

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Unified IoT Network Architectures

Revolutionising Industrial Connectivity with Overlay Technologies

Cameron Dry, Solutions Engineer
CCIE 10705
BRKIOT-2356

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live 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 November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKIOT-2356>



Agenda

- Industrial Network Challenges
- Architecture
 - IP Underlay
 - FlexVPN Overlay
 - Ethernet Virtual Private Network (EVPN) Fabric
- Hardware platforms
- Q & A

Session Goals



Industrial Network Challenges

Industrial Network Challenges



24x7x365



Legacy apps



Mission critical



Environmental

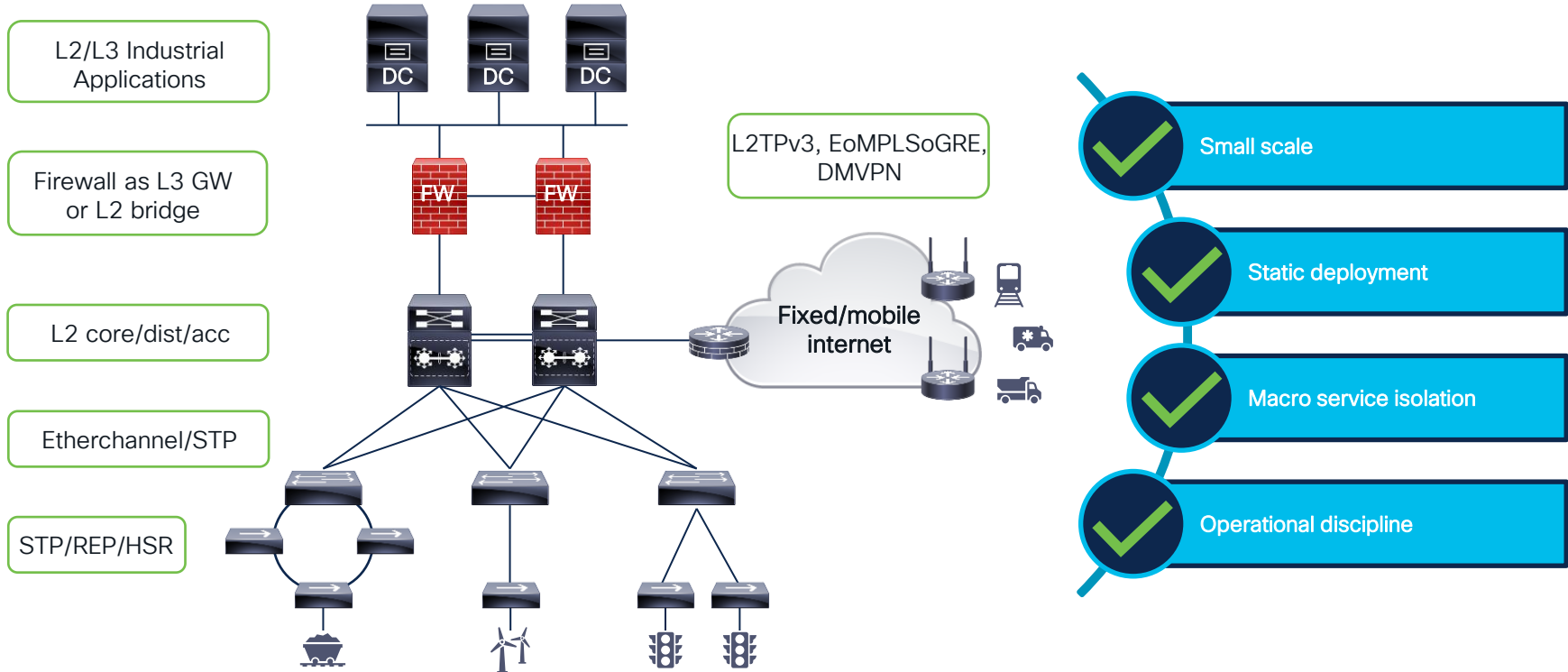


Transmission

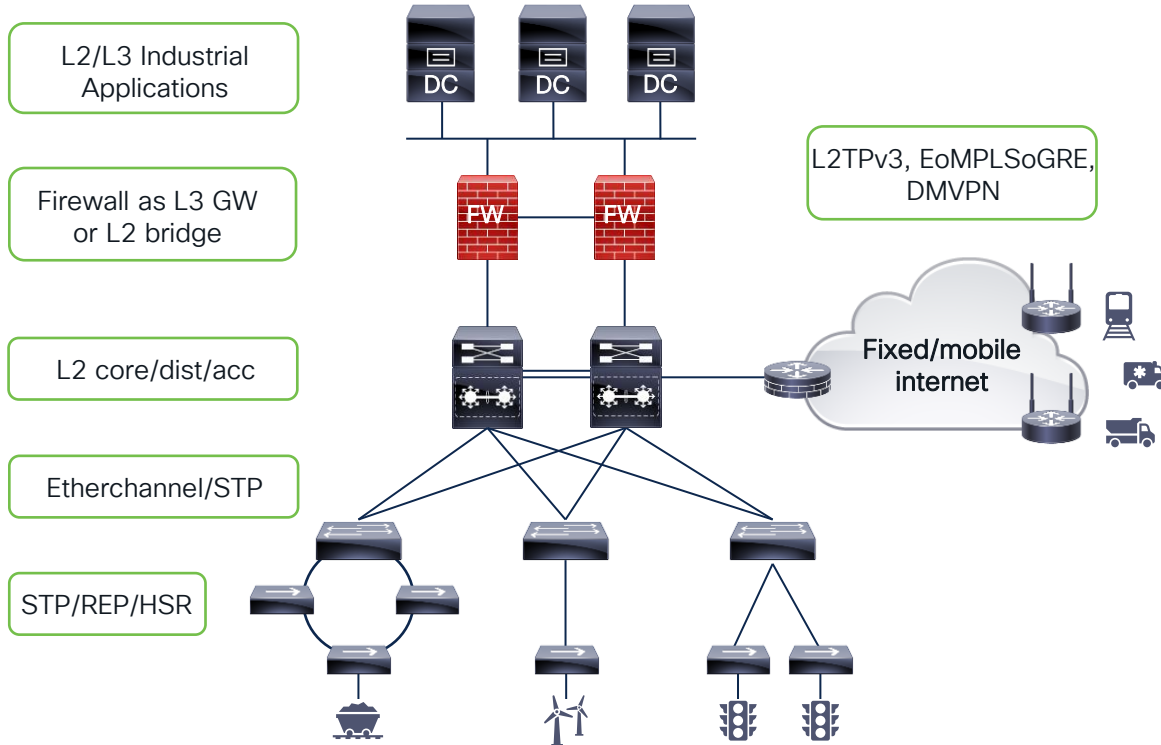


Budget

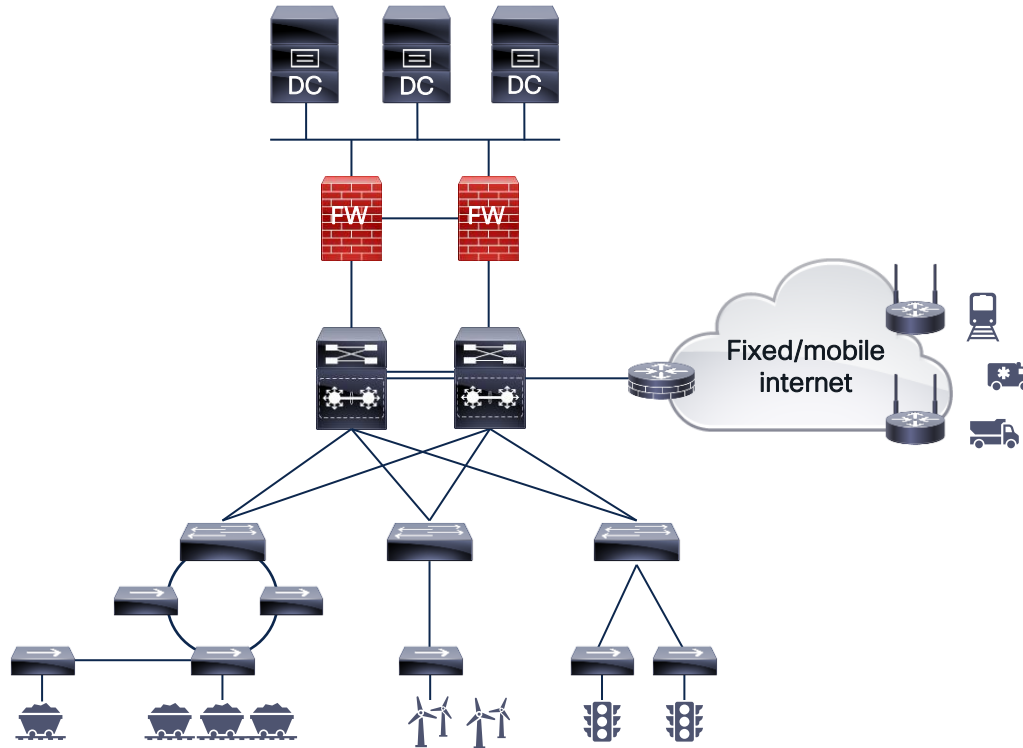
Classic Topology



Classic Topology - Greenfield

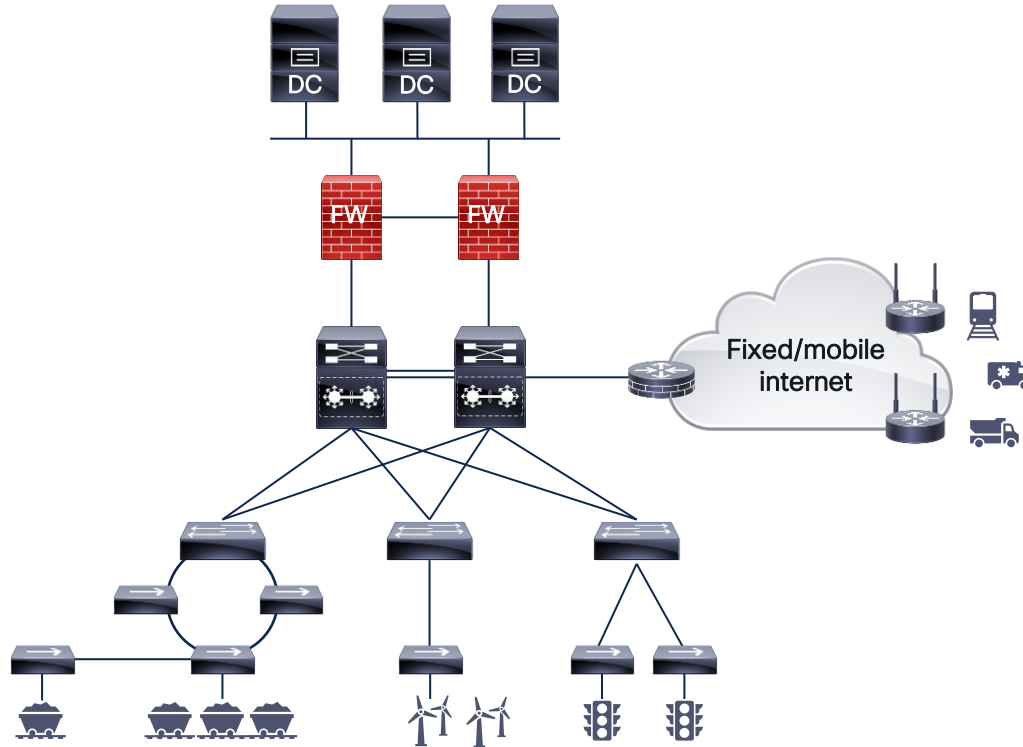


Classic Topology - Greenfield

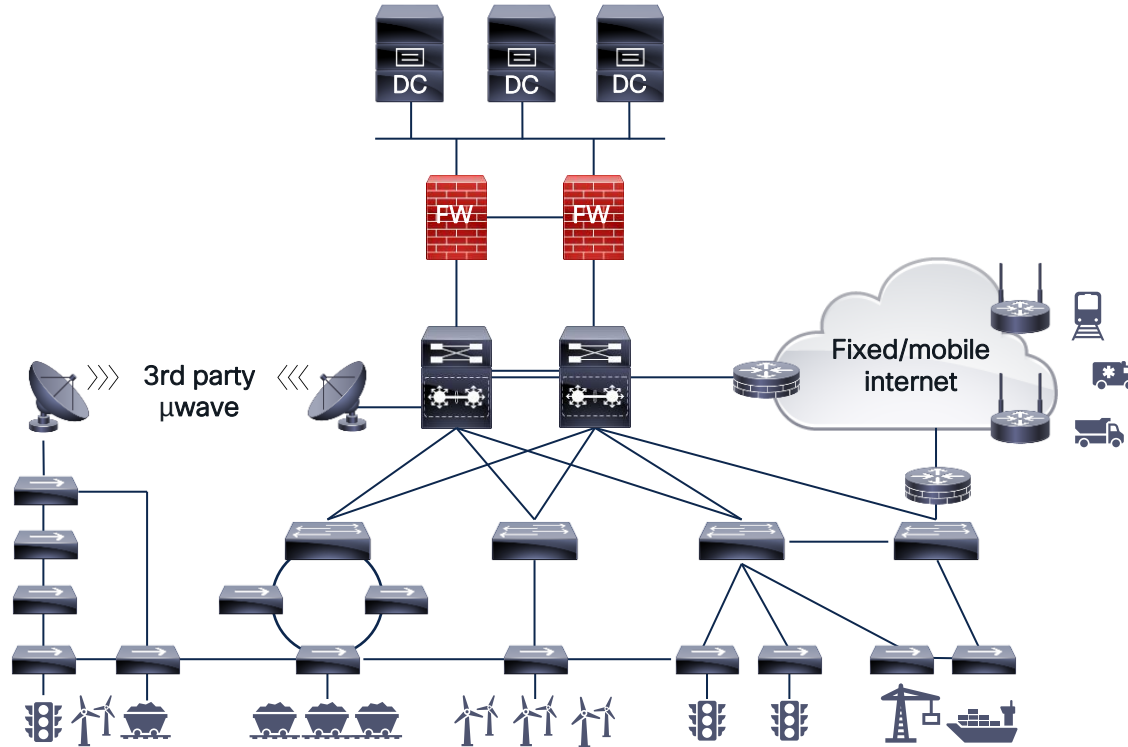


- ✓ Limited expansion
- ✓ Adhere to hierarchical design
- ✓ Maintain service isolation
- ✓ Continue operational discipline

Classic Topology - Brownfield

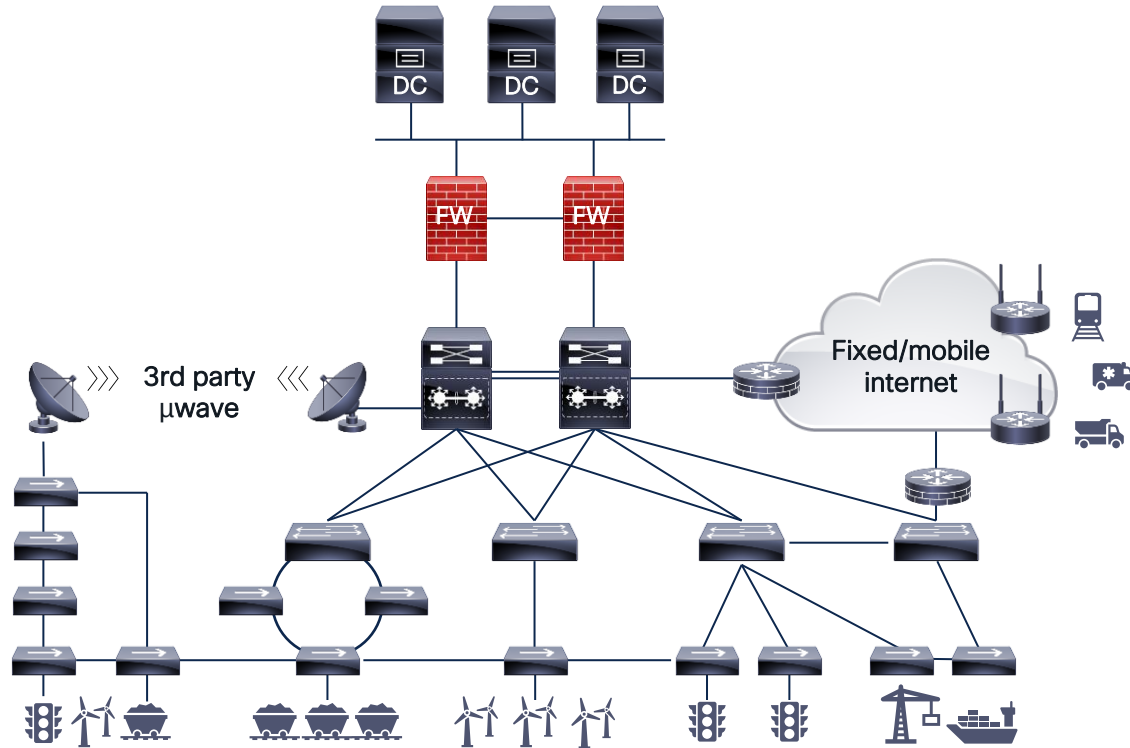
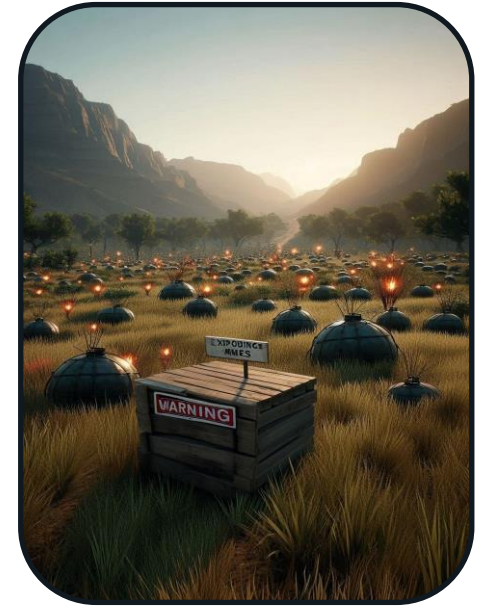


