CCNP Enterprise Certification

ENSDWI : 300-415

CCNP Enterprise Certification

ENSDWI : 300-415

CCNP Enterprise Certification

ENSDWI : 300-415

3.0 Router Deployment 20 %

3.0 Topics

- 3.1 Describe WAN Edge deployment
- 3.1.a On-boarding
- 3.1.b Orchestration with zero-touch provisioning/plug-and-play
- 3.1.c Single/multi data center/regional hub deployments
- 3.2 Configure and verify SD-WAN data plane
- 3.2.a Circuit termination/TLOC-extension
- 3.2.b Underlay-overlay connectivity
- 3.3 Configure and verify OMP
- 3.4 Configure and verify TLOCs
- 3.5 Configure and verify CLI and vManage feature configuration templates
- 3.5.a VRRP
- 3.5.b OSPF
- 3.5.c BGP

Deploy vEdge Routers

- Create a minimal configuration for vEdges and establish IP connectivity into the WAN circuits (Deploy vEdge section).
- Verify that vEdge routers are able to reach the Controllers (vEdge Connections section).
- Authenticate each vEdge router (Certify vEdges section).
- Register each vEdge router with vManage (Register vEdge section).
- Verify that the vEdge are up in the vManage dashboard .

Vedgedc1 & Vedgedc2

vedgedc1

Launch

```
conf t
     system
          host-name vedgedc1
          system-ip 172.27.0.10
          site-id 10
         no route-consistency-check
         organization-name "
         vbond 2.2.6.2
               !
         commit and-quit
```

vedgedc2

Launch

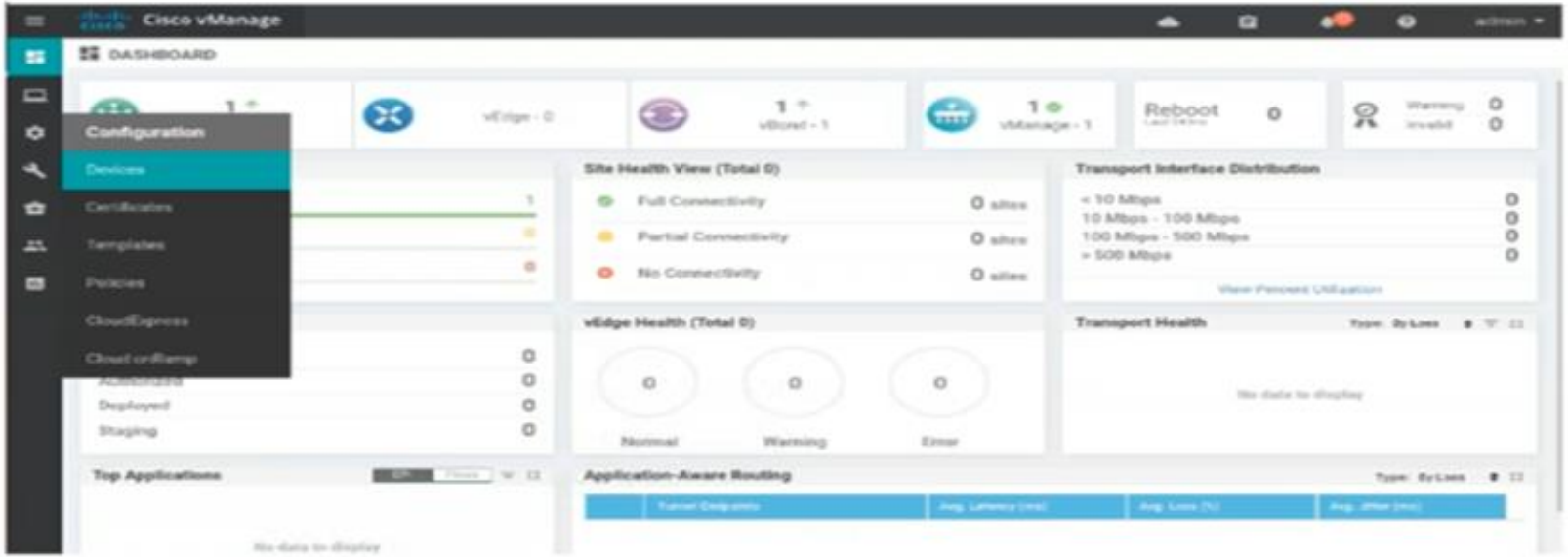
```
conf t
     system
          host-name vedgedc2
          system-ip 172.27.0.11
          site-id 10
         no route-consistency-check
         organization-name "                    !1"
         vbond 2.2.6.2
```

```
conf t
vpn 0
 interface ge0/1
    ip address 2.2.4.2/24
    tunnel-interface
     encapsulation ipsec
     color gold
     allow-service all
    !
    no shutdown
 !
 interface ge0/2
    ip address 12.20.50.2/24
    tunnel-interface
     encapsulation ipsec
     color mpls
     allow-service all
    !
    no shutdown
 !
 ip route 0.0.0.0/0 2.2.4.1
 ip route 0.0.0.0/0 12.20.50.1
!
commit and-quit
```

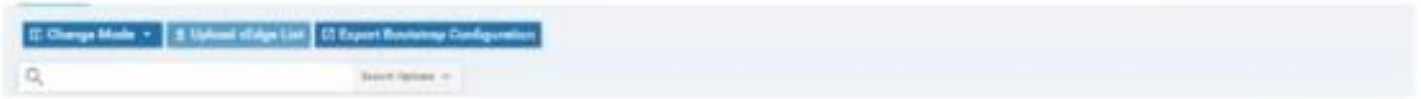
```
Commit complete.
vebranch1# conf t
Entering configuration mode terminal
vebranch1(config)# vpn 0
vebranch1(config-vpn-0)#  interface ge0/1
vebranch1(config-interface-ge0/1)#     ip address 2.2.8.2/24
vebranch1(config-interface-ge0/1)#     tunnel-interface
vebranch1(config-tunnel-interface)#      encapsulation ipsec
vebranch1(config-tunnel-interface)#      color gold
vebranch1(config-tunnel-interface)#      allow-service all

vebranch1(config-tunnel-interface)#     !
vebranch1(config-tunnel-interface)#     no shutdown
vebranch1(config-tunnel-interface)#  !
vebranch1(config-tunnel-interface)#  interface ge0/2
vebranch1(config-interface-ge0/2)#     ip address 12.20.90.2/24
vebranch1(config-interface-ge0/2)#     tunnel-interface
vebranch1(config-tunnel-interface)#      encapsulation ipsec
vebranch1(config-tunnel-interface)#      color mpls
vebranch1(config-tunnel-interface)#      allow-service all

vebranch1(config-tunnel-interface)#     !
vebranch1(config-tunnel-interface)#     no shutdown
vebranch1(config-tunnel-interface)#  !
vebranch1(config-tunnel-interface)#  ip route 0.0.0.0/0 2.2.8.1
vebranch1(config-vpn-0)#  ip route 0.0.0.0/0 12.20.90.1
vebranch1(config-vpn-0)# !
vebranch1(config-vpn-0)# commit and-quit
Commit complete.
vebranch1# request root-cert-chain install scp://ubuntu@192.168.122.84:/home/ubuntu/certify/root-ca vpn 512
Uploading root-ca-cert-chain via VPN 512
Copying ... ubuntu@192.168.122.84:/home/ubuntu/certify/root-ca via VPN 512
Warning: Permanently added '192.168.122.84' (ECDSA) to the list of known hosts.
ubuntu@192.168.122.84's password:
Permission denied, please try again.
ubuntu@192.168.122.84's password:
```

Download the serial file from the following link,

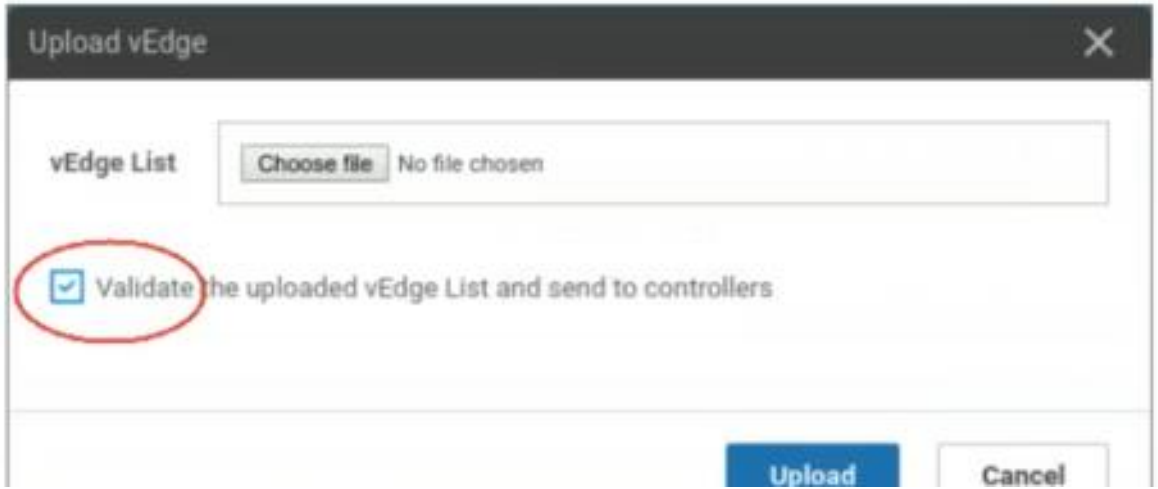
https://s3-us-west-2.amazonaws.com/bringup/viptela_serial_file.viptela

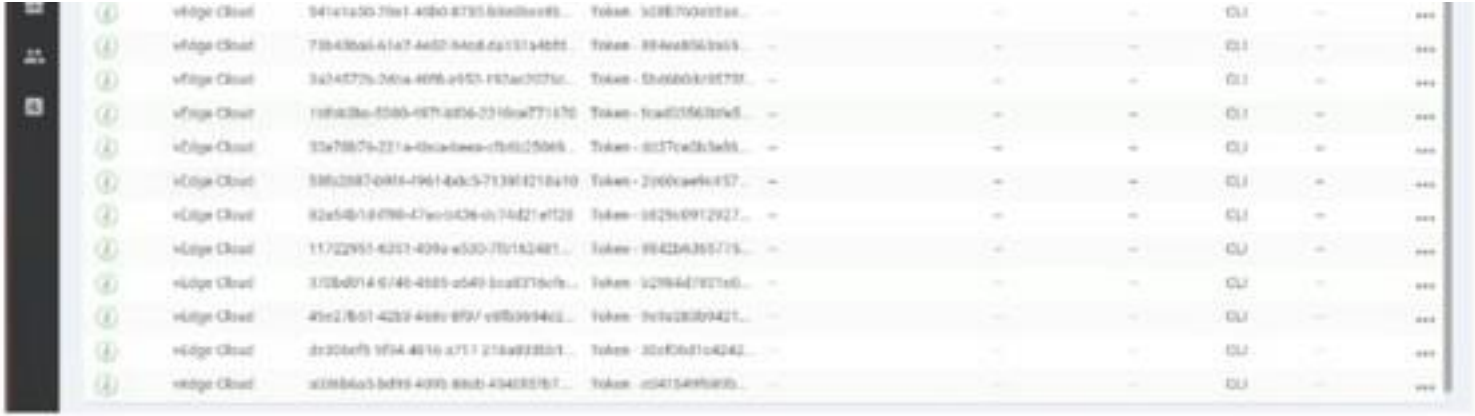


To Upload the serial file, click on **Configuration > Devices > Upload vEdge** List and choose the downloaded file



Enable checkbox to validate the uploaded vEdge List and send to controllers

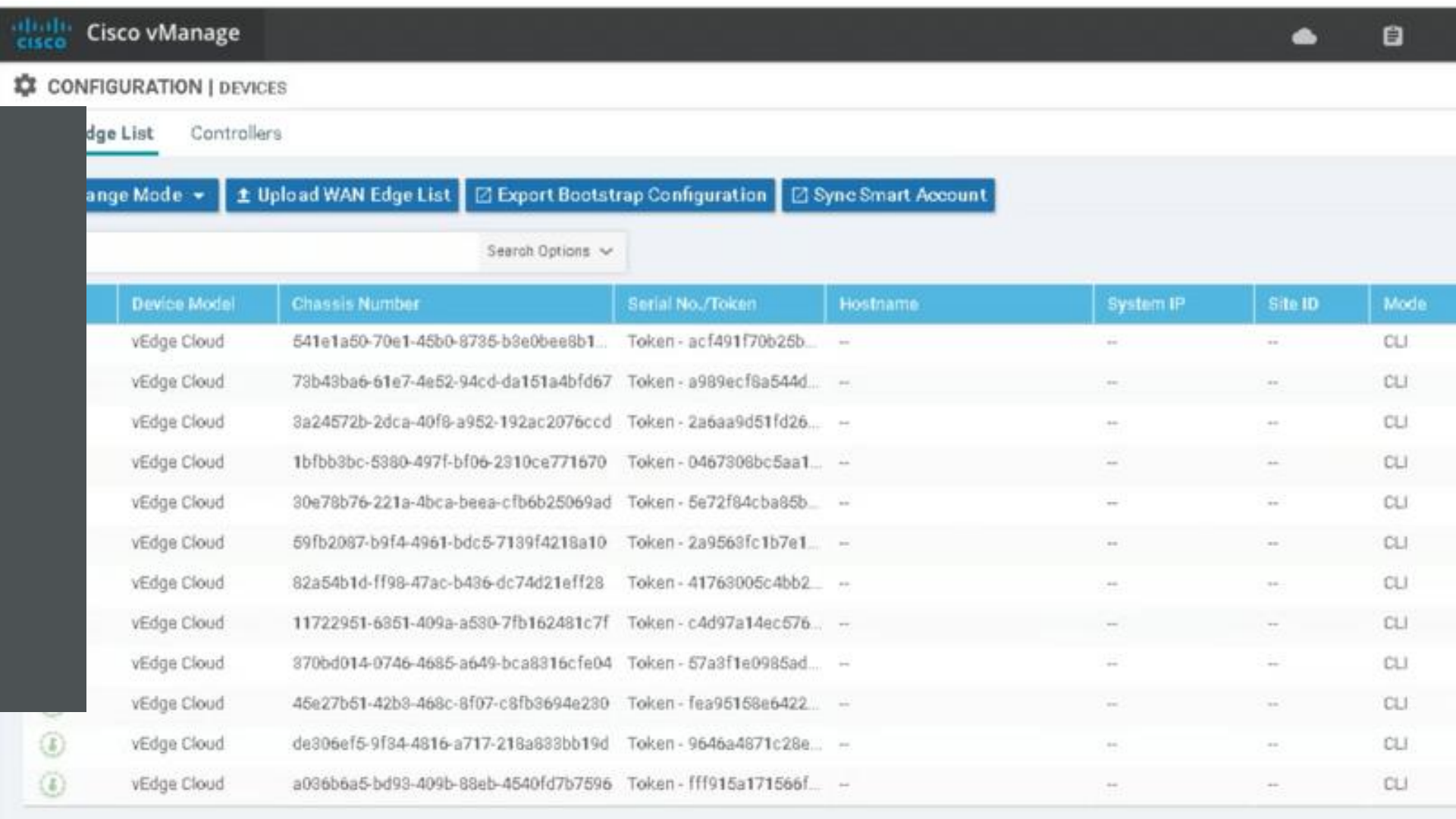




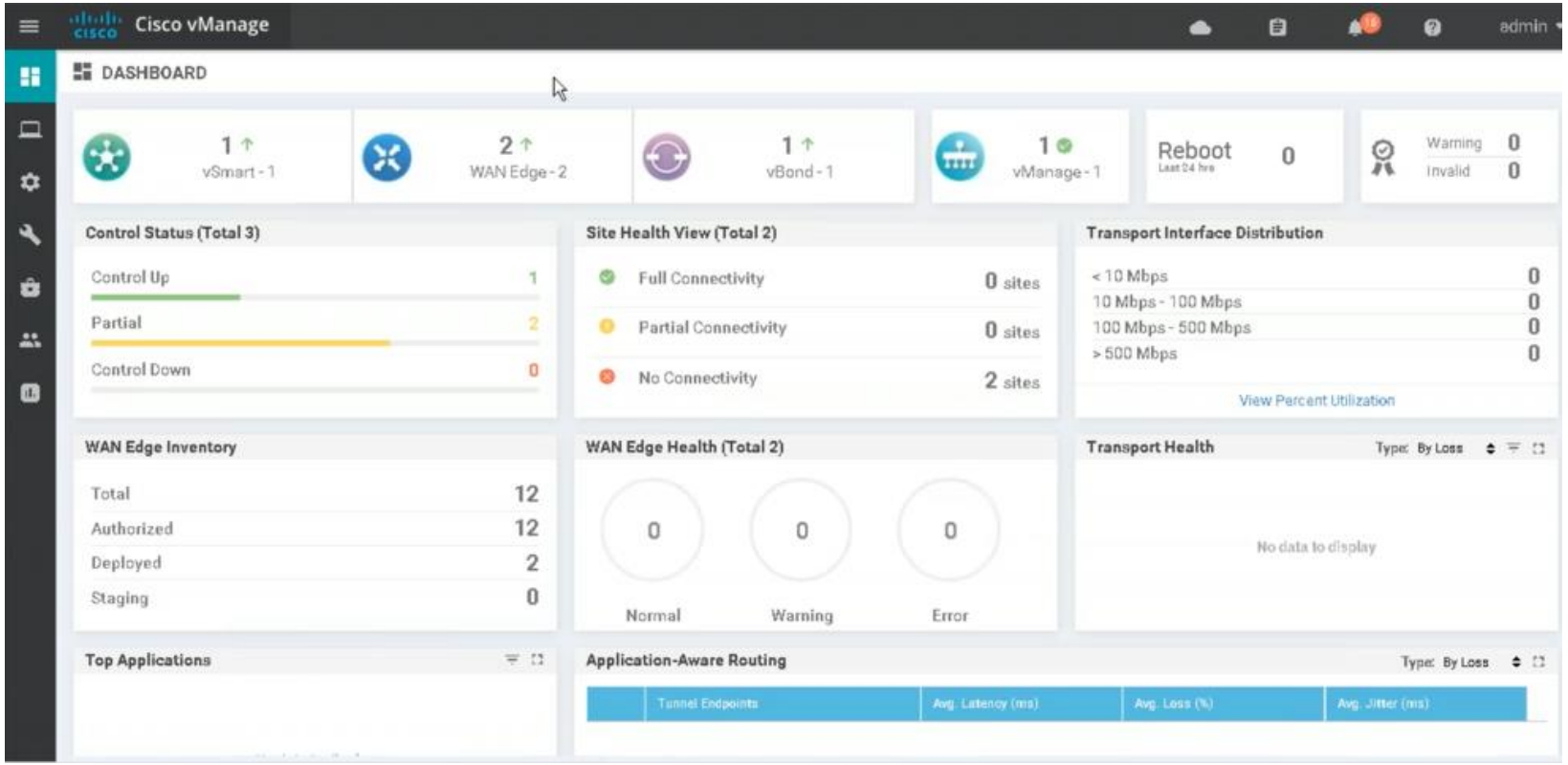
Note: This information is provided by Cisco SD-WAN upon purchase of licenses for the vEdge cloud routers.

If the token and chassis number are not visible, adjust the column width.

1. Download the list, because a direct copy might not be allowed.
2. Open the CSV file and select the first four serial numbers and their token numbers for the four vEdge routers.
3. SSH into each vEdge and register the vEdge using the command below. In each vEdge use a unique

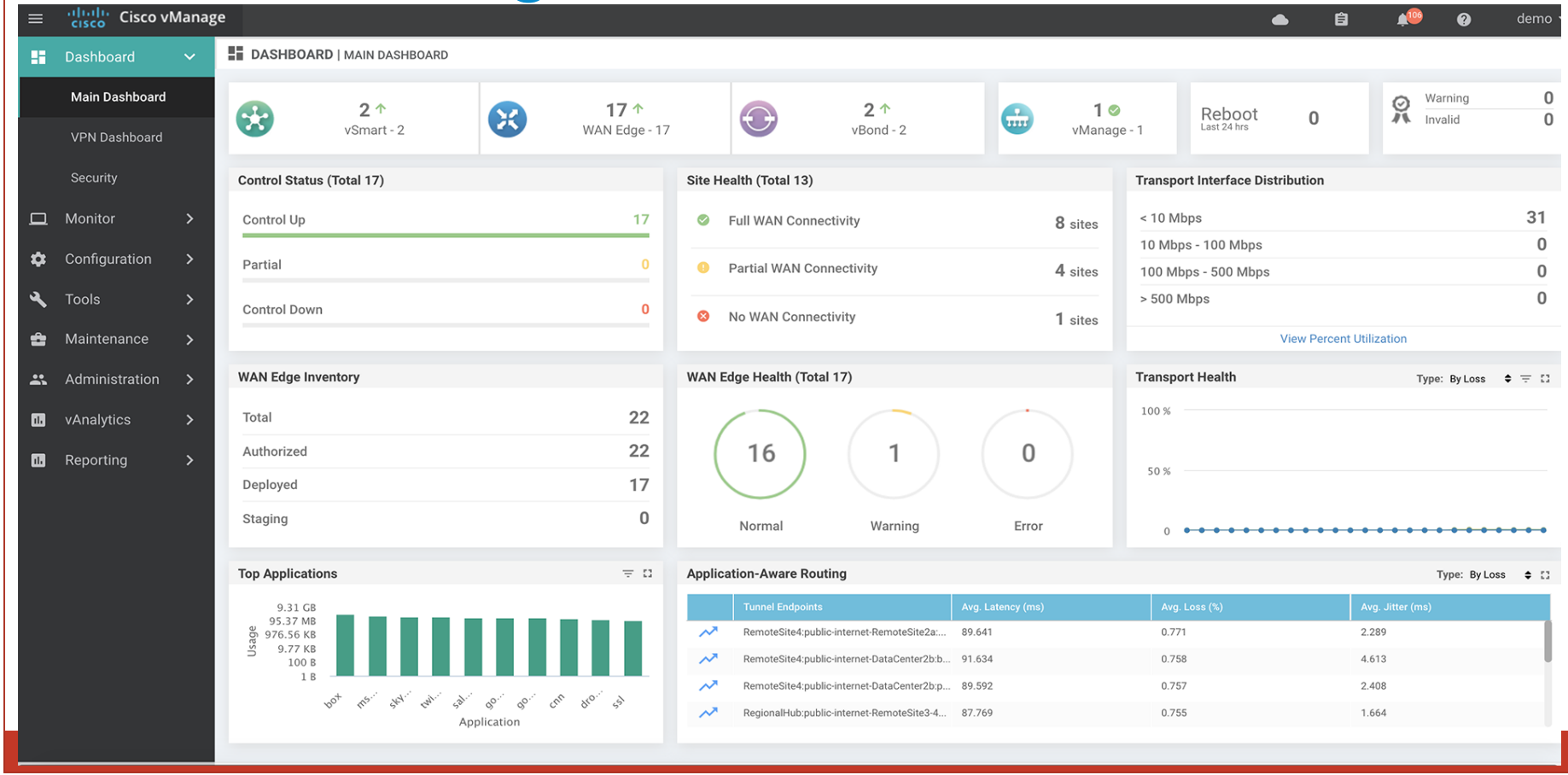

Cisco vManage
CONFIGURATION | DEVICES
dge List
Controllers
ange Mode
Upload WAN Edge List
Export Bootstrap Configuration
Sync Smart Account
Search Options
Device Model
Chassis Number
Serial No./Token
Hostname
System IP
Site ID
Mode
vEdge Cloud 541e1a50-70e1-45b0-8735-b3e0bee8b1... Token - acf491f70b25b... -- -- -- CLI
vEdge Cloud 73b43ba6-61e7-4e52-94cd-da151a4bfd67 Token - a989ecf8a544d... -- -- -- CLI
vEdge Cloud 3a24572b-2dca-40f8-a952-192ac2076ccd Token - 2a6aa9d51fd26... -- -- -- CLI
vEdge Cloud 1bfbb3bc-5380-497f-bf06-2310ce771670 Token - 0467306bc5aa1... -- -- -- CLI
vEdge Cloud 30e78b76-221a-4bca-beea-cfb6b25069ad Token - 5e72f84cba85b... -- -- -- CLI
vEdge Cloud 59fb2087-b9f4-4961-bdc5-7139f4218a10 Token - 2a9563fc1b7e1... -- -- -- CLI
vEdge Cloud 82a54b1d-ff98-47ac-b436-dc74d21eff28 Token - 41763005c4bb2... -- -- -- CLI
vEdge Cloud 11722951-6351-409a-a530-7fb162481c7f Token - c4d97a14ec576... -- -- -- CLI
vEdge Cloud 870bd014-0746-4685-a649-bca8316cfe04 Token - 57a3f1e0985ad... -- -- -- CLI
vEdge Cloud 45e27b51-42b3-468c-8f07-c8fb3694e230 Token - fea95158e6422... -- -- -- CLI
vEdge Cloud de306ef5-9f34-4816-a717-218a833bb19d Token - 9646a4871c28e... -- -- -- CLI
vEdge Cloud a036b6a5-bd93-409b-88eb-4540fd7b7596 Token - fff915a171566f... -- -- -- CLI


Untitled - Notepad
File Edit Format View Help
541e1a50-70e1-45b0-8735-b3e0bee8b148 acf491f70b25b3085702b9eb6717624d
73b43ba6-61e7-4e52-94cd-da151a4bfd67 a989ecf8a544d10309e235ec421439c
request vedge-cloud activate chassis-number 541e1a50-70e1-45b0-8735-b3e0bee8b148 token acf491f70b25b3085702b9eb6717624d
request vedge-cloud activate chassis-number 541e1a50-70e1-45b0-8735-b3e0bee8b148 token acf491f70b25b3085702b9eb6717624d

