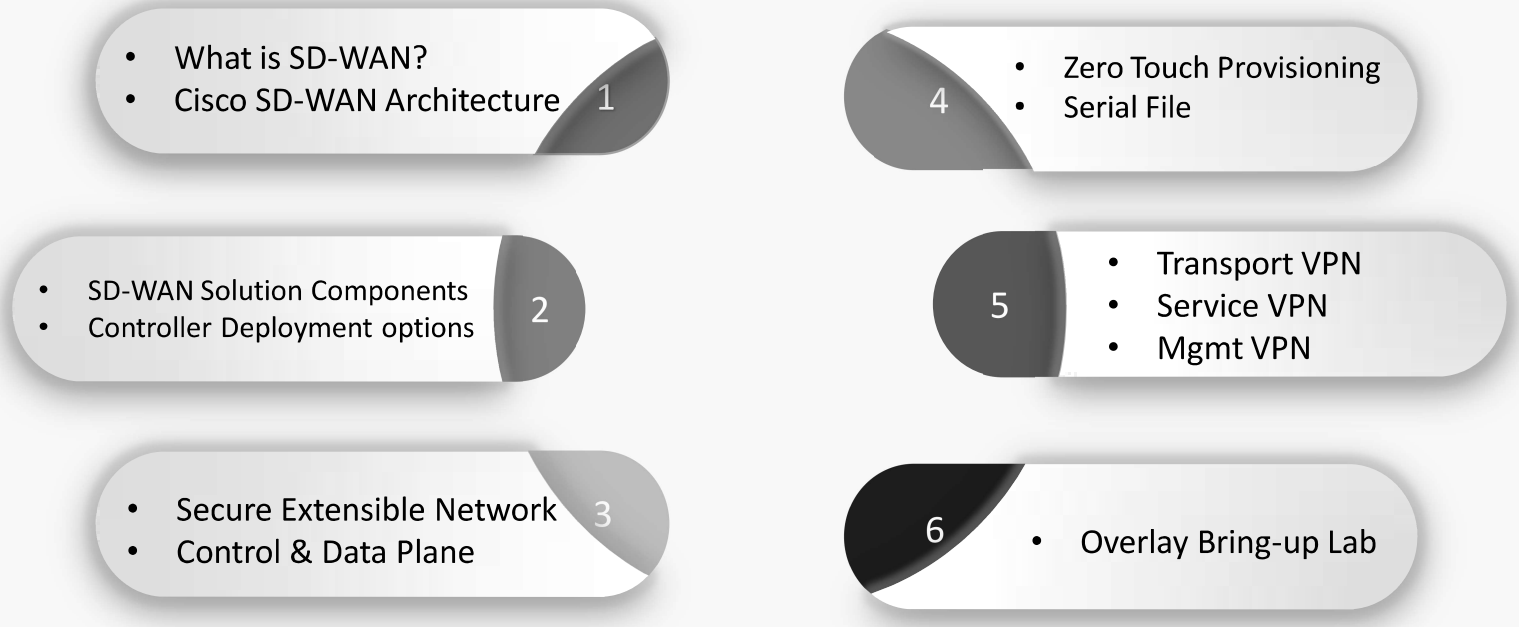
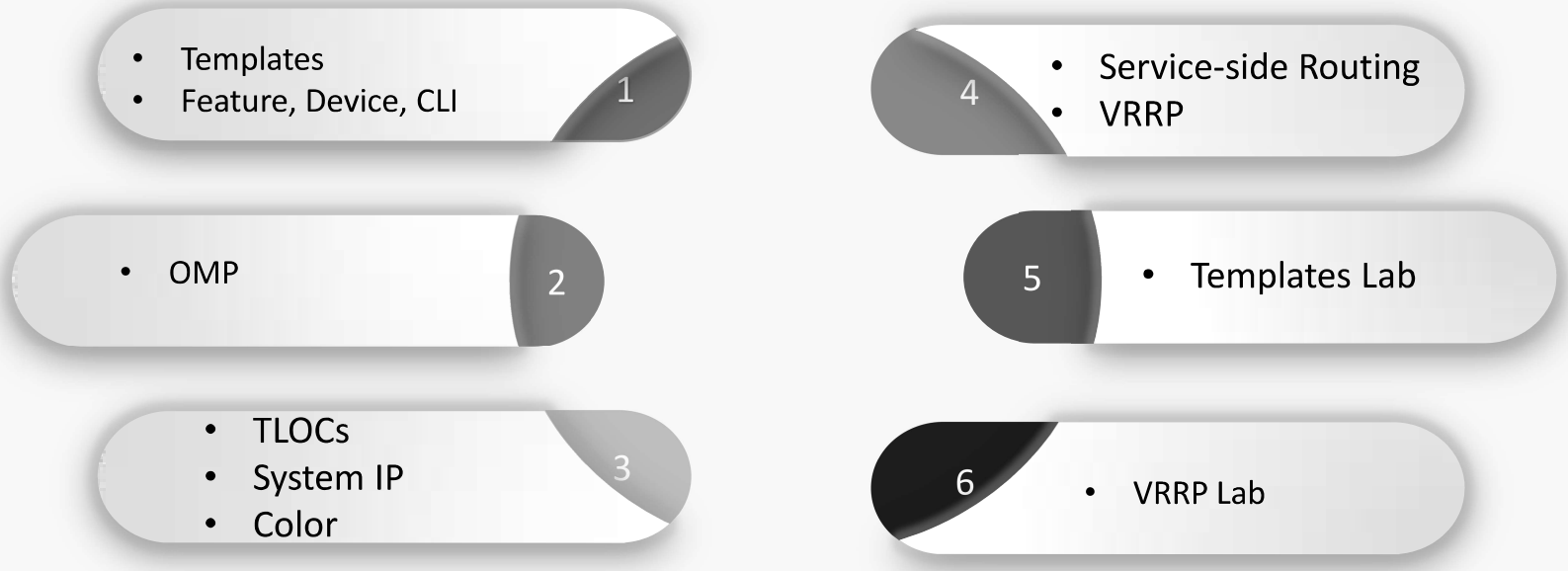
CISCO SD-WAN (Viptela) Training

Cisco SD-WAN 5-Day Training Agenda

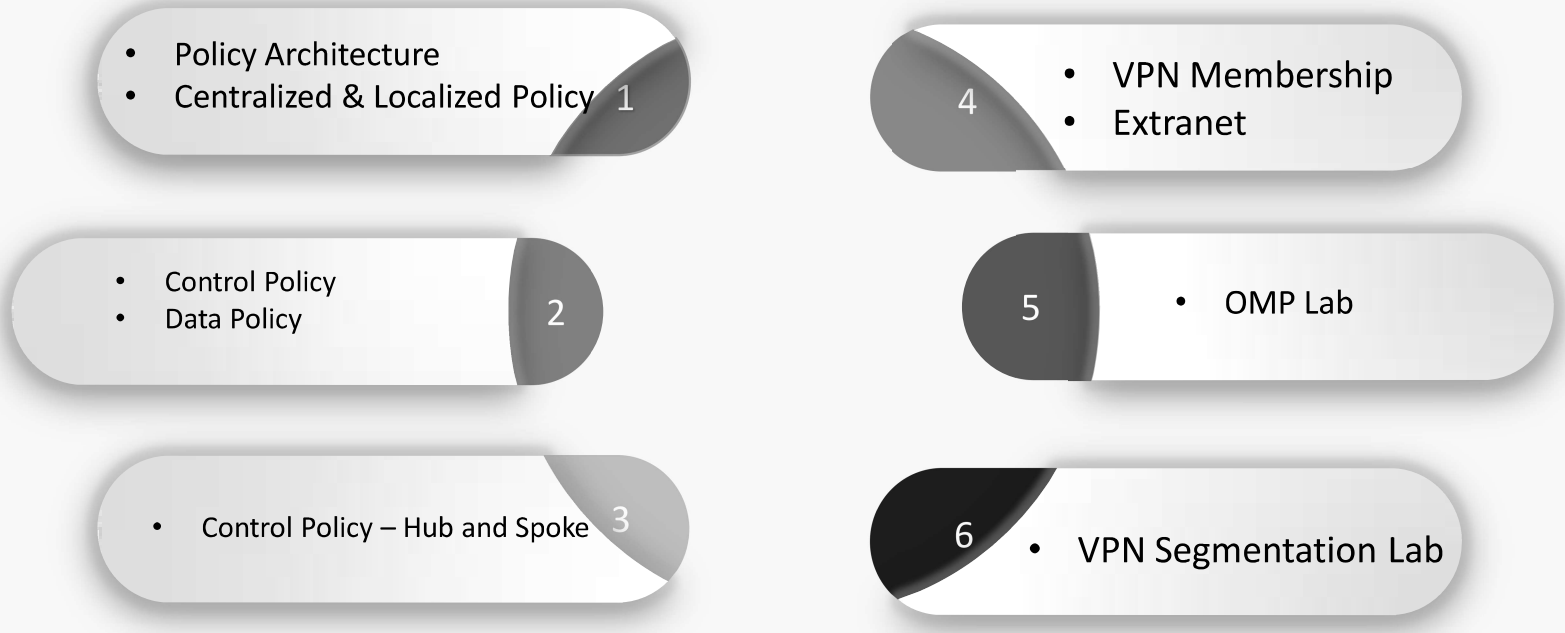
Cisco SD-WAN Training - Day1



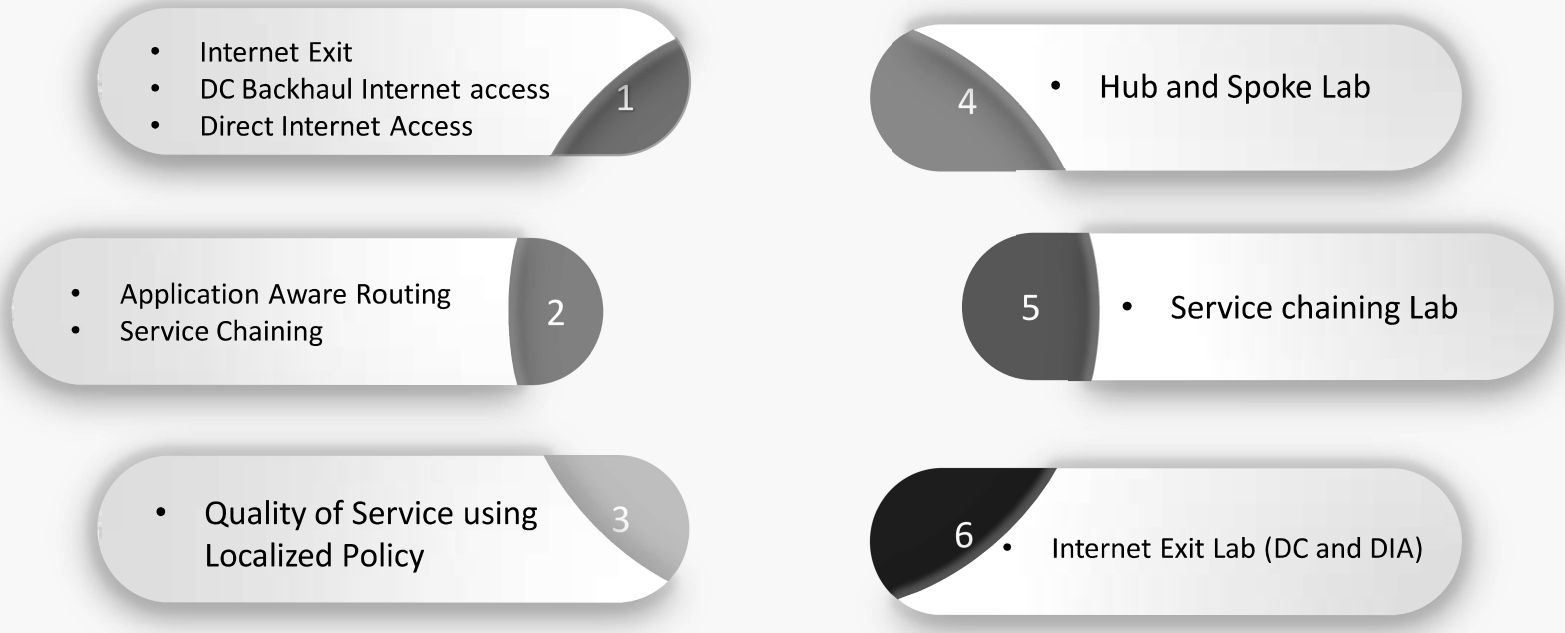
Cisco SD-WAN Training – Day2



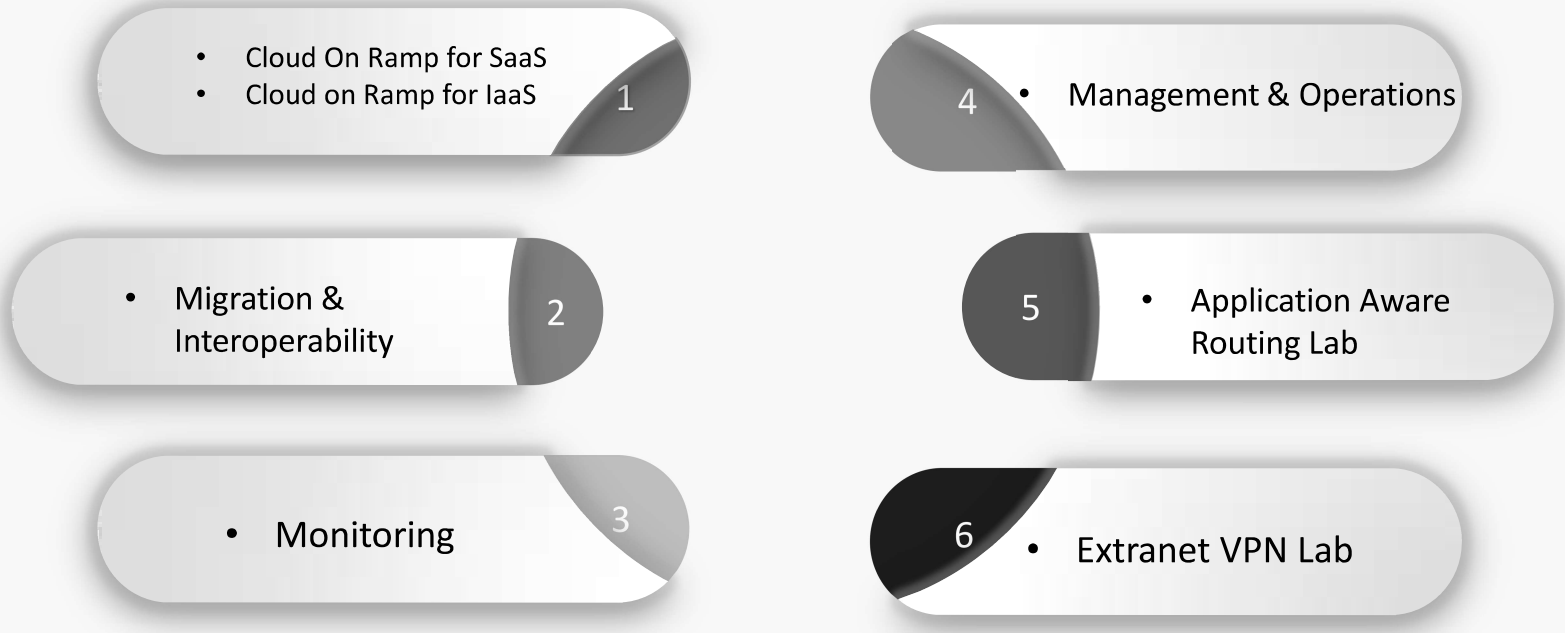
Cisco SD-WAN Training – Day3



Cisco SD-WAN Training – Day4



Cisco SD-WAN Training – Day5



References

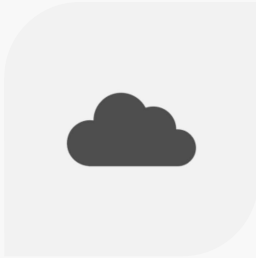
- Cisco Documentation
- https://sdwan-docs.cisco.com/Product_Documentation
- CiscoLive
- Cisco.com/go/sdwan
- Cisco SD-WAN Routing Matrix
- ENSDWI Exam Topics
- https://learningnetwork.cisco.com/s/ensdwi-exam-topics

Participants Introduction

NAME

COMPANY

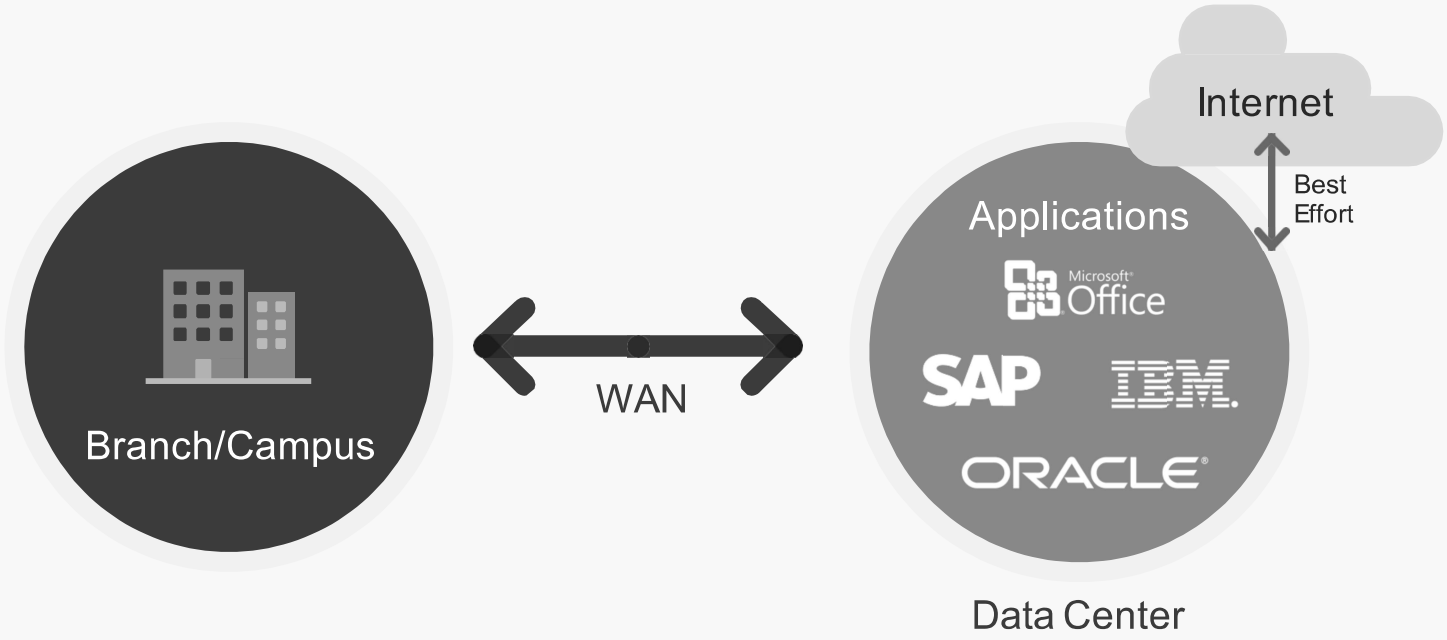
TEAM



EXPOSURE TO CISCO SD-WAN?

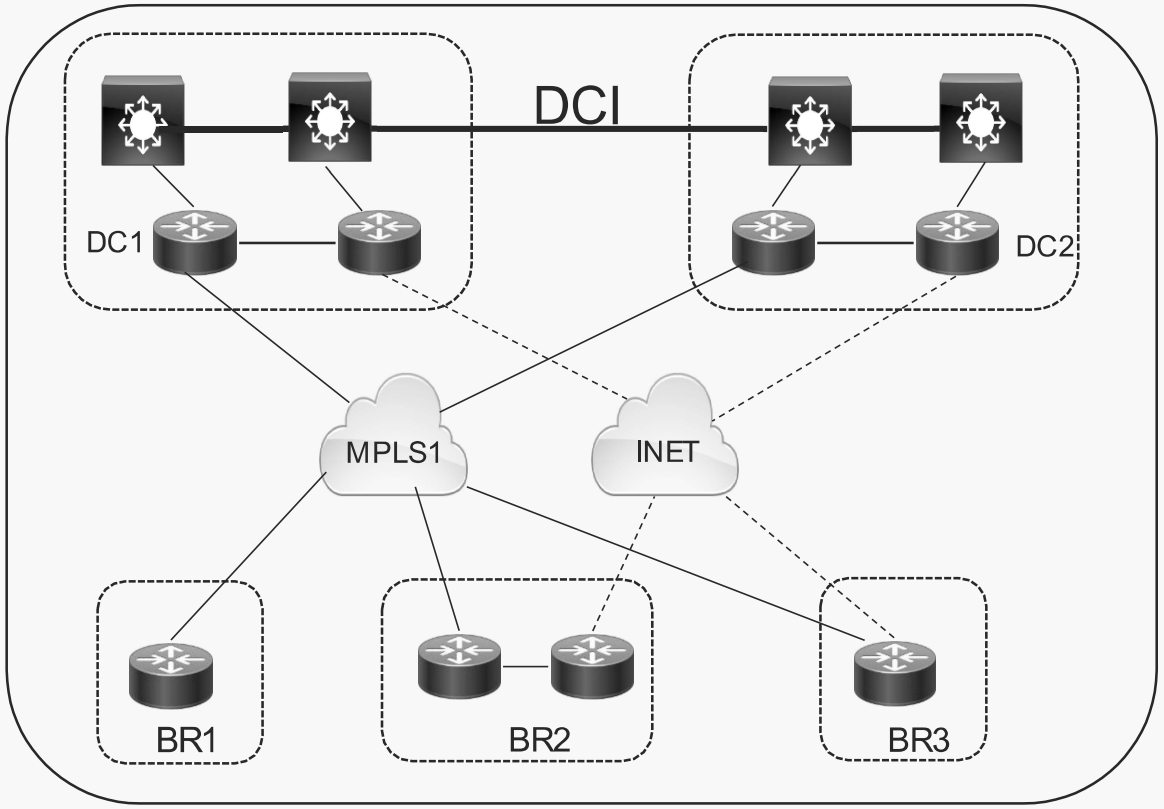
Current WAN

Connecting Users to Data Centers was the Priority



Traditional WAN Architecture

- Two or more circuits
- All MPLS, or, MPLS and INET/LTE
- Active/Standby Redundancy
- Internet/SaaS access backhauled via DC



Then the Way We Worked Changed

Applications Moving to Not One Cloud, But Many

Challenges with Traditional WAN

What is SD-WAN?

What is SD-WAN?

- Must Support multiple connection(transports) types
  - MPLS, Internet, LTE …
- Dynamic Path Selection
  - Load sharing on multiple links. Path selection for Apps based on the SLA
- Simple interface for Managing the WAN
  - Single UI, ZTP support, setting up should be easy like home Wi-Fi
- Must support
  - VPNs, Optimization, Firewall and other security

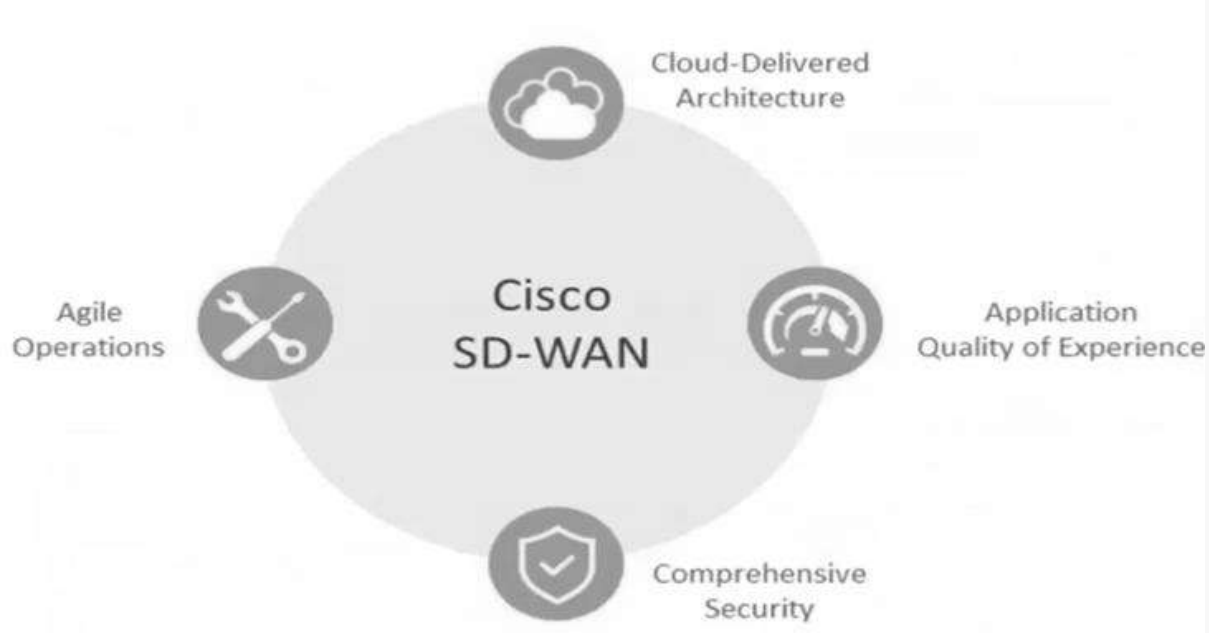
Source: Gartner

The benefits Business is looking for

Prioritize and secure	Prioritize and secure traffic with granular control
Reduce	Reduce costs and lower operational complexity
Augment or replace	Augment or replace premium WAN bandwidth
Provide	Provide a consistent, high-quality user experience
Offload	Offload guest and public cloud traffic
Ensure	Ensure remote site uptime

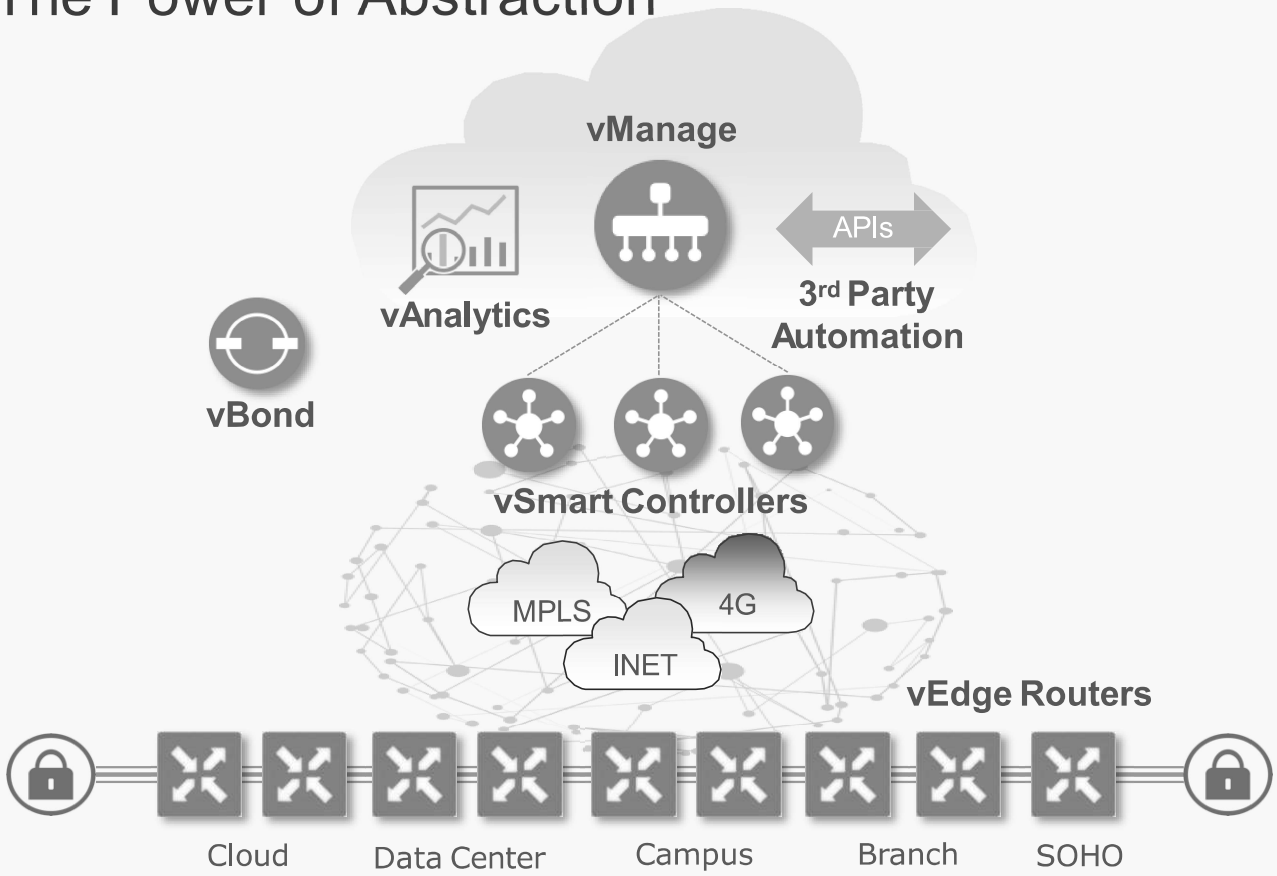
Cisco SD-WAN Architecture

Cisco SD-WAN Solution Pillars



Cisco SD-WAN Architecture

The Power of Abstraction



Orchestration Plane

Management Plane

Control Plane

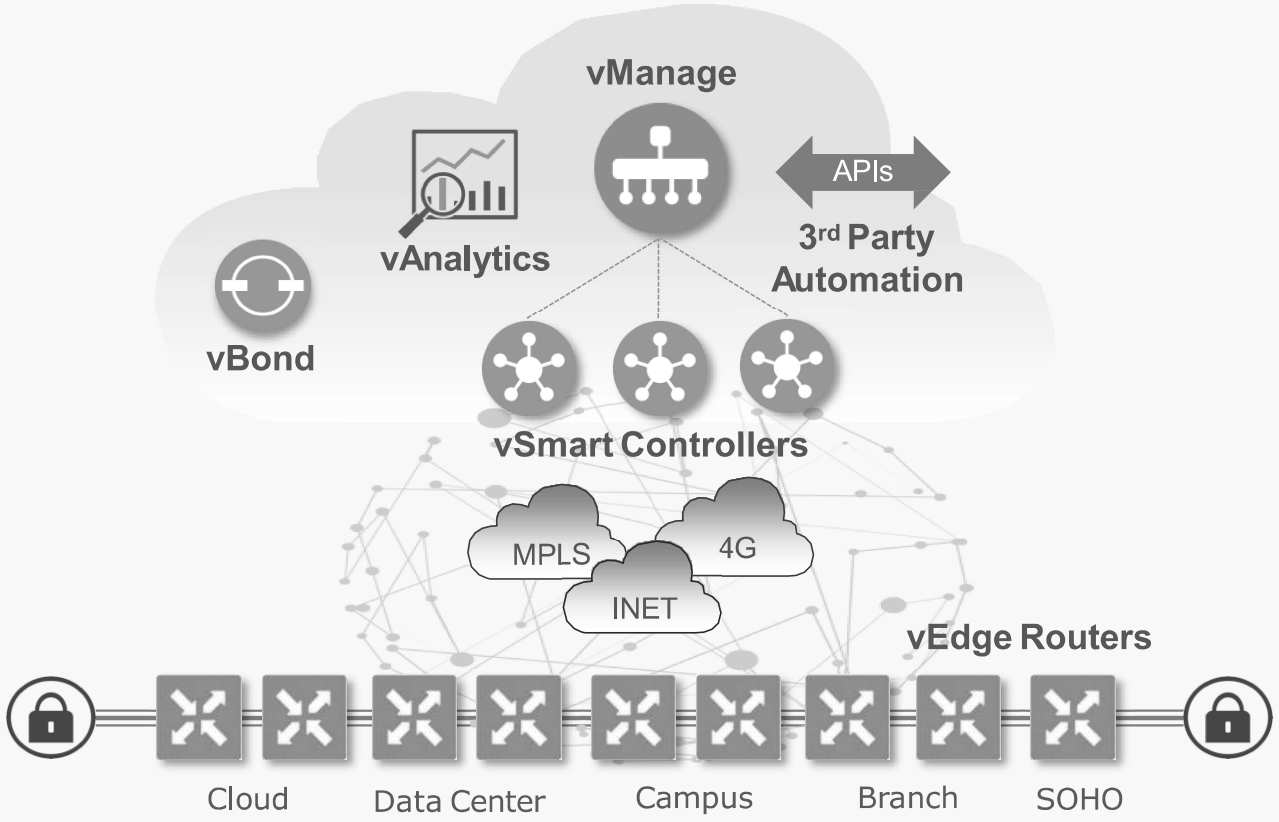
Data Plane

Cisco SD-WAN Solution Components

Management Plane

Cisco vManage

- Single pane of glass for Day0, Day1 and Day2 operations
- Multitenant with web scale
- Centralized provisioning
- Policies and Templates
- Troubleshooting and Monitoring
- Software upgrades
- GUI with RBAC
- Programmatic interfaces (REST, NETCONF)
- Highly resilient

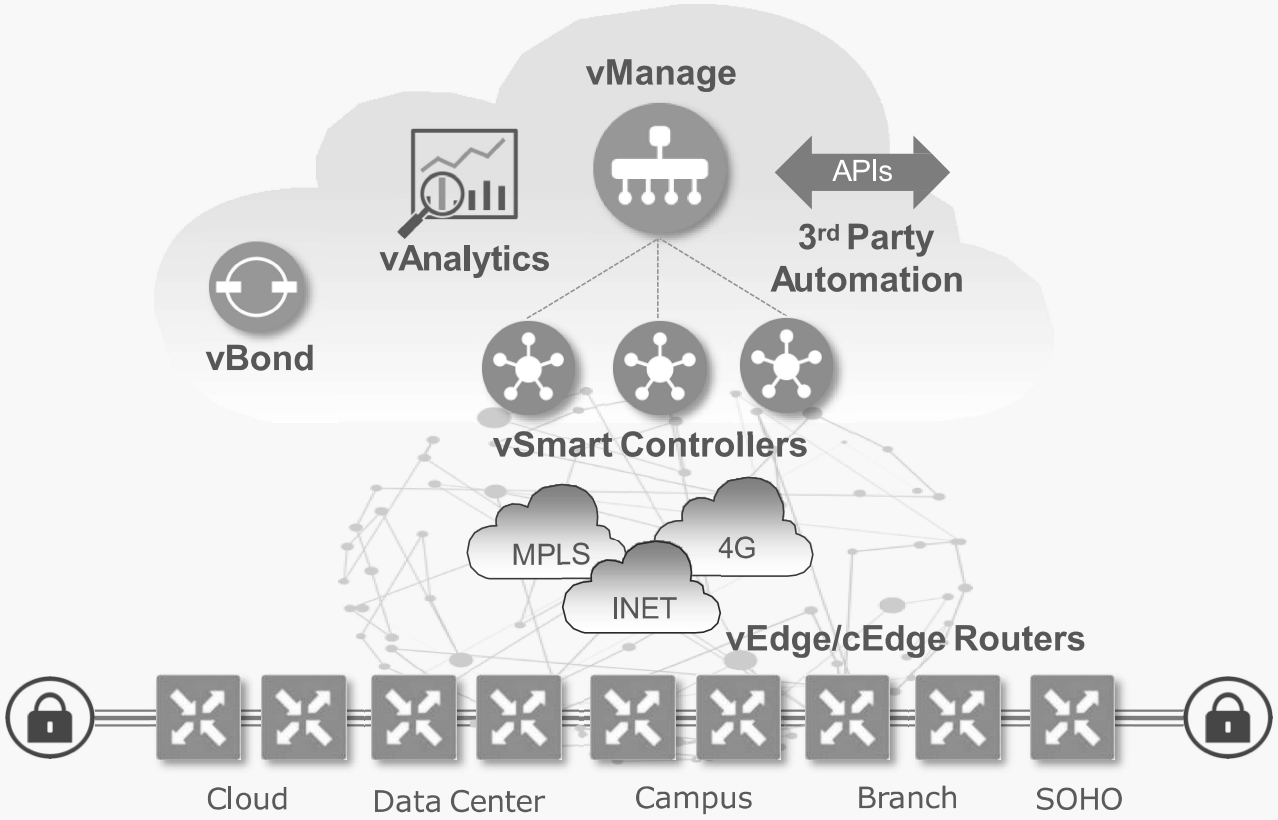


Control Plane

Control Plane

Cisco vSmart

- Facilitates fabric discovery
- Dissimilates control plane information between vEdges
- Distributes data plane and app-aware routing policies to the vEdge routers
- Implements control plane policies, such as service chaining, multi-topology and multi-hop
- Dramatically reduces control plane complexity
- Highly resilient

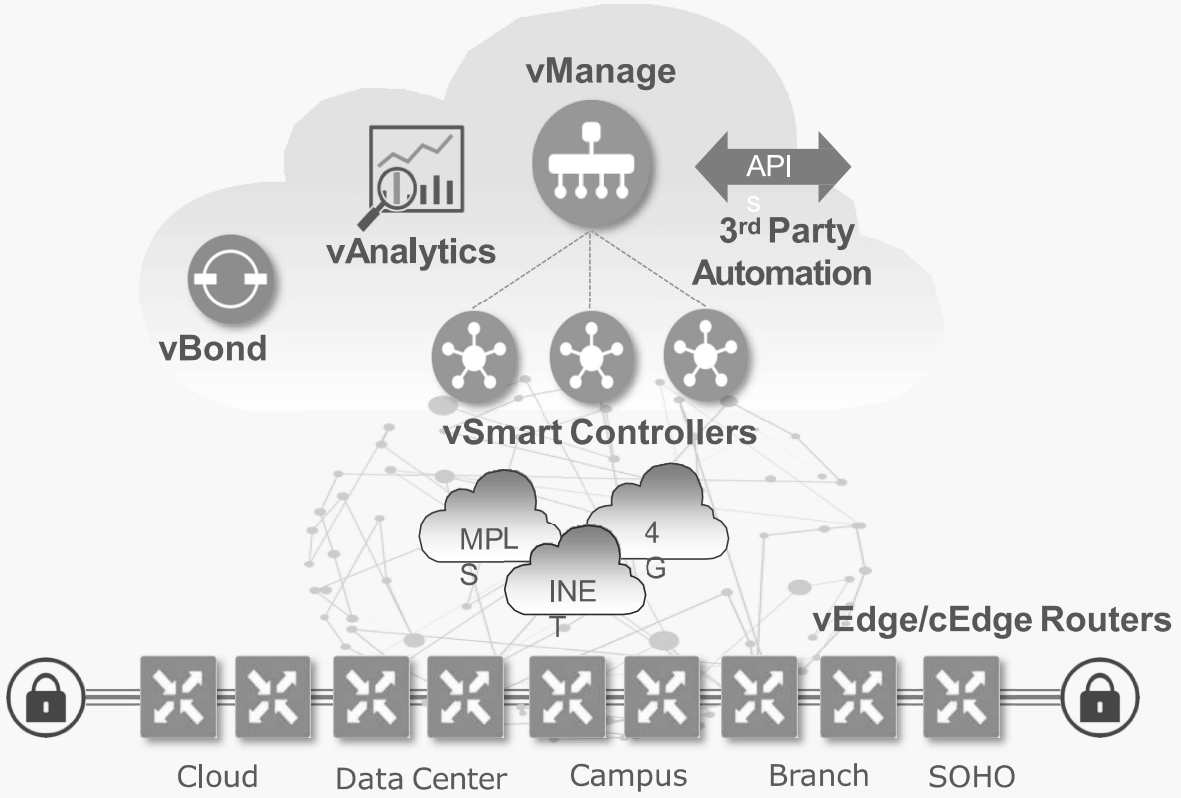


Orchestration Plane

Orchestration Plane

Cisco vBond

- Orchestrates control and management plane
- First point of authentication (white-list model)
- Distributes list of vSmarts/ vManage to all WAN Edge routers
- Facilitates NAT traversal
- Requires public IP Address [could sit behind 1:1 NAT]
- Highly resilient

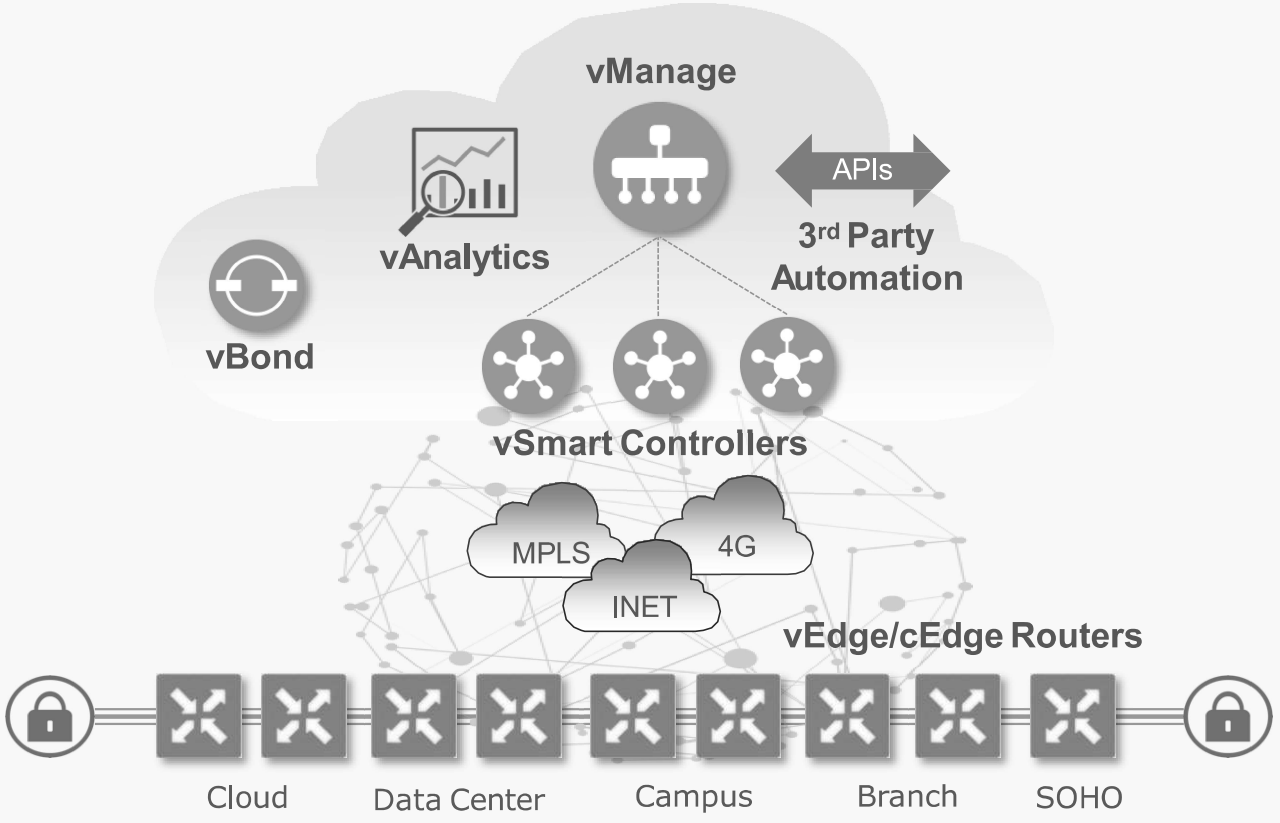


Data Plane

Data Plane
Physical/Virtual

Cisco vEdge/cEdge

- WAN edge router
- Provides secure data plane with remote vEdge routers
- Establishes secure control plane with vSmart controllers (OMP)
- Implements data plane and application aware routing policies
- Exports performance statistics
- Leverages traditional routing protocols like OSPF, BGP and VRRP
- Support Zero Touch Deployment
- Physical or Virtual form factor (100Mb, 1Gb, 10Gb)



Cisco SD-WAN rebranded by Cisco recently from 20.12.1

Existing Name

- Cisco SD-WAN
- Cisco vManage
- Cisco vBond
- Cisco vSmart
- Cisco vAnalytics

Rebranded Name

- Cisco Catalyst SD-WAN
- Cisco Catalyst SD-WAN Manager
- Cisco Catalyst SD-WAN Validator
- Cisco Catalyst SD-WAN Controller
- Cisco Catalyst SD-WAN Analytics

Note: For the purposes of this training existing name will be used in all the slides

Product portfolio

The entire Cisco SD-WAN routing portfolio includes:

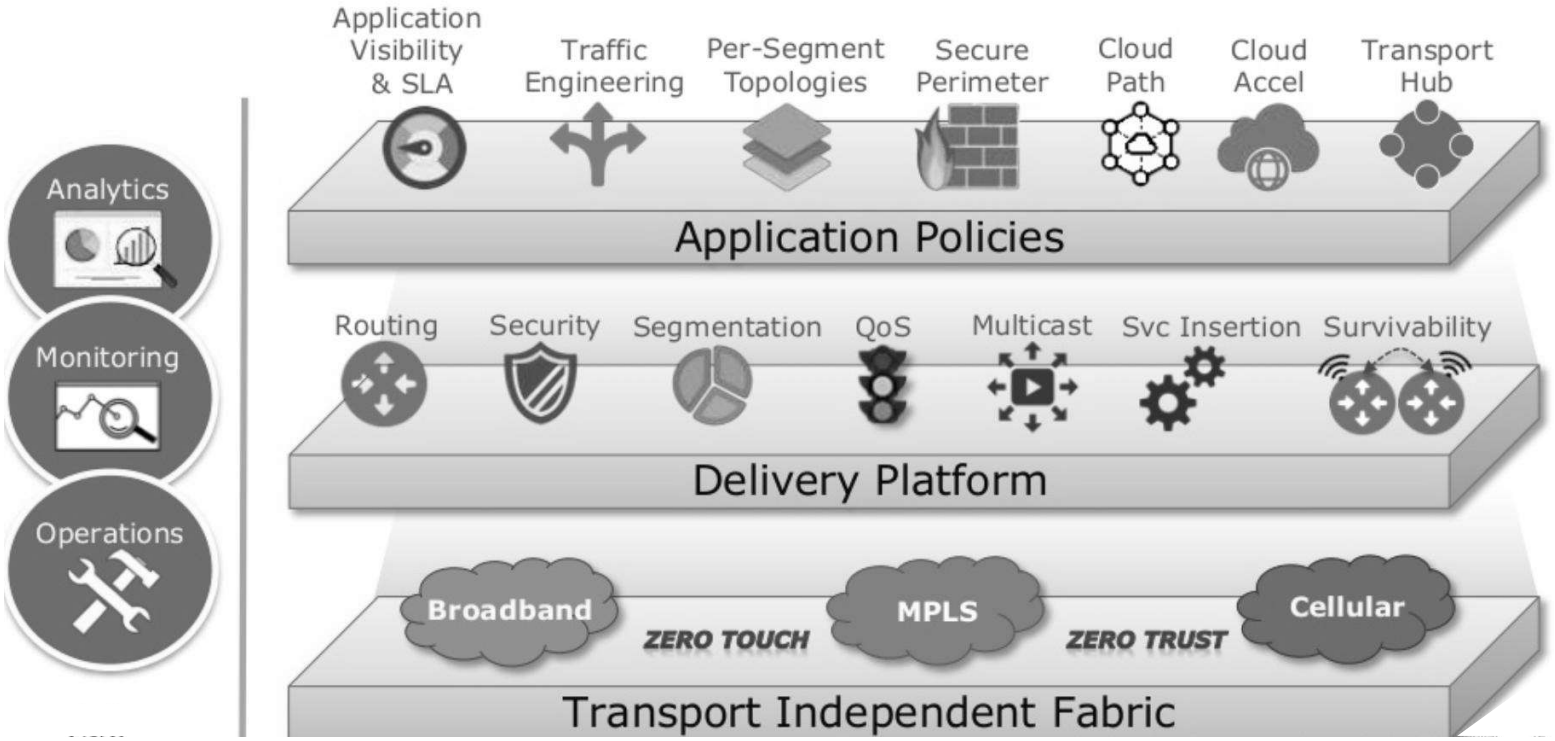
Viptela OS Routers

1. **vEdge-100:** five fixed 10/100/1000 Mbps ports. Comes in three different flavors:
- **vEdge 100b:** Ethernet only
- **vEdge 100m:** Ethernet and integrated 2G/3G/4G modem
- **vEdge 100wm:** Ethernet and integrated 2G/3G/4G modem + Wireless LAN
2. **vEdge-1000:** 8 ports of fixed GE SFP
3. **vEdge-2000:** 2 Pluggable Interface Modules
4. **vEdge-5000:** 4 Network Interface Modules
5. **ISR 1100-4G:** 4 GE WAN ports
6. **ISR 1100-6G:** 6 GE WAN ports (4 GE and 2 SFP)

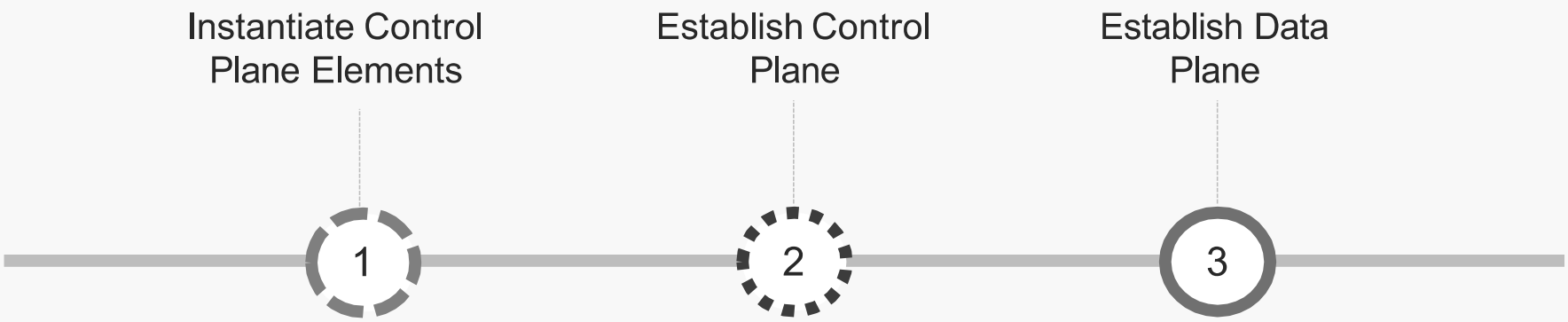
IOS XE SD-WAN Routers

1. **ISR & ASR Series:** With IOS XE SD-WAN software image, SD-WAN capability can be enabled on select ISR 1000 series, ISR 4000 series and ASR 1000 series routers. For more details, refer the respective data sheets.
2. **ENCS:** With IOS XE SD-WAN software image, SD-WAN capability can be enabled on select ENCS 5000 series platforms. For more details, refer to the respective data sheets.
3. **vEdge Cloud** and **CSR** 1000V are the cloud elements of the SD-WAN solution. For more details, refer to the respective data sheets.