Classic Topology - Brownfield



- Complex L2 topology
- Large failure domain
- Service fate-sharing
- High risk of L2 loops
- FW's are single enforcement point
- Prone to misconfiguration
- Difficult to troubleshoot

Classic Topology - Minefield



Vicious Cycle



Architecture

Requirements

Unified Architecture

- Transport agnostic
- Support mission-critical L2/L3 applications
- Multitenanted
- Data confidentiality
- High availability

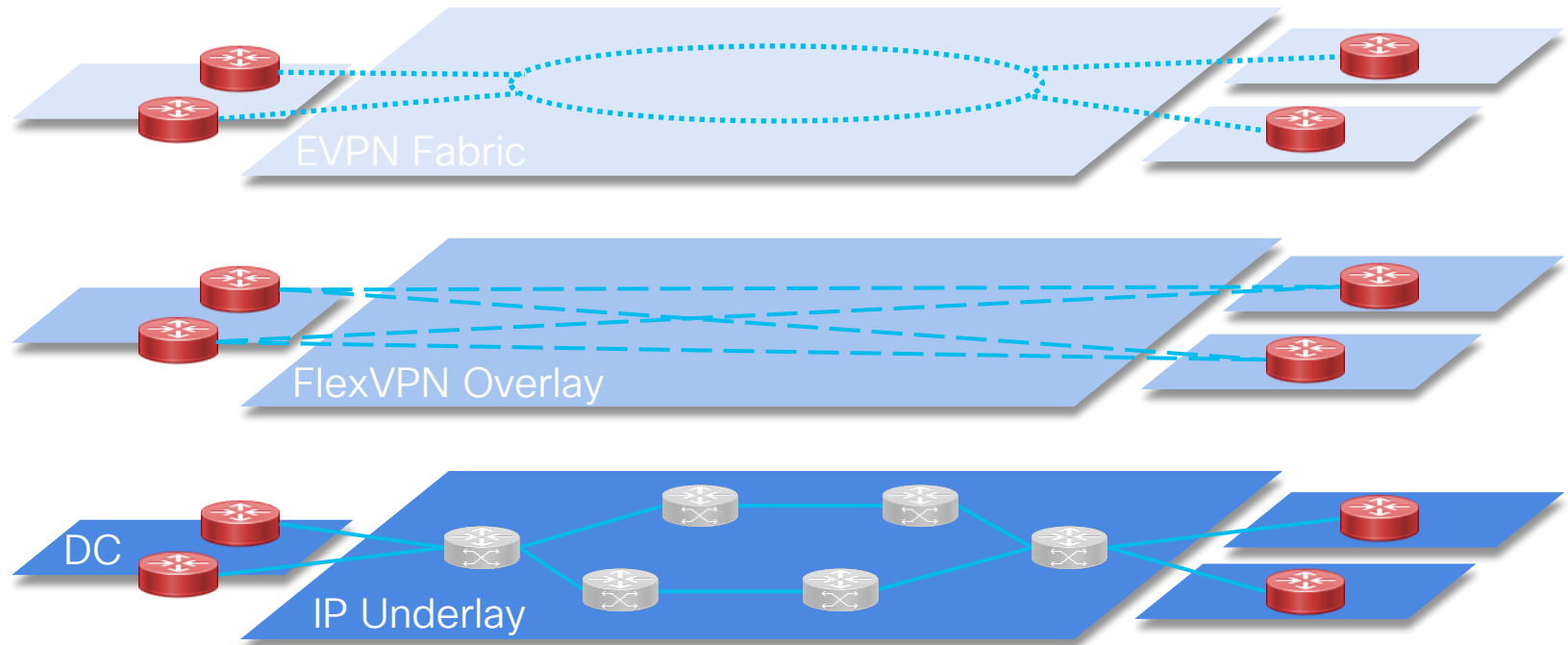
Operational Efficiency

- Simple
- Deterministic
- Maintainable
- Isolated failure domains
- Automatable

Industrial Hardware

- Environmentally hardened
- Small resource footprint
- Open standards
- Zero/low touch provisioning

Fabric Architecture



IP Underlay

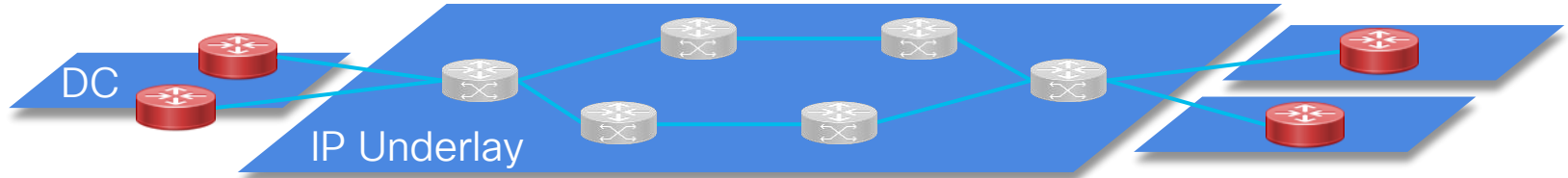
Move packets



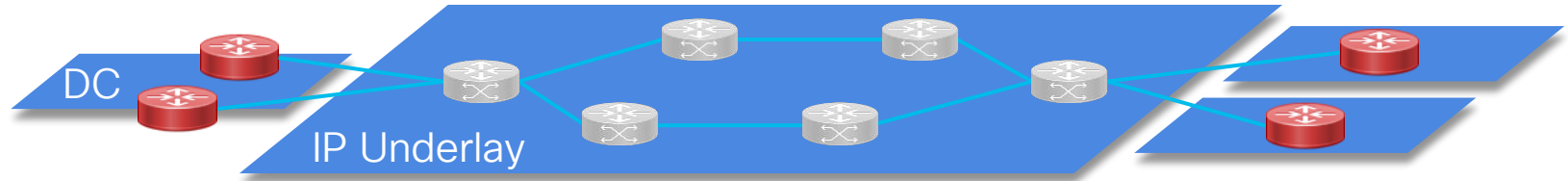
Public/Private network



Requirements



Private IP Underlay Desirables

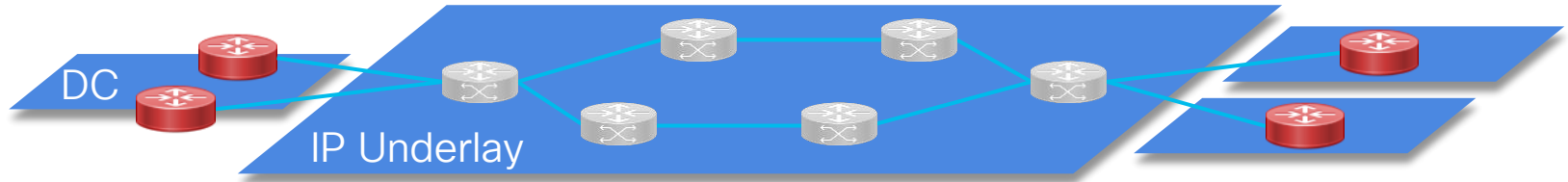


Private IP Underlay Desirables

Routers or
Layer 3 Switches

Addressing:
/31 p2p and
/32 Loopback

Link state and/or BFD
for failure detection

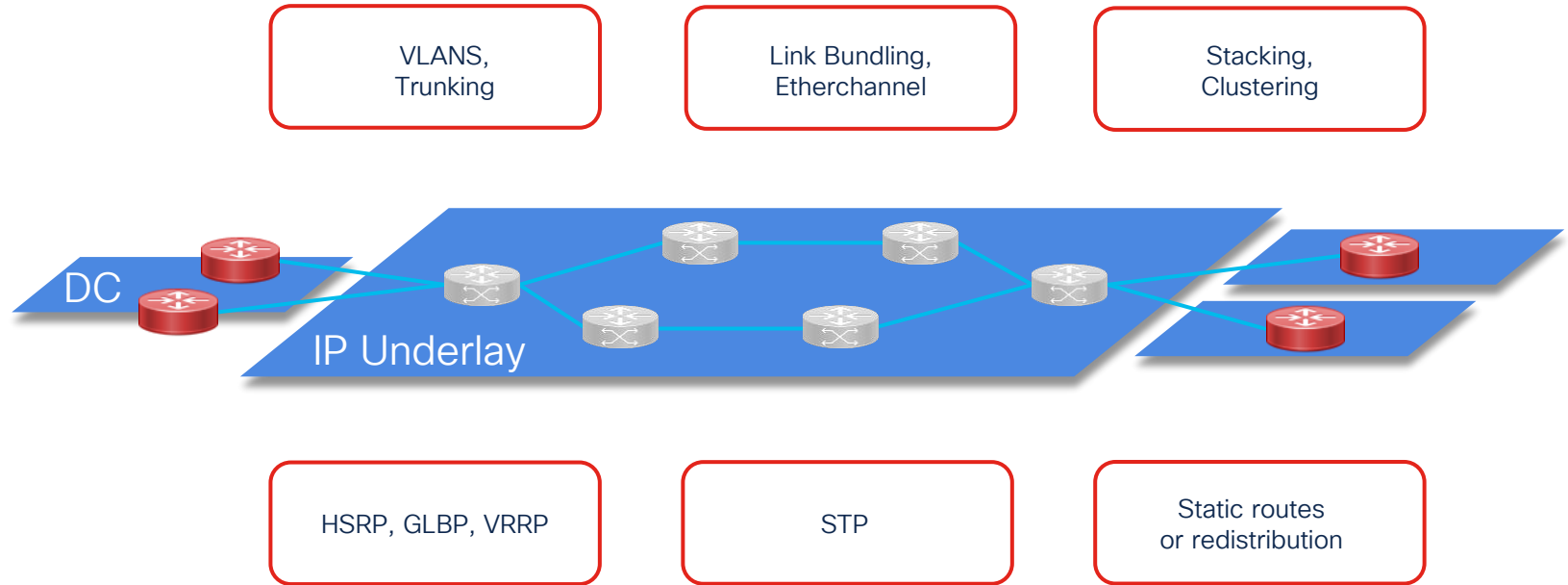


Single IGP
OSPF/ISIS/EIGRP

Lean IGP
Links and Loopbacks only

Multicast
PIM Sparse Mode

Private IP Underlay Undesirables

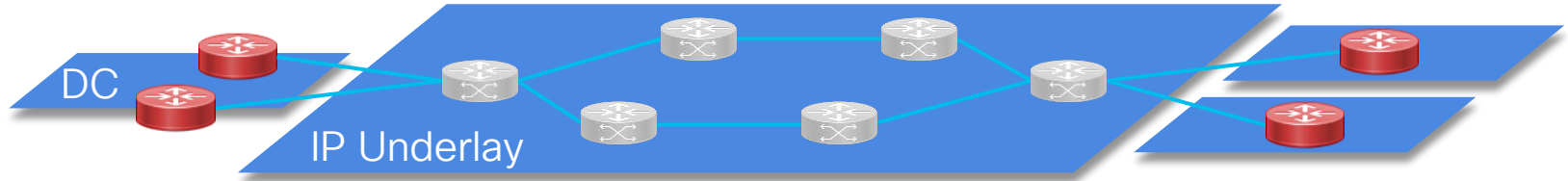


Private IP Underlay Benefits

Any topology and
simple to scale links
or nodes

Efficient use of
capacity with ECMP

Fast convergence

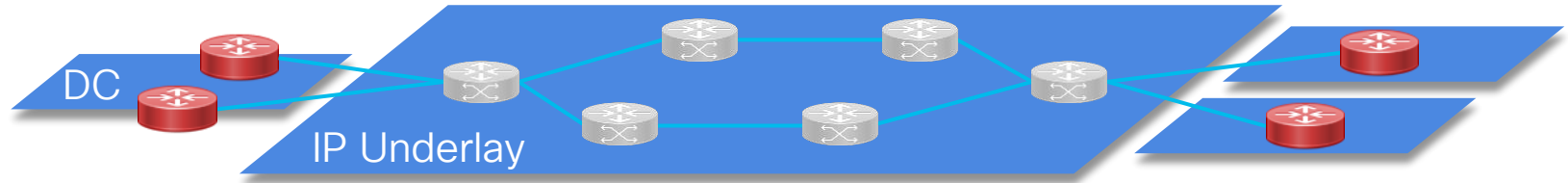


Transparent to user
traffic

Resistant to broadcast
storms and loops

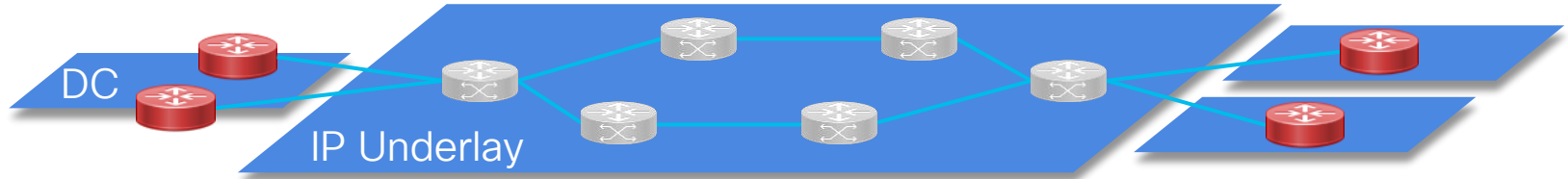
Easier to maintain
and troubleshoot than
layer 2 networks

Private IP Underlay FAQ

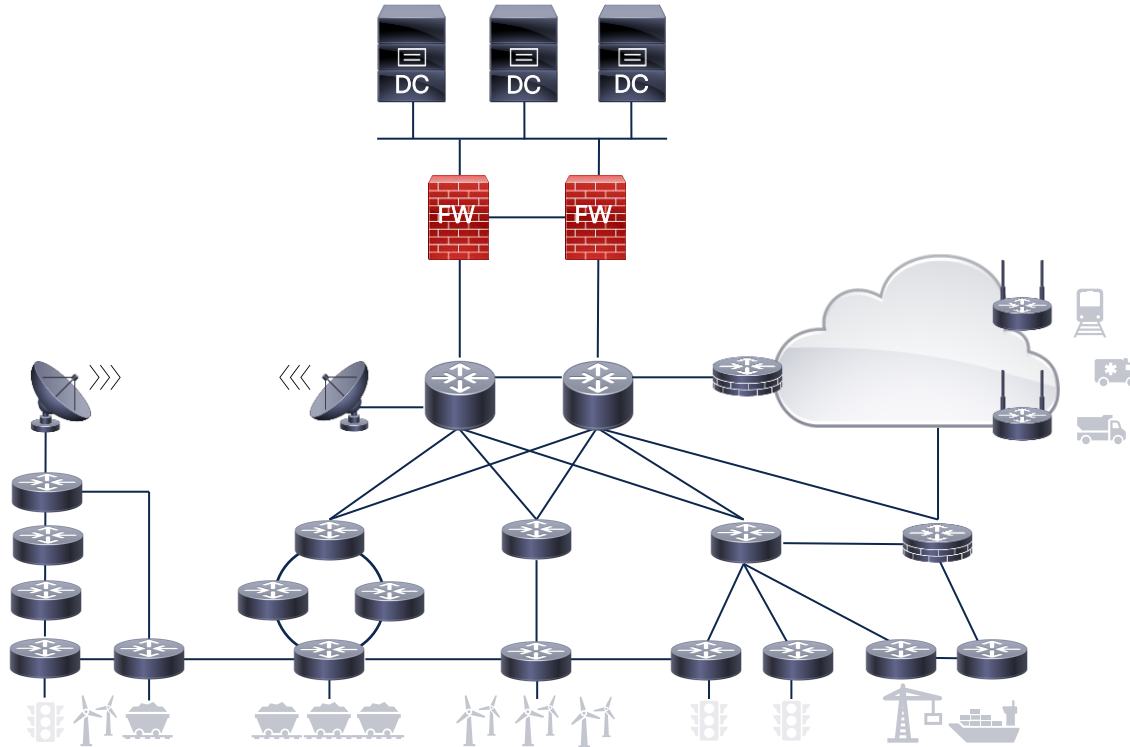


Private IP Underlay FAQ

- Should the underlay be all-active or active-standby ?
 - *All-active ECMP is the default behaviour. Consider the operational impact of either approach before making a design decision.*
- Will asymmetric routing in the underlay cause a problem ?
 - *No, provided application SLAs are met by the network.*
- I have 1.21 Gigawatts of bandwidth. Do I need QoS ?
 - *Coarse Diffserv per-hop-behaviour is recommended using CBWFQ/LLQ.*