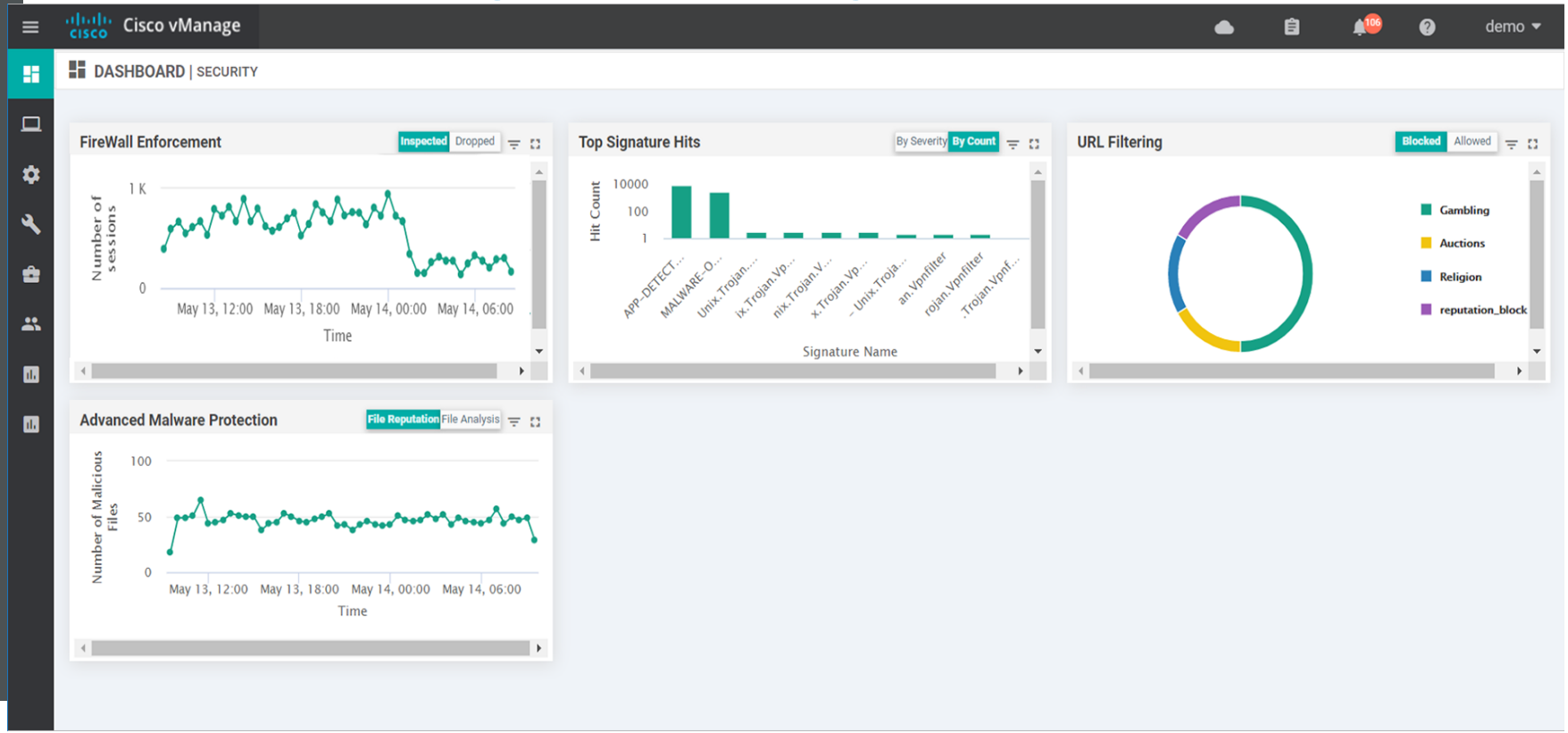

Cisco vManage
admin
DASHBOARD
1 vSmart - 1
2 WAN Edge - 2
1 vBond - 1
1 vManage - 1
Reboot 0
Last 24 hrs
Warning 0
Invalid 0
Control Status (Total 3)
Control Up 1
Partial 2
Control Down 0
Site Health View (Total 2)
Full Connectivity 0 sites
Partial Connectivity 0 sites
No Connectivity 2 sites
Transport Interface Distribution
< 10 Mbps 0
10 Mbps - 100 Mbps 0
100 Mbps - 500 Mbps 0
> 500 Mbps 0
View Percent Utilization
WAN Edge Inventory
Total 12
Authorized 12
Deployed 2
Staging 0
WAN Edge Health (Total 2)
0 0 0
Normal Warning Error
Transport Health
Type: By Loss
No data to display
Top Applications
Application-Aware Routing
Type: By Loss
Tunnel Endpoints
Avg. Latency (ms)
Avg. Loss (%)
Avg. Jitter (ms)