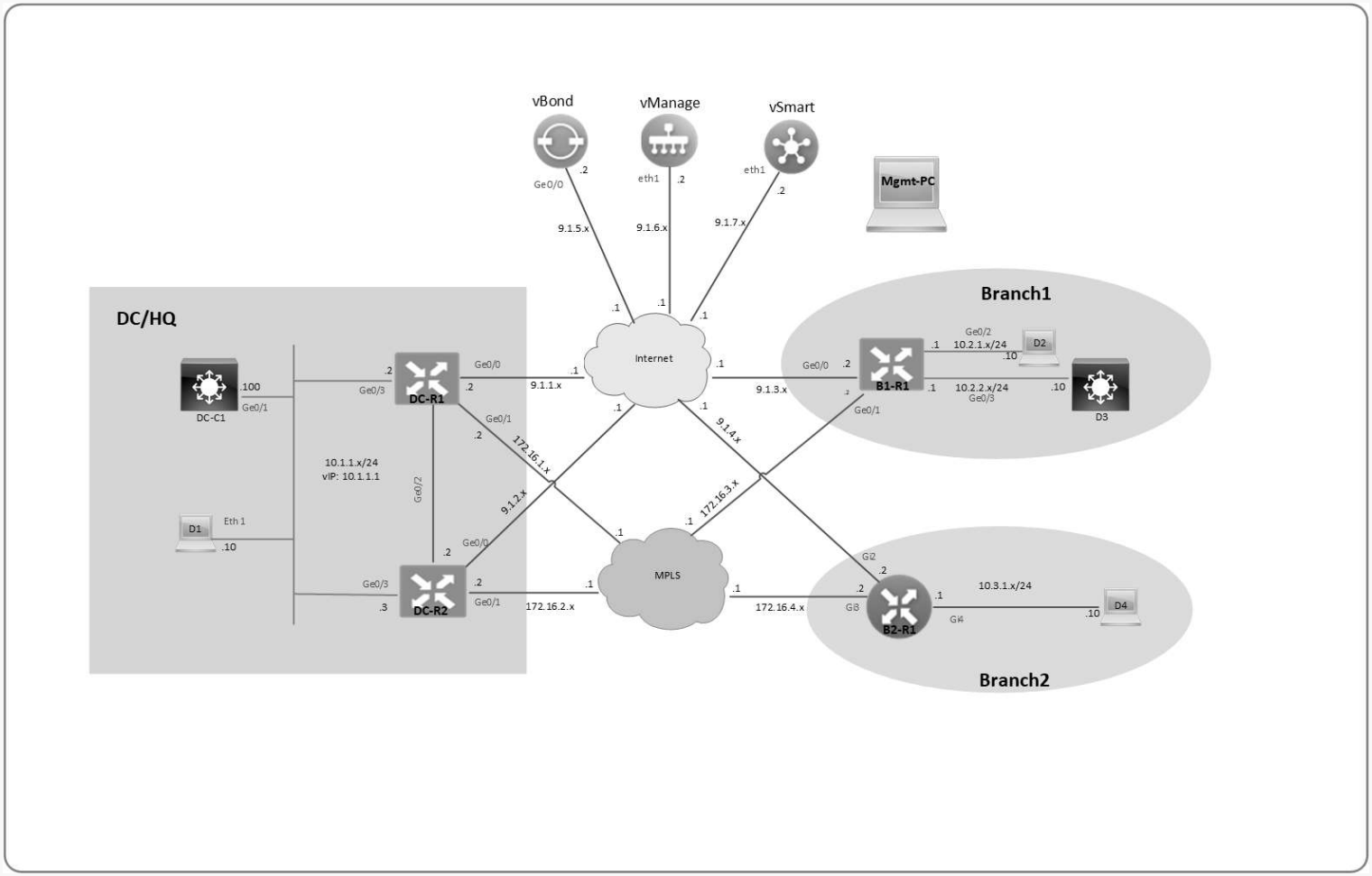
Cisco SD-WAN Solution



Steps in Establishing Cisco SD-WAN Fabric

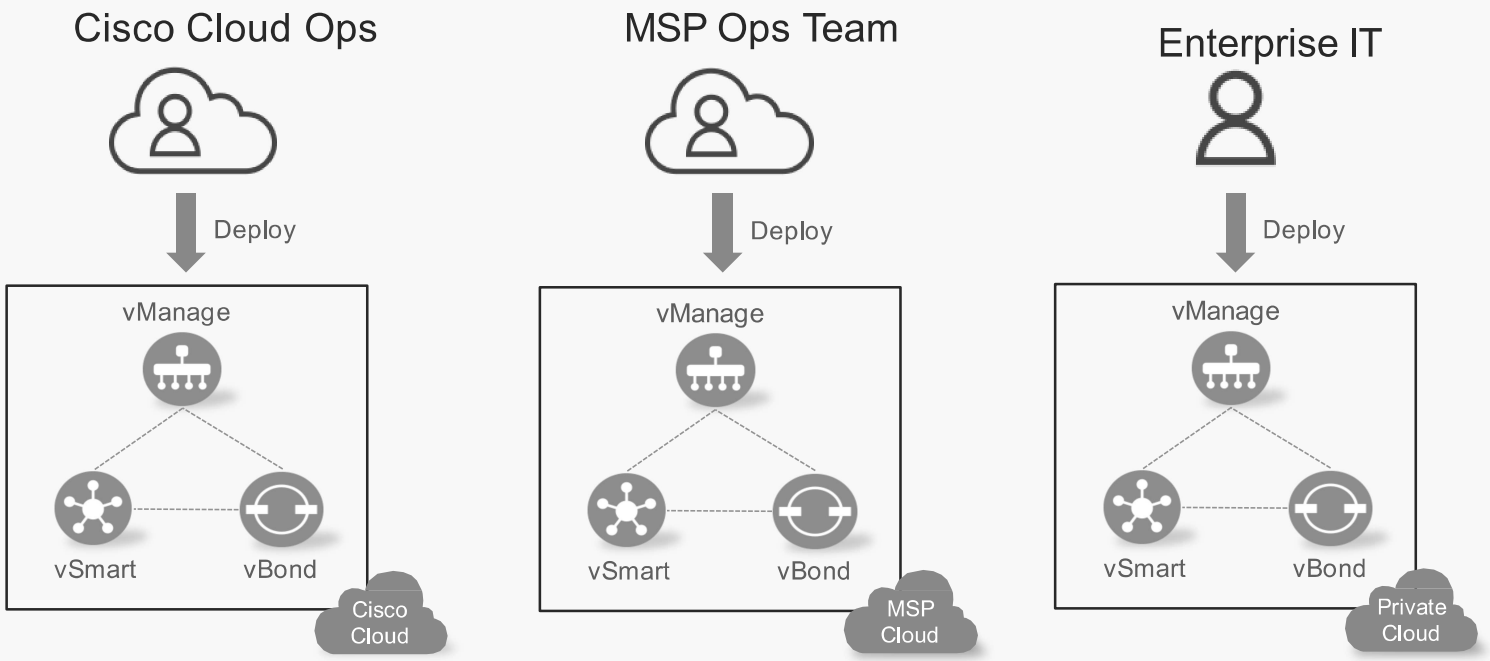


Lab Topology

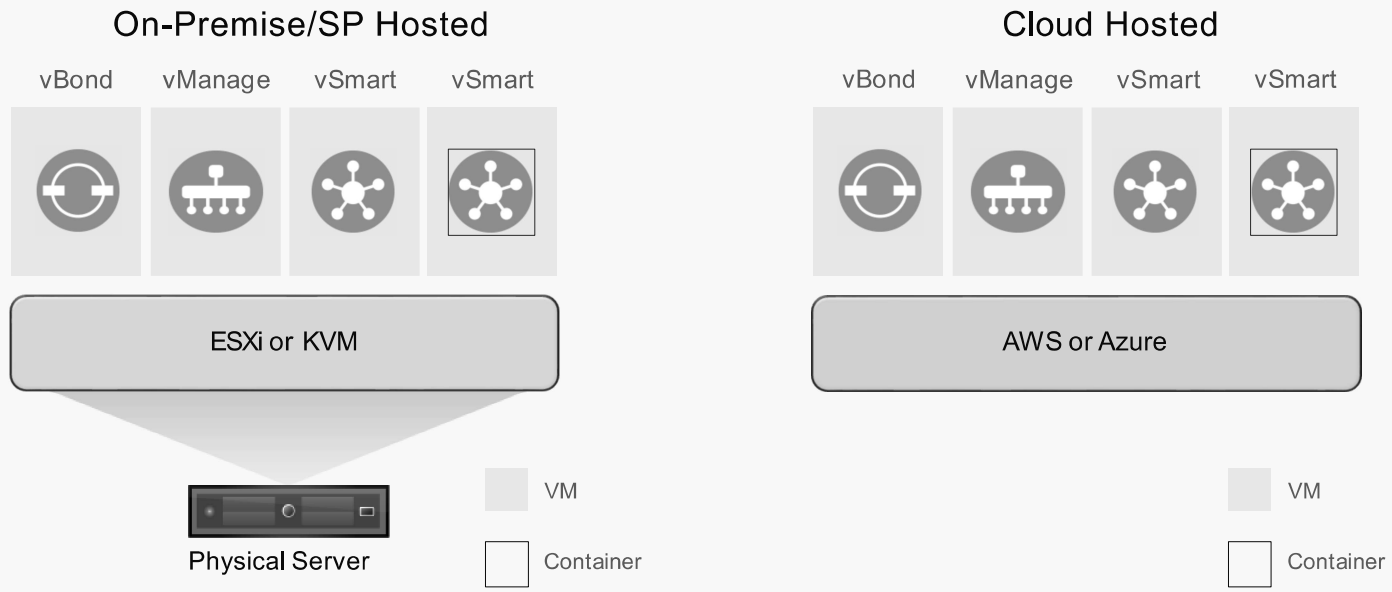


Cisco SD-WAN
Controller Deployment

Flexible Deployment Options

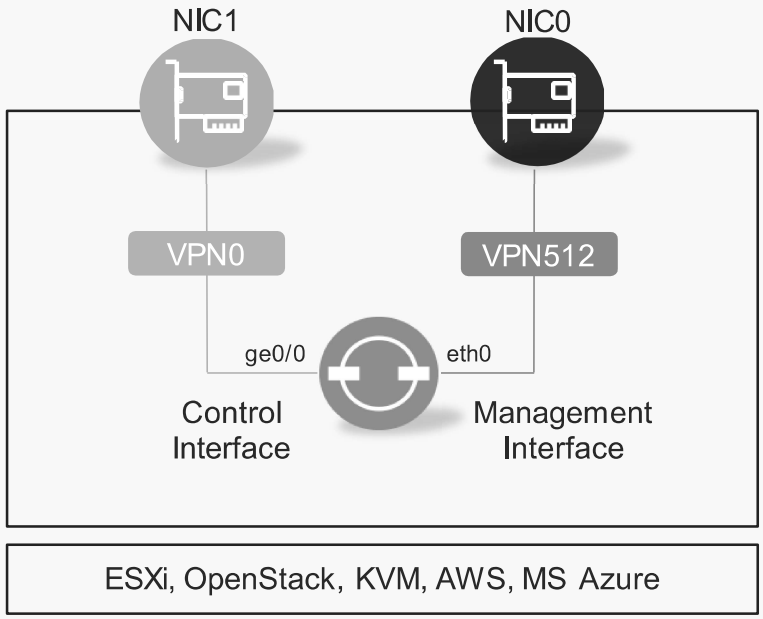


Controllers Deployment Methodology



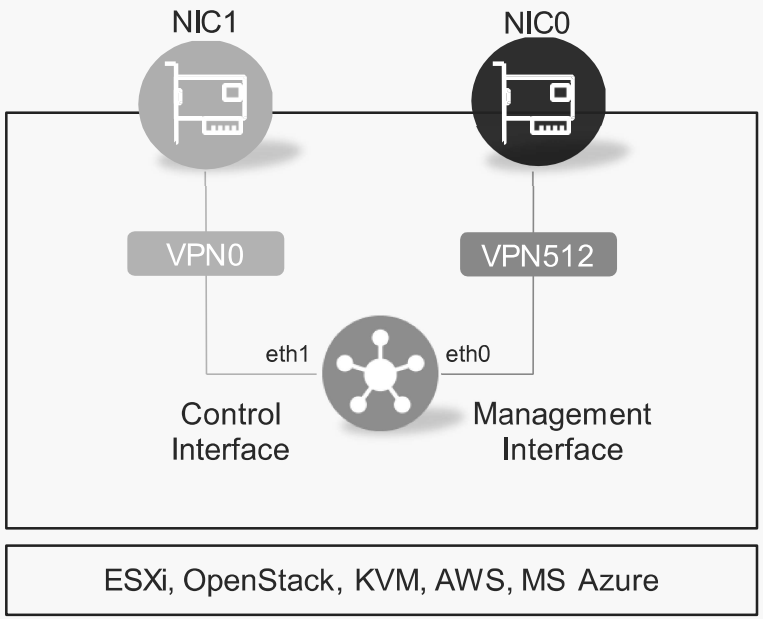
vBond Deployment

- Virtual machine
- Separate interfaces for control and management
- Separate VPNs for control and management
  - Zone-based security
- Minimal configuration for bring-up
  - Connectivity, System IP, Site ID, Org-Name, vBond IP (local)



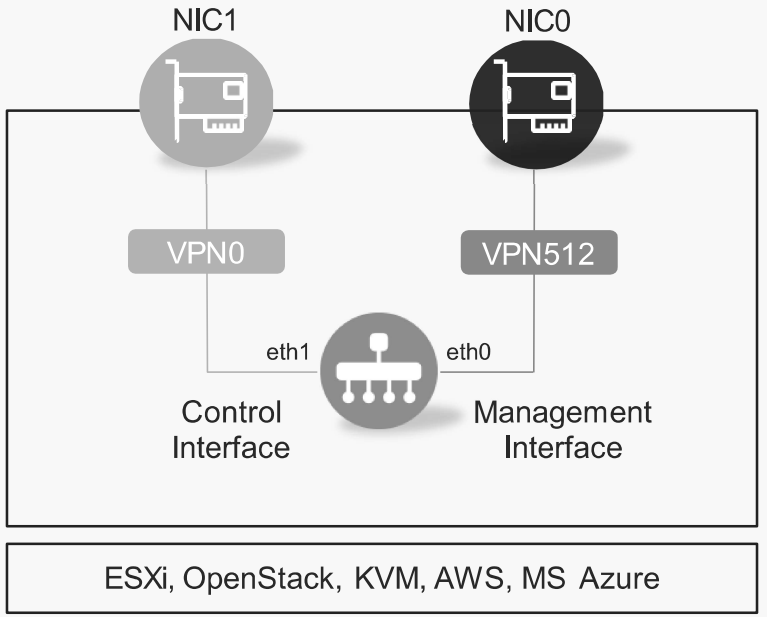
vSmart Deployment

- Virtual machine or container
- Separate interfaces for control and management
- Separate VPNs for control and management
  - Zone-based security
- Minimal configuration for bring-up
  - Connectivity, System IP, Site ID, Org-Name, vBond IP



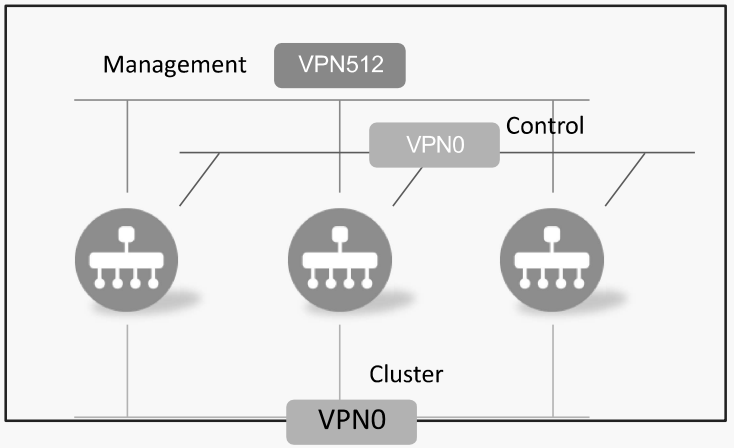
vManage Deployment

- Virtual machine
- Separate interfaces for control and management
- Separate VPNs for control and management
  - Zone-based security
- Minimal configuration for bring-up
  - Connectivity, System IP, Site ID, Org-Name, vBond IP



vManage Cluster

- Reasons to deploy a vManage cluster
  - High availability and redundancy for fault tolerance
  - Managing more than 2000 WAN Edges
  - Distributing NMS Service Loads
- Not for geo-redundancy!
- The vManage cluster consists of at least three vManage devices
- Dedicated interface in VPN0 for cluster communication
- 1Gb bandwidth between cluster members
- <5ms latency between cluster members



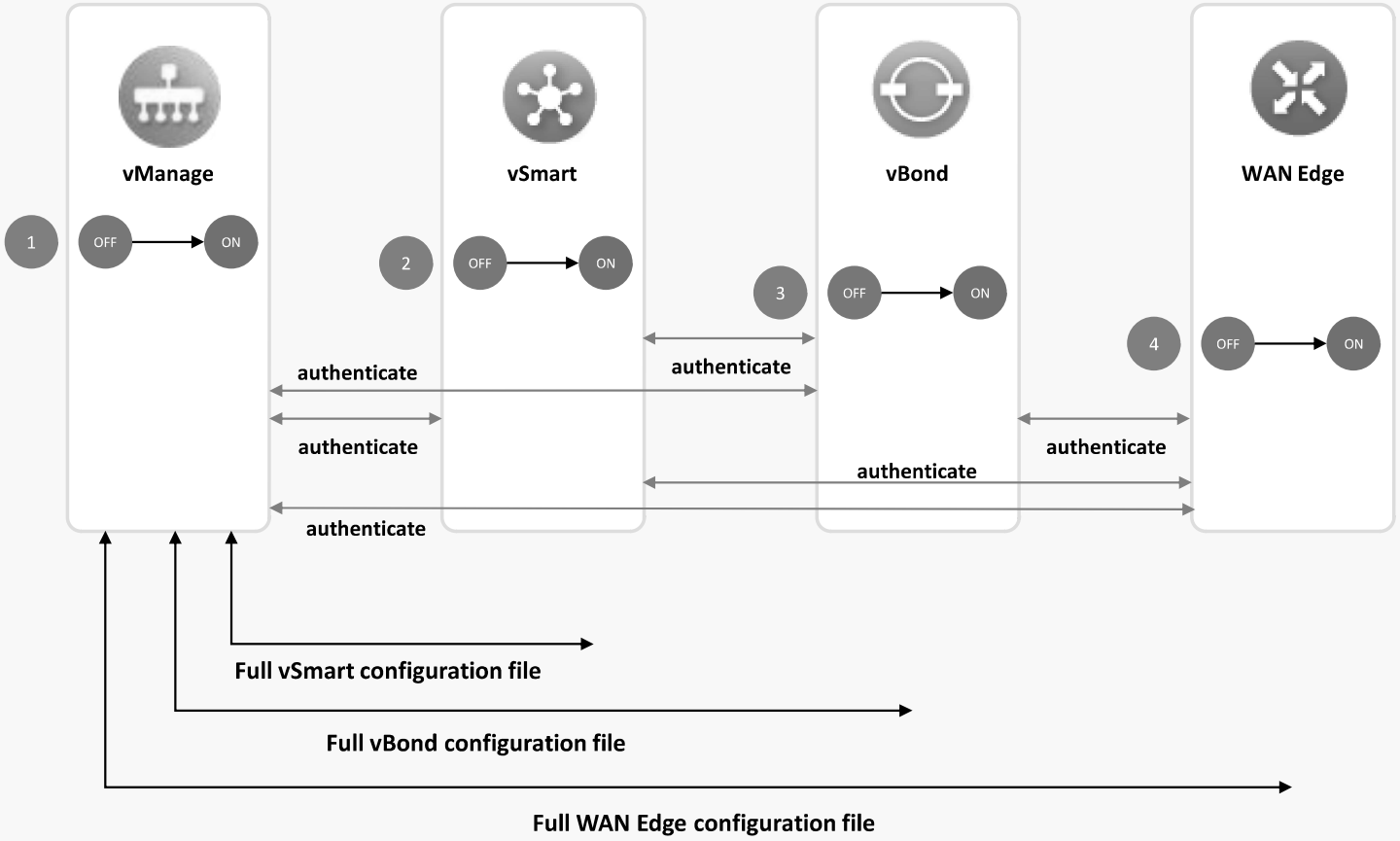
ESXi, OpenStack, KVM, AWS, MS Azure

Break

Cisco SD-WAN

Secure Extensible Network – Control Plane

Bring Up Sequence of Events



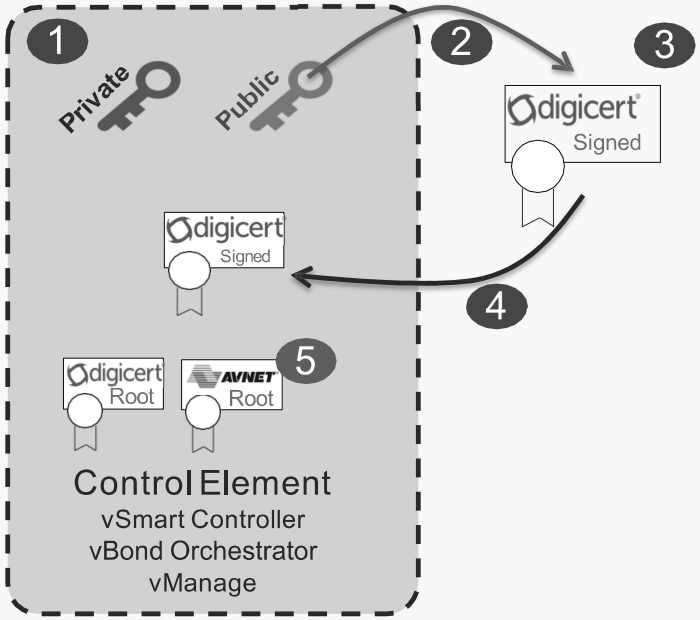
Key Points

- Certificates and Org name are used for mutual Authentication
- Configuration templates can be defined in vManage before bringing up the WAN Edges
- Configuration templates are pushed when the devices are authenticated and added into the network

Control Connections

- Control connections will be established between all the control elements vBond, vManage and vSmart
- Control Connections will be established between all the control elements and WAN edges
  - Not between the WAN edges
- Uses DTLS by default
  - TLS can be enabled on all except vBond
- Certificate based authentication

Establishing Control Elements Identity



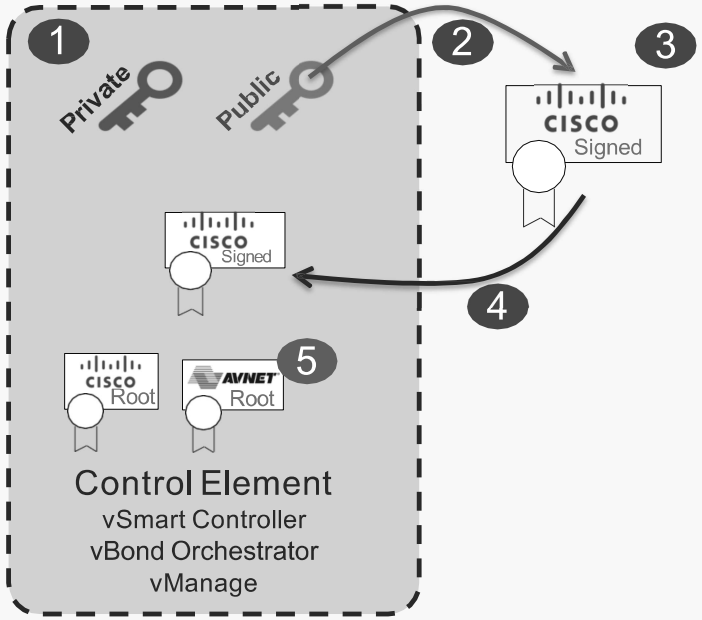
1. Private and public keys are generated on the control element
2. Certificate Signing Request is generated
3. Certificate is signed by Digicert/Cisco
4. Certificate is installed into the control element
5. Control element has a built-in root CA trust chain for Avnet, Digicert and Cisco to Validate other controllers and WAN Edge routers.

This process is fully automated within vManage.

Q: Can I Use Enterprise CA?
A: YES!

Establishing Control Elements Identity – Cisco PKI

19.1

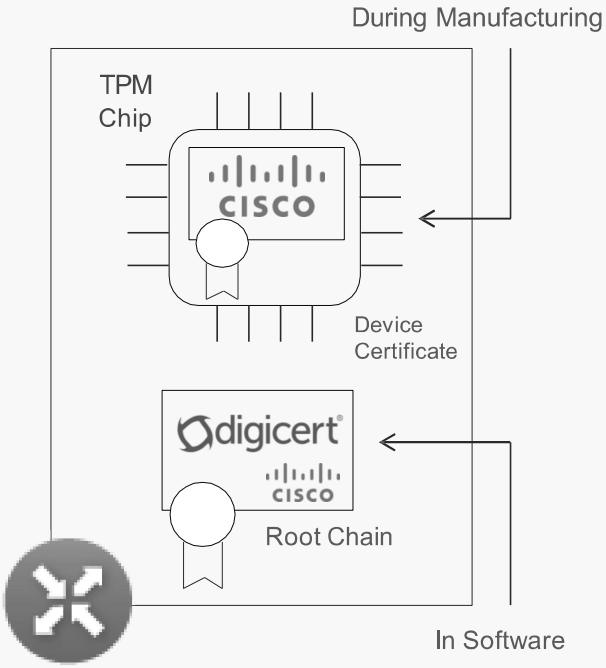


1. Private and public keys are generated on the control element
2. Certificate Signing Request is generated
3. Certificate automatically signed by Cisco PnP linked to your Smart Account (when Cisco signing is selected in vManage)
4. Certificate is installed into the control element
5. Control element will have a built-in root CA trust chain for Cisco and Avnet, to Validate other controllers and WAN Edges

This process is fully automated within vManage.

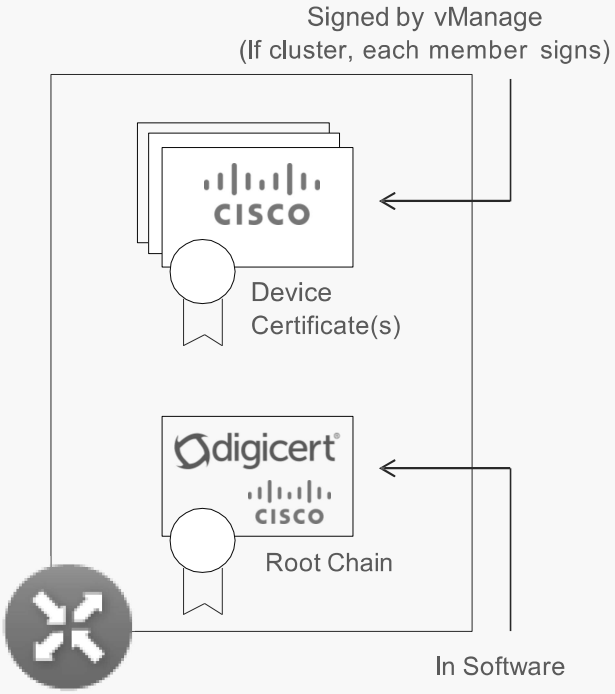
Q: Can I Use Enterprise CA?
A: YES!

WAN Edge Router Identity



- Each physical WAN Edge router is uniquely identified by the chassis ID and certificate serial number
- Avnet Certificate is stored in on-board Tamper Proof Module (TPM)
  - Installed during manufacturing process
- Certificate is signed by Avnet root CA or Cisco root CA
  - Trusted by Control Plane elements
- DigiCert or Cisco root CA chain of trust is used to validate Control Plane elements
- Alternatively, Enterprise root CA chain of trust can be used to validate Control Plane elements
  - Can be automatically installed during ZTP

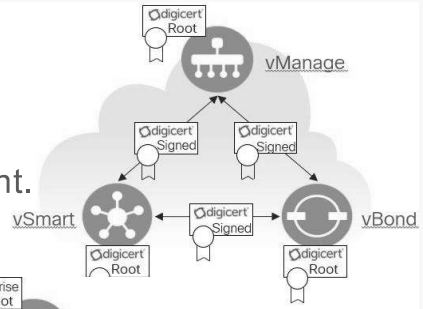
WAN Edge Virtual/Cloud Router Identity



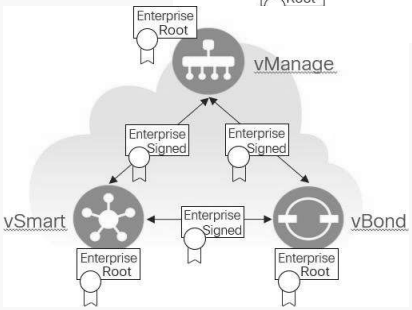
- OTP/Token is generated by vManage
  - One per-(chassis ID, serial number) in the uploaded WAN Edge list
- OTP/Token is supplied to Cloud router in Cloud-Init during the VM deployment
  - Can activate from CLI post VM deployment
- vManage signs certificate(s) for the Cloud router post OTP/Token validation
  - If vManage cluster, each member signs
  - vManage removes OTP to prevent reuse
- DigiCert or Cisco root CA chain of trust is used to validate Control Plane elements
- Alternatively, Enterprise root CA chain of trust can be used to validate Control Plane elements
  - Can be provided in Cloud-Init

Certificate Authority Options

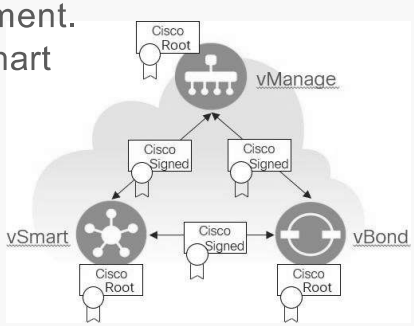
- DigiCert certificates can be used also in on-prem deployment.
- Need to contact CloudOps for approval.
- Root certificate is preinstalled in the software.



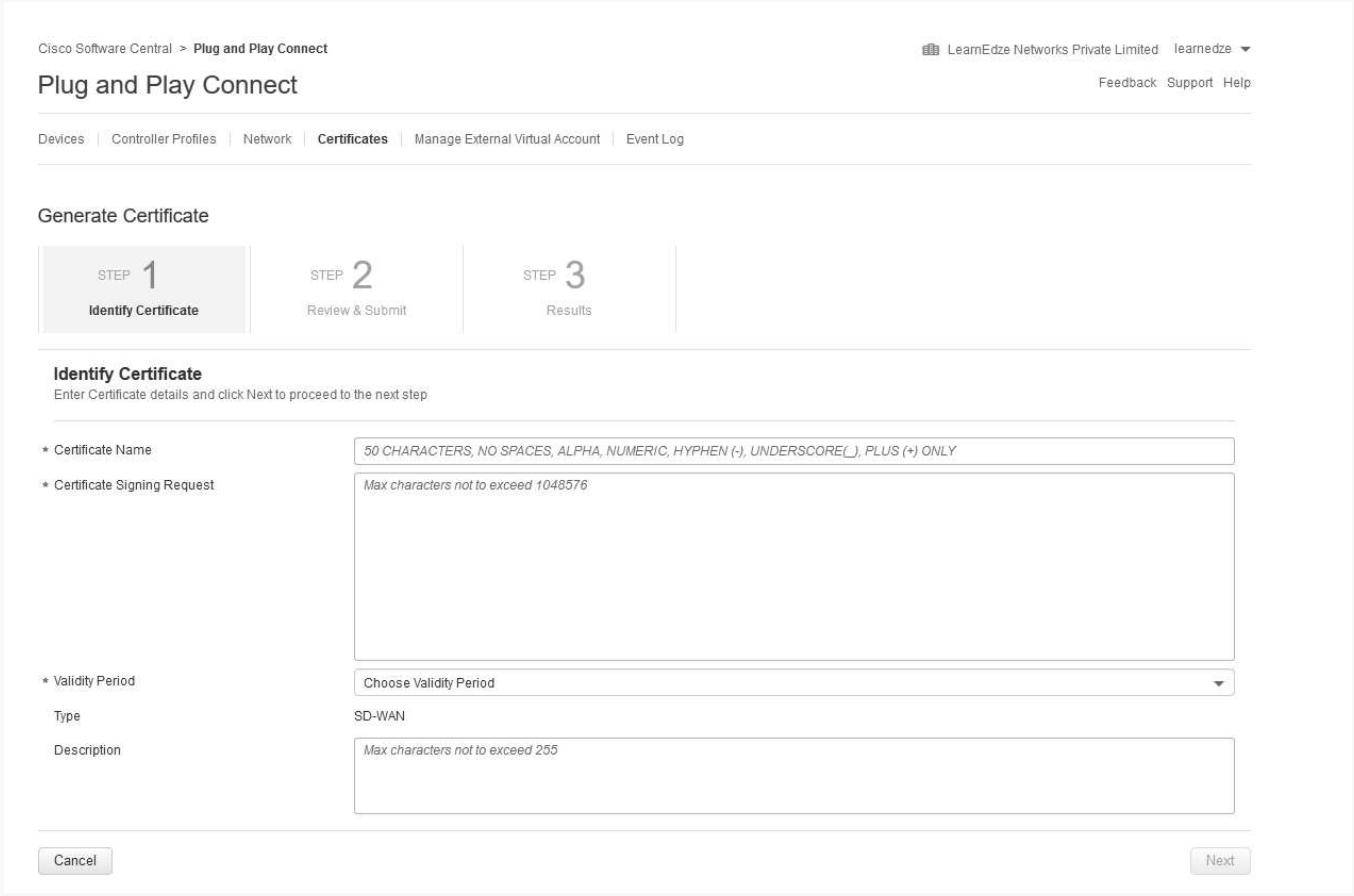
- Enterprise certificates can be used for on-prem controllers deployment.
- Need to install root certificate chain and sign all CSRs manually.



- Cisco PKI can be used for on-prem controllers deployment.
- CSRs can be automatically signed using configured Smart account and internet connectivity from vManage.
- Manual signing is supported via PnP portal.



Cisco SD-WAN Certificate Signing using PnP



Initial Configuration Settings

- System-IP – Unique identifier of a SD-WAN component
  - 32-Bit dot decimal notation (an IPv4 Address)
  - Logically a VPN 0 Loopback Interface, referred to as “system”
  - Like a router-id, should be unique
- Organization-Name – SD-WAN overlay identifier
  - Must match on all components
  - Example: learnedze
- Site-ID – Identifies logical location of individual node
  - Configured on every WAN Edge
  - When not unique, same location is assumed

Integrating Controllers

1. Configure tunnel interfaces and Initial config
2. Add vBond and vSmart controllers into the vManage.
3. Generate CSRs.
4. Sign CSRs and Install certificates.
5. Control Connections will be established between control elements.