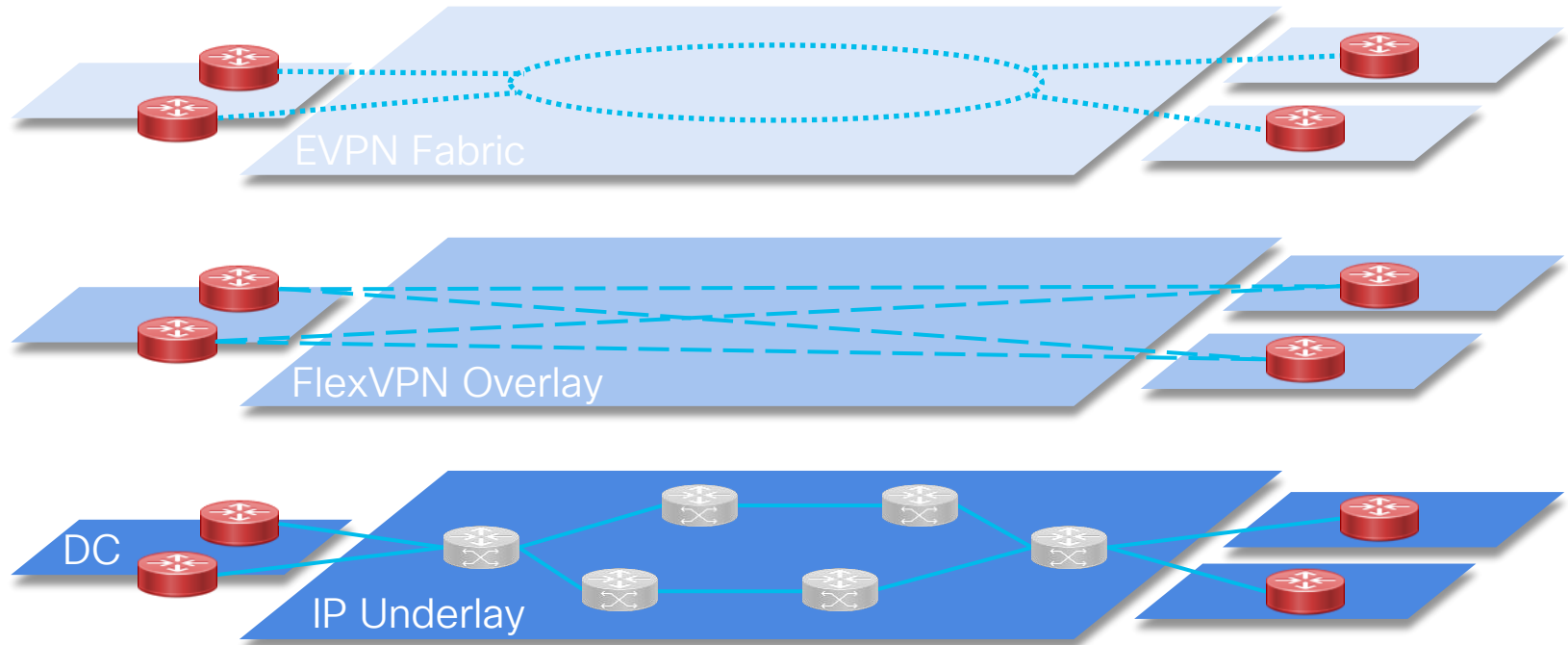


Private Underlay

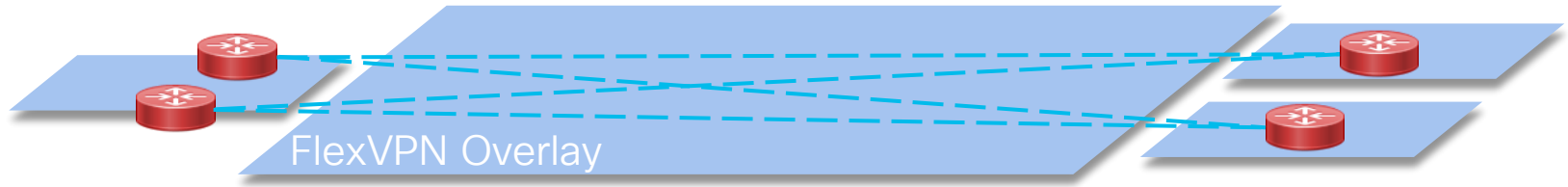


- ✓ Layer 3 routed topology
- ✓ Independent device control planes
- ✓ Automatic loop-free topology
- ✓ All-active by default
- ✓ Simple traffic engineering if required
- ✓ L3 path visibility

FlexVPN Overlay



FlexVPN Overlay

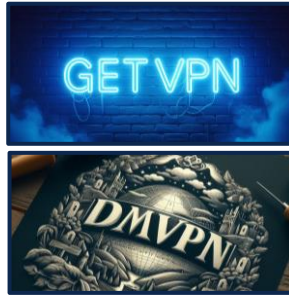


FlexVPN Overlay

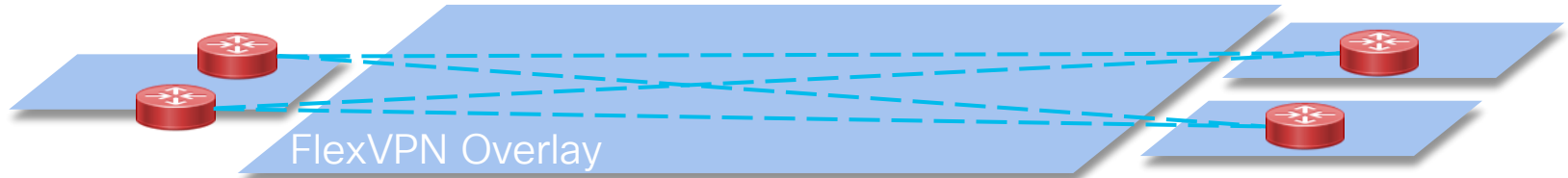
IKEv2-based unified
VPN technology



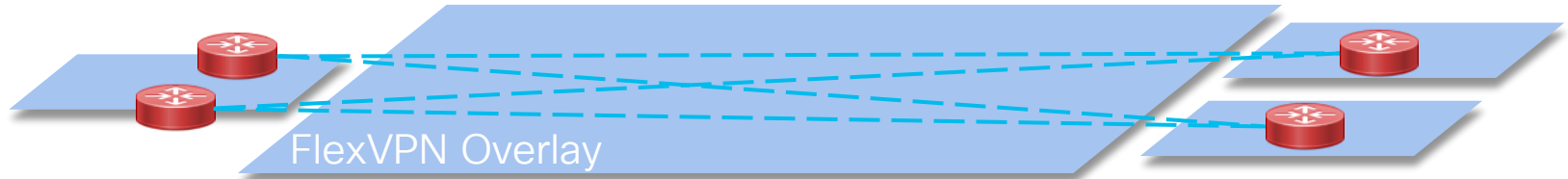
Next
Generation



Data Privacy
and Integrity



FlexVPN Overlay

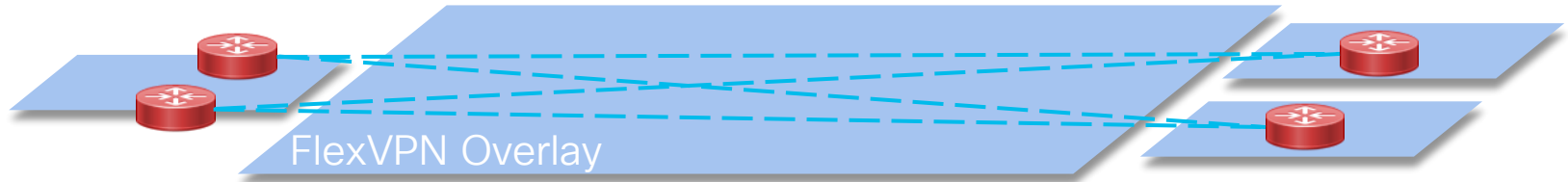


FlexVPN Overlay - Functionality

IKEv2 SA management
IPSec payload protection

Static or dynamic
point-to-point tunnel
interfaces

Scalable per-tunnel
policies from
AAA/RADIUS server



Authentication using PSK,
certificates, EAP

Support for
static, dynamic, PIM
or IKEv2 routing

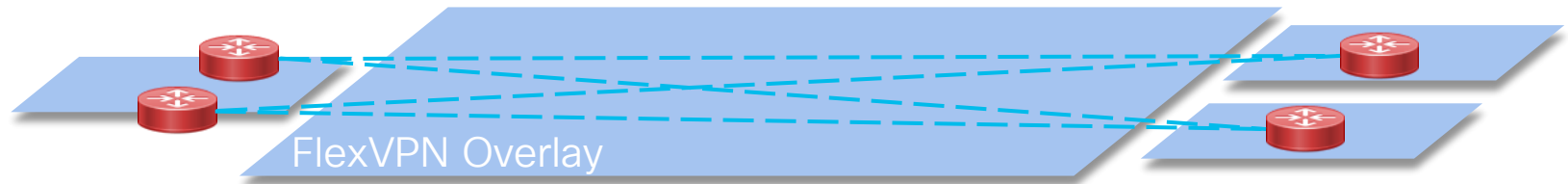
BFD for fast failure
detection on static
tunnels

FlexVPN Overlay – When to Use

Data integrity and
privacy across
public networks

Additional layer of
security over private
networks

IPv6 underlay



No multicast support
in IP underlay

Hub-and-spoke
environments.
e.g. mobile fleet

Authentication of
network endpoint

FlexVPN Overlay - Dynamic Hub and Spoke

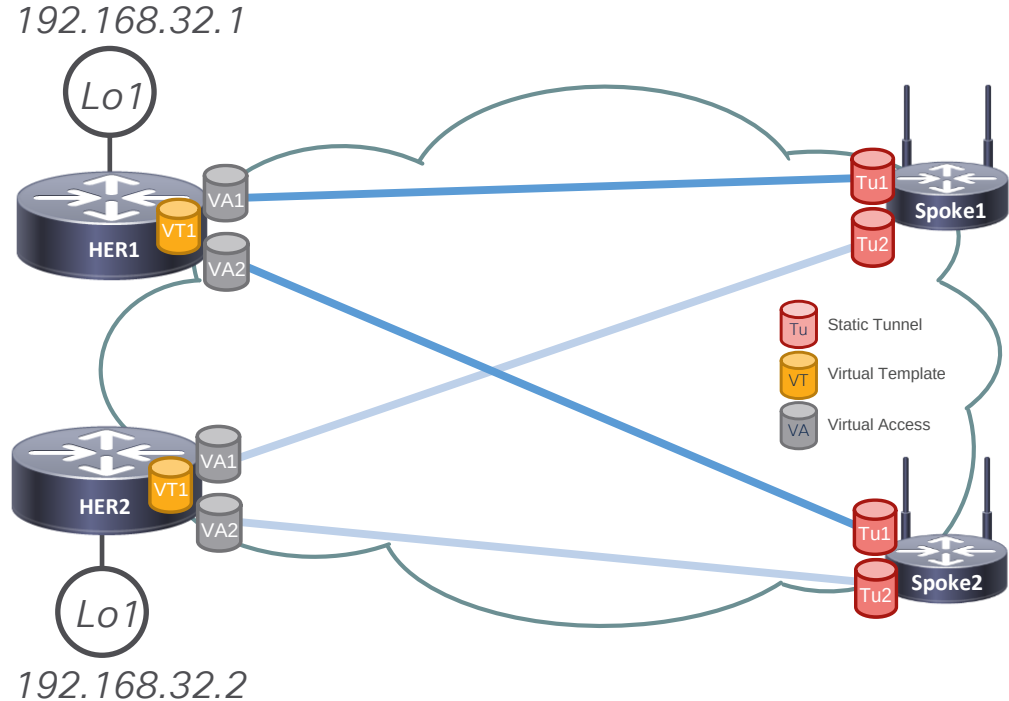
Head End Router (HER) dynamic tunnel interface configuration

HER1

```
interface Virtual-Template1 type tunnel
ip unnumbered Loopback1
tunnel protection ipsec profile default
!
ip local pool FlexVPN 192.168.0.1 192.168.3.255
```

HER2

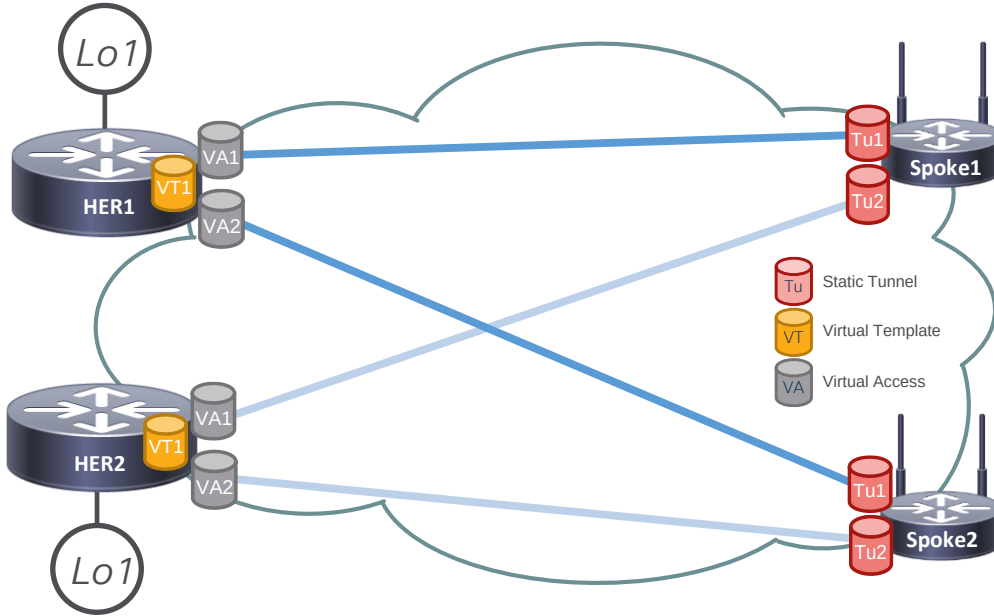
```
interface Virtual-Template1 type tunnel
ip unnumbered Loopback1
tunnel protection ipsec profile default
!
ip local pool FlexVPN 192.168.4.1 192.168.7.255
```



FlexVPN Overlay - Dynamic Hub and Spoke

Spoke static tunnel interface configuration

192.168.32.1



192.168.32.2

CISCO Live!

