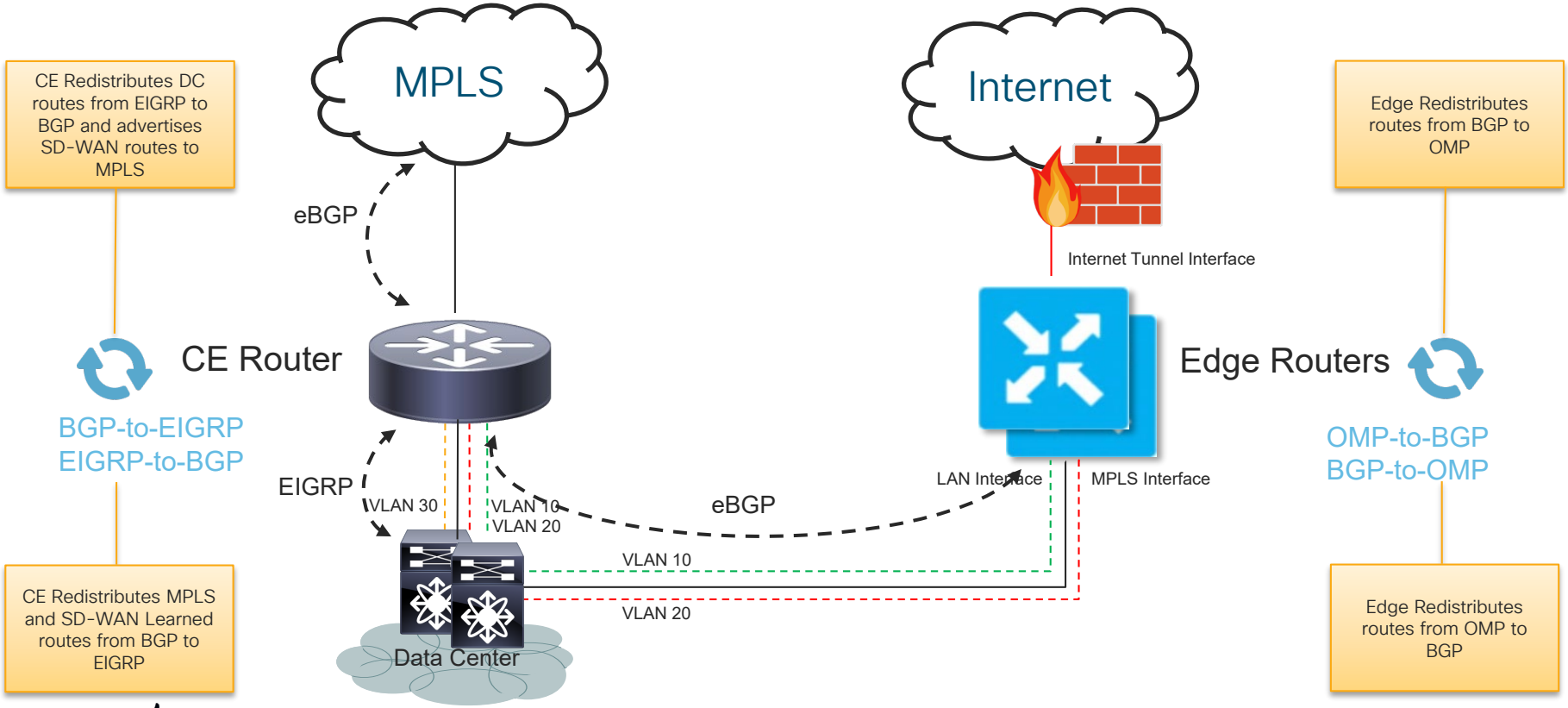
Layer 3 Integration with CE Router

Indirect Integration through DC LAN



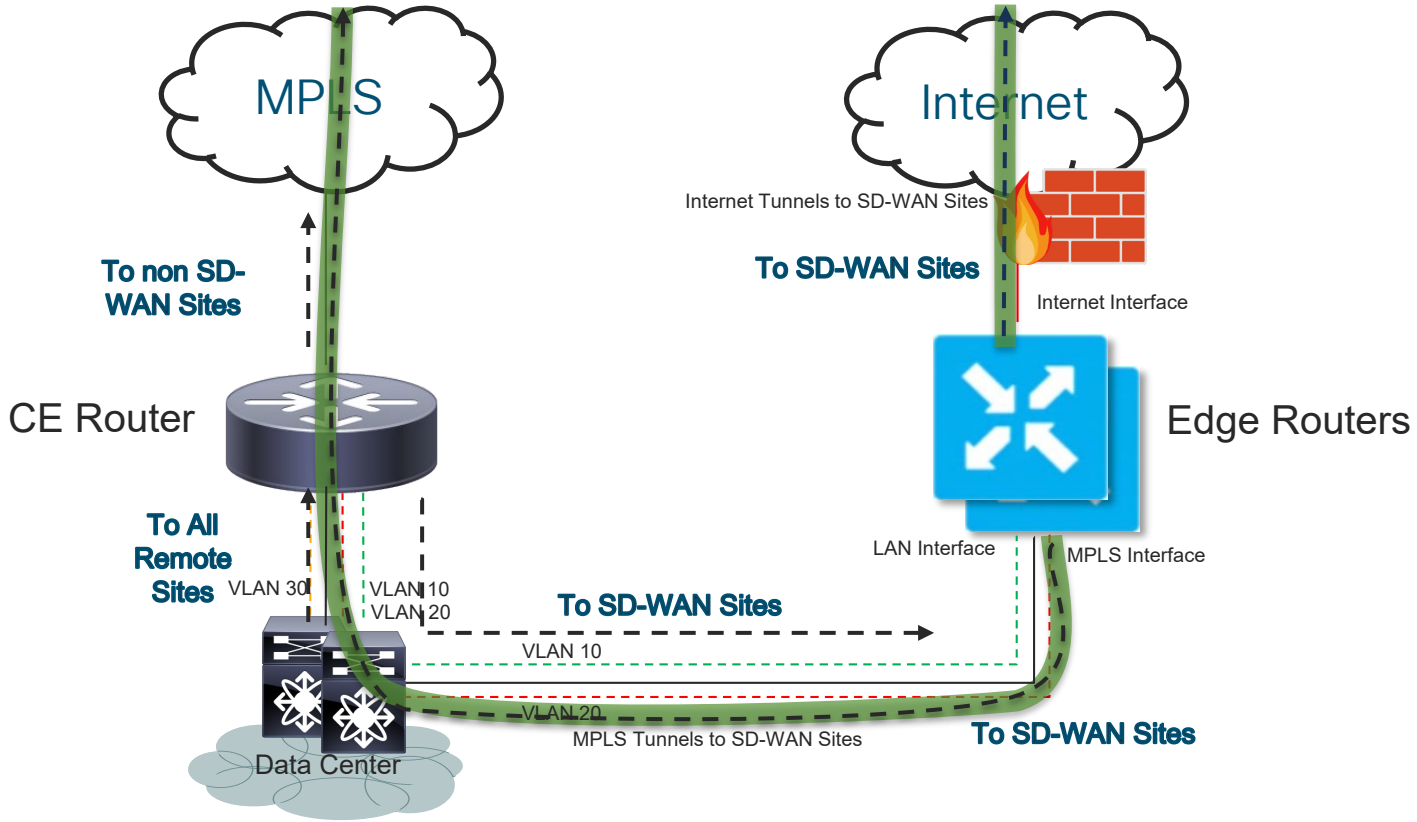
Layer 3 Integration with CE Router

Routing

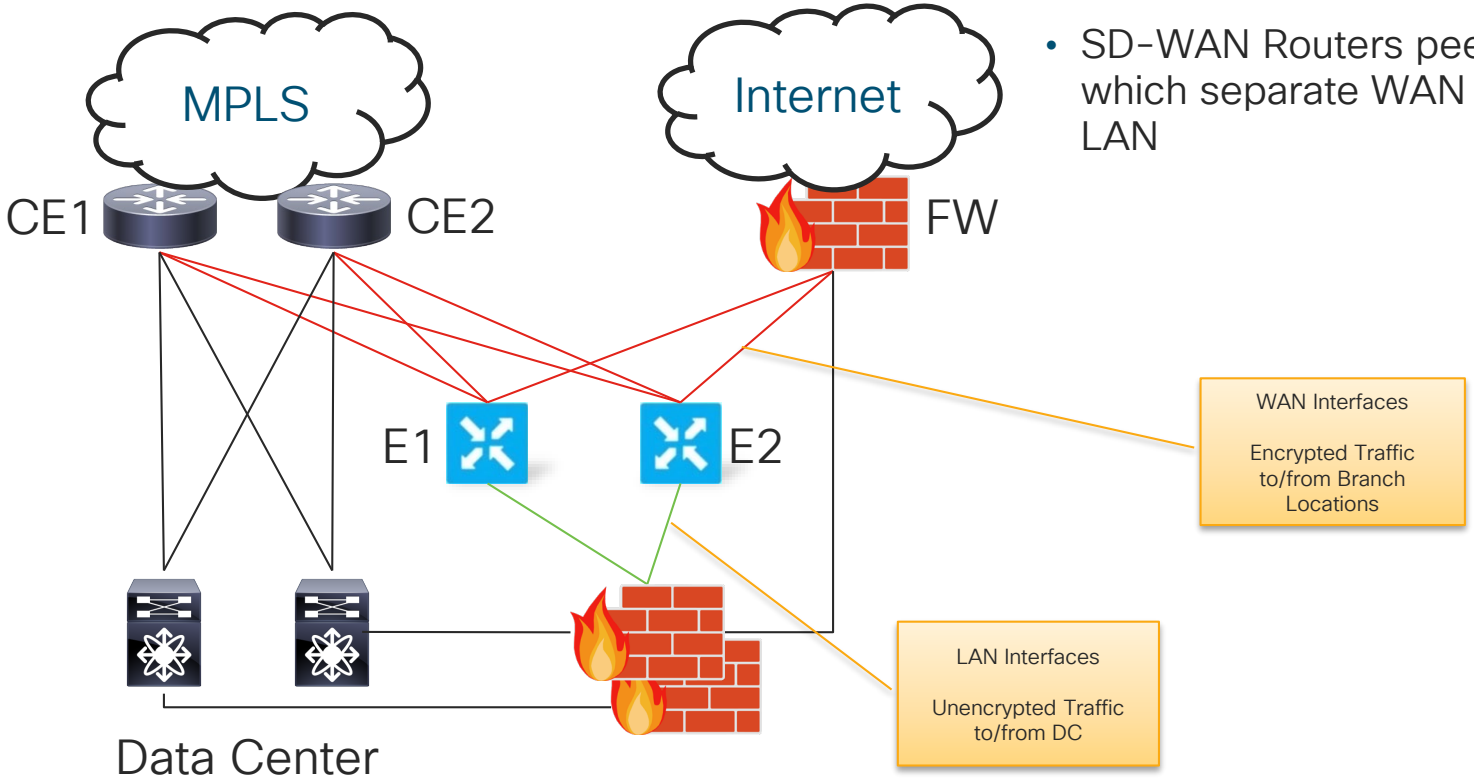


Layer 3 Integration with CE Router

Traffic Flow



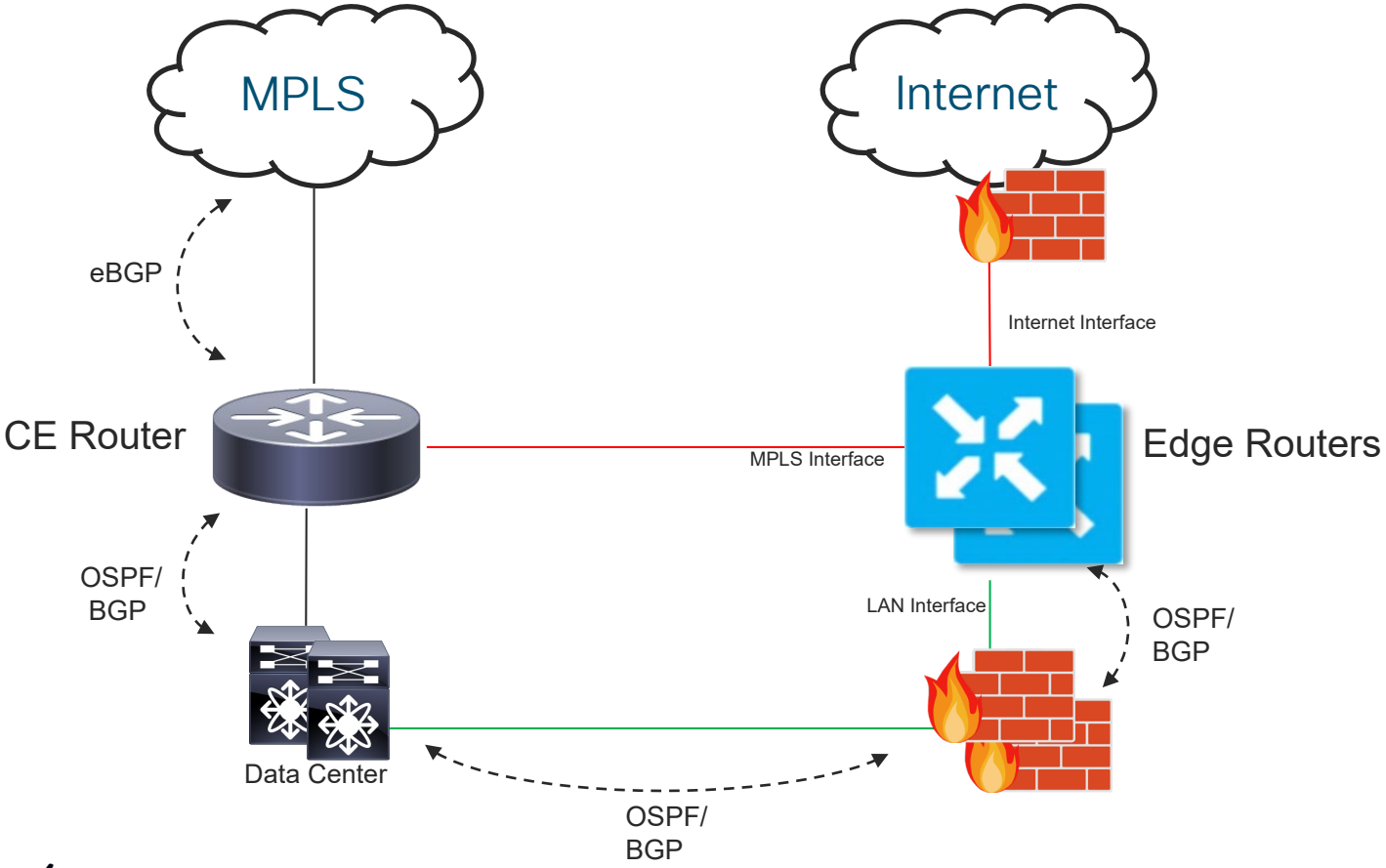
Layer 3 to Data Center Firewalls



- SD-WAN Routers peer with Firewalls which separate WAN from Data Center LAN

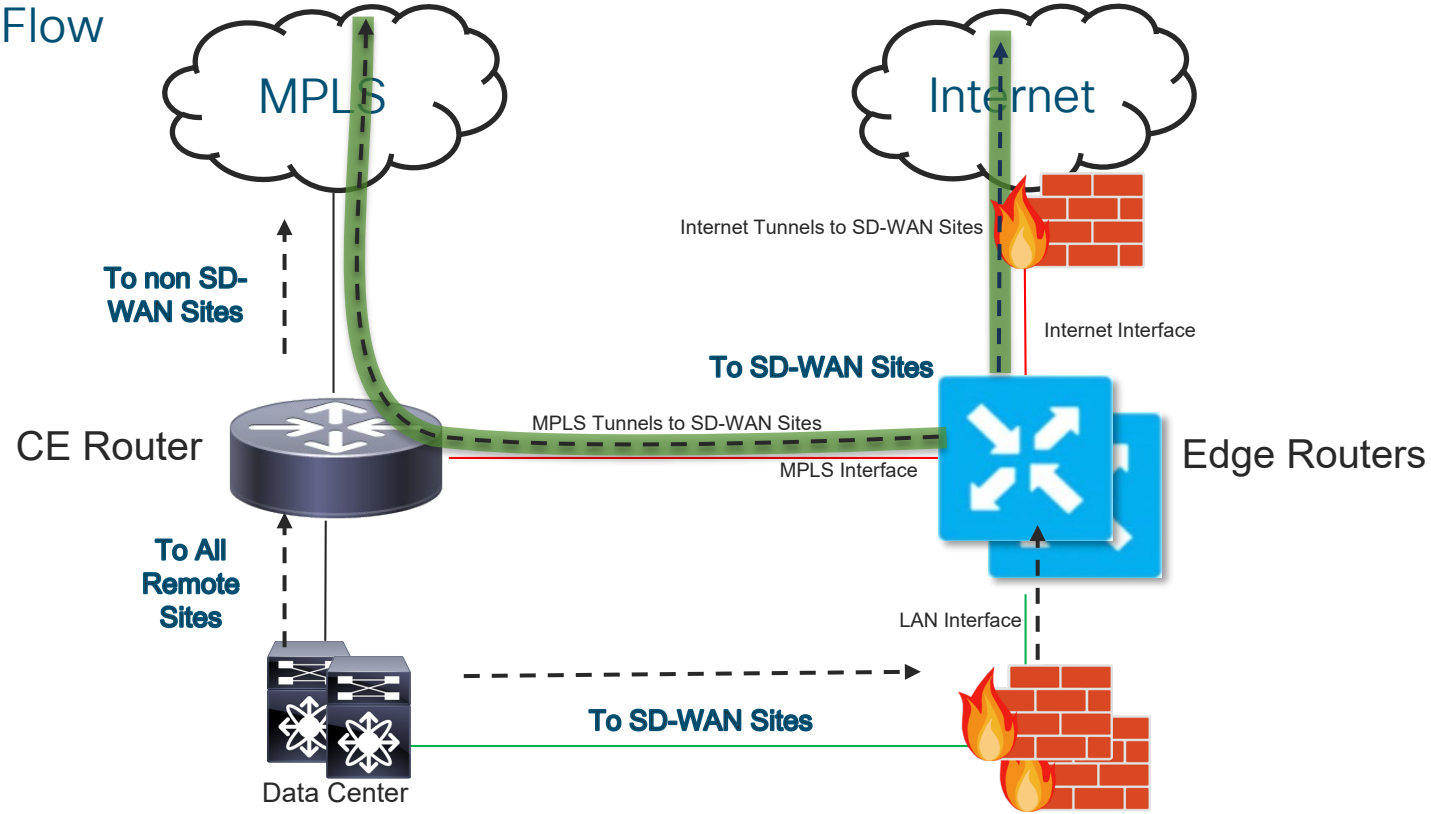
Layer 3 to Data Center Firewalls

Routing



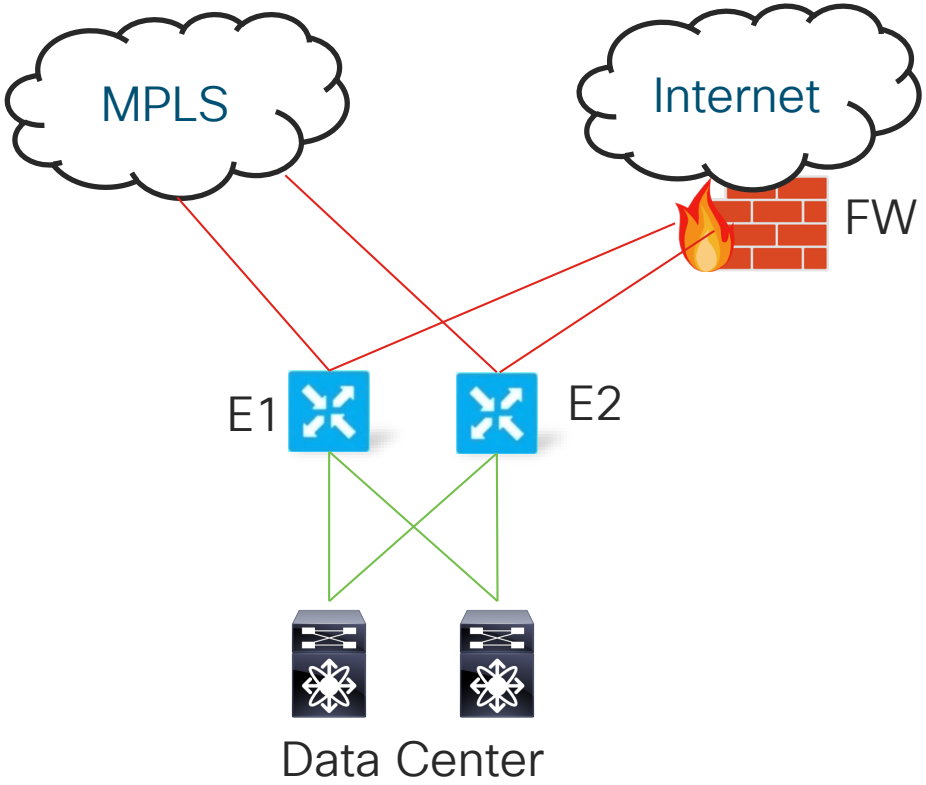
Layer 3 to Data Center Firewalls

Traffic Flow



Complete CE Replacement in the DC – End State