Validated Controller Scale

vManage:

2,000 Devices per-single instance
Max Production Deployment: 6 instances

vSmart:

5,400 Connections per-single vSmart Max Production Deployment: 20 vSmarts

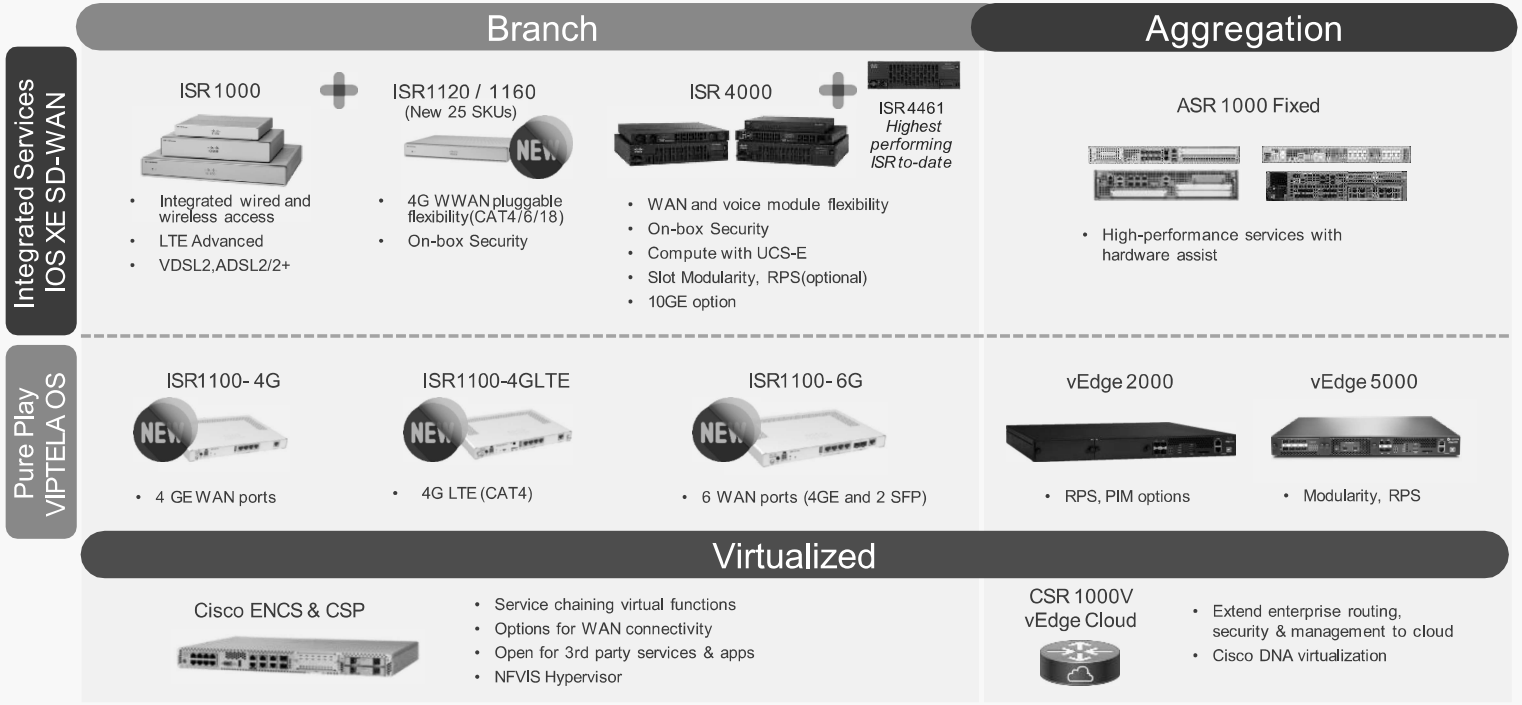
vBond:

1,500 Connections per-single vBond
Max Production Deployment: 6 vBonds

Cisco SD-WAN

Secure Extensible Network – Data Plane

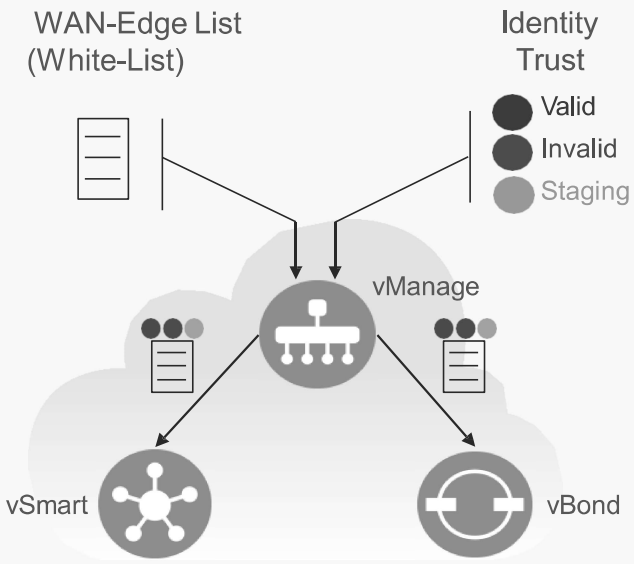
SD-WAN Portfolio with New Platforms



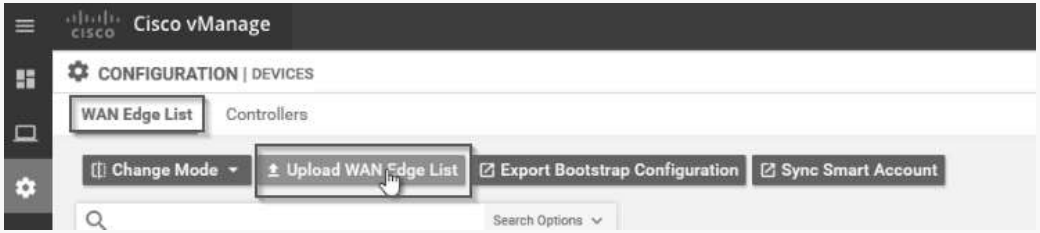
Cisco SD-WAN

Zero Touch Provisioning

WAN Edge - Whitelisting

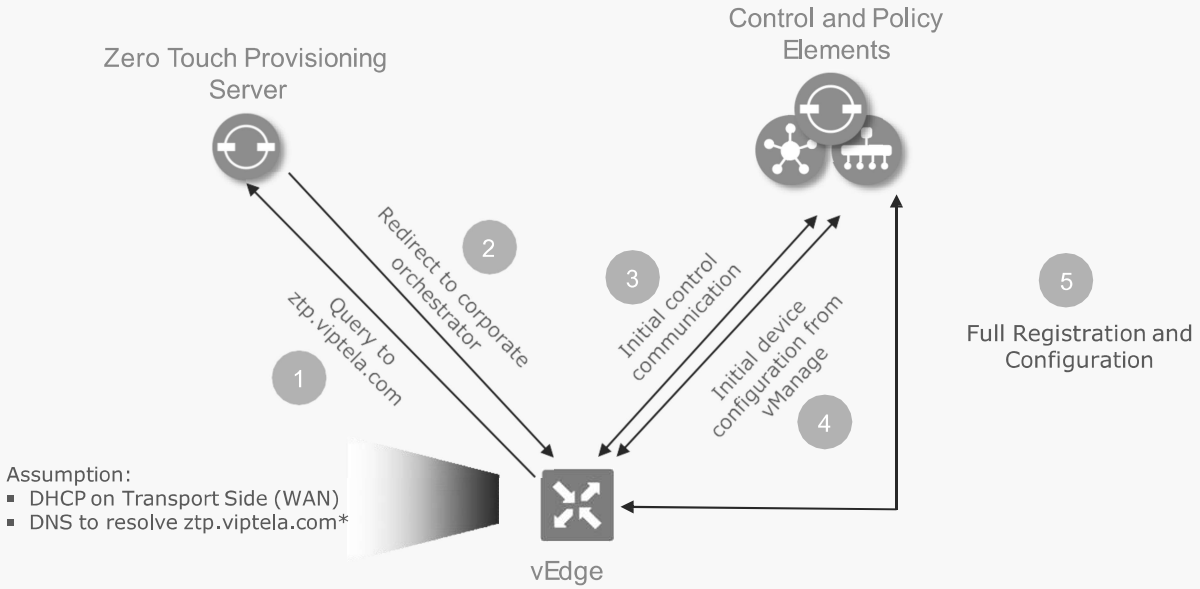


- Administrator uploads digitally signed WAN-Edge list in the vManage GUI
  - White-list for WAN-Edge routers
  - Downloadable from PnP Portal
  - Sync Smart Account



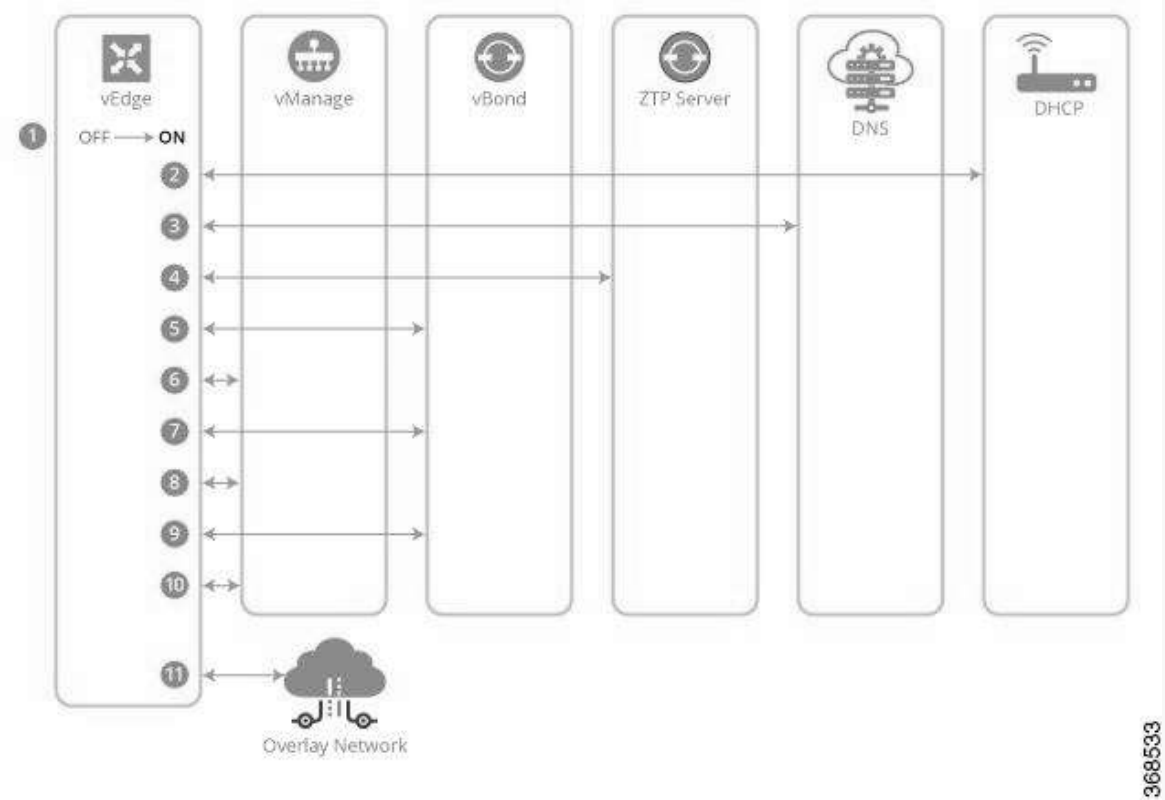
- Administrator decides on identity trust
  - Valid, invalid, staging
- WAN-Edge list and identity trust are distributed by vManage to vSmart and vBond

Zero Touch Provisioning



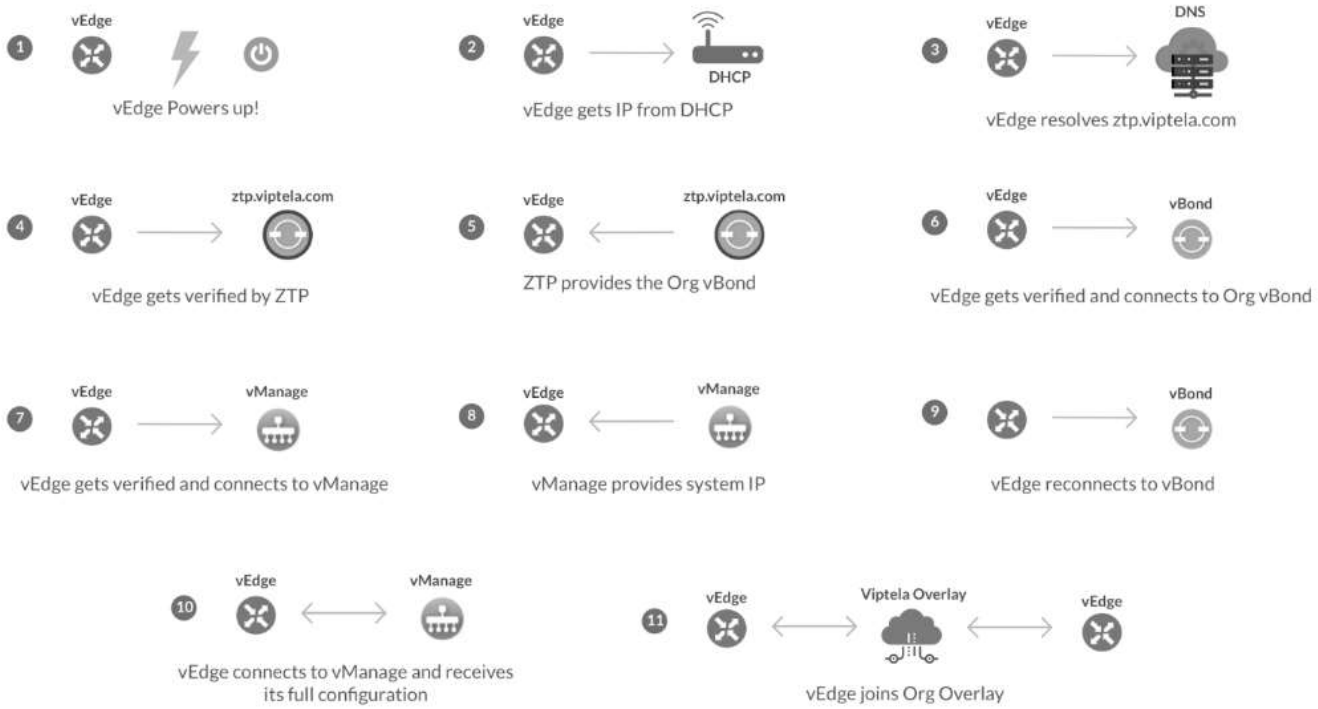
* devicehelper.cisco.com in case of cEdge

ZTP Process



For the ZTP process to succeed, the vManage NMS must contain a device configuration template for the vEdge router. If the NMS has no template, the ZTP process fails.

ZTP Process



Ve1k - ge0/0

Ve2K - ge2/0

Ve100b/m - ge0/4

For the ZTP process to succeed, the vManage NMS must contain a device configuration template for the vEdge router. If the NMS has no template, the ZTP process fails.

ZTP Process

The hardware WAN Edge router powers up.

The router attempts to contact a DHCP server and receives IP address and DNS details from DHCP server.

The router contacts a DNS server to resolve the hostname ztp.viptela.com and receives the IP address of the Cisco SD-WAN ZTP server

The router connects to the ZTP server. The ZTP server verifies the vEdge router and sends the IP address of the vBond orchestrator. This is a vBond orchestrator that is in the same organization as the vEdge router.

The router establishes a transient connection to the vBond orchestrator and sends its chassis ID and serial number. (At this point in the ZTP process, the router does not have a system IP address, so the connection is established with a null system IP address.) The vBond orchestrator uses these two numbers to verify the router. The vBond orchestrator then sends the IP address of the vManage NMS to the router.

The router establishes a connection to the vManage NMS and is verified by the NMS. The vManage NMS sends the router its system IP address.

ZTP Process(Continued…)

The router re-establishes a connection to the vBond orchestrator using its system IP address.

The router re-establishes a connection to the vManage NMS using its system IP address.

If necessary, the NMS pushes the proper software image to the vEdge router.

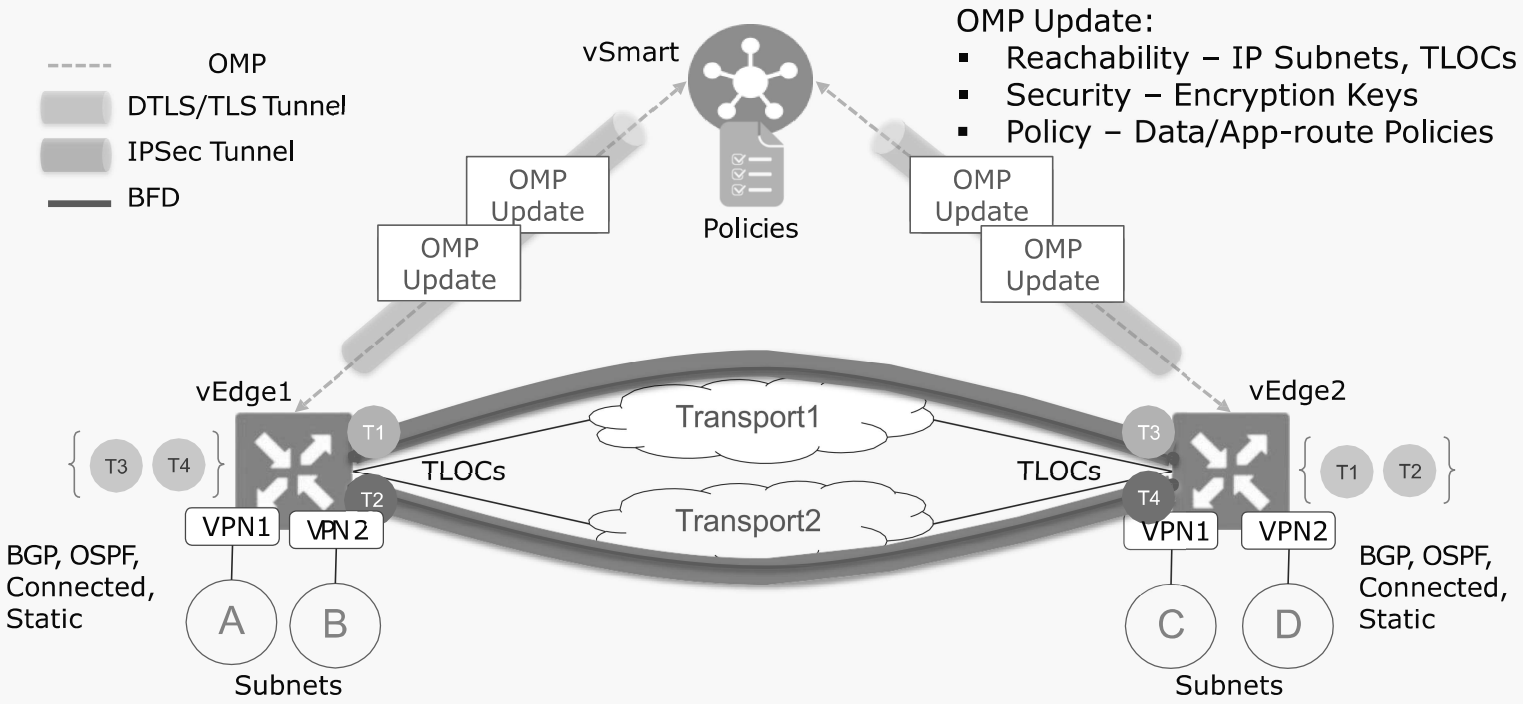
As part of the software image installation, the router reboots.

After the reboot, the router re-establishes a connection to the vBond orchestrator, which again verifies the router.

The router establishes a connection to the vManage NMS, which pushes the full configuration to the router. (If the router has rebooted, it re-establishes a connection to the vManage NMS.)

Finally Router joins the Overlay Network

SD-WAN Fabric Walk-Through



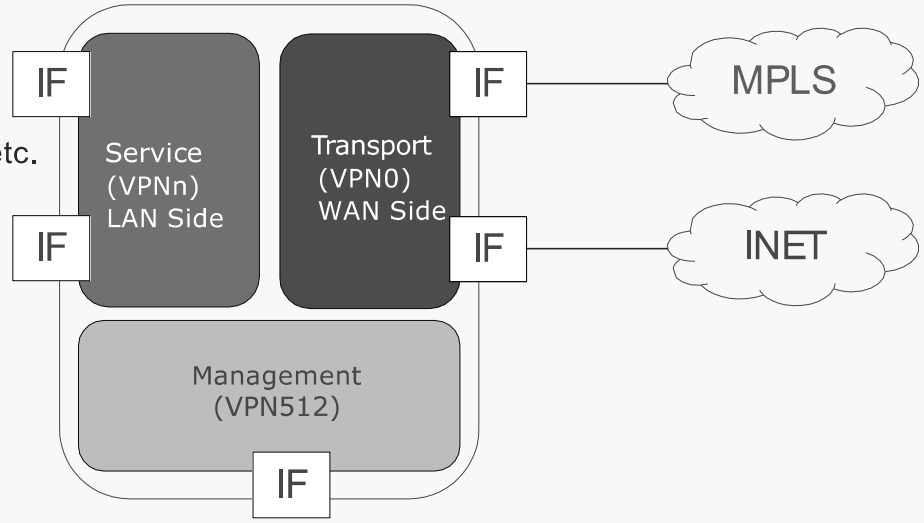
Terminology

- System-IP – Unique identifier of a SD-WAN component
  - 32-Bit dot decimal notation (an IPv4 Address)
  - Logically a VPN 0 Loopback Interface, referred to as “system”
- Organization-Name – SD-WAN overlay identifier
  - Must match on all SD-WAN components
- Site-ID – Identifies logical location of individual node
  - Configured on every WAN Edge
  - When not unique, same location is assumed

Terminology

VPNs

- These are similar to VRFs; used for segmenting traffic and providing routing table isolation
- VPN0 is System Defined
  - Used for control plane traffic for OMP, Orchestration, vManage, etc.
  - IPsec Tunnels terminate on VPN0 interfaces
  - WAN Transports are associated to VPN0
- VPN512 is used for Out-Of-Band System Management
- VPN1-511 is defined by user and used for site-to-site data traffic

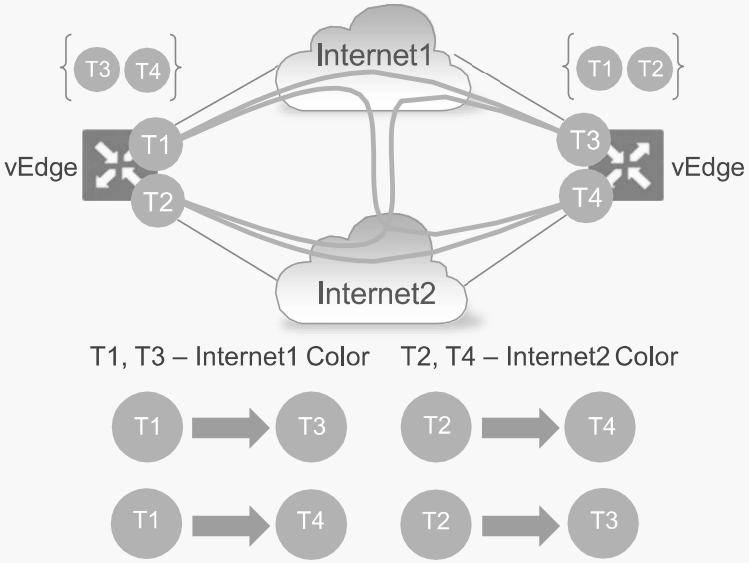


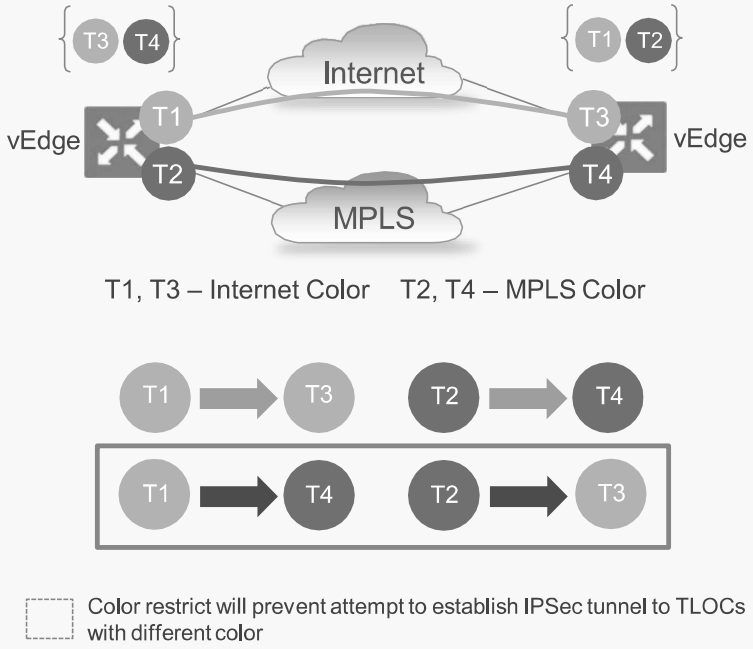
VPN0 in vEdge = Default VRF in cEdge

Terminology

Colors

- Used to associate an interface in VPN0 to a specific transport type
- Examples include: Private(MPLS, Private1, Private2 etc..),Public (biz-internet, gold, silver etc…)

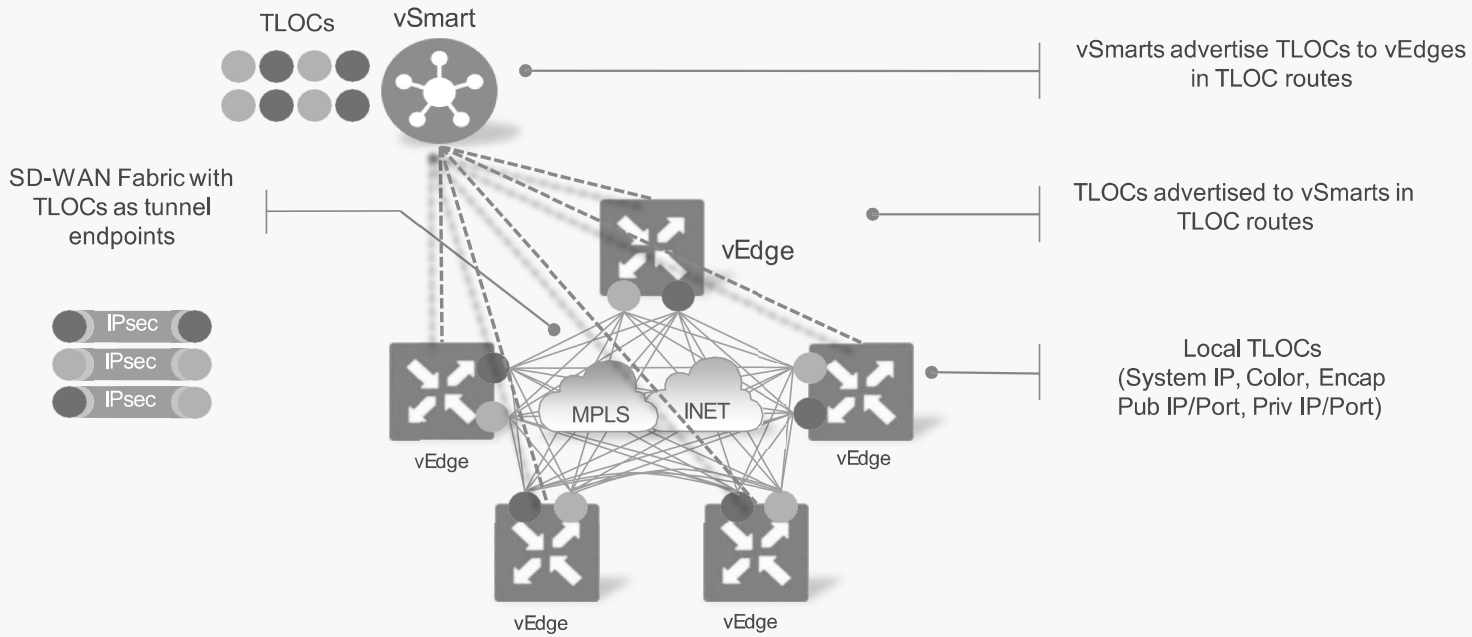




Terminology

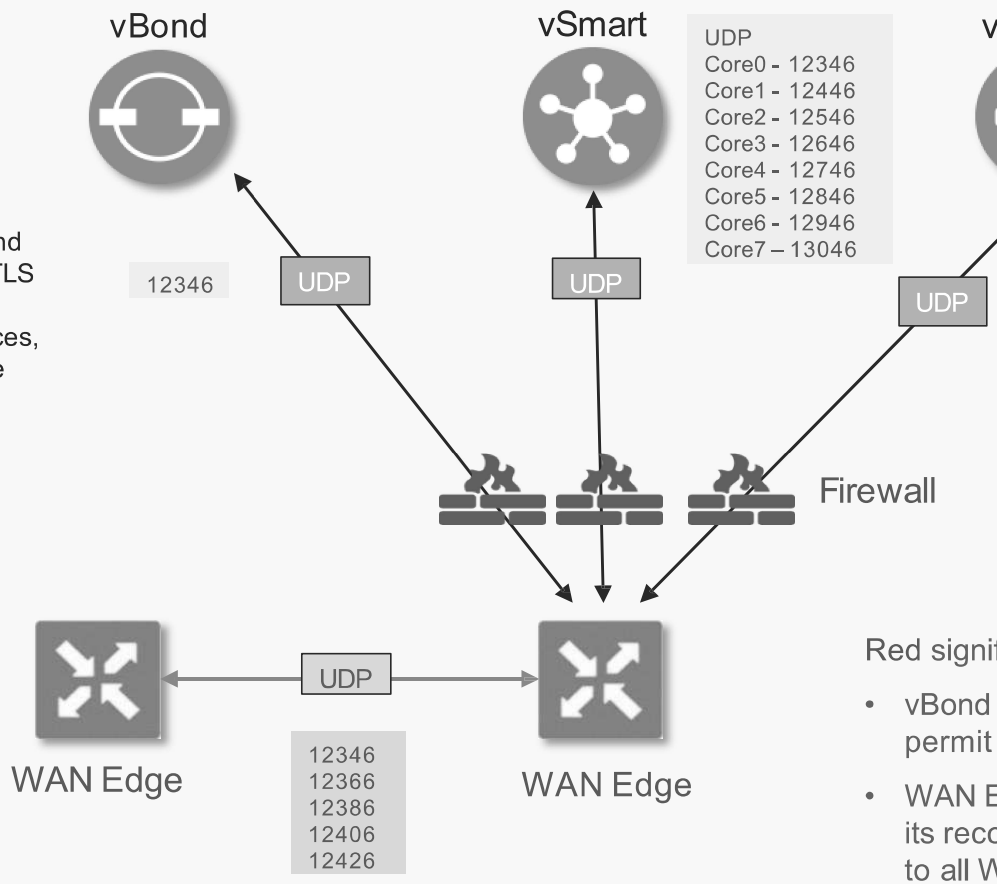
Transport Locator IDs (TLOCS)

- Used to identify the encapsulating interface(WAN) of a Device
- System-IP, Encapsulation and Color
- Similar to Router ID



Firewalls Ports – DTLS

vBond orchestrators do not support multiple cores. vBond orchestrators always use DTLS tunnels to establish control connections with other devices, so they always use UDP. The UDP port is 12346



The vManage NMSs and vSmart controllers can run on a virtual machine (VM) with up to eight virtual CPUs (vCPUs). The vCPUs are designated as Core0 through Core7.
Each core is allocated separate base ports for control connections

Red signifies primary protocol or first port used

- vBond IP's are not Elastic, its recommended to permit UDP/12346 to/from any from the WAN Edge
- WAN Edge's can port hop to establish a connection, its recommended to permit all 5 UDP ports inbound to all WAN Edges

CLI Config on WAN Edge

```
vedge# conf t
Entering configuration mode terminal
vedge(config)# system
vedge(config-system)#  host-name                B1-R1
vedge(config-system)#  system-ip                192.168.1.103
vedge(config-system)#  site-id                  100
```

```
vedge(config-system)#  organization-name       learnedze
vedge(config-system)#  vbond 9.1.5.2
```

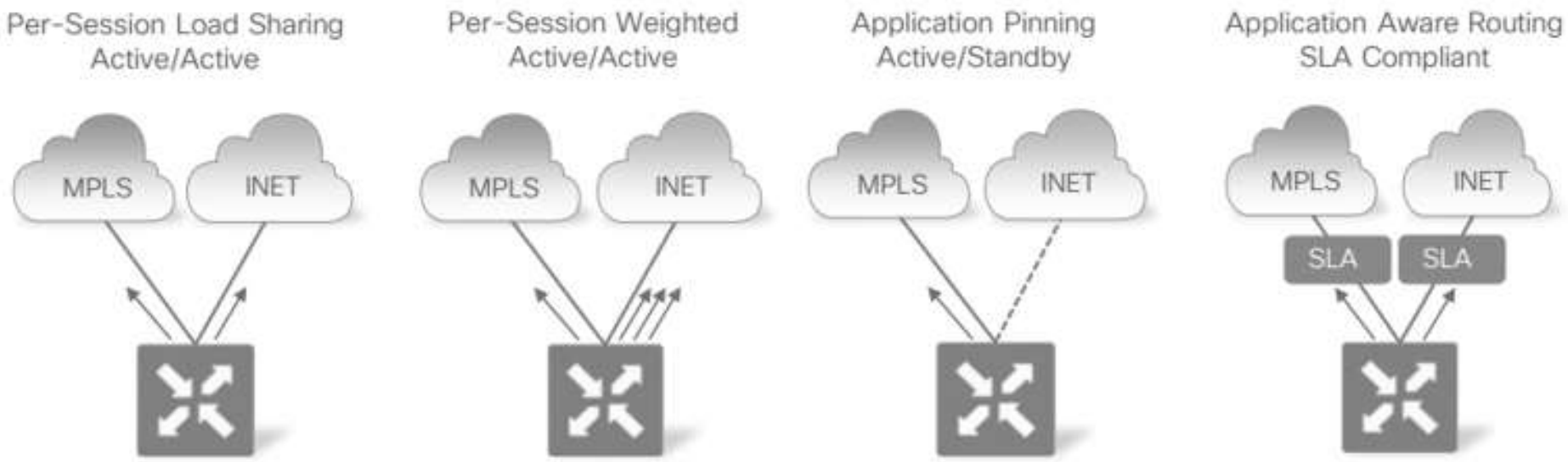
```
vedge(config-system)# vpn 0
vedge(config-vpn-0)#  interface ge0/0
vedge(config-interface-ge0/0)#   ip address 9.1.3.2/24
vedge(config-interface-ge0/0)#   ipv6 dhcp-client
vedge(config-interface-ge0/0)#   tunnel-interface
vedge(config-tunnel-interface)#    encapsulation ipsec
vedge(config-tunnel-interface)#    color biz-internet
```

Installing Certificate and activating WAN Edge

```
B1-R1# request download vpn 512 tftp://192.168.122.160/root-ca.crt
B1-R1#
B1-R1# request root-cert-chain install /home/admin/root-ca.crt
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/root-ca.crt via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
B1-R1#
B1-R1#
B1-R1# show certificate root-ca-cert | in Learnedze
        Issuer: C=US, ST=CA, L=San Jose, O=Learnedze, OU=Learnedze, CN=Learnedze/emailAddress=caserver@learnedze.local
        Subject: C=US, ST=CA, L=San Jose, O=Learnedze, OU=Learnedze, CN=Learnedze/emailAddress=caserver@learnedze.local
B1-R1#
```

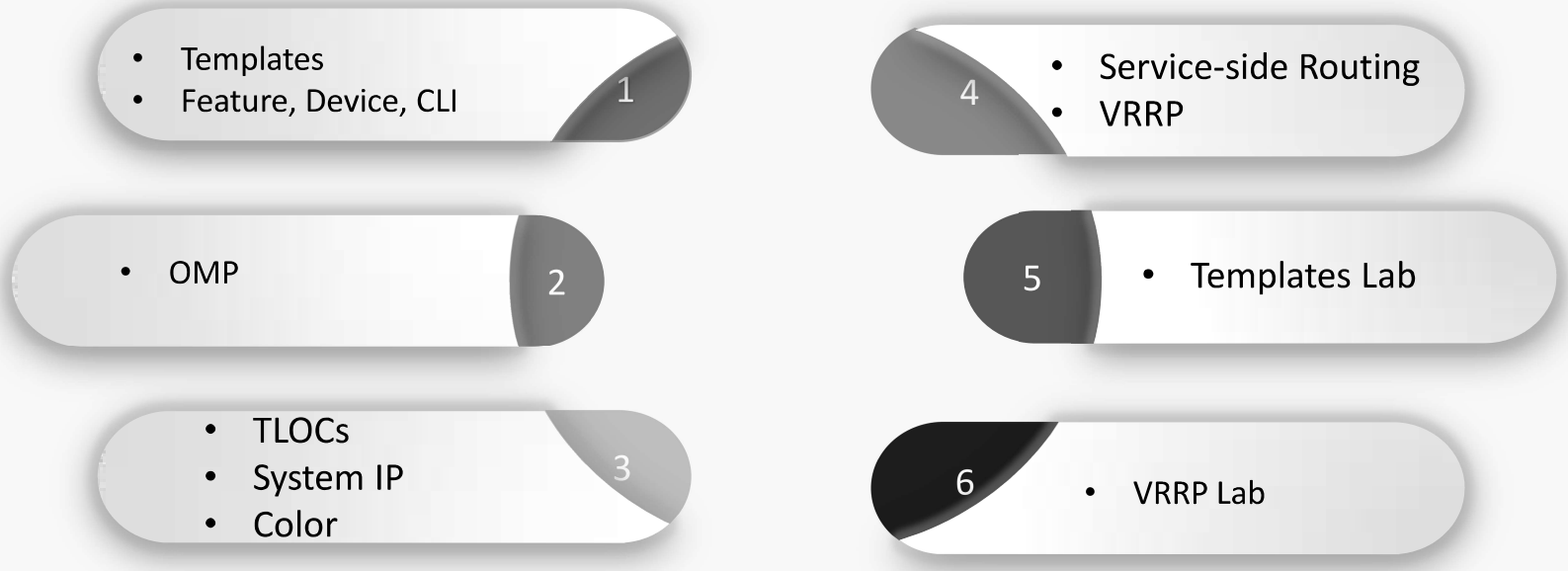
```
B1-R1# request vedge-cloud activate chassis-number f73ab637-6519-8cce-4a30-cb350be7ccf1 token cb392fd13f0ad0ba201d538315bf74f8
```

Common Data Plane Communication



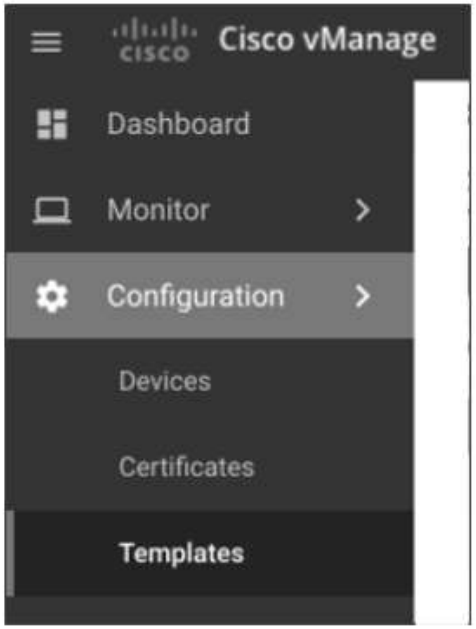
Break

Cisco SD-WAN Training – Day2



Templates

What are Configuration Templates

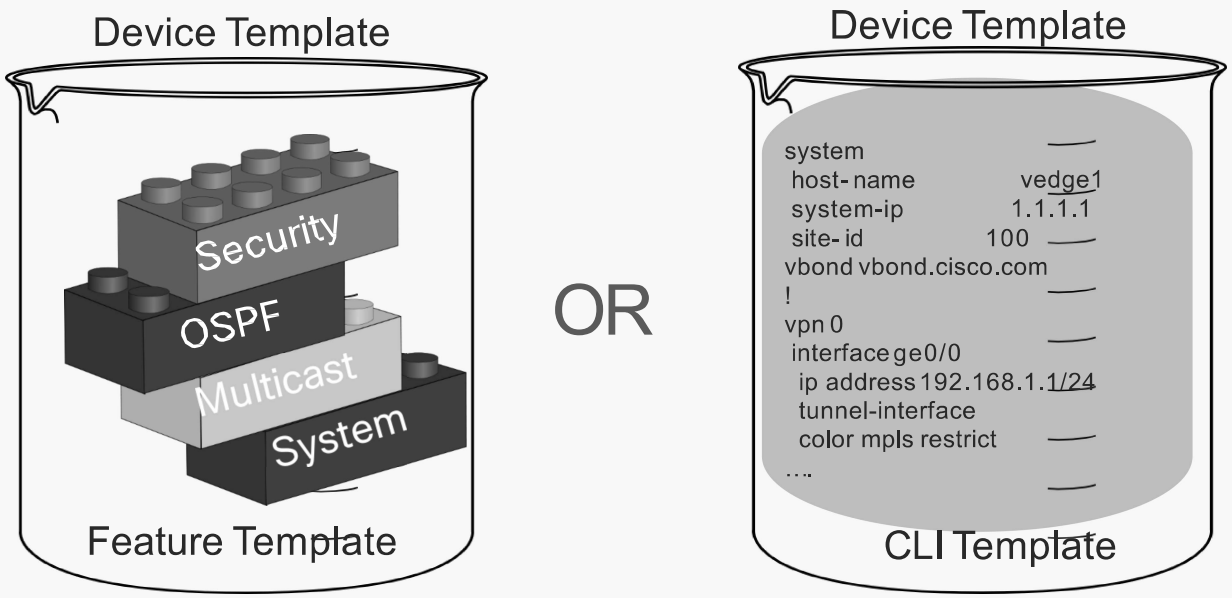


Cisco vManage GUI

- Define all device configuration parameters
- Enforce device configuration consistency and compliance across entire network
- Allow high degree of device configuration customization
- Simple bulk device configuration provisioning using variables
- Centrally provisioned from vManage GUI

Device Templates

Device templates contain a devices complete configuration. You can create device templates by consolidating individual feature templates or by using a CLI template. You cannot mix and match CLI and feature templates. A device template is specific to the type of device, you may use the same device template if the device type is the same.

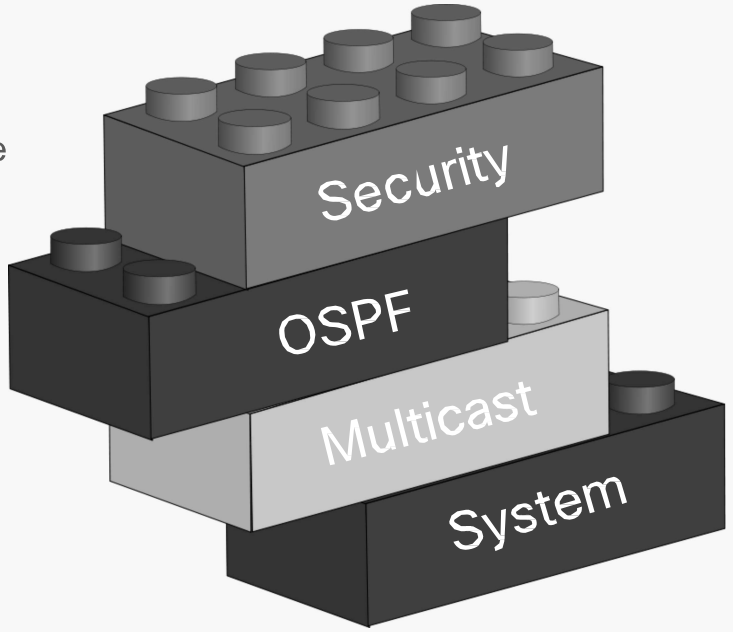


Feature Templates

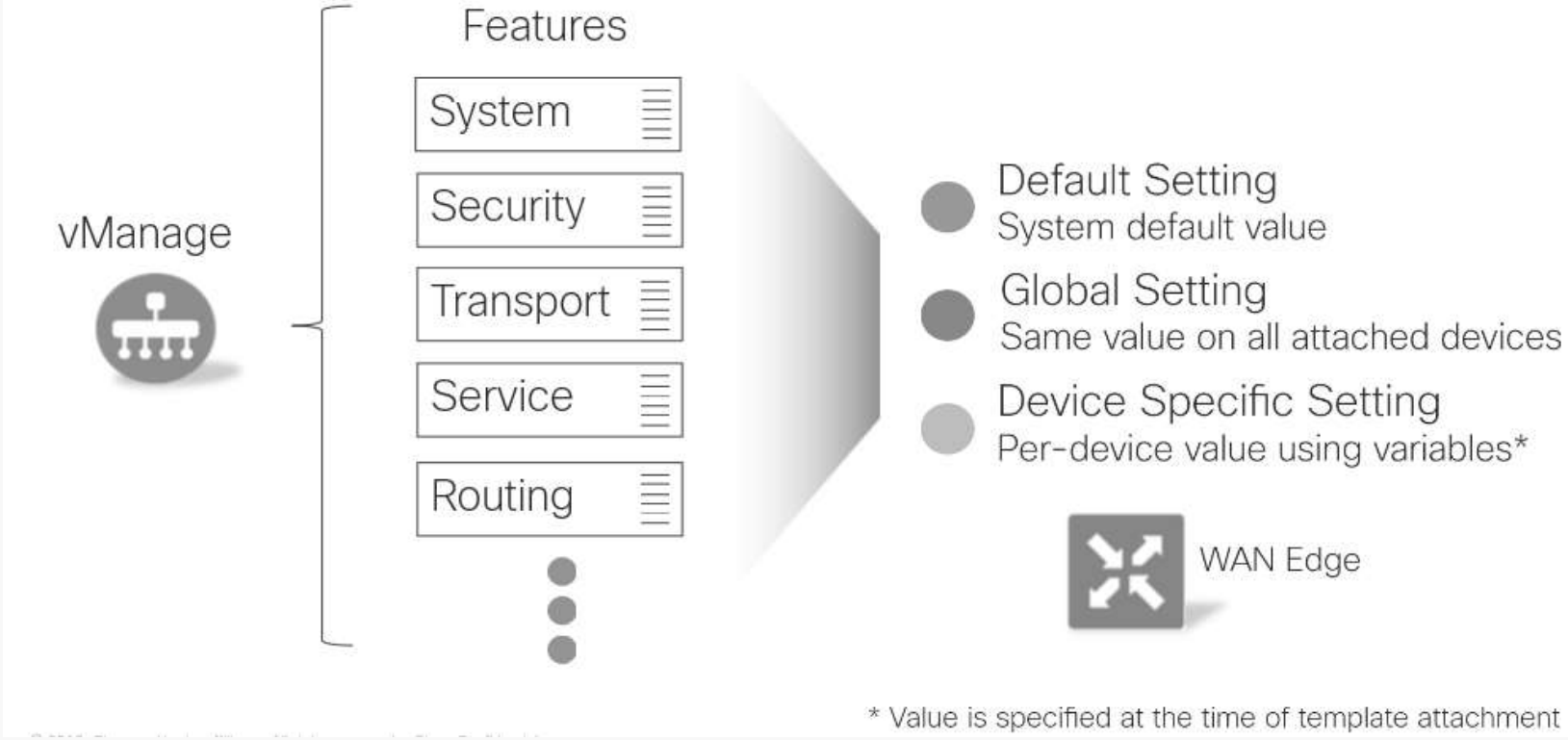
Feature templates are the building blocks for a device's configuration. For each feature that you can enable on a Viptela device, vManage provides you an easy to use form to populate with the required variables. Since device configuration varies depending on the device type feature templates are device type specific. Some common features templates are:

- Security
- Multicast
- Routing protocol configuration
- SNMP
- DHCP
- …

Some features are mandatory for device operation



Device Configuration Templates Structure



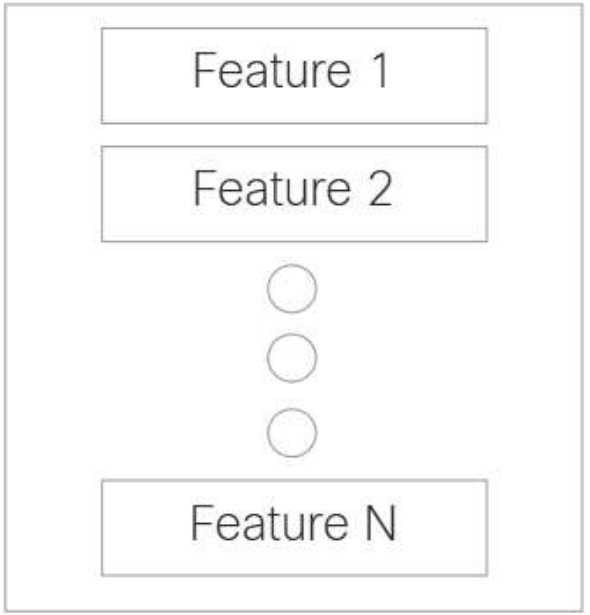
Types of Device Configuration Templates

CLI Template

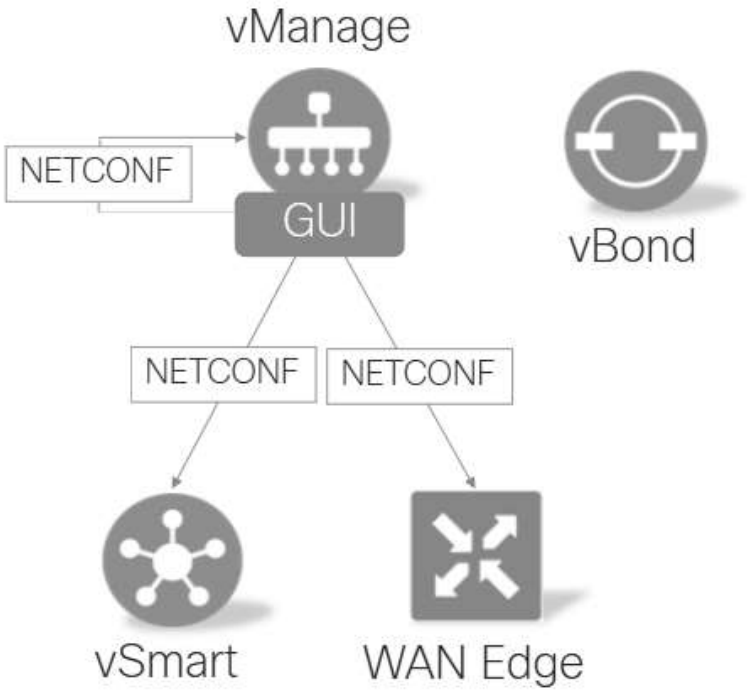
```
omp
 no shutdown
 graceful-restart
 advertise connected
 advertise static
!
security
 ipsec
  authentication-type sha1-hmac ah-sha1-hmac
 !
!
vpn 0
 dns 8.8.4.4 secondary
 dns 8.8.8.8 primary
 interface ge0/0
  ip dhcp-client
  !
  tunnel-interface
   encapsulation ipsec
   color public-internet
.....
```