Spoke n

```
interface Tunnel1
ip address negotiated
tunnel source Cellular0/4/0
tunnel destination <HER1 underlay ipaddr>
tunnel protection ipsec profile default
```

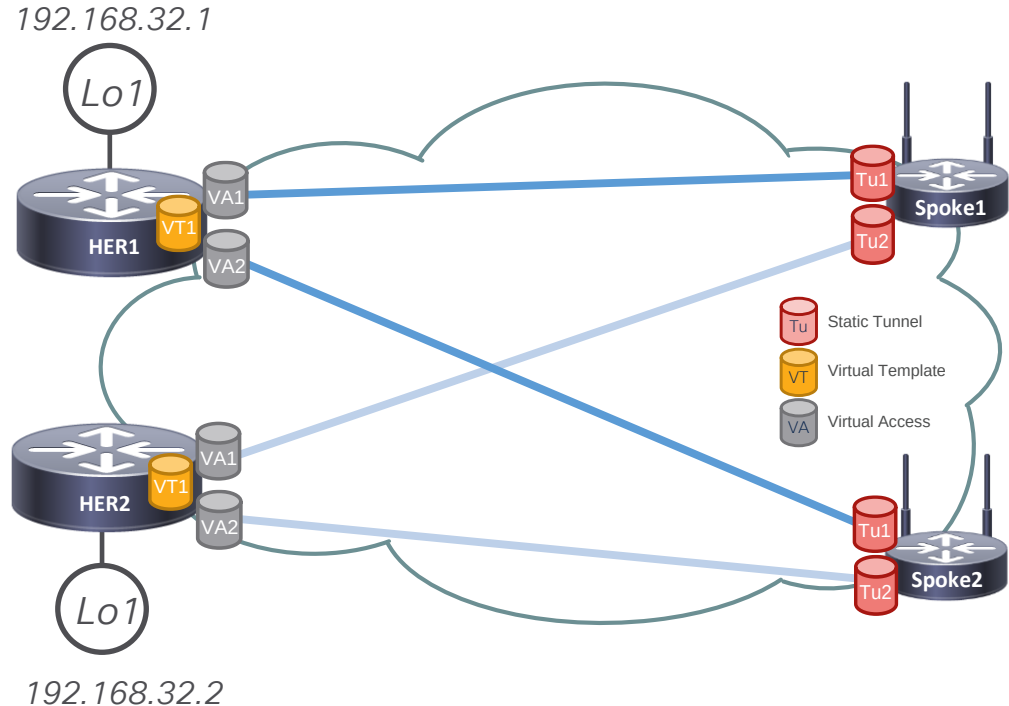
```
interface Tunnel2
ip address negotiated
tunnel source Cellular0/4/0
tunnel destination <HER2 underlay ipaddr>
tunnel protection ipsec profile default
```

FlexVPN Overlay – Dynamic Hub and Spoke

HER IKEv2 profile configuration

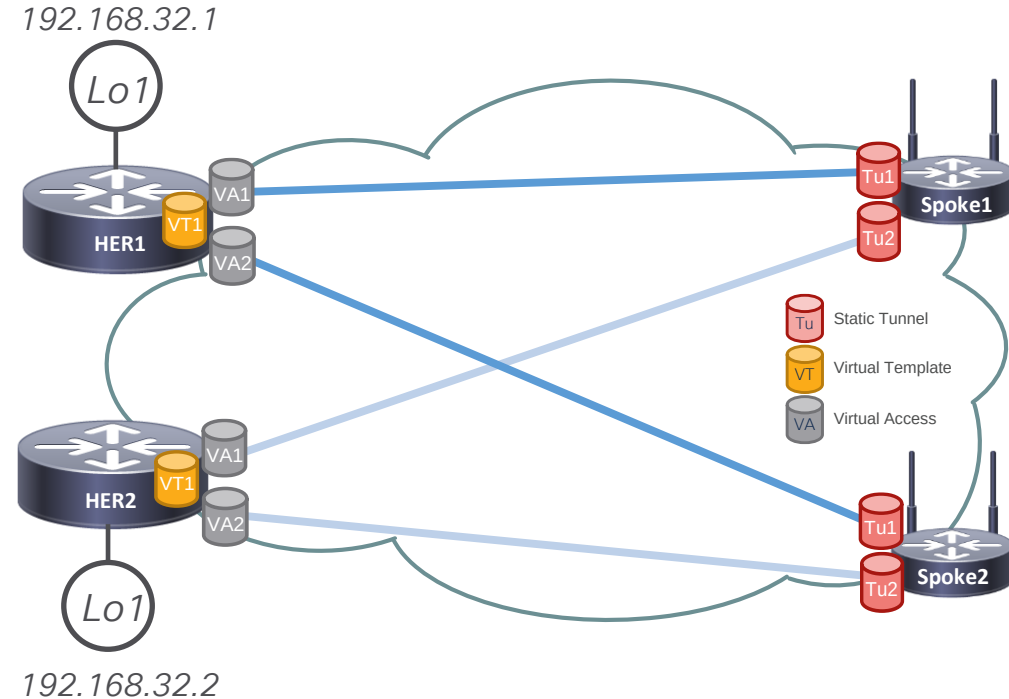
HER

```
crypto ikev2 profile default
match identity remote address <Spoke_IP_range>
authentication remote pre-share key cisco123
authentication local pre-share key cisco456
aaa authorization group psk list default default
!
aaa authorization network default local
```



FlexVPN Overlay - Dynamic Hub and Spoke

Spoke IKEv2 profile configuration

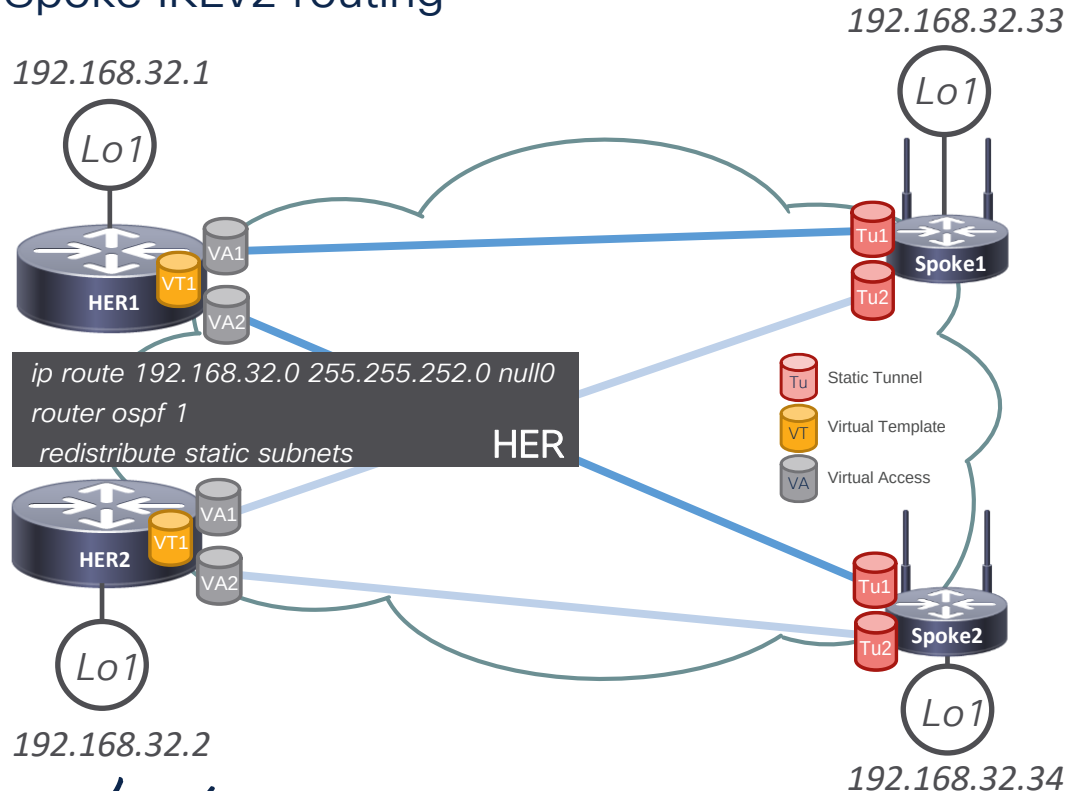


Spoke *n*

```
crypto ikev2 profile default
match identity remote address <HER_IP_addr>
authentication remote pre-share key cisco456
authentication local pre-share key cisco123
aaa authorization group psk list default default
!
aaa authorization network default local
!
```

FlexVPN Overlay - IKEv2 Routing

Spoke IKEv2 routing



Spoke 1

```
crypto ikev2 authorization policy default
 route set access-list Loopback1
 !
 ip access-list standard Loopback1
 10 permit 192.168.32.33
```

Spoke 2

```
crypto ikev2 authorization policy default
 route set access-list Loopback1
 !
 ip access-list standard Loopback1
 10 permit 192.168.32.34
```

FlexVPN Overlay - Static Point-to-Point

Static tunnel interface configuration



HER1

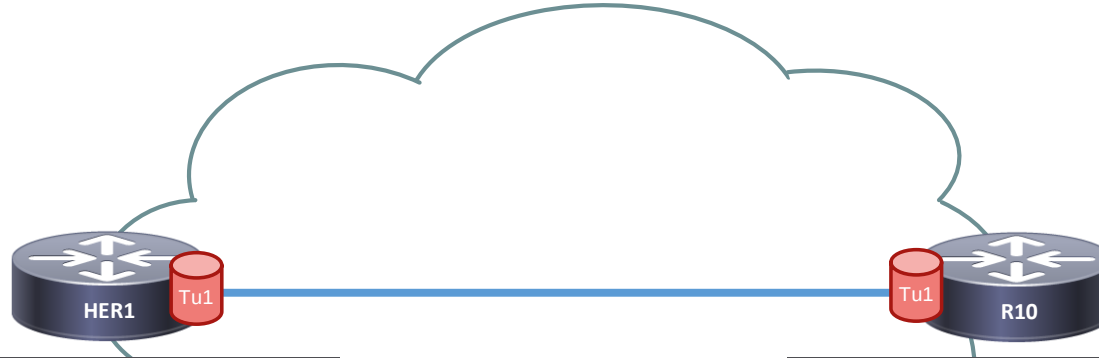
```
interface tunnel1
ip address 10.0.0.0 255.255.255.254
tunnel source <physical or underlay loopback>
tunnel destination <R10 underlay ipaddr>
tunnel protection ipsec profile default
```

R10

```
interface tunnel1
ip address 10.0.0.1 255.255.255.254
tunnel source <physical or underlay loopback>
tunnel destination <HER underlay ipaddr>
tunnel protection ipsec profile default
```

FlexVPN Overlay - Static Point-to-Point IKEv2

IKEv2 profile configuration



HER1

```
crypto ikev2 profile default
match identity remote address <R10 ipaddr>
authentication remote pre-share key cisco123
authentication local pre-share key cisco456
```

R10

```
crypto ikev2 profile default
match identity remote address <HER ipaddr>
authentication remote pre-share key cisco456
authentication local pre-share key cisco123
```

FlexVPN Overlay – Smart Crypto Defaults

IKEv2

HER1#show crypto ikev2 proposal default

IKEv2 proposal: default

Encryption : AES-CBC-256

Integrity : SHA512 SHA384

PRF : SHA512 SHA384

DH Group : DH_GROUP_256_ECP/Group 19

DH_GROUP_2048_MODP/Group 14

DH_GROUP_521_ECP/Group 21

IPSec

HER1#show crypto ipsec profile default

IPSEC profile default

IKEv2 Profile: default

*Security association lifetime: 4608000 kilobytes
3600 seconds*

Dualstack (Y/N): N

Responder-Only (Y/N): N

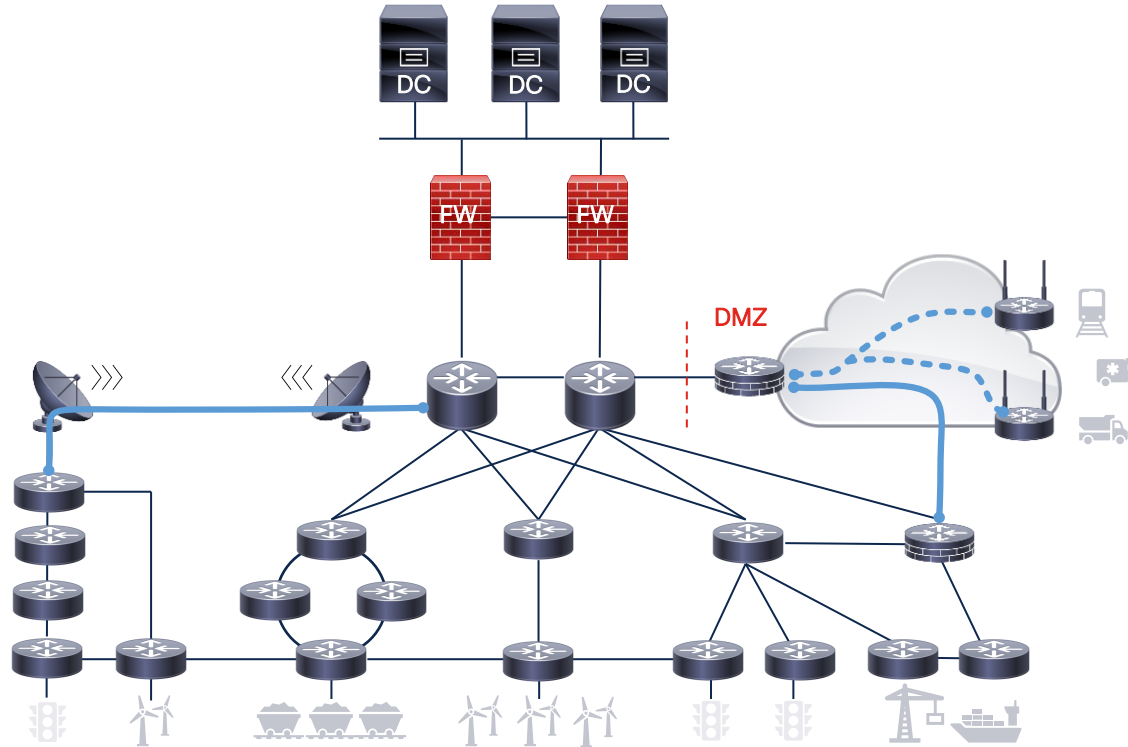
PFS (Y/N): N

Mixed-mode : Disabled

*Transform sets={
 default: { esp-aes esp-sha-hmac },
}*

https://sec.cloudapps.cisco.com/security/center/resources/next_generation_cryptography

Architecture - FlexVPN Overlay

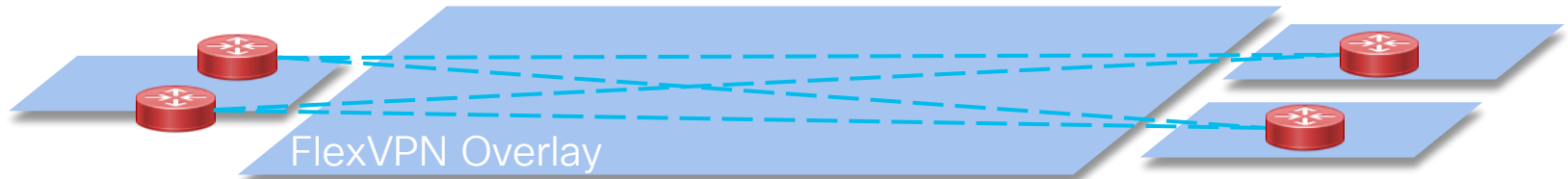


- ✓ Static and dynamic tunnels
- ✓ Fully private underlay/overlay
- ✓ Option to extend FlexVPN overlay to all network nodes
- ✓ IGP across static tunnels
- ✓ Dynamic endpoints appear as directly connected routes
- ✓ Optionally move HER in to DMZ

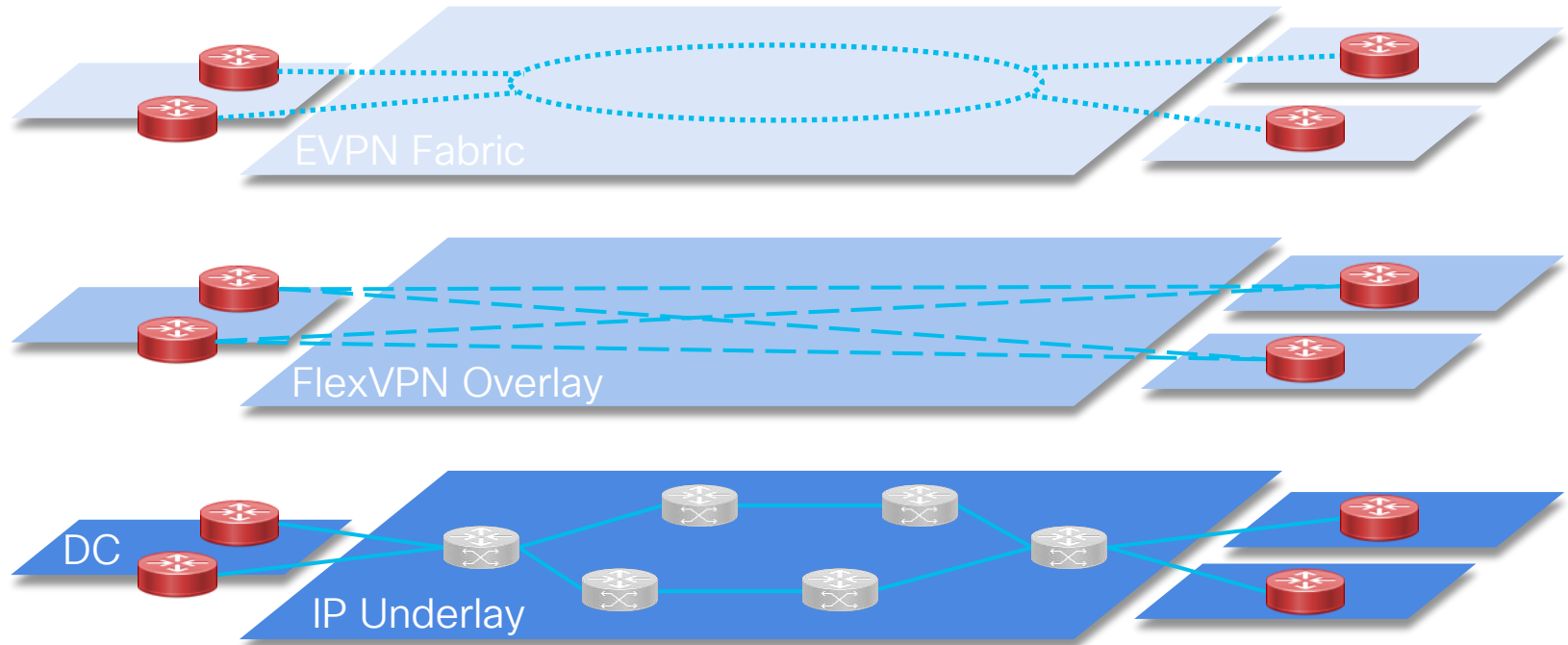
..... Static tunnel
———— Dynamic tunnel

FlexVPN – FAQ

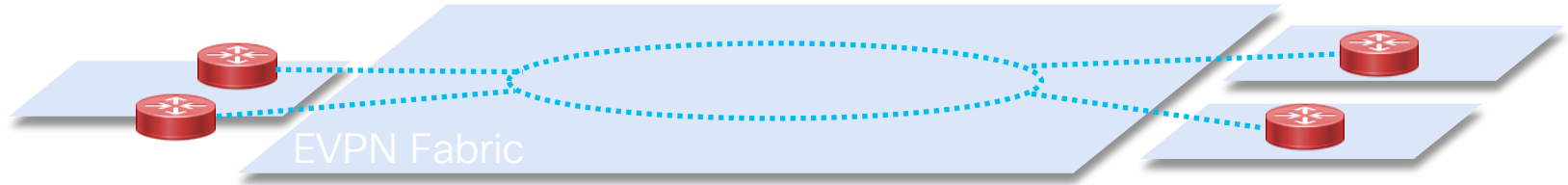
- Is FlexVPN Cisco proprietary ?
 - *No, IKEv2 implementations are available on most OS' including Android, Apple IOS, Linux, Windows and third party NOS'.*
- Can I have different policies for each Spoke ?
 - *Yes, by using a RADIUS server such as ISE to dynamically apply profiles.*
- How does Spoke-to-Spoke traffic work ?
 - *Either using NHRP and dynamic Spoke-Spoke tunnels or via the HER.*