vManage Dashboard Tour

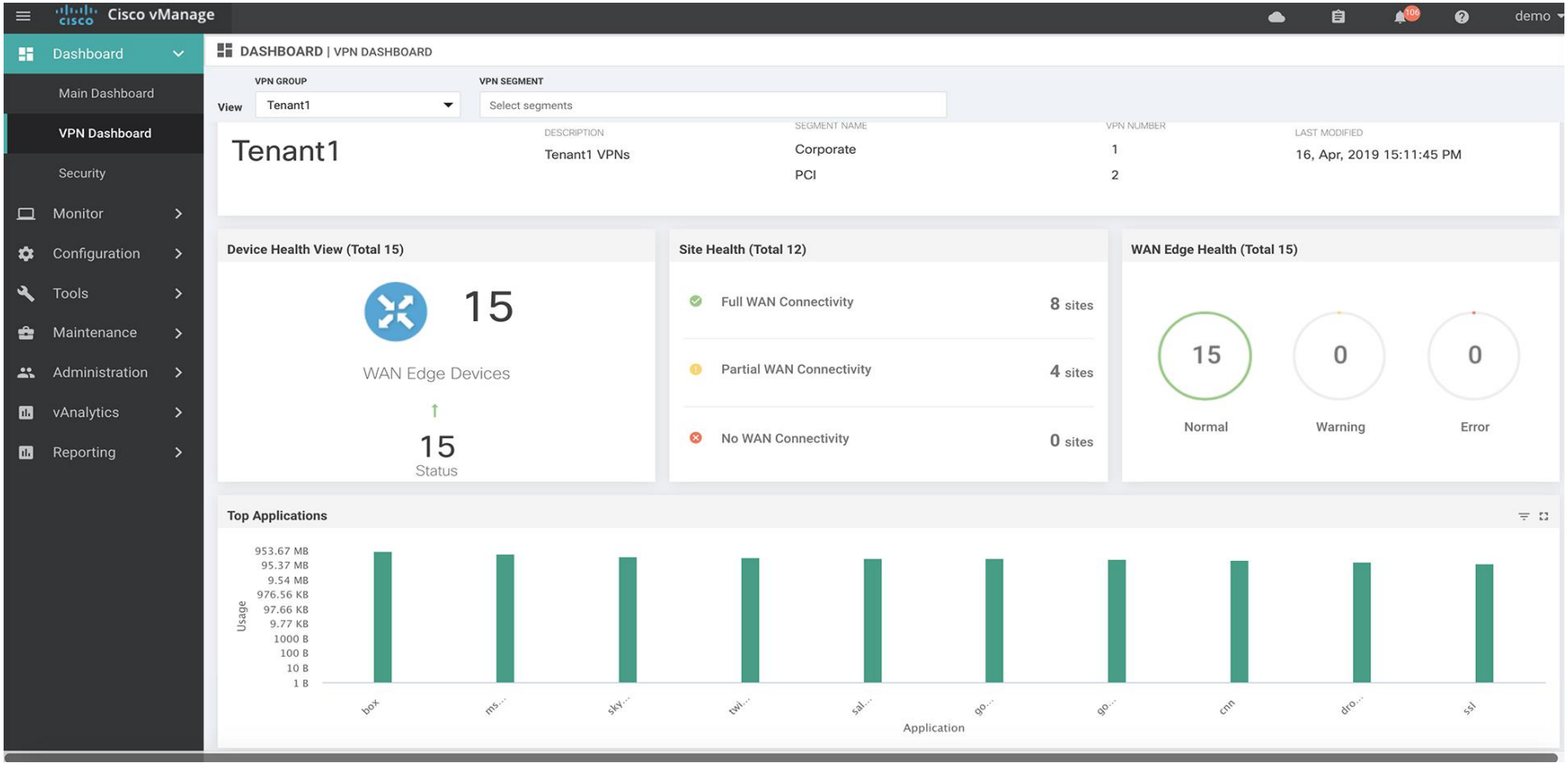
Cisco vManage main dashboard



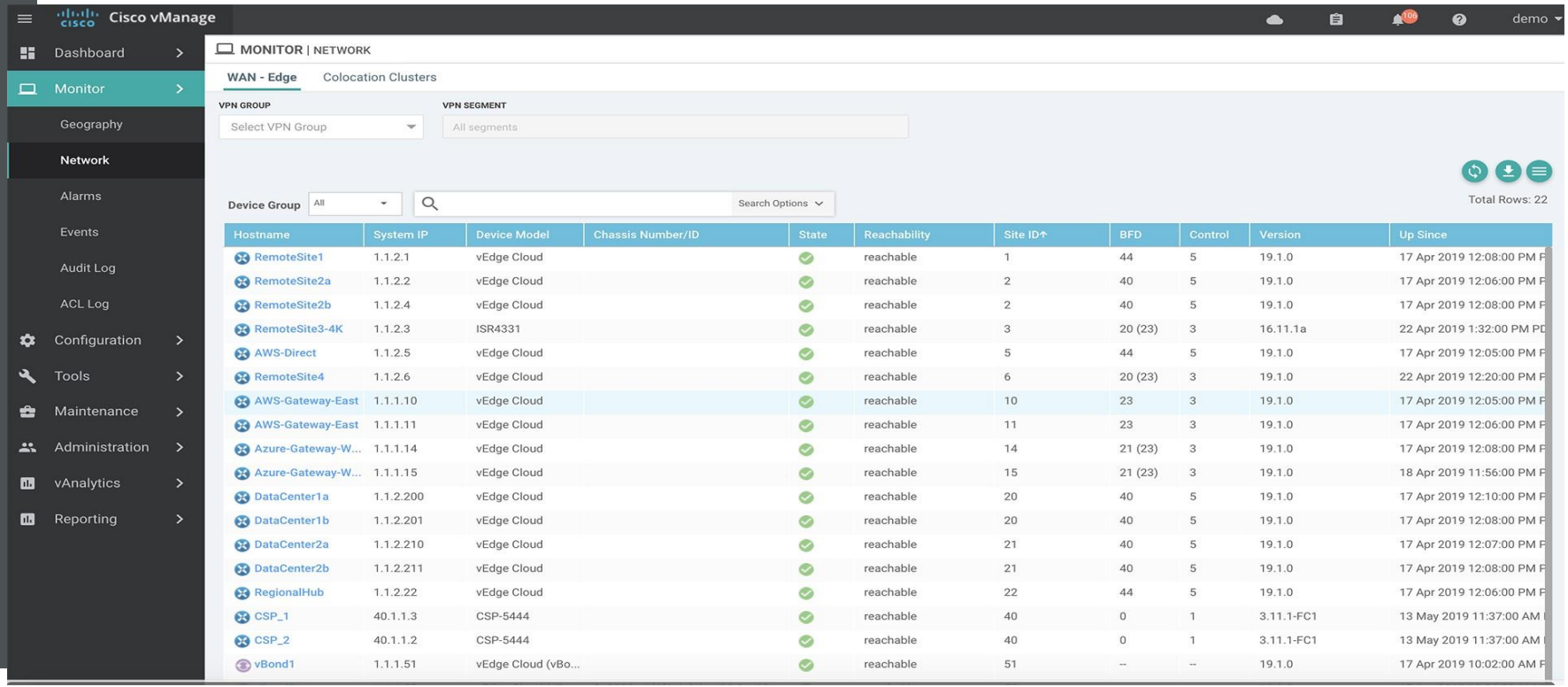
Cisco vManage security dashboard



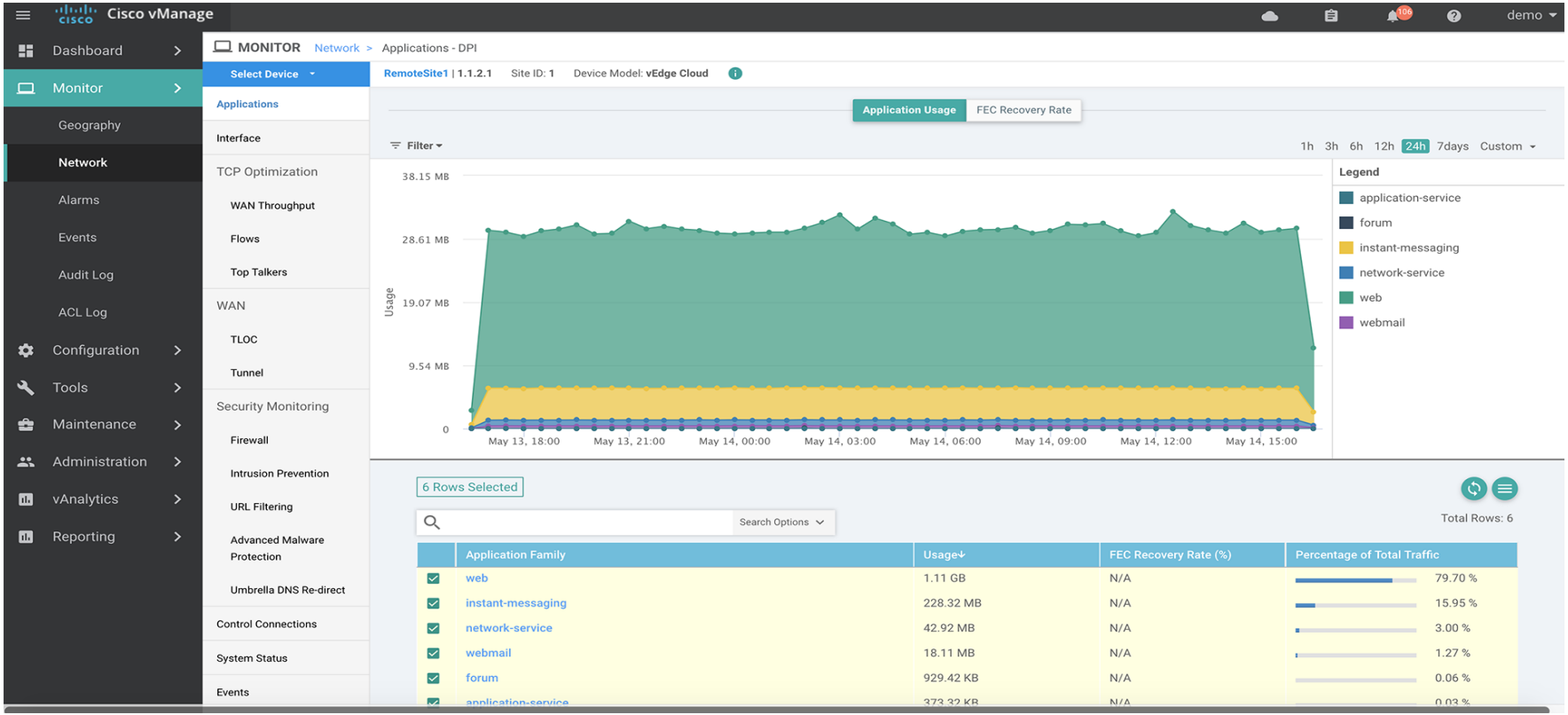
Cisco vManage VPN dashboard



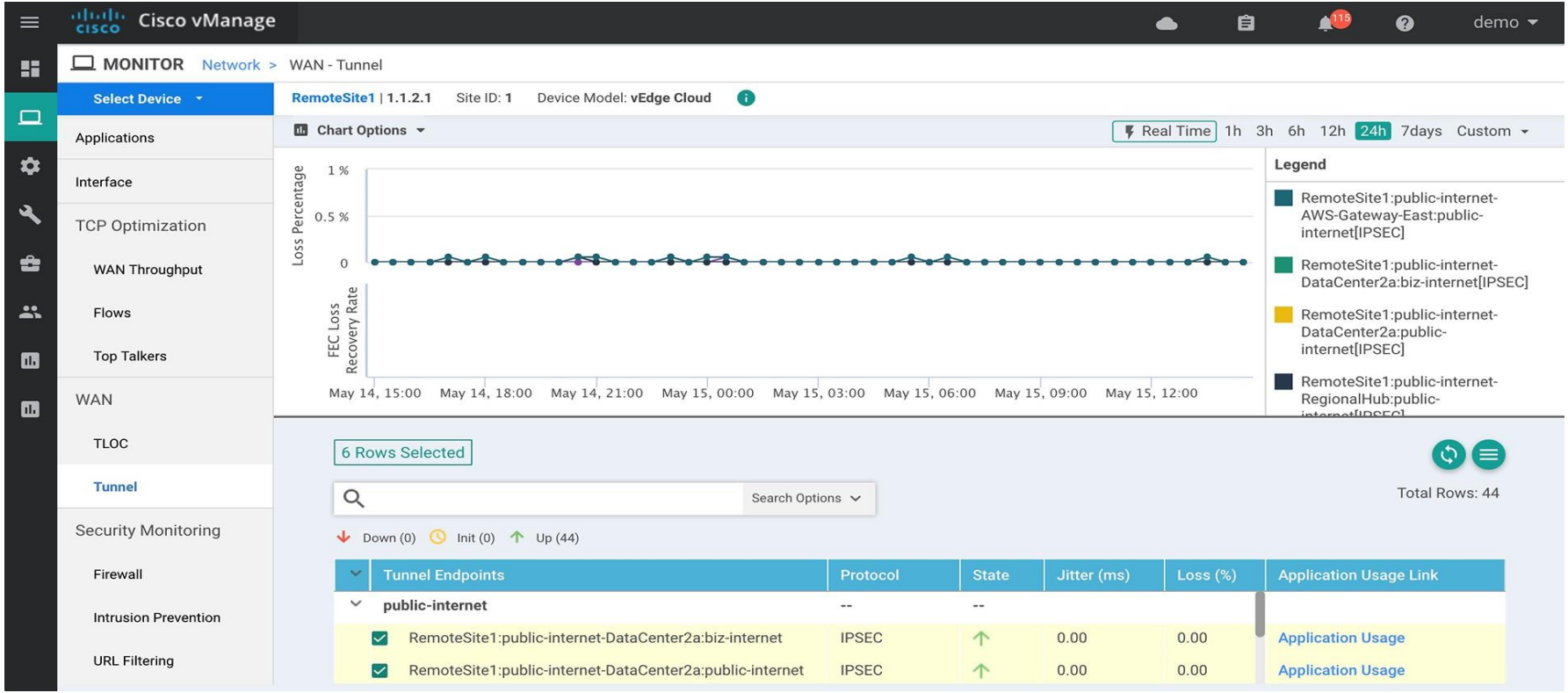
WAN Edge device list



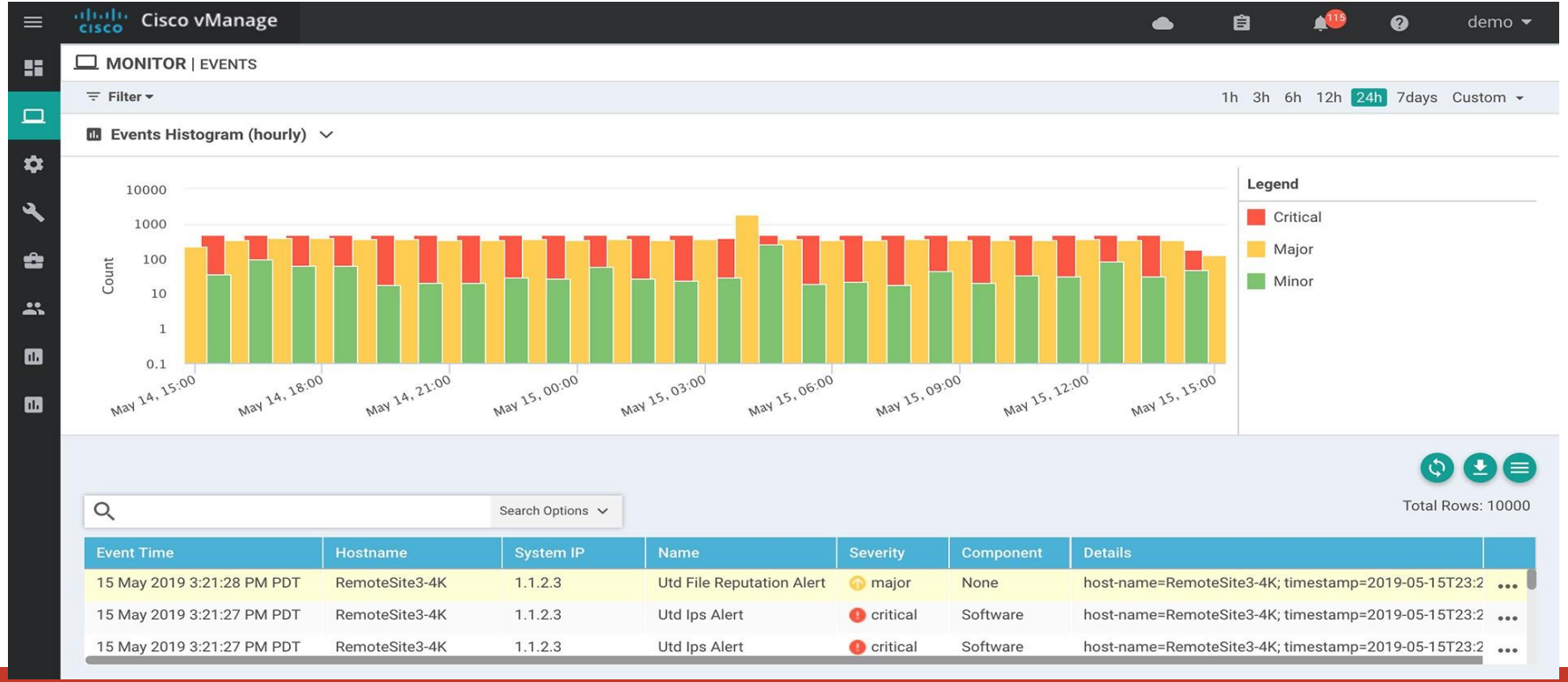
Application recognition view



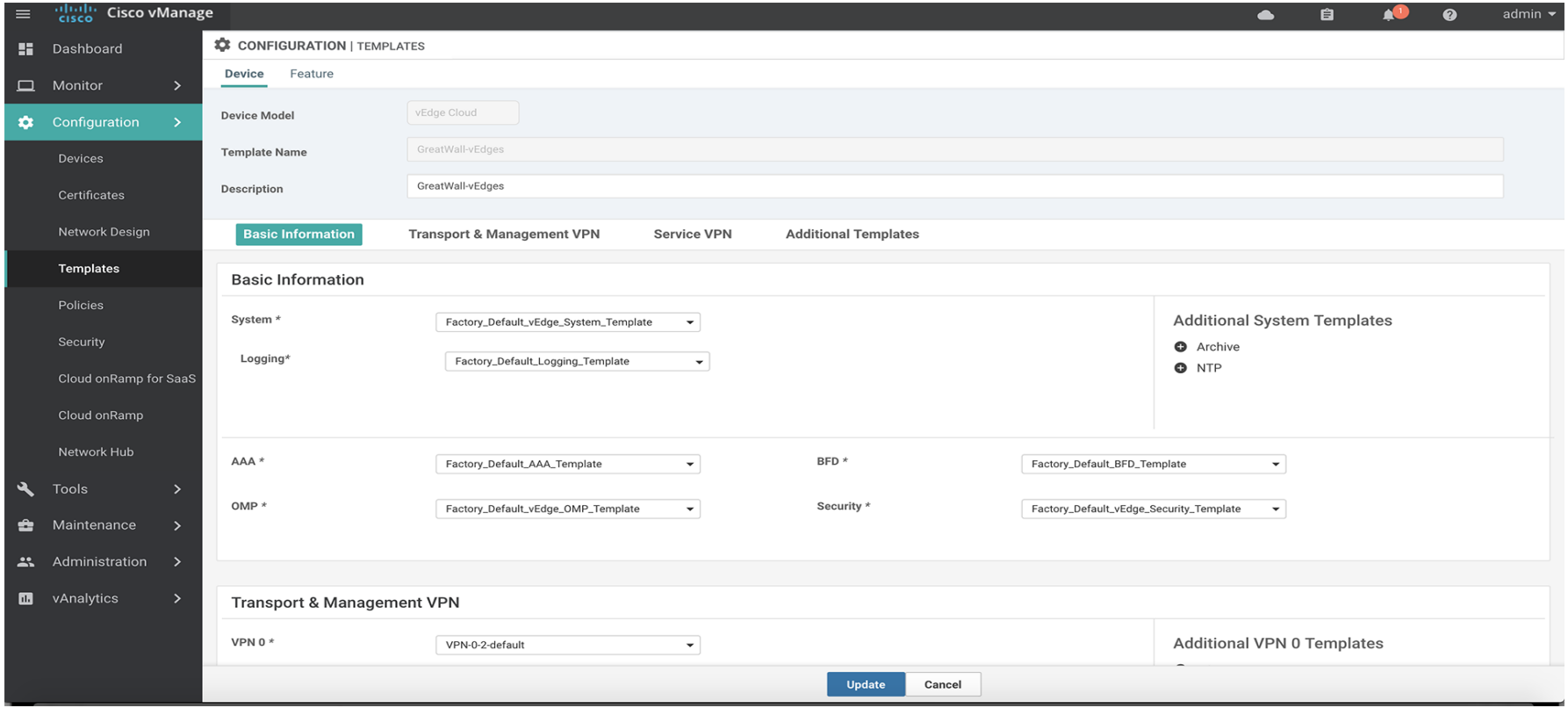
Tunnel performance in vManage



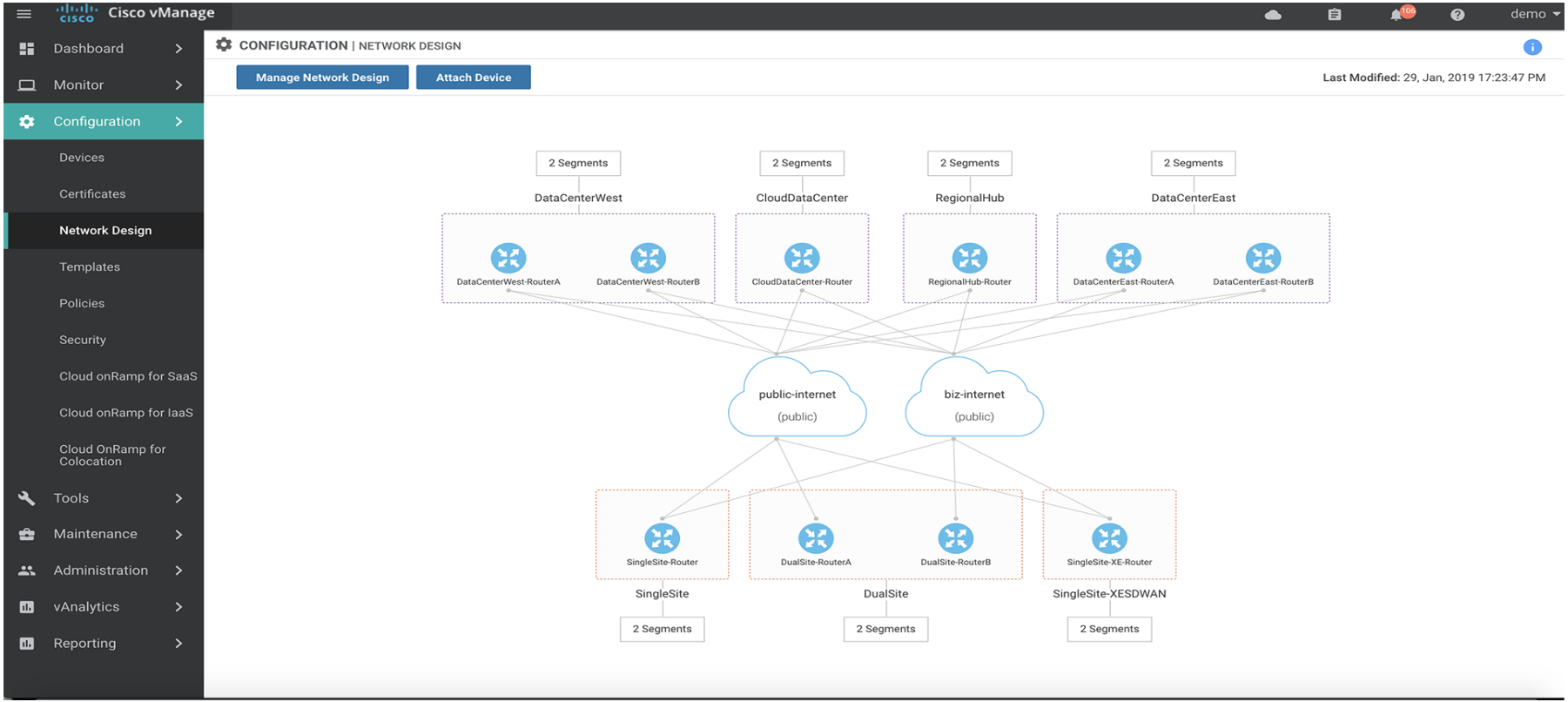
Events in vManage



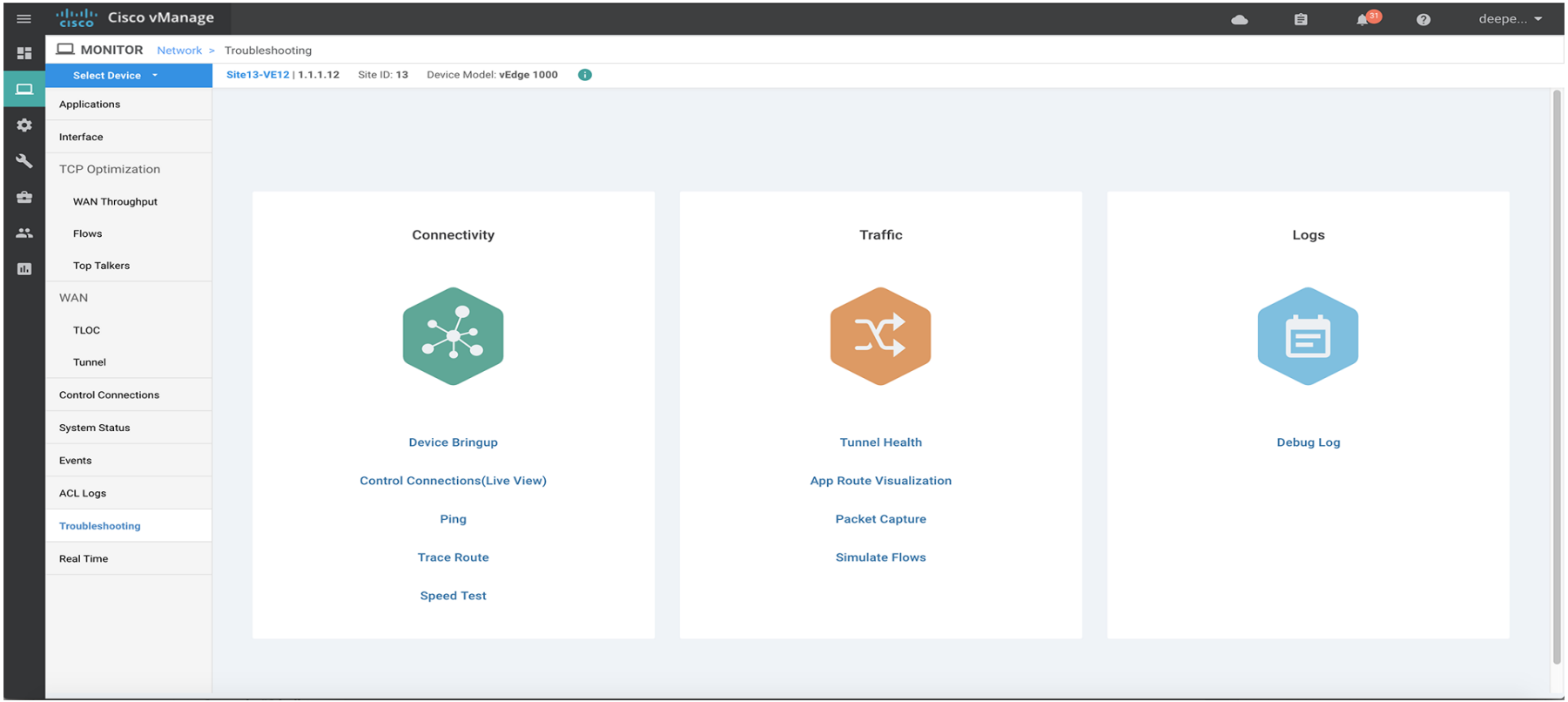
Sample Device Template



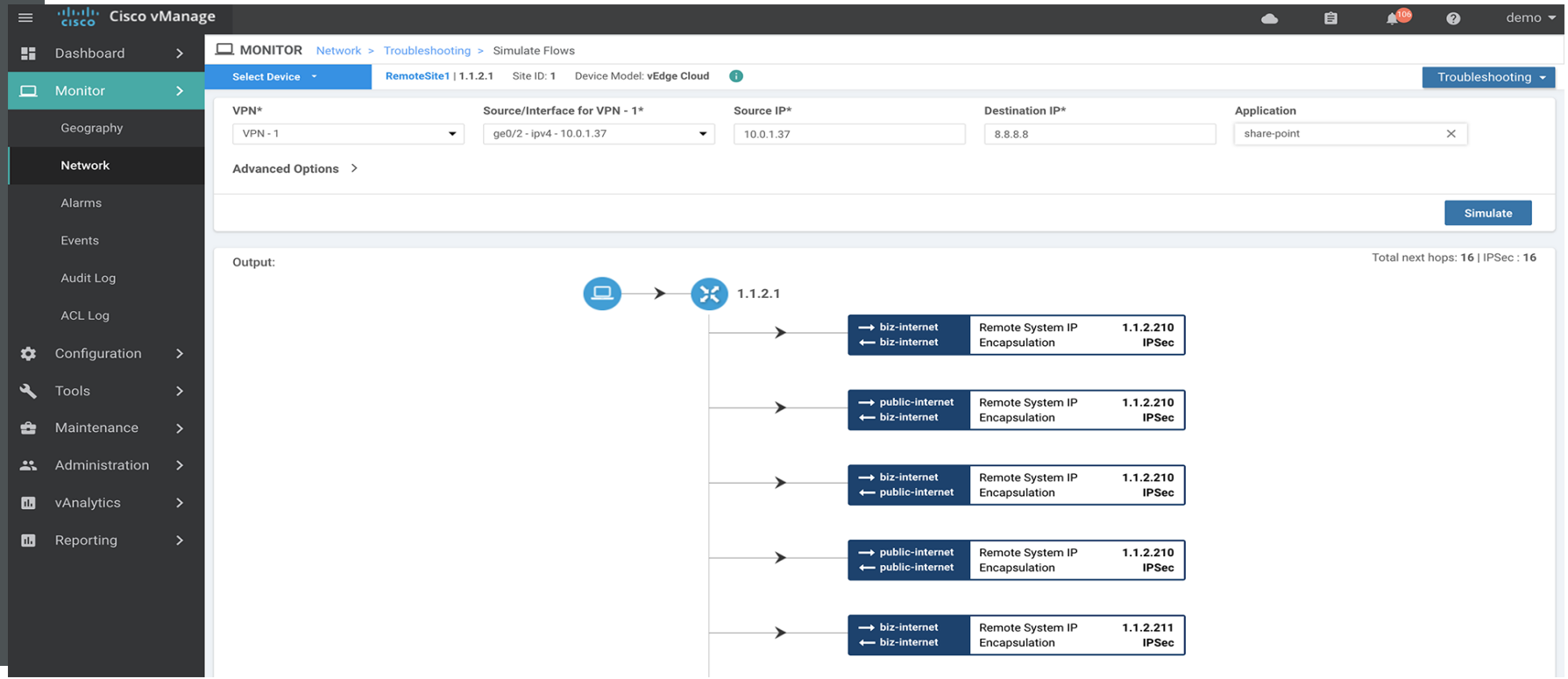
Network Design



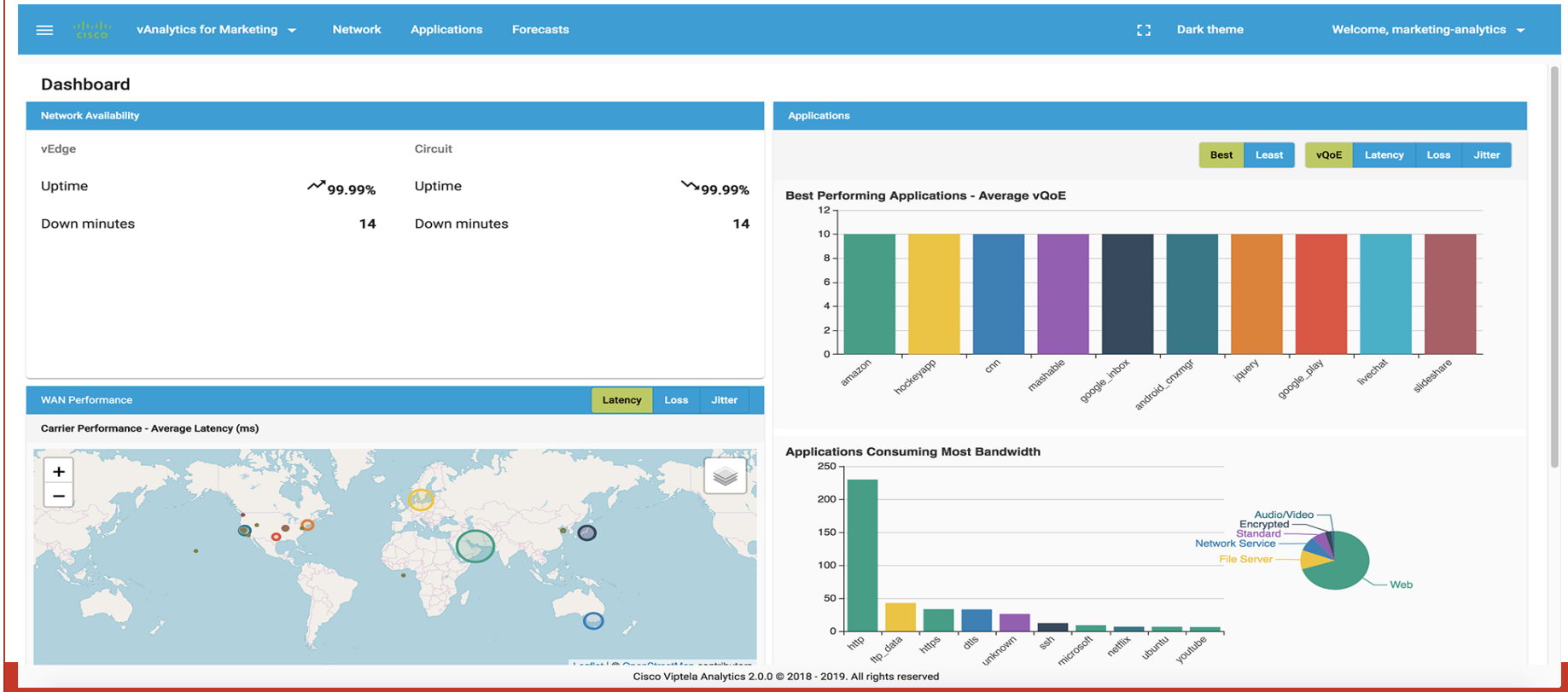
Cisco vManage Troubleshooting



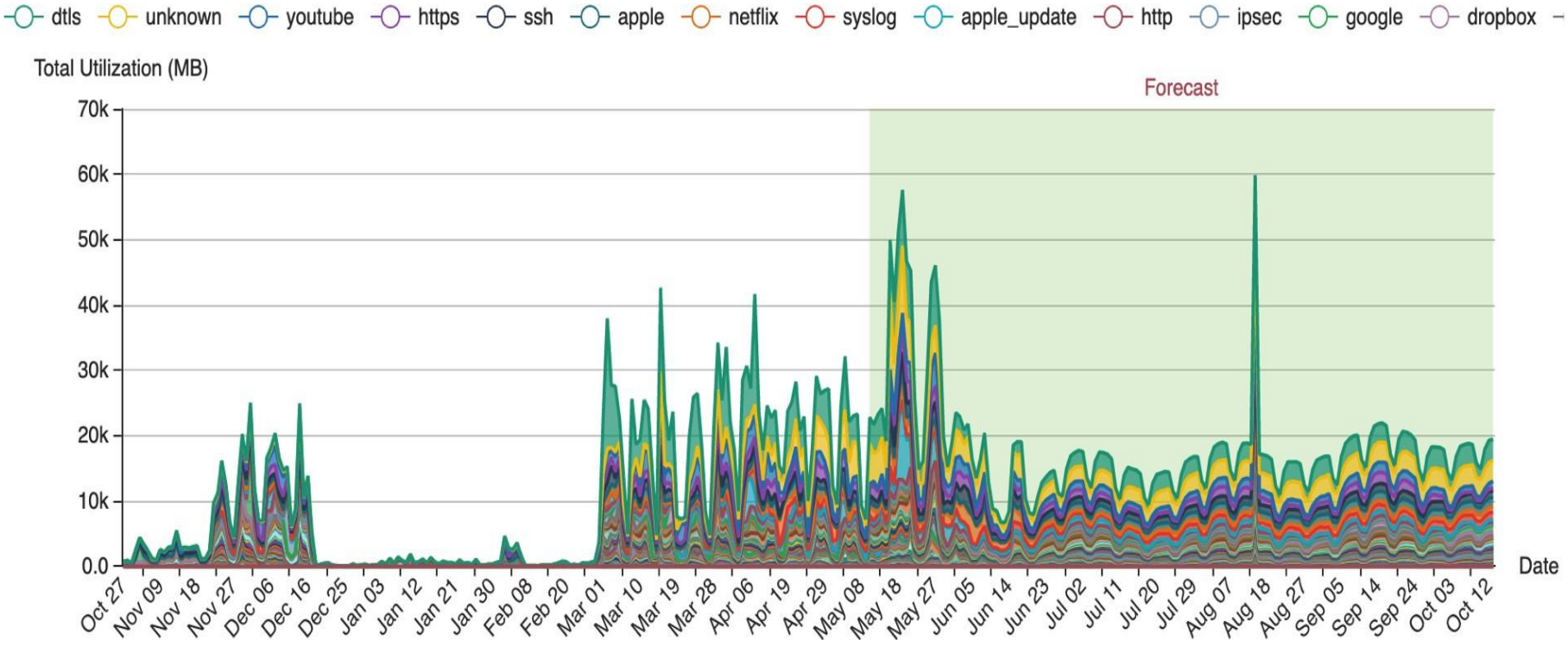
Cisco vManage Troubleshooting Simulate Flows



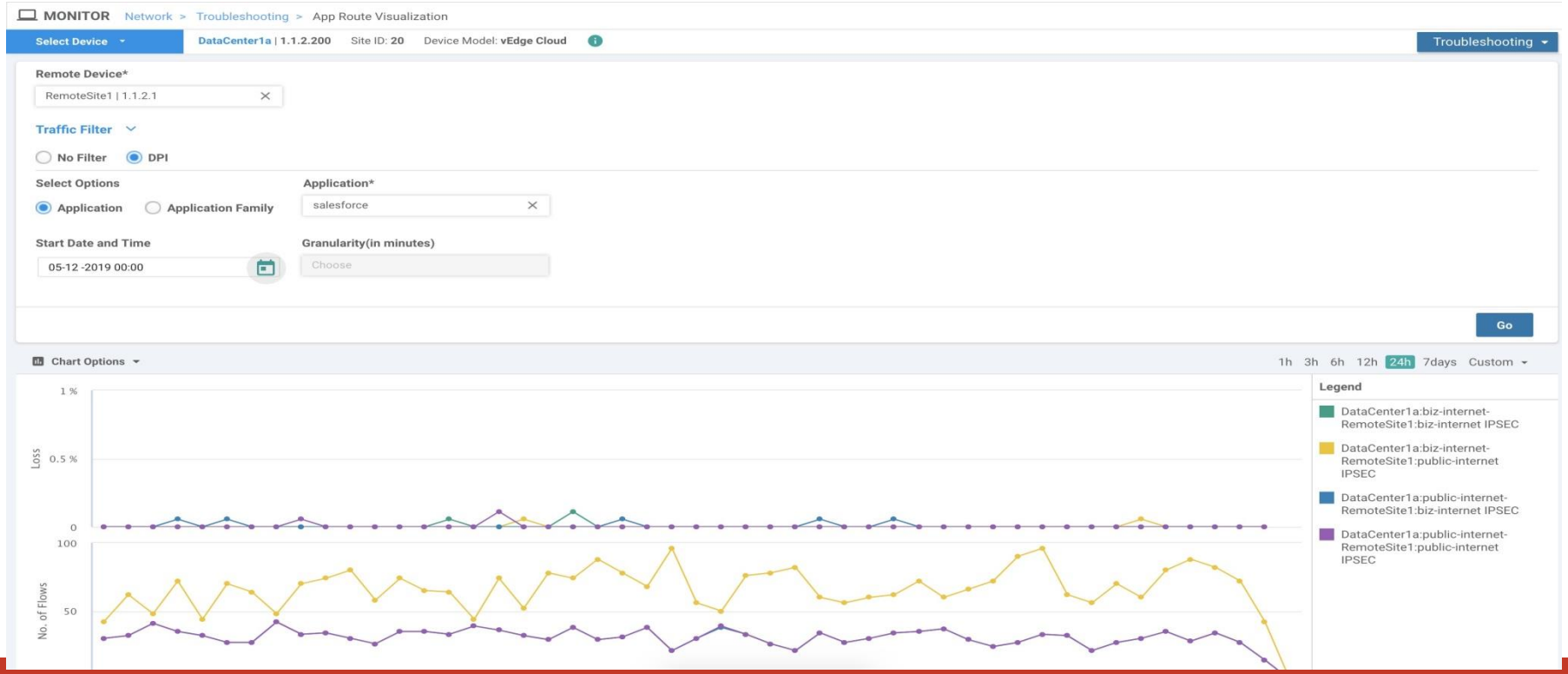
Cisco vAnalytics dashboard



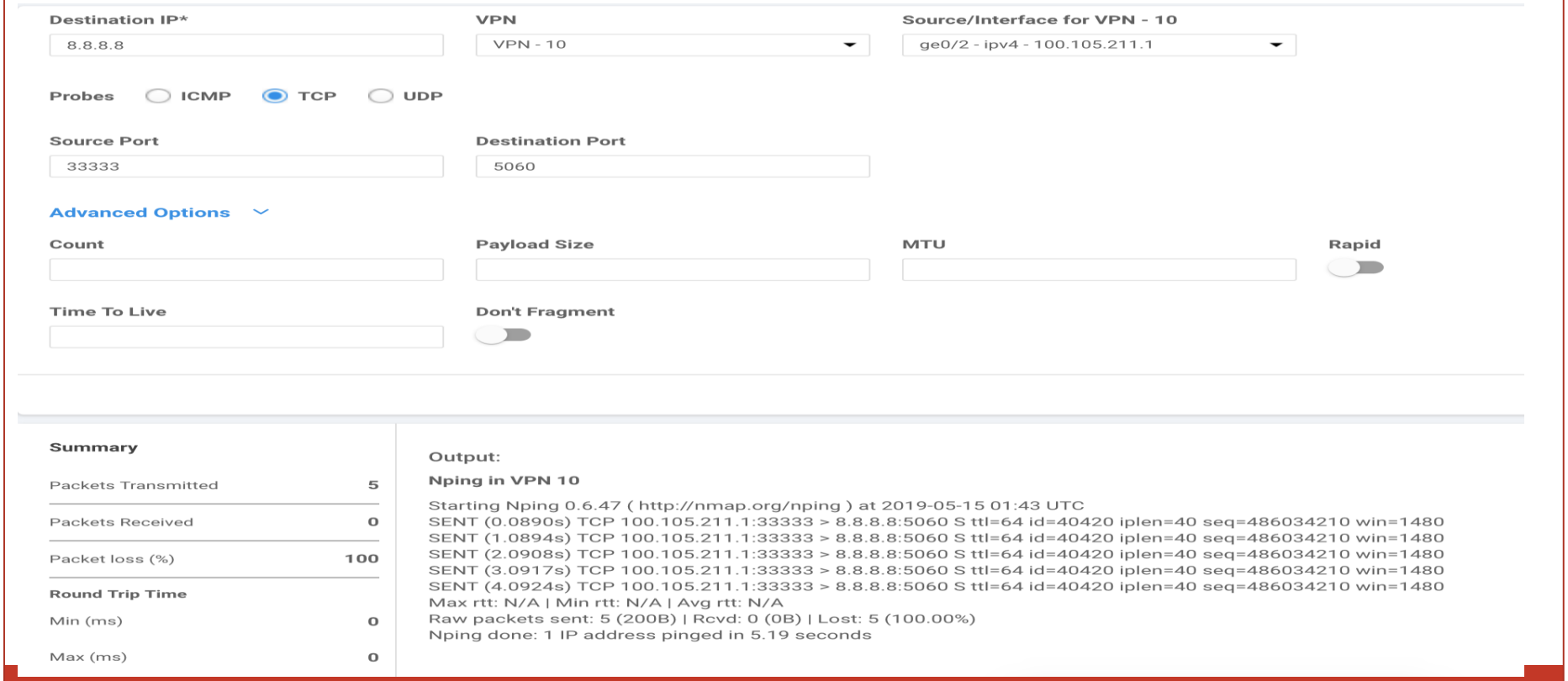
Cisco vAnalytics forecasting



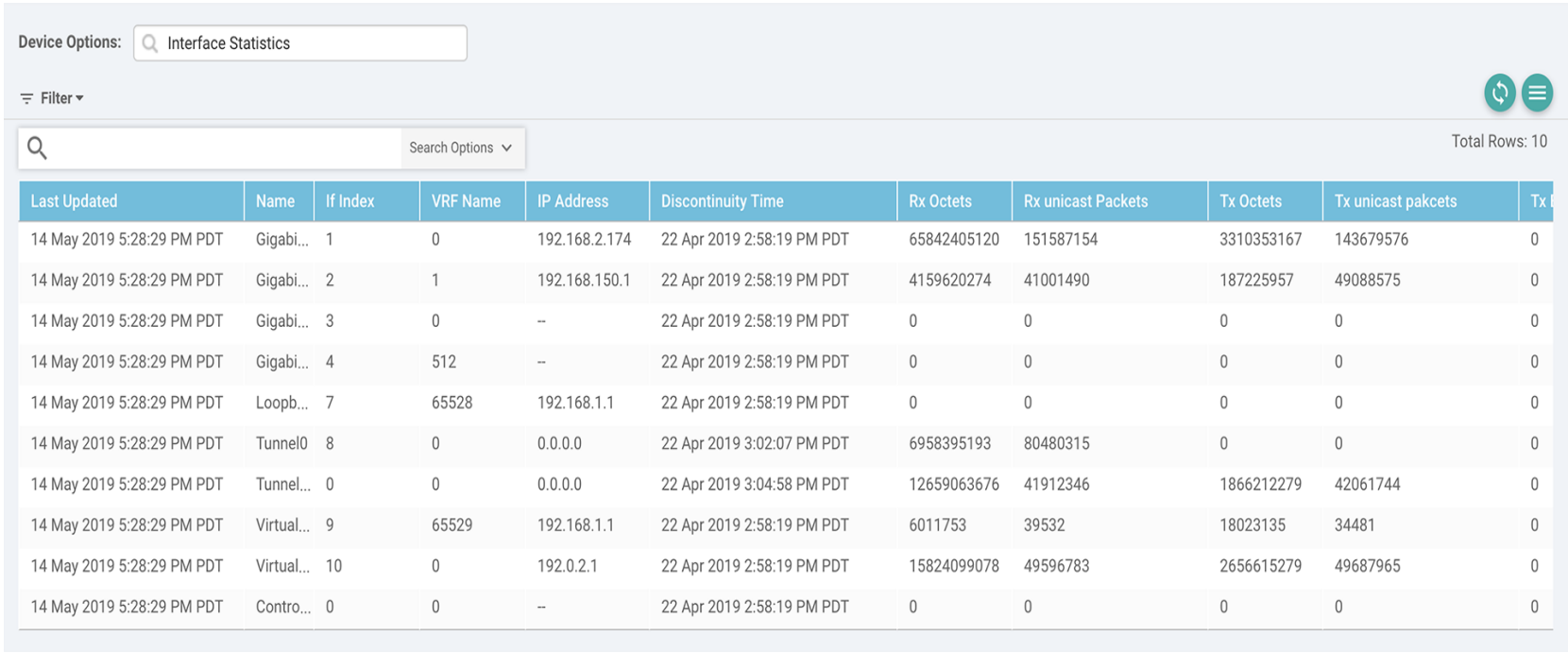
App-route visualization



vManage troubleshooting tools



Interface statistics



Last Updated	Name	If Index	VRF Name	IP Address	Discontinuity Time	Rx Octets	Rx unicast Packets	Tx Octets	Tx unicast pakcets	Tx
14 May 2019 5:28:29 PM PDT	Gigabi...	1	0	192.168.2.174	22 Apr 2019 2:58:19 PM PDT	65842405120	151587154	3310353167	143679576	0
14 May 2019 5:28:29 PM PDT	Gigabi...	2	1	192.168.150.1	22 Apr 2019 2:58:19 PM PDT	4159620274	41001490	187225957	49088575	0
14 May 2019 5:28:29 PM PDT	Gigabi...	3	0	--	22 Apr 2019 2:58:19 PM PDT	0	0	0	0	0
14 May 2019 5:28:29 PM PDT	Gigabi...	4	512	--	22 Apr 2019 2:58:19 PM PDT	0	0	0	0	0
14 May 2019 5:28:29 PM PDT	Loopb...	7	65528	192.168.1.1	22 Apr 2019 2:58:19 PM PDT	0	0	0	0	0
14 May 2019 5:28:29 PM PDT	Tunnel0	8	0	0.0.0.0	22 Apr 2019 3:02:07 PM PDT	6958395193	80480315	0	0	0
14 May 2019 5:28:29 PM PDT	Tunnel...	0	0	0.0.0.0	22 Apr 2019 3:04:58 PM PDT	12659063676	41912346	1866212279	42061744	0
14 May 2019 5:28:29 PM PDT	Virtual...	9	65529	192.168.1.1	22 Apr 2019 2:58:19 PM PDT	6011753	39532	18023135	34481	0
14 May 2019 5:28:29 PM PDT	Virtual...	10	0	192.0.2.1	22 Apr 2019 2:58:19 PM PDT	15824099078	49596783	2656615279	49687965	0
14 May 2019 5:28:29 PM PDT	Contro...	0	0	--	22 Apr 2019 2:58:19 PM PDT	0	0	0	0	0

vEdge Routers for ZTP & Lab

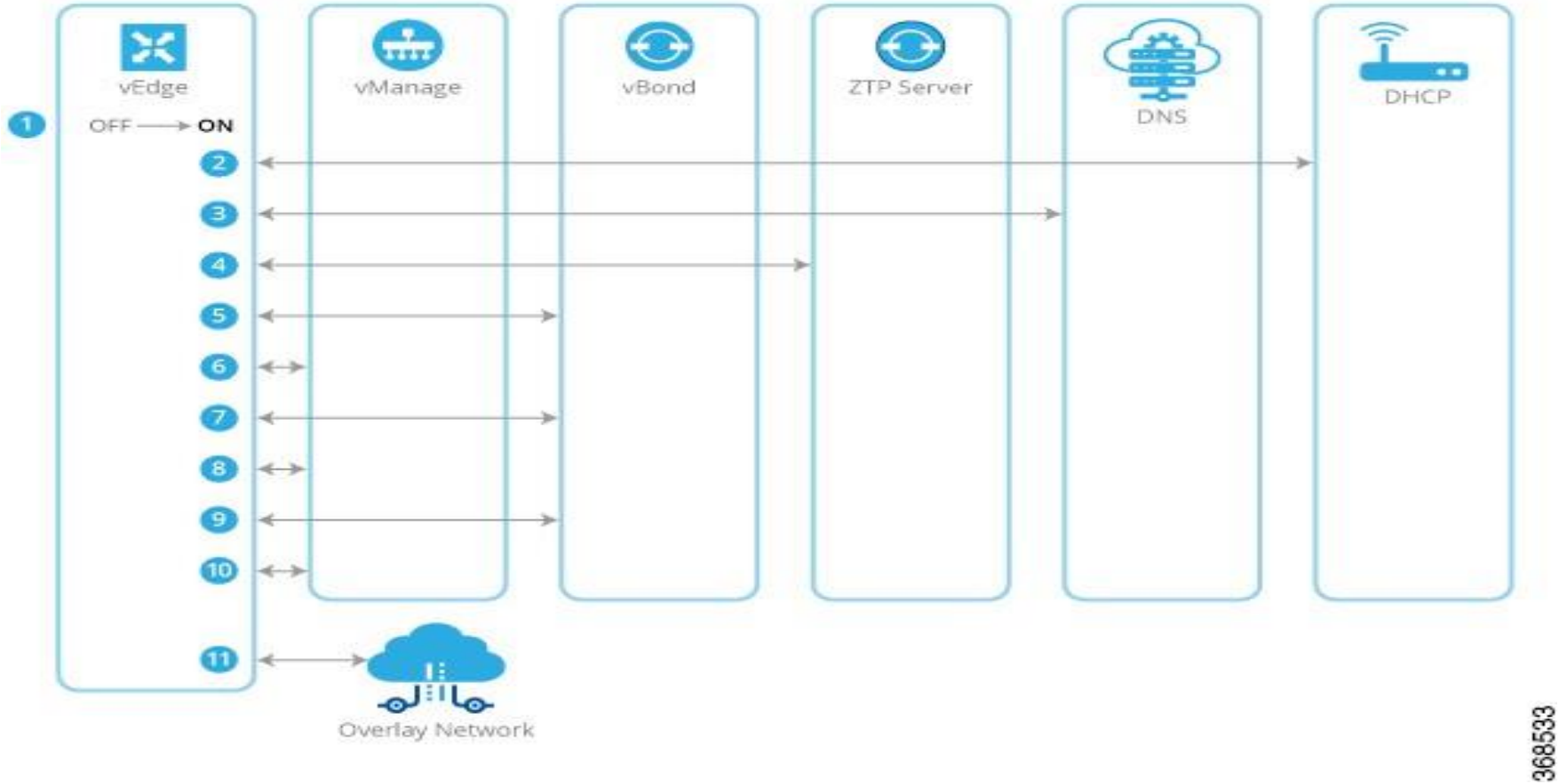
- Followed by Lab

Prepare vEdge Routers for ZTP

For the ZTP process to work:

- The edge or gateway router at the site where the hardware vEdge router is located must be able to reach public DNS servers. It is recommended that they be configured to reach the Google public DNS servers 8.8.8.8 and 8.8.4.4.
- The edge or gateway router at the site must be able to reach ztp.viptela.com.
- A network cable must be plugged into the interface that the hardware router uses for ZTP. These interfaces are:
  - For vEdge 1000 routers: ge0/0
  - For vEdge 2000 routers: ge2/0
  - For vEdge 100 series routers: ge0/4

The ZTP process occurs in the following sequence:


vEdge
vManage
vBond
ZTP Server
DNS
DHCP
1
OFF → ON
2
3
4
5
6
7
8
9
10
11
Overlay Network
368533

1. The hardware vEdge router powers up.
2. The router attempts to contact a DHCP server, sending a DHCP discovery message.
   a. If a DHCP server is present in the network, the router receives a DHCP offer message that contains the IP address of its ZTP interface. Then, the ZTP process continues with Step 3.
   b. If no DHCP server is present and so the router does not receive a DHCP offer, the router initiates an automatic IP address detection process (sometimes called auto-IP). This process examines the ARP packets on the subnetwork and, from these packets, it infers the IP address of the ZTP interface. Then, the ZTP process continues with Step 3.
3. 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

4. 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.

5. 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.

6. 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.

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

8. 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.
9. After the reboot, the router re-establishes a connection to the vBond orchestrator, which again verifies the router.
10. 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.)
11. The router joins the organization's overlay network.