Same Capabilities

Feature Template

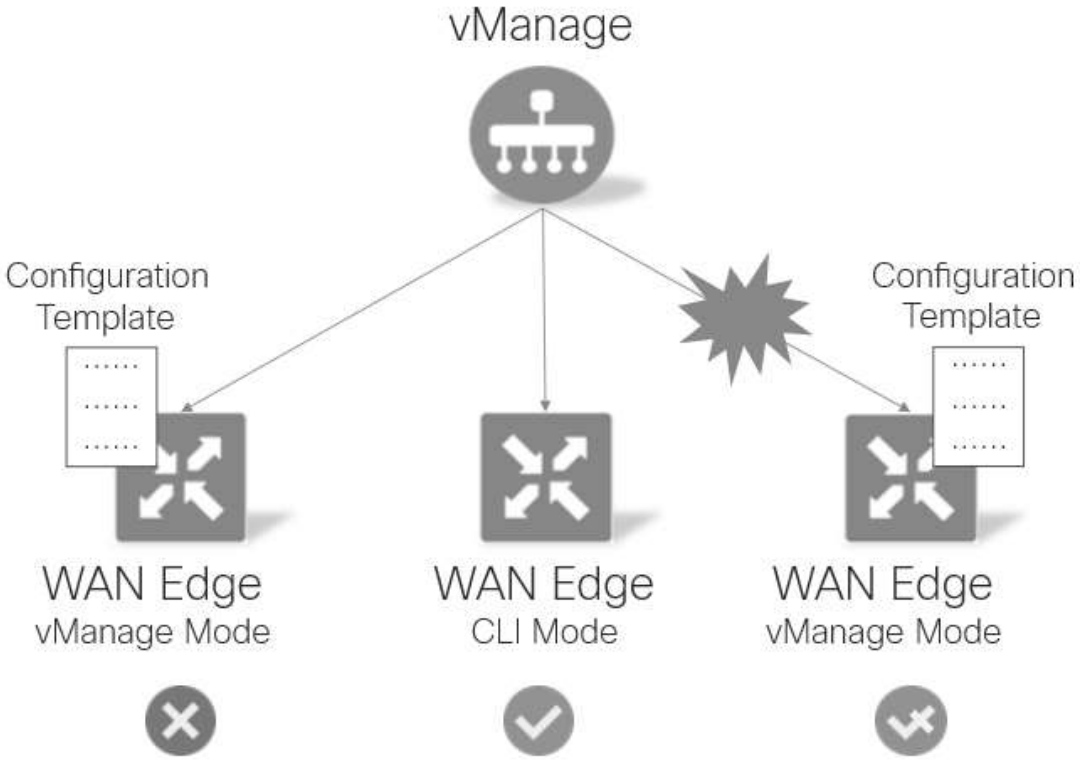


Device Configuration Template Distribution



- Configuration templates are distributed using NETCONF
- Configuration templates are defined for specific device model
  - vSmart, vManage and WAN Edge
  - Not vBond
- vManage itself can also be configured using configuration template

Device Configuration Template Impact



Local Changes Disallowed

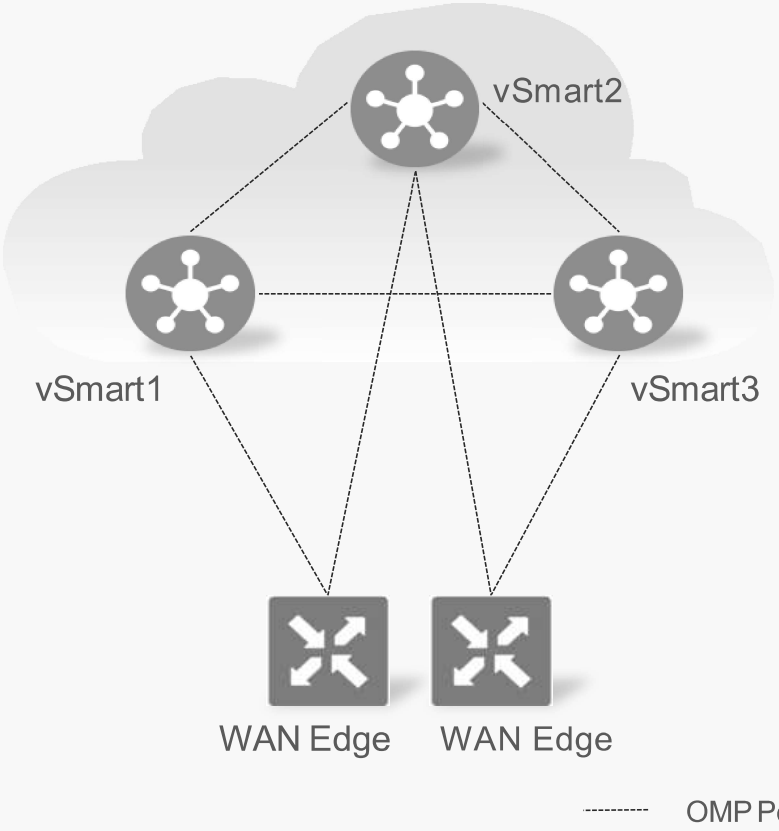
Local Changes Allowed

Local Changes Allowed

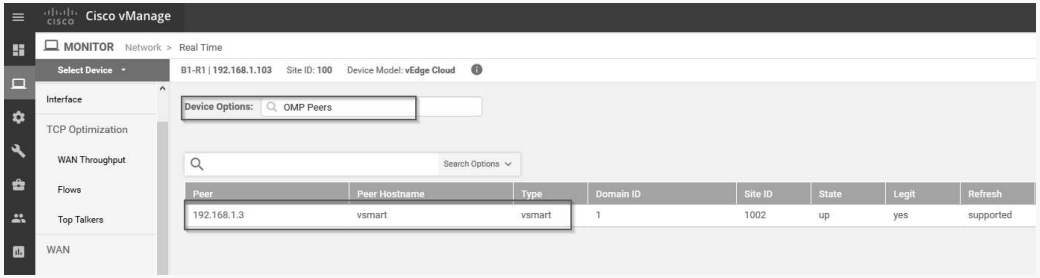
- Confirmation upon commit is required
- Rewritten by configuration template upon vManage connectivity recovery

Overlay Management Protocol

Overlay Management Protocol Overview

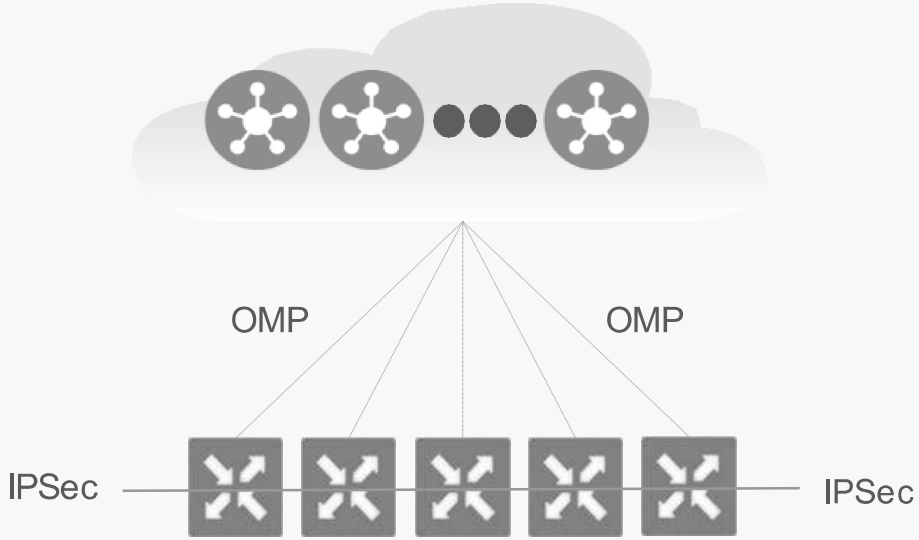


- TCP based extensible control plane protocol
- Runs between WAN Edge routers and vSmart controllers and between the vSmart controllers
  - Inside permanent TLS/DTLS connections
  - Automatically enabled on bring-up
- vSmarts create full mesh of OMP peers
- WAN Edge routers need not peer with all vSmarts



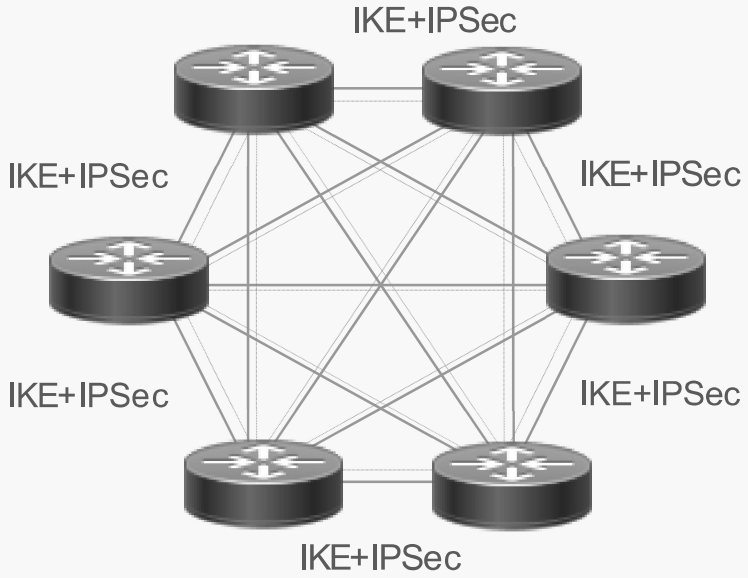
Control Plane Complexity

SD- WAN



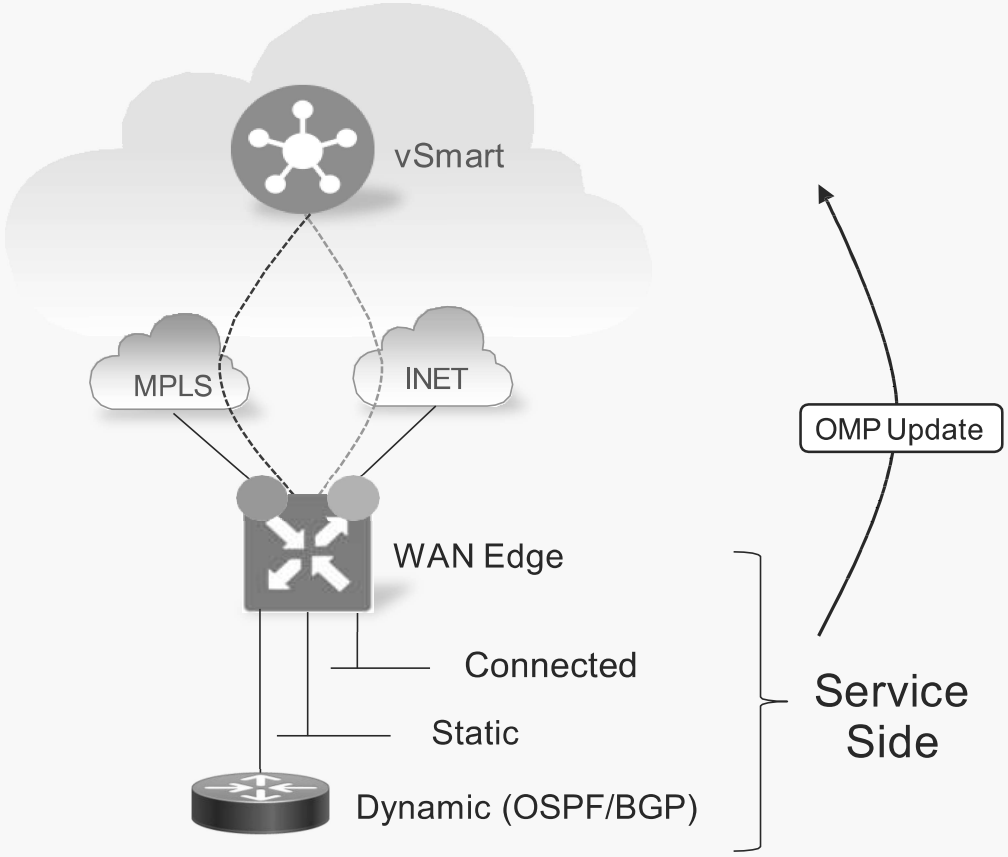
Linear Control Plane Complexity
O(n)

Traditional IPSec networks

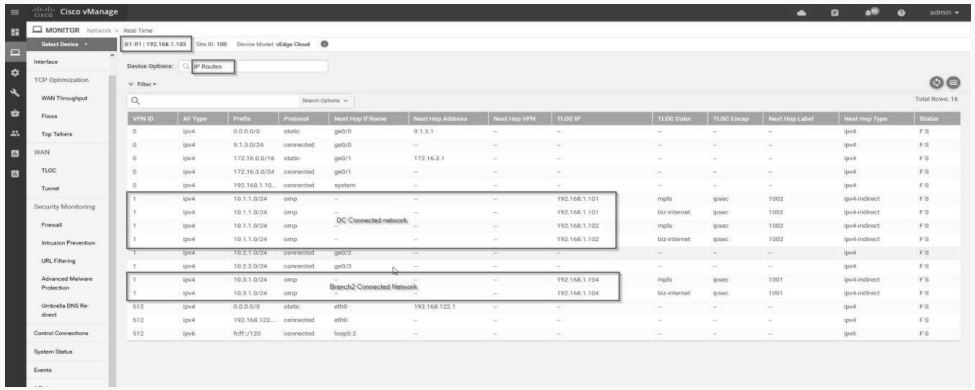


Quadratic Control Plane Complexity
O(n^2)

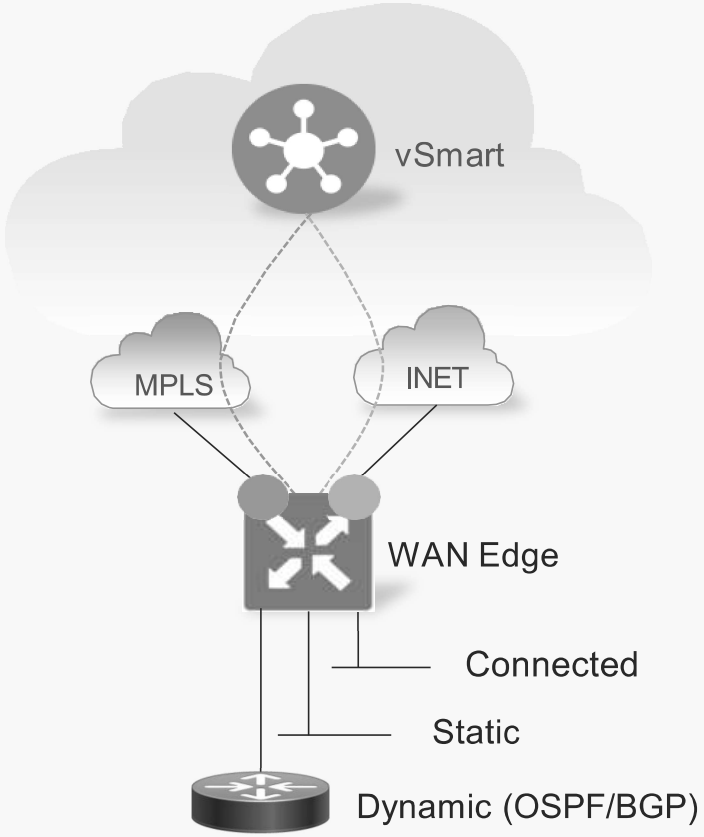
Overlay Routing: OMP Routes

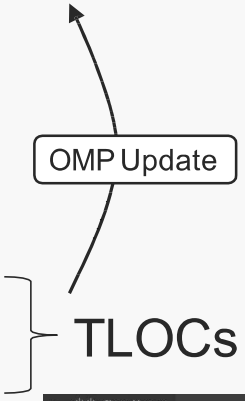


- Routes learnt from local service-side
- Advertised to vSmart controllers
- Most prominent attributes:
  - TLOC
  - Site-ID
  - Label
  - Tag
  - Preference
  - Originator System IP
  - Origin Protocol
  - Origin Metric
  - AS PATH

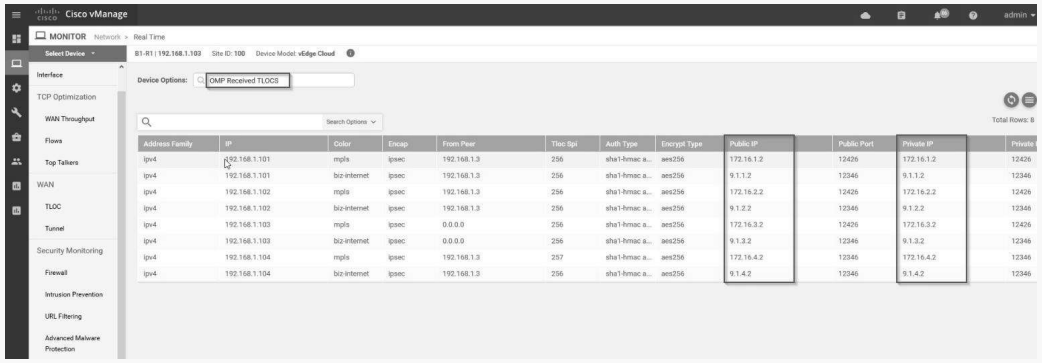


Overlay Routing: TLOC Routes

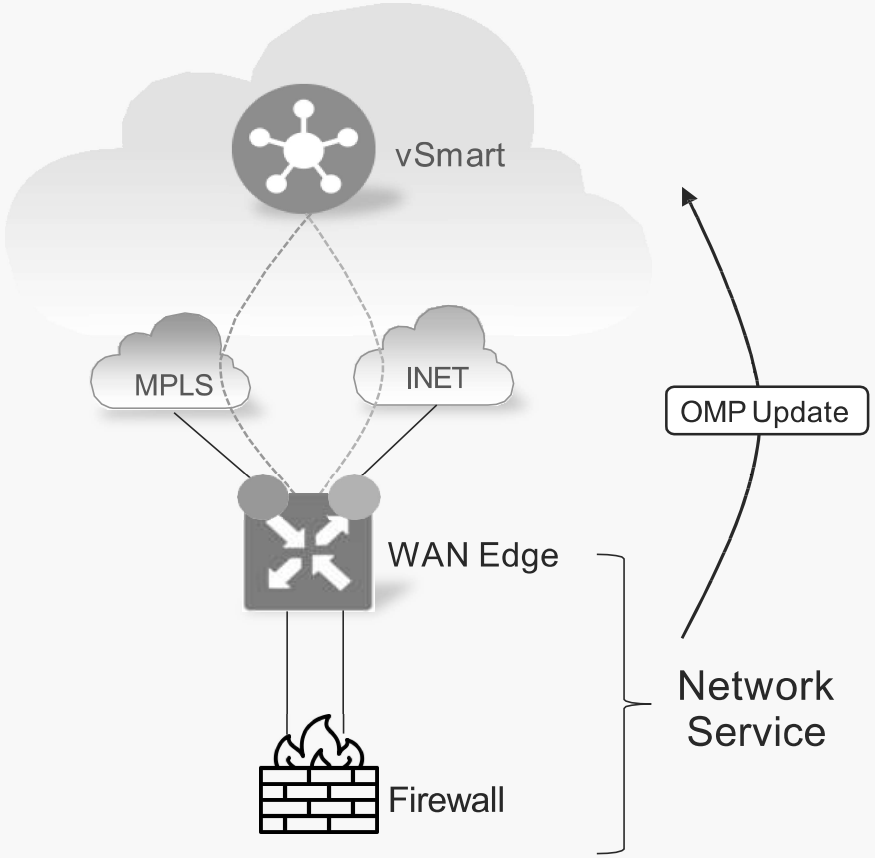




- Routes connecting locations to physical networks
- Advertised to vSmart controllers
- Most prominent attributes:
  - Site-ID
  - Encap-SPI
  - Encap-Authentication
  - Encap-Encryption
  - Public IP
  - Public Port
  - Private IP
  - Private Port
  - BFD-Status
  - Tag
  - Weight

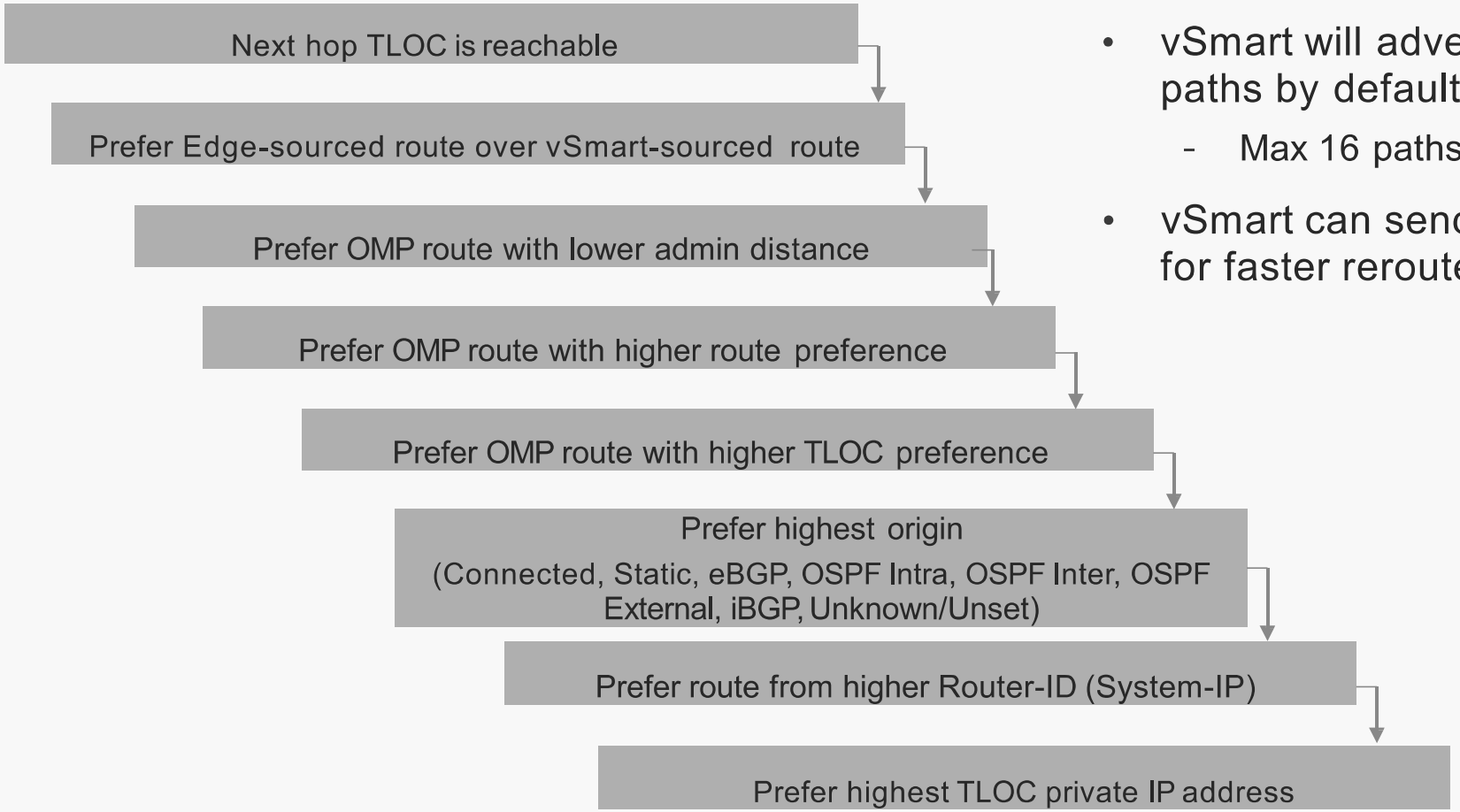


Overlay Routing: Network Service Routes



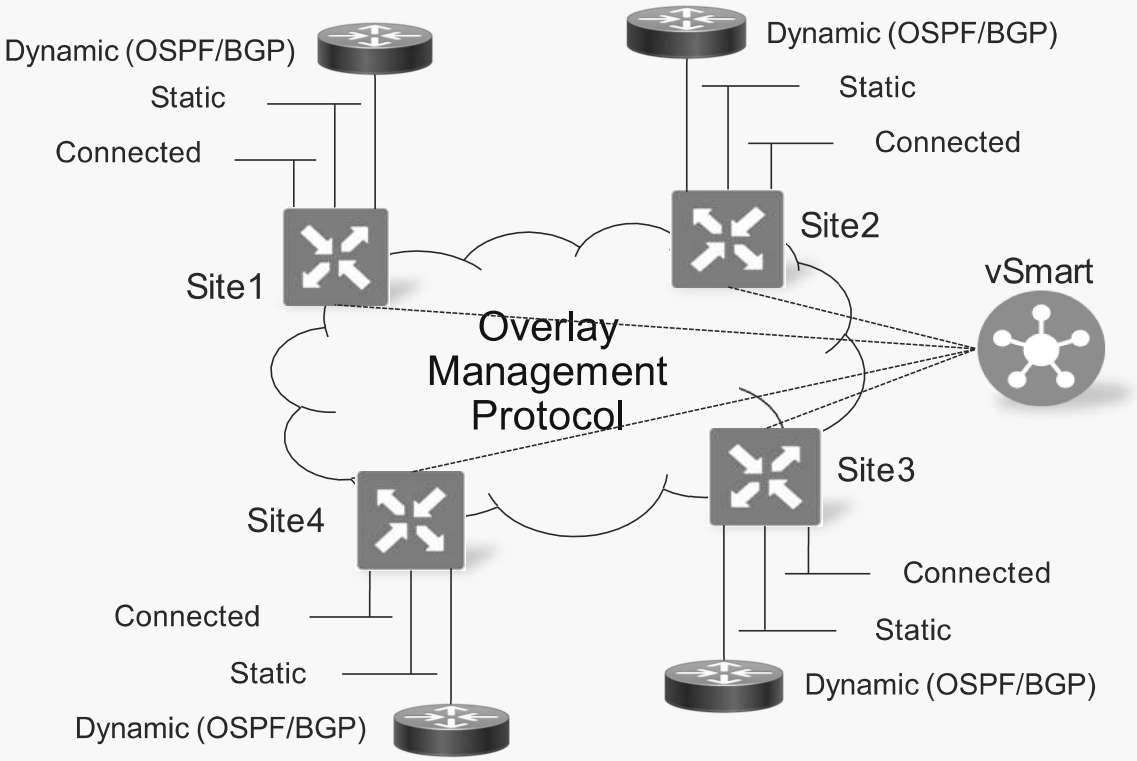
- Routes for advertised network services, i.e. Firewall, IDS, IPS, generic
- Advertised to vSmart controllers
- Most prominent attributes:
  - VPN-ID
  - Service-ID
  - Originator System IP
  - TLOC

OMP Best-Path Algorithm and Loop Avoidance



- vSmart will advertise 4 ECMP paths by default
  - Max 16 paths
- vSmart can send backup path for faster reroute on WAN Edge

Overlay Routing

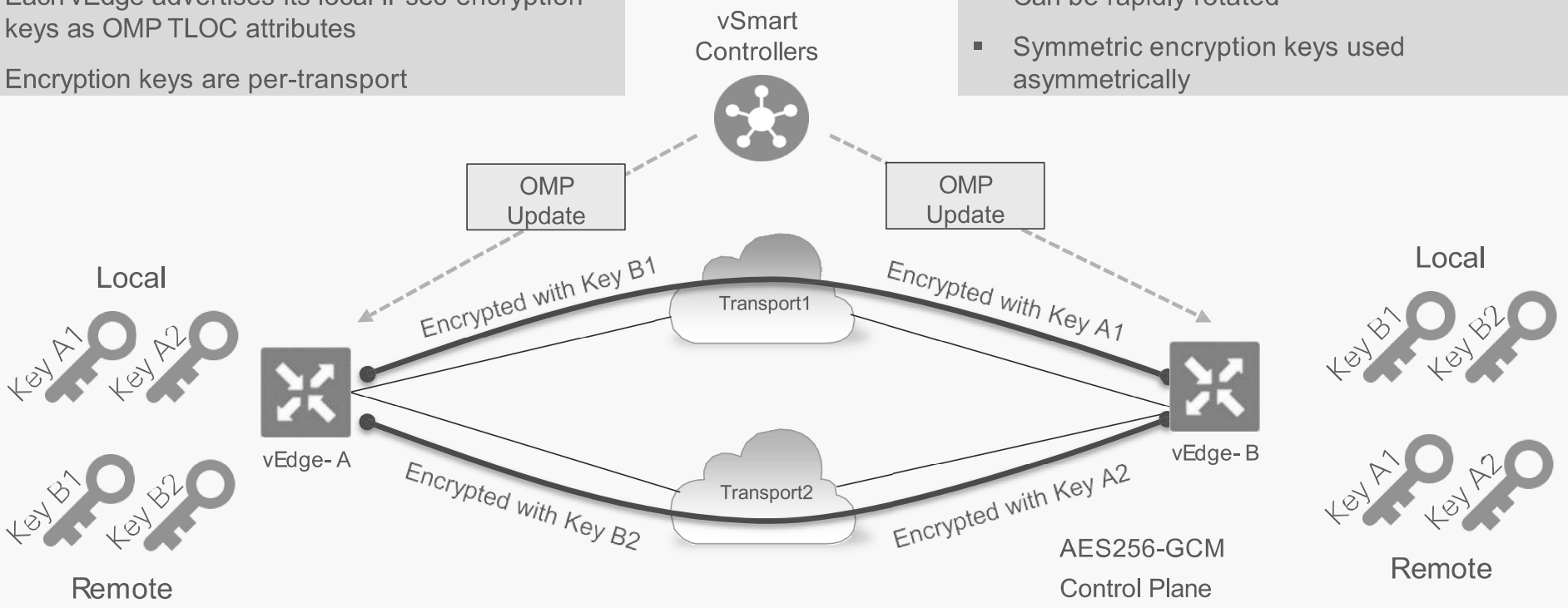


- Uniform control plane protocol
- OMP learns and translates routing information across the overlay
  - OMP routes, TLOC routes, network service routes
  - Unicast and multicast address families
  - IPv4 and IPv6 (future)
- Distribution of data-plane security parameters and policies
- Implementation of control (routing) and VPN membership policies

Data Plane Security Encryption

- Each vEdge advertises its local IPsec encryption keys as OMP TLOC attributes
- Encryption keys are per-transport

- Can be rapidly rotated
- Symmetric encryption keys used asymmetrically



OMP - Routes

Advertise routes (Similar to BGP prefixes)

```
pm8003# show omp routes vpn 1 1.17.100.0/24 |t
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
U   -> TLOC unresolved

                PATH                    ATTRIBUTE
FROM PEER       ID     LABEL    STATUS  TYPE       TLOC IP          COLOR            ENCAP  PREFERENCE
-----------------------------------------------------------------------------------------------------
172.16.240.172  43265  1002     C,I,R   installed  172.16.248.6     biz-internet     ipsec  -
172.16.240.172  43266  1002     C,I,R   installed  172.16.248.6     public-internet  ipsec  -
172.16.240.172  43267  1002     C,I,R   installed  172.16.248.6     gold             ipsec  -
172.16.240.174  43576  1002     C,R     installed  172.16.248.6     biz-internet     ipsec  -
172.16.240.174  43577  1002     C,R     installed  172.16.248.6     public-internet  ipsec  -
172.16.240.174  43578  1002     C,R     installed  172.16.248.6     gold             ipsec  -
```

OMP - TLOCS

Advertise TLOCS (Similar to BGP next-hops)

```
pm8003# show omp tlocs received
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Stg -> staged
Inv -> invalid
```

TLOC IP	COLOR	ENCAP	FROM PEER	STATUS	PSEUDO KEY	PUBLIC IP	PUBLIC PORT	PRIVATE IP	PRIVATE PORT	PUBLIC IPV6	PUBLIC IPV6 PORT	PRIVATE IPV6	PRIVATE IPV6 PORT	BFD STATUS
172.16.241.1	gold	ipsec	172.16.240.172	C,I,R	1	183.103.103.11	12346	183.103.103.11	12346	8034::20c:29ff:fe2b:d08d	12346	8034::20c:29ff:fe2b:d08d	12346	up
			172.16.240.174	C,R	1	183.103.103.11	12346	183.103.103.11	12346	8034::20c:29ff:fe2b:d08d	12346	8034::20c:29ff:fe2b:d08d	12346	up
172.16.241.2	biz-internet	ipsec	172.16.240.172	C,I,R	1	183.102.102.12	12346	183.102.102.12	12346	8033::20c:29ff:fea7:4d82	12346	8033::20c:29ff:fea7:4d82	12346	up
			172.16.240.174	C,R	1	183.102.102.12	12346	183.102.102.12	12346	8033::20c:29ff:fea7:4d82	12346	8033::20c:29ff:fea7:4d82	12346	up
172.16.241.2	public-internet	ipsec	172.16.240.172	C,I,R	1	183.101.101.12	12346	183.101.101.12	12346	8033::20c:29ff:fea7:4d64	12346	8033::20c:29ff:fea7:4d64	12346	up
			172.16.240.174	C,R	1	183.101.101.12	12346	183.101.101.12	12346	8033::20c:29ff:fea7:4d64	12346	8033::20c:29ff:fea7:4d64	12346	up
172.16.241.2	3g	ipsec	172.16.240.172	C,I,R	1	183.104.104.12	12346	183.104.104.12	12346	::	0	::	0	up
			172.16.240.174	C,R	1	183.104.104.12	12346	183.104.104.12	12346	::	0	::	0	up
172.16.241.2	red	ipsec	172.16.240.172	C,I,R	1	183.103.103.13	12346	200.200.200.2	12346	::	0	::	0	down
			172.16.240.174	C,R	1	183.103.103.13	12346	200.200.200.2	12346	::	0	::	0	down
172.16.241.2	gold	ipsec	172.16.240.172	C,I,R	1	183.103.103.12	12346	183.103.103.12	12346	8034::20c:29ff:fea7:4d8c	12346	8034::20c:29ff:fea7:4d8c	12346	up
			172.16.240.174	C,R	1	183.103.103.12	12346	183.103.103.12	12346	8034::20c:29ff:fea7:4d8c	12346	8034::20c:29ff:fea7:4d8c	12346	up

OMP - Routes

Best path selection

- When multiple vSmarts advertise the same prefix, the vEdge has to make a decision of selecting the best-path out of the multiple vSmarts
- The vEdge would INSTALL those routes, where the vSmart has a lower system-ip
- Below, 172.16.240.172 is lower than 172.16.240.174.
- Hence, the vEdge has marked the routes coming from .172 as C,I,R (I-installed) and .174 as C,R
- It will then ECMP between the tlocs advertised by .172

```
pm8003# show omp routes vpn 1 1.17.100.0/24 |t
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
U   -> TLOC unresolved

                PATH                    ATTRIBUTE
FROM PEER       ID     LABEL    STATUS  TYPE       TLOC IP          COLOR            ENCAP  PREFERENCE
-----------------------------------------------------------------------------------------------------
172.16.240.172  43265  1002     C,I,R   installed  172.16.248.6     biz-internet     ipsec  -
172.16.240.172  43266  1002     C,I,R   installed  172.16.248.6     public-internet  ipsec  -
172.16.240.172  43267  1002     C,I,R   installed  172.16.248.6     gold             ipsec  -
172.16.240.174  43576  1002     C,R     installed  172.16.248.6     biz-internet     ipsec  -
172.16.240.174  43577  1002     C,R     installed  172.16.248.6     public-internet  ipsec  -
172.16.240.174  43578  1002     C,R     installed  172.16.248.6     gold             ipsec  -
```

OMP - Routes

Advertise Routes:
with preference 100 on biz-internet and public-internet set on far-end vEdge which has system-ip 172.16.248.6)

FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP	COLOR	ENCAP
172.16.240.172	43265	1002	C,I,R	installed	172.16.248.6	biz-internet	ipsec
172.16.240.172	43266	1002	C,I,R	installed	172.16.248.6	public-internet	ipsec
172.16.240.172	43267	1002	R	installed	172.16.248.6	gold	ipsec
172.16.240.174	43576	1002	C,R	installed	172.16.248.6	biz-internet	ipsec
172.16.240.174	43577	1002	C,R	installed	172.16.248.6	public-internet	ipsec
172.16.240.174	43578	1002	R	installed	172.16.248.6	gold	ipsec

Best path selection in this case:

- .172 wins over .174
- Higher preference wins. So color=gold (preference=0) has lost to colors biz-internet and public-internet (which have preference=100 each)

Route Prioritization

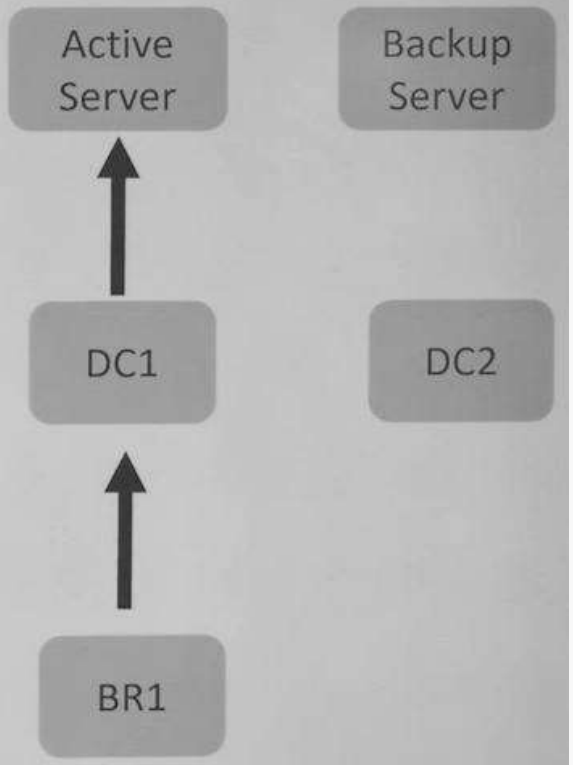
Problem Description

Setup:

- Two Data Centers
- Critical Server has the same IP in both DCs

Problem:

How can I prefer 1st DC and use the 2nd as backup?



Solution

Define different OMP route preferences on DC1 and DC2 for desired IP network.

OMP Route Preference Values: 0 through 255. Higher value is preferred.

OMP Table

"192.168.55.55/32 via DC1 has preference 200"
"192.168.55.55/32 via DC2 has preference 100"

IP Table

"192.168.55.55/32 via DC1"

If the OMP route via DC1 will fail, we will immediately install route via DC2.