EVPN Fabric



EVPN Fabric



EVPN Fabric

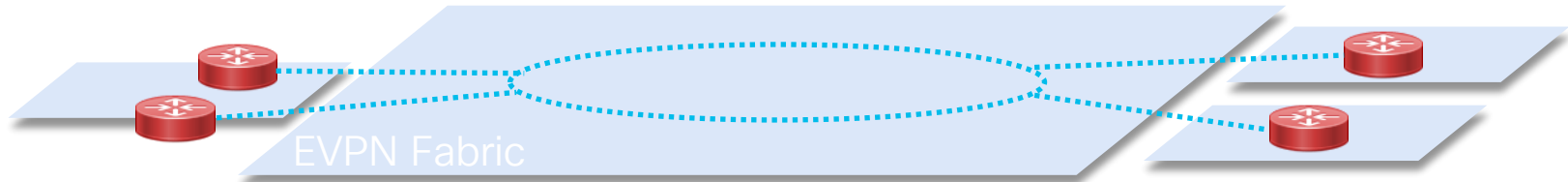
Network virtualisation
using BGP control plane



Integrated L2
and L3 Services



Next Generation,
Open Standard

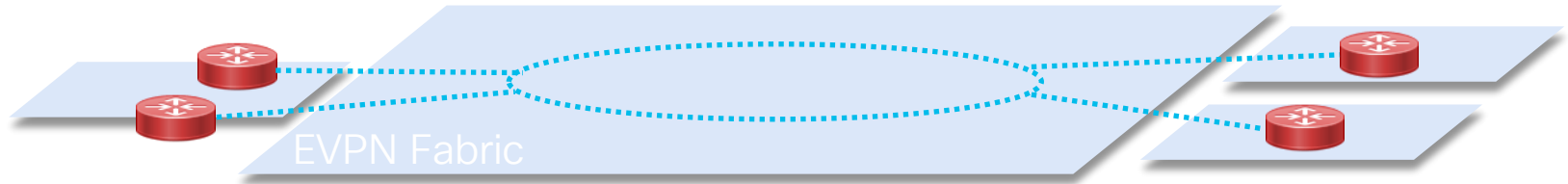


EVPN Fabric – Functionality

Control Plane:
MP-BGP for
reachability

Data plane:
VXLAN, MPLS or SRv6 for
encapsulation

Full mesh, P2P, P2MP,
partial mesh topologies
for both L2 and L3 VPNs

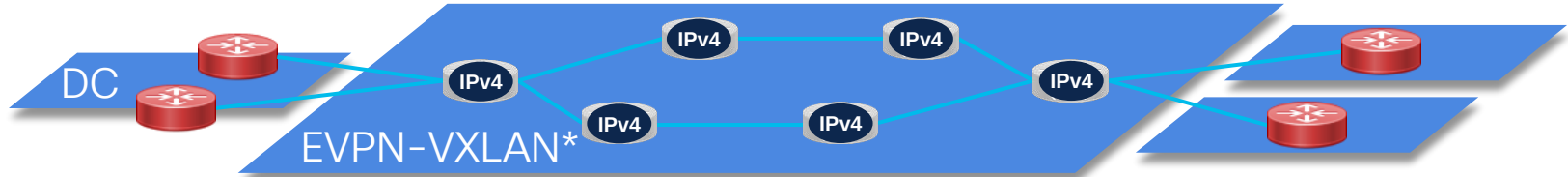


High scalability with
inherent
loop-prevention

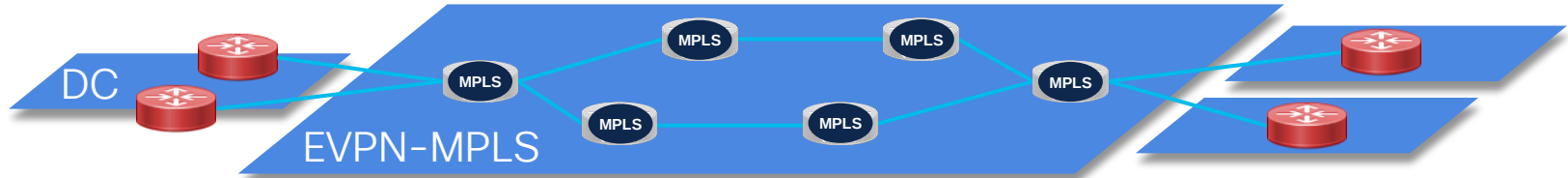
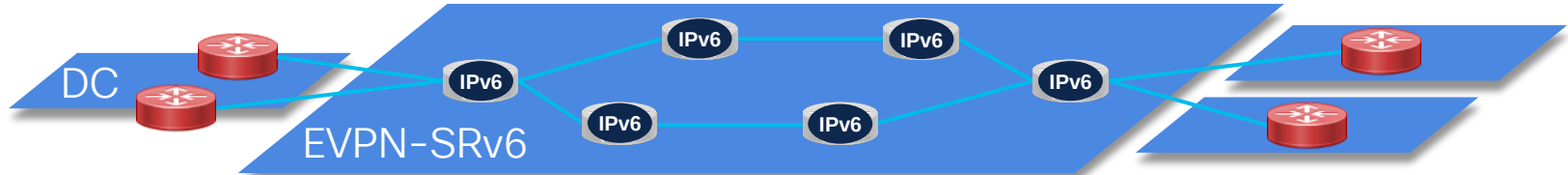
Multihoming and
load-balancing

Fast convergence

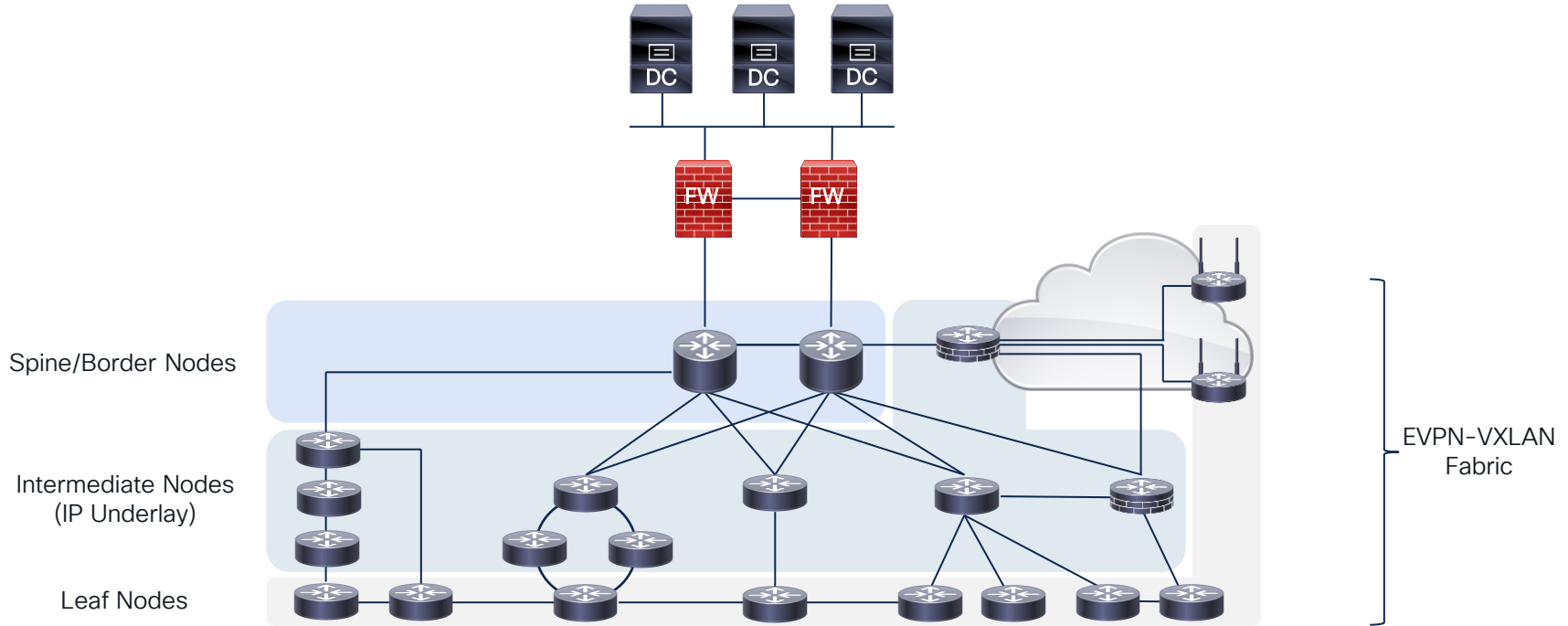
EVPN Fabric - Data Plane Options



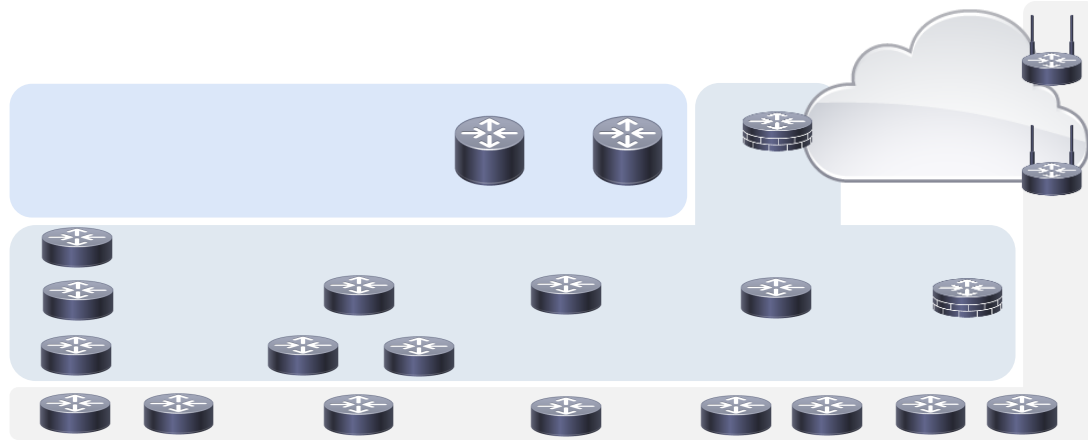
*Recent support for IPv6 underlay EVPN-VXLANv6 on some platforms



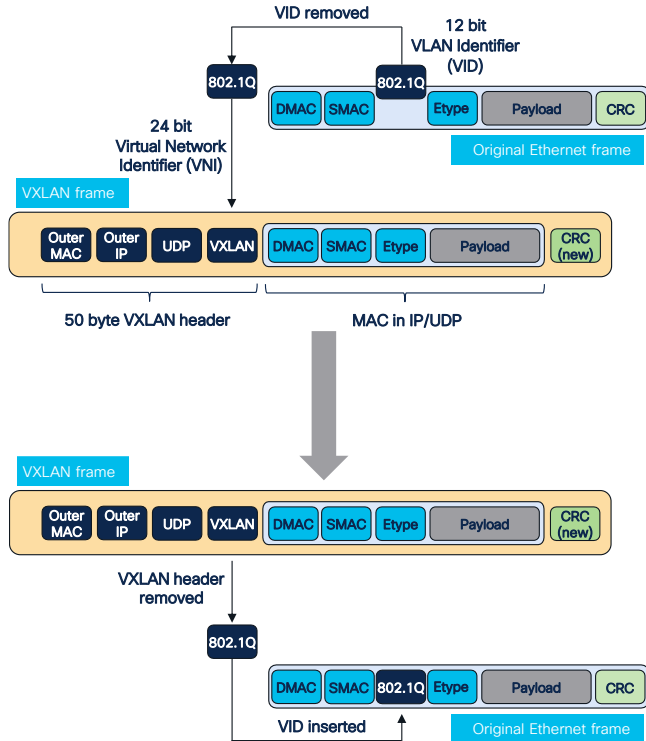
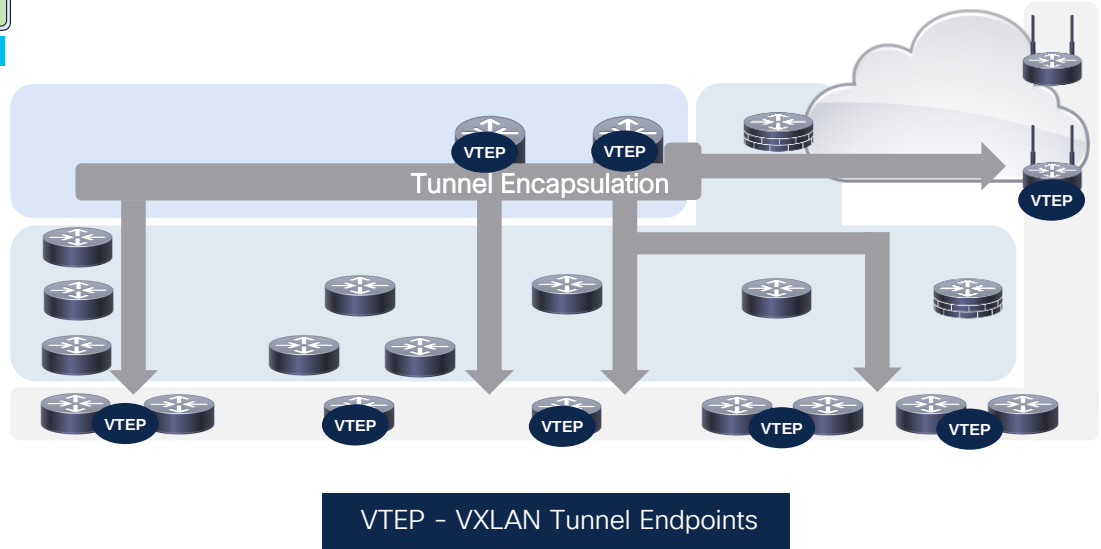
EVPN-VXLAN Fabric