Important

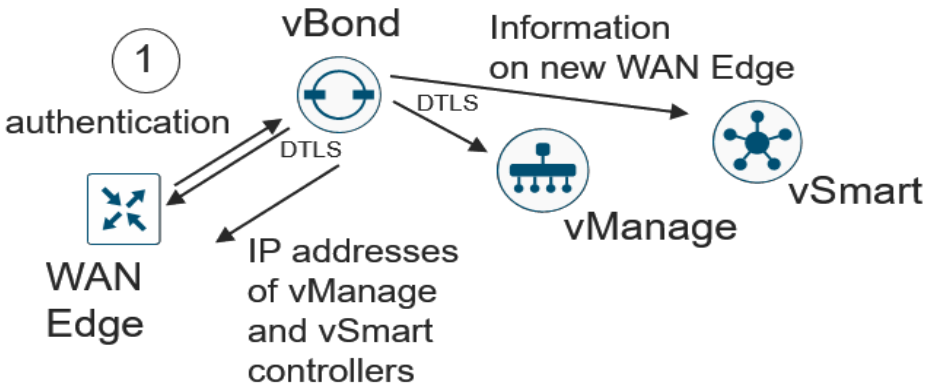
For the ZTP process to succeed, the vManage NMS must contain a device configuration template for the vEdge router. If the NMS has no template, the ZTP process fails.

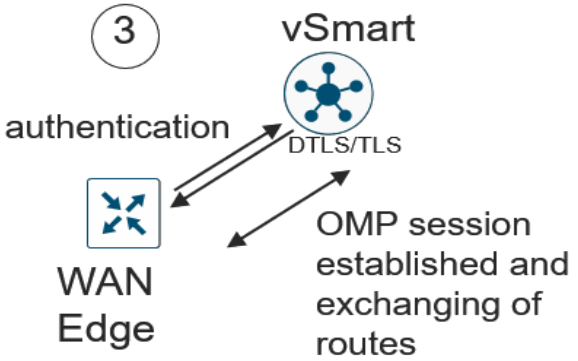
Cisco SD-WAN: WAN Edge Onboarding

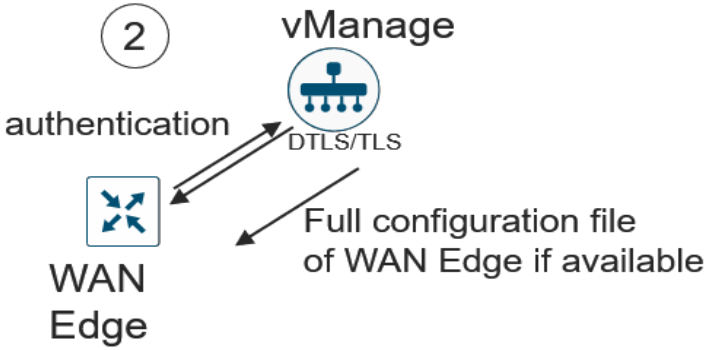
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sd-wan-wan-edge-onboarding-deploy-guide-2020jan.pdf

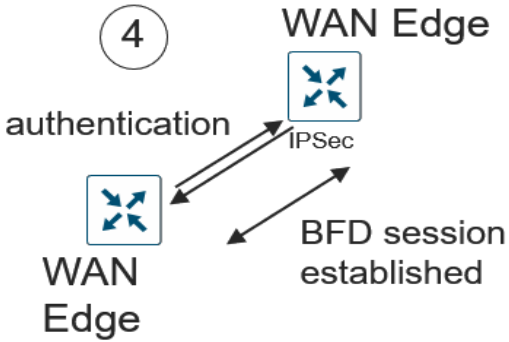
https://www.cisco.com/c/dam/en_us/services/downloads/SD-WAN_pnp_support_guide.pdf

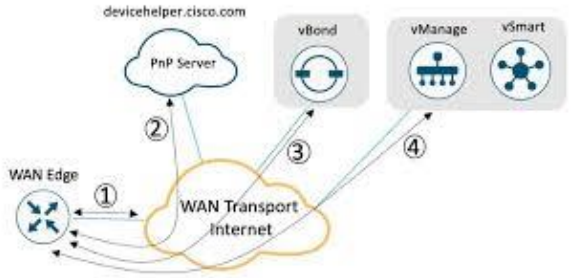
WAN Edge onboarding steps

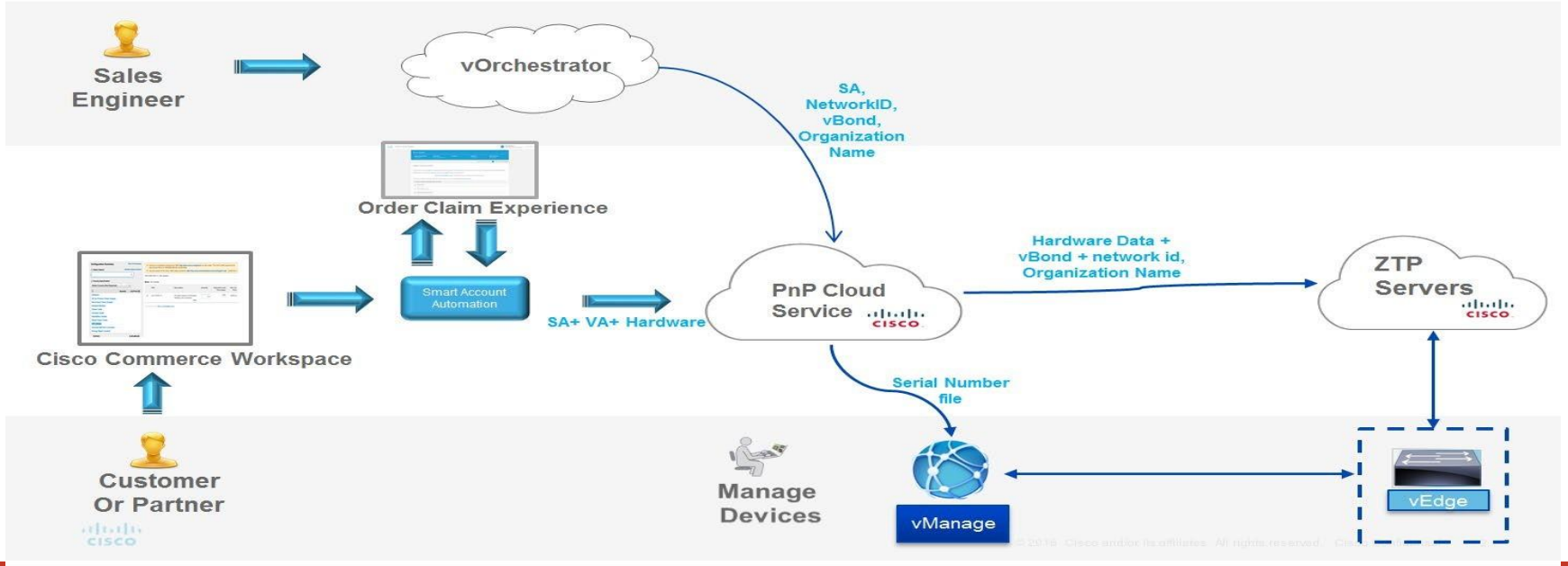




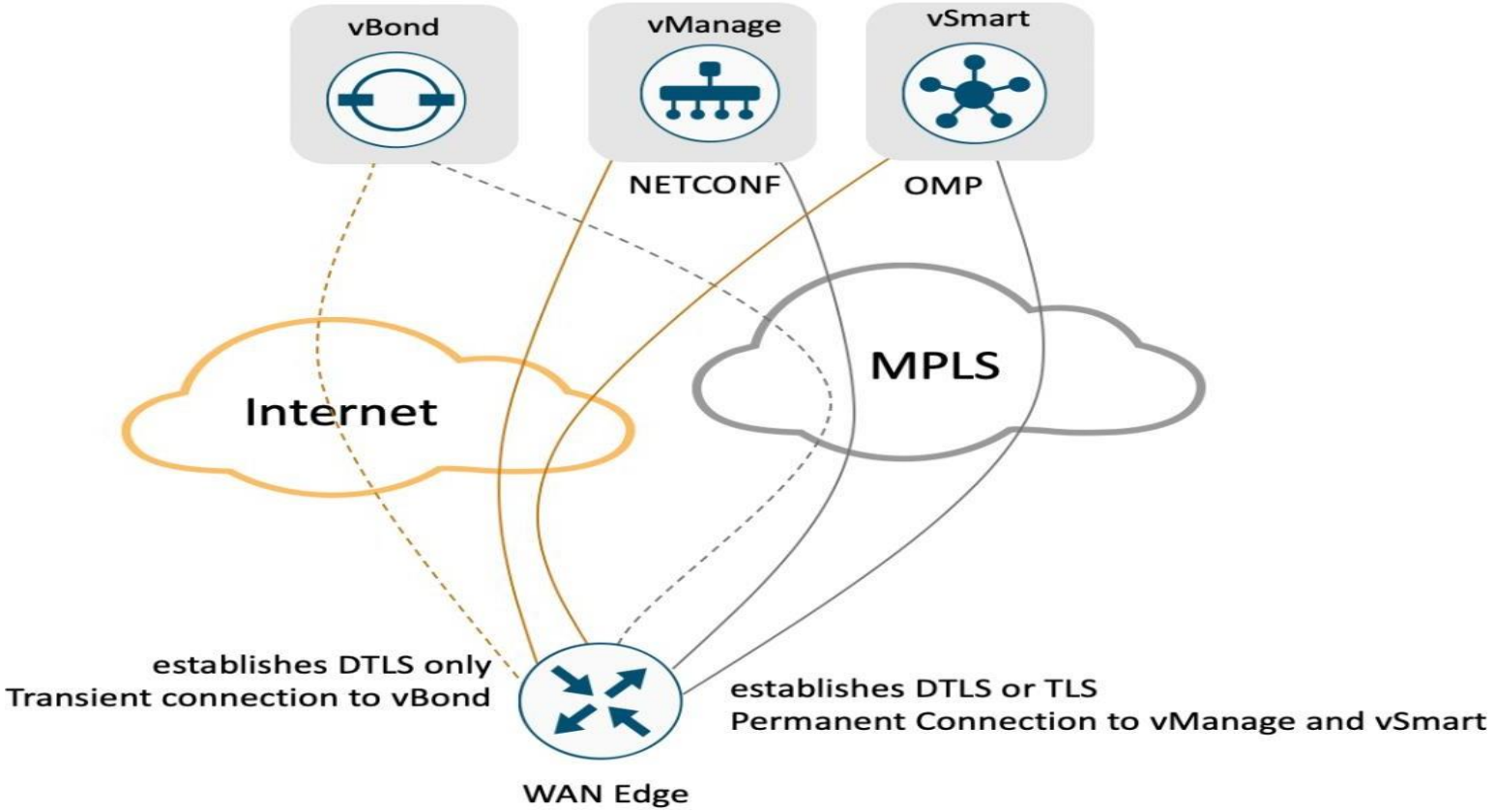





devicehelper.cisco.com
PnP Server
vBond
vManage
vSmart
WAN Edge
WAN Transport
Internet
1
2
3
4


Sales Engineer
vOrchestrator
SA, NetworkID, vBond, Organization Name
Order Claim Experience
Cisco Commerce Workspace
Smart Account Automation
SA+ VA+ Hardware
PnP Cloud Service
Hardware Data + vBond + network id, Organization Name
ZTP Servers
Serial Number file
Customer Or Partner
Manage Devices
vManage
vEdge

WAN Edge control connections to different SD-WAN controllers

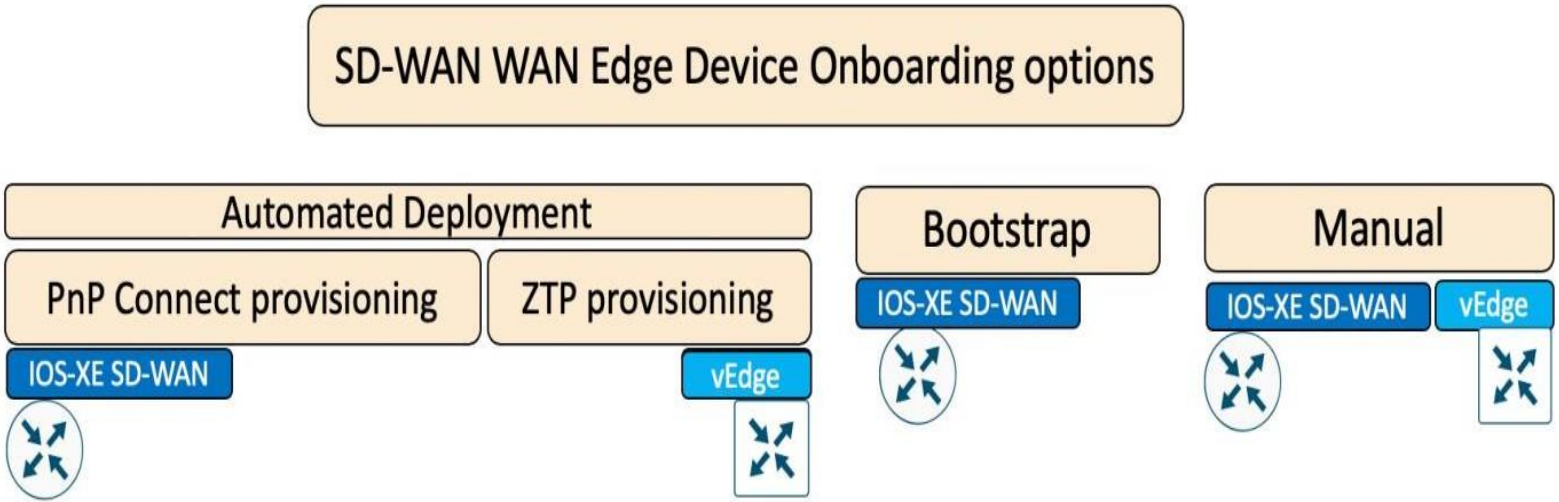


Design

WAN Edge Onboarding options

There are several options available to securely onboard SD-WAN Edge devices.

WAN Edge onboarding options overview

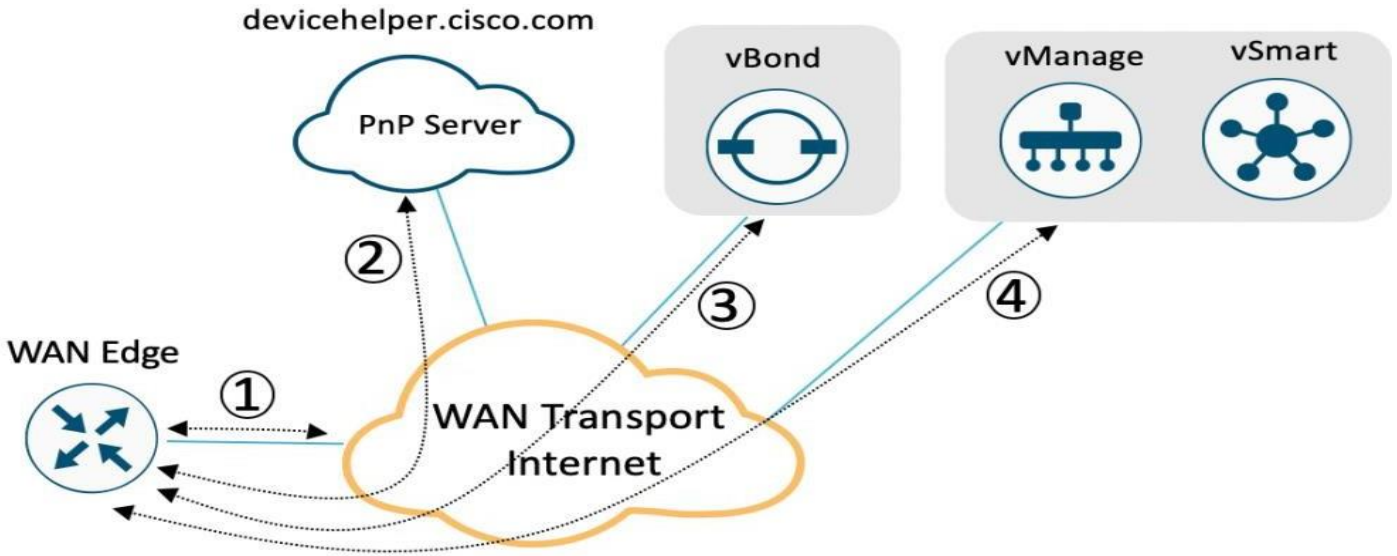


IOS-XE SD-WAN WAN Edge onboarding options

Platform	Plug-and-Play (PnP)	Bootstrap	Manual
ASR1K	✓	✓	✓
ASR1002-X	×	✓	×
ISR4K	✓	✓	✓
ISR1K	✓	✓	✓

vEdge WAN Edge onboarding options

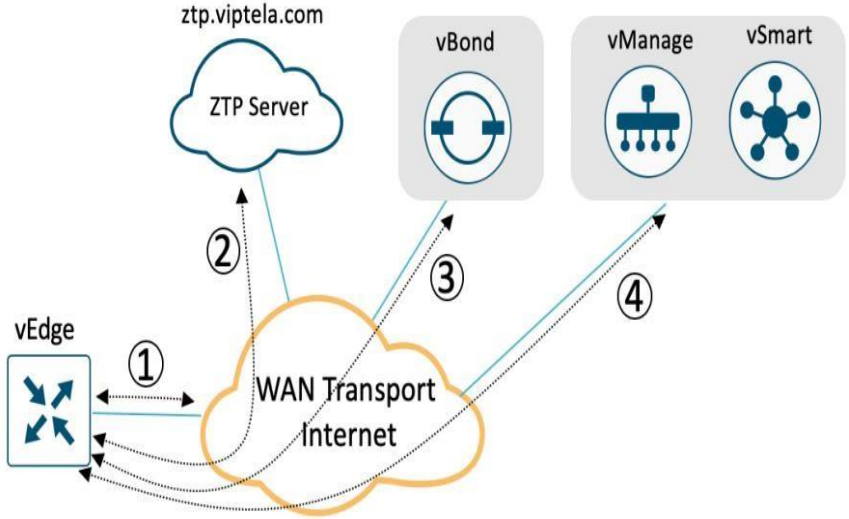
Platform	Zero-Touch Provisioning (ZTP)	Manual
vEdge 100	✓	✓
vEdge 1000	✓	✓
vEdge 2000	✓	✓
vEdge 5000	×	✓
vEdge Cloud		



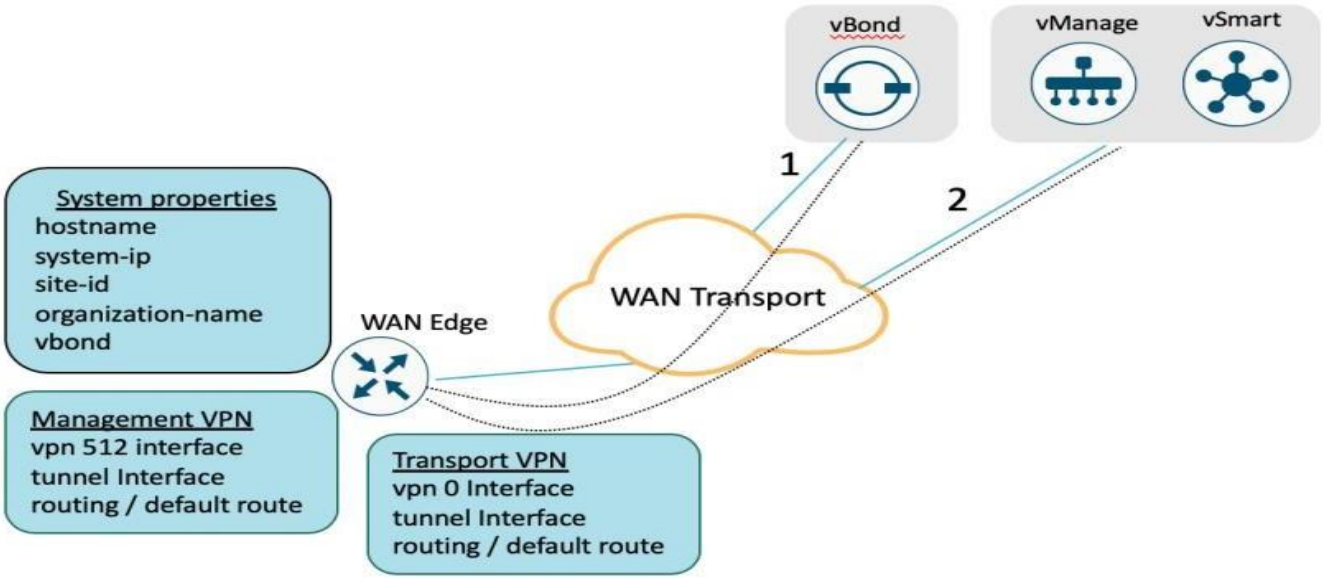
Platform	Plug-and-Play	Interface
ASR1K	✓	GigabitEthernet (routed interface)
ASR1002-X	✗	NA
ISR1K	✓	GigabitEthernet (routed interface) Cellular
ISR4K	✓	GigabitEthernet (routed interface) Cellular

vEdge onboarding – ZTP process

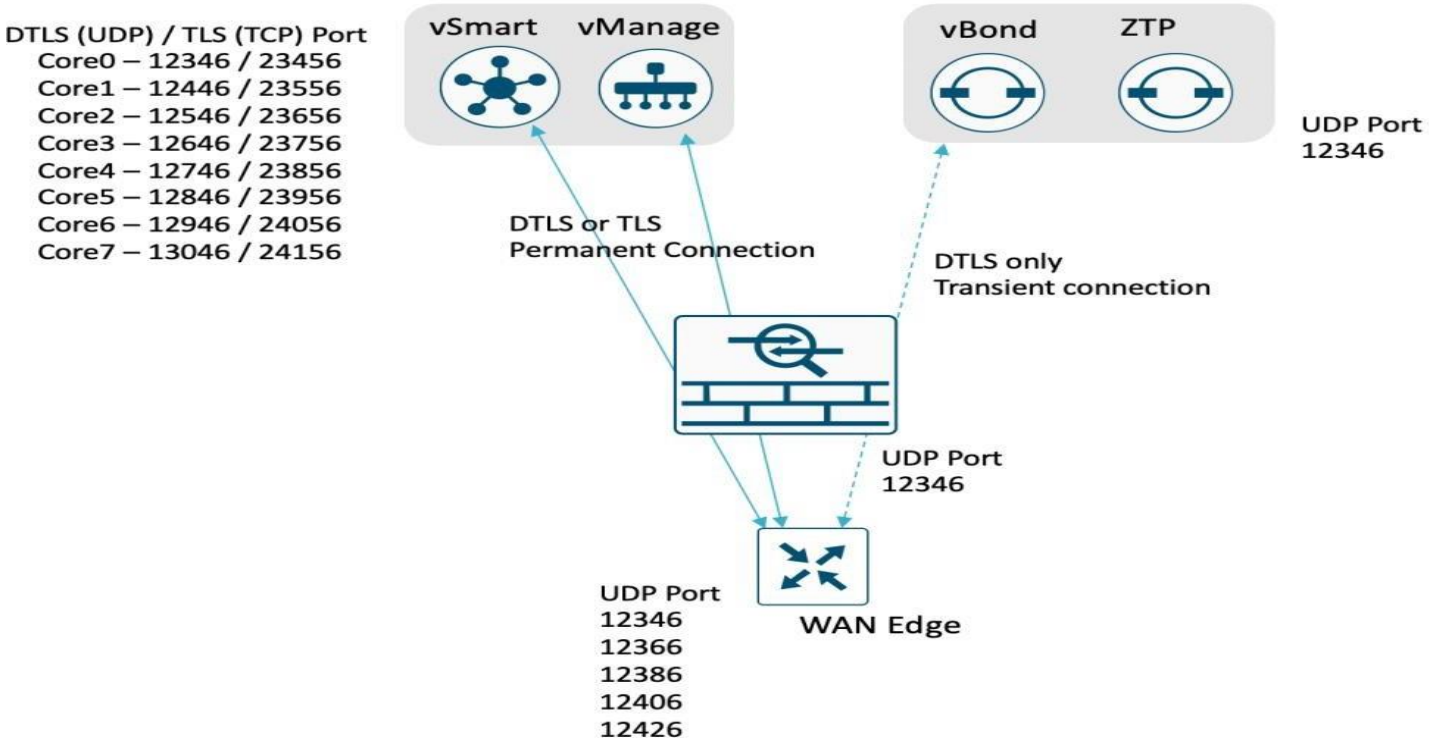
Platform	ZTP	Interface
vEdge 100, 100b	✓	ge0/4
vEdge 100m, 100wm	✓	ge0/4 Cellular0
vEdge 1000	✓	ge0/0
vEdge 2000	✓	ge2/0
vEdge 5000	✓ ×	ge0/0 (first port on the first available network slot)
vEdge cloud		NA



WAN Edge onboarding – Manual process



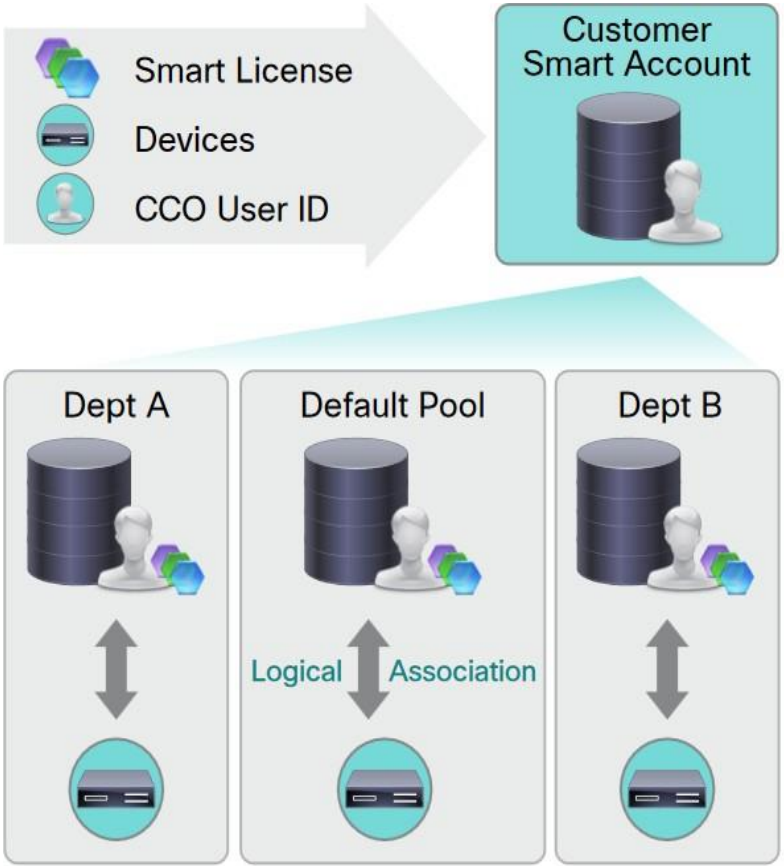
WAN Edge firewall ports



The following are miscellaneous show commands for reference to verify control connections on the WAN Edge device:

vEdge platform	IOS-XE SD-WAN platform
show control connections	**show sdwan control connections**
show control connections-history	**show sdwan control connection-history**
show control connections-info	**show sdwan control connection-info**
show control local-properties	**show sdwan control local-properties**
show control statistics	**show sdwan control statistics**
show control summary	**show sdwan control summary**
show control valid-vsmarts	**show sdwan control valid-vsmarts**
show control valid-vmanage-id	**show sdwan control valid-vmanage-id**

Cisco Plug and Play



Virtual Accounts

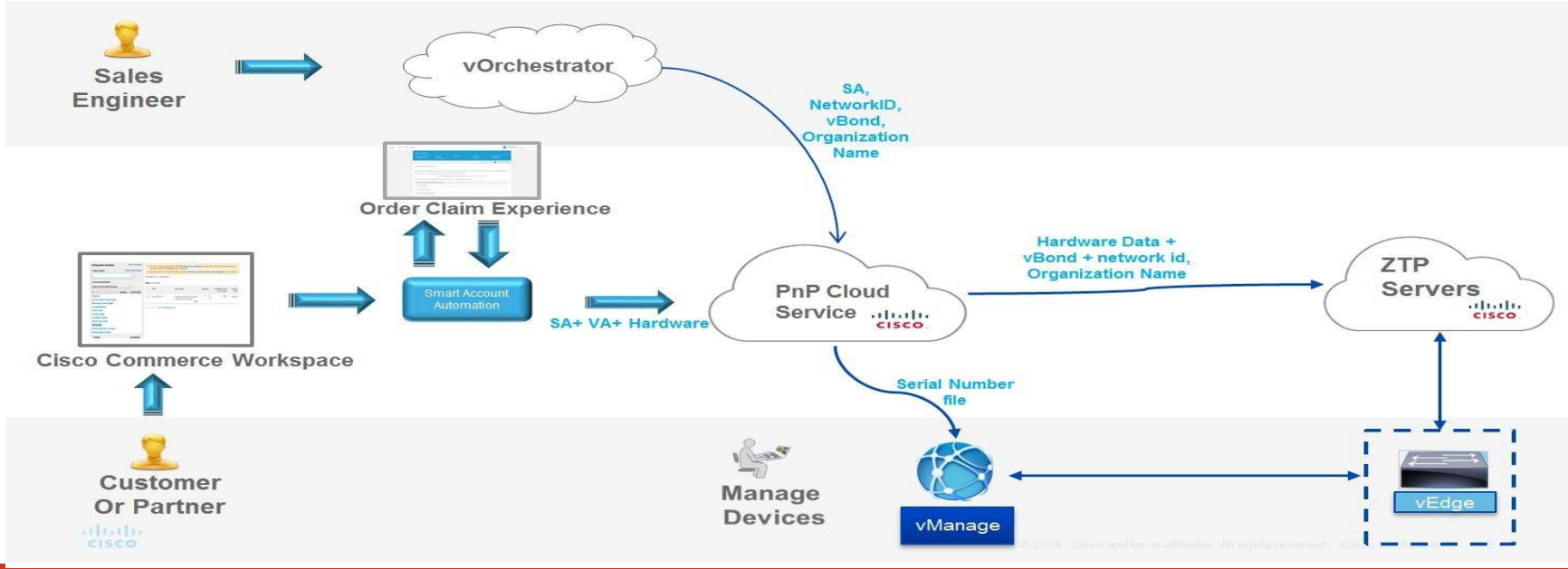
- A customer defined construct to reflect company organization, geography, budgeting, or other structure.
- Created and maintained by the customer on the Cisco Smart Software Manager with full visibility to company assets.
- Enable Delegated Authority and Differential Access.
- Flexible, allowing licenses and products to be shared between products (without contacting Cisco TAC!)