Configuration for Route Prioritization

DC1 Routers (site-id 101)

```
vpn 10
 ...
 ip route 192.168.55.55/32 10.101.10.254
!
```

DC2 Routers (site-id 102)

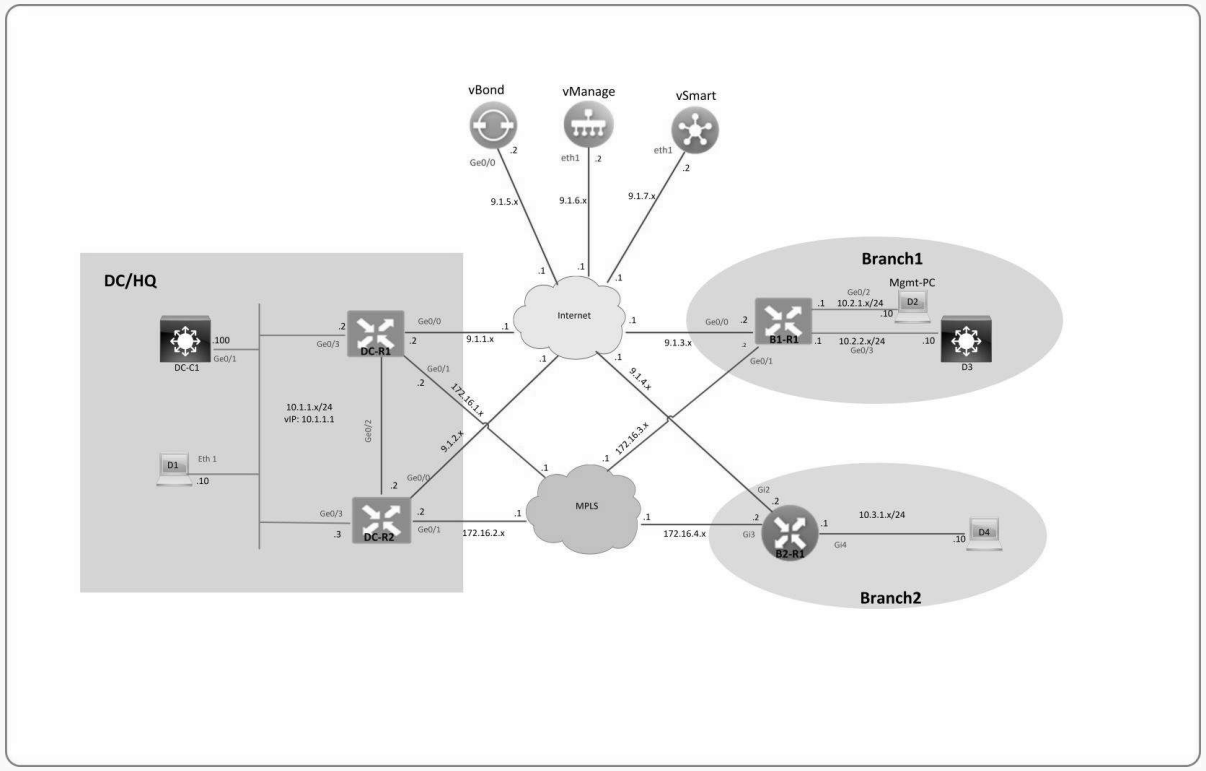
```
vpn 10
 ...
 ip route 192.168.55.55/32 10.102.10.254
!
```

vSmart

```
omp
 send-backup-paths
!
control-policy part-mesh-br1
 sequence 10
  match route
   site-id 101
   vpn     10
  !
  action accept
   set
    preference 200
   !
  !
 !
 default-action accept
!
```

Control Policy

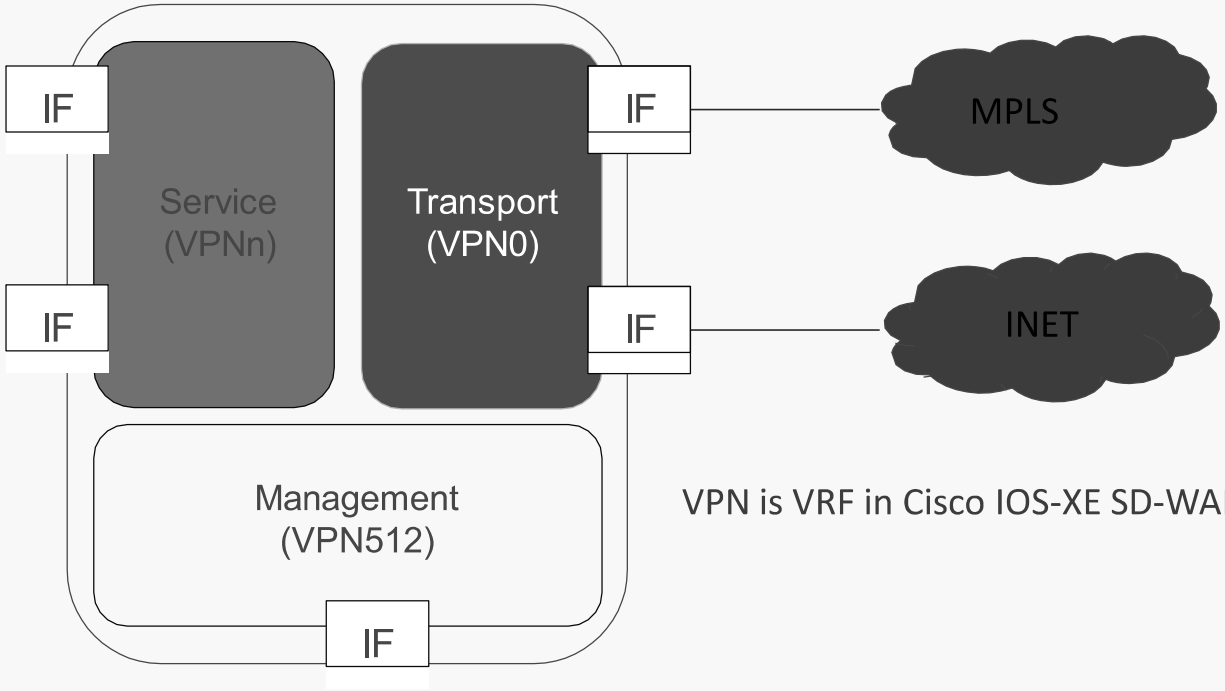
VRRP



- Similar to VRRP on IOS Routers
- OMP Tracking

Segmentation

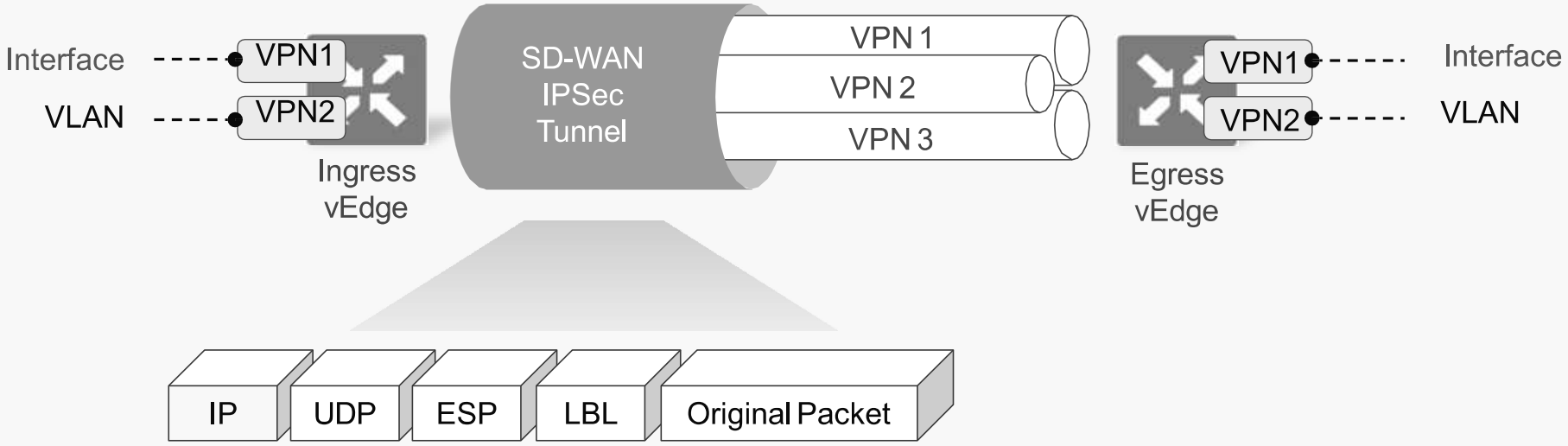
Secure Segmentation – VPNs



VPN is VRF in Cisco IOS-XE SD-WAN Routers

VPN0 (vEdge) = Default VRF (cEdge)

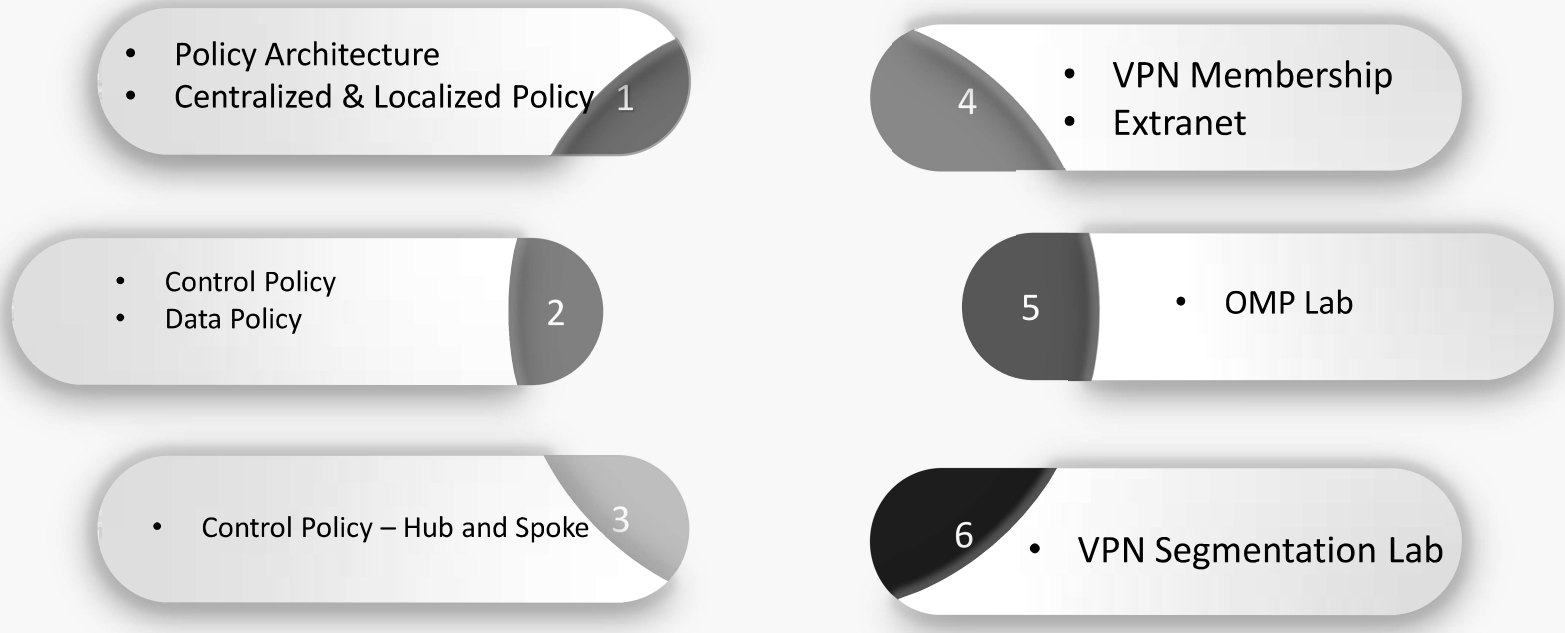
End-to-End Segmentation



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

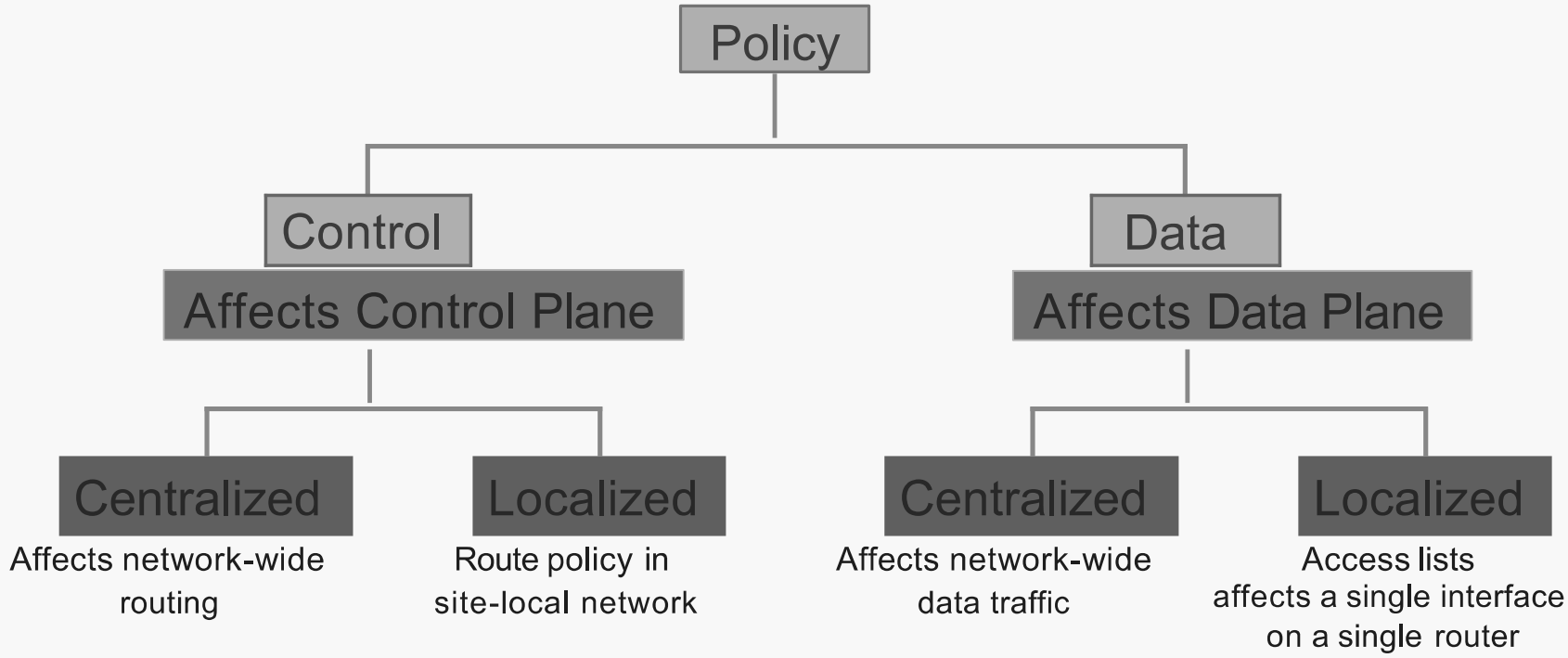
Break

Cisco SD-WAN Training – Day3



Policy Framework

Policy Configuration Overview



- Clear separation exists between control plane and data plane policies
- Clear separation exists between centralized and localized functions

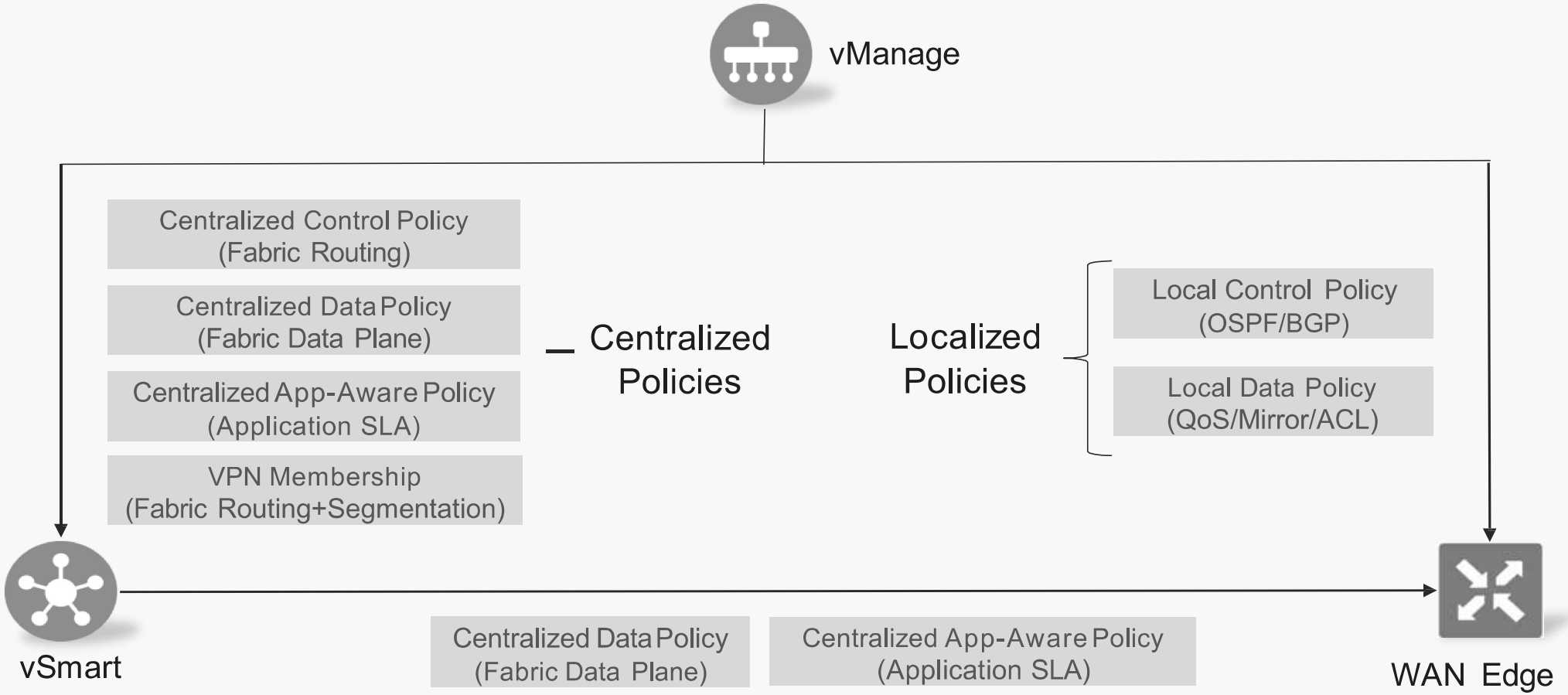
vSmart Overlay Policy Architecture

- vSmart Policies consist of these building blocks:
- Lists used for defining targets of policy application or matching
- Policies controlling aspects of control and forwarding
  - app-route-policy
  - cflowd-template
  - control-policy
  - data-policy
  - vpn-membership-policy
- Policy Application to control towards what a policy is applied
  - Site-oriented and defined by a site-list

WAN Edge Service Routing Policy Architecture

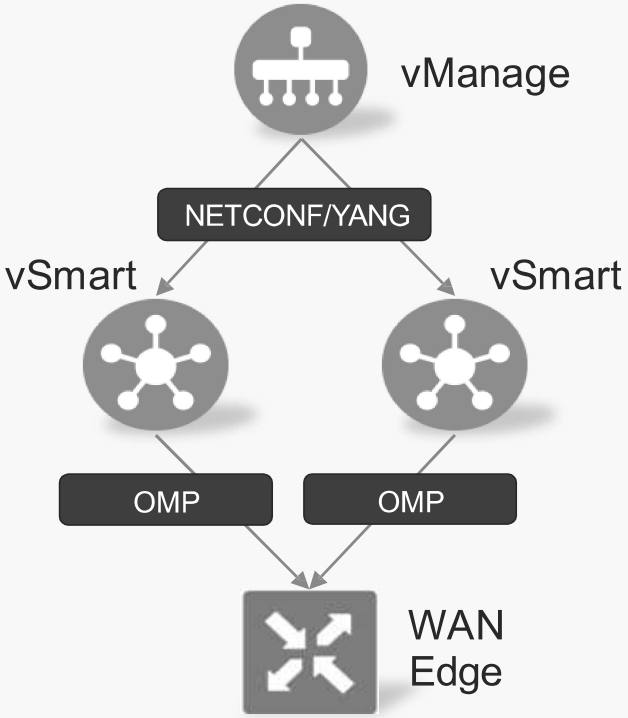
- Routing Policies are traditional routing policies
- Attaches to BGP or OSPF locally on the WAN Edge
- Used in the traditional sense for controlling BGP and OSPF
  - Information exchange
  - Attributes
  - Path Selection

Policy Framework

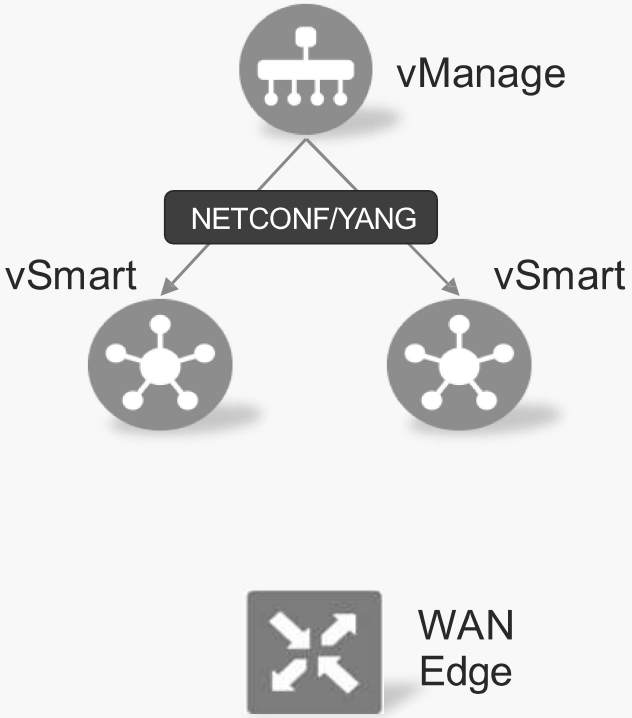


Policy Distribution

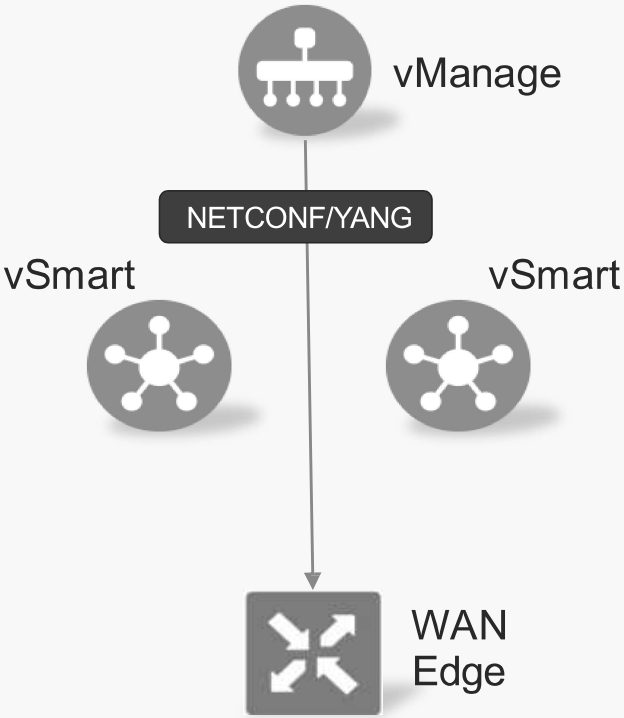
Data Policy
App Aware Routing Policy



Control Policy
VPN Membership Policy

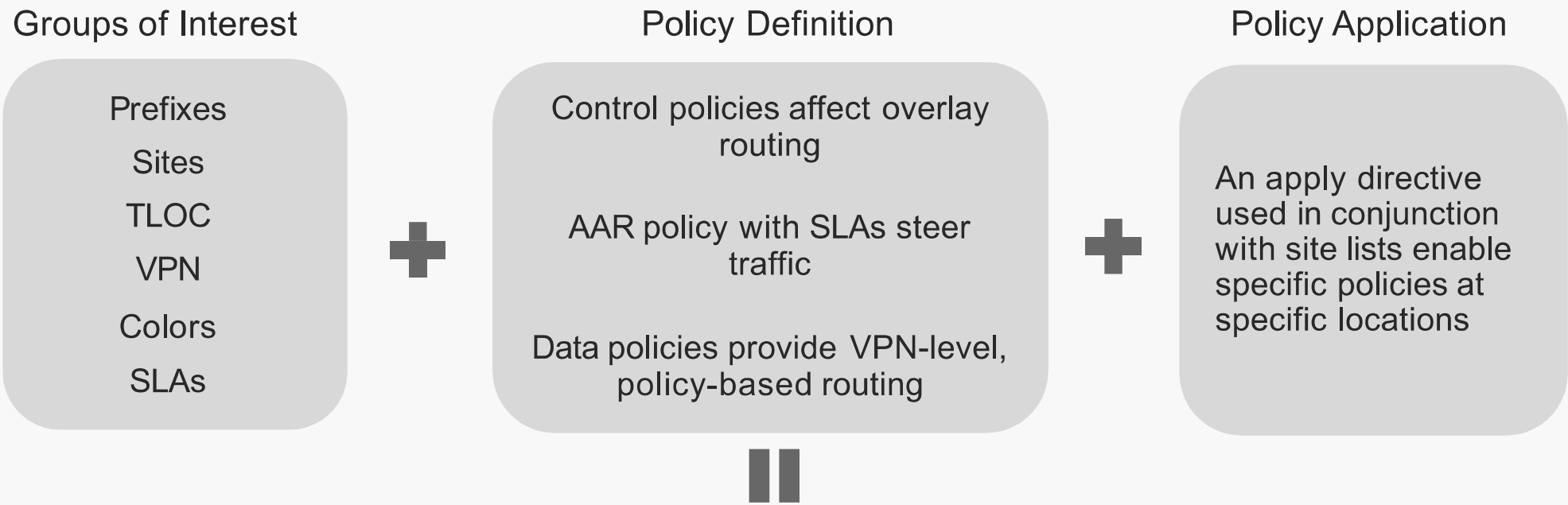


Local Policies

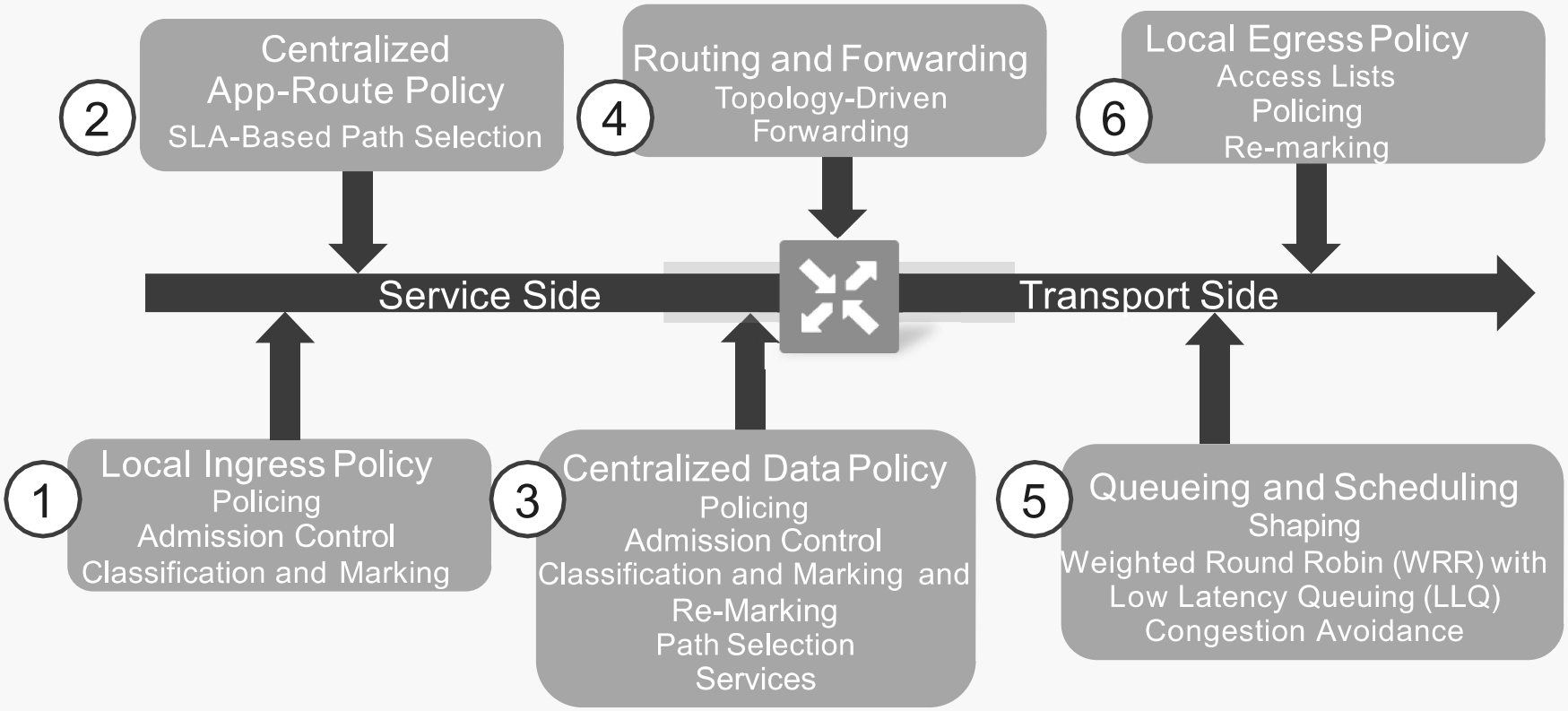


Building Blocks of Centralized Policies

- Assemble the three building blocks to configure vSmart policies: Groups of Interest, Policy Definition, and Policy Application.



Order of Operation on WAN Edge



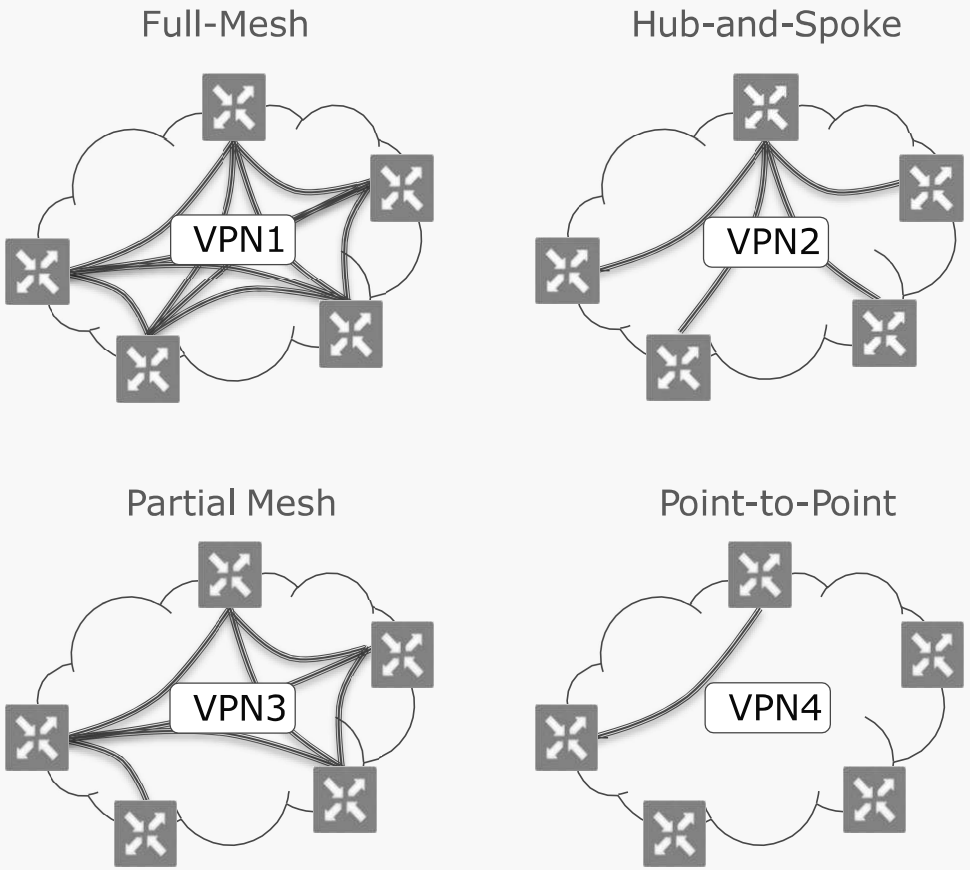
Control Policies

Control Policies

- Configured on vManage. Enabled and enforced on vSmart controllers. They do not get forwarded to WAN Edge routers.
  - Control policies operate on OMP routing information received from or sent to WAN Edge routers. They can filter OMP updates or modify various attributes.
- Control policies can be very powerful tool changing routing behavior of the entire SD-WAN fabric
- Control policies are used to enable many services, such as:
  - Service Chaining
  - Traffic Engineering
  - Extranet VPNs
  - Service and Path affinity
  - Arbitrary VPN Topologies
  - and more …

Arbitrary VPN Topologies

- Each VPN can have it's own topology
  - Full-mesh, hub-and-spoke, partial-mesh, point-to-point, etc…
- VPN topology can be influenced by leveraging control policies
  - Filtering TLOCs or modifying next-hop TLOC attribute for routes
- Applications can benefit from shortest path, e.g. voice takes full-mesh toplogy
- Security compliance can benefit from controlled connectivity topology, e.g. PCI data takes hub-and-spoke topology

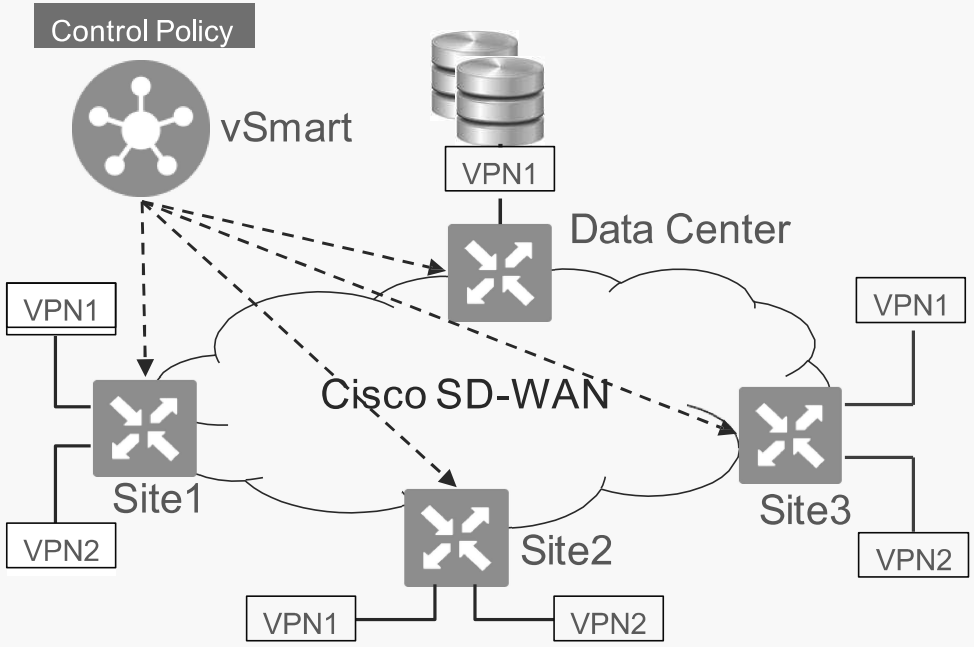


Control Policy – Arbitrary VPN Topologies

- Problem: Different VPNs must be provided with different connectivity based on applications being serviced in each VPN

  VPN 1: CRM System = Hub and Spoke, VPN 2: Voice = Full Mesh

- Solution: Deploy control policy to control VPN topology



Policy Details:

VPN1 - vSmart advertises just the DC prefixes to Spokes and denies everything else on VPN1.

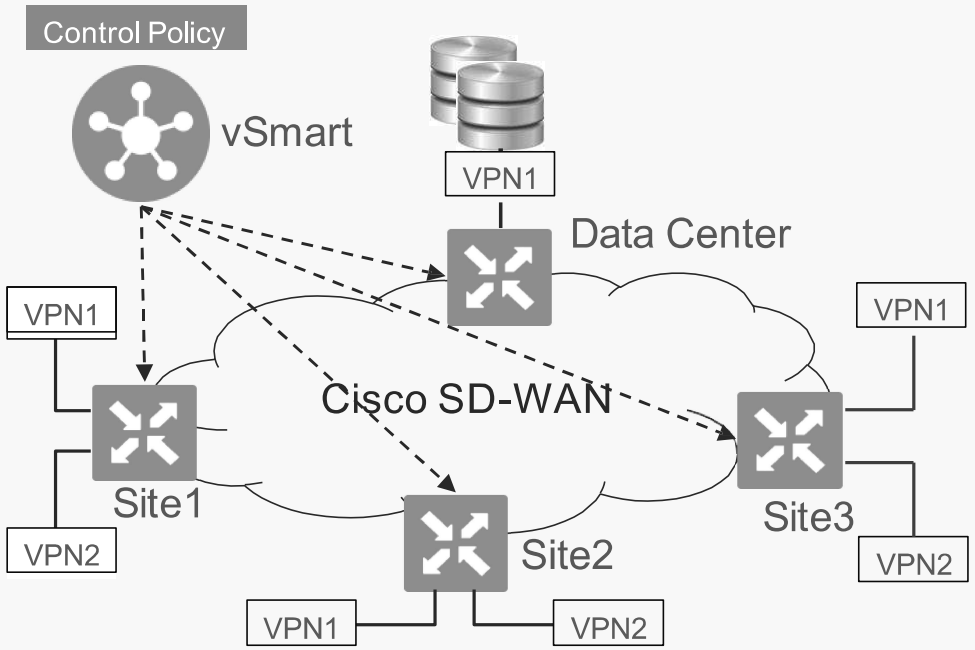
VPN2 - No filter all the prefixes are advertised to every node on VPN2

Control Policy – Arbitrary VPN Topologies

```
policy
 lists
  site-list Branches
   site-id 1-3
 !
  vpn-list CRM
   vpn 1
 !
```

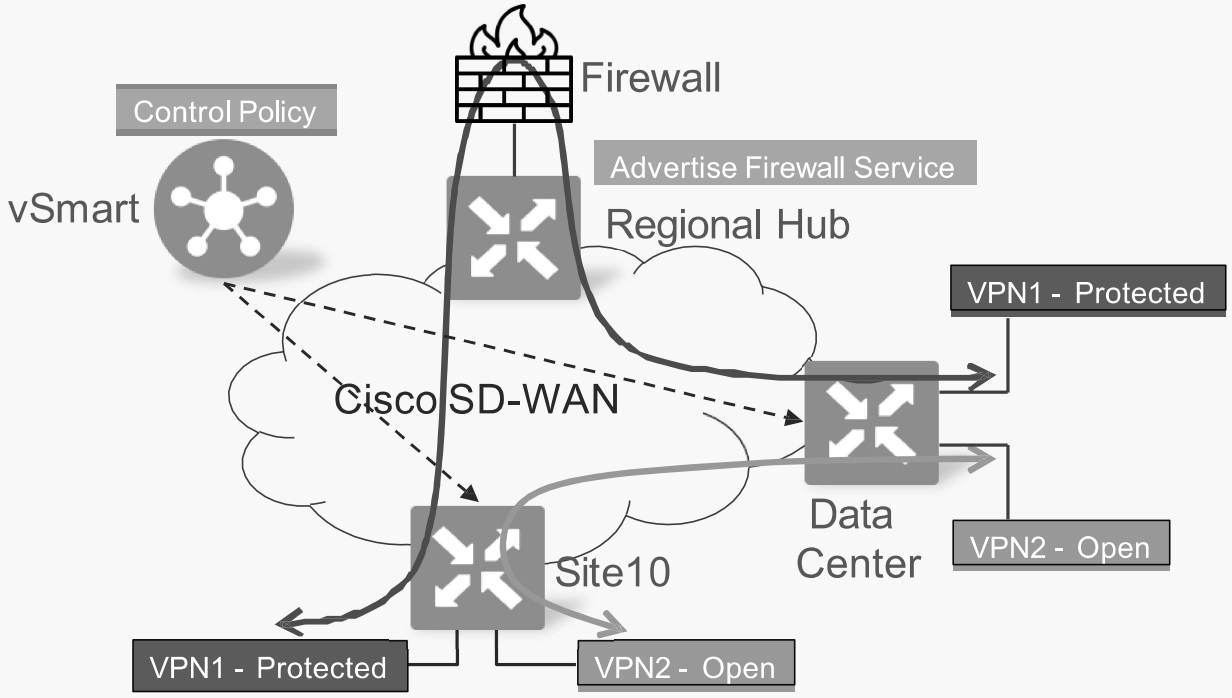
```
control-policy ArbitraryTopology
  sequence 10
   match route
    vpn-list CRM
    site-list Branches
   !
   action reject
  !
!
default-action accept
```

```
apply-policy
 site-list Branches
  control-policy ArbitraryTopology out
```



Control Policy Example – Service Insertion

- Problem: Certain departments require Firewall protection when interacting with data center networks, while other departments do not
- Solution: Deploy a service chained Firewall service per-VPN



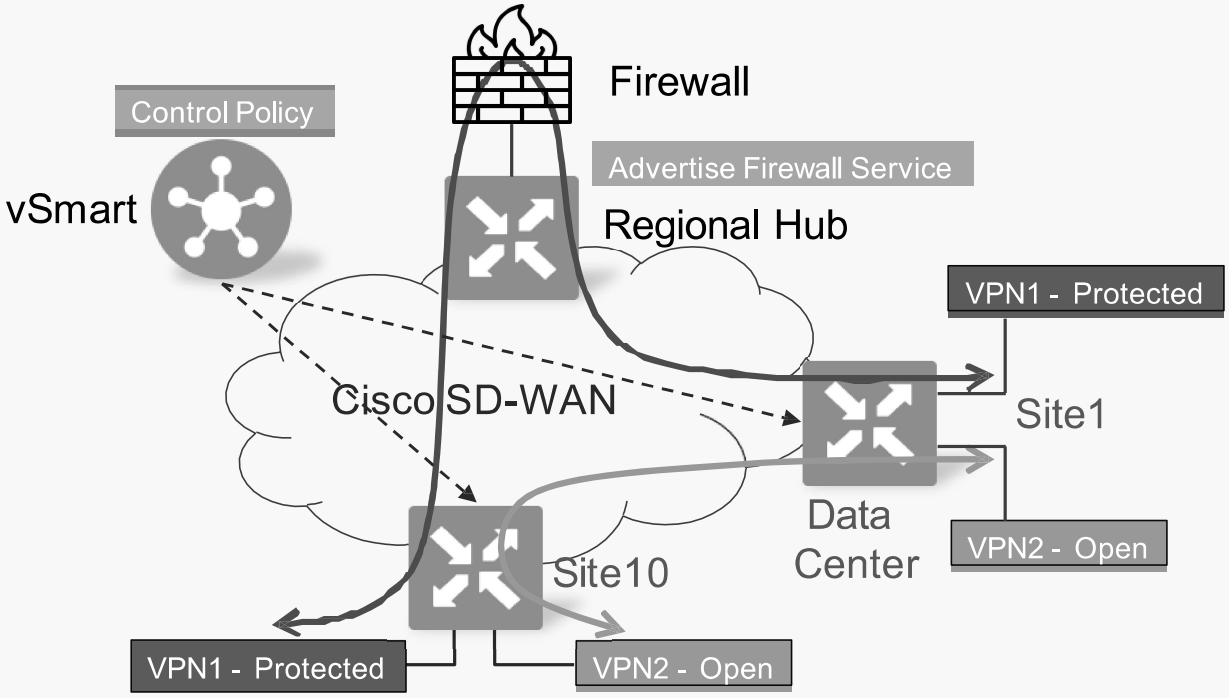
Policy Details:

Regional hub advertises availability of Firewall service

Bi-directionally modify TLOC next hop attribute for VPN1 traffic between Site1 and Data Center to point at regional hub TLOCs

Control Policy Example – Service Insertion

```
! Applied on Regional Hub
  vpn 1
    service netsvc1 address 10.0.1.1
```



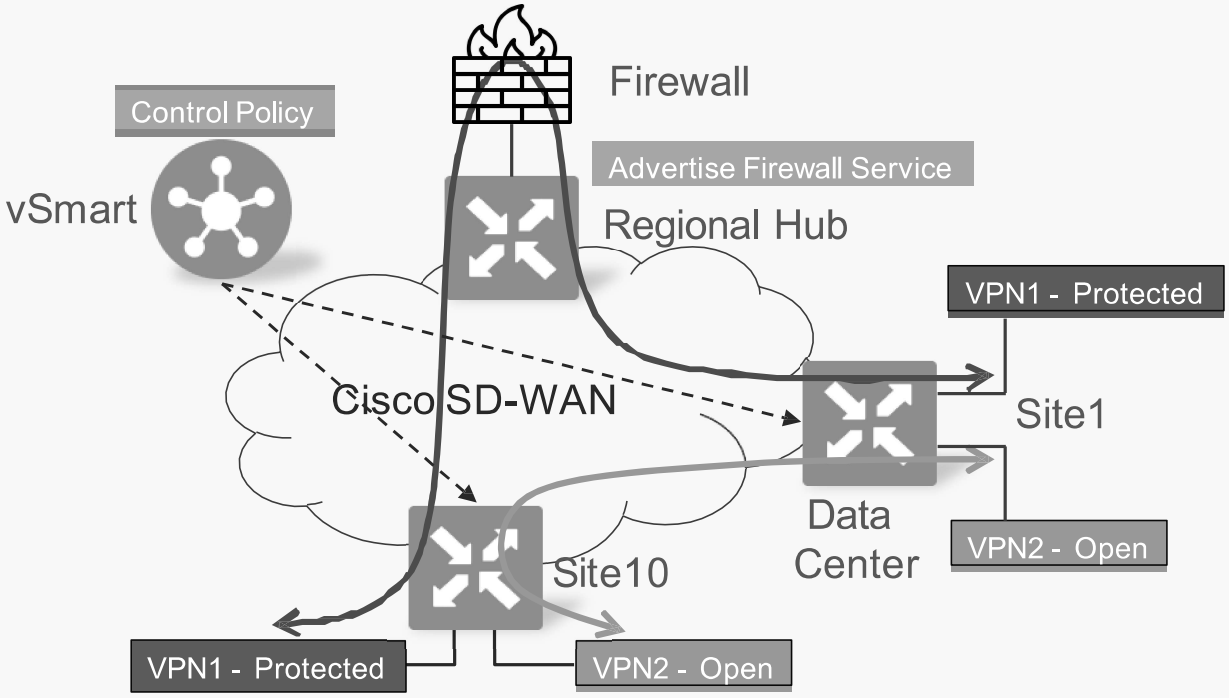

```
policy
 lists
   site-list fw-inspected
     site-id 10
   !
```

```
control-policy fw-service
   sequence 10
    match  route
    vpn 1
     site-id 1
    action accept
     set service netsvc1 vpn 1
   !
   default-action accept
  !
```

```
apply-policy
 site-list fw-inspected
  control-policy fw-service out
 !
```

Control Policy Example – Service Insertion

```
! Applied on Regional Hub
  vpn 1
    service netsvc1 address 10.0.1.1
```



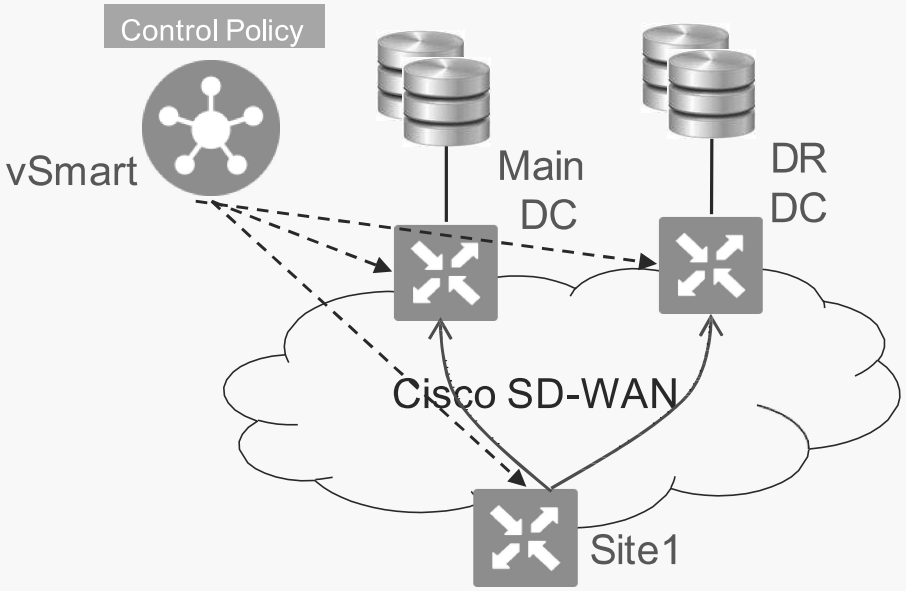

```
policy
 lists
  site-list dc
   site-id 1
  !
```

```
control-policy fw-service-return
  sequence 10
   match  route
   vpn 1
    site-id 10
   action accept
    set service netsvc1 vpn 1
  !
  default-action accept
 !
```

```
apply-policy
 site-list dc
  control-policy fw-service-return out
 !
```

Control Policy Example – Data Center Priority

- Problem: Prefer main data center over DR data center. If main data center fails, traffic should reroute to DR data center.
- Solution: Deploy control policy to influence TLOC priority



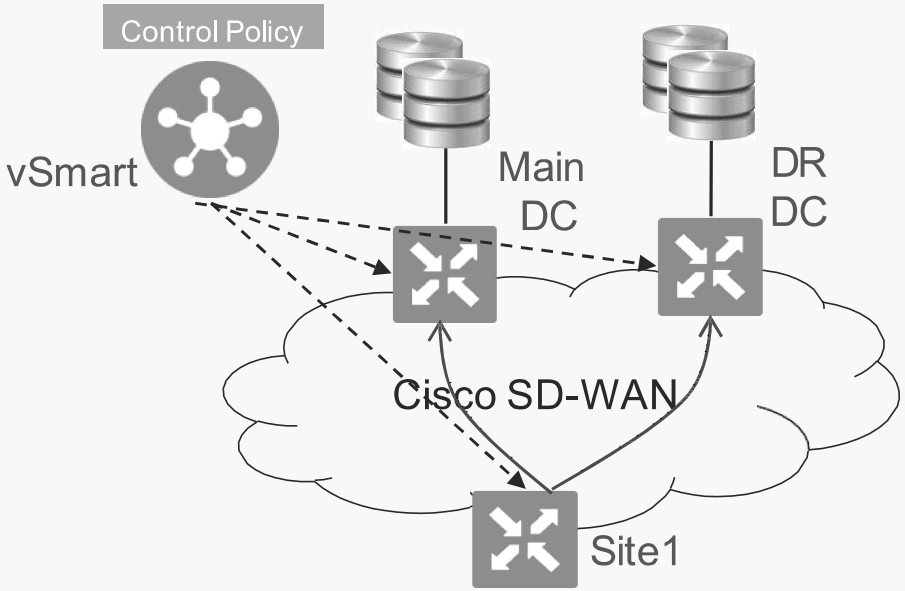
Policy Details:

Set higher preference on main data center TLOCs than on DR data center TLOCs

Preference is set on all TLOC colors using TLOC list

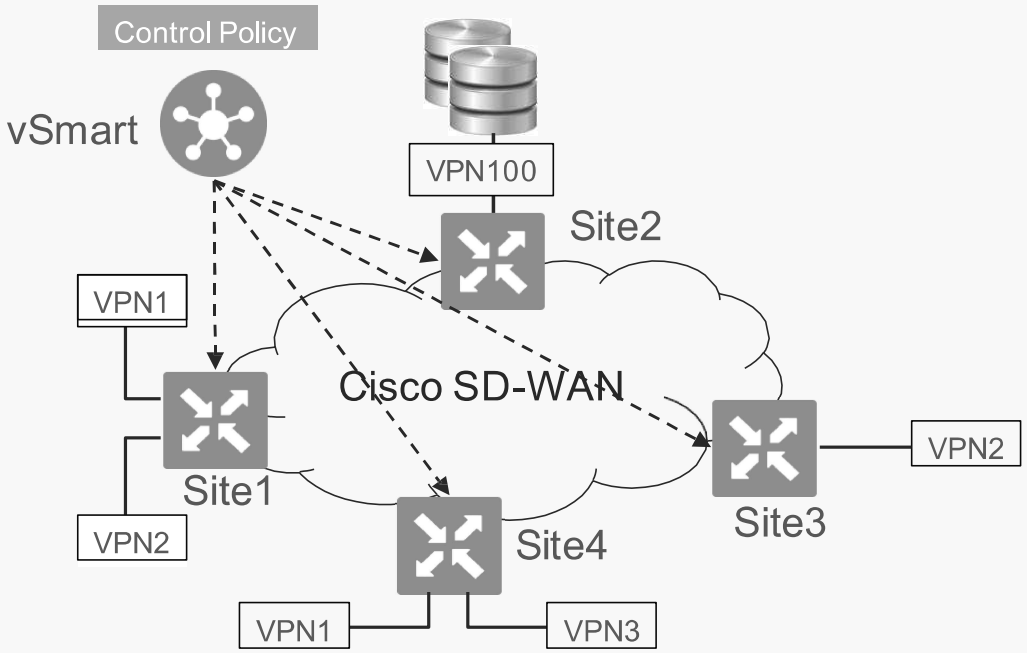
Control Policy Example – Data Center Priority

```
policy
 lists
  site-list Branches
   site-id 3-10
  tloc-list Main-DC-tlocs
   tloc-id 10.1.1.1 biz-internet
   tloc-id 10.1.1.1 mpls

control-policy prefer-Main-DC
  sequence 10
   match tloc
    tloc-list Main-DC-tlocs
   action accept
    set preference 50
 default-action accept

apply-policy
 site Branches
  control-policy prefer-Main-DC out
```



Control Policy Example – Shared Services

- Problem: Services residing in a VPN must be shared across users residing in multiple other VPNs. Some VPNs don't need access to shared services.
- Solution: Deploy control policy with route exports



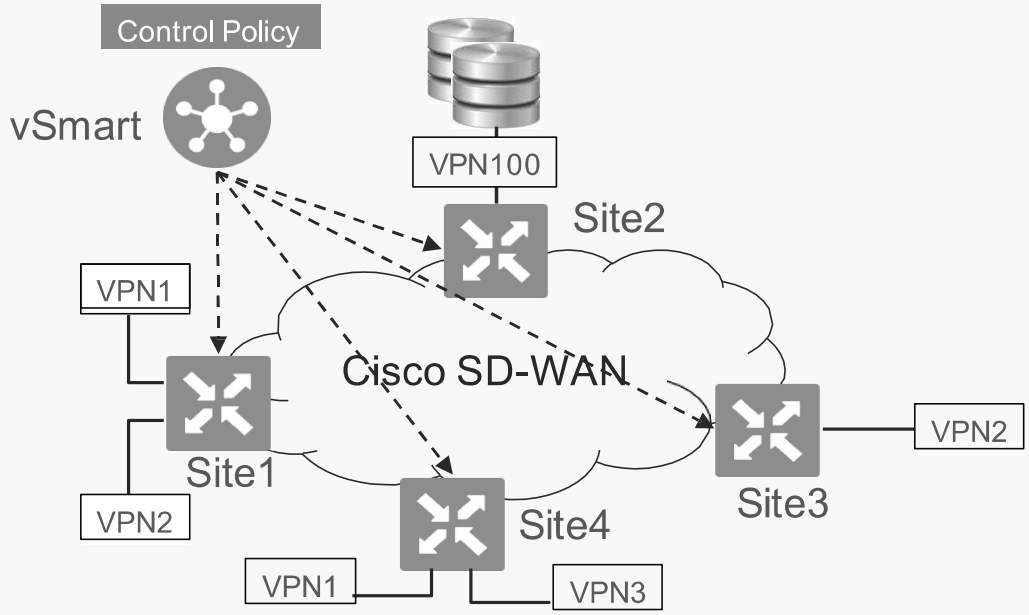
Policy Details:

Export VPN2 and VPN3 routes into shared service VPN100, and vice versa

VPN1 cannot communicate with VPN2, VPN3 or VPN100

Control Policy Example – Shared Services

```
policy
 lists
  site-list all-extranet-sites
   site-id 1-4
  vpn-list extranet-clients
   vpn-id 2-3
  prefix-list extranet-srv-prefix
   ip-prefix 10.1.1.0/24
```




```
control-policy extranet
   sequence 10
    match route
     vpn-list extranet-clients
    action accept
     export-tovpn 100
   !
   sequence 20
    match  route
    vpn 100
     prefix-list extranet-srv-prefix
    action accept
     export-to vpn-listextranet-clients
     !
    !
   default-action accept
  !
```

```
apply-policy
 site-list all-extranet-sites
  control-policy extranet in
!
```

Break

Cisco SD-WAN Training – Day4

1
- Internet Exit
- DC Backhaul Internet access
- Direct Internet Access

2
- Application Aware Routing
- Service Chaining

3
- Quality of Service using Localized Policy

4
- Hub and Spoke Lab

5
- Service chaining Lab

6
- Internet Exit Lab (DC and DIA)

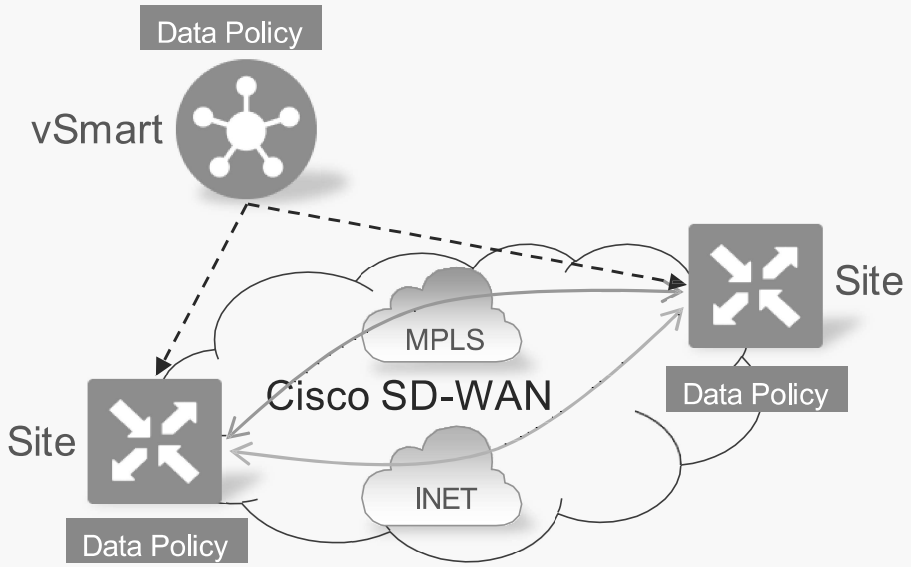
Data Policies

Data Policies

- Data policies are configured on vManage, enabled on vSmart controllers and enforced on WAN Edge routers
- Data policies allow easier fine-grain traffic controls when compared to control policies
- Certain objectives can be equally achieved by both control and data policies. Control policies act on OMP routing advertisements, data policies act on application traffic characteristics.
- Data policies are used to enable many services, such as:
  - Service Chaining
  - Cflowd
  - NAT
  - Traffic Policing and Counting
  - Transport Selection, TE

Data Policy Example – Path Preference

- Problem: Send critical applications over MPLS transport and non-critical applications over Internet transport
- Solution: Deploy data policy to set transport for relevant traffic



Policy Details:

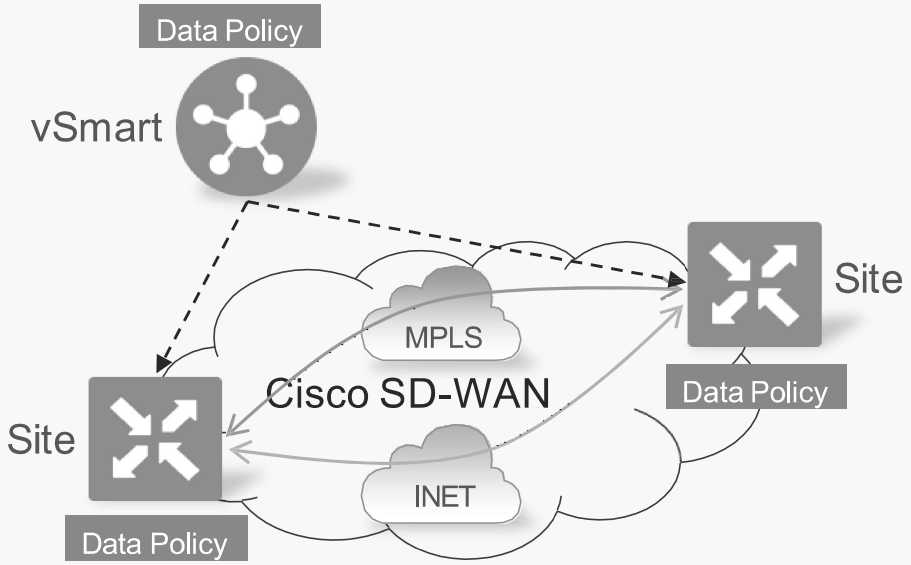
Bi-directionally set local TLOC for desired traffic

Override OMP routing decision

Fallback on overlay routing if transport fails

Data Policy Example – Path Preference

```
apply-policy
 site-list Site1-2
  data-policy prefer_mpls from-service
```

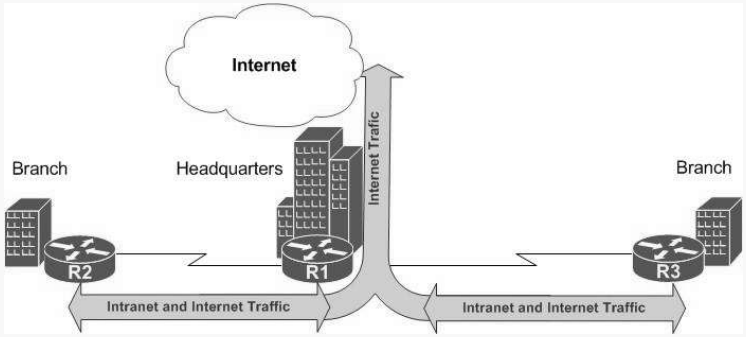


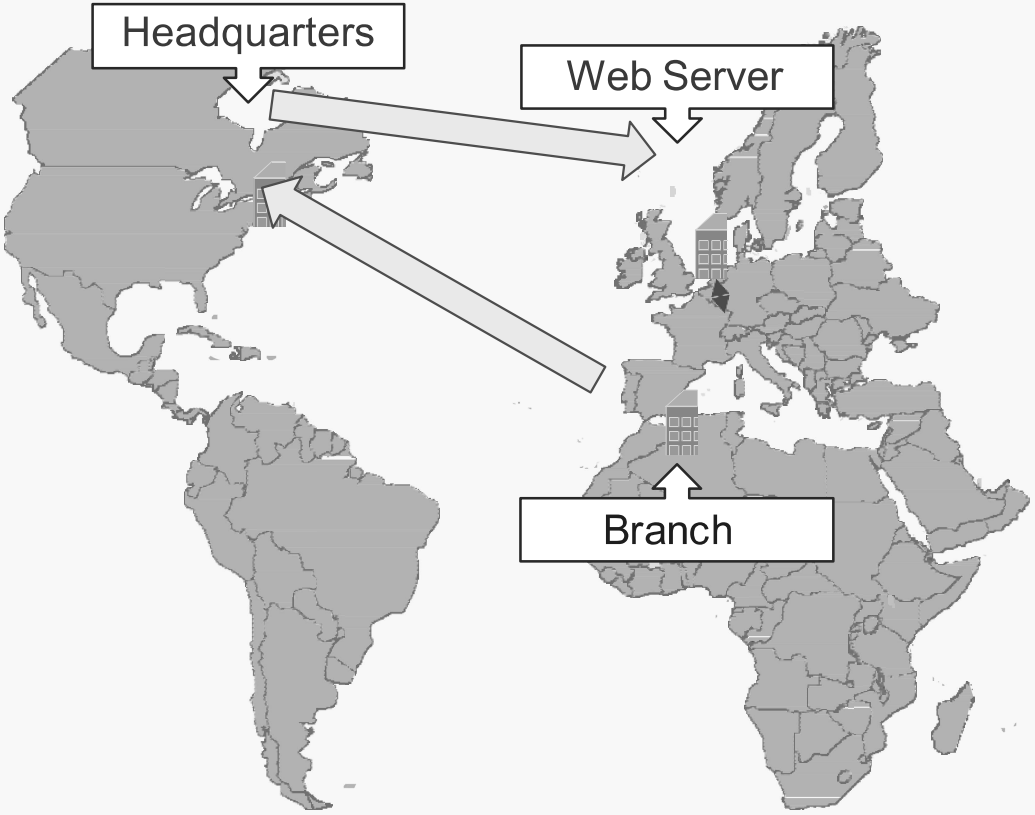

```
lists
  data-prefix-list DC-Servers
   ip-prefix 10.1.1.0/24
!
  site-list Site1-2
   site-id 1-2
  !
  vpn-list vpn10
   vpn 10
```

```
data-policy prefer_mpls
 vpn-list vpn10
 sequence 5
   match
    destination-data-prefix-list DC-Servers
   !
   action accept
    set
     local-tloc-list
      color mpls
    !
default-action accept
```

Direct Internet Access

Internet Access Models





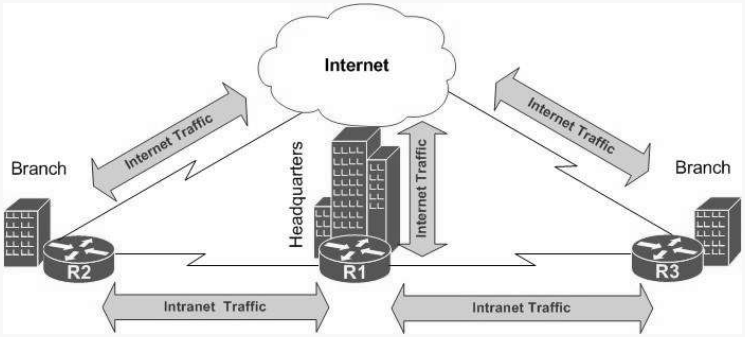
Centralized Access Model

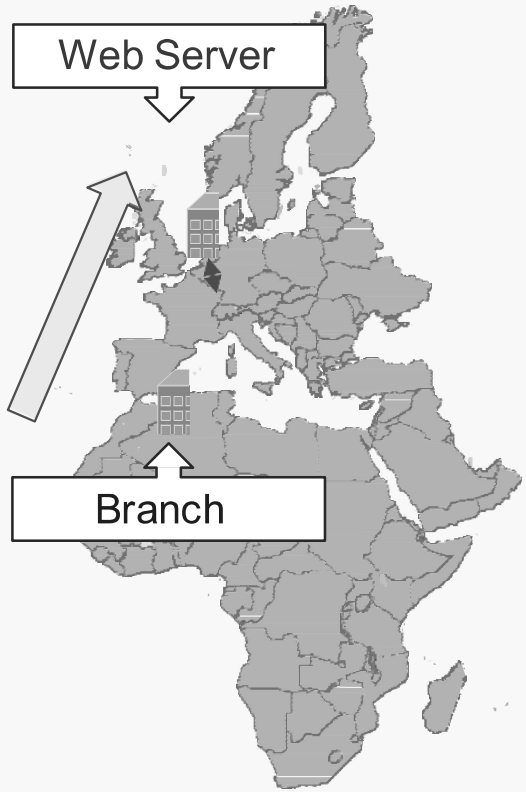
Centralized deployment of security policy.

Internet traffic travels across the WAN circuit.

Potential for additional latency.

Internet Access Models





Distributed Access Model

Distributed deployment of security policy via:

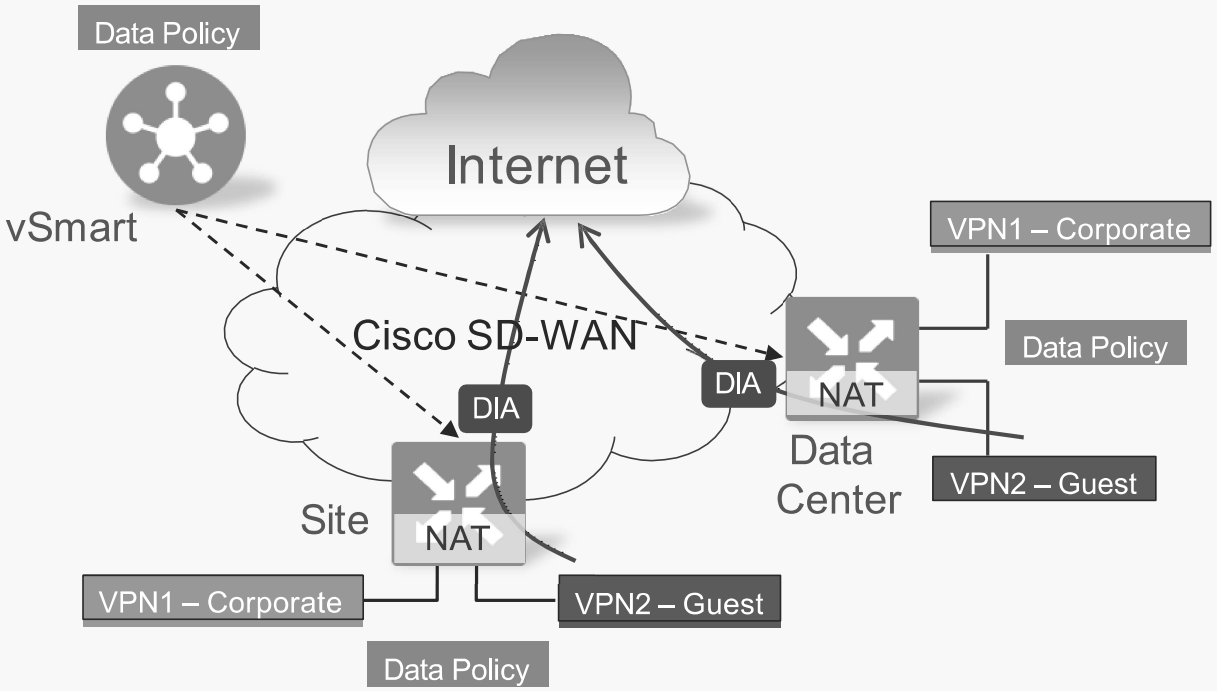
- Distributed devices
- Cloud based security models

Internet traffic leaves the branch site direct to the web site.

Latency is reduced

Data Policy Example – DIA with NAT

- Problem: Local Internet exit needs to be provided to guest WiFi users. Guest WiFi users need to be isolated from corporate users.
- Solution: Deploy a data policy in guest VPN with a network address translation

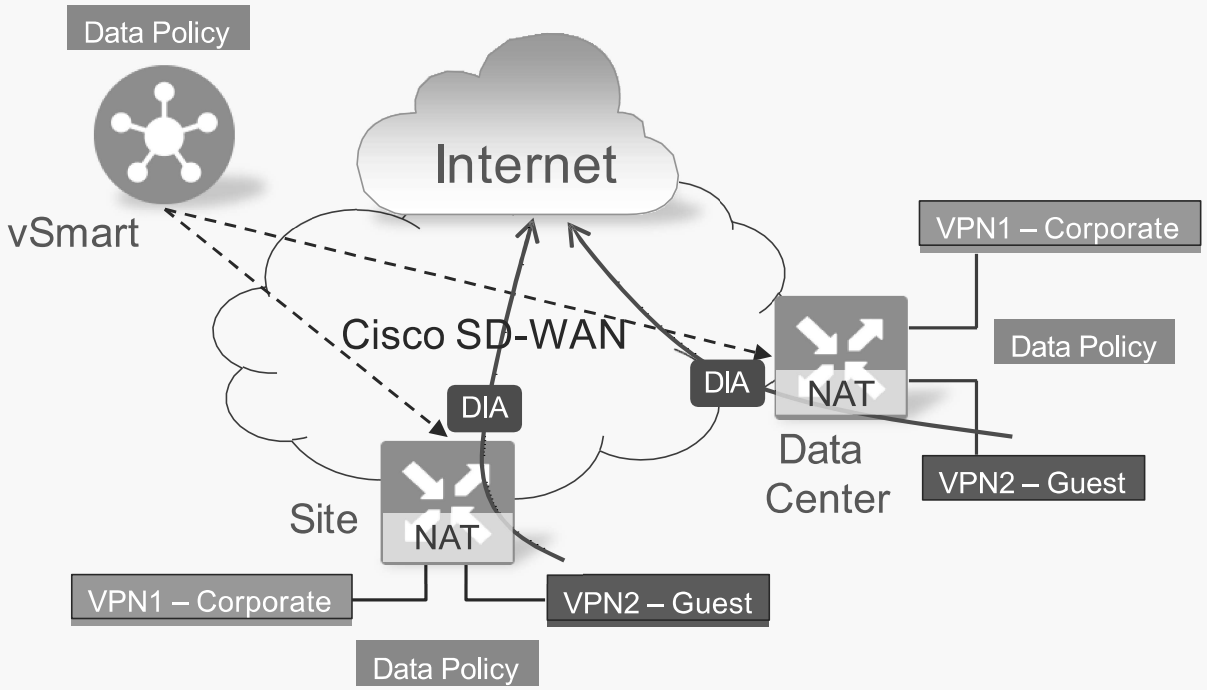


Policy Details:

Define NAT on transport side interface

Force matching traffic in guest WiFi VPN through a locally defined NAT on transport side interface

Data Policy Example – DIA with NAT




```
apply-policy
 site-list Site1-2
  data-policy guest-wifi from-service
```

```
site-list Site1-2
   site-id 1-2
  !
  vpn-list guest-vpn
   vpn 100
```

```
policy data-policy guest-wifi
 vpn-list guest-vpn
 sequence 10
    action accept
       nat use-vpn 0
     !
   !
  default-action drop
!
```

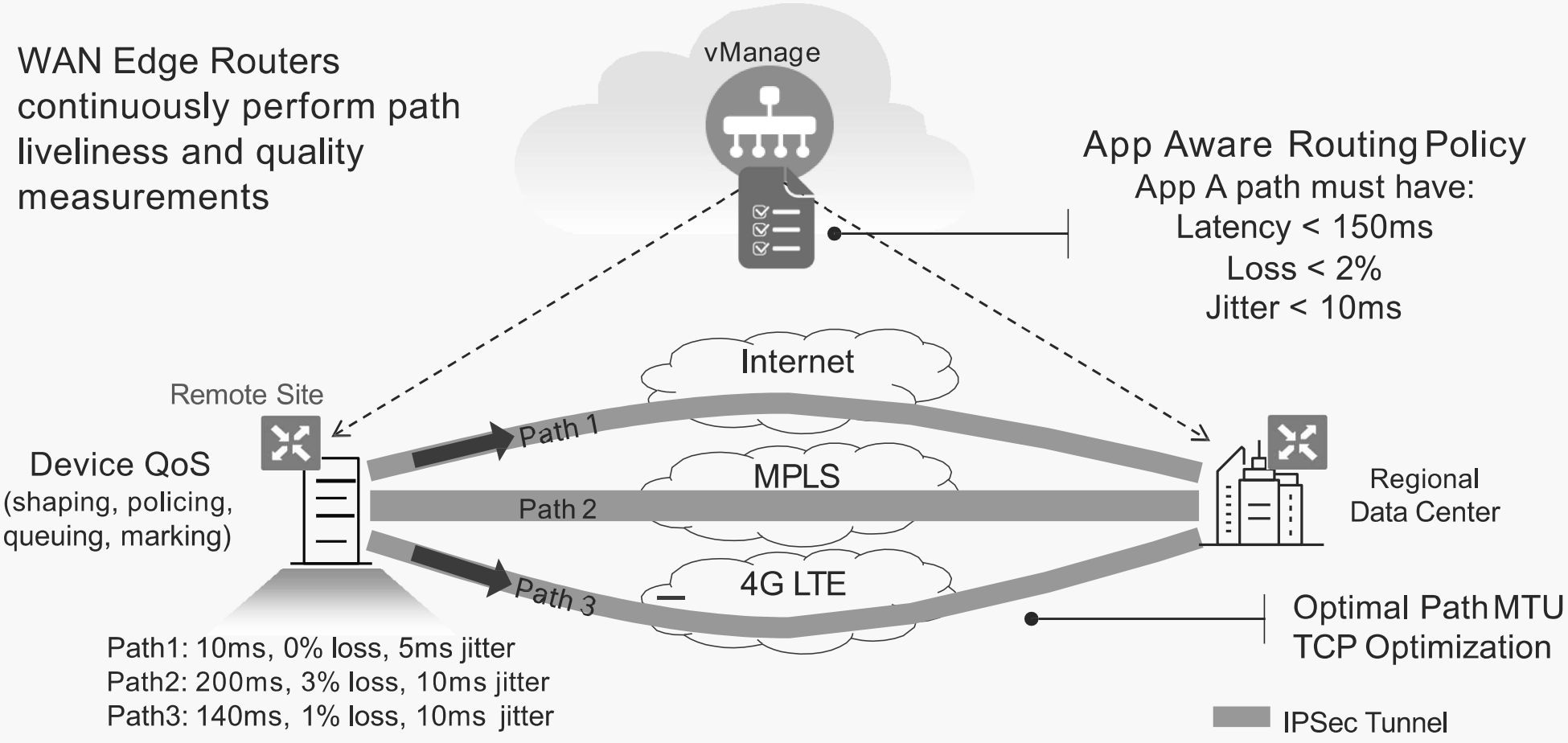
Application Aware Routing

Application Aware Routing Policies

- Application Aware Routing policies are configured on vManage, enabled on vSmart controllers and enforced on WAN Edge routers
- Application Aware Routing policies ensure SLA compliant path through the SD-WAN fabric
- The SLA class defines loss, latency and jitter thresholds
- Application Aware Routing policy matches on the application traffic of interest. Match can be based on 6-tuple matching or DPI signature.
- Application Aware Routing policy is enforced in VPNs and sites of interest

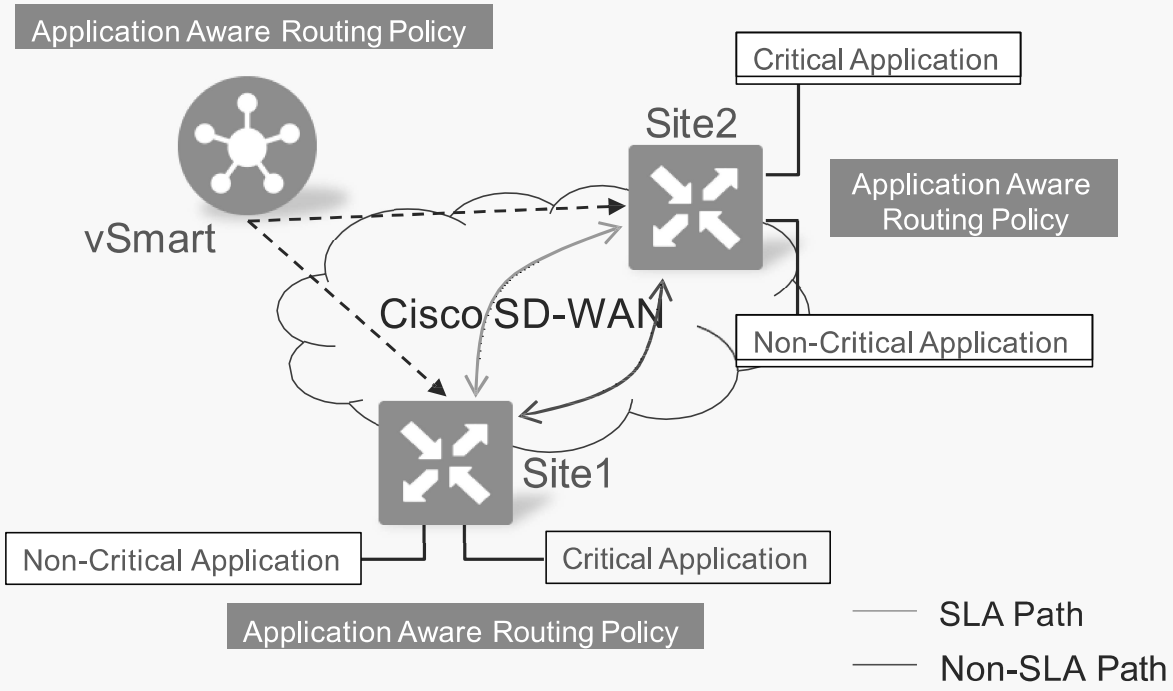
Critical Applications SLA

- WAN Edge Routers continuously perform path liveliness and quality measurements



Application Aware Routing Policy Example

- Problem: Critical applications traffic needs to take SLA compliant path through the network to achieve better user quality of experience
- Solution: Deploy Application Aware Routing policy for critical application traffic



Policy Details:

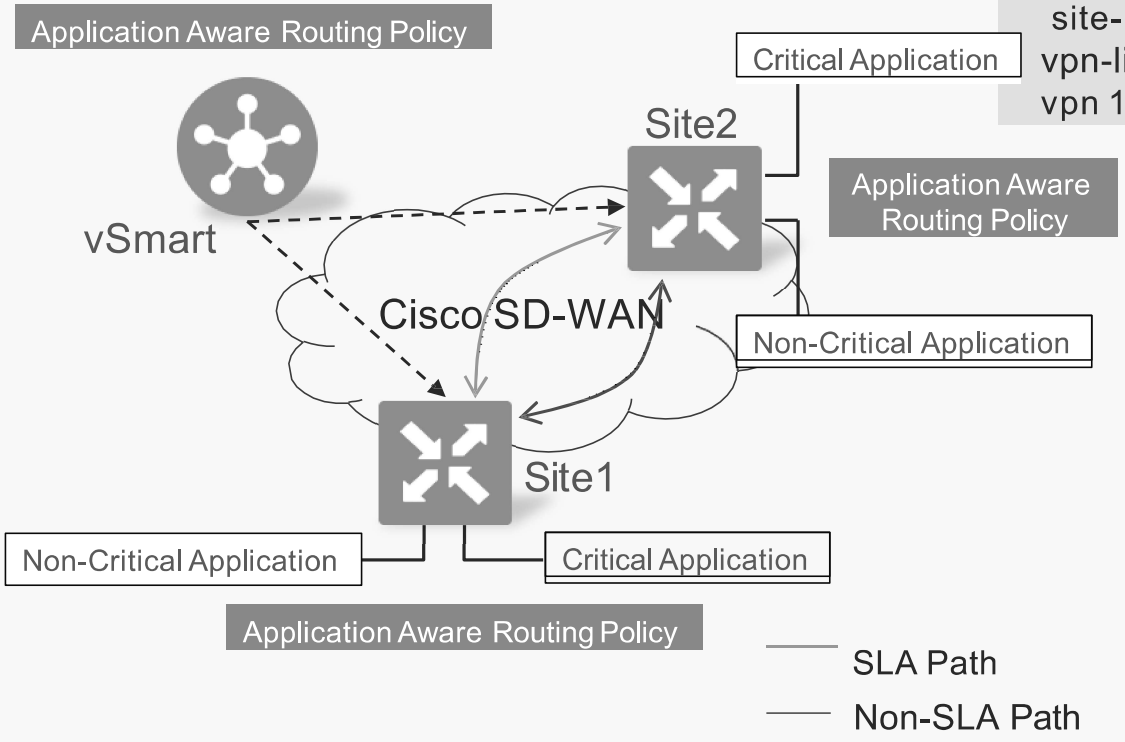
Define SLA class for acceptable SLA thresholds for loss, latency and jitter

Apply SLA class to the application aware routing policy matching on the application traffic of interest

Bi-directionally apply application aware routing policy in the VPNs of choice

Application Aware Routing Policy Example

```
apply-policy
 site-list spokes
  app-route-policy  voice-priority
```

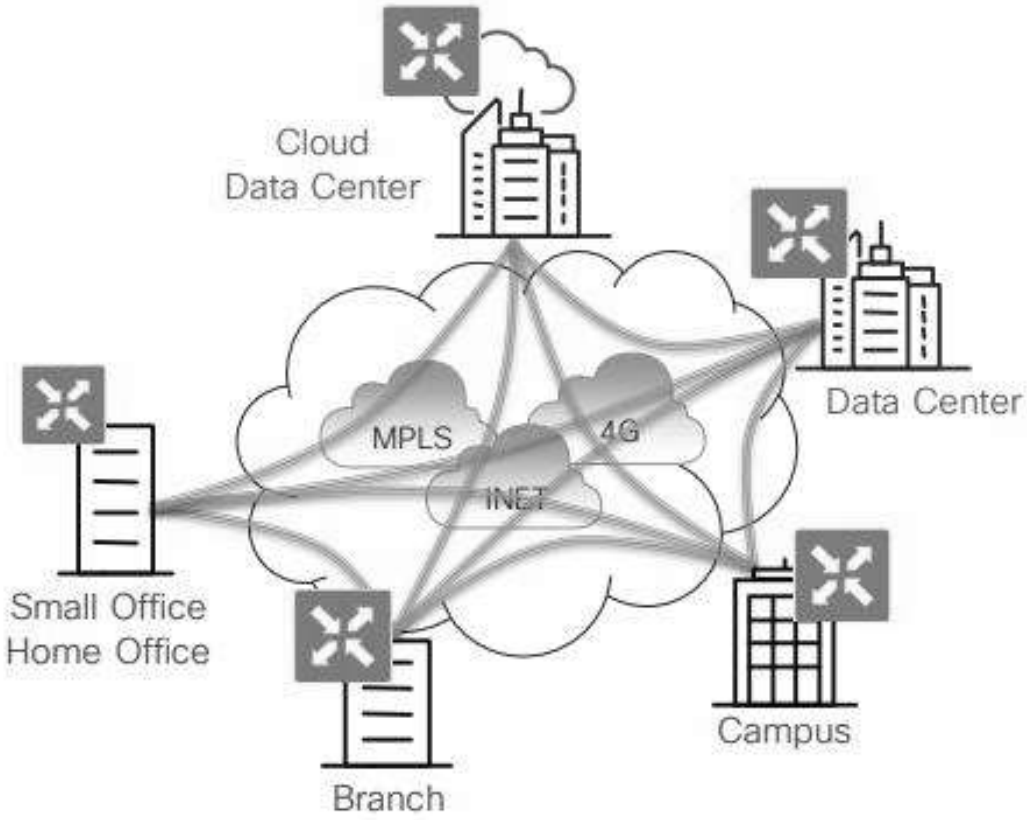



```
lists
  app-list voice
   app-family audio_video
  site-list spokes
   site-id 1-2
  vpn-list vpn10
  vpn 10
```

```
policy
  sla-class sla-voice
   latency 150
   loss 1
  !
 app-route-policy  voice-priority
  vpn-list vpn10
    sequence 1
    match
      app-list voice
     !
     action
      sla-class sla-voice preferred-color mpls
      backup-sla-preferred-color  biz-internet
```

QoS

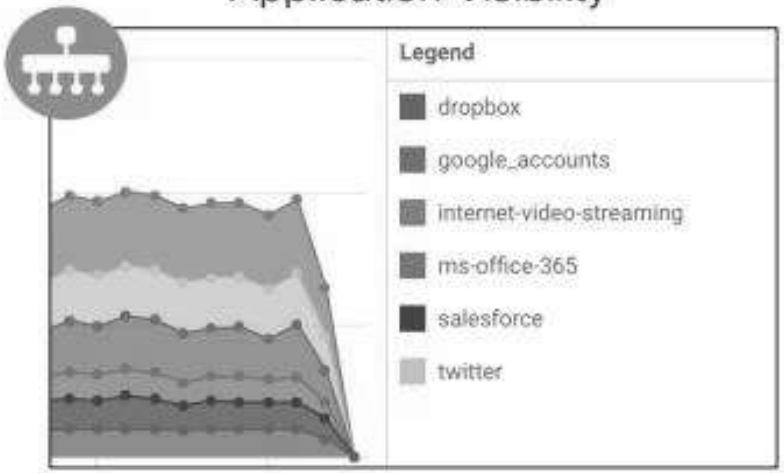
Application Visibility and Recognition



NBAR2: XE-SDWAN, DPI: vEdge

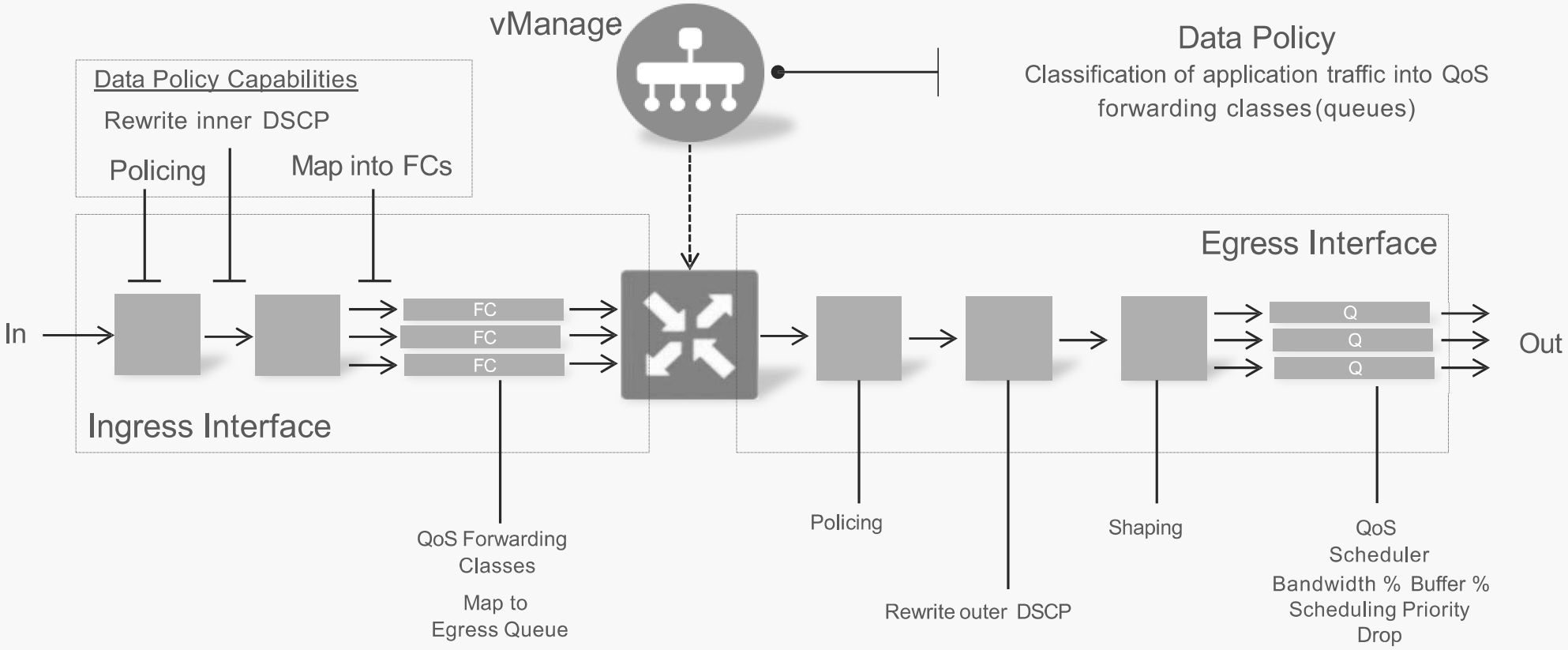
Application Recognition

Application Visibility



WAN Edge Router Device QoS Overview

WAN Edge Router

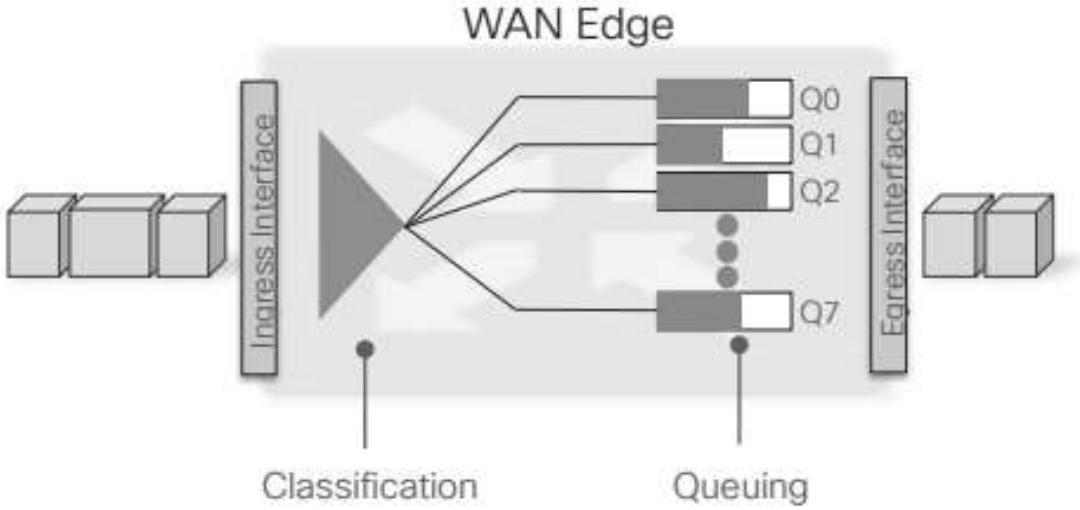


Device QoS: Queuing

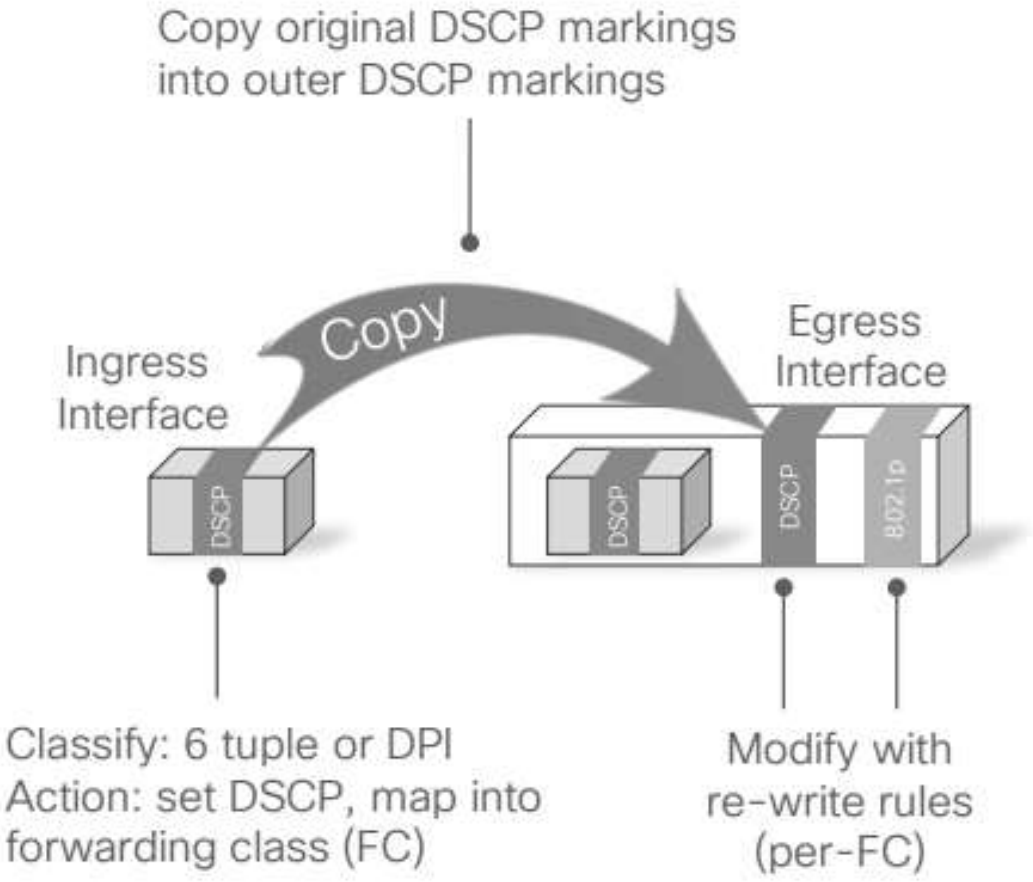
- Per-Egress Interface Queuing
  - 8 queues
- Classification
  - 6-tuple or DPI
  - Local or central data policy
- Q0: Control traffic
  - DTLS/TLS, BFD, routing protocols
  - Not subjected to LLQ policer
- Q0: LLQ
  - Unused bandwidth is distributed between Q1-Q7

* Random Early Discard

- Q1-Q7: Weighted Round Robin
  - Bandwidth percent determines queue weight
- Q1-Q7: Queue drop is RED* or tail-drop
  - Linear drop probability, i.e. X% queue depth results in X% drop probability

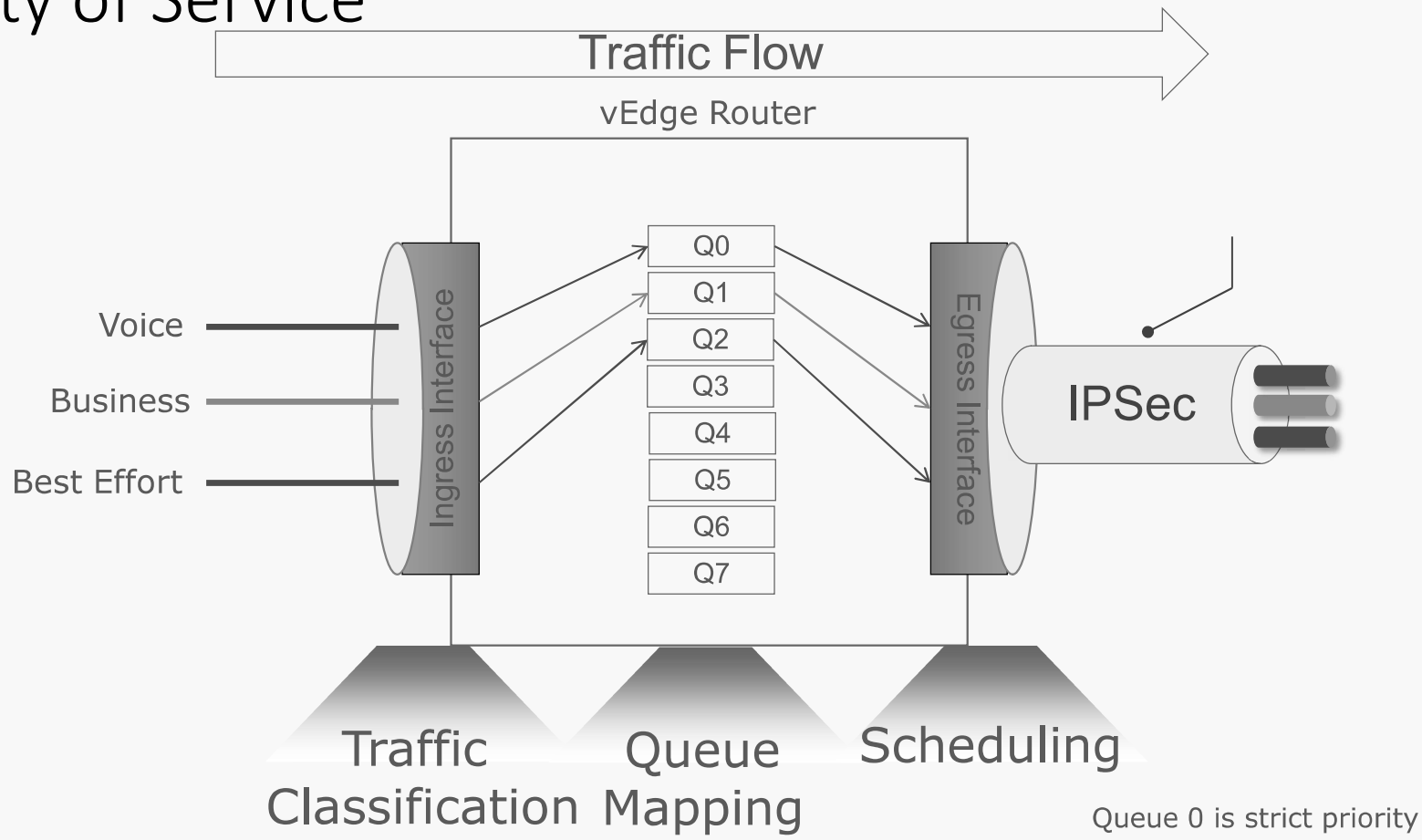


DSCP and COS (802.1p) Re-marking

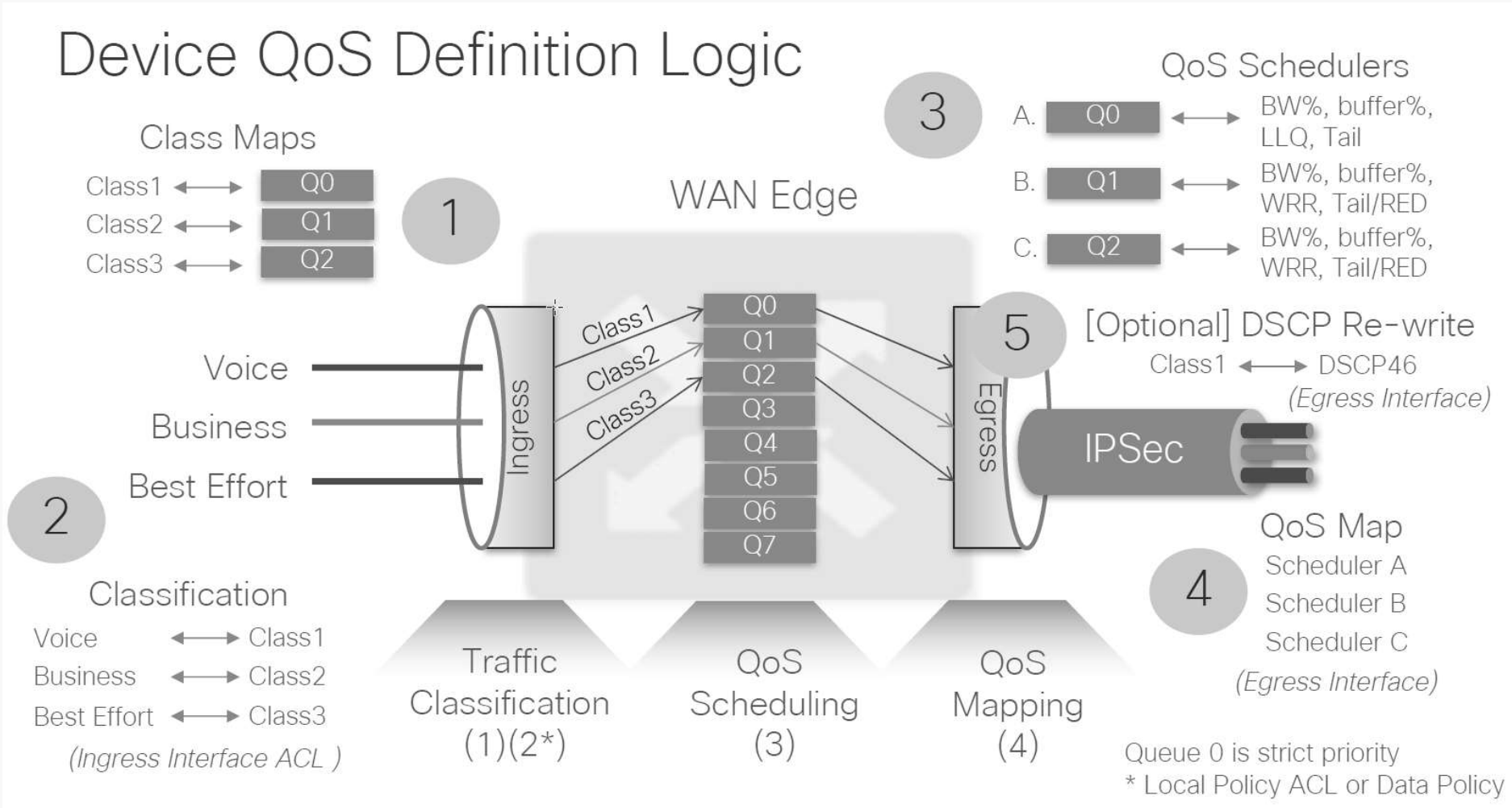


- Comply with service provider provisioned classes of service
- (Optional) Original DSCP rewrite
  - Classification: 6 tuple or DPI
  - Action: Local or central data policy
- (Default) Original DSCP marking is copied to the outer DSCP marking
- (Optional) Egress outer DSCP rewrite
  - Re-write rules based on forwarding class mapping on ingress
- (Optional) Egress COS rewrite
  - Re-write rules based on forwarding class mapping on ingress

Differentiated Services
Quality of Service



Device QoS Definition Logic



Localized Data Policy (QoS) Configuration

Step1: Configure forwarding classes and mapping to output queues

```
policy
 class-map
  class best-effort queue 3
  class bulk-data queue 2
  class critical-data queue 1
  class voice queue 0
```

Step 3: Define QoS Map by grouping QoS Schedulers.

```
policy
 qos-map MyQoSMap
  qos-scheduler be-scheduler
  qos-scheduler bulk-scheduler
  qos-scheduler critical-scheduler
  qos-scheduler voice-scheduler
```

Step 4: Apply the QoS map to the egress interface

```
interface ge0/1
  qos-map  MyQoSMap
```

Step2: Configure the QoS scheduler forwarding classes

```
policy
 qos-scheduler be-scheduler
  class              best-effort
  bandwidth-percent  20
  buffer-percent     20
  scheduling         wrr
  drops              red-drop
 !
 qos-scheduler bulk-scheduler
  class              bulk-data
  bandwidth-percent  20
  buffer-percent     20
  scheduling         wrr
  drops              red-drop
 !
 qos-scheduler critical-scheduler
 class              critical-data
  bandwidth-percent  40
  buffer-percent     40
  scheduling         wrr
  drops              red-drop
 !
 qos-scheduler voice-scheduler
  class              voice
  bandwidth-percent  20
  buffer-percent     20
  scheduling         llq
  drops              tail-drop
```

Localized Data Policy (QoS) Configuration

Step 5: Define an Access List to Classify Data Packets into appropriate Forwarding Classes

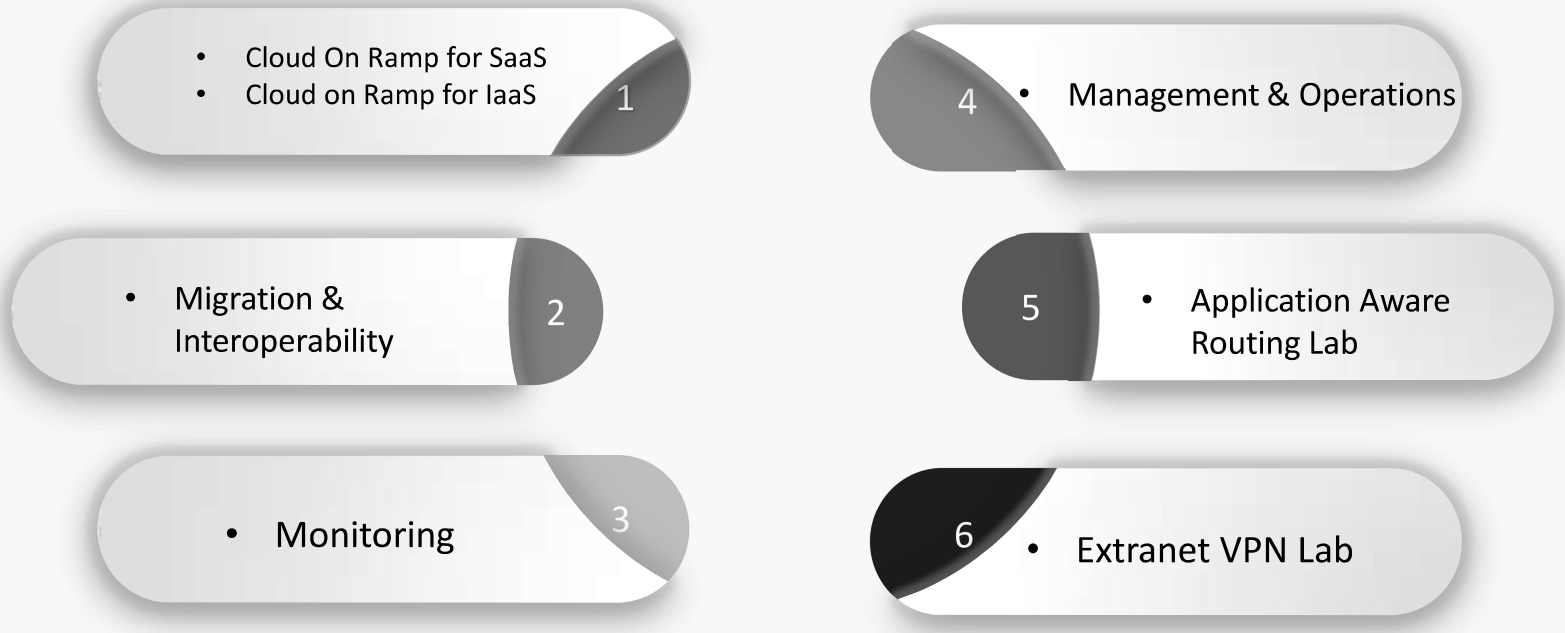
```
policy
 access-list MyACL
  sequence 10
   match
    dscp 46
   !
   action accept
    class voice
   !
  !
  sequence 20
   match
    source-ip      10.1.1.0/24
    destination-ip 192.168.10.0/24
   !
   action accept
    class bulk-data
    set
     dscp 32
    !
   !
  !
  sequence 30
   match
    destination-ip 192.168.20.0/24
   !
   action accept
    class critical-data
    set
     dscp 22
    !
   !
  !
  sequence 40
   action accept
    class best-effort
    set
     dscp 0
    !
   !
  !
  default-action drop
```

Step 6: Apply the Access List to an Interface

```
vpn 10
 interface ge0/0
  access-list MyACL in
 !
```

Break

Cisco SD-WAN Training – Day5



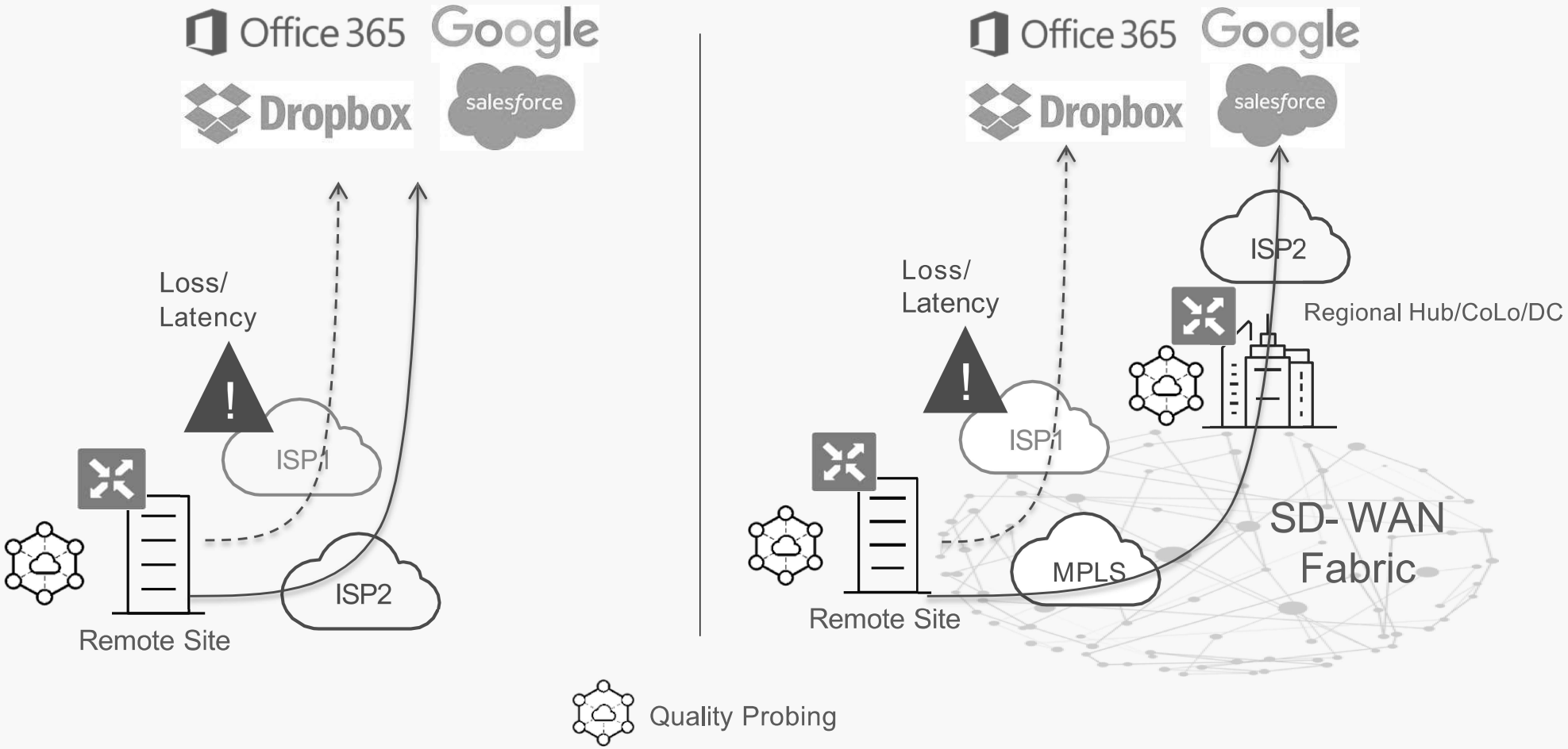
Cloud On Ramp

Traditional SaaS Applications Access

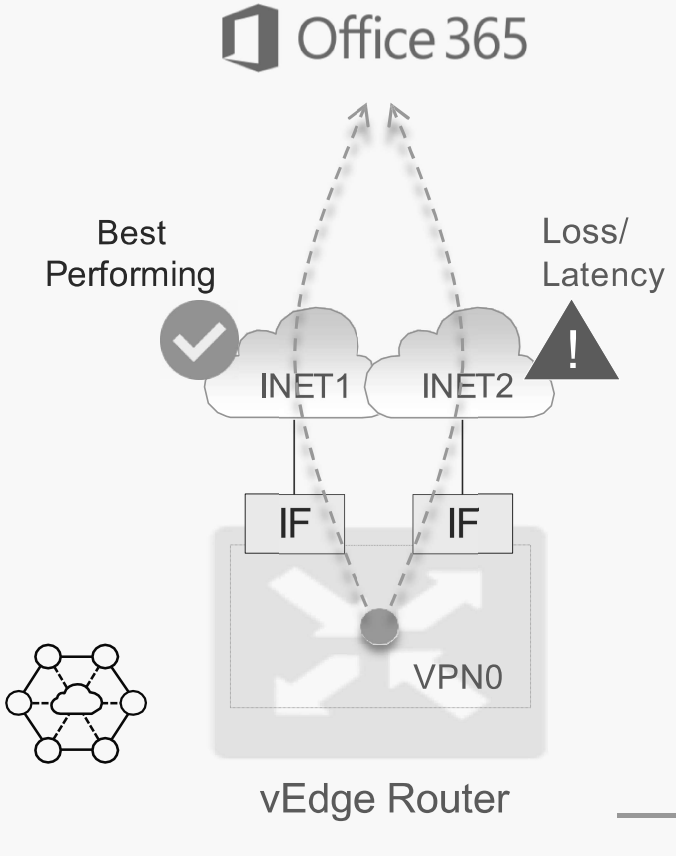
Which way is cloud?

- Direct Internet Access
- Regional Breakout
- Data Center Backhaul

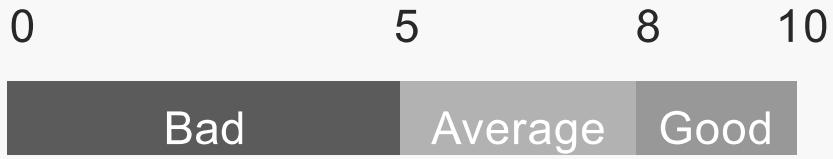
Cloud onRamp for SaaS



Cloud onRamp Application Performance



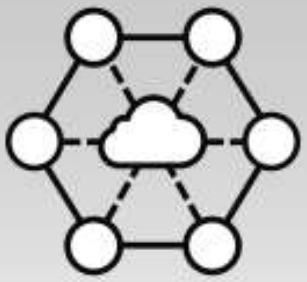
- vEdge router determines average loss and latency toward cloud applications based on HTTP probes measurements
  - vQoE [Loss] = Desired Loss / Average Loss * 100
  - vQoE [Lat] = Desired Lat / Average Lat * 100
- vEdge router determines best performing DIA path based on vQoE score
  - vQoE = Average (vQoE[Loss] + vQoE[Latency])



Cloud onRamp for SaaS Operation

Discover Cloud Application

1



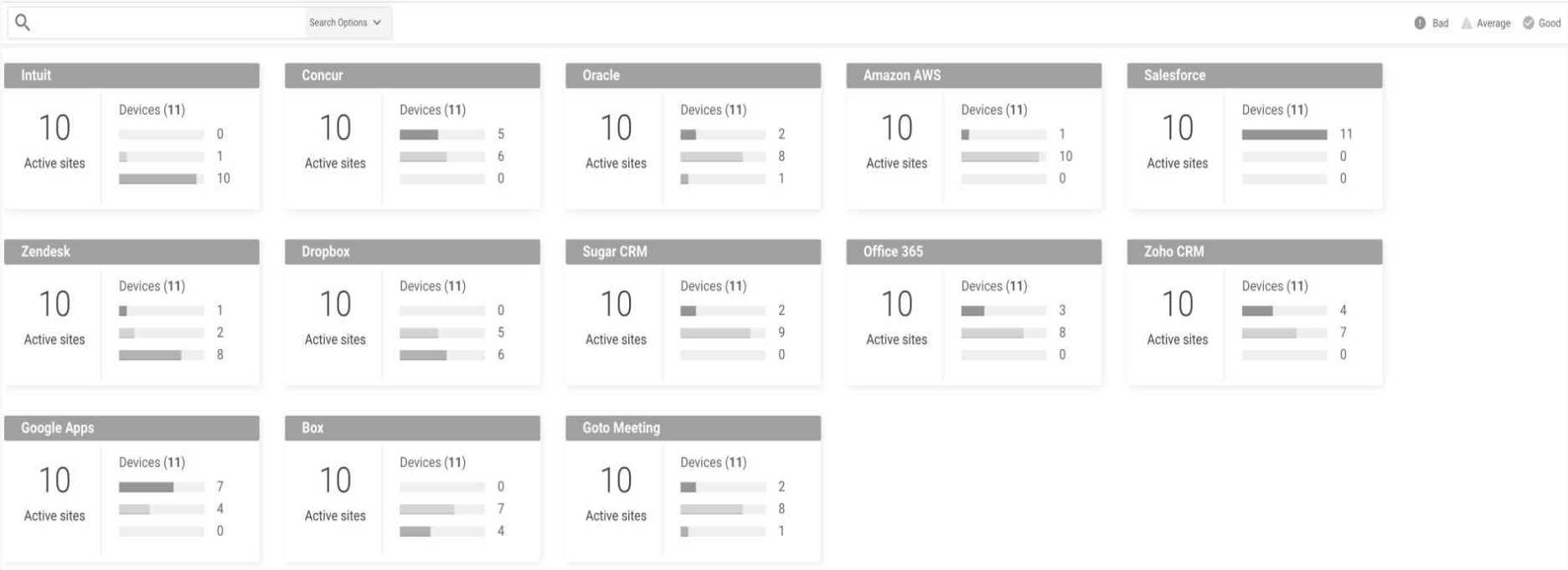
Determine Cloud Application Performance

2

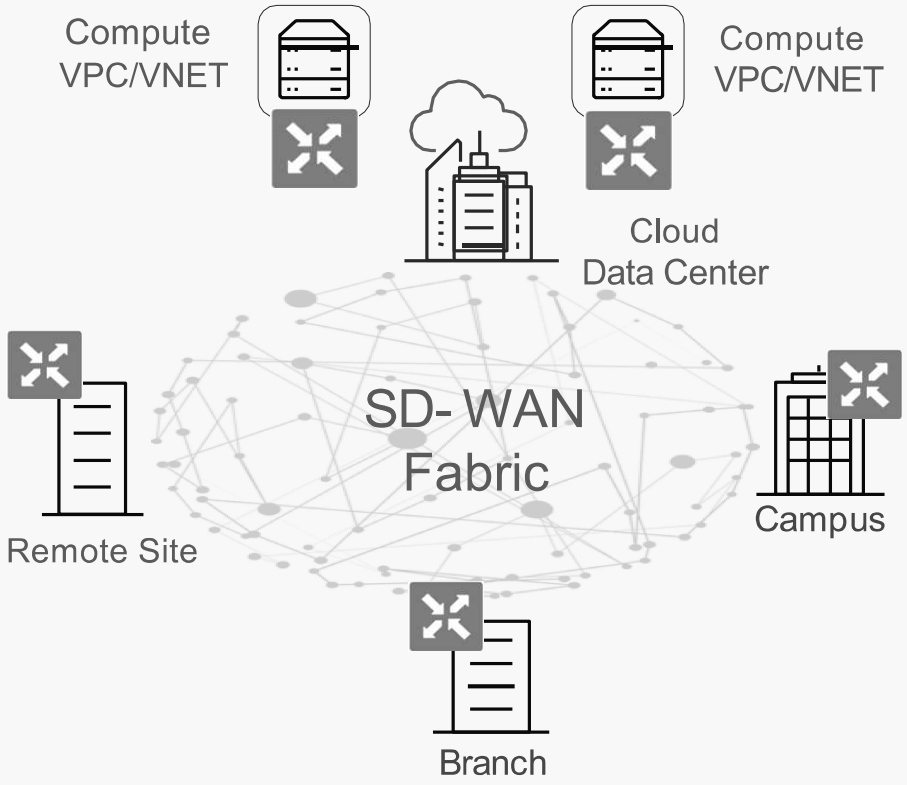
Route Cloud Application Traffic

3

SaaS Performance

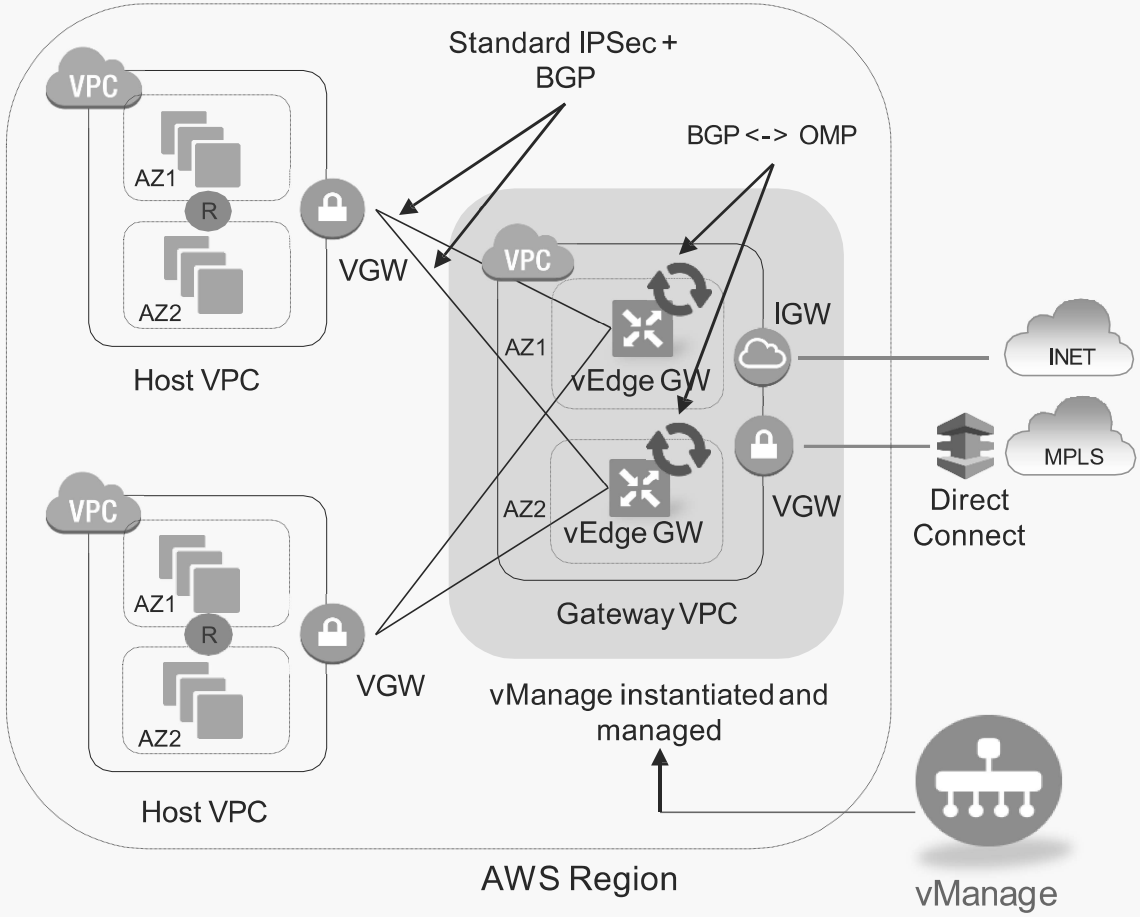


Cloud onRamp for IaaS – Attached Compute



- vEdge Cloud routers are instantiated in Amazon VPCs or Microsoft Azure VNETs
  - Posted in marketplace
  - Use Cloud-Init for ZTP
- vEdge Cloud routers join the fabric, all fabric services are extended to the IaaS instances, e.g. multipathing, segmentation and QoS
  - For multipathing, can combine AWS Direct Connect or Azure ExpressRoute with direct Internet connectivity

Cloud onRamp for IaaS – Gateway VPC/VNET

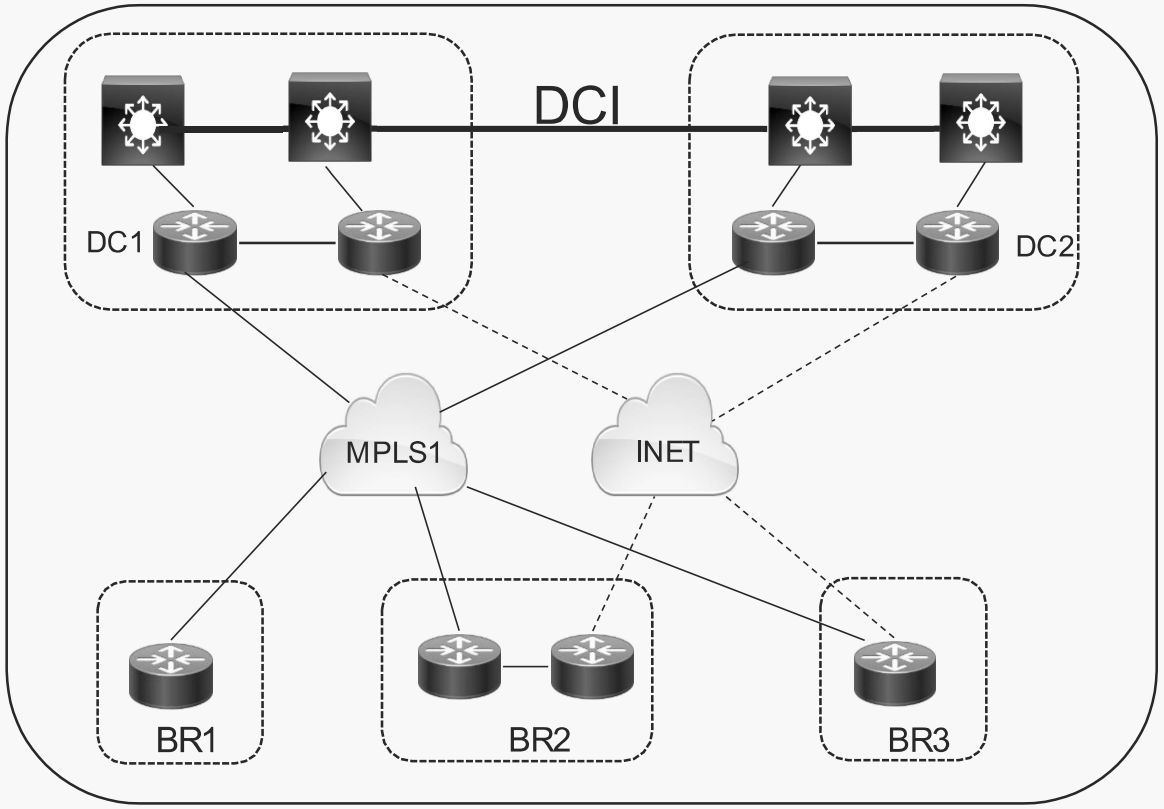


- Full automated through vManage wizard
- Greatly simplifies brownfield integration
  - No changes are required on host/compute VPCs
- Multipathing through SD-WAN fabric
- Security segmentation
  - To Gateway VPC
- Fast failover
- Speed of routing convergence

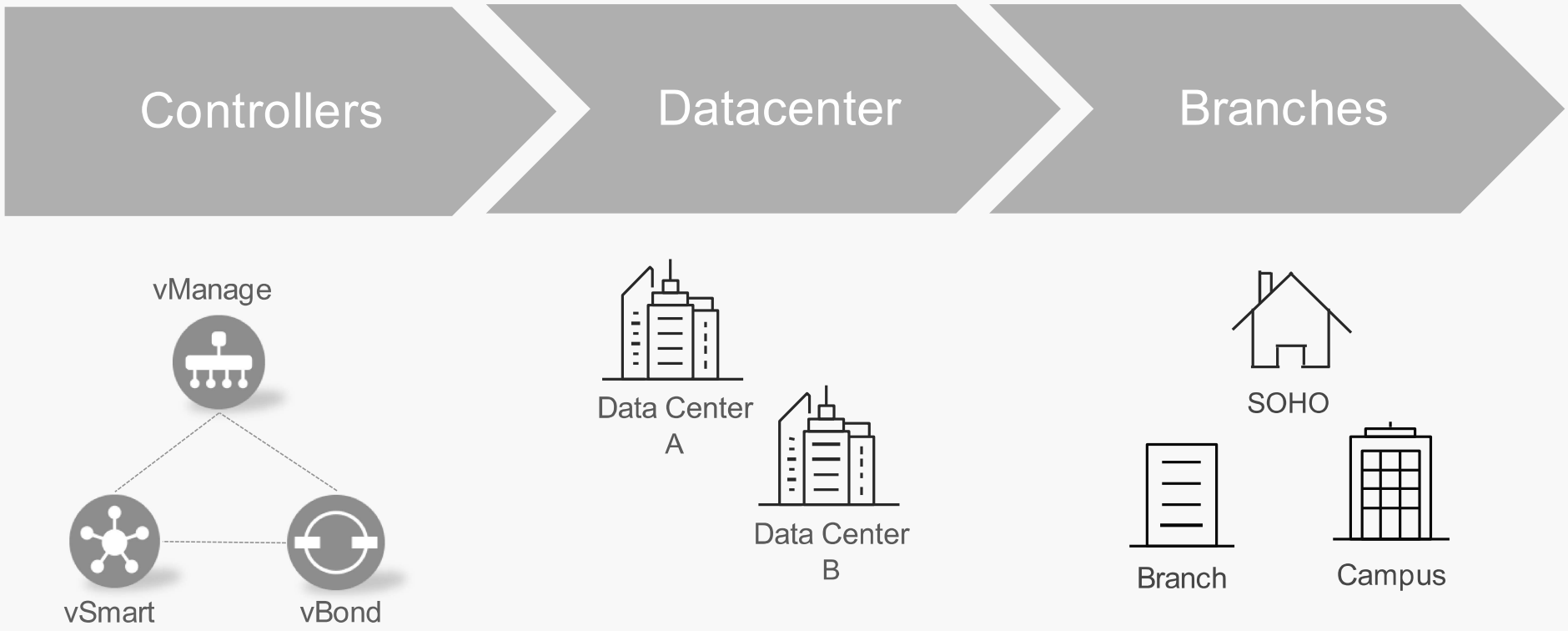
Migration & Interoperability Basics

Legacy WAN Architecture

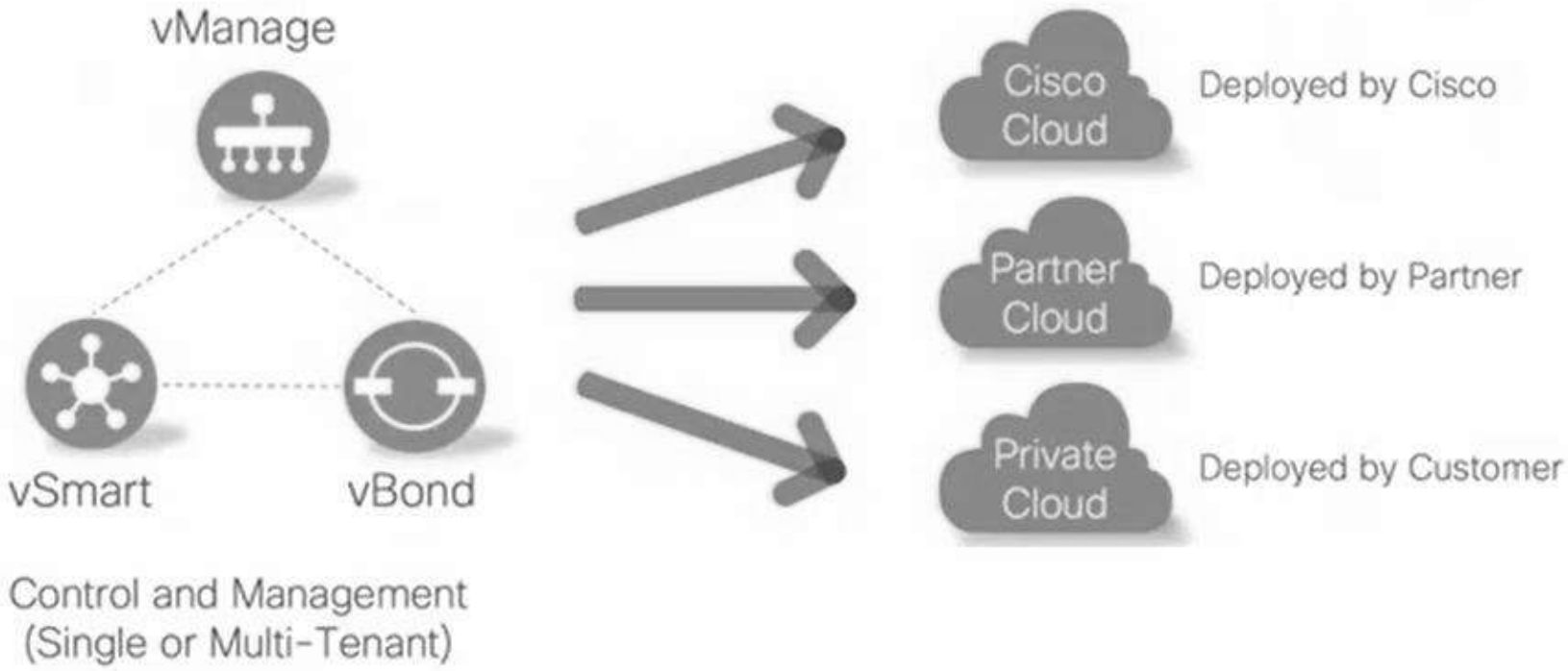
- Two or more circuits
- All MPLS, or, MPLS and INET/LTE
- Active/Standby Redundancy
- Internet/SaaS access backhauled via DC