VXLAN Data Plane

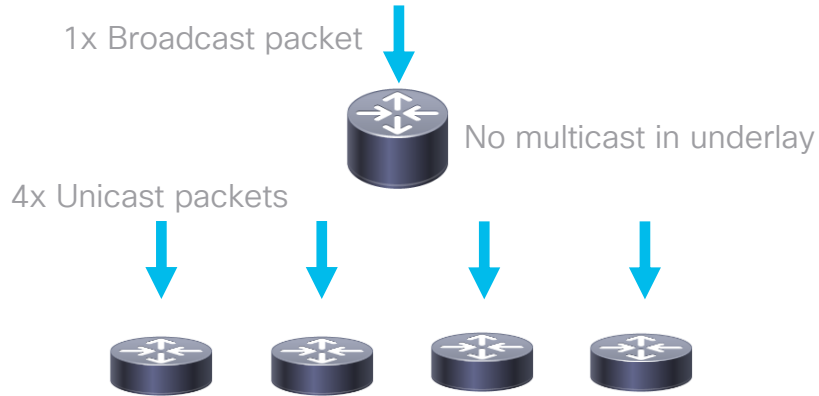


VXLAN Data Plane



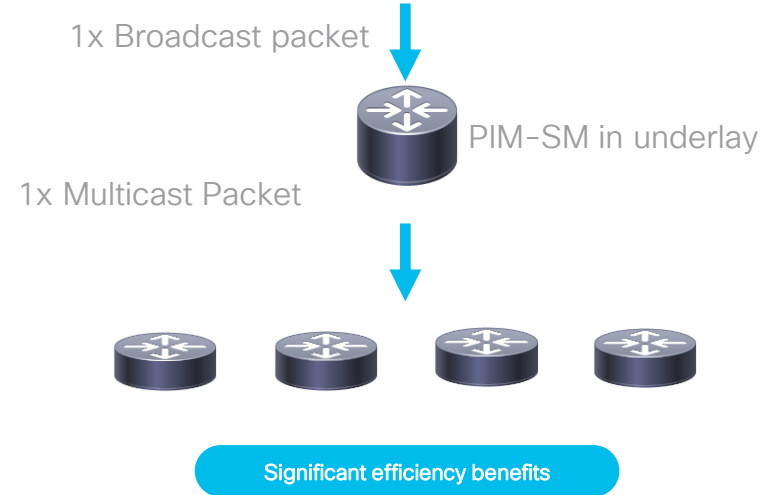
Layer 2 BUM Domain

Ingress Replication



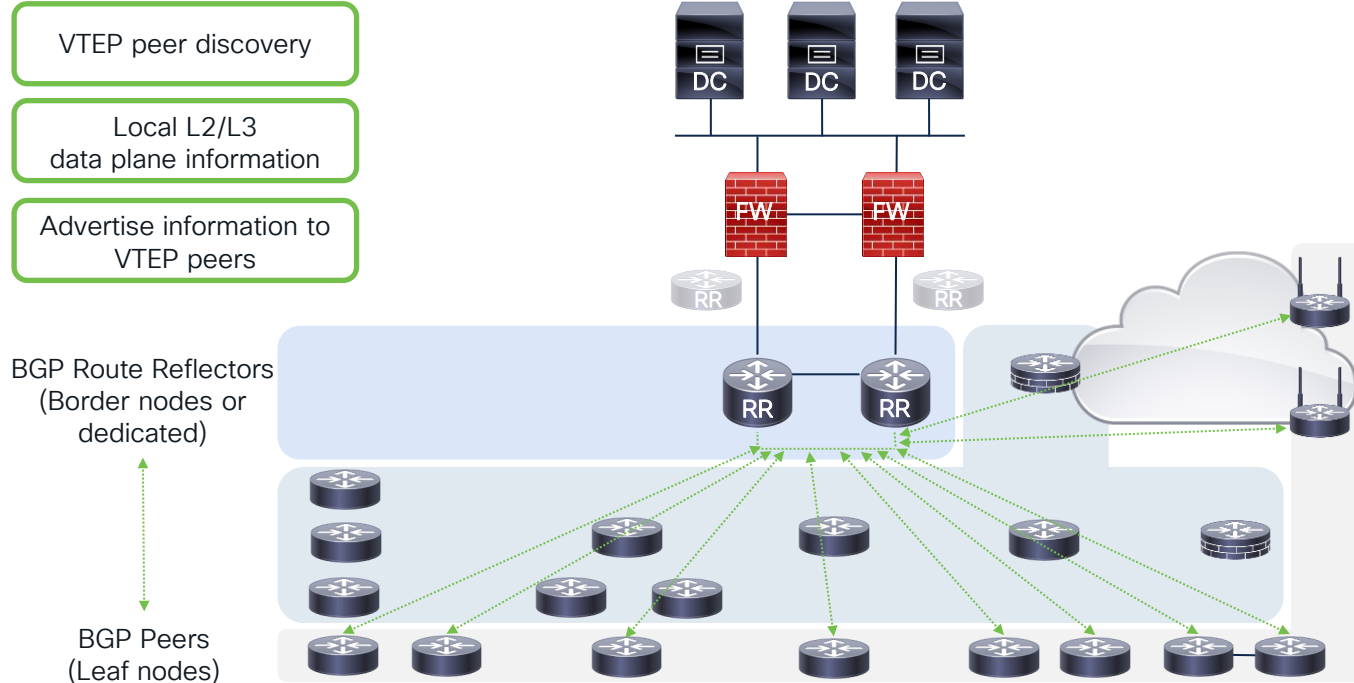
Ingress-Replication: Convert each BUM packet to **multiple** unicast packets and transmit to each remote VTEP

Multicast/Static Replication



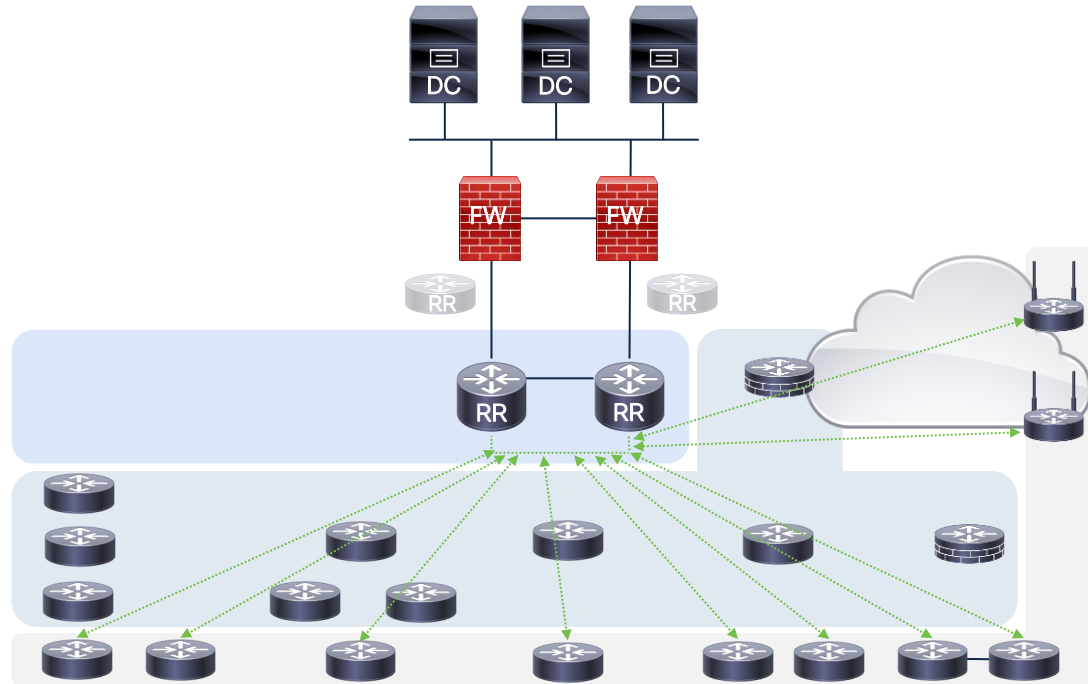
Multicast-Replication: Convert each BUM packet to **single** multicast packet and transmit in underlay network

EVPN Control Plane - MP-BGP

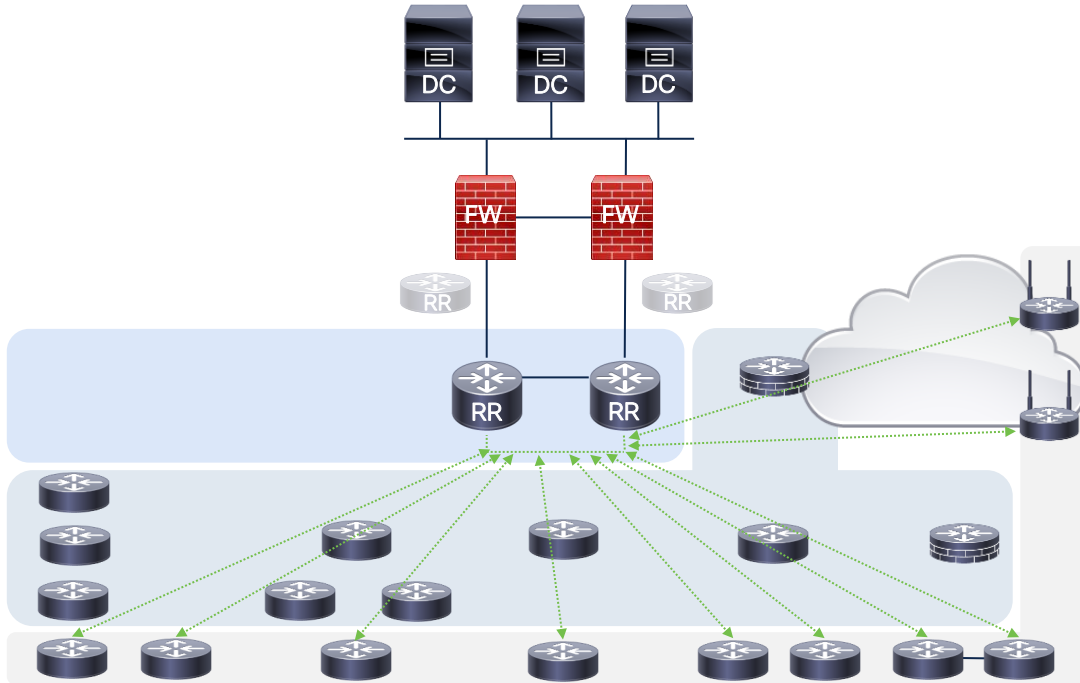


- ✓ Single ASN (iBGP)
- ✓ Loopbacks for peering
- ✓ Default timers
- ✓ MD5 authentication

EVPN Control Plane



EVPN Control Plane



MP-BGP EVPN NLRI

Route	What it carries	Use case
Type 1	Ethernet segment identifier	Multihomed endpoints
Type 2	MAC, VNI, IP	MAC address reachability
Type 3	VNI/VTEP association	Assists with BUM flooding
Type 4	Multicast information	Multicast DF election on multihomed segments
Type 5	IP prefix, L3 VNI	Advertises IP prefixes
Type 6	Multicast group membership info	Restricts multicast to interested hosts

CISCO *Live!*



Sample Configuration – EVPN Data Plane

L2/L3 Interface Configuration

```
interface Vlan10
no ip address
service instance 1 ethernet
encapsulation dot1q 10
rewrite ingress tag pop 1 symmetric
!
vrf definition VRF_BLUE
rd 65000:100
address-family ipv4
route-target export 65000:100 stitching
route-target import 65000:100 stitching
exit-address-family
!
interface Loopback100
vrf forwarding VRF_BLUE
ip address 10.100.0.1 255.255.255.255
!
interface BDI100
mac-address beef.0065.0100
vrf forwarding VRF_BLUE
ip unnumbered Loopback100
```

Local L2 access interface

Send/receive prefixes to/from local EVPN RIB

Loopback for core facing BDI

Core facing interface for each local VRF

EVPN Data Plane Configuration

```
l2vpn evpn
replication-type ingress
router-id Loopback1
!
l2vpn evpn instance 1 vlan-aware
encapsulation vxlan
!
bridge-domain 10
member Vlan10 service-instance 1
member evpn-instance 1 vni 10010
!
bridge-domain 100
member vni 65100
!
interface nve1
no ip address
source-interface Loopback1
host-reachability protocol bgp
member vni 10010 ingress-replication
member vni 65100 vrf VRF_BLUE
```

EVPN instance

L2VNI

L3VNI

Network Virtualisation Endpoint interface

Sample Configuration – EVPN Control Plane

Route Reflector Configuration

```
router bgp 65000
  bgp listen range 10.10.0.0/22 peer-group RRC
  neighbor RRClient peer-group
  neighbor RRClient remote-as 65000
  neighbor RRClient transport connection-mode passive
  neighbor RRClient route-reflector-client
  neighbor RRClient update-source Loopback1
  neighbor RRClient password cisco123
!
address-family I2vpn evpn
  neighbor RRClient activate
  neighbor RRClient send-community both
  exit-address-family
!
```

Dynamic peering

EVPN SAFI

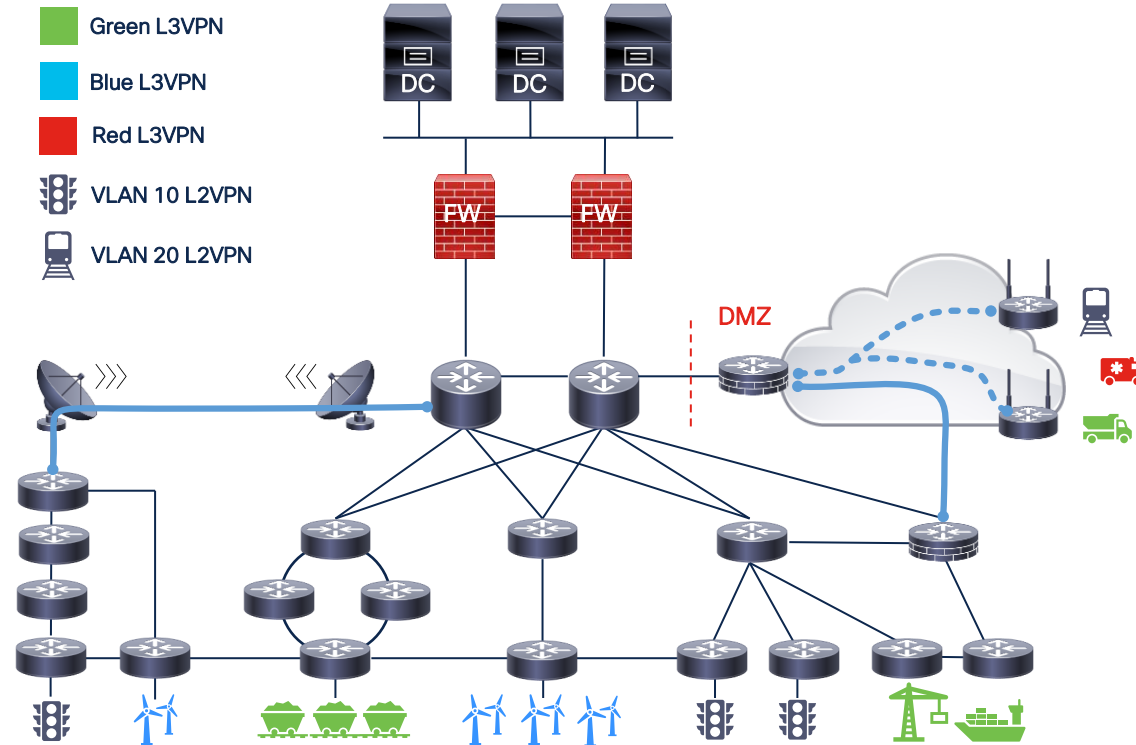
Border/Leaf Configuration

```
router bgp 65000
  neighbor RR peer-group
  neighbor RR remote-as 65000
  neighbor RR update-source Loopback1
  neighbor RR password cisco123
  neighbor 10.10.1.1 peer-group RR
  neighbor 10.10.1.2 peer-group RR
!
address-family I2vpn evpn
  neighbor RR activate
  neighbor RR send-community both
  exit-address-family
!
address-family ipv4 vrf VRF_BLUE
  advertise I2vpn evpn
  redistribute connected
  exit-address-family
!
```