Overview



- Not recommended unless all sites are SD-WAN sites.
- Adds a little complexity but removes extra CE hardware and reduces cost in the DC.
- Need to allow advertisement of the controller IPs and/or the default route to the MPLS carrier. This is only necessary if control connections for branch sites needs to traverse the DC for private transports. Might require extending VPN0 to DC core depending on environment.

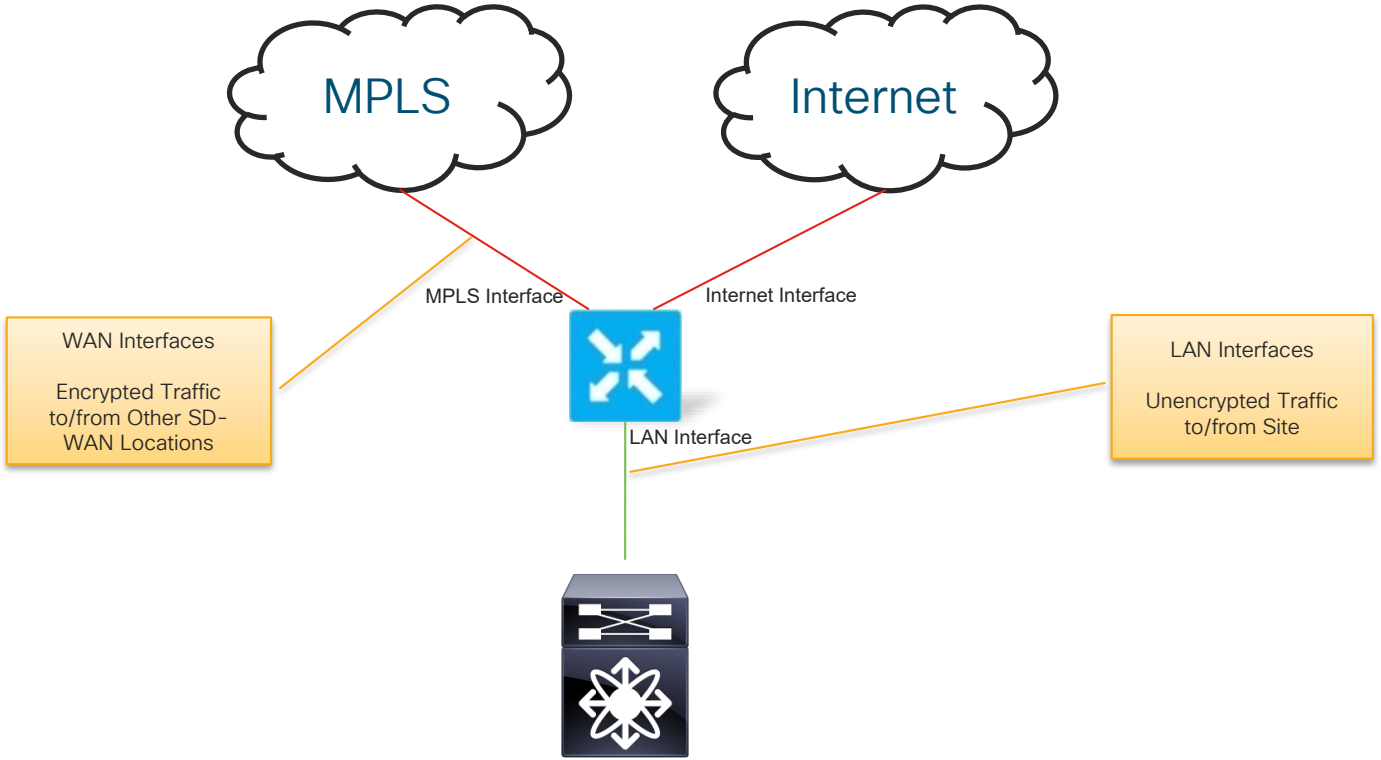
Branch Design

Branch Design Principles

- Keep it simple
- Integrate routing with the LAN Core if possible
- Integrate routing with CE when necessary
- Voice and Security services need to be taken into account