Licenses and devices are always explicitly moved, enabled or disabled by the customer administrator.

For on-premises deployment

The customer or sales engineer who is helping with the customer's deployment would need to enter the vBond profile information into the Plug-and-Play portal, so that the controller information can be passed to zProv.

Figure 1. PnP workflow



Edge Configuration

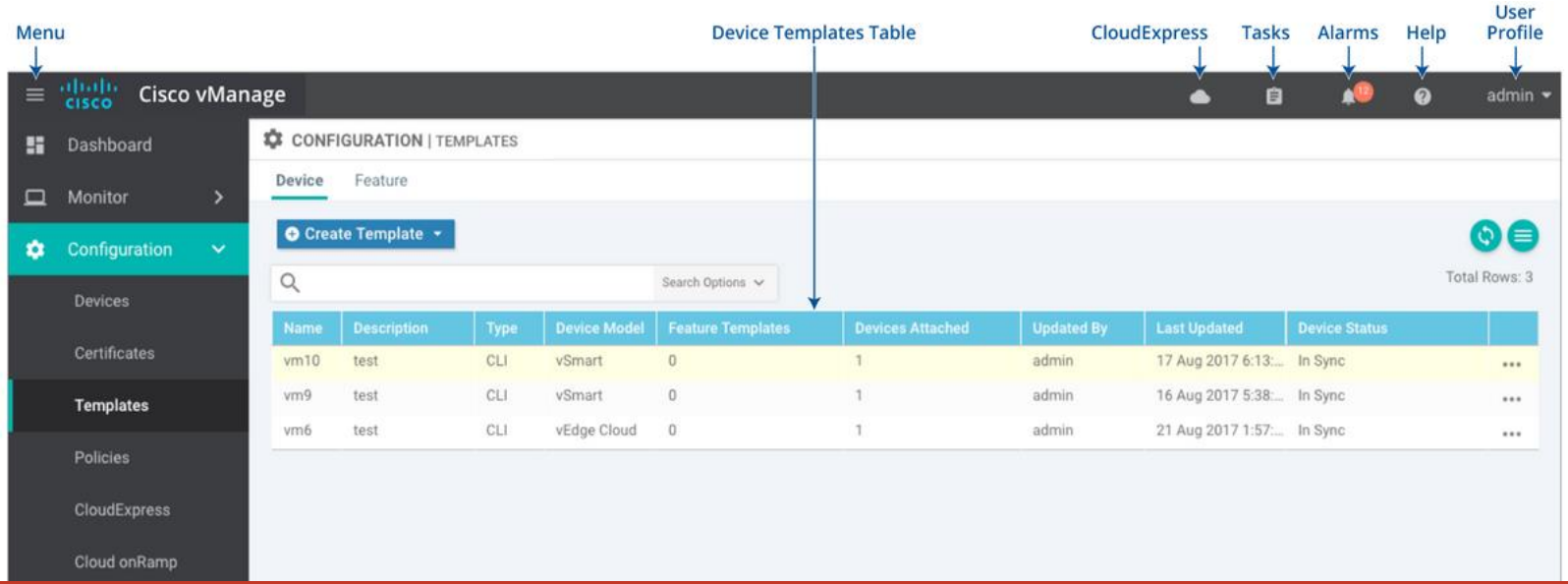
- 3.1 Describe WAN Edge deployment
- 3.1.a On-boarding
- 3.1.b Orchestration with zero-touch provisioning/plug-and-play
- 3.1.c Single/multi data center/regional hub deployments

3.1.c Single/multi data center/regional hub deployments

Templates

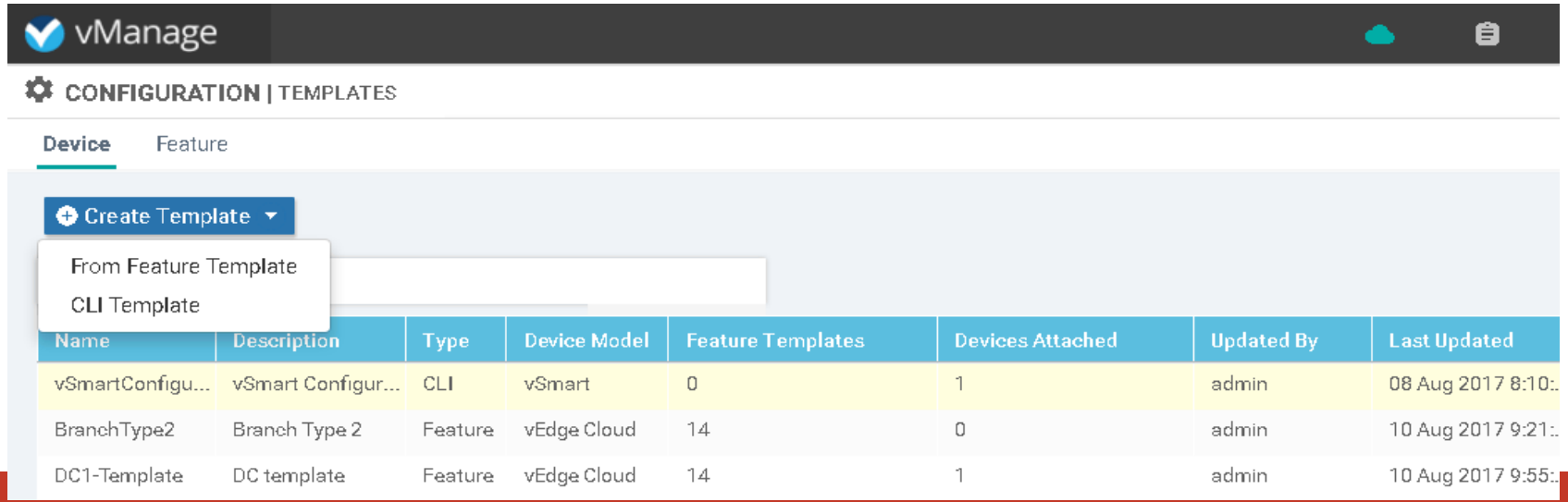
Use the Templates screen to configure all Viptela devices in the overlay network that are managed by the vManage NMS. To do so:

1. Create a device template.
2. Attach Viptela devices to the device template.

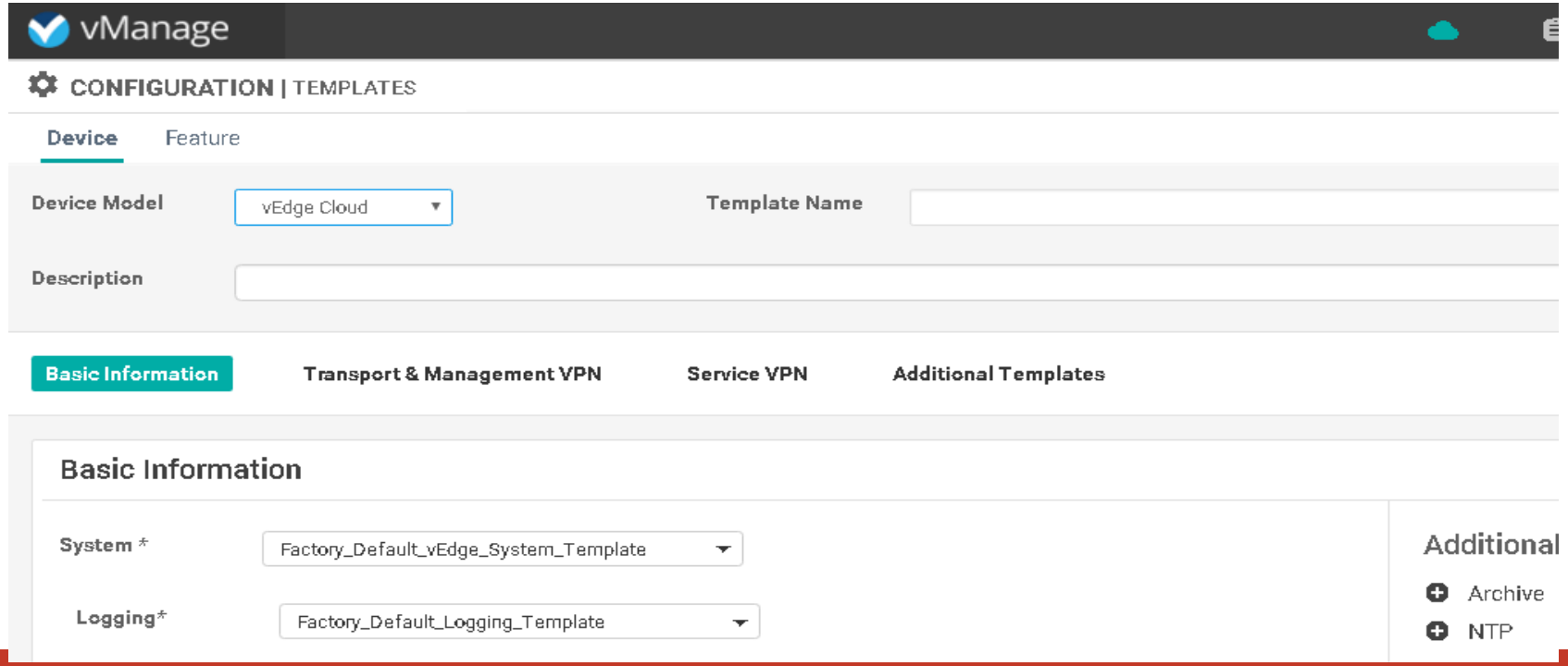


Create a Device Template

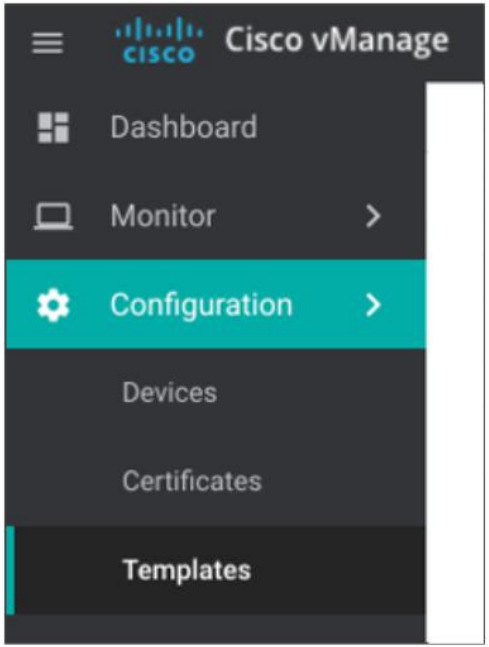
Device templates define a device's complete operational configuration. A device template consists of a number of feature templates. Each feature template defines the configuration for a particular Viptela software feature. Some feature templates are mandatory, indicated with an asterisk (*), and some are optional. Each mandatory feature template, and some of the optional ones too, have a factory-default template. For software features that have a factory-default template, you can use either the factory-default template (named Factory_Default_*feature-name*_Template) or you can create a custom feature template.



Create a Device Template from Feature Templates



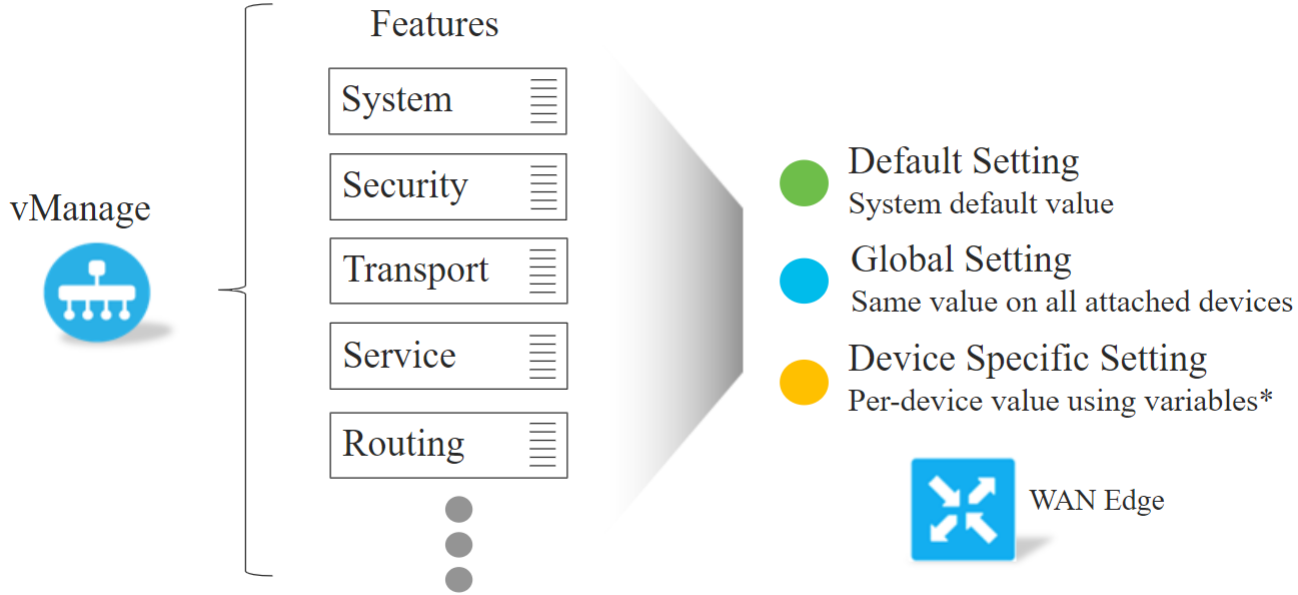
What are Configuration Templates



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 Configuration Templates Structure