EVPN SAFI

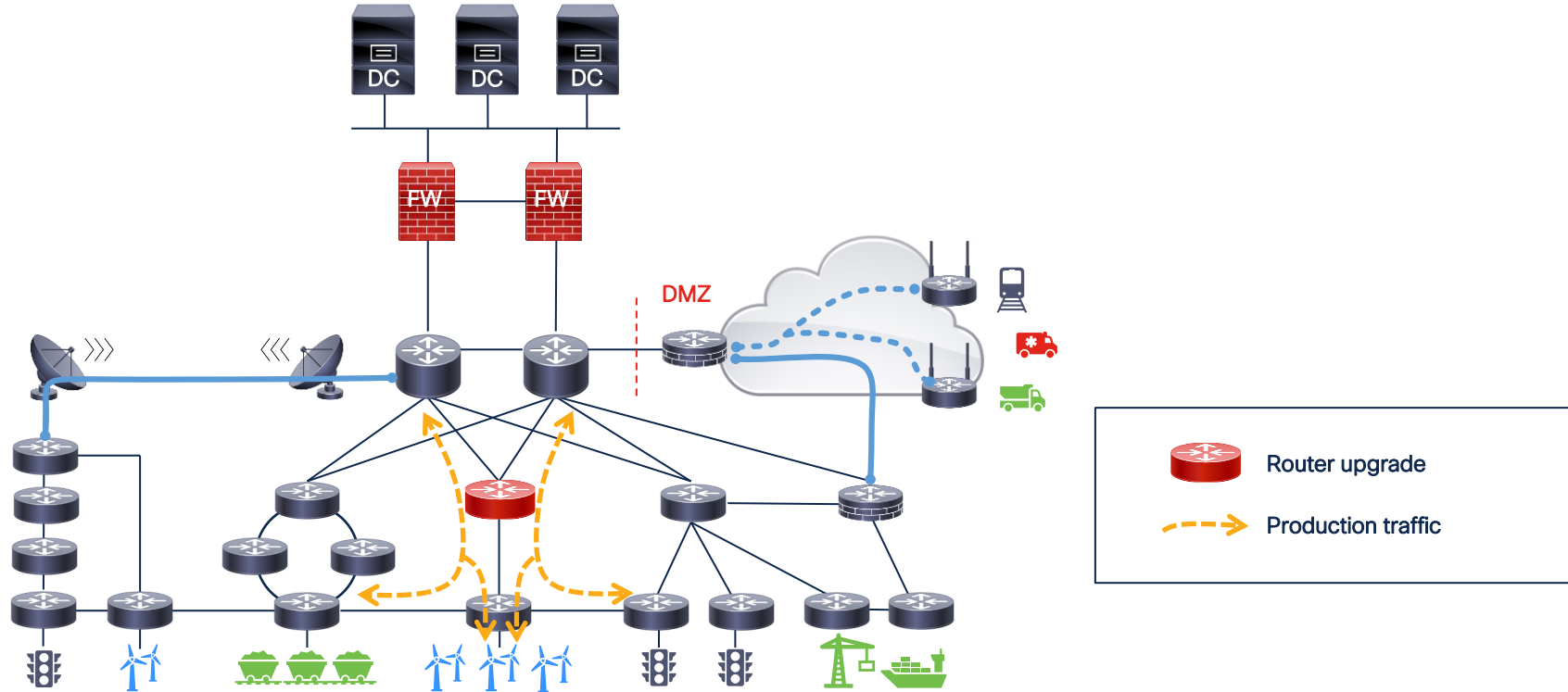
Send VRF routes to EVPN SAFI

EVPN-VXLAN Fabric

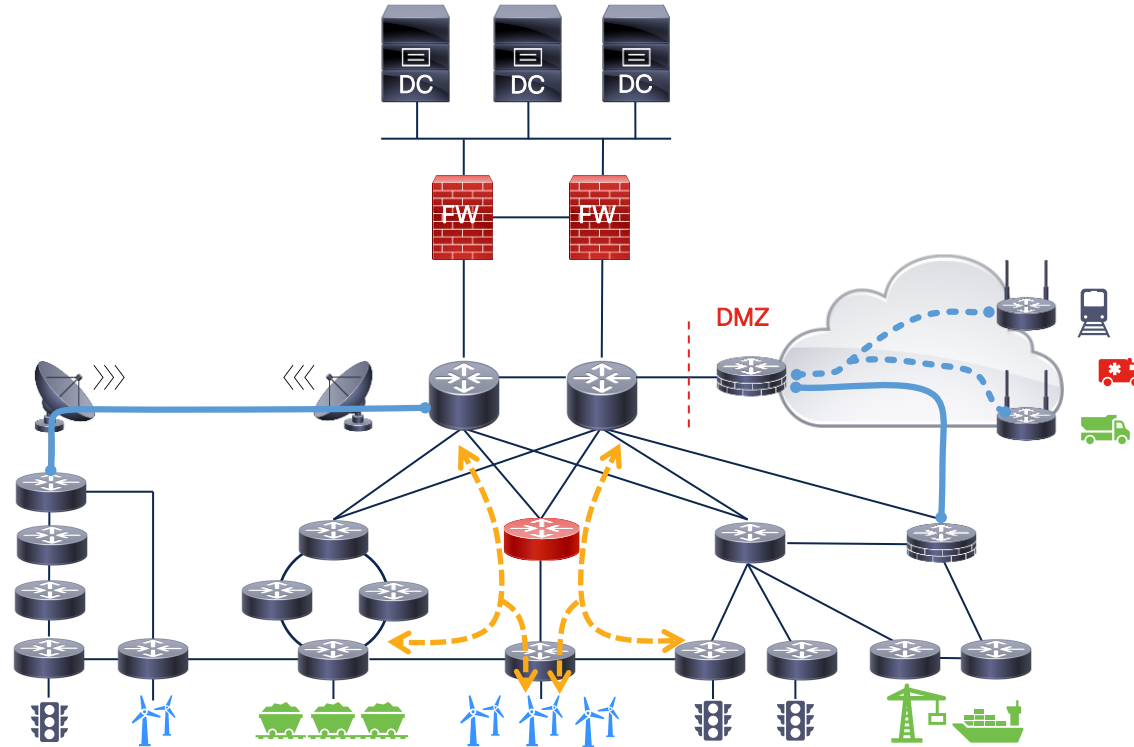


- ✓ End-to-end layer 3 underlay for stability
- ✓ Integrated L2/L3 services
- ✓ Isolated fault domains
- ✓ Fast convergence and ECMP
- ✓ Secured over public networks
- ✓ Simplified firewall deployment
- ✓ Ease of operation and troubleshooting

EVPN-VXLAN Fabric - Example Maintenance



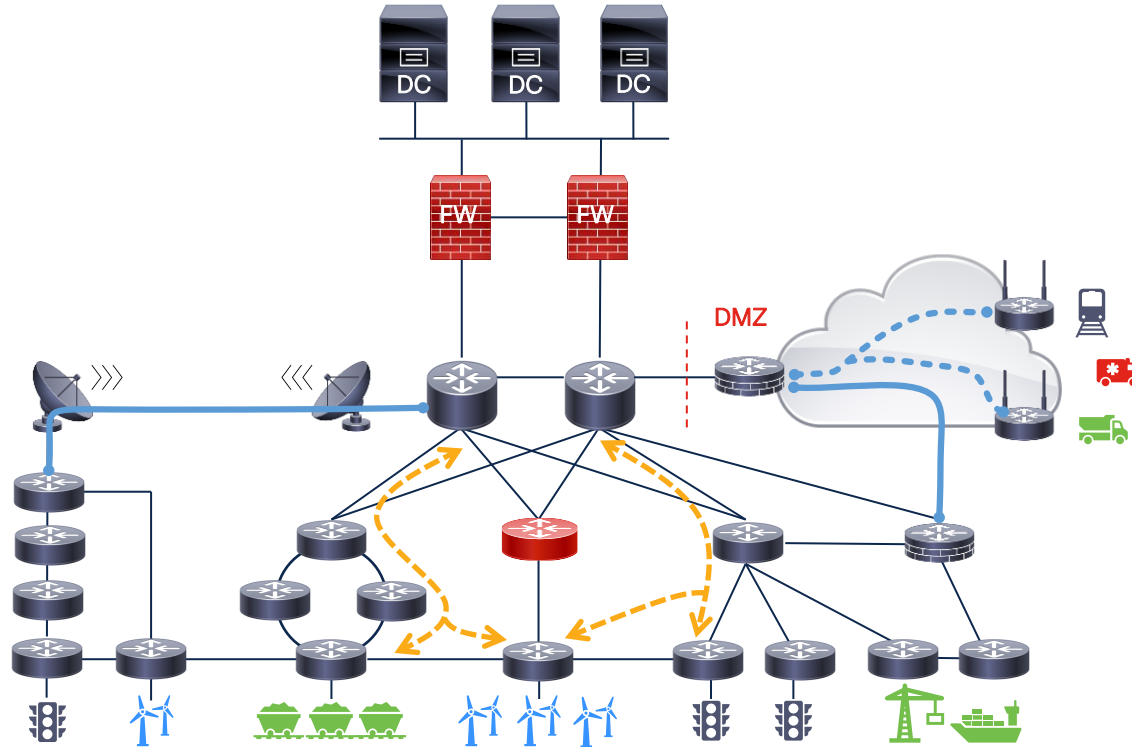
EVPN-VXLAN Fabric - Example Maintenance



1. Gracefully remove router from underlay:

```
router ospf 1
max-metric router-lsa
wr mem
```

EVPN-VXLAN Fabric - Example Maintenance

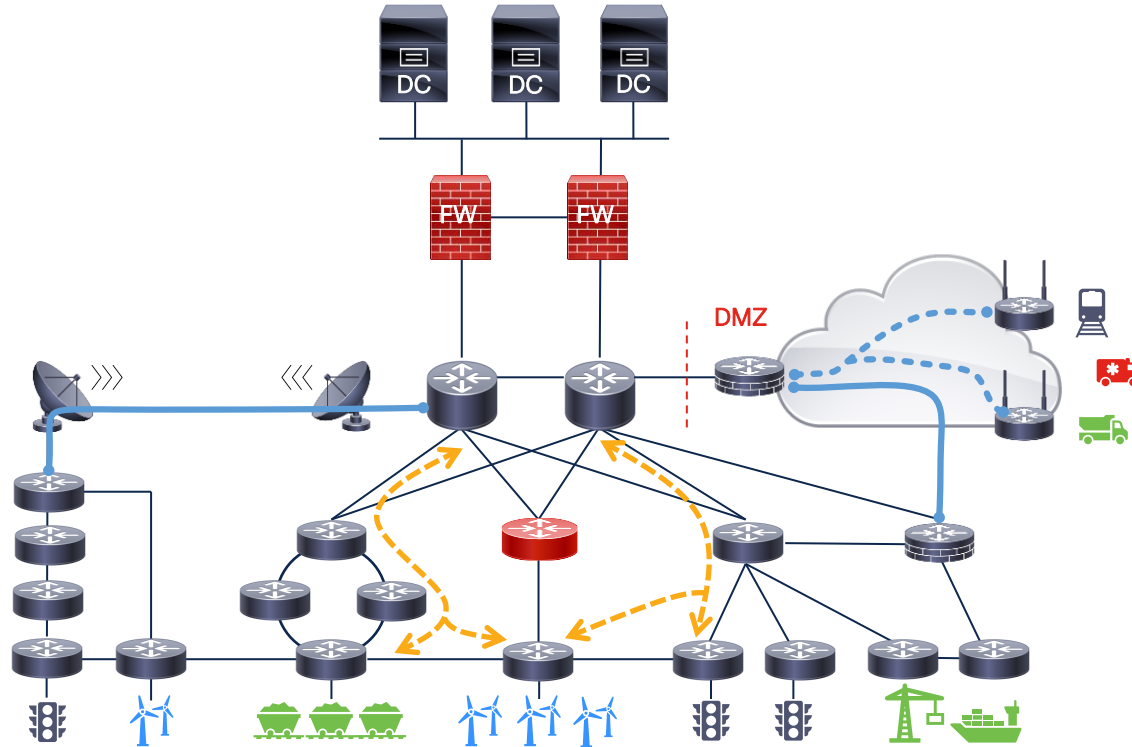


1. Gracefully remove router from underlay:

```
router ospf 1  
max-metric router-lsa  
wr mem
```

2. Confirm router removed from traffic path.

EVPN-VXLAN Fabric - Example Maintenance

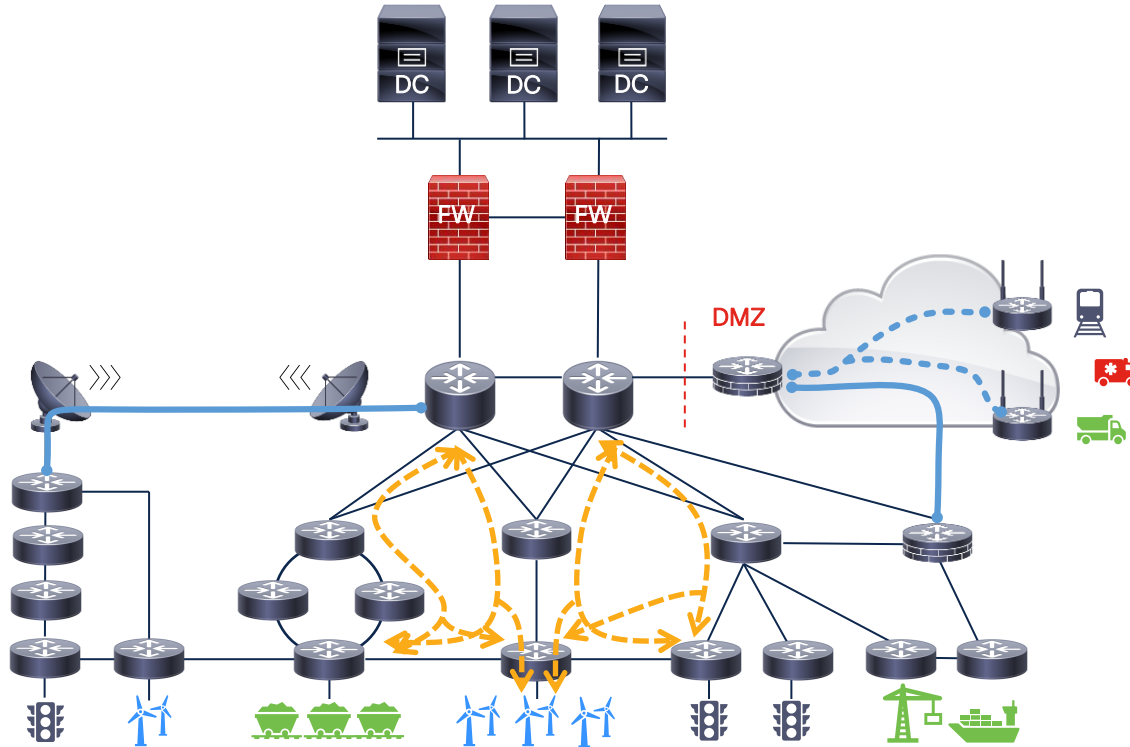


1. Gracefully remove router from underlay:

```
router ospf 1  
max-metric router-lsa  
wr mem
```

2. Confirm router removed from traffic path.
3. Upgrade router and confirm success.

EVPN-VXLAN Fabric - Example Maintenance



1. Gracefully remove router from underlay:

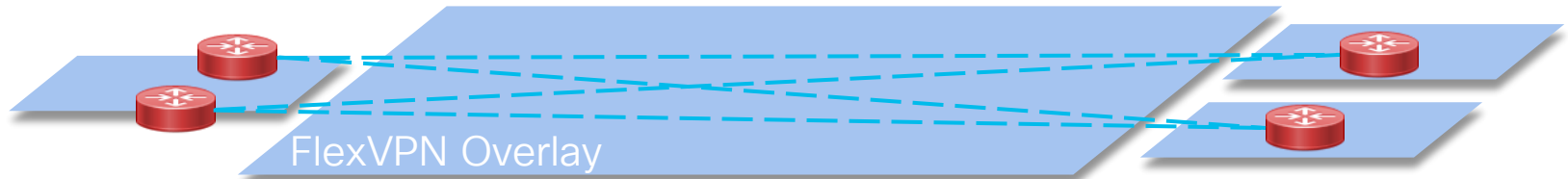
```
router ospf 1  
max-metric router-lsa  
wr mem
```

2. Confirm router removed from traffic path.
3. Upgrade router and confirm success.
4. Return router to service.

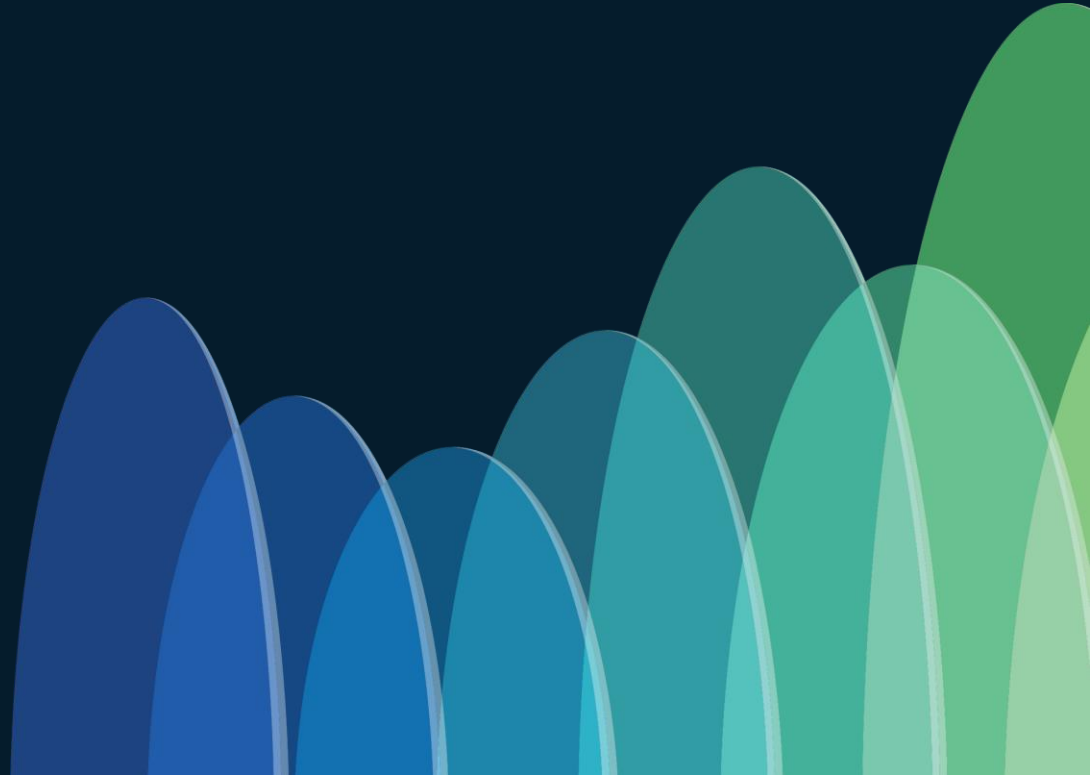
```
router ospf 1  
no max-metric router-lsa  
wr mem
```