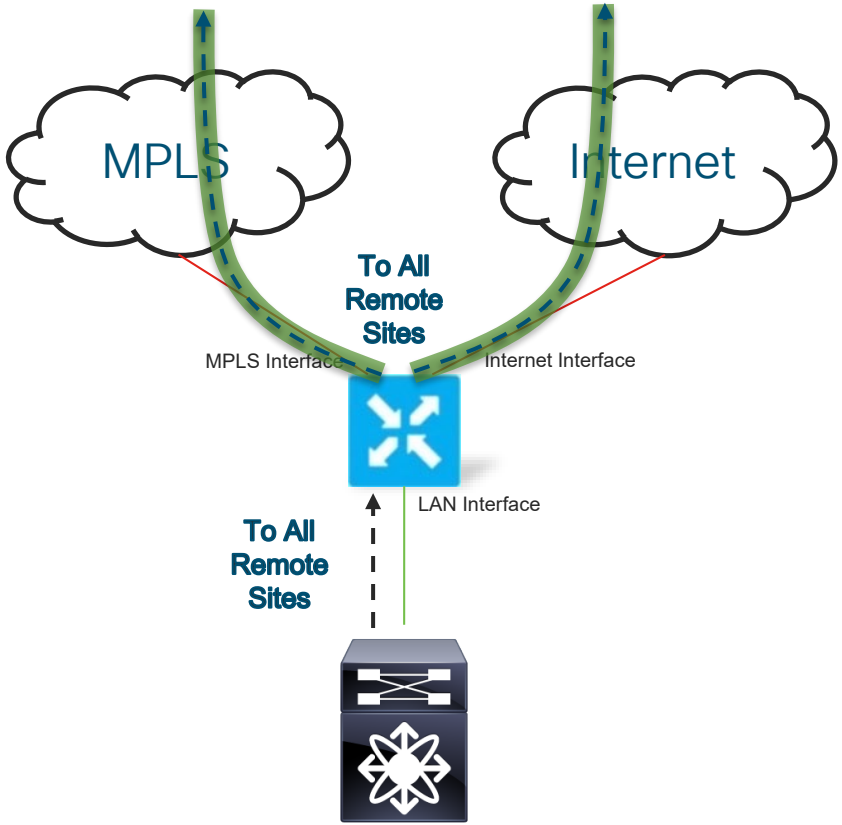
Complete CE Replacement

Single Edge



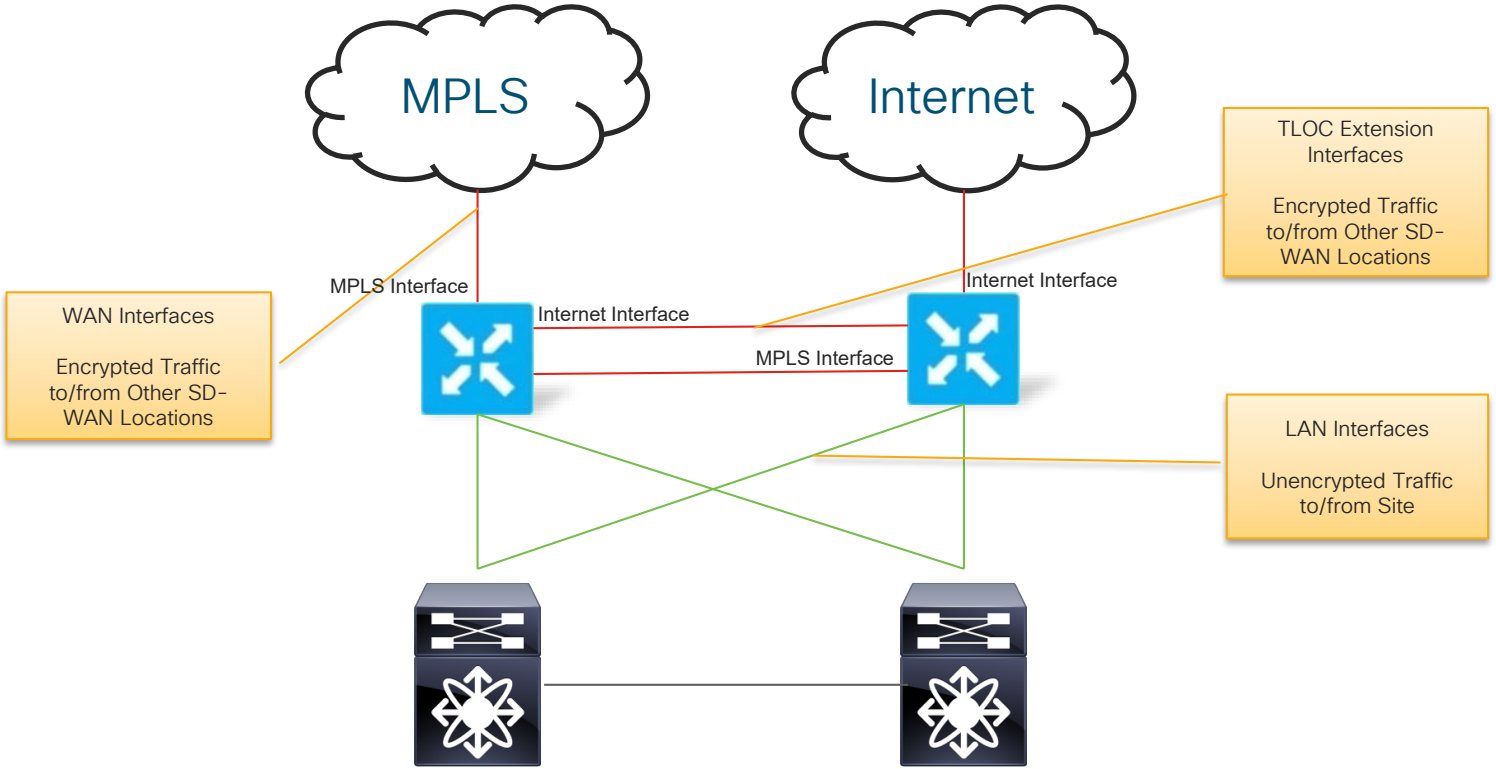
Complete CE Replacement

Single Edge



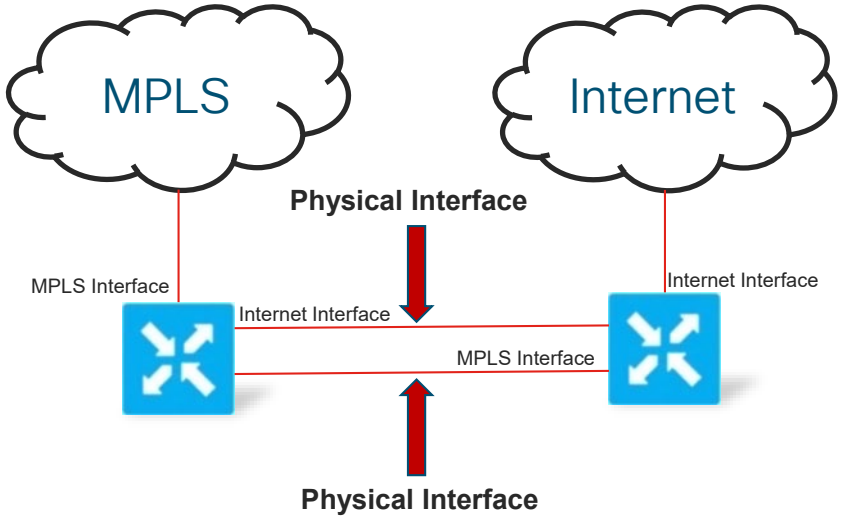
Complete CE Replacement

Dual Edge with TLOC Extension



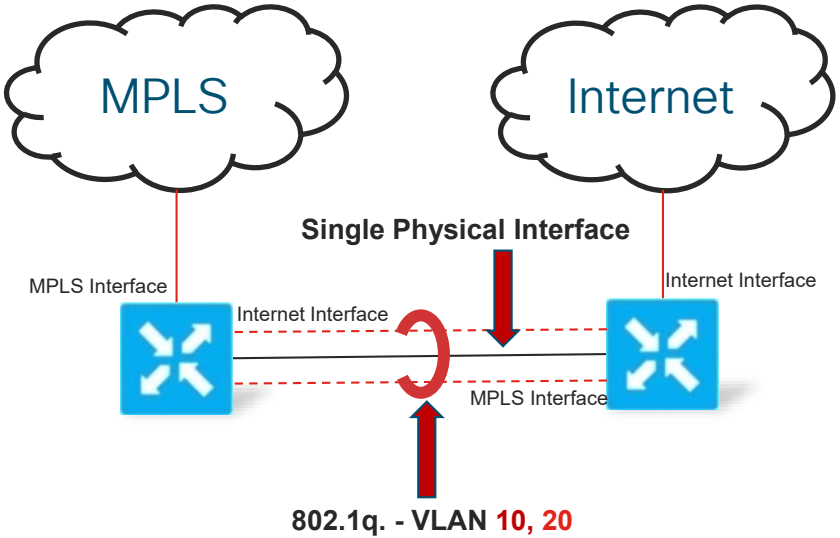
TLOC Interconnect

Separate Physical Links



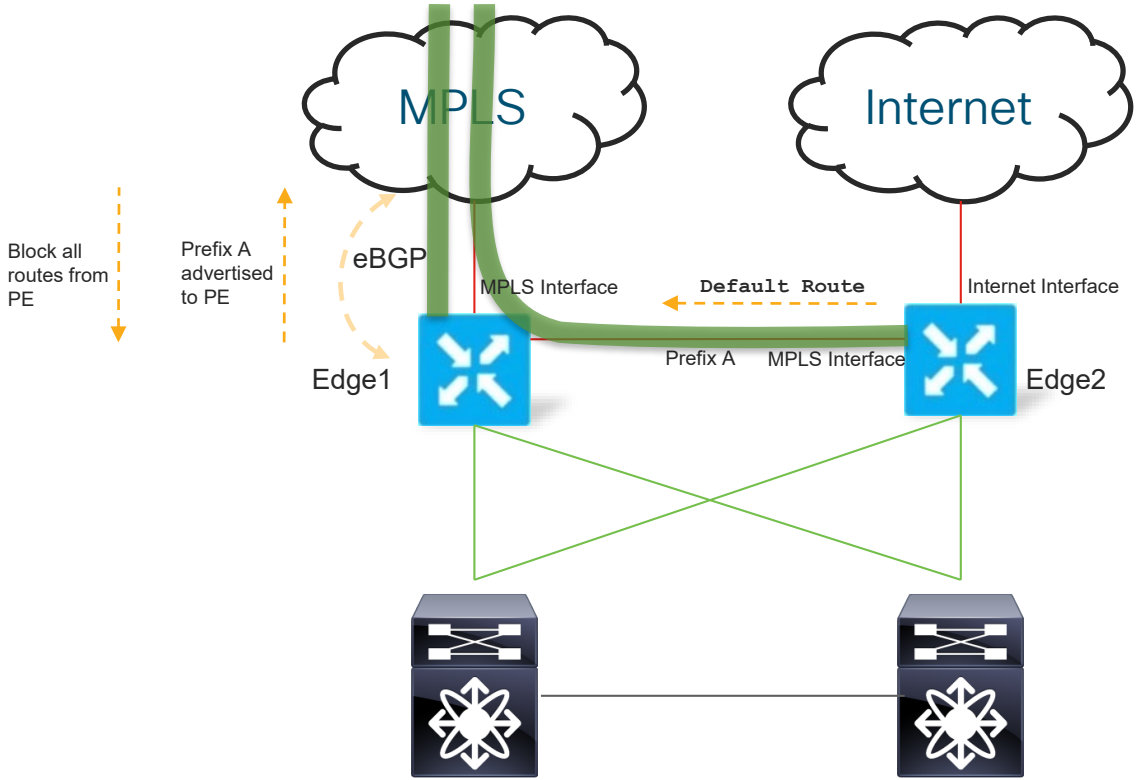
TLOC Interconnect

Single Physical Link



Complete CE Replacement

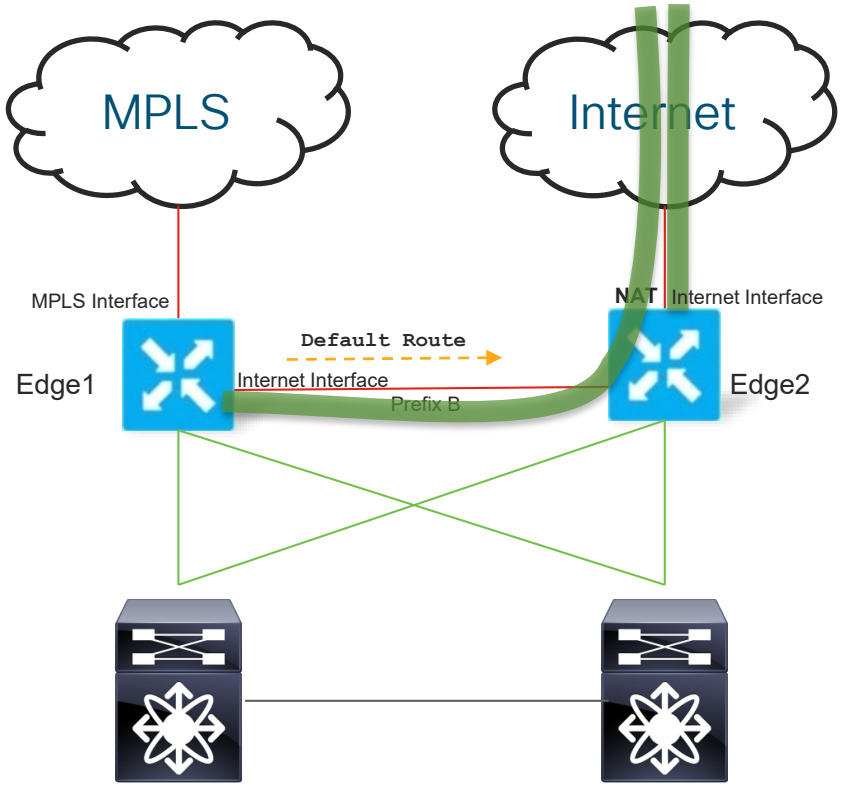
TLOC Extension – MPLS



- Dynamic routing in VPN0 (Transport VPN) is necessary in this design on the MPLS side only. Prefix A between Edges needs to be advertised to MPLS Carrier to allow tunnels to form with the MPLS interface on Edge2
- Note: Edge1 doesn't need to learn any BGP routes from the MPLS PE. It simply needs to advertise Prefix A from Edge2 to the MPLS Underlay. Edge1 will simply use a static default to the PE to build tunnels.
- Edge2 can now route through Edge1 to build tunnels across the MPLS transport from its MPLS interface

Complete CE Replacement

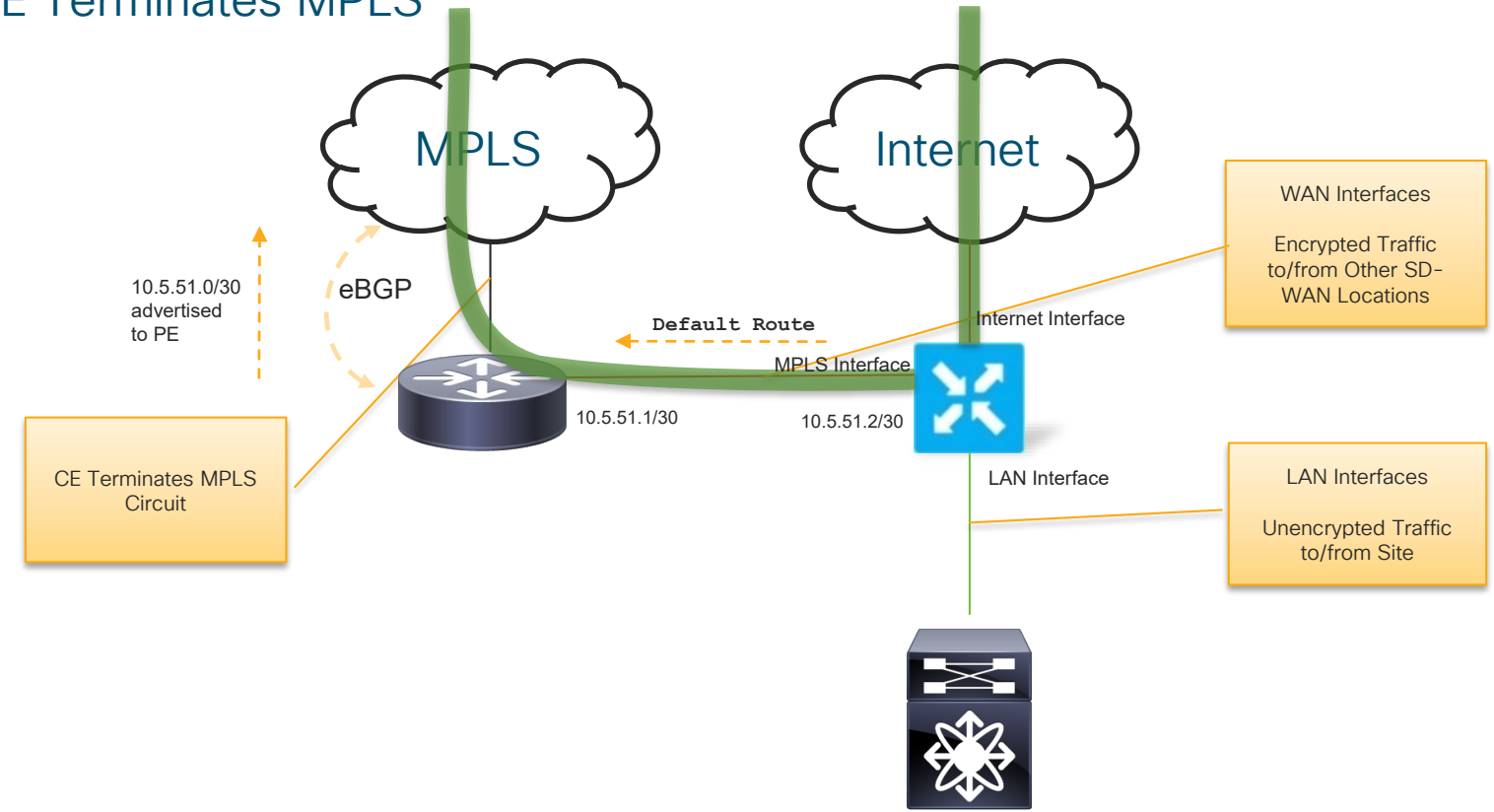
TLOC Extension – Internet



- Edge2 uses NAT on its Internet facing interface to allow the Internet interface from Edge1 to build tunnels across the Internet path.
- Edge1 has a static default route pointing to Edge2 from its Internet Interface
- Edge1 can now route through Edge2 to build tunnels across the Internet transport from its Internet interface

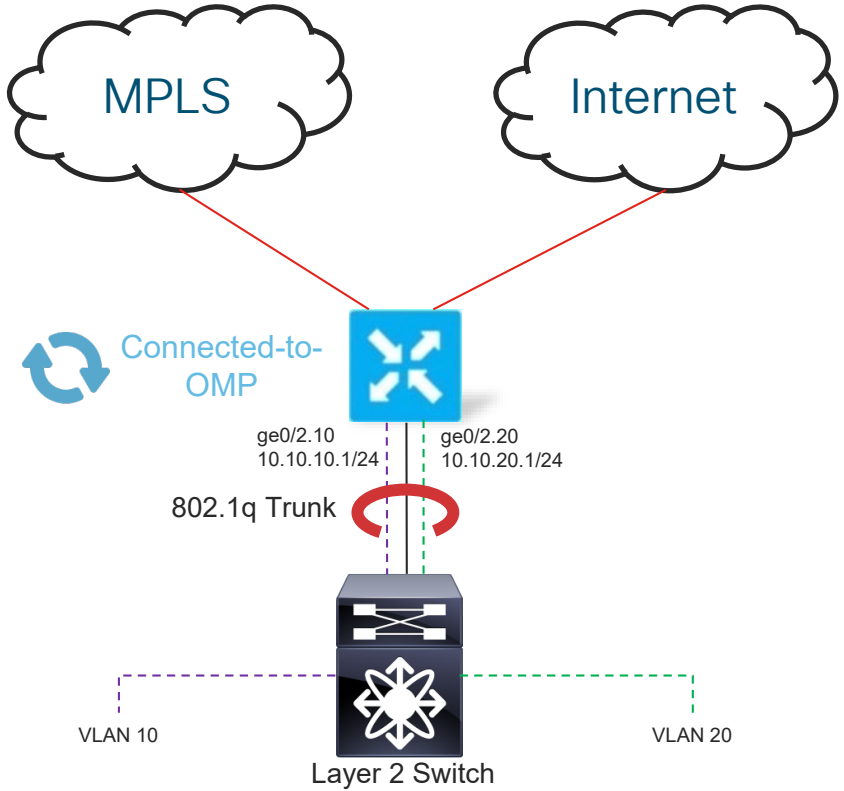
Integration with CE

CE Terminates MPLS



Complete CE Replacement

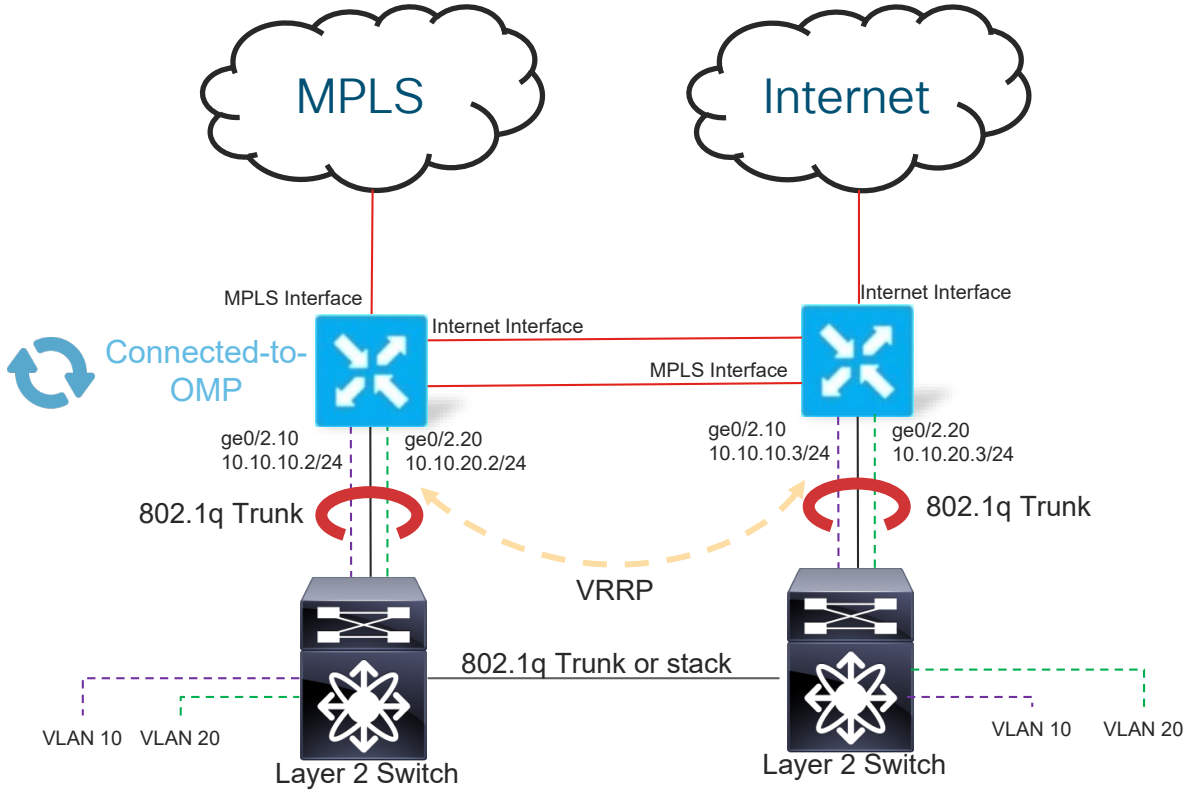
Single Edge – VPN1 Detail L2 LAN



- Site Prefixes are learned via Connected, or Static Routes.
- Site Prefixes are advertised via OMP to controllers.
- Edge is the gateway for each VLAN at the site
- NOTE* Recommend Native VLAN not be same as user VLAN.

Complete CE Replacement

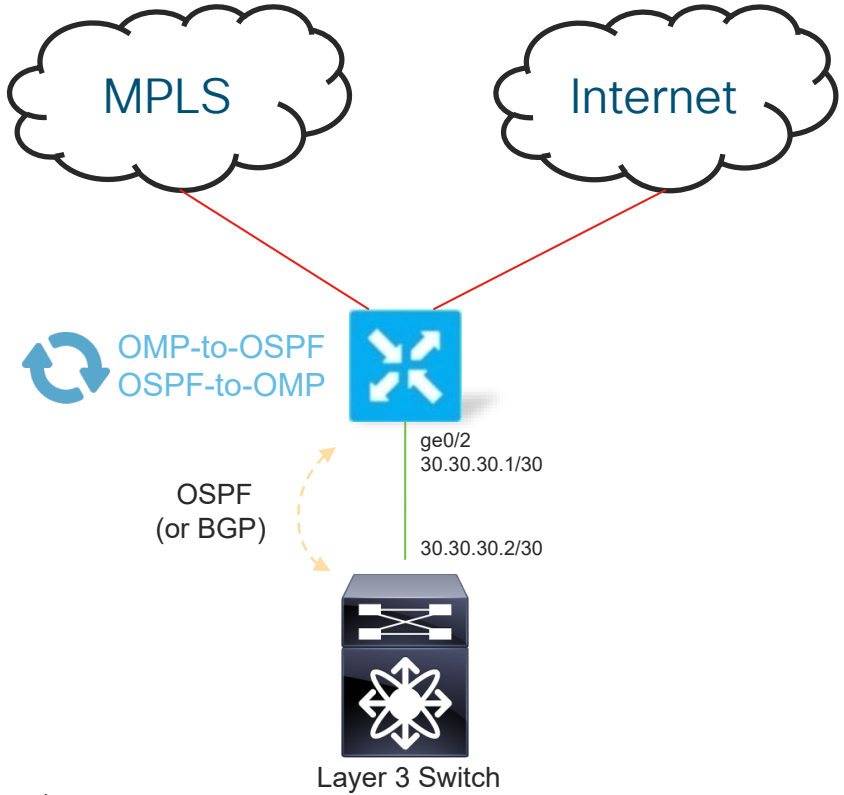
Dual Edge – VPN1 Detail L2 LAN



- Site Prefixes are learned via Connected, or Static Routes.
- Site Prefixes are advertised via OMP to controllers.
- One Edge is the gateway for all VLANs at the site using VRRP priority (LAN) and OMP preference (WAN).

Complete CE Replacement

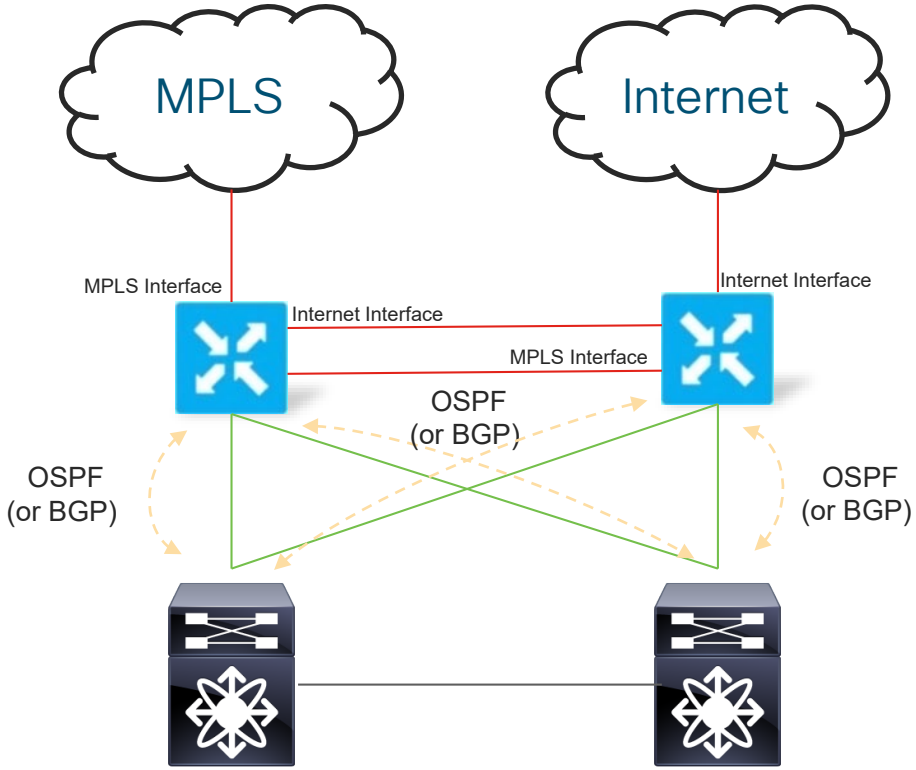
Single Edge – VPN1 Detail L3 LAN



- Site Prefixes are learned via OSPF, BGP, Connected, or Static Routes.
- Site Prefixes are advertised via OMP to controllers.
- Overlay Routes are advertised to LAN via redistribution.
- Alternatively, the Edge can originate a default route and only send the default to the LAN

Complete CE Replacement

Dual Edge – VPN1 Detail L3 LAN



- Layer 3 to each switch provides optimal HA
- One Edge is configured as the primary using routing protocol metric (LAN) and OMP preference (WAN).

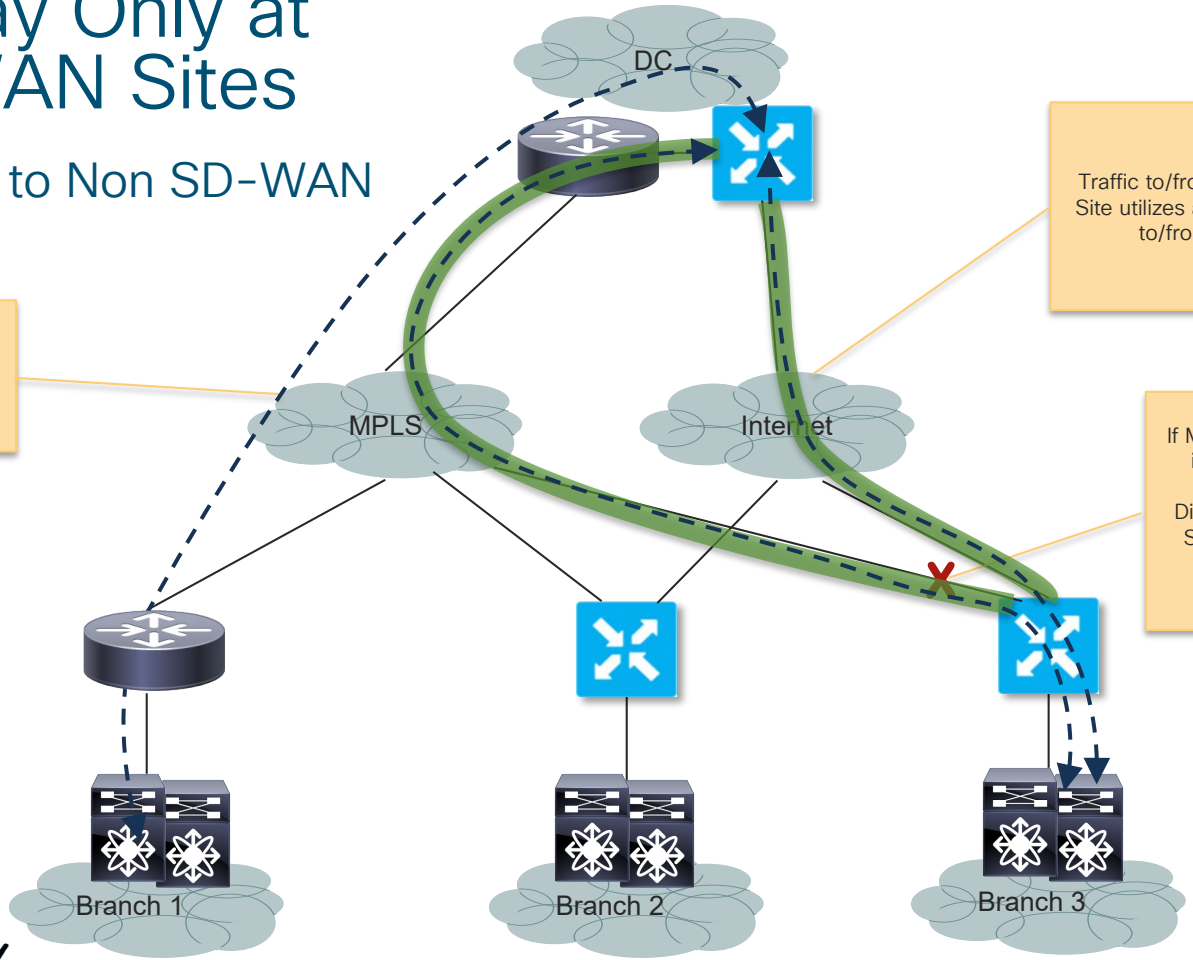
Overlay/Underlay Routing

Overlay/Underlay Routing Principles

- Keep it simple (Notice a theme yet?)
- Communication between migrated and non-migrated sites should traverse a regional hub if possible
- Very similar process to migrating from one MPLS carrier to another
- Don't forget that voice has a 300ms round trip latency budget before the human ear can detect delay.
- Routing between migrated and non-migrated sites is possible but does add complexity
- All concepts discussed in the upcoming slides apply to migration from IWAN as well.

Overlay Only at SD-WAN Sites

SD-WAN to Non SD-WAN Site Flow



Legacy Site Traverses Regional DC over MPLS to reach SD-WAN Site

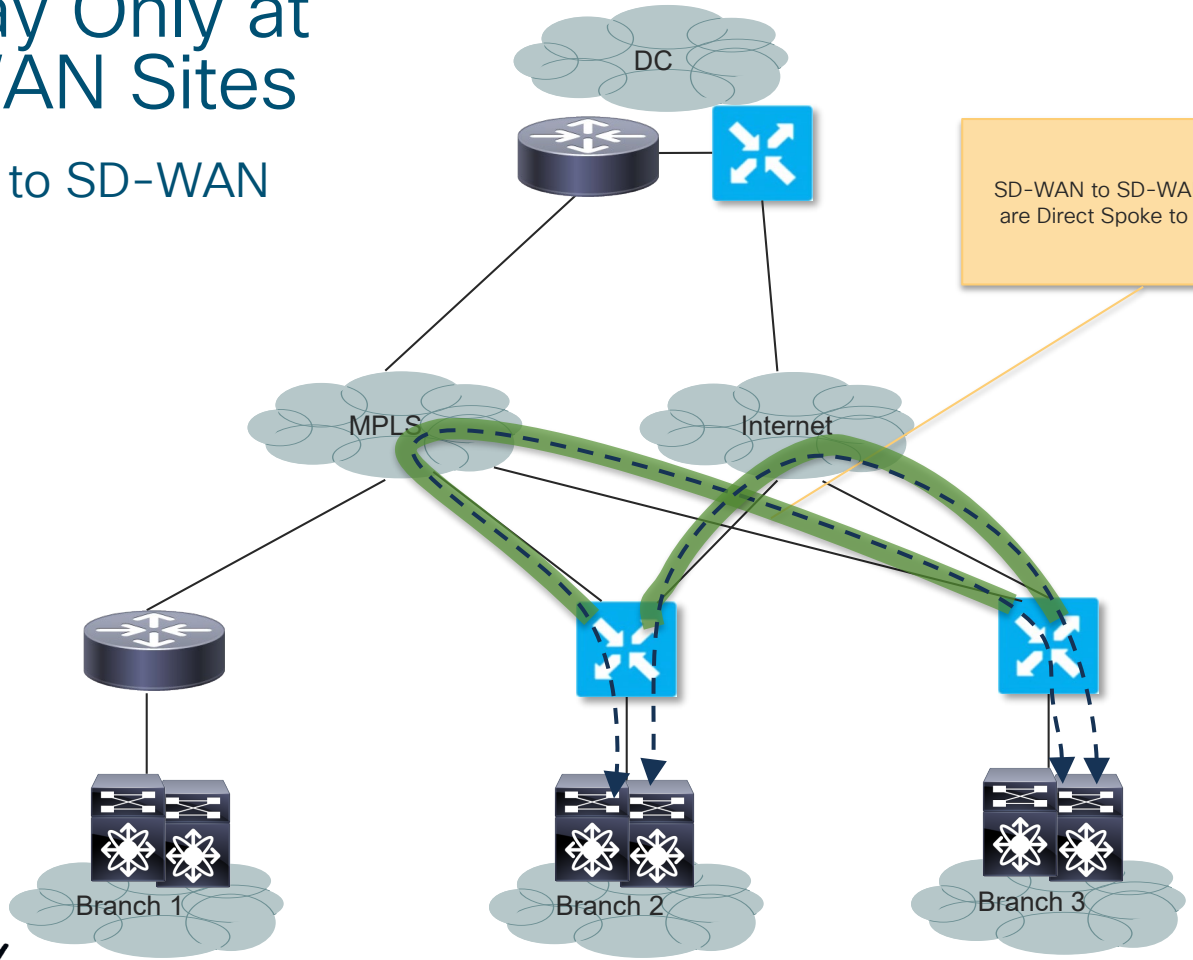
Traffic to/from SD-WAN Site utilizes all transports to/from DC.

If MPLS at Branch3 has issues, traffic is protected to DC over Internet.

Direct Site-to-Site Design Between SD-WAN and Non SD-WAN sites over MPLS would not have this protection

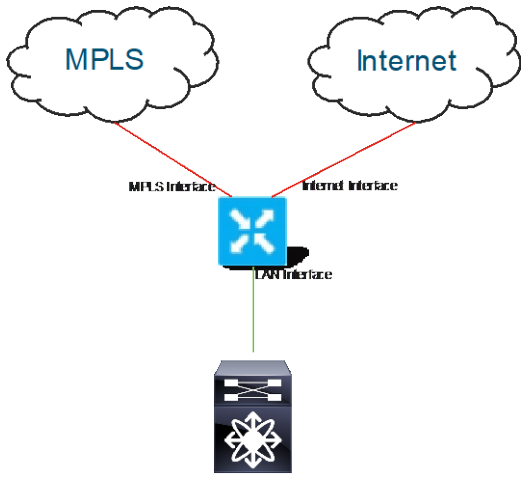
Overlay Only at SD-WAN Sites

SD-WAN to SD-WAN Site Flow

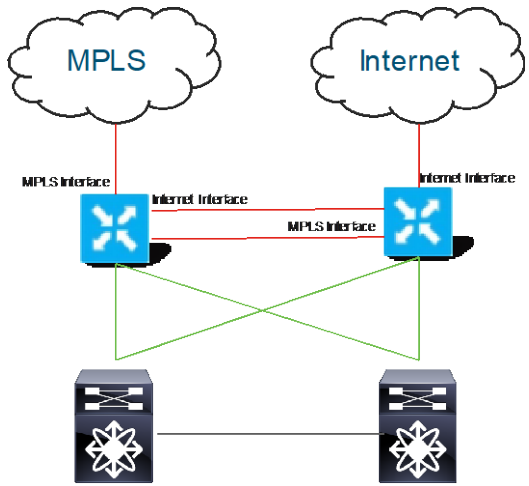


Common Overlay Only Site Designs

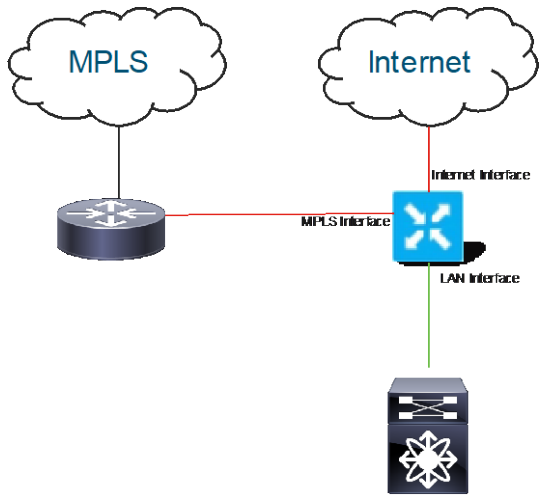
Single Edge



Dual Edge

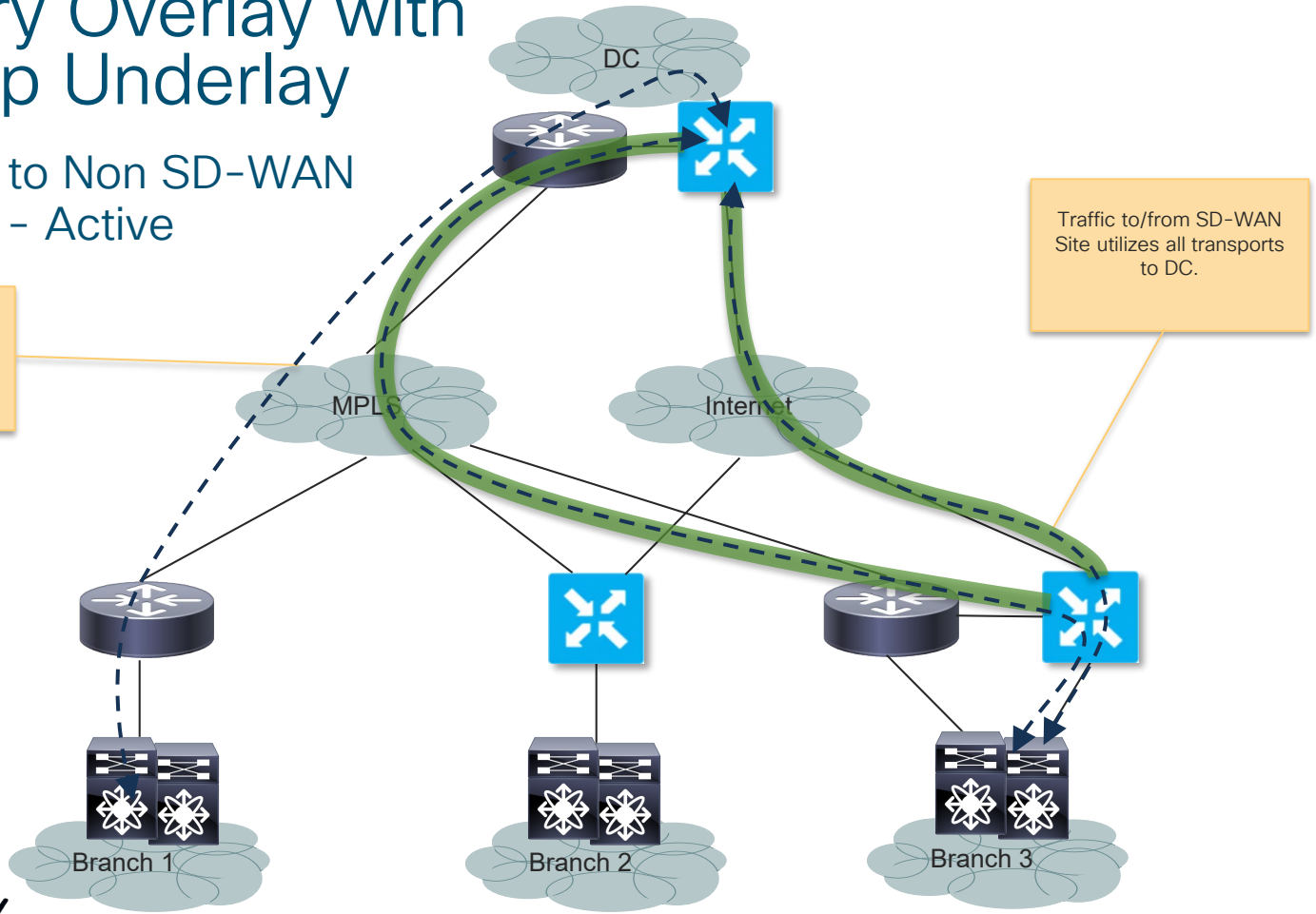


Edge + CE



Primary Overlay with Backup Underlay

SD-WAN to Non SD-WAN Site Flow - Active

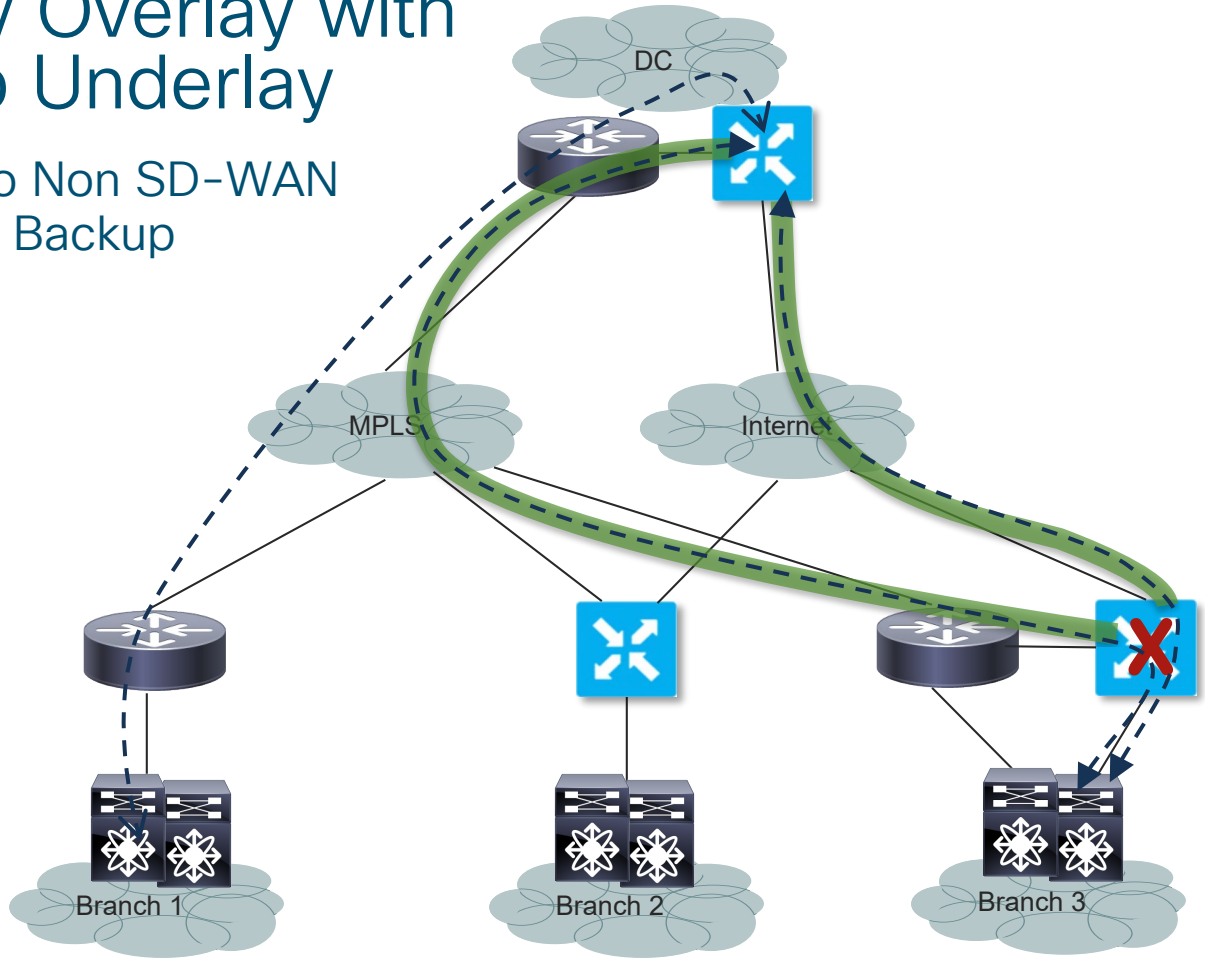


Legacy Site Traverses Regional DC over MPLS to reach SD-WAN Site

Traffic to/from SD-WAN Site utilizes all transports to DC.

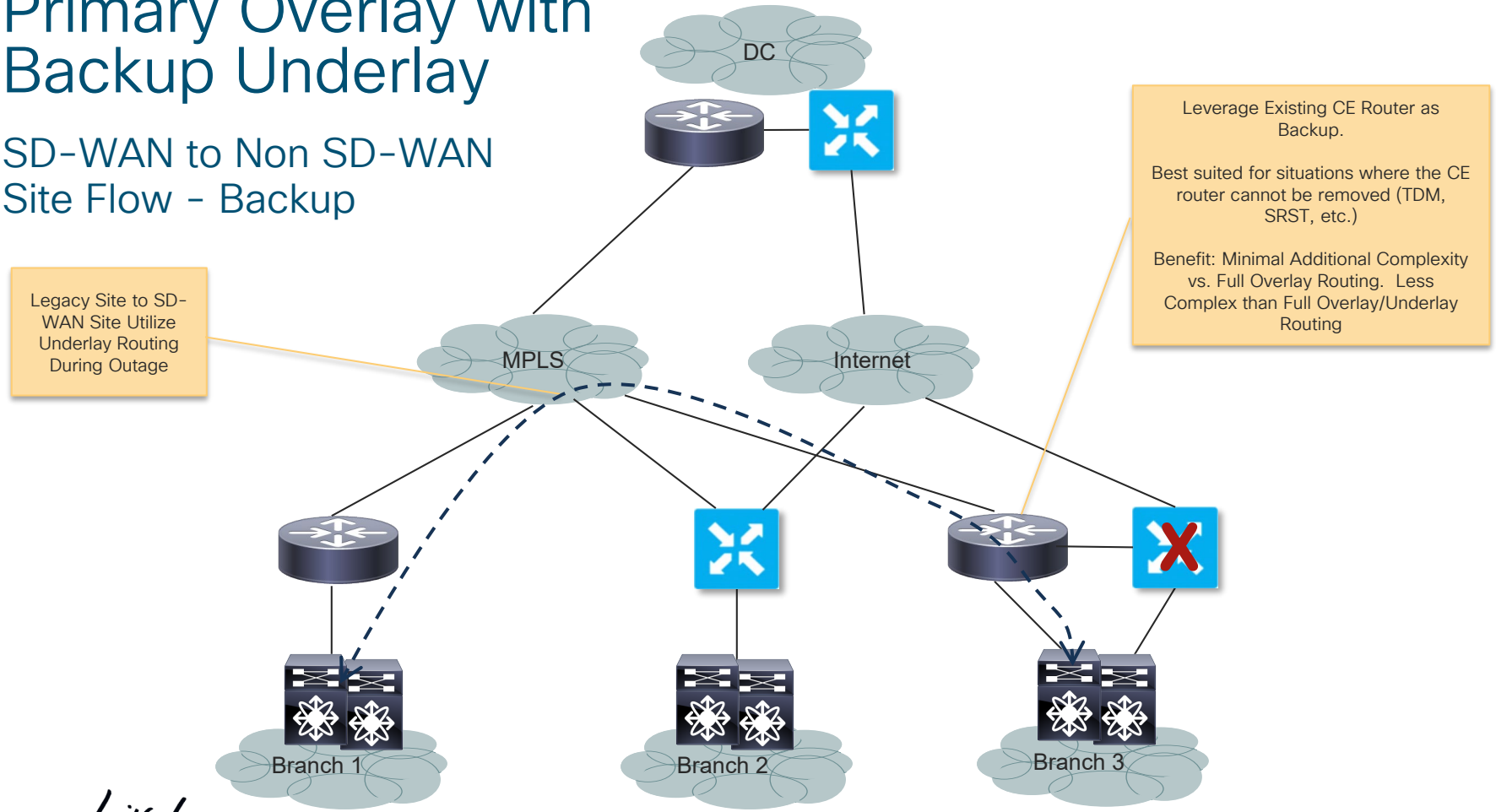
Primary Overlay with Backup Underlay

SD-WAN to Non SD-WAN Site Flow - Backup



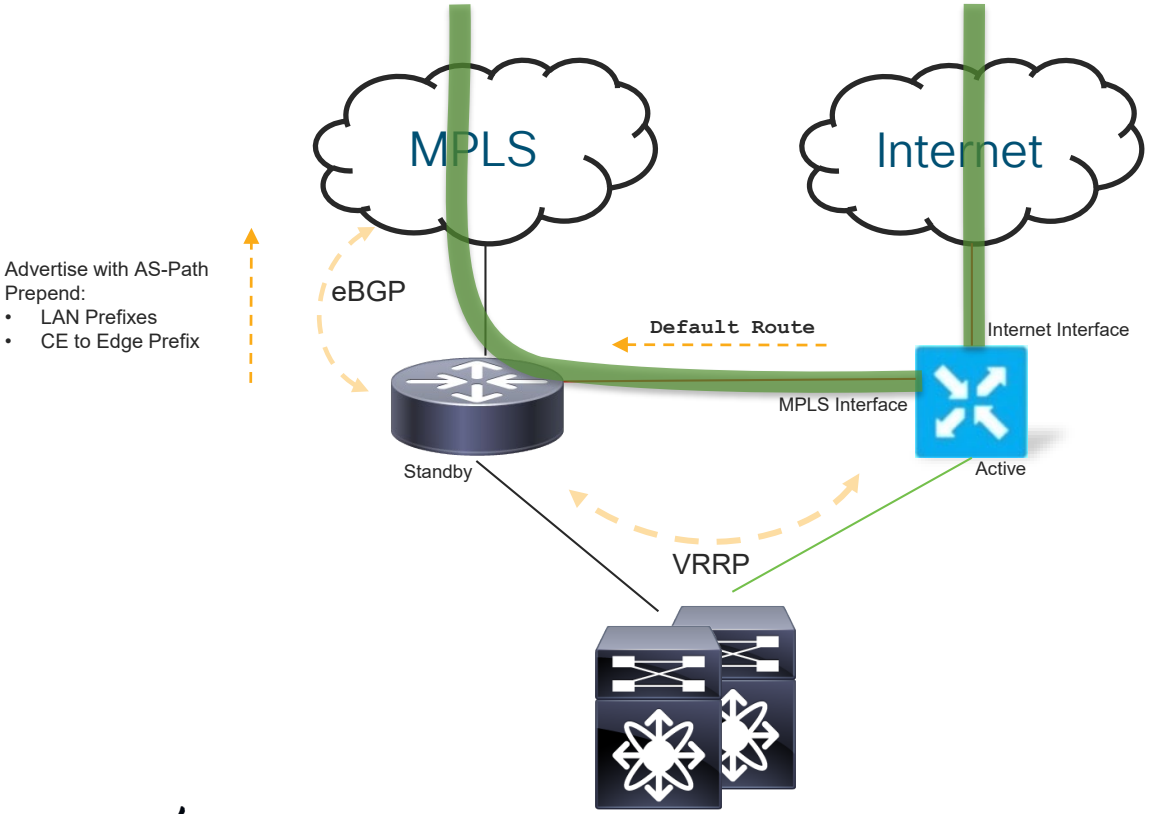
Primary Overlay with Backup Underlay

SD-WAN to Non SD-WAN Site Flow - Backup



Overlay/Underlay Routing

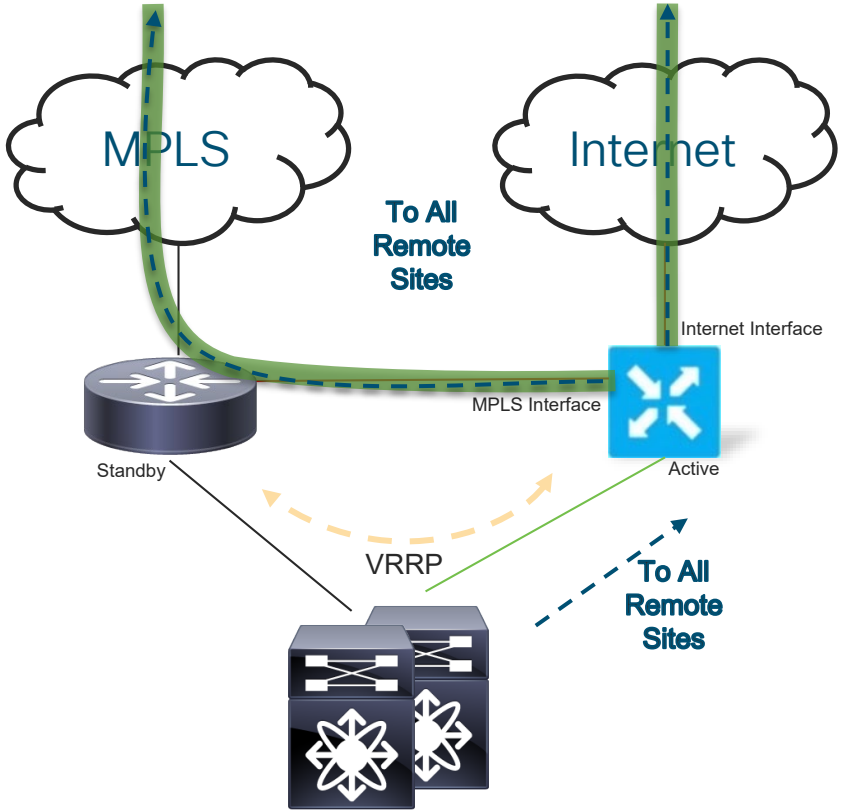
CE Backup with L2 LAN



- CE advertises local site and CE to Edge prefixes to MPLS PE with AS-Path Prepend
- DC advertises site prefixes from overlay to underlay. Remote sites not on SD-WAN prefer DC path to site due to AS Prepend at branch
- Edge is Active VRRP. CE is Standby

Overlay/Underlay Routing

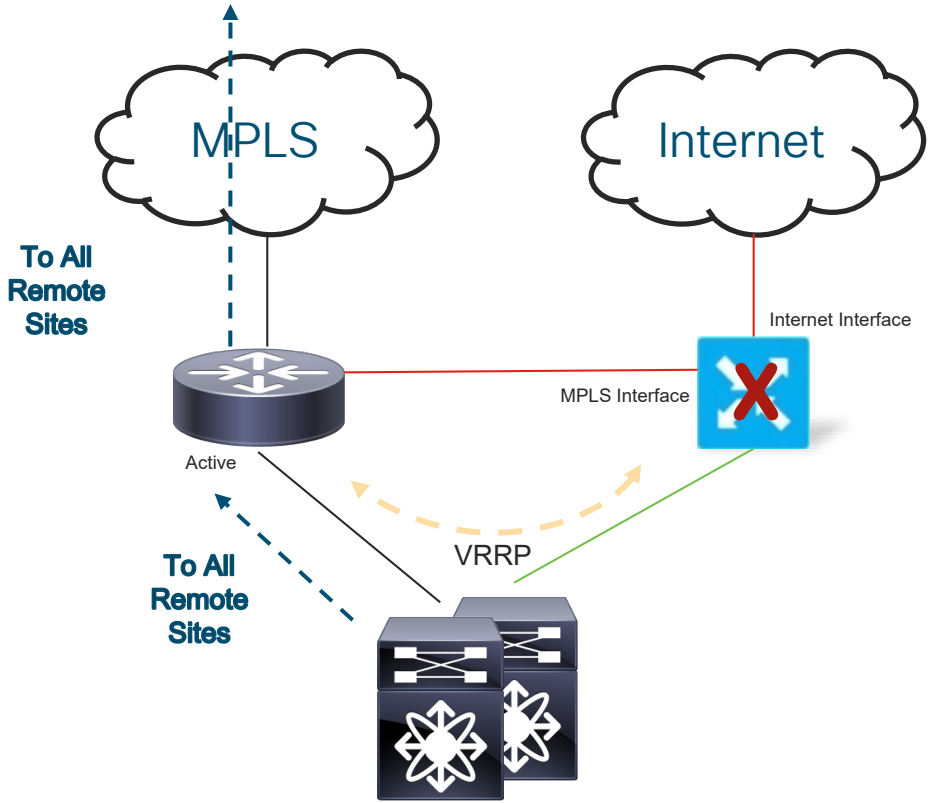
CE Backup with L2 LAN



- Traffic to/from site prefers overlay
- Non SD-WAN sites route to SD-WAN site through regional DC since site prefixes have lower AS Path Count.

Overlay/Underlay Routing

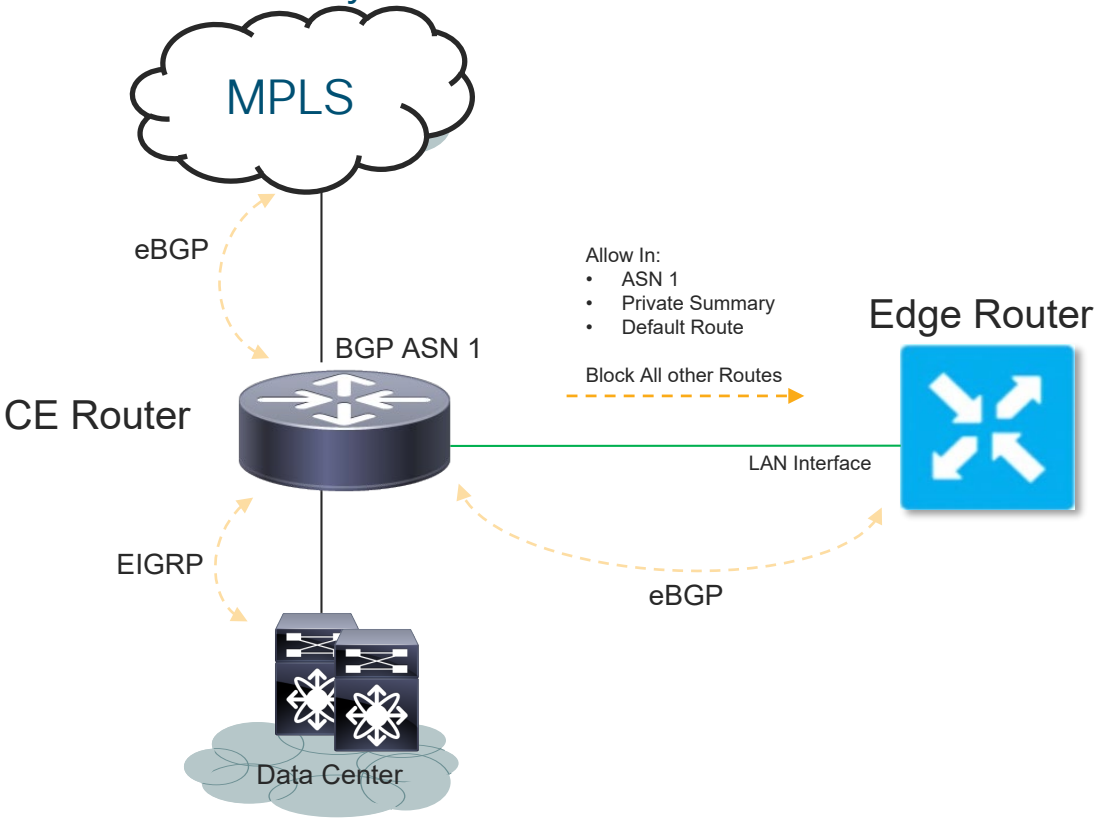
CE Backup with L2 LAN



- Edge is Active VRRP. CE is Standby
- CE advertises local site and CE to Edge prefixes to MPLS PE with AS-Path Prepend
- Traffic to/from site prefers overlay
- Non SD-WAN sites route to SD-WAN site through regional DC since site prefixes have lower AS Path Count.

Data Center Considerations

CE in Standby Mode at Branch

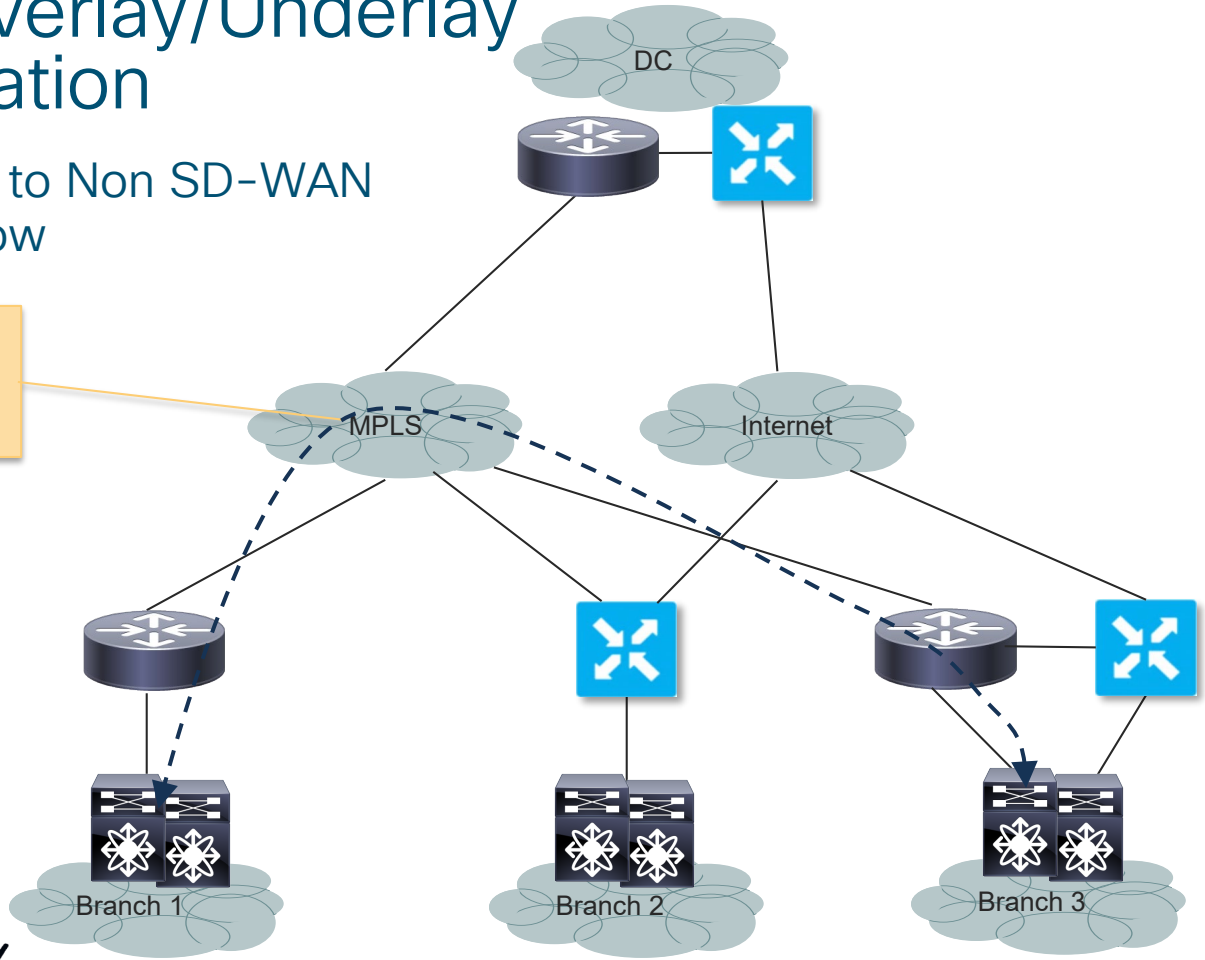


- Only allow routes which originate from Data Center BGP AS Number
- Allow default route and private summary routes
- This BGP filter inbound on the Edge keeps branch routes from being learned from underlay via BGP and overlay via OMP
- Best Practice for avoiding loops or asymmetric routing

Full Overlay/Underlay Integration

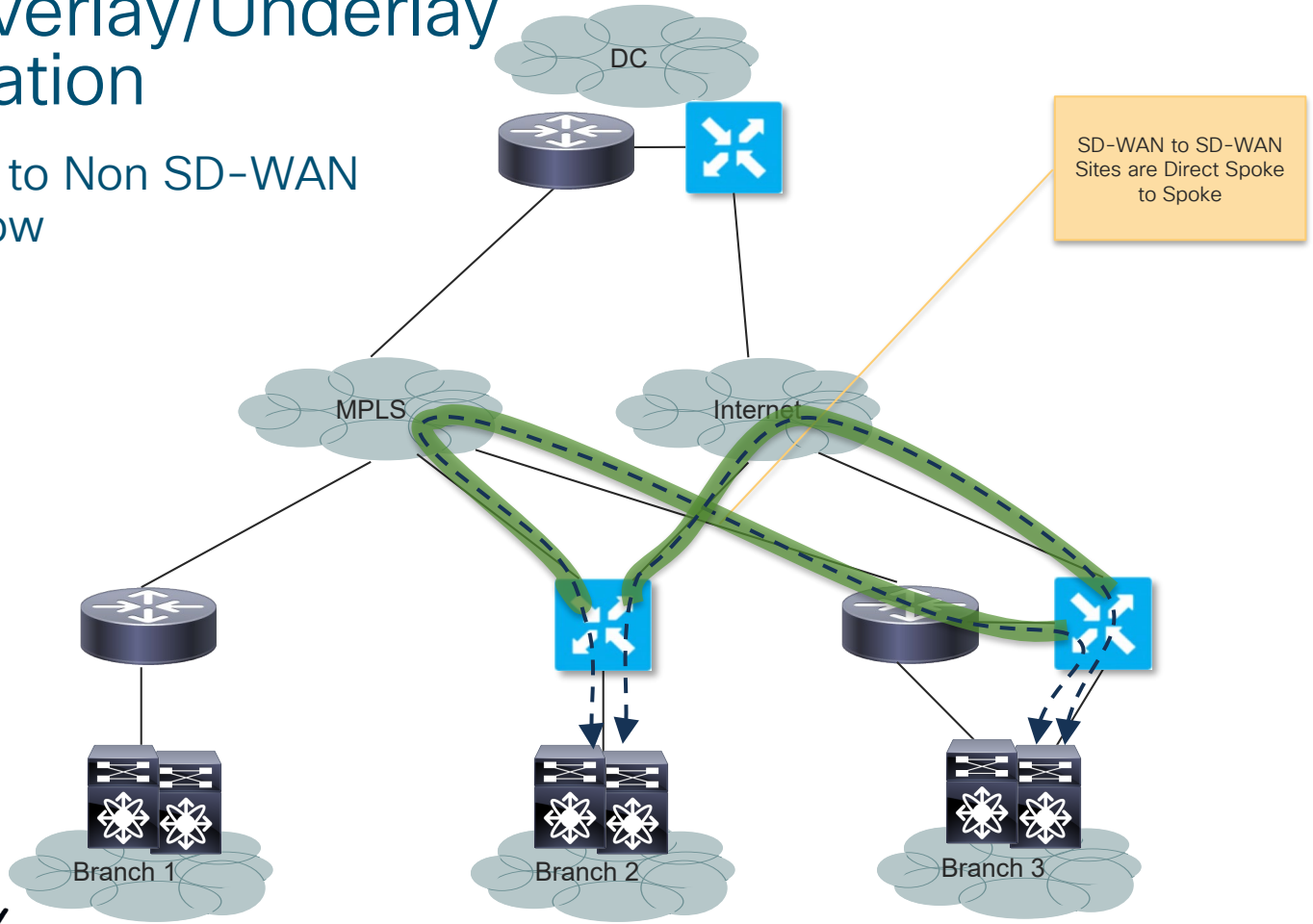
SD-WAN to Non SD-WAN Traffic Flow

Legacy Site to SD-WAN Site Utilize Underlay Routing At All Times



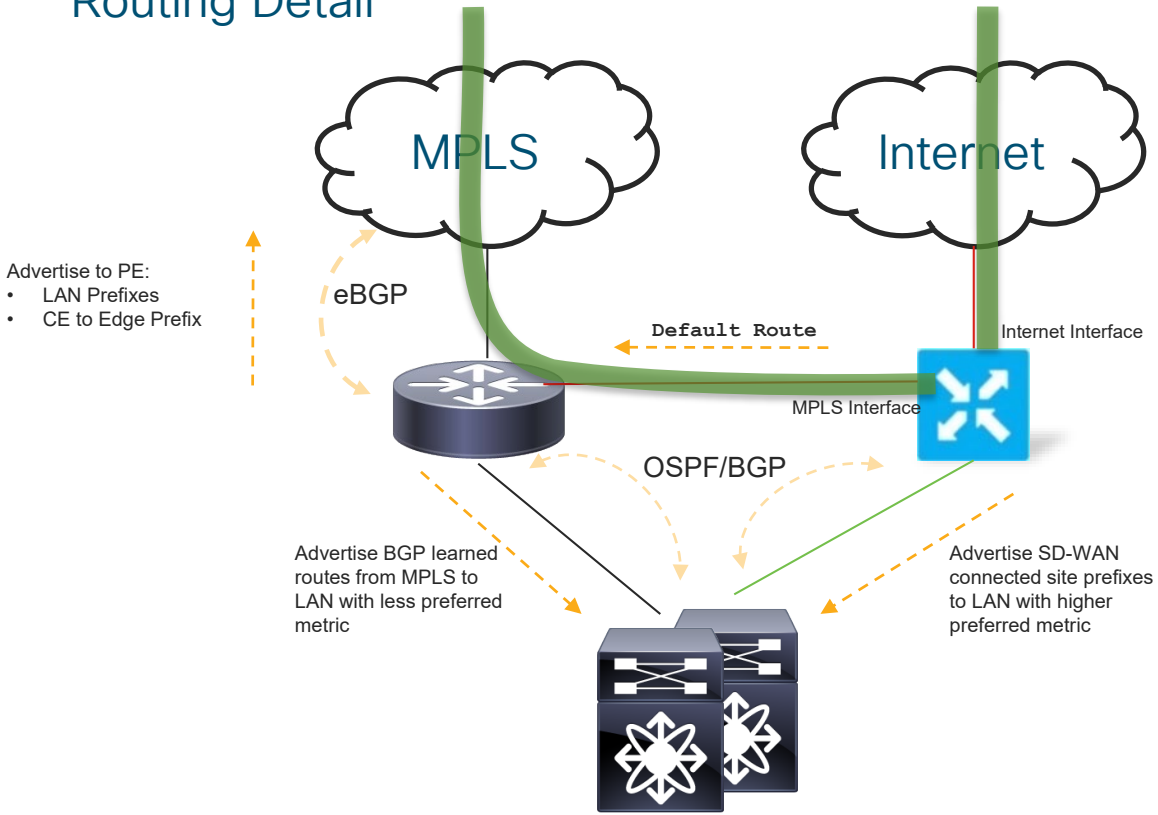
Full Overlay/Underlay Integration

SD-WAN to Non SD-WAN Traffic Flow



Full Overlay/Underlay Integration

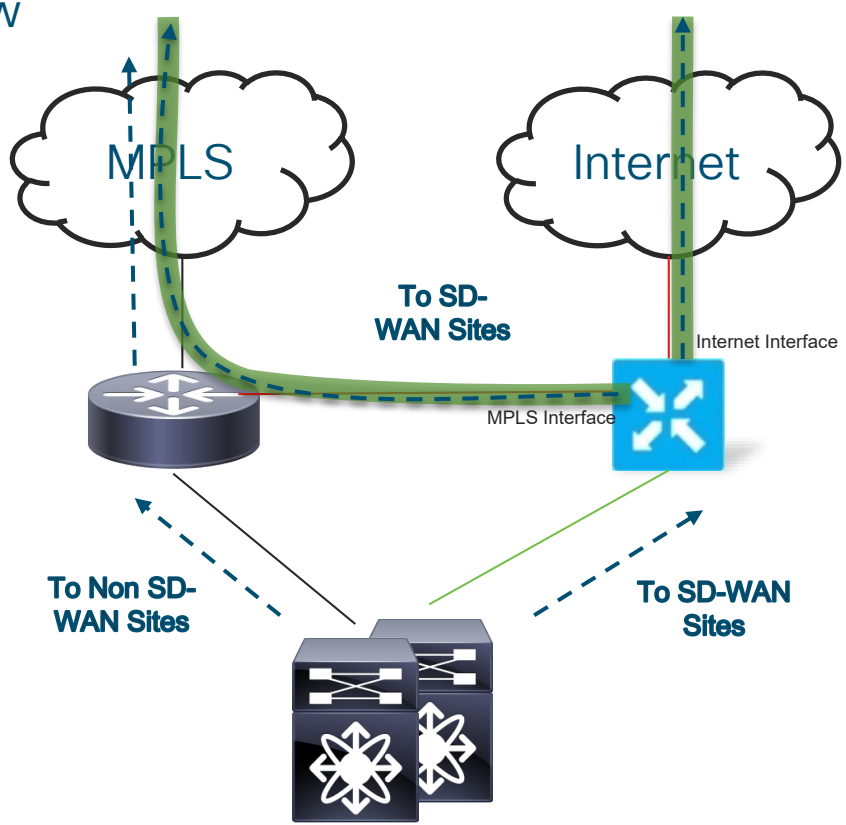
Routing Detail



- CE continues to advertise site prefixes to MPLS PE
- CE continues to advertise all WAN prefixes learned from MPLS to the LAN
- Edge advertises all SD-WAN site prefixes to LAN with better metric than CE
- Recommend iBGP to LAN from Edge and CE. This will keep the branch from becoming a transit site as the LAN will not advertise iBGP learned routes to another iBGP peer.
- If using OSPF, Apply a tag on routes redistributed into site and filter on the TAG inbound on both the CE and the Edge

Full Overlay/Underlay Routing

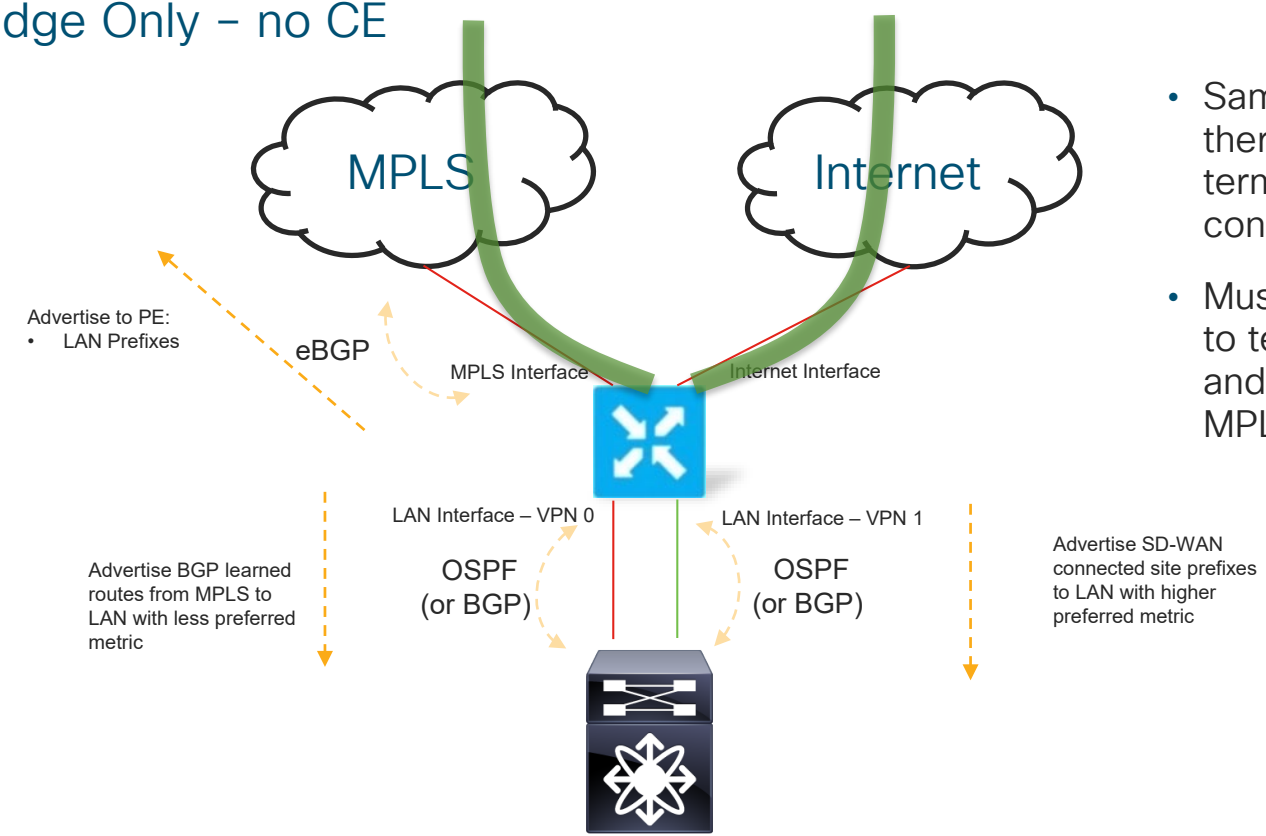
Traffic Flow



- SD-WAN destined traffic goes over the VPN1 connection to the Edge and then out the overlay tunnels
- Non SD-WAN destined traffic goes to the CE and then out unencrypted to the MPLS transport

Full Overlay/Underlay Routing

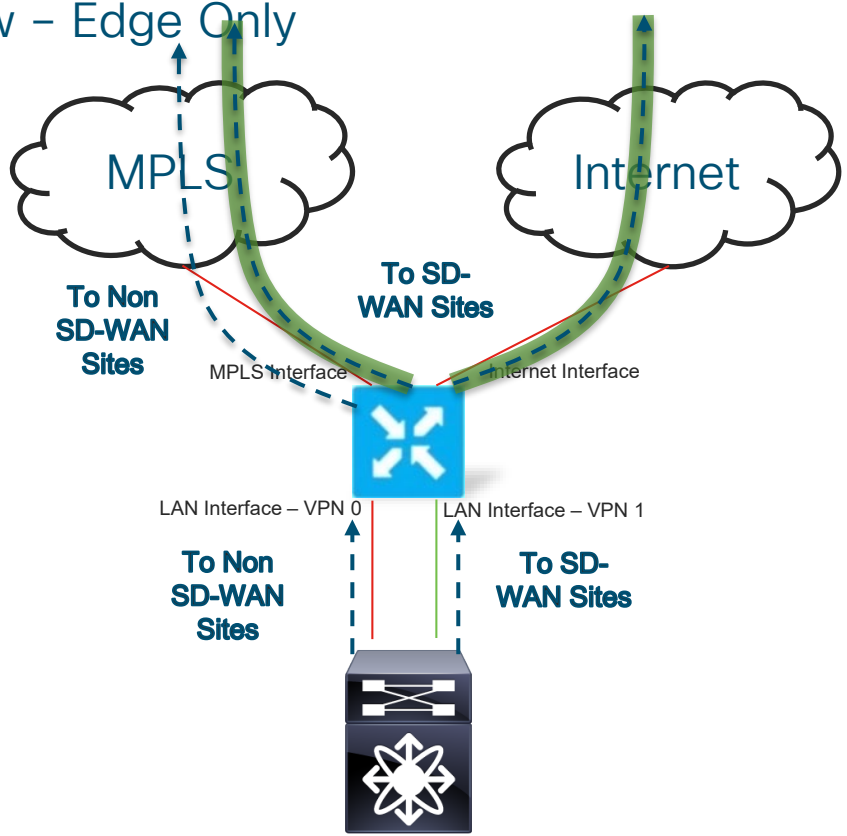
Edge Only – no CE



- Same principles apply as if there were a separate CE terminating the MPLS connection
- Must use a Loopback interface to terminate the MPLS tunnel and bind the loopback to the MPLS Interface

Full Overlay/Underlay Integration

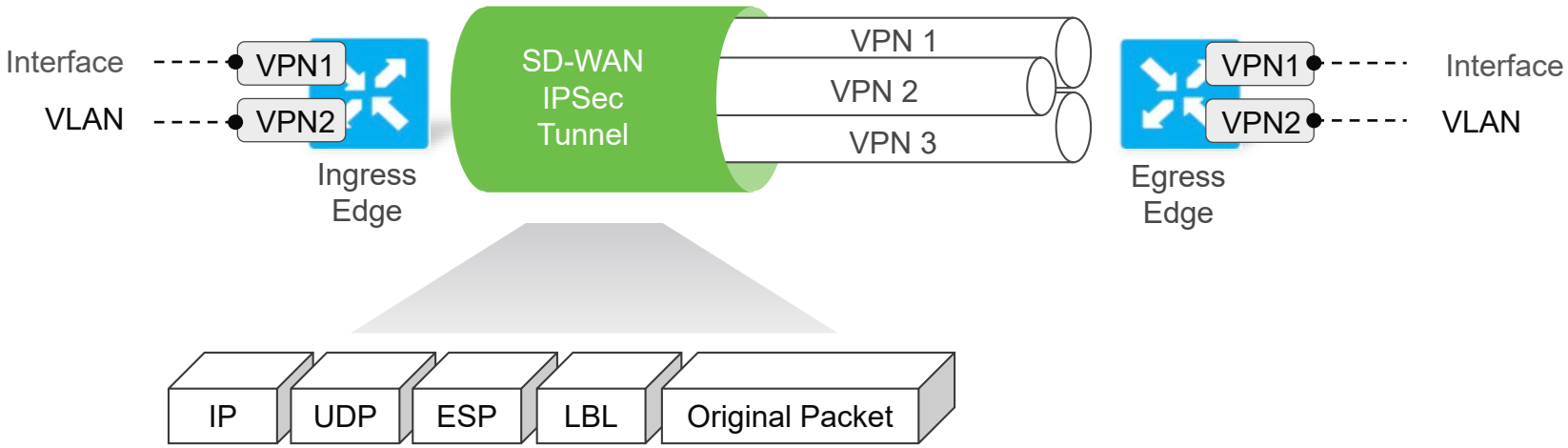
Traffic Flow – Edge Only



- SD-WAN destined traffic goes over the VPN1 connection to the Edge and then out the overlay tunnels
- Non SD-WAN destined traffic goes over VPN0 connection to the Edge and then out unencrypted to the MPLS transport

Segmentation

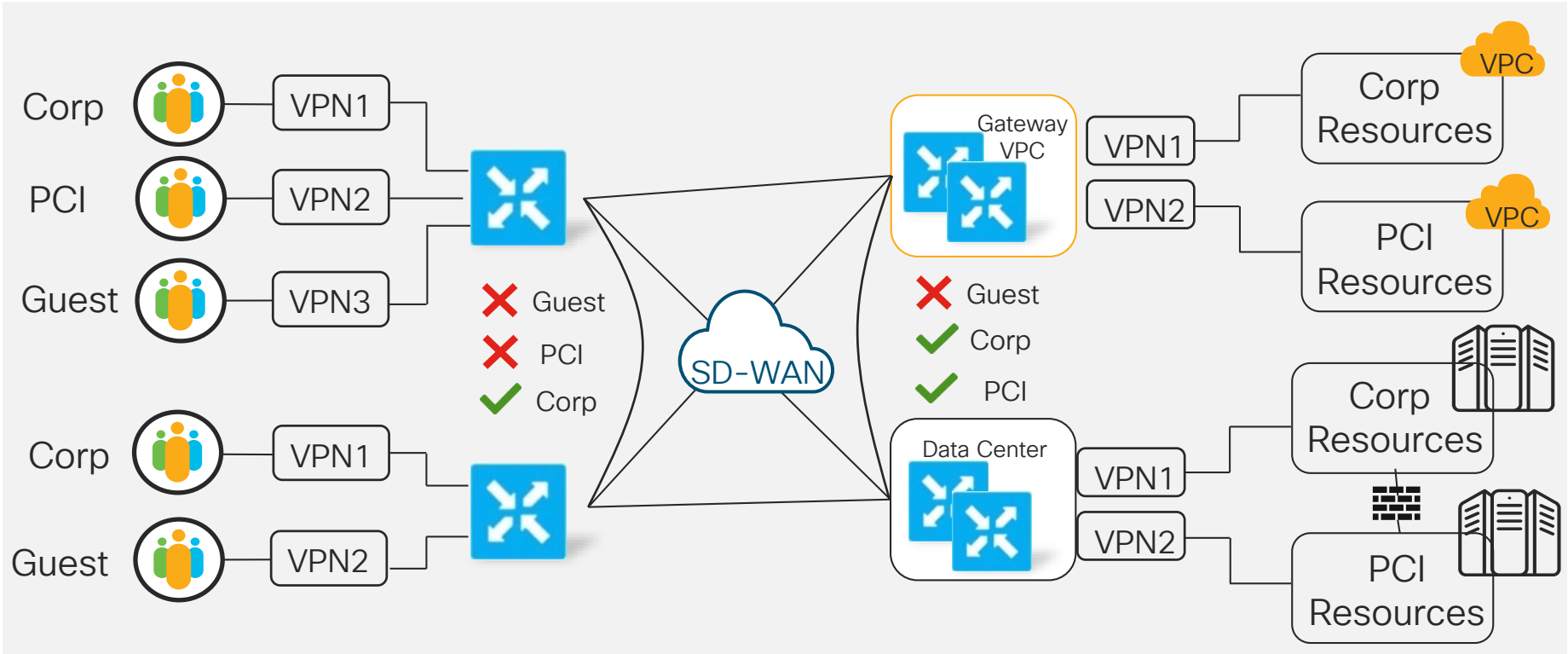
End-to-End Segmentation



- Segment connectivity across fabric w/o reliance on underlay transport
- Interfaces and sub-interfaces (802.1Q tags) are mapped into VPNs
- Edge routers maintain per-VPN routing table for complete control plane separation
- Labels are used to map packets into VPNs for complete data plane separation

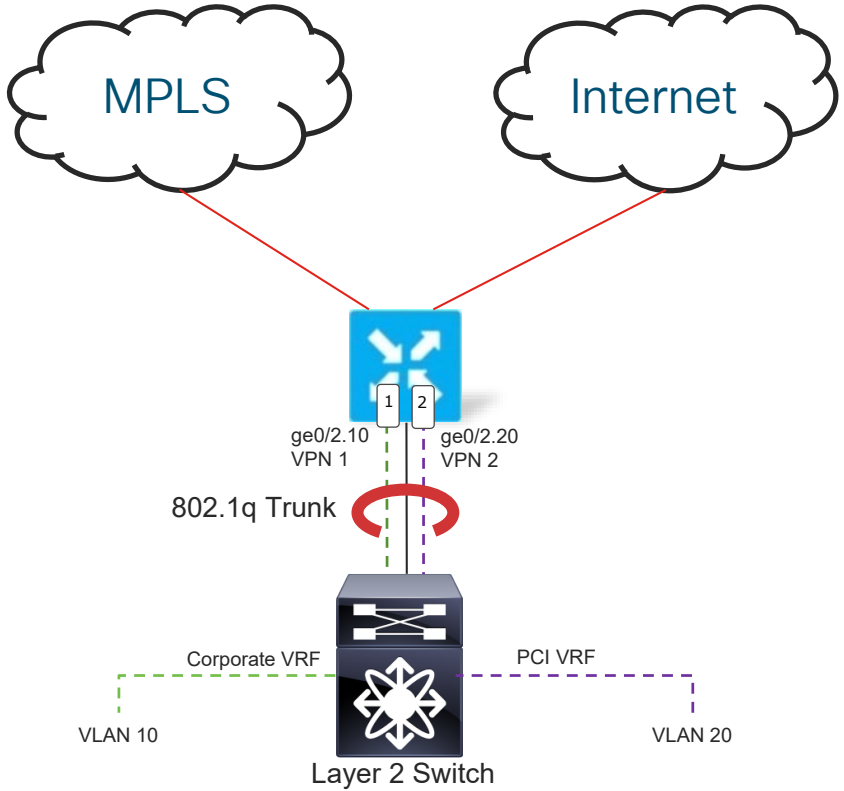
Segmentation across the Stack

End-to-end segmentation across public and private Data Centers



Branch Segmenation

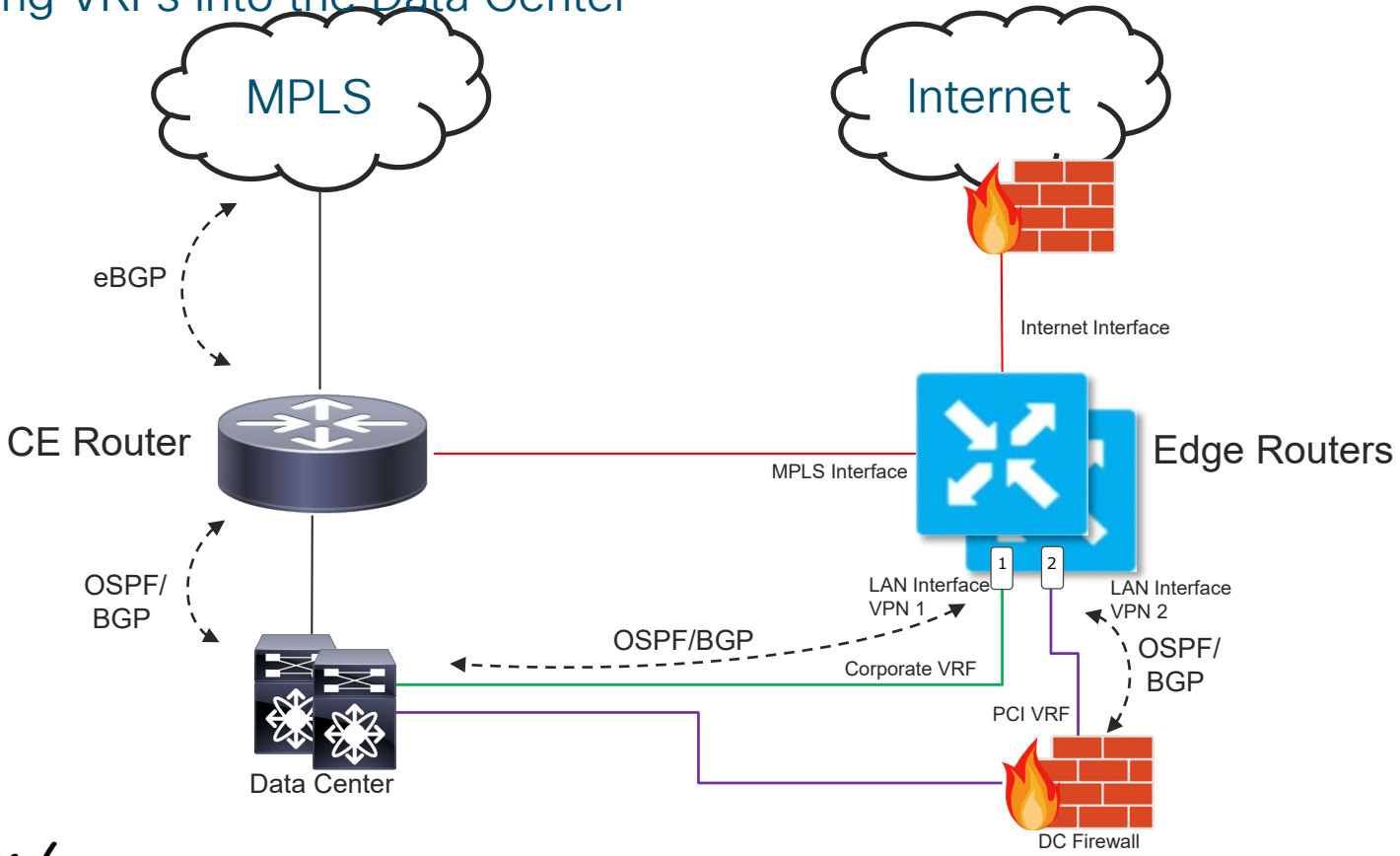
Simple Example of 2 VRFs at Branch with L2 LAN



- VLAN 10 is placed in VPN 1
- VLAN 20 is placed in VPN 2
- Only users in VLAN 10 can communicate in VPN 1 and only users in VLAN 20 can communicate in VPN 2
- *Layer 3 LAN requires VRF-Lite to extend VRFs into campus

Data Center Segmentation

Extending VRFs into the Data Center



Conclusion

- Keep it simple
- SD-WAN in the DC should be transparent to the business
- Integration with the Network is via routing protocols
- Can completely replace the Branch CE in many cases
- Consider if Overlay and Underlay routing in the branch is necessary
- Easily extend segmentation across the WAN

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

cisco Live!

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

Thank you

You make **possible**