* Value is specified at the time of template attachment

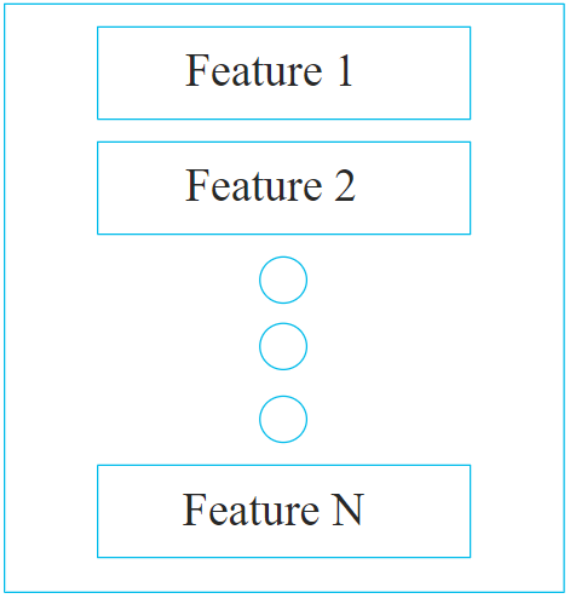
Types of Device Configuration Templates

CLI Template

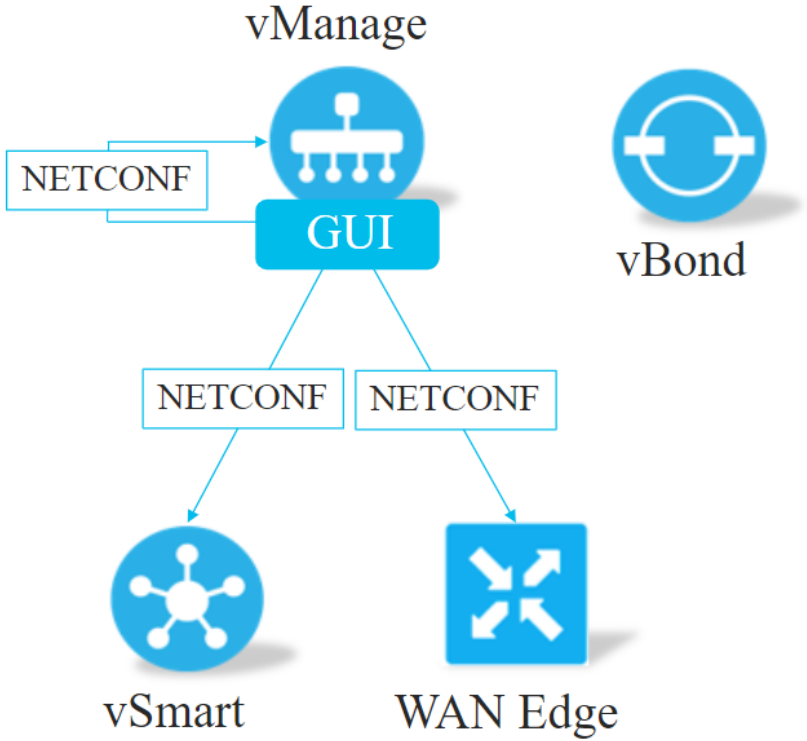
```
omp
 no shutdown
 graceful-restart
 advertise connected
 advertise static
!
security
 ipsec
  authentication-type sha1-hmac ah-sha1-hmac
 !
!
vpn 0
 dns 8.8.4.4 secondary
 dns 8.8.8.8 primary
 interface ge0/0
  ip dhcp-client
  !
  tunnel-interface
   encapsulation ipsec
   color public-internet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

Same Capabilities

Feature Template

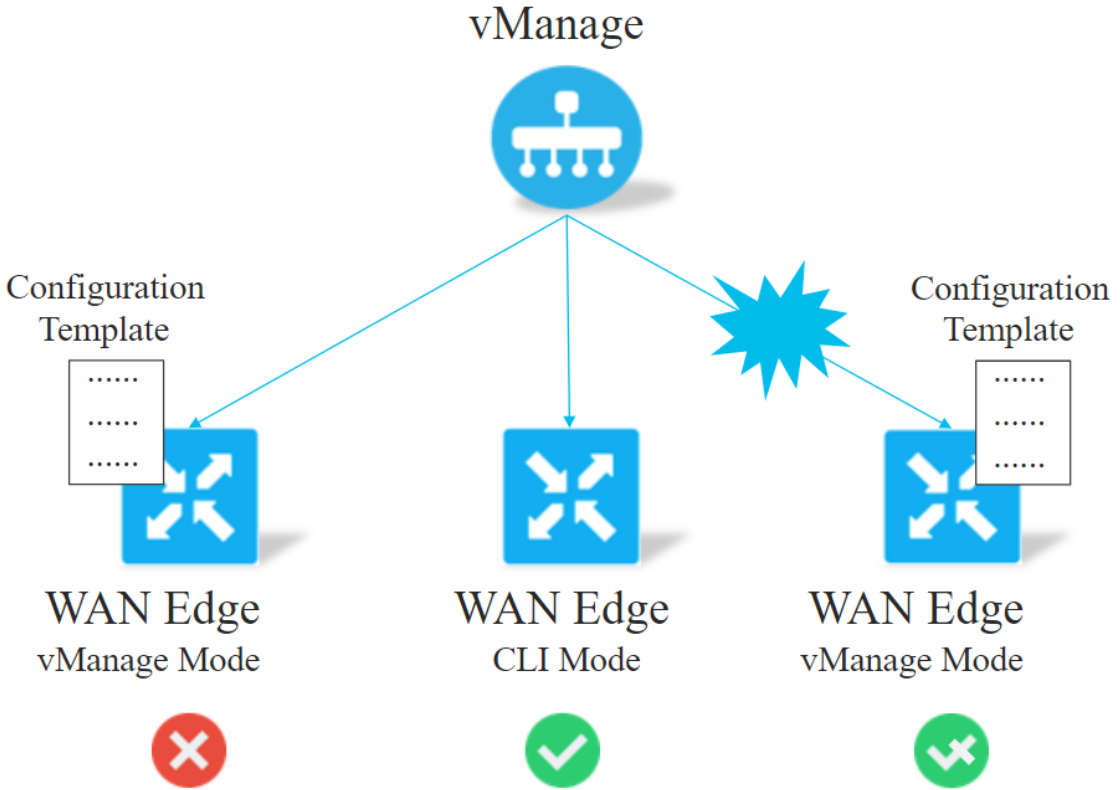


Device Configuration Template Distribution



- 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



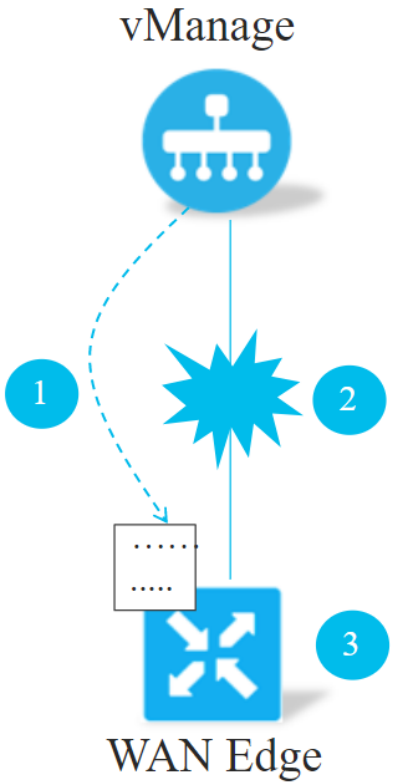
Local Changes Disallowed

Local Changes Allowed

Local Changes Allowed

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

Operational Enhancement: Configuration Rollback

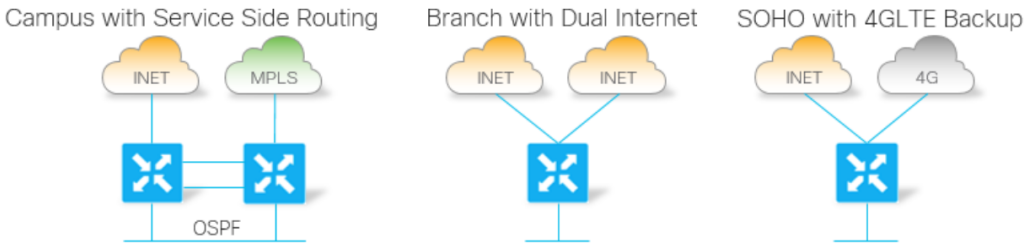


- (1) Configuration template is deployed from vManage
- (2) Control connection between WAN Edge and vManage goes down
- (3) WAN Edge rolls back most recent configuration change and restores contol connection between WAN Edge and vManage
  - 5 min interval by default

Device Template Planning & CLI Template

Typical Device Configuration Template Planning

- Classify sites into categories
- Define configuration features for each category. Examples:



- Use variables for per-device specific values, e.g. geo-coordinates, interface IP addresses, default route next-hop etc…
- Plan out values for key system variables: Hostname, System IP, Site-ID

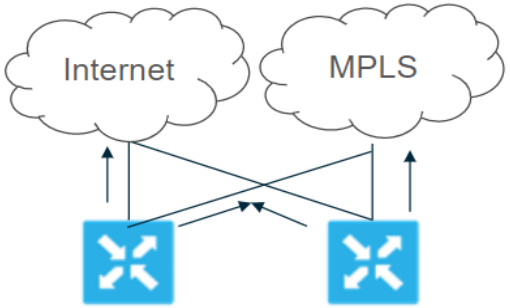
Design

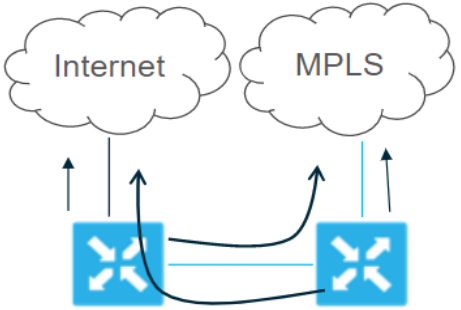
Data Center Designs

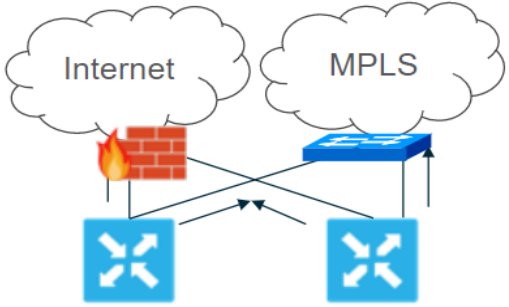
(Transport Variants)

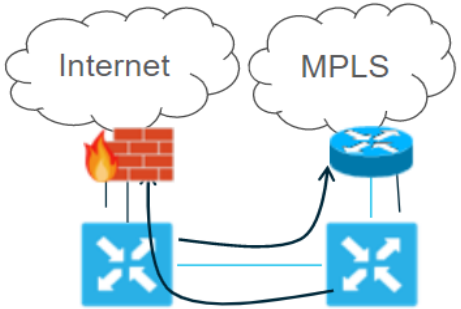
Up to 7 Transport Interfaces

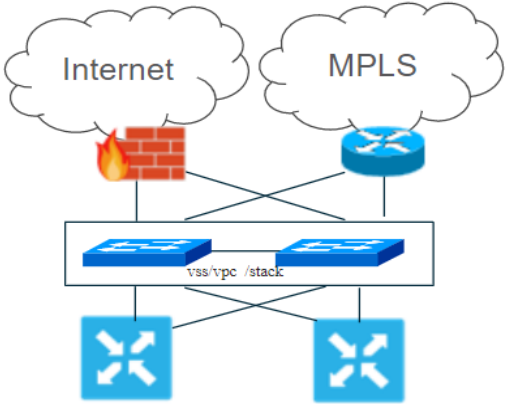
1 2 3 4 5 6 7







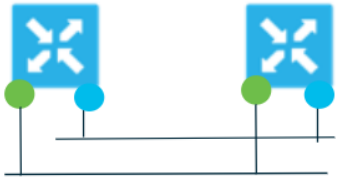




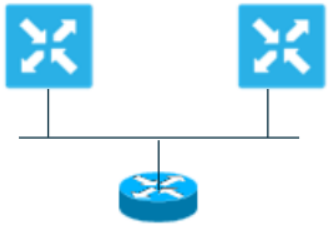
Data Center Designs

(Service LAN Variants)

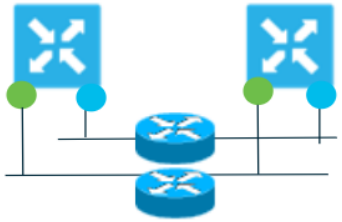
L2 VRRP



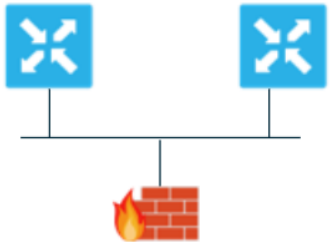
L2 VRRP/Multi-VPN



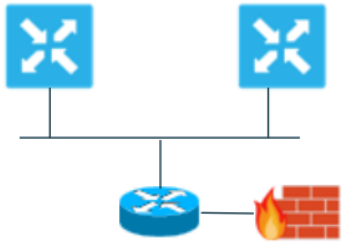
L3 static/ospf/bg p



L3 Multi-VPN static/ospf/bg p

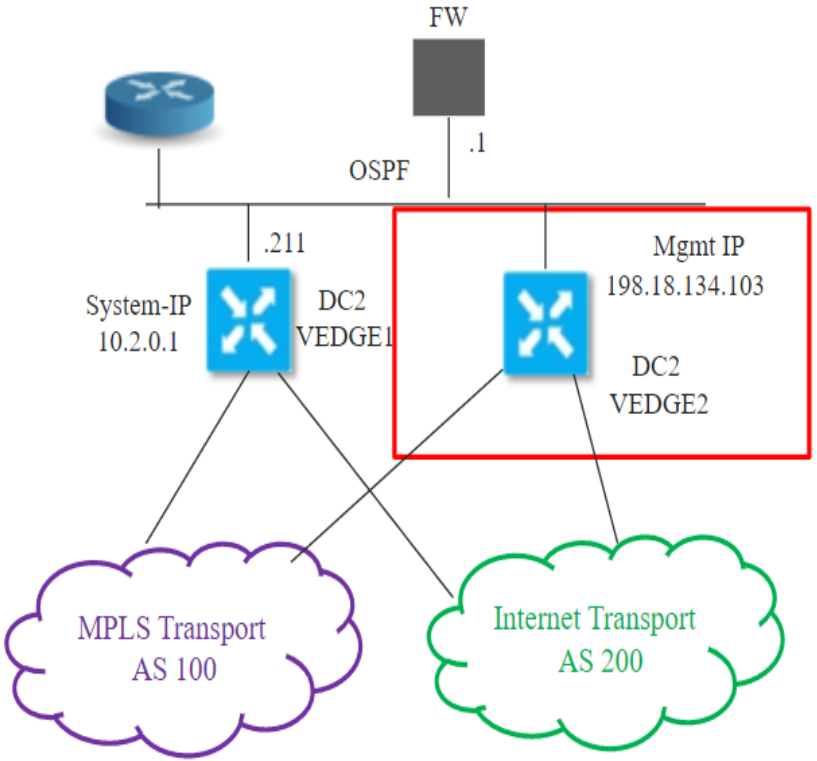


L3 Service Insertion Direct

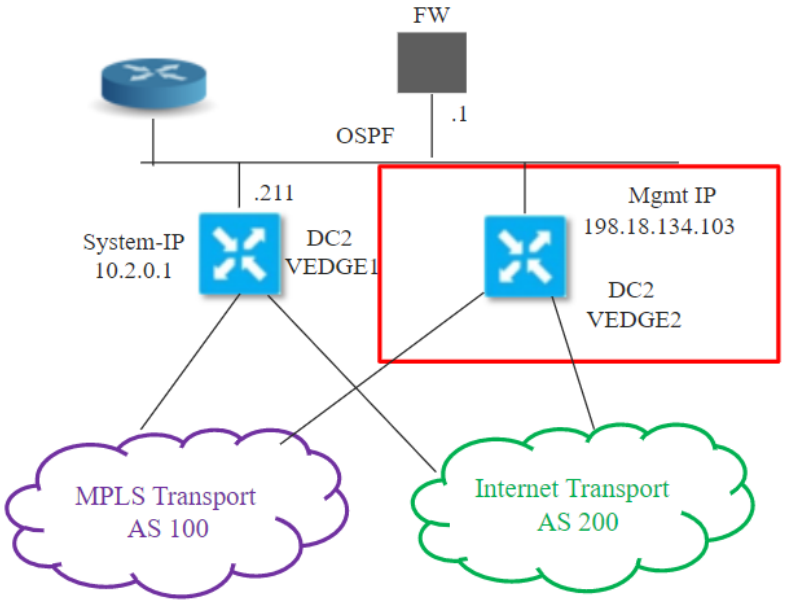


L3 Service Insertion multihop

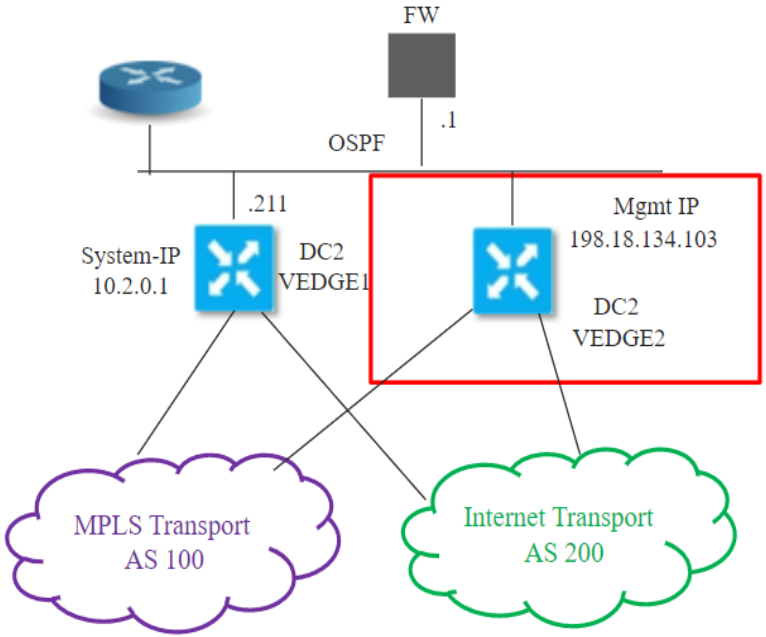
DC Template Planning



DC Specific Custom Feature Templates	
Feature template Name	**Customization**
DC-VPN-0	FW Service Insertion (announce service into VPN0)
InternetTLOC	Static IP, color biz-internet, ge0/2
VPN10withService	FW IP for Service Insertion
VPN10-Interface-Template	static IP, no QoS Marking, ge0/0
OSPF-DC-with-filtering	OSPF with Route-Filter to deny remote routes from LAN
VPN20-VRRP	VPN20, VRRP enabled for HA



Custom Feature Templates common to all Sites in dCloud network	
Feature Template Name	**Customization**
System-dCloud-Feature	Site ID variable, system IP variable, hostname variable, GPS variable,
OMP-dCloud-Feature	ECMP Limit 8,
BFD-dCloud-Feature	Poll Interval
MPLS-TLOC-Interface	Static IP, color mpls, interface ge0/1
VPN512-dCloud-Feature	VPN 512
VPN512-Interface	Eth0, Static IP variable
VPN-20-Template	VPN 20
dCloud-Banner	Custom Banner
LocalizedPolicyBaseline	QoS, OSPF filtering, application visibility
Snmp-dCloud-feature	SNMP Community, View, Trap Server



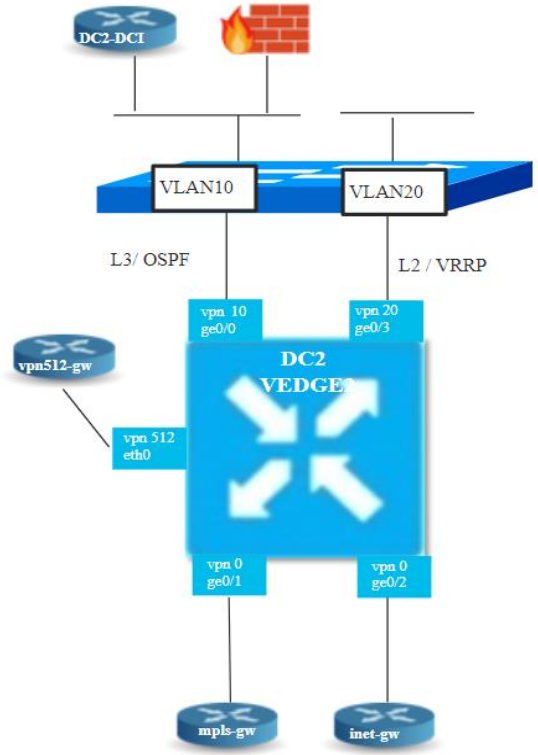
Factory Default Feature Templates
Logging
AAA
Security

Unused Feature Templates
Archive
Bridge
DHCP
IGMP
Multicast
NTP
PIM
VPN Interface Bridge, GRE, IPSec, NATPoolm PPP, PPP Ethernet

DC2-vEdge2 Template variables

System Variables	
Hostname	DC2-VEDGE2
GPS latitude	41.87
GPS longitude	-87.62
System IP	10.2.0.2
Site ID	200

Management VPN (VPN512) Variables	
eth0 IP Address	198.18.134.103/18
vpn512-GW-IP	198.18.128.1



Transport VPN (VPN0) Variables	
ge0/1 interface IP address (MPLS transport)	172.16.22.2/30
MPLS GW IP	172.16.22.1
ge0/2 interface IP address (INET transport)	172.16.23.2/30
INET GW IP	172.16.23.1

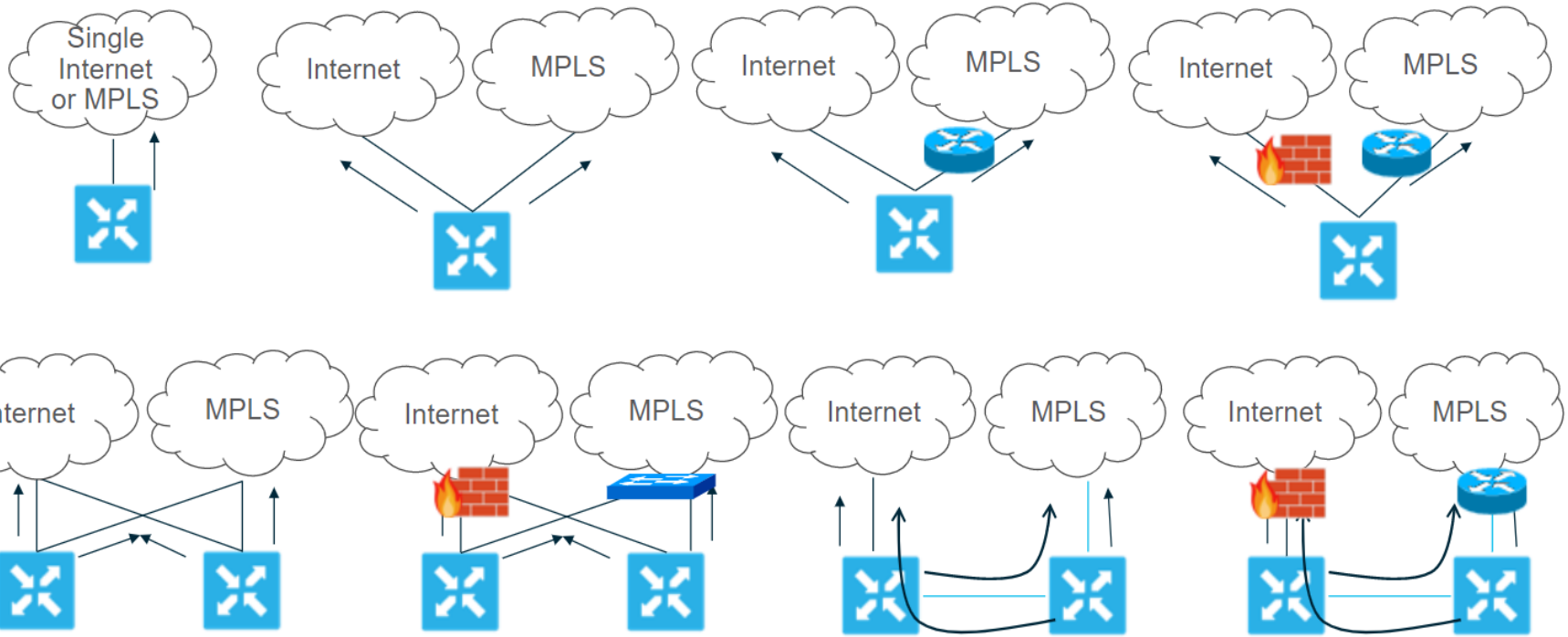
Service VPN 10 Variables	
vpn 10 interface	ge0/0
vpn 10 IP address	10.2.0.212/24
Service Firewall Address	10.2.0.1
OSPF Router ID	10.2.0.200

Service VPN 20 Variables	
vpn 20 interface	ge0/3
vpn 20 IP address	10.2.20.3/24
VRRP IP address	10.2.20.1/24
VRRP Priority	50

Branch Template

Remote Site Designs

(Transport Variants)

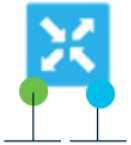


Remote Site Designs

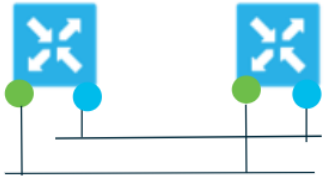
(Service LAN Variants)

L2

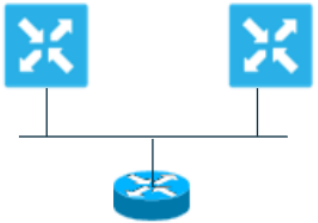
L2 VRRP

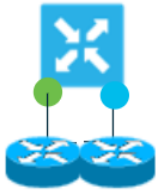


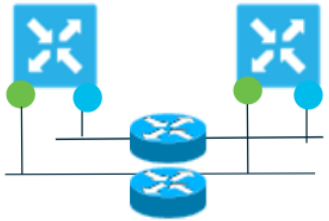
L2 Multi-VPN



L2 VRRP/Multi-VPN

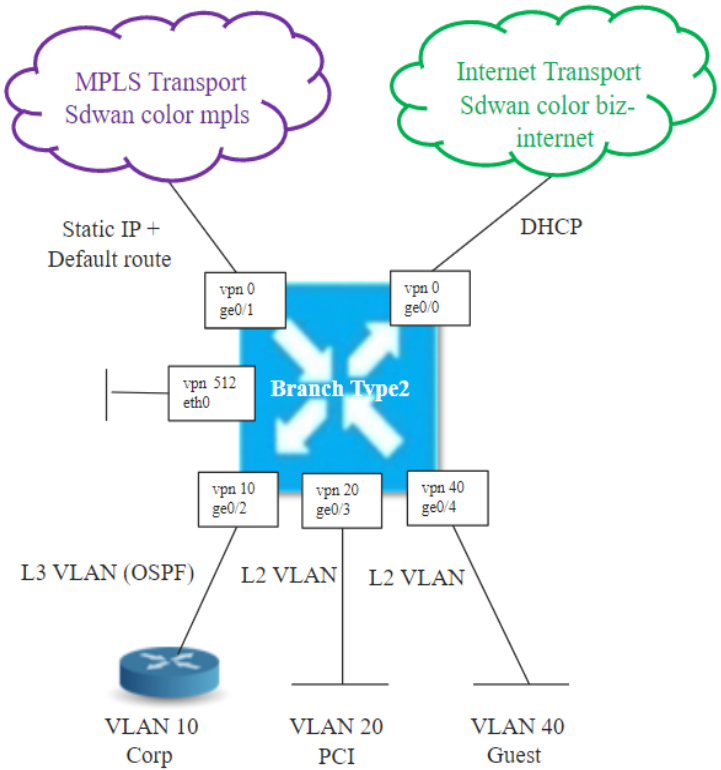






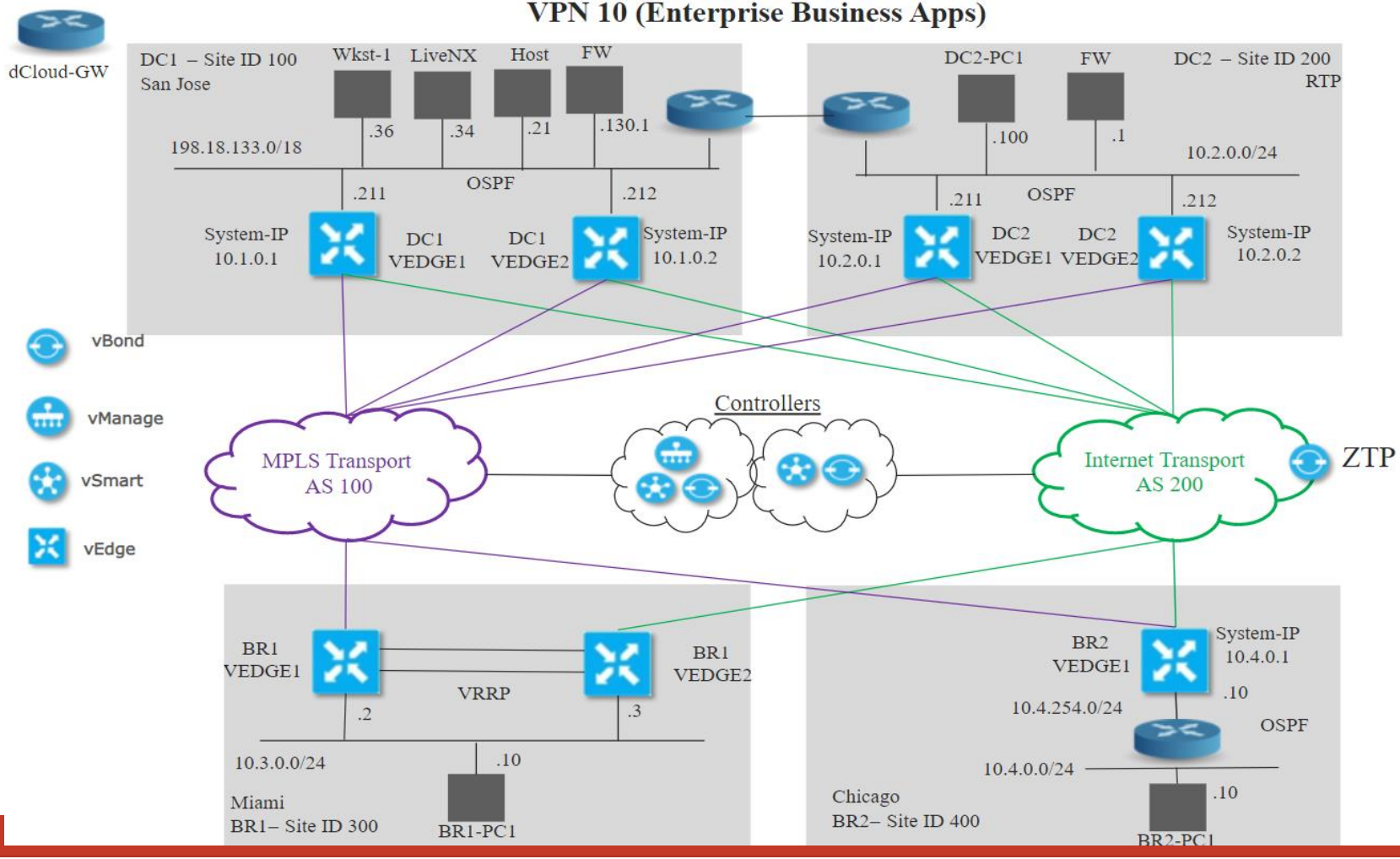
L3 Static/OSPF/BGP

Develop vManage Feature Templates for Branch Type 2

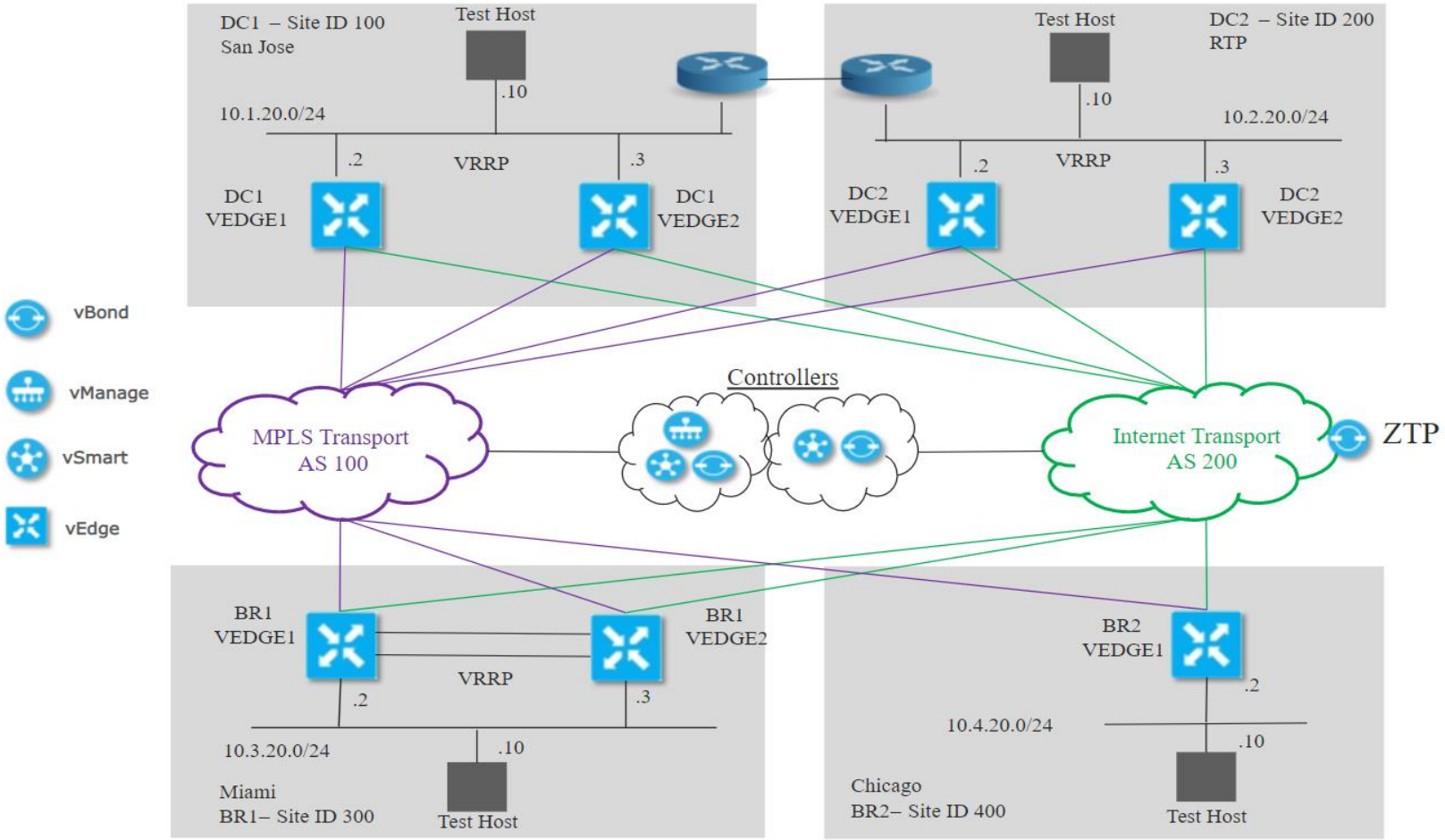


- Branch Type2 is a small density remote office
  - MPLS and Internet Transport
  - VPN 10 for Corp with L3 OSPF Routing to legacy router
  - VPN 20 for PCI with L2 VLAN
  - VPN 40 for Guest Wifi with L2 VLAN
- Create custom feature templates from factory default vManage templates
  - vpn-vedge feature templates for VPN0, VPN10, VPN20, VPN 40
  - vpn-vedge-interface feature templates for VPN0 TLOC interfaces
  - vpn-vedge-interface feature templates for Service VPNs 10,20,40
  - OSPF feature template for VPN10
- Create new Device Template for BranchType2
  - Reuse existing templates for basic information section (aaa, omp
  - Apply custom feature templates for VPN and VPN interfaces
  - Apply custom OSPF template for VPN0
  - Use default templates for others

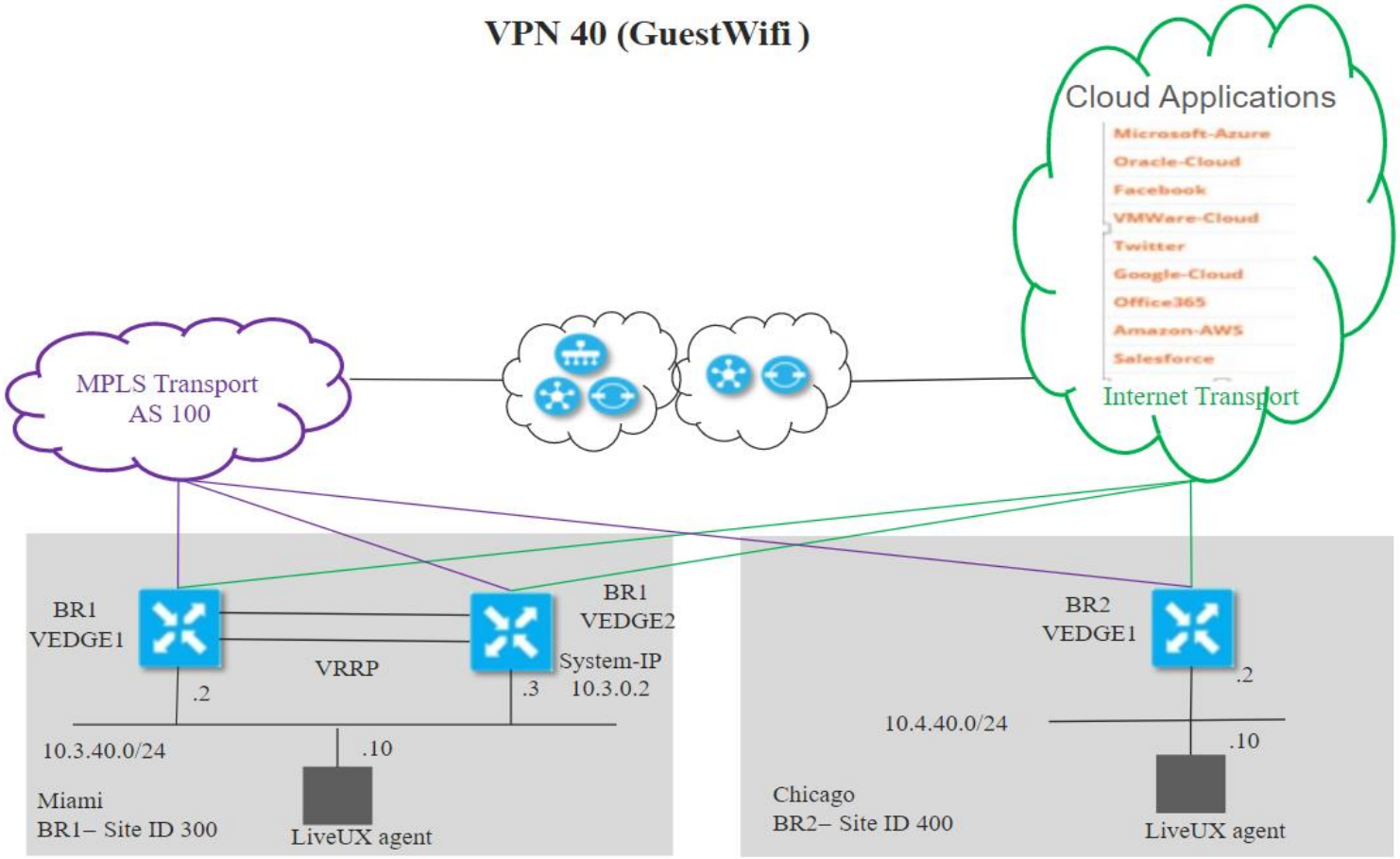
VPN 10 (Enterprise Business Apps)



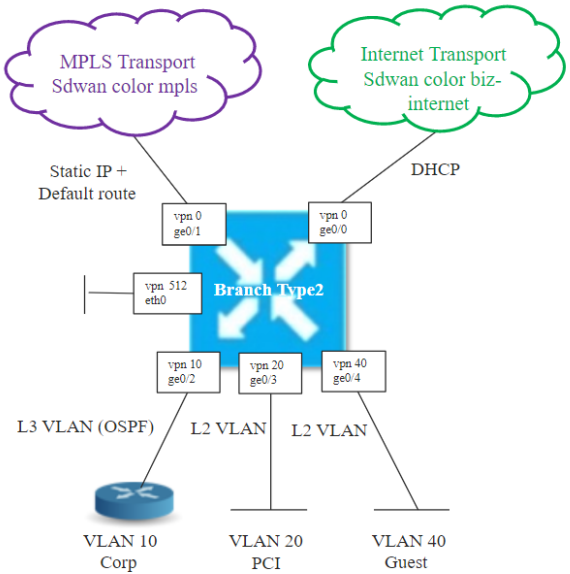
VPN 20 (PCI Apps)



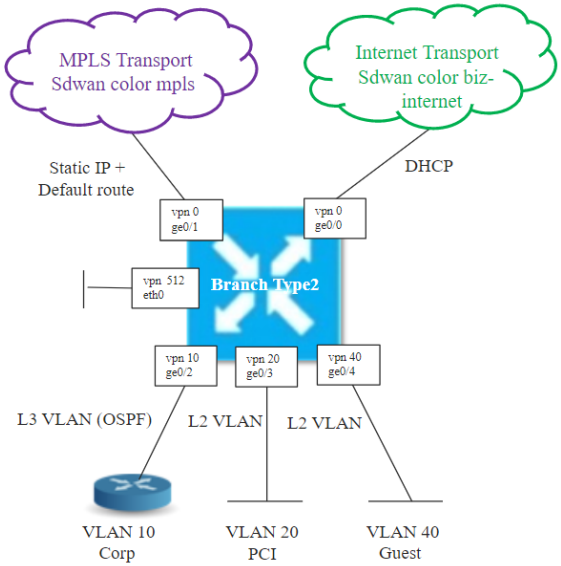
VPN 40 (GuestWifi)



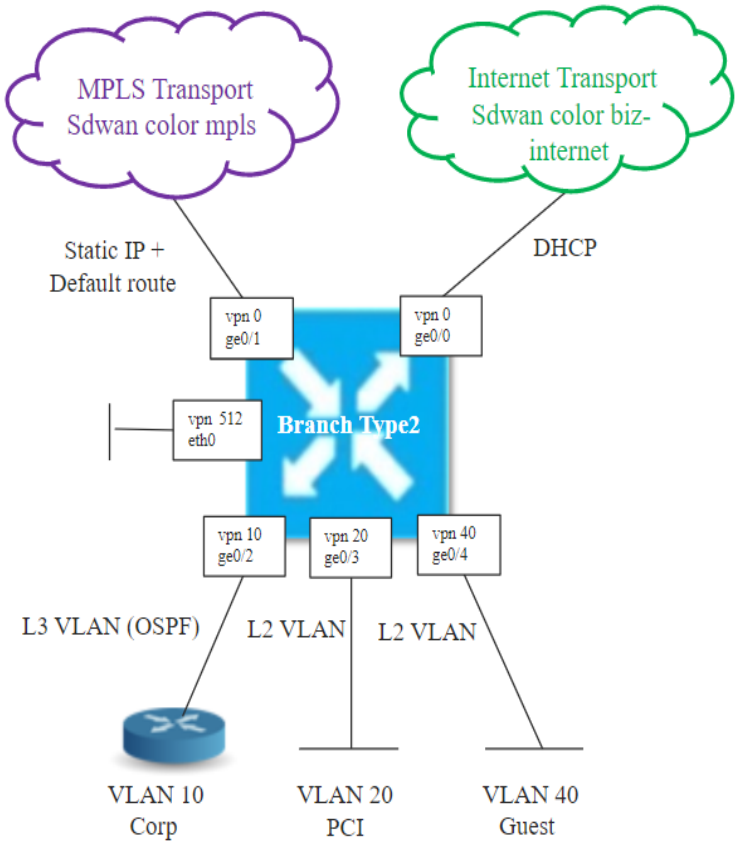
Template Planning



Branch 2 Specific Custom Feature Templates	
Feature template Name	**Customization**
VPN0-BR2-Feature-Template	FW Service Insertion (announce service into VPN0)
BR2-MPLS-TLOC	Static IP, color mpls, ge0/1, restrict
BR2-Internet-TLOC-DHCP	Dynamic IP, color biz-internet, ge0/0
BR2-VPN10-Feature	Advertise OMP: OSPF
BR2-OSPF-Feature	Redistribute OMP (OMP -> OSPF) Area 0, interface ge0/2, Policy denyInfraRoutes
VPN10-BR-Interface	ge0/2, IP ACL ingress
VPN20-BR-Interface	ge0/3, IP ACL ingress
VPN40-BR2-Interface	ge0/4, IP ACL ingress

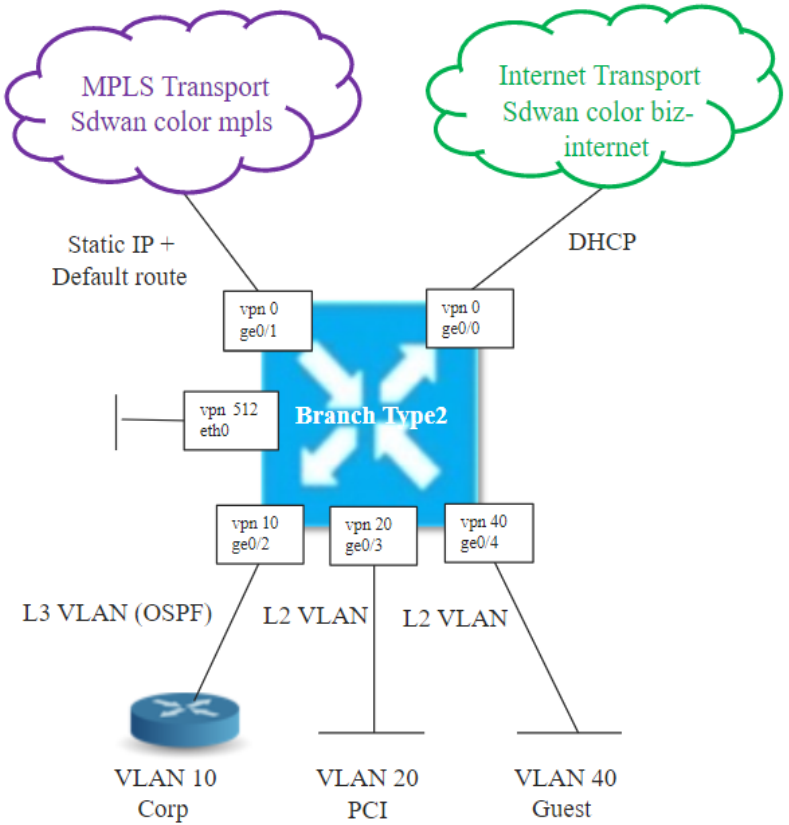


Custom Feature Templates common to all Sites in dCloud network	
Feature Template Name	**Customization**
System-dCloud-Feature	Site ID variable, system IP variable, hostname variable, GPS variable,
OMP-dCloud-Feature	ECMP Limit 8,
BFD-dCloud-Feature	Poll Interval
VPN512-dCloud-Feature	VPN 512
VPN512-Interface	Eth0, Static IP variable
dCloud-Banner	Custom Banner
LocalizedPolicyBaseline	QoS, OSPF filtering, application visibility
Snmp-dCloud-feature	SNMP Community, View, Trap Server

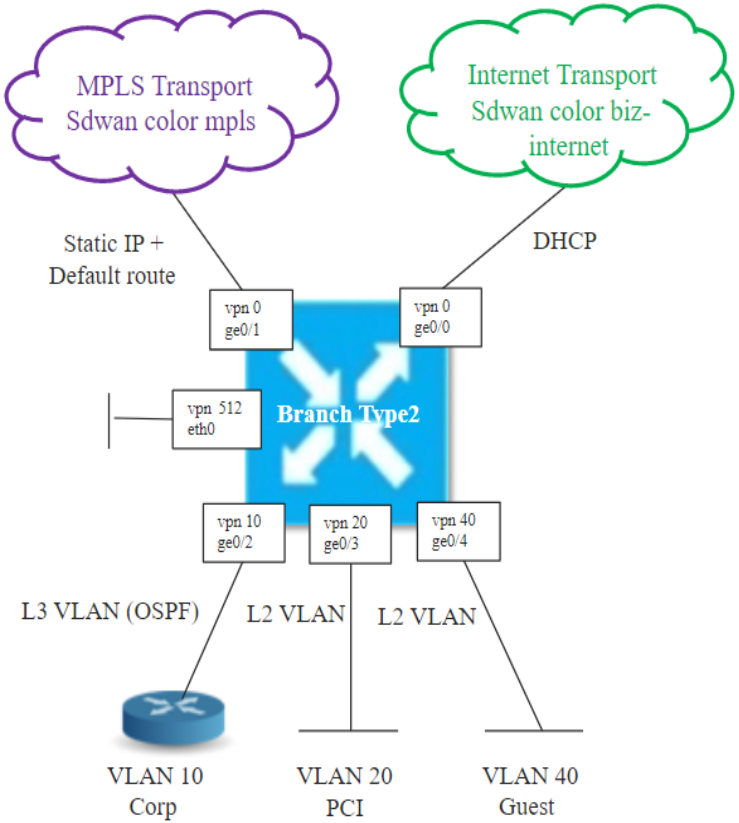


Factory Default Feature Templates
Logging
AAA
Security

Unused Feature Templates
Archive
Bridge
DHCP
IGMP
Multicast
NTP
PIM
VPN Interface Bridge, GRE, IPSec, NATPoolm PPP, PPP Ethernet

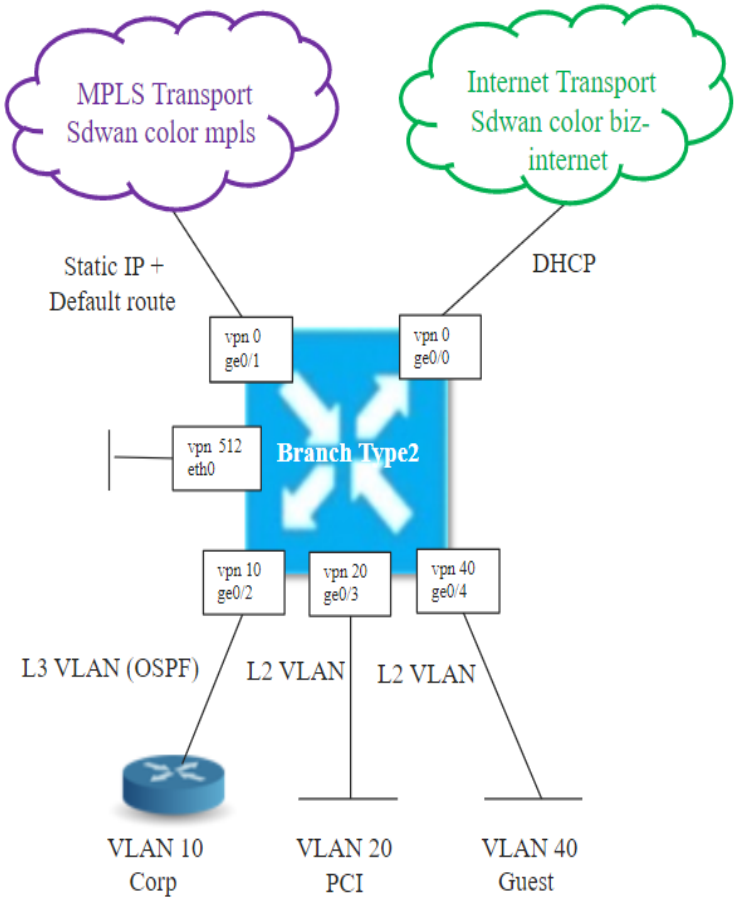


Branch 2 Specific Custom Feature Templates	
Feature template Name	**Customization**
VPN0-BR2-Feature-Template	VPN 0, dns vbond.cisco.com, 0.0.0.0/0
BR2-MPLS-TLOC	Static IP, color mpls, ge0/1, restrict
BR2-Internet-TLOC-DHCP	Dynamic IP, color biz-internet, ge0/0
BR2-VPN10-Feature	Advertise OMP: OSPF
BR2-OSPF-Feature	Redistribute OMP (OMP -> OSPF) Area 0, interface ge0/2, Policy denyInfraRoutes
VPN10-BR-Interface	ge0/2, IP ACL ingress
VPN20-BR-Interface	ge0/3, IP ACL ingress
VPN40-BR2-Interface	ge0/4, IP ACL ingress

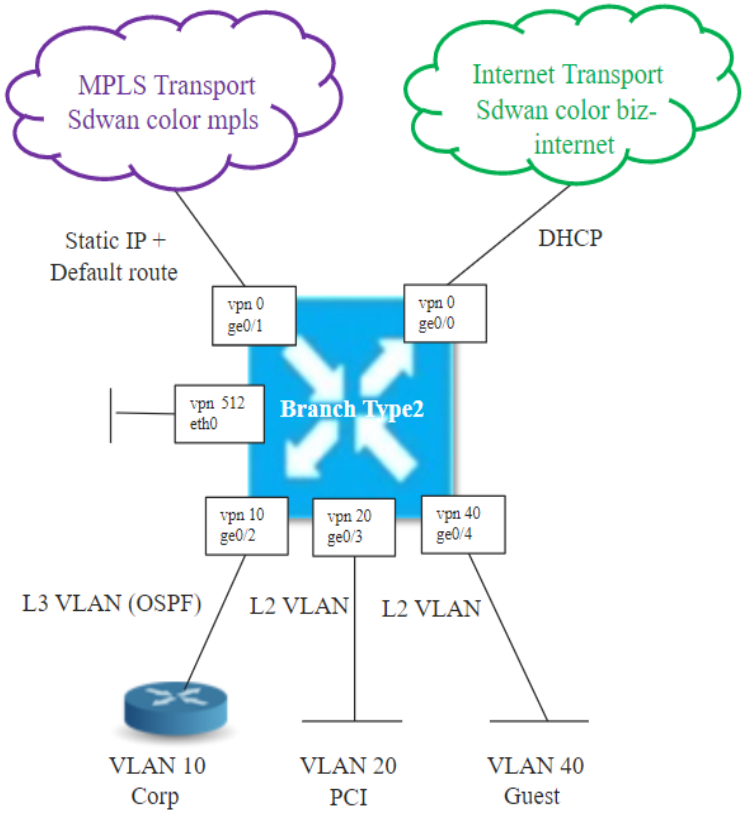


Factory Default Feature Templates
Logging
AAA
Security

Unused Feature Templates
Archive
Bridge
DHCP
IGMP
Multicast
NTP
PIM
VPN Interface Bridge, GRE, IPSec, NATPoolm PPP, PPP Ethernet



- Branch Type2 is a small density remote office
  - MPLS and Internet Transport
  - VPN 10 for Corp with L3 OSPF Routing to legacy router
  - VPN 20 for PCI with L2 VLAN
  - VPN 40 for Guest Wifi with L2 VLAN
- Create custom feature templates from factory default vManage templates
  - vpn-vedge feature templates for VPN0, VPN10, VPN20, VPN 40
  - vpn-vedge-interface feature templates for VPN0 TLOC interfaces
  - vpn-vedge-interface feature templates for Service VPNs 10,20,40
  - OSPF feature template for VPN10
- Create new Device Template for BranchType2
  - Reuse existing templates for basic information section (aaa, omp
  - Apply custom feature templates for VPN and VPN interfaces
  - Apply custom OSPF template for VPN0
  - Use default templates for others

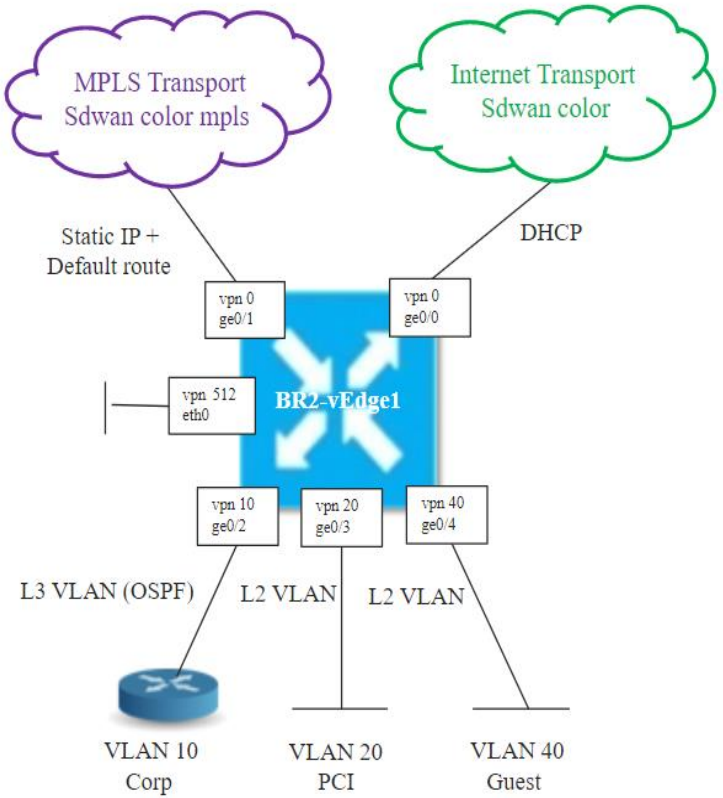


Branch 2 Specific Custom Feature Templates	
Feature template Name	**Customization**
VPN0-BR2-Feature-Template	VPN 0, dns vbond.cisco.com, 0.0.0.0/0
BR2-MPLS-TLOC	Static IP, color mpls, ge0/1, restrict
BR2-Internet-TLOC-DHCP	Dynamic IP, color biz-internet, ge0/0
BR2-VPN10-Feature	Advertise OMP: OSPF
BR2-OSPF-Feature	Redistribute OMP (OMP -> OSPF) Area 0, interface ge0/2, Policy denyInfraRoutes
VPN10-BR-Interface	ge0/2, IP ACL ingress
VPN20-BR-Interface	ge0/3, IP ACL ingress
VPN40-BR2-Interface	ge0/4, IP ACL ingress

Bring up new vEdge Cloud as BR2-vEdge1

System Variables	
Hostname	BR2-VEDGE1
GPS latitude	32.79
GPS longitude	-96.77
System IP	10.4.0.1
Site ID	400

Management VPN (VPN512) Variables	
eth0 IP Address	198.18.134.106/18
vpn512-GW-IP	198.18.128.1



Transport VPN (VPN0) Variables	
ge0/1 interface IP address (MPLS transport)	172.16.4.2/30
MPLS GW IP	172.16.4.1

Service VPN Variables	
vpn 10 IP address	10.4.254.10/24
vpn 20 IP address	10.4.20.1/24
vpn40 IP address	10.4.40.1/24

BR2-vEdge2 Device Onboarding

Request vedge-cloud activate chassis-number [UUID] token [OTP]

```
system
 organization-name       "Cisco Sy1 - 19968"
 vbond vbond.cisco.com
 site-id 40
 system-ip 10.4.0.1
 !
vpn 0
 host vbond.cisco.com ip 198.18.1.11 198.18.1.21
 interface ge0/1
  ip address 172.16.4.2/30
  tunnel-interface
   encapsulation ipsec
  !
  no shutdown

ip route 0.0.0.0/0 172.16.4.1
```

Steps:

Create a Device Template from Feature Templates

Create a Device Template from the CLI

Edit a Template

View a Template

Delete a Template

View Device Templates Attached to a Feature Template

View Devices Attached to a Device Template

Perform Parallel Template Operations

On Viptela devices in the overlay network, you can perform the same operations, in parallel, from one or more vManage servers.

Attach Devices to a Device Template

Copy a Template

Edit a CLI Device Template

Export a Variables Spreadsheet in CSV Format for a Template

Change the Device Rollback Time and View Configuration Differences

Available Feature Templates

AAA
Archive
Banner
BFD
BGP
Bridge
Cellular Profile
DHCP Server
IGMP
Logging
Multicast
NTP
OMP
OSPF
PIM
Security
SNMP
System
VPN
VPN Interface Bridge
VPN Interface Cellular
VPN Interface Ethernet
VPN Interface GRE
VPN Interface IPsec
VPN Interface NAT Pool
VPN Interface PPP
VPN Interface PPP Ethernet
WiFi Radio
WiFi SSID

OMP _ TLOC _

- 3.2 Configure and verify SD-WAN data plane
- 3.2.a Circuit termination/TLOC-extension
- 3.2.b Underlay-overlay connectivity
- 3.3 Configure and verify OMP
- 3.4 Configure and verify TLOCs

OMP Routing Protocol

- The Viptela Overlay Management Protocol (OMP) is the protocol responsible for establishing and maintaining the Viptela control plane. It provides the following services:

- **Orchestration of overlay network communication**, including connectivity among network sites, service chaining, and VPN topologies

- **Distribution of service-level routing** information and related location mappings

- **Distribution of data plane security parameters**

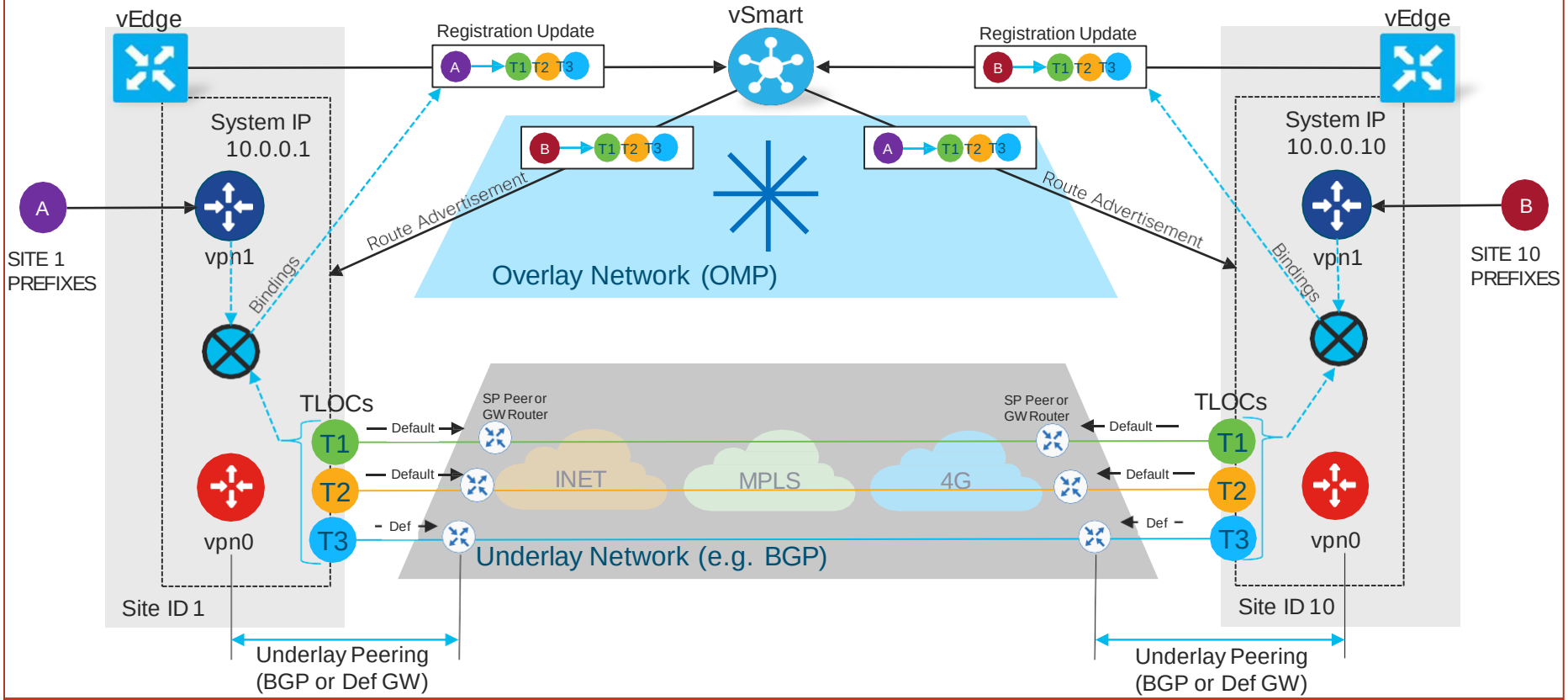
- **Central control and distribution of routing policy**

OMP Route Advertisements

- On vSmart controllers and vEdge routers, OMP advertises to its peers the routes and services that it has learned from its local site, along with their corresponding transport location mappings, which are called TLOCs. These routes are called OMP routes or vRoutes, to distinguish them from standard IP routes. It is through OMP routes that the vSmart controllers learn the topology of the overlay network and the services available in the network.

- OMP performs path selection, loop avoidance, and policy implementation on each local device to decide which routes are installed in the local routing table of any edge device.

Understanding OMP



OMP advertises the following types of routes:

OMP routes (also called vRoutes)

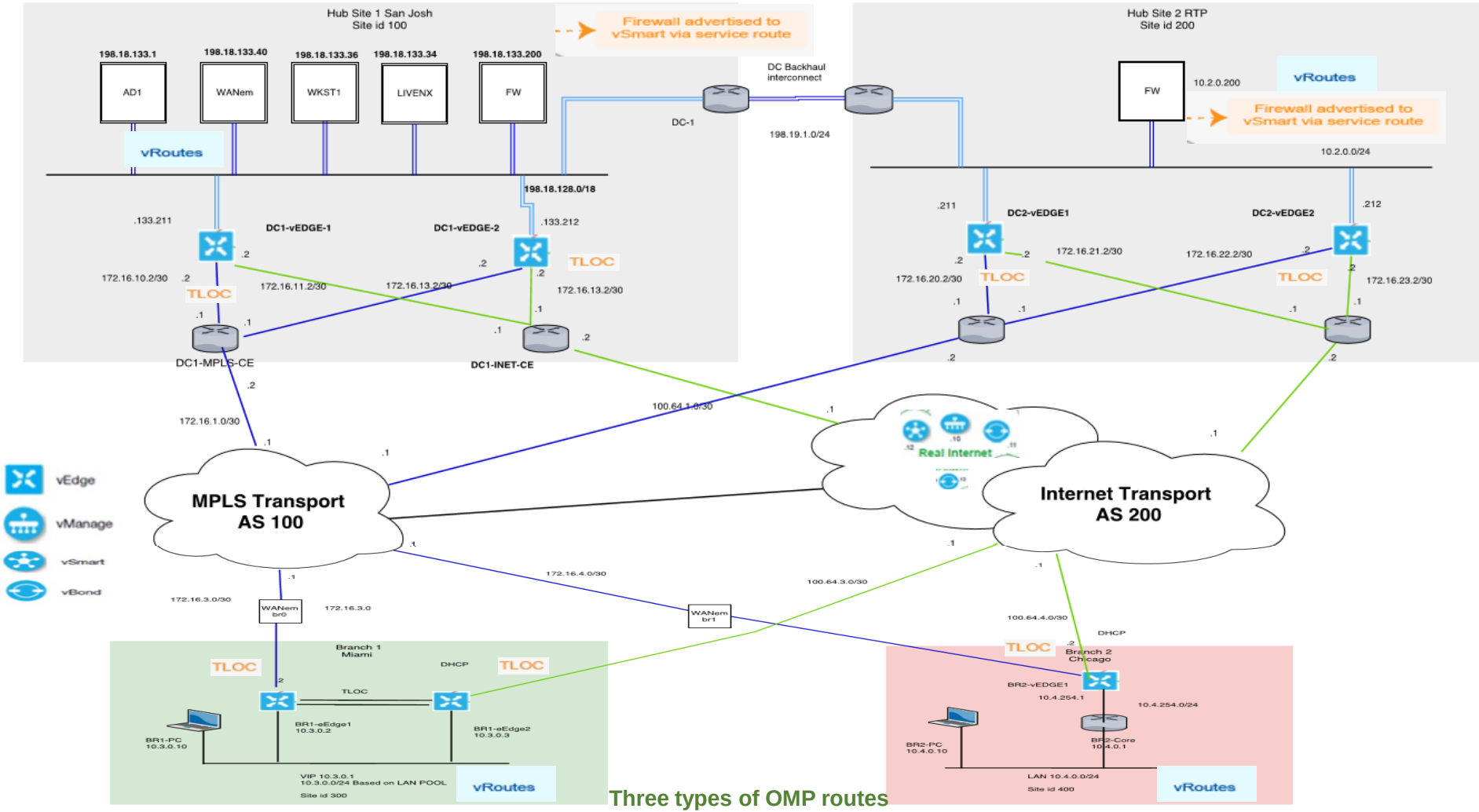
Service routes—Identifiers

Transport locations (TLOCs)

- **OMP routes (also called vRoutes)**—Prefixes that establish reachability between end points that use the OMP-orchestrated transport network. OMP routes can represent services in a central data center, services at a branch office, or collections of hosts and other end points in any location of the overlay network. OMP routes require and resolve into TLOCs for functional forwarding. In comparison with BGP, an OMP route is the equivalent of a prefix carried in any of the BGP AFI/SAFI fields.

- **Service routes—**Identifiers that tie an OMP route to a service in the network, specifying the location of the service in the network. Services include firewalls, Intrusion Detection Systems (IDPs), and load balancers. Service route information is carried in both service and OMP routes.

- **Transport locations (TLOCs)—**Identifiers that tie an OMP route to a physical location. The TLOC is the only entity of the OMP routing domain that is visible to the underlying network, and it must be reachable via routing in the underlying network. A TLOC can be directly reachable via an entry in the routing table of the physical network, or it must be represented by a prefix residing on the outside of a NAT device and must be included in the routing table. In comparison with BGP, the TLOC acts as the next hop for OMP routes.



Three types of OMP routes

OMP Routes

- Each vEdge router at a branch or local site advertises OMP routes to the vSmart controllers in its domain. These routes contain routing information that the vEdge router has learned from its site-local network.

- A vEdge router can advertise one of the following types of site-local routes:
- Connected (also known as direct)
- Static
- BGP
- OSPF (inter-area, intra-area, and external)

OMP routes advertise the following attributes:

- **TLOC—**Transport location identifier of the next hop for the vRoute. It is similar to the BGP NEXT_HOP attribute. A TLOC consists of three components:
  - System IP address of the OMP speaker that originates the OMP route
  - Color to identify the link type
  - Encapsulation type on the transport tunnel

- **Origin—**Source of the route, such as BGP, OSPF, connected, and static, and the metric associated with the original route.

- **Originator—**OMP identifier of the originator of the route, which is the IP address from which the route was learned.

- **Preference—Degree** of preference for an OMP route. A higher preference value is more preferred.

- **Service—Network** service associated with the OMP route.

- **Site ID—Identifier** of a site within the Viptela overlay network domain to which the OMP route belongs.

- **Tag—Optional**, transitive path attribute that an OMP speaker can use to control the routing information it accepts, prefers, or redistributes.

- **VPN—VPN** or network segment to which the OMP route belongs.

TLOC Routes

- TLOC routes identify transport locations. These are locations in the overlay network that connect to physical transport, such as the point at which a WAN interface connects to a carrier. A TLOC is denoted by a 3-tuple that consists of the system IP address of the OMP speaker, a color, and an encapsulation type. OMP advertises each TLOC separately.

- TLOC routes advertise the following attributes:
- **TLOC private address—Private** IP address of the interface associated with the TLOC.

- **TLOC public address—NAT-translated** address of the TLOC.

- **Carrier**—An identifier of the carrier type, which is generally used to indicate whether the transport is public or private.
- **Color**—Identifies the link type.

- **Encapsulation type—Tunnel** encapsulation type.

- **Preference**—Degree of preference that is used to differentiate between TLOCs that advertise the same OMP route.

- **Site ID—Identifier** of a site within the Viptela overlay network domain to which the TLOC belongs.

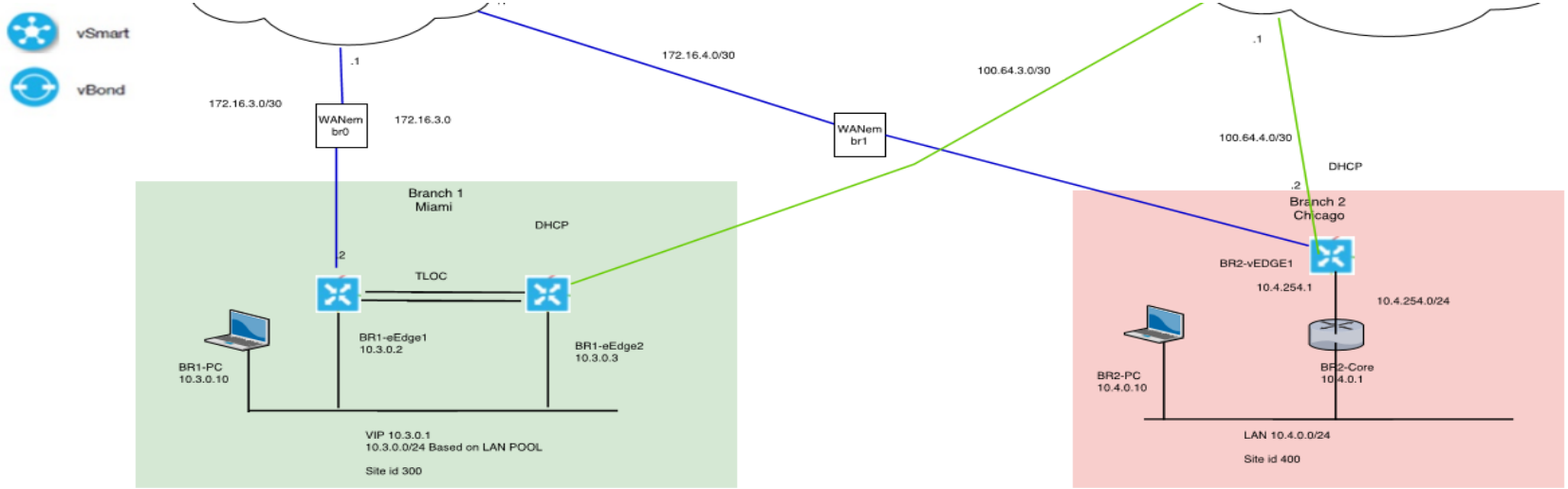
- **Tag**—Optional, transitive path attribute that an OMP speaker can use to control the flow of routing information toward a TLOC. When an OMP route is advertised along with its TLOC, both or either can be distributed with a community TAG, to be used to decide how send traffic to or receive traffic from a group of TLOCs.

- **Weight**—Value that is used to discriminate among multiple entry points if an OMP route is reachable through two or more TLOCs.

TLOC Example

The system IP address of the router is 10.4.0.1. The TLOC on the left is uniquely identified by the system IP address 10.4.0.1, the color metro-ethernet, and the encapsulation IPsec, and it maps to the physical WAN interface with the IP address 100.64.4.1.

The TLOC on the right is uniquely identified by the system IP address 10.4.0.1, the color biz-internet, and the encapsulation IPsec, and it maps to the WAN IP address 10.4.0.1.



OMP Best-Path Algorithm and Loop Avoidance

vEdge routers advertise their local routes to the vSmart controller using OMP. Depending on the network topology, some routes might be advertised from multiple vEdge routers. Viptela devices use the following algorithm to choose the best route:

1.Check whether the OMP route is valid. If not, ignore it.

2.If the OMP route is valid and if it has been learned from the same Viptela device, select the OMP route with the lower administrative distance.

3.If the administrative distances are equal, select the OMP route with the higher OMP route preference value.

OMP Best-Path Algorithm and Loop Avoidance

4.On vEdge routers only, if the OMP route preference values are equal, select the OMP route with the higher TLOC preference value.

5. On vEdge routers only, if the TLOC preference values are equal, compare the origin type, and select one in the following order (select the first match):
Connected
Static
EBGP
OSFP intra-area
OSPF inter-area
OSPF external
IBGP
Unknown

6.If the origin types are the same, select the OMP route the higher router ID.

OMP Best-Path Algorithm and Loop Avoidance

7.If the router IDs are equal, a vEdge router selects the OMP route with the higher private IP address. If a vSmart controller receives the same prefix from two different sites and if all attributes are equal, the vSmart controller chooses both of them.

A vEdge router installs an OMP route in its forwarding table (FIB) only if the TLOC to which it points is active. For a TLOC to be active, an active BFD session must be associated with that TLOC. BFD sessions are established by each vEdge router, which creates a separate BFD session with each of the remote TLOCs. If a BFD session becomes inactive, the vSmart controller removes from the forwarding table all the OMP routes that point to that TLOC.

Graceful Restart for OMP

Graceful restart for OMP allows the data plane in the Viptela overlay network to continue functioning if the control plane stops functioning or becomes unavailable.

With graceful restart, if the vSmart controller in the network goes down, or if multiple vSmart controllers go down simultaneously, the vEdge routers can continue forwarding data traffic.

They do this using the last known good information that they received from the vSmart controller. When a vSmart controller is again available, its DTLS connection to the vEdge router is re-established, and the vEdge router then receives updated, current network information from the vSmart controller.

Configuring OMP

By default, OMP is enabled on all vEdge routers and vSmart controllers. OMP must be operational for the Viptela overlay network to function. If you disable it, you disable the overlay network.

Configure OMP Graceful Restart

OMP graceful restart is enabled by default on vSmart controllers and vEdge routers. The default graceful restart time is 43,200 seconds (12 hours).

OMP graceful restart has a timer that tells the OMP peer how long to retain the cached advertised routes. When this timer expires, the cached routes are considered to be no longer valid, and the OMP peer flushes them from its route table. The default timer is 43,200 seconds (12 hours), and the timer range is 1 through 604,800 seconds (7 days). To modify the default timer value:

Viptela(config-omp)# timers graceful-restart-timer *seconds*

Advertise Routes **to OMP**

By default, a vEdge router advertises connected, static routes, and OSPF inter-area and intra-area routes to OMP, and hence to the vSmart controller responsible for the vEdge router's domain. The router does not advertise BGP or OSPF external routes to OMP. To have the vEdge router advertise these routes to OMP, and hence to the vSmart controller responsible for the vEdge router's domain, use the advertise command: To configure the routes that the vEdge router advertises to OMP for all VPNs configured on the router:

vEdge(config-omp)# **advertise** (**bgp** | **connected** | **ospf** *type* | **static**)

To configure the routes that the vEdge router advertises to OMP for a specific VPN on the router:
vEdge(config-vpn-omp)# **advertise** (**aggregate** *prefix* [**aggregate-only**] | **bgp** | **connected** | **network** *prefix* | **ospf** *type* | **static**)

For OSPF, the route type can be **external**.

The **bgp**, **connected**, **ospf**, and **static** options advertise all learned or configured routes of that type to OMP. To advertise a specific route instead of advertising all routes for a protocol, use the **network** option, specific the prefix of the route to advertise.

Route advertisements that you set with the **omp advertise** command apply to all VPNs configured on the router. Route advertisements that you set with the **vpn omp advertise** command apply only to the specific VPN. If you configure route advertisements with both commands, they are both applied.

Configure the Number of Advertised Routes

vEdge routers advertise the routes that they learn from their local site to the vSmart controller, and the vSmart controller redistributes this routes to other vEdge routers in the overlay network. The routes advertised are actually a tuple consisting of the route and the TLOC associated with that route.

A **vEdge router can have up to six WAN interfaces**, and each WAN interface has a different TLOC. (A WAN interface is any interface in VPN 0 that is configured as a tunnel interface. Both physical and loopback interfaces can be configured to be tunnel interfaces.) The vEdge router advertises each route–TLOC tuple to the vSmart controller.

The vSmart controller redistributes the routes it learns from vEdge routers, advertising each route–TLOC tuple. If, for example, a local site as two vEdge routers, a vSmart controller could potentially learn eight route–TLOC tuples for the same route.

Configure the OMP Hold Time

The OMP hold time determines how long to wait before closing the OMP connection to a peer. If the peer does not receive three consecutive keepalive messages within the hold time, the OMP connection to the peer is closed. The default OMP hold time is 60 seconds. To modify the OMP hold time interval:
Viptela(config-omp)# **timers holdtime** *seconds*

The hold time can be in the range 0 through 65535 seconds.
The keepalive timer is one-third the hold time and is not configurable.
If the local device and the peer have different hold time intervals, the higher value is used.
If you set the hold time to 0, the keepalive and hold timers on the local device and the peer are set to 0.
The hold time must be at least two times the hello tolerance interval set on the WAN tunnel interface in VPN 0. To configure the hello tolerance interface, use the **hello-tolerance** command.

Configure the OMP Update Advertisement Interval

By default, OMP sends Update packets once per second. To modify this interval:

Viptela(config-omp)# **timers advertisement-interval** *seconds*
The interval can be in the range 0 through 65535 seconds.

Configure the End-of-RIB Timer
After an OMP session goes down and then comes back up, an end-of-RIB (EOR) marker is sent after 300 seconds (5 minutes). After this maker is sent, any routes that were not refreshed after the OMP session came back up are considered to be stale and are deleted from the route table. To modify the EOR timer:
Viptela(config-omp)# **timers eor-timer** *seconds*

The time can be in the range 1 through 3600 seconds (1 hour).

OMP Route Redistribution

OMP automatically redistributes the following types of routes that it learns either locally or from its routing peers:

- Connected
- Static
- OSPF intra-area routes
- OSPF inter-area routes

To avoid routing loops and less than optimal routing, redistribution of following types of routes requires explicit configuration:

- BGP
- OSPF external routes

To avoid propagating excessive routing information from the edge to the access portion of the network, the routes that vEdge routers receive via OMP are not automatically redistributed into the other routing protocols running on the routers. If you want to redistribute the routes received via OMP, you must enable this redistribution locally, on each vEdge router.

OMP route to indicate the route's origin

OMP sets the origin and sub-origin type in each OMP route to indicate the route's origin (see the table below). When selecting routes, the vSmart controller and the vEdge routers take the origin type and subtype into consideration.

OMP Route Origin Type	OMP Route Origin Subtype
BGP	**External** **Internal**
Connected	**—**
OSPF	**External-1** **External-2** **Intra-area** **Inter-area**
Static	**—**

OMP also carries the metric of the original route. A metric of 0 indicates a connected route.

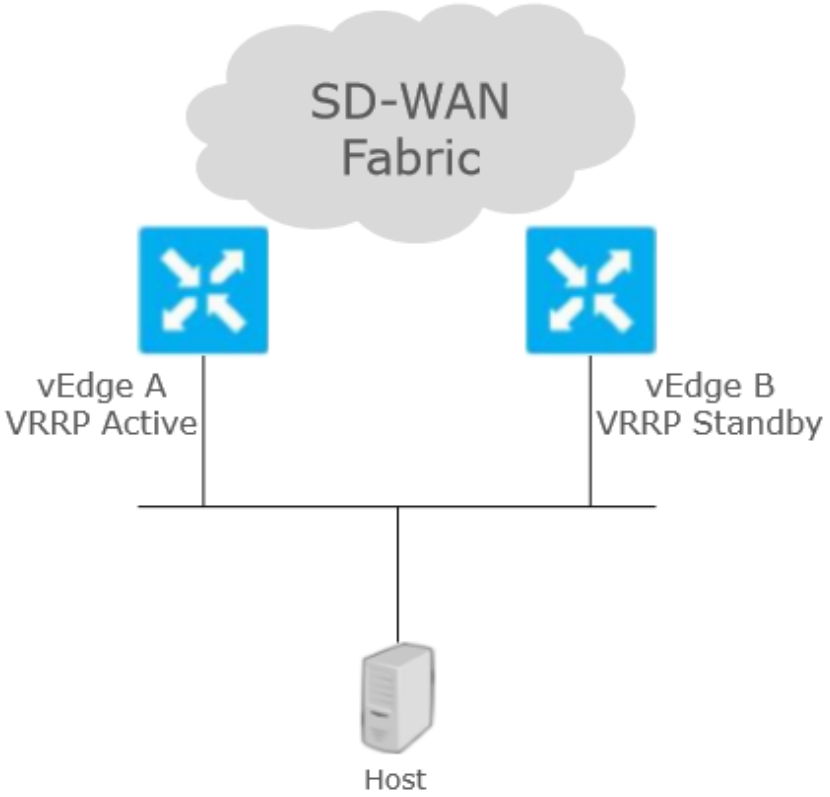
Administrative Distance

Protocol	Administrative Distance
Connected	0
Static	1
NAT (NAT and static routes cannot coexist in the same VPN; NAT overwrites static routes)	1
Learned from DHCP	1
GRE	5
EBGP	20
OSPF	110
IBGP	200
OMP	250

VRRP
Virtual Router Redundancy Protocol

Site Redundancy - Bridged

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



Virtual Router Redundancy Protocol (VRRP)

- Configure the Virtual Router Redundancy Protocol (VRRP) to allow multiple routers to share a common virtual IP address for default gateway redundancy (on vEdge routers only).
- **Hosts are assigned a single default gateway** (also called default router) IP address, either through DHCP or statically for the first-hop router.

- VRRP provides default gateway (first-hop router) redundancy through configuration of a virtual IP address shared by multiple routers on a single LAN or subnet.

- You cannot configure VRRP on an interface that is in the transport
- VPN (VPN 0).

Command

vpn *vpn-id*
interface ge*slot*/*port*[.*subinterface*]
vrrp *group-number*
ipv4 *ip-address*
priority *number*
timer *seconds*
(track-omp | track-prefix-list *list-name*)

Options

Advertisement Time

timer *seconds*

How often the VRRP master sends VRRP advertisement messages. If slave routers miss three consecutive VRRP advertisements, they elect a new master.

Range: 1 through 3600 seconds

Default: 1 second

Options

- Priority To Be Elected Master
  - **priority** *number*
    Priority level of the router. The router with the highest priority is elected as master.
  - If two vEdge routers have the same priority, the one with the higher IP address is
  - elected as master.
    Range: 1 through 254
    Default: 100

Track Interface State

(**track-omp | track-prefix-list** *list-name*)

By default, VRRP uses of the state of the service (LAN) interface on which it is

running to determine which vEdge router is the master virtual router.

When the interface for the master goes down, a new VRRP master virtual router is elected based on the VRRP priority value . Because VRRP runs on a LAN interface, if a vEdge router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, you can configure one of the following:

track-omp—Track the Overlay Management Protocol (OMP) session running on the WAN connection when determining the VRRP master virtual router. If all OMP sessions are lost on the master VRRP router, VRRP elects a new default gateway from among all the gateways that have one or more active OMP sessions even if the gateway chosen has a lower VRRP priority than the current master.

With this option, VRRP failover occurs once the OMP state changes from up to down, which occurs when the OMP hold timer expires. (The default OMP hold timer interval is 60 seconds.) Until the hold timer expires and a new VRRP master is elected, all overlay traffic is dropped.

When the OMP session recovers, the local VRRP interface claims itself as master even before it learns and installs OMP routes from the vSmart controllers. Until the routes are learned, traffic is also dropped.

track-prefix-list *list-name*—Track both the OMP session and a list of remote prefixes. *list-name* is the name of a prefix list configured with the **policy lists prefix-list** command on the vEdge router.

If all OMP sessions are lost, VRRP failover occurs as described for the **track-omp** option. In addition, if reachability to all the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the vEdge routers determine the VRRP master.

Default: VRRP tracks only the interface on which it is configured.

Virtual Router ID

vrrp *group-number*

Virtual router ID, which is a numeric identifier of the virtual router. For each interface or subinterface, you can configure only a single VRRP group.

Range: 1 through 255

Virtual Router IP Address

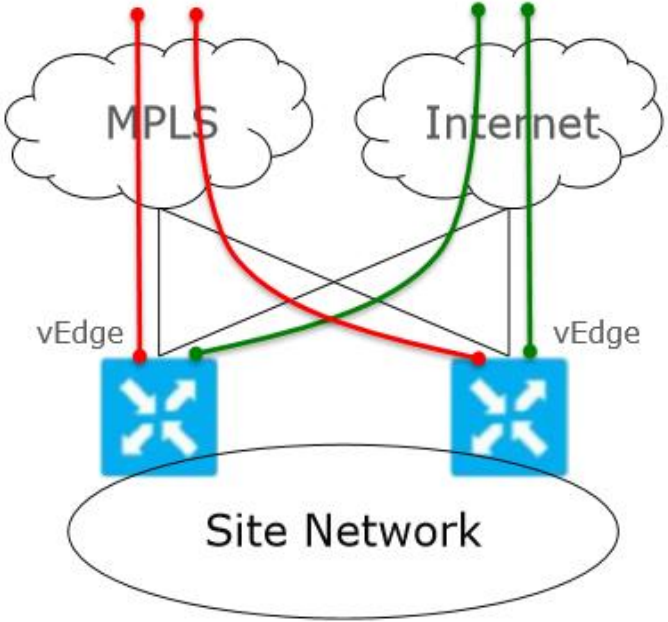
ip address *ip-address*

IP address of the virtual router. The virtual IP address must be different from the configured interface IP addresses of both the local vEdge router and the peer running VRRP. For eachinterface or subinterface, you can configure only a single virtual IP address.

Verification Commands

- show running-config vpn 10
- Show vrrp interfaces
- Show vrrp vpn 10
- Show vrrp vpn 10 interface ge0/0 group 11
- Show vrrp vpn 10 interfaces groups
- Show vrrp vpn 10 interfaces group 10
-

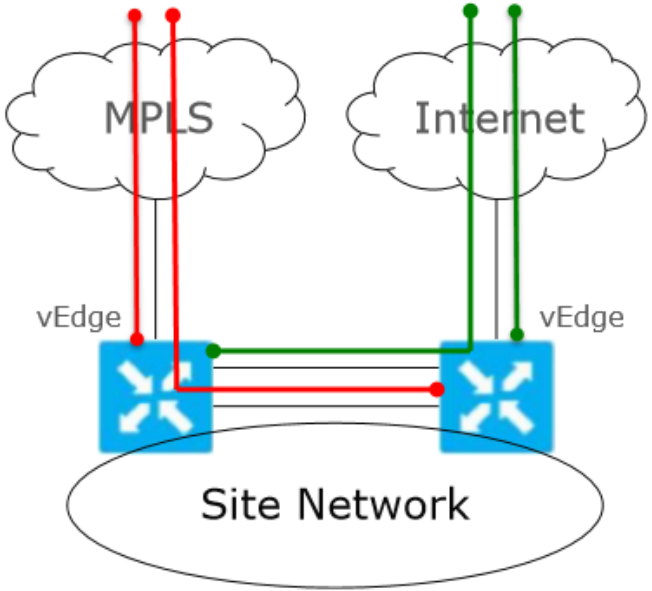
Transport Redundancy - Meshed



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

- If one of the vEdge routers fails, second vEdge router takes over forwarding the traffic in and out of site - Both transport are still available

Transport Redundancy – TLOC Extension

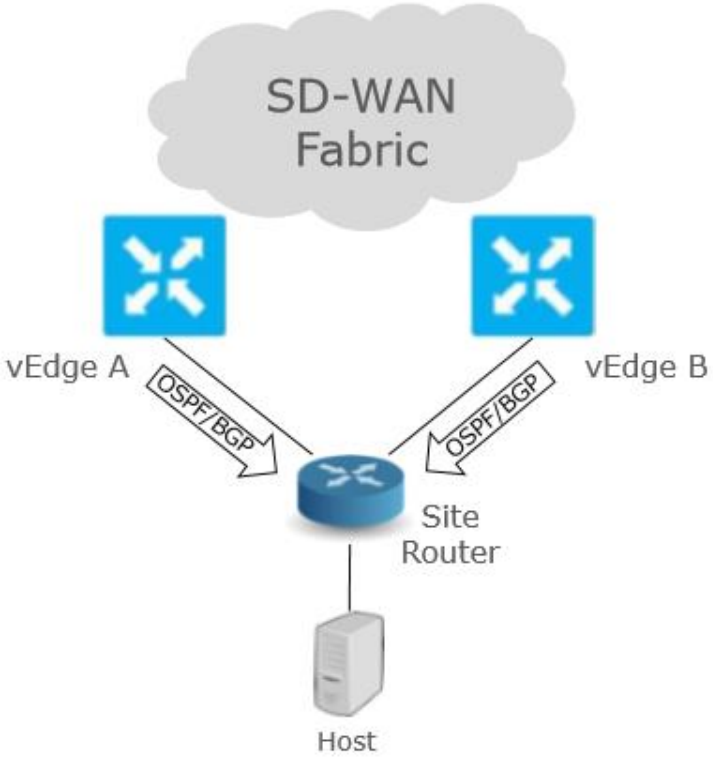


- vEdge routers are connected only to their respective transports
- vEdge routers build IPSec tunnels across directly connected transport and across the transport connected to the neighboring vEdge router - Neighboring vEdge router acts as an underlay router for tunnels initiated from the other vEdge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

Example & Lab :

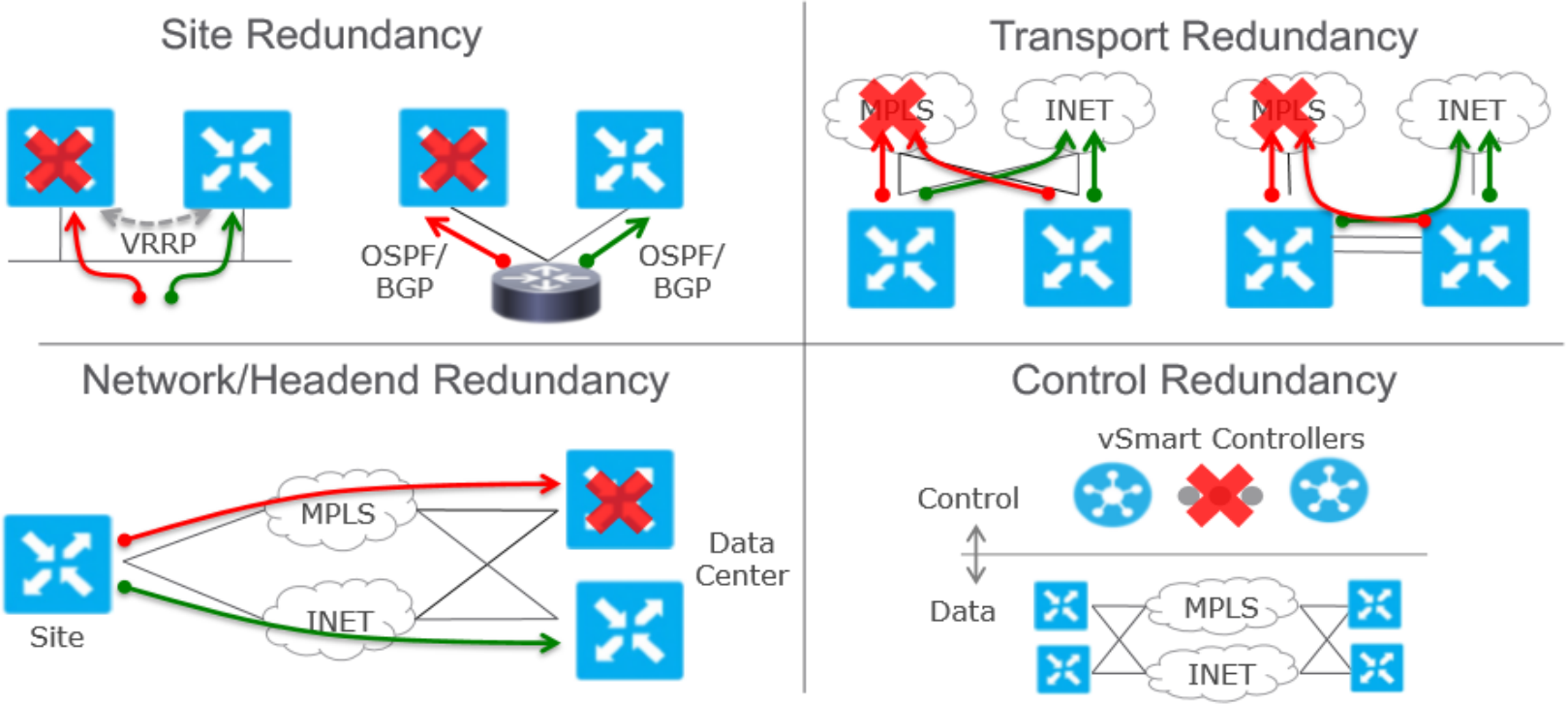
```
!
 interface ge0/3
  ip address 10.10.10.1/24
  tloc-extension ge0/1
  no shutdown
 !
 ip route 0.0.0.0/0 10.20.20.1
 ip route 0.0.0.0/0 172.16.3.1
!
```

Site Redundancy - Routed



- Redundant pair of vEdge routers operate in active/active mode
- vEdge routers are one or more Layer 3 hops away from the hosts
- Standard OSPF or BGP routing protocols are running between the redundant pair vEdge routers and the site router
- Bi-directional redistribution between OMP and OSPF/BGP and vice versa on the vEdge routers
- Site router performs equal cost multipathing for remote destinations across SD-WA Fabric - Can manipulate OSPF/BGP to prefer one vEdge router over the other

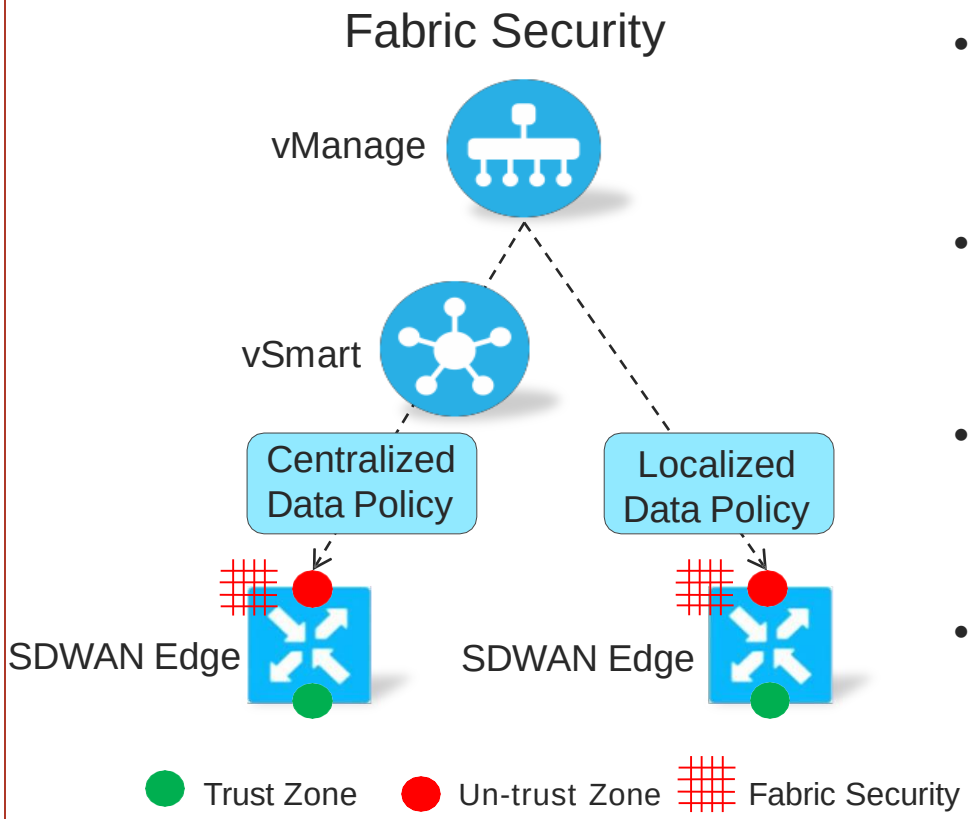
High Availability and Redundancy Connectivity Assurance



Thanks ☺

Terms	Description
Network ID	The equivalent of the overlay ID in Viptela. Auto-generated when a profile is present in PnP. Can be edited only when no profiles exist in a Virtual Account. All devices for a given organization name in ZTP should be associated to one network ID.
Organization name	An attribute that vManage used to tie all the controllers together. The organization name is associated to a vBond controller in the PnP portal.
vBond controller	Represents the vBond IP or domain name. Only IPv4 is supported today.
Base product ID (PID)	Hardware product ID that is on the label.
Ordered PID	An ordered SKU that was selected in CCW. In some cases, the ordered PID and base PID can have the same value.
Secure device ID (SUDI)	A secure board ID that is used to validate anti-tampered devices.
International Mobile station Equipment Identity (IMEI) or device IMEI	IMEI information for an LTE-enabled vEdge controller. Both of the values would be the same for vEdge devices.

Local SD-WAN Fabric Secure Perimeter



- Centralized data policy is defined on vManage and distributed by vSmart controllers
- Centralized data policy match on application traffic of interest
  - DPI or 6 tuple matching
- Centralized data policy takes drop action to block unwanted traffic
  - Can log
- Localized data policy works similarly to centralized data policy, but it is distributed directly from vManage