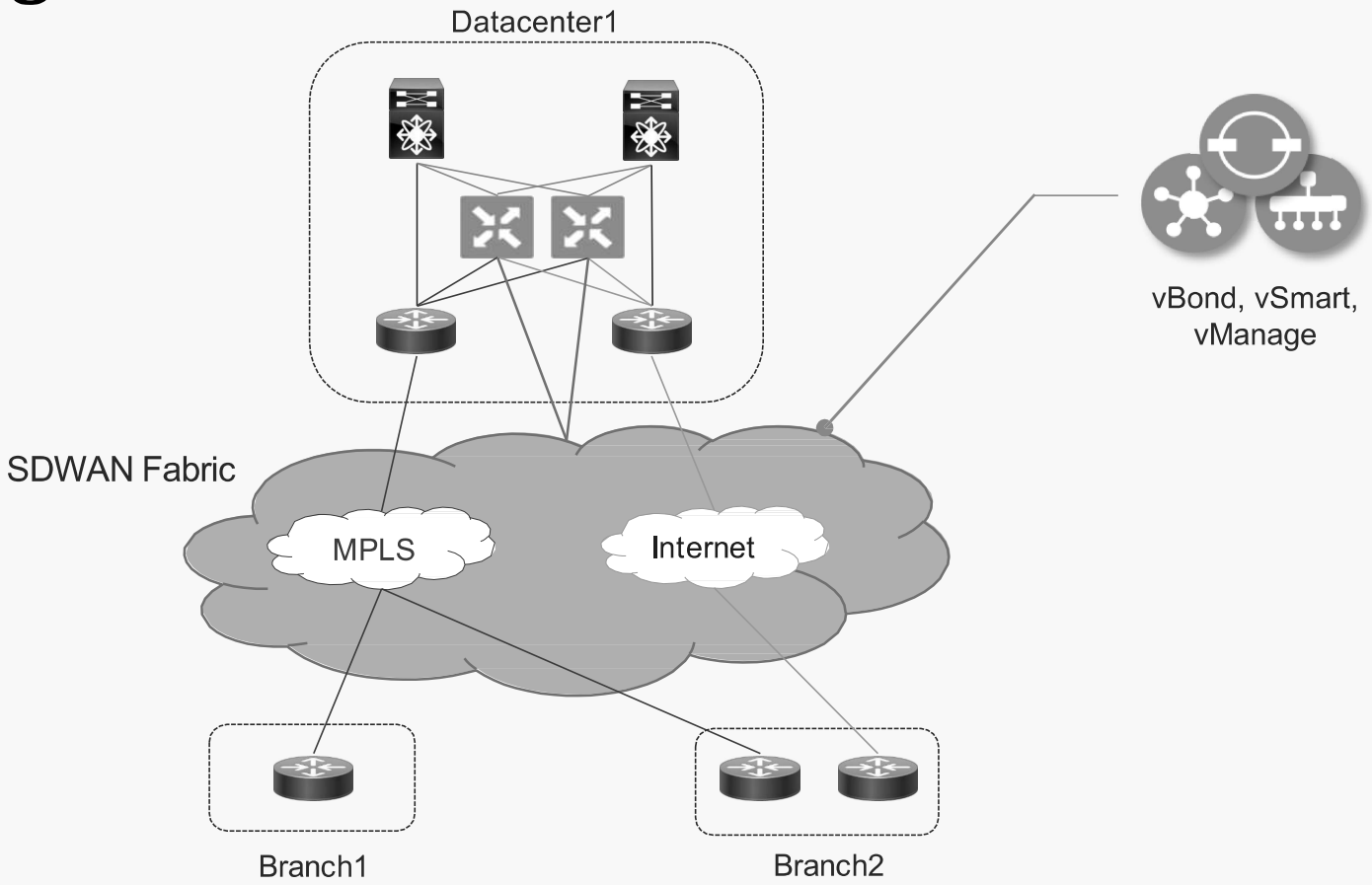
Migration Sequence



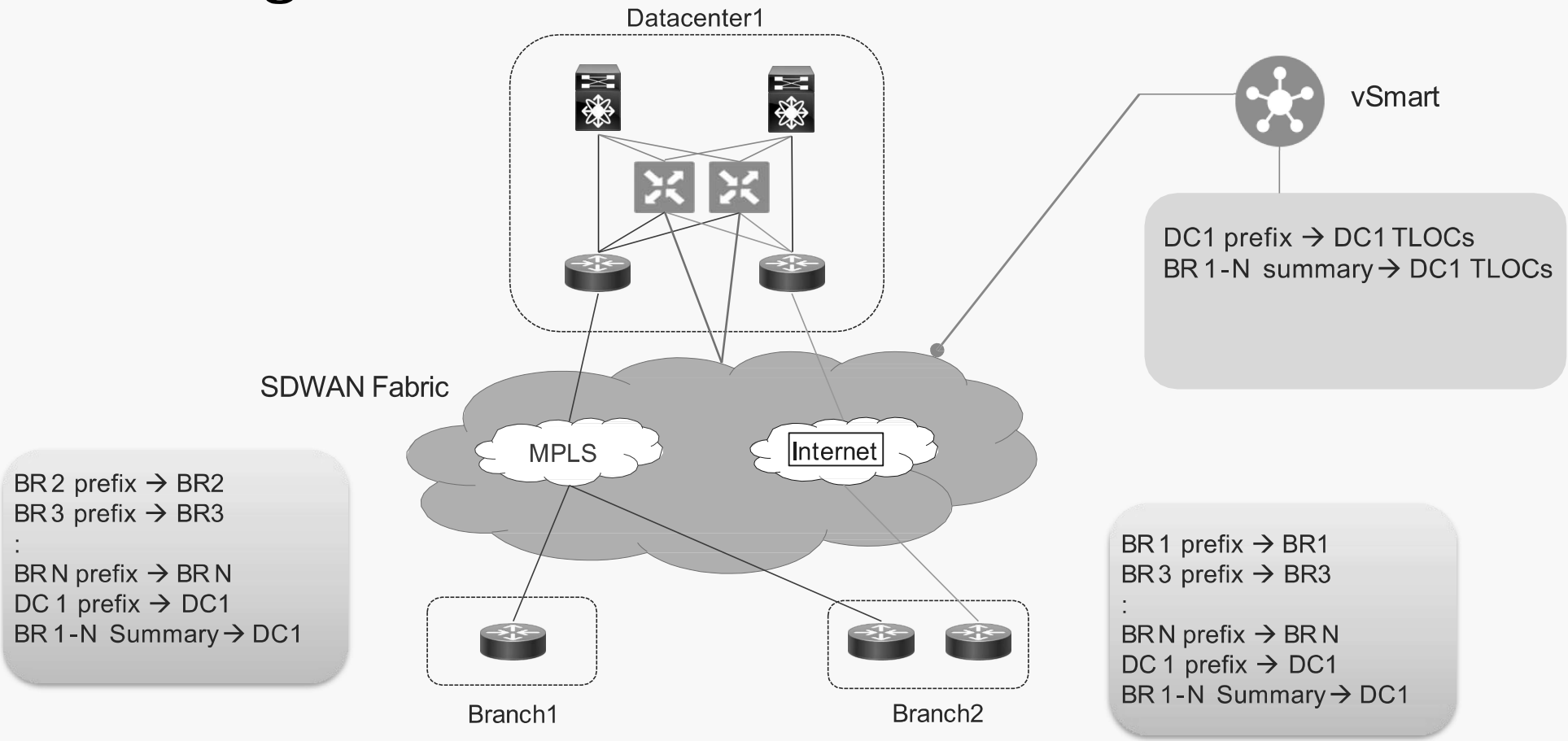
Controllers Deployment Models



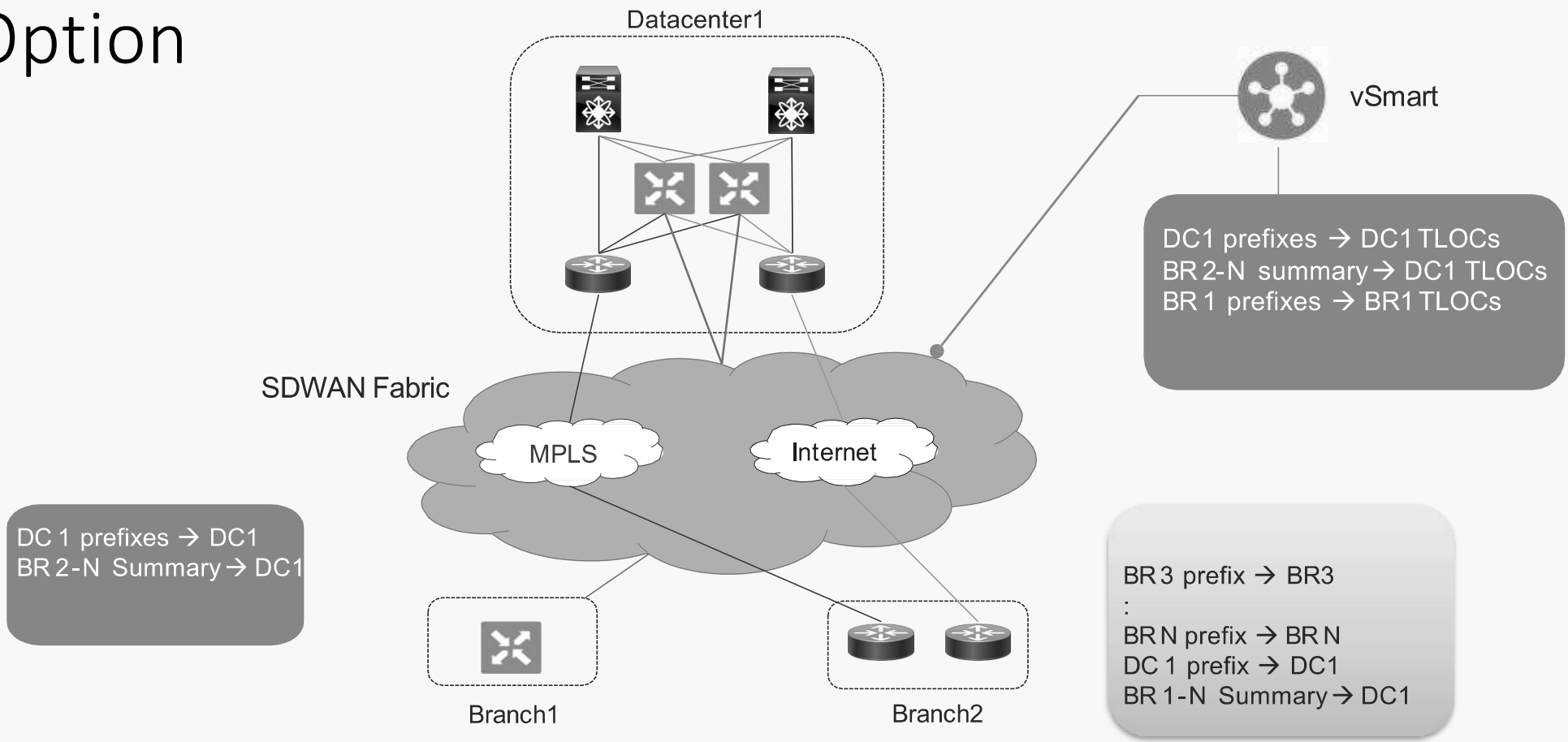
DC Migration - Overview



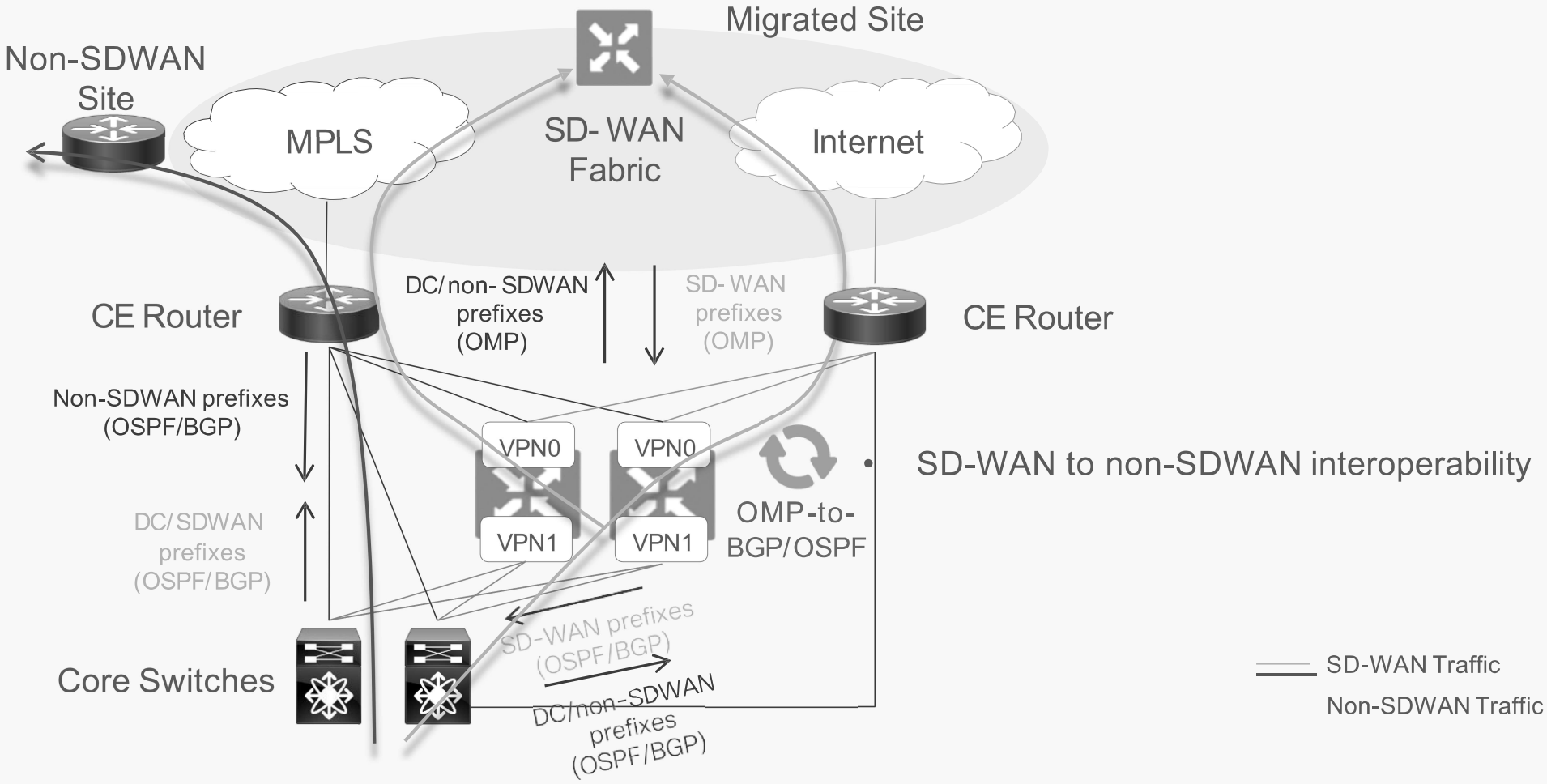
DC Migration - Overview



Branch Migration – Replace CE Option



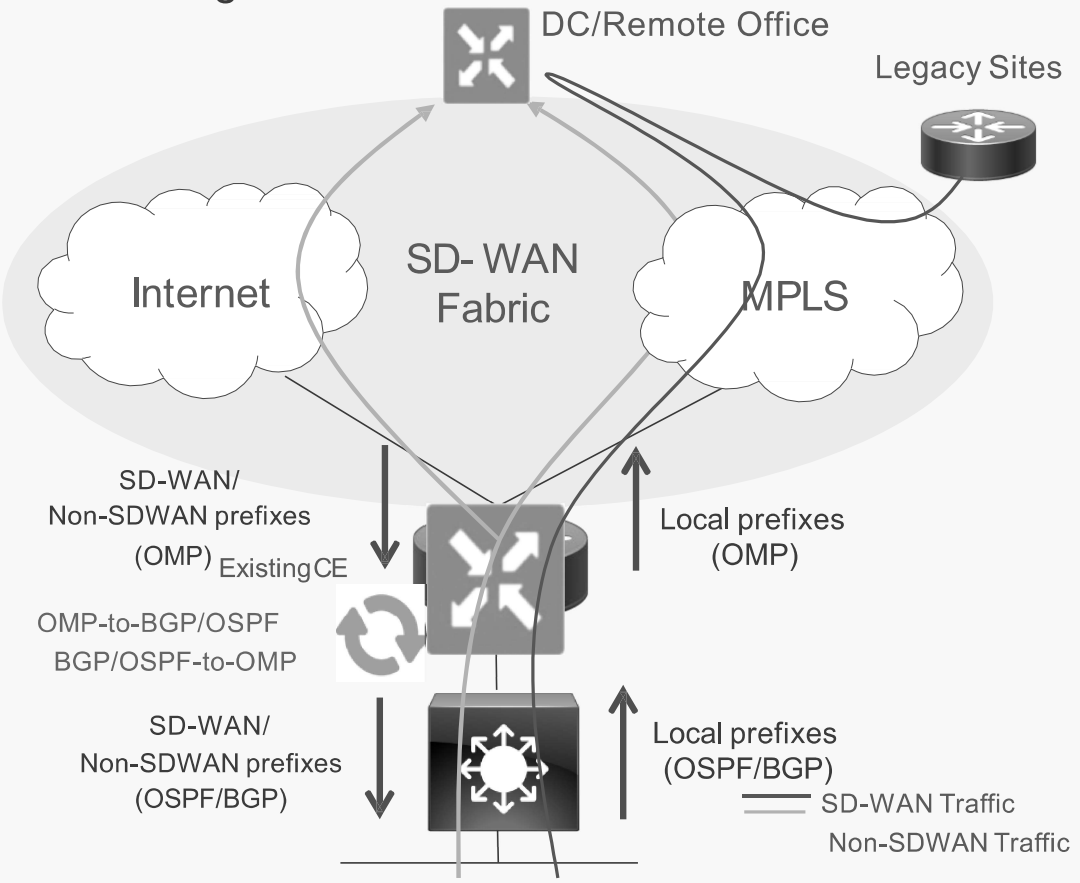
Routing at the Datacenter



Routing after Branch Migration – Replace CE

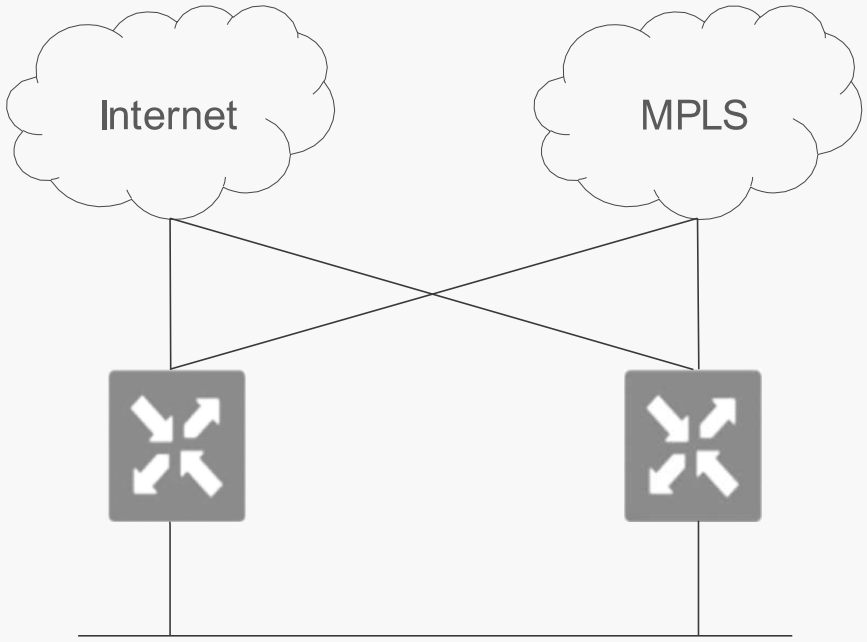
SD-WAN to Legacy site communication via DC/Regional Hub

- Replace CE or Upgrade to SDWAN-XE
  - Verify HW/module compatibility
  - Upgrade ROMMON if needed
- ZTP → Configuration Template
- Direct SD-WAN ←→ SD-WAN sites communication
- SD-WAN ←→ Legacy communication via DC/hub

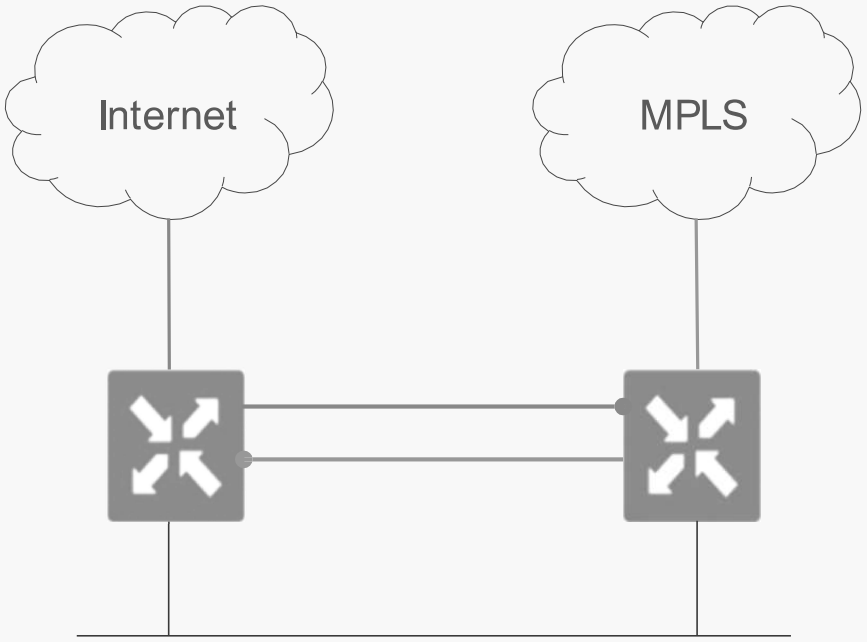


Branch Migration

Adding Redundancy

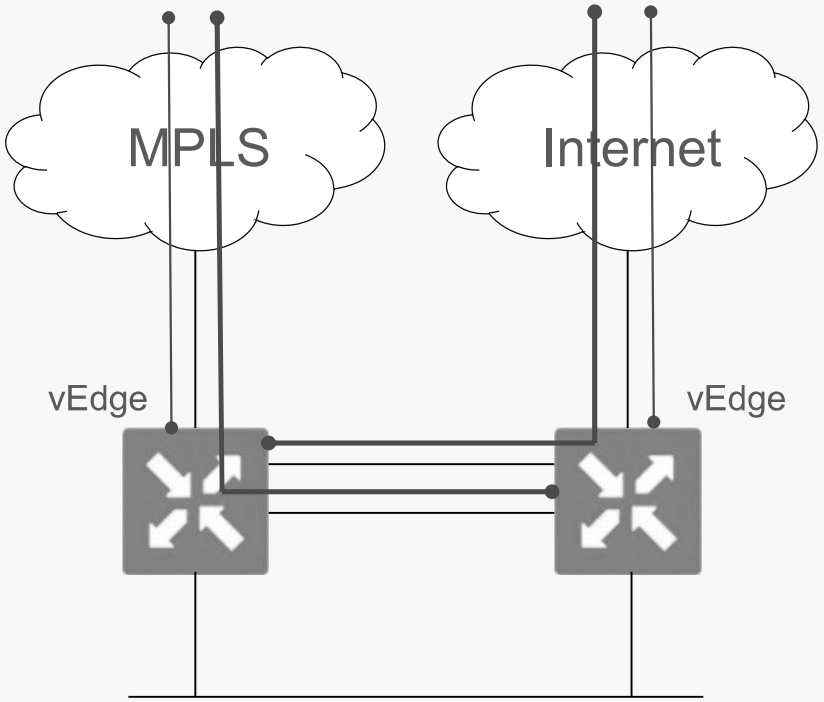


Device-level Redundancy



TLOC Extension

Transport Redundancy – TLOC Extension



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

Monitoring ,Management ,Operations

Agile Operations

Power Tools

CLI

Linux Shell

REST

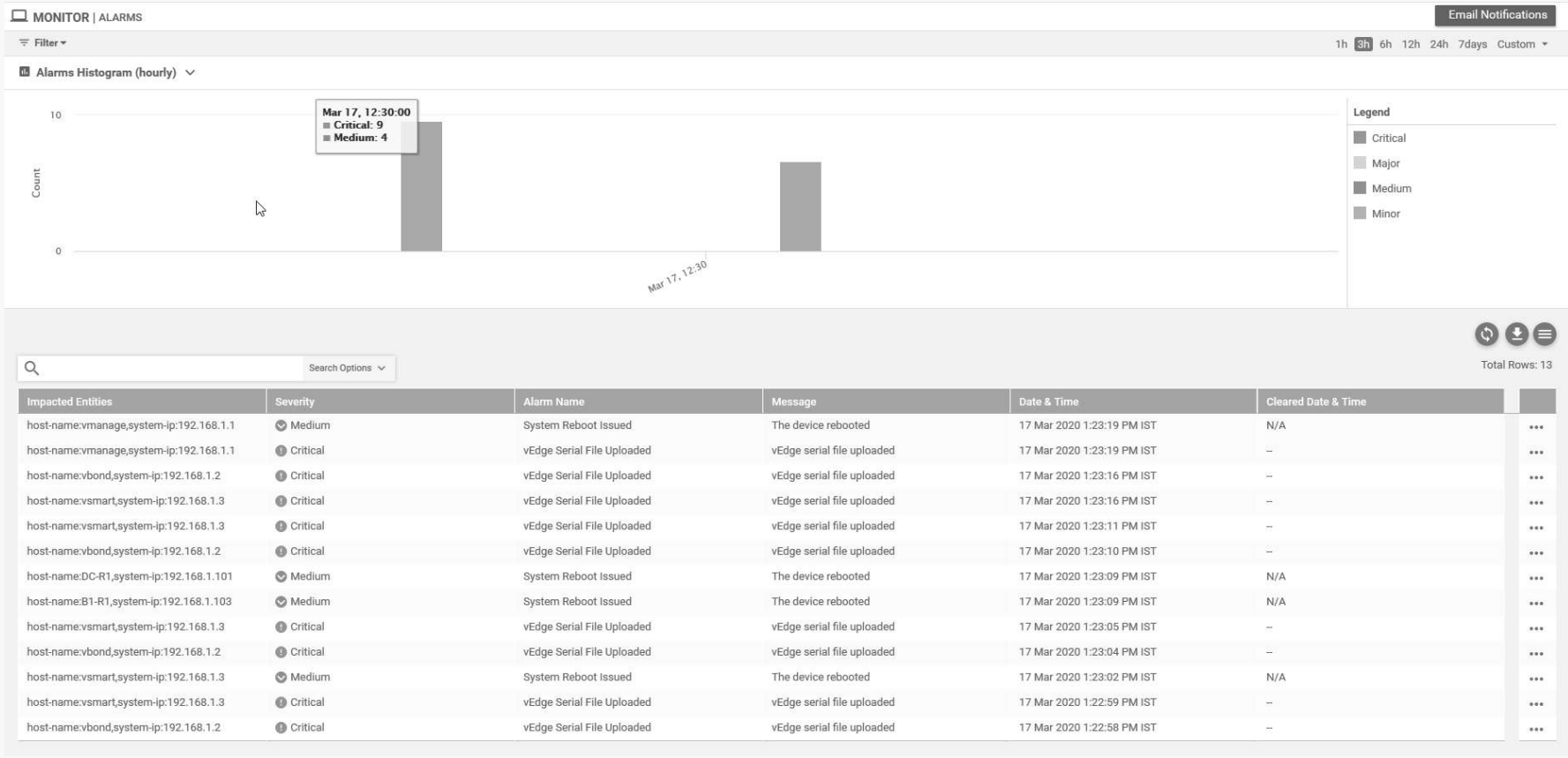
NETCONF

Syslog

SNMP

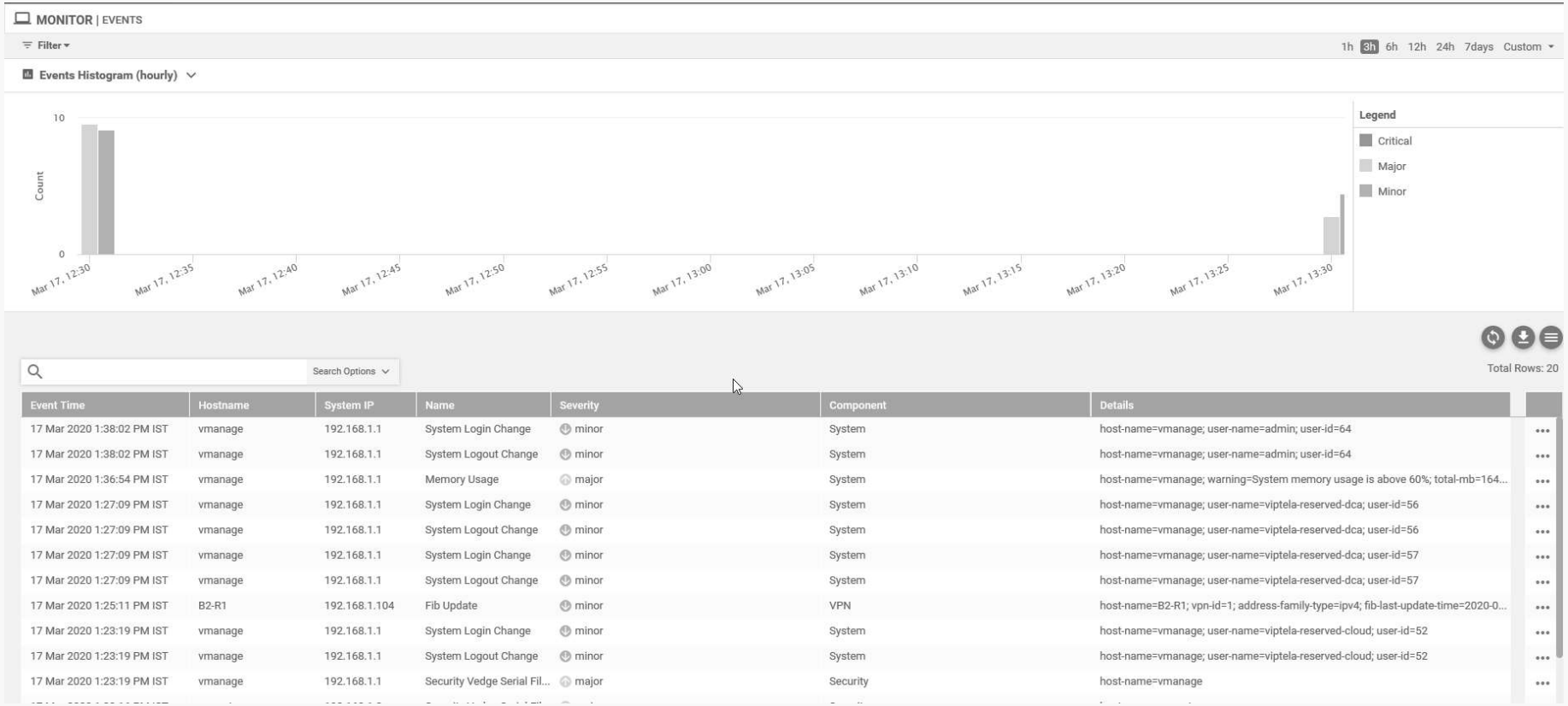
Flow Export

Alarms



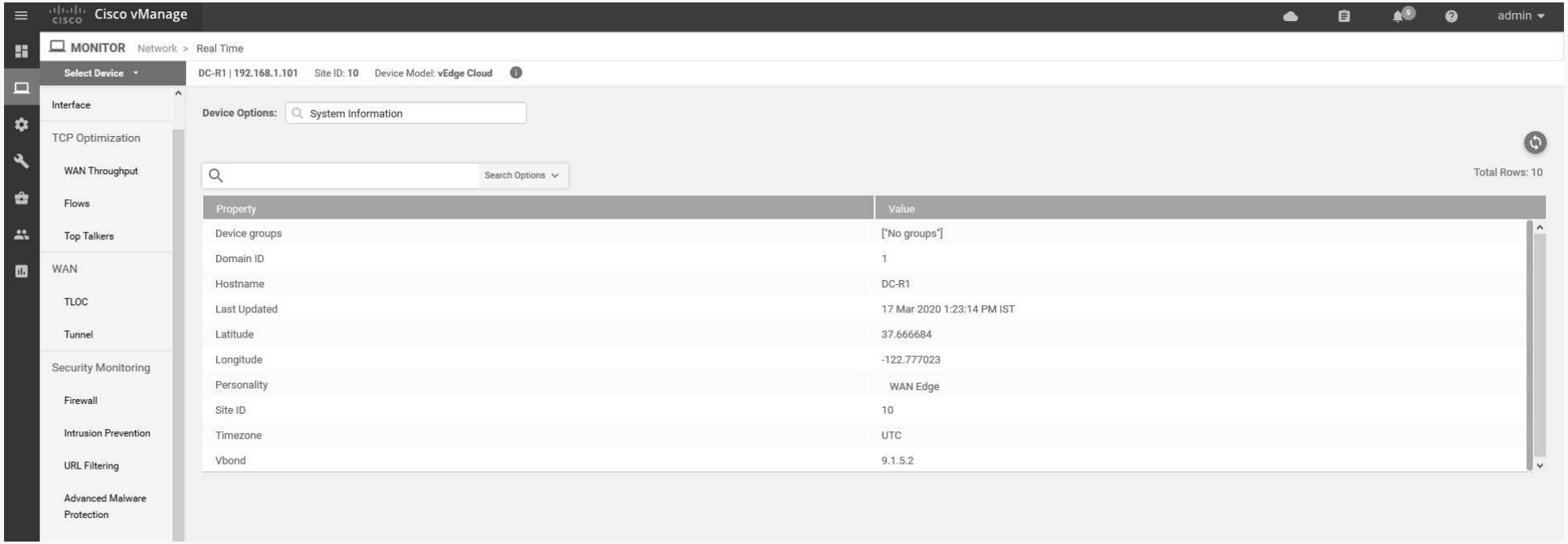
Impacted Entities	Severity	Alarm Name	Message	Date & Time	Cleared Date & Time
host-name:vmanage,system-ip:192.168.1.1	Medium	System Reboot Issued	The device rebooted	17 Mar 2020 1:23:19 PM IST	N/A
host-name:vmanage,system-ip:192.168.1.1	Critical	vEdge Serial File Uploaded	vEdge serial file uploaded	17 Mar 2020 1:23:19 PM IST	--
host-name:vbond,system-ip:192.168.1.2	Critical	vEdge Serial File Uploaded	vEdge serial file uploaded	17 Mar 2020 1:23:16 PM IST	--
host-name:vsmart,system-ip:192.168.1.3	Critical	vEdge Serial File Uploaded	vEdge serial file uploaded	17 Mar 2020 1:23:16 PM IST	--
host-name:vsmart,system-ip:192.168.1.3	Critical	vEdge Serial File Uploaded	vEdge serial file uploaded	17 Mar 2020 1:23:11 PM IST	--
host-name:vbond,system-ip:192.168.1.2	Critical	vEdge Serial File Uploaded	vEdge serial file uploaded	17 Mar 2020 1:23:10 PM IST	--
host-name:DC-R1,system-ip:192.168.1.101	Medium	System Reboot Issued	The device rebooted	17 Mar 2020 1:23:09 PM IST	N/A
host-name:B1-R1,system-ip:192.168.1.103	Medium	System Reboot Issued	The device rebooted	17 Mar 2020 1:23:09 PM IST	N/A
host-name:vsmart,system-ip:192.168.1.3	Critical	vEdge Serial File Uploaded	vEdge serial file uploaded	17 Mar 2020 1:23:05 PM IST	--
host-name:vbond,system-ip:192.168.1.2	Critical	vEdge Serial File Uploaded	vEdge serial file uploaded	17 Mar 2020 1:23:04 PM IST	--
host-name:vsmart,system-ip:192.168.1.3	Medium	System Reboot Issued	The device rebooted	17 Mar 2020 1:23:02 PM IST	N/A
host-name:vsmart,system-ip:192.168.1.3	Critical	vEdge Serial File Uploaded	vEdge serial file uploaded	17 Mar 2020 1:22:59 PM IST	--
host-name:vbond,system-ip:192.168.1.2	Critical	vEdge Serial File Uploaded	vEdge serial file uploaded	17 Mar 2020 1:22:58 PM IST	--

Events

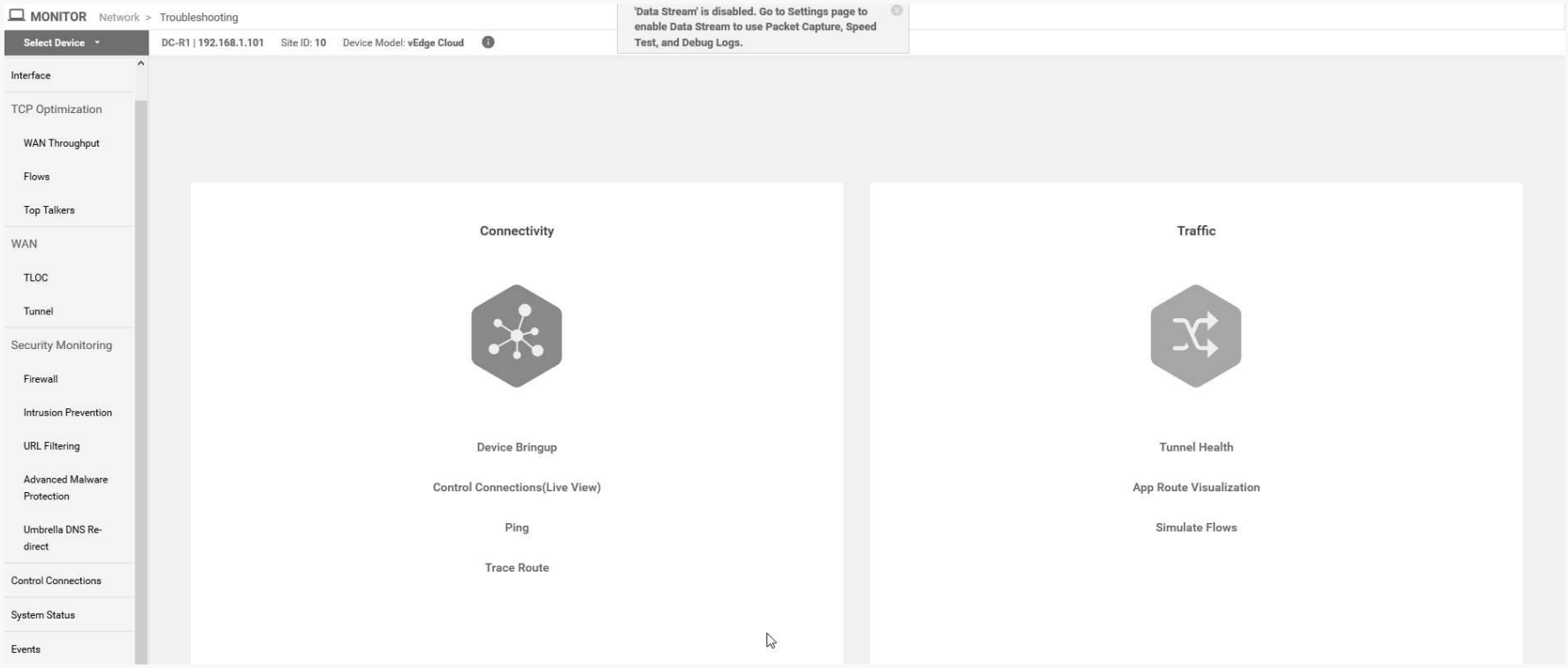


Event Time	Hostname	System IP	Name	Severity	Component	Details
17 Mar 2020 1:38:02 PM IST	vmanage	192.168.1.1	System Login Change	minor	System	host-name=vmanage; user-name=admin; user-id=64
17 Mar 2020 1:38:02 PM IST	vmanage	192.168.1.1	System Logout Change	minor	System	host-name=vmanage; user-name=admin; user-id=64
17 Mar 2020 1:36:54 PM IST	vmanage	192.168.1.1	Memory Usage	major	System	host-name=vmanage; warning=System memory usage is above 60%; total-mb=164...
17 Mar 2020 1:27:09 PM IST	vmanage	192.168.1.1	System Login Change	minor	System	host-name=vmanage; user-name=viptela-reserved-dca; user-id=56
17 Mar 2020 1:27:09 PM IST	vmanage	192.168.1.1	System Logout Change	minor	System	host-name=vmanage; user-name=viptela-reserved-dca; user-id=56
17 Mar 2020 1:27:09 PM IST	vmanage	192.168.1.1	System Login Change	minor	System	host-name=vmanage; user-name=viptela-reserved-dca; user-id=57
17 Mar 2020 1:27:09 PM IST	vmanage	192.168.1.1	System Logout Change	minor	System	host-name=vmanage; user-name=viptela-reserved-dca; user-id=57
17 Mar 2020 1:25:11 PM IST	B2-R1	192.168.1.104	Fib Update	minor	VPN	host-name=B2-R1; vpn-id=1; address-family-type=ipv4; fib-last-update-time=2020-0...
17 Mar 2020 1:23:19 PM IST	vmanage	192.168.1.1	System Login Change	minor	System	host-name=vmanage; user-name=viptela-reserved-cloud; user-id=52
17 Mar 2020 1:23:19 PM IST	vmanage	192.168.1.1	System Logout Change	minor	System	host-name=vmanage; user-name=viptela-reserved-cloud; user-id=52
17 Mar 2020 1:23:19 PM IST	vmanage	192.168.1.1	Security Vedge Serial Fil...	major	Security	host-name=vmanage

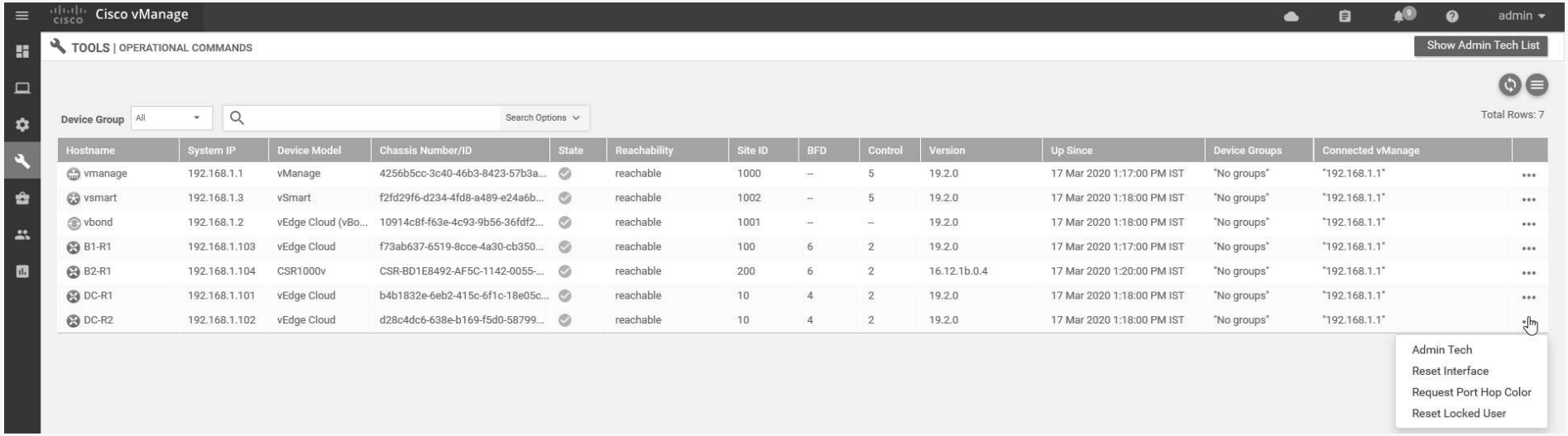
System Information – Real Time



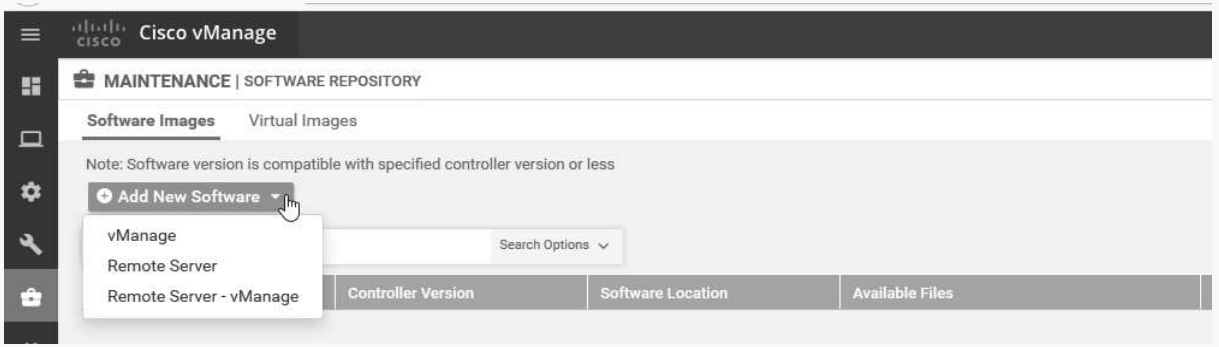
Troubleshooting

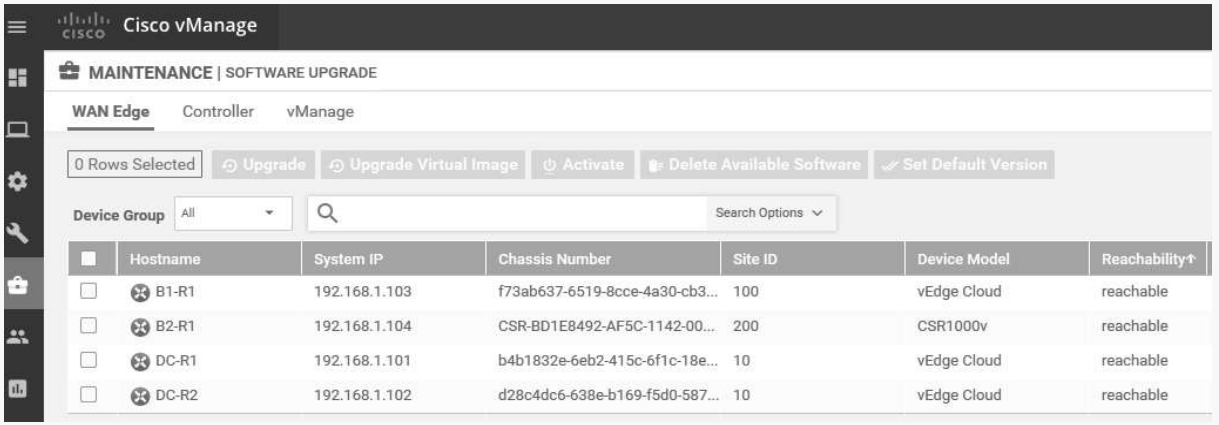


Operational Commands

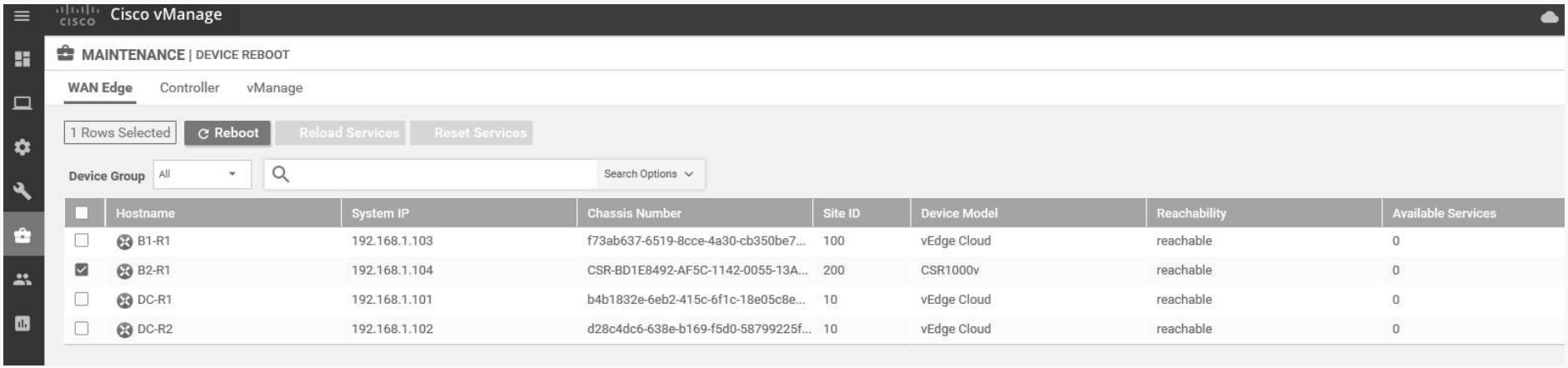


Software Repository and upgrades





Device Reboot



Manage users and user groups

Settings


Cisco vManage
admin
ADMINISTRATION | SETTINGS
Organization Name
learnedze
View
vBond
9.1.5.2 : 12346
View | Edit
Email Notifications
Disabled
View | Edit
Hardware WAN Edge Certificate Authorization
Onbox
View | Edit
Controller Certificate Authorization
Enterprise
View | Edit
WAN Edge Cloud Certificate Authorization
Automated
View | Edit
Web Server Certificate
13 Jul 2024 4:00:30 AM
CSR | Certificate
Enforce Software Version (ZTP)
View | Edit
Banner
Disabled
View | Edit
Reverse Proxy
Statistics Setting
View | Edit
Cloud onRamp for SaaS
Manage Encrypted Password
vAnalytics
Call Home
Disabled
View | Edit
Client Session Timeout
Disabled
View | Edit