EVPN – FAQ

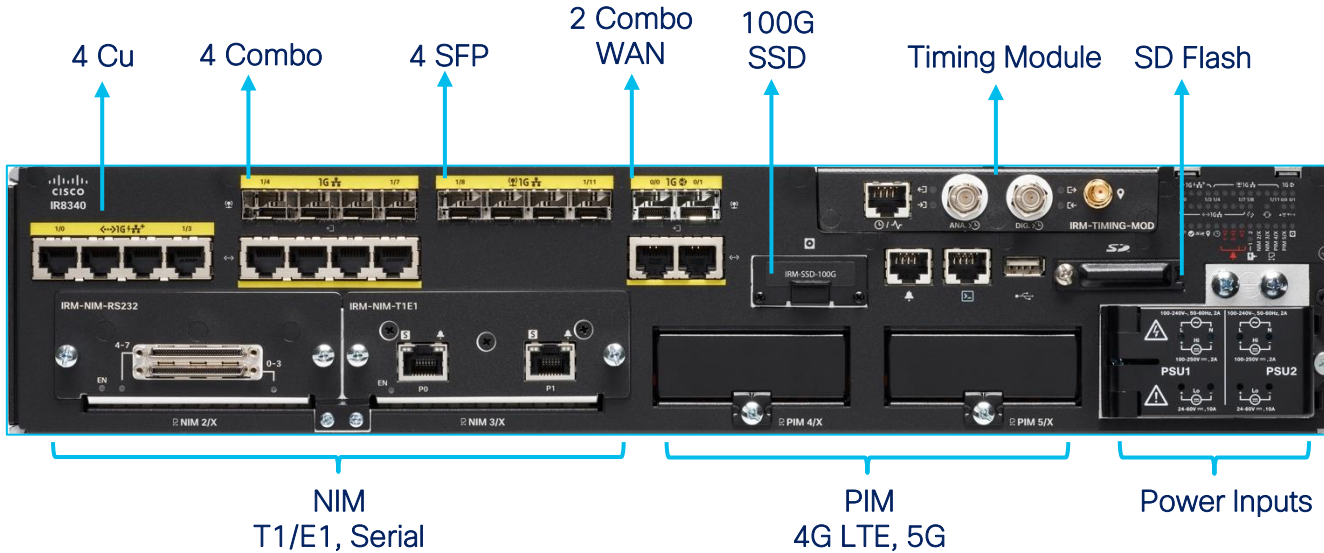
- Does EVPN replace traditional MPLS L3VPNs and VPLS ?
 - *It can. EVPN does not require an LDP/RSVP control plane. VPLS is a flood and learn technology with L2 network limitations (e.g. STP for multihoming).*
- How does EVPN compare to SD-Access and SD-WAN ?
 - *These are all fabric technologies providing L2/L3 services however are optimised for different deployment scenarios. There is no central "controller" for EVPN.*
- Do I just throw away all my switches ?
 - *These devices still have a role to play in the underlay (L3) and access layers (L2).*



Hardware Platforms



IR 8340 Router



Underlay



FlexVPN HER



FlexVPN Spoke



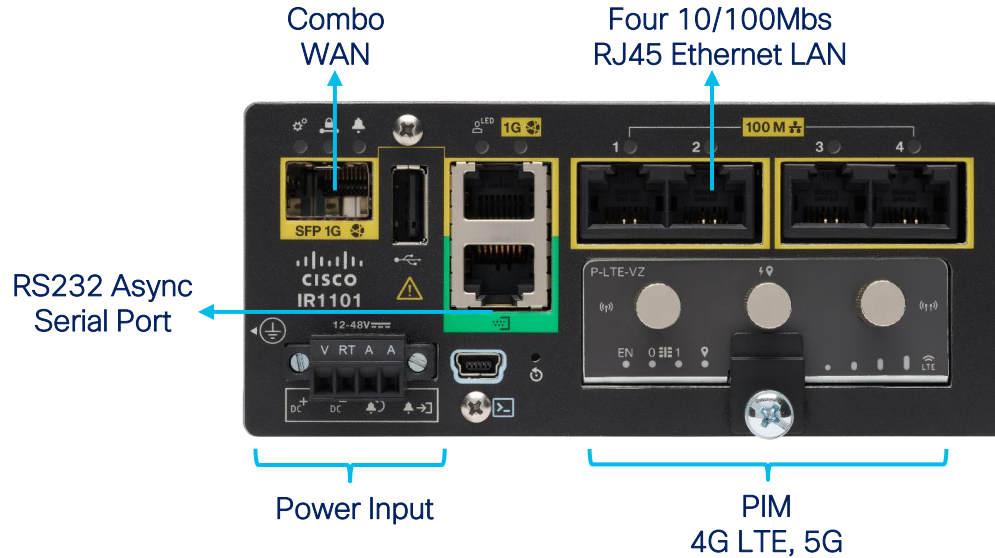
EVPN Border/Leaf



EVPN RR

cisco *Live!*

IR1101 Router



Underlay



FlexVPN HER



FlexVPN Spoke



EVPN Border/Leaf



EVPN RR

IR1101 Modularity

IR1101 + single
Expansion Module



OR



Majority of use
cases

IR1101 + LTE Expansion
Module + Serial
Expansion Module
(Bottom)



Ethernet ports on
bottom expansion
module disabled

IR1101 + Serial
Expansion Module + LTE
Expansion Module
(Bottom)



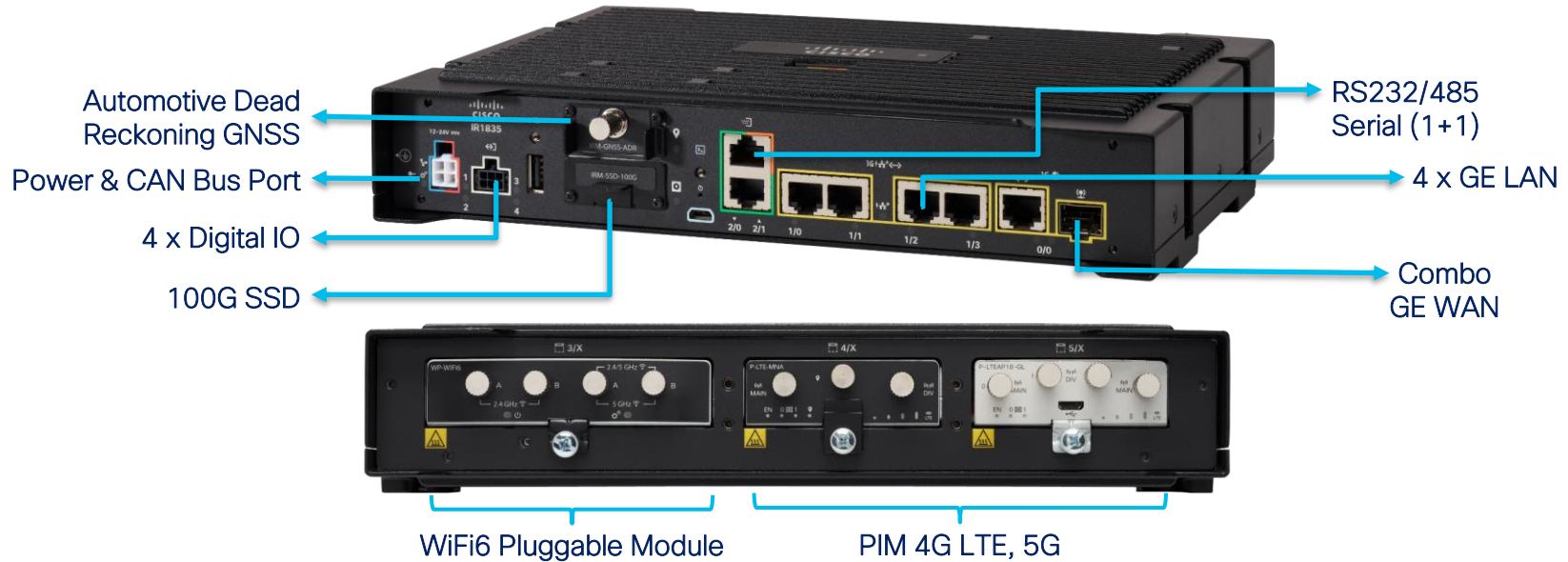
SFP on the expansion
module disabled

IR1101 + 2x Serial
Expansion



Ethernet ports on
bottom expansion
module disabled

Catalyst IR1800 Series Router



Underlay



FlexVPN HER



FlexVPN Spoke



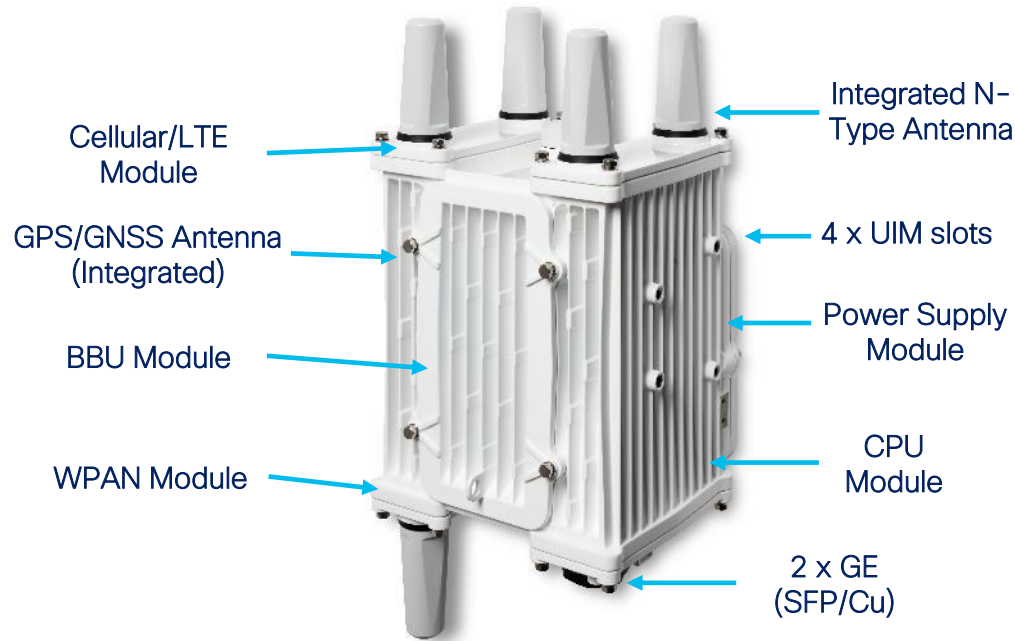
EVPN Border/Leaf



EVPN RR

CISCO *Live!*

IR8140H Heavy Duty Router



Underlay



FlexVPN HER



FlexVPN Spoke



EVPN Border/Leaf



EVPN RR

Industrial Switching



IE-3300, IE-3300X



IE-4010, IE-5000



IE-3400, IE-3400H



IE-9310, IE-9320



Underlay



FlexVPN HER



FlexVPN Spoke



EVPN Border/Leaf



EVPN RR

Cisco Catalyst 8000 Edge Platform

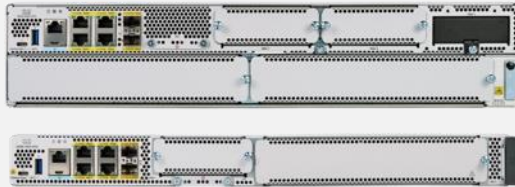


Hypervisor/Cloud

Catalyst 8000V



Catalyst 8500
Catalyst 8500L



Catalyst 8300



Controlled Environments

Controlled Environments



Underlay



FlexVPN HER



FlexVPN Spoke



EVPN Border/Leaf



EVPN RR

cisco *Live!*

Cisco Catalyst 9000 Switches

Controlled Environments



Catalyst 9600



Catalyst 9500



Catalyst
9300/9400*

*Catalyst 9300X and 9400X also support IKEv2 IPSec



Controlled Environments



Underlay



FlexVPN HER



FlexVPN Spoke



EVPN Border/Leaf



EVPN RR

Hardware Platforms - FAQ

- How many tunnels/VTEPs/routes/MAC addresses etc. does each platform support ?
 - *Varies between platforms, software releases and what other features are configured. A single device can perform underlay, FlexVPN and EVPN functions.*
- Is EVPN interoperable between platforms ?
 - *Yes, however the syntax is slightly different between the routing platforms and the Catalyst 9000 switching platform.*
- This sounds like a lot of work. Is there a tool I can use for zero touch provisioning and configuration management ?
 - *Yes, Cisco Catalyst Center VM or appliance.*

The Next Step - Software Defined Segmentation

Traditional Security Policy

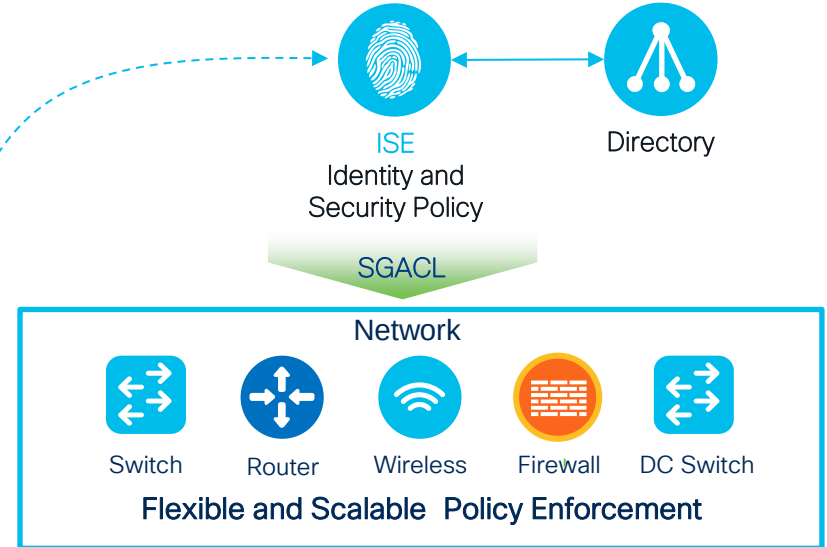


TrustSec Security Policy

Source	Destination			
	Packaging Line PLC	HMI	Site Historian	SCADA Server
Packaging Line PLC	✓	✗	✓	✗
HMI	✗	✓	✗	✓
Site Historian	✓	✗	✓	✓
SCADA Server	✗	✓	✓	✓

Scalable Group Tags

- Policy enforcement at edge in silicon
- Remove firewall dependency for segmentation
- Improved security efficacy, operations
- Macro and micro segmentation

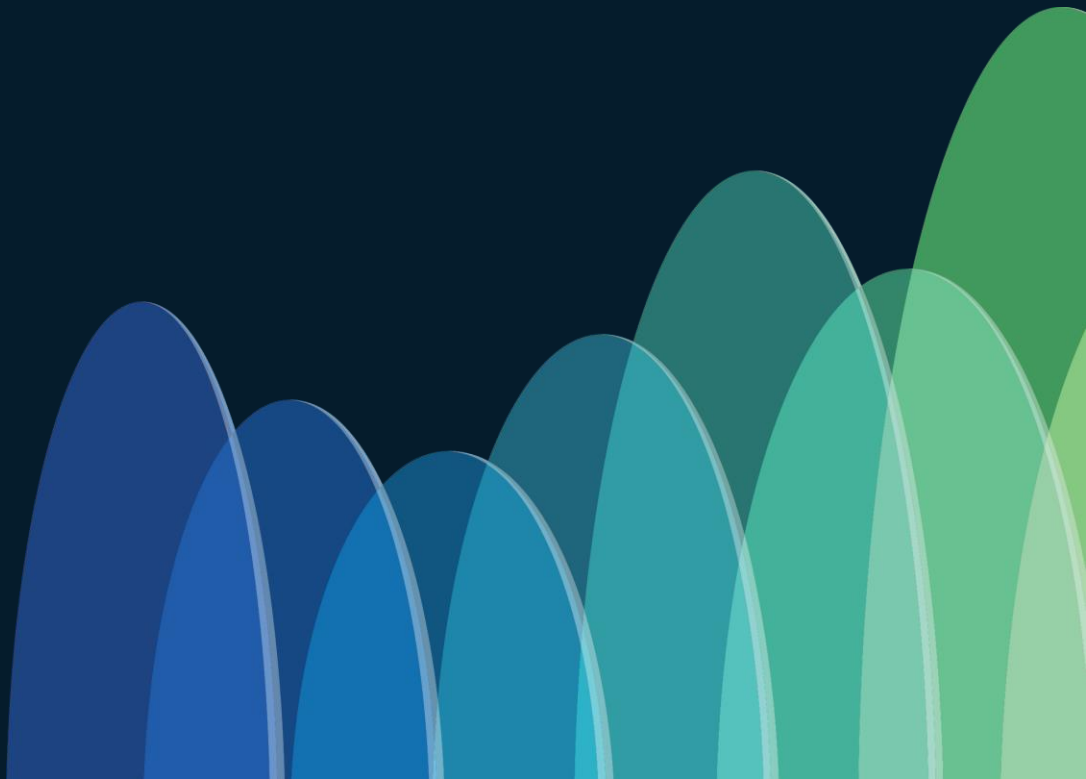


The OSI Model in Reality





Questions?



Cisco Webex App

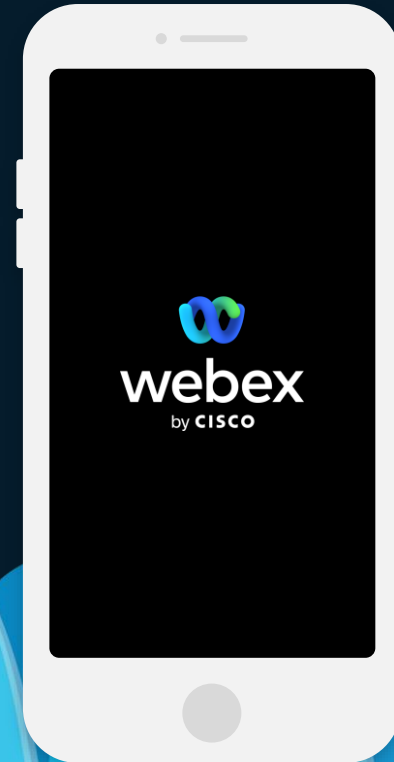
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live 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 November 15, 2024.



Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: cadry@cisco.com



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC