

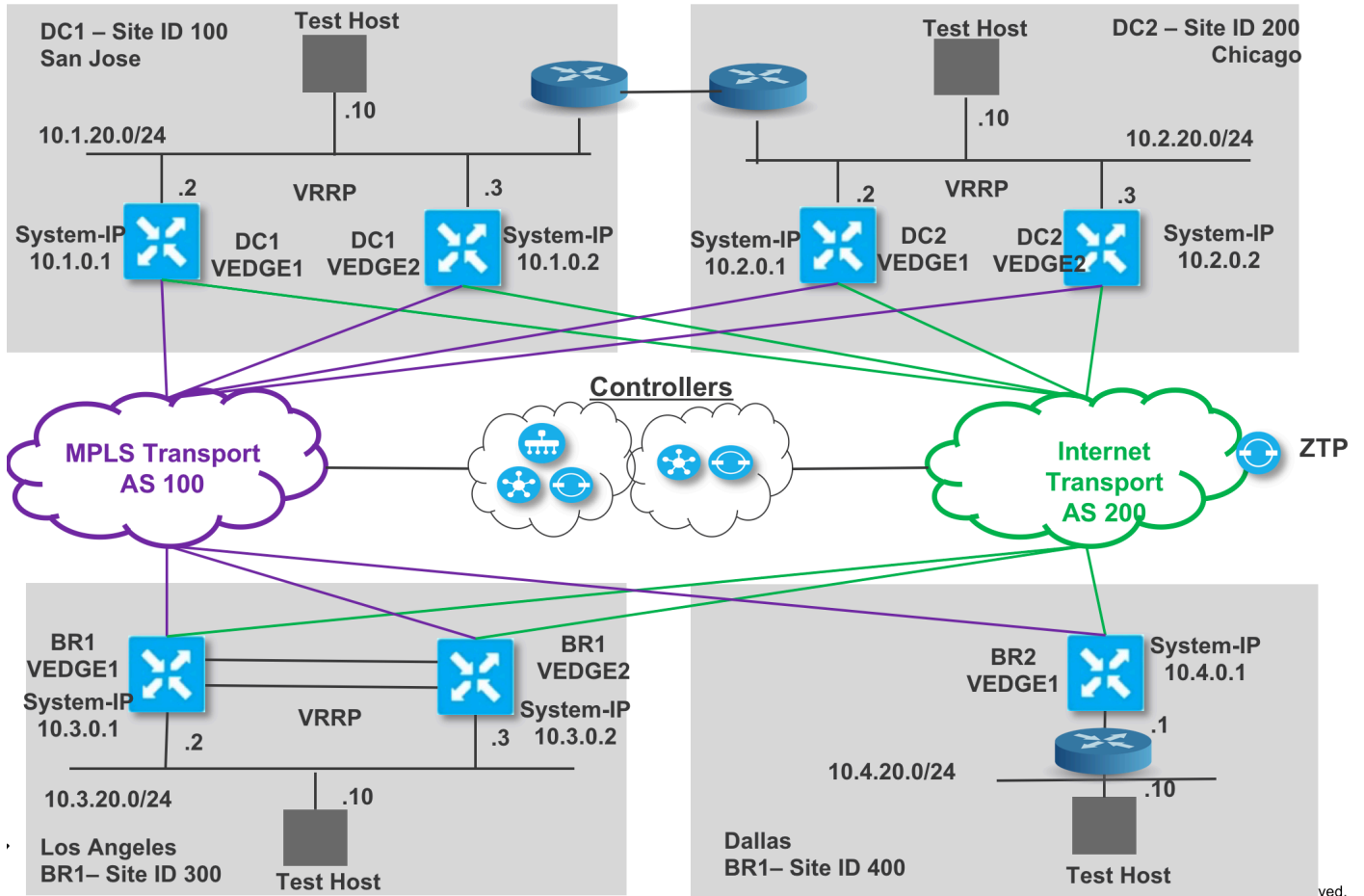
# Introduction to Cisco SD-WAN (Viptela) Lab Guide

LABEN-2010

<b>INTRODUCTION TO CISCO SD-WAN (VIPTELA)      LAB GUIDE.....</b>	<b>1</b>
<b>LAB01 – DEPLOY VEDGE IN BRANCH 2 USING ZTP .....</b>	<b>3</b>
STEPS.....	4
<i>DPI</i> .....	26
<i>IPFIX Flow Records</i> .....	26
<i>Interface Stats</i> .....	26
<b>LAB 02 - STRICT HUB-N-SPOKE TOPOLOGY .....</b>	<b>28</b>
STEPS.....	28
<b>LAB 03 - PREFER DATA CENTER DC1 AND DC2 FOR DIFFERENT SET OF BRANCHES FOR REGIONAL INTERNET EXIT .....</b>	<b>46</b>
STEPS.....	46
<b>LAB 04 - SERVICE (FW) INSERTION .....</b>	<b>53</b>
STEPS.....	53
<b>LAB 06 - APPLICATION AWARE ROUTING .....</b>	<b>59</b>
STEPS.....	59
<b>LAB 07 - CLOUD ONRAMP FOR SAAS (CLOUDEXPRESS) .....</b>	<b>68</b>
STEPS.....	68
<b>LAB 08 - MULTI-TOPOLOGY/DIFFERENT TOPOLOGIES PER VPN .....</b>	<b>87</b>
STEPS.....	87
<b>LAB 09 - APPLICATION FIREWALLING USING CENTRALIZED POLICIES.....</b>	<b>101</b>
STEPS.....	101
<b>UPGRADING SOFTWARE ON CISCO SD-WAN .....</b>	<b>107</b>
STEPS.....	107



## Lab Topology



# Lab01 – Deploy vEdge in Branch 2 using ZTP

In this scenario we will bring up Branch 2 site using ZTP.

## Steps

Deploy a Branch using vManage configuration template and Viptela's Zero Touch Provisioning (ZTP) service. ZTP process is simulated in this lab using default configuration from the factory for the vEdge in Branch 2.

The only difference is the out of band VPN 512 configuration. This is configured for the demo user to be able to login to the vEdge. The ZTP port (ge0/0) in this case is in shutdown mode. A "no shut" will be done to simulate connecting vEdge to the transport.

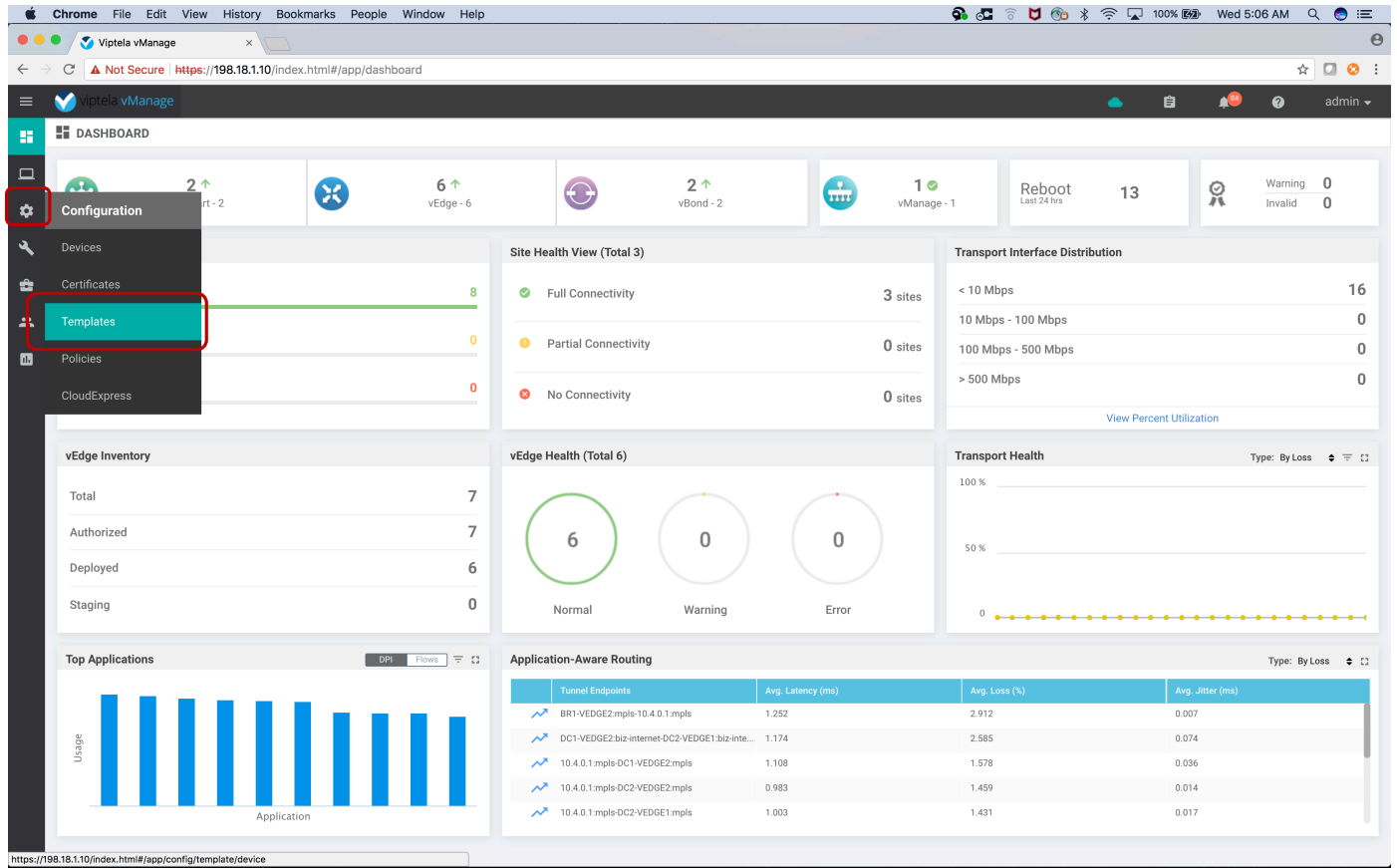
Go to the vManage Dashboard (login/password admin/admin). The dashboard shows the controllers are up and there are 6 operational vEdges. BR2-VEEDGE1 is still need to be provisioned via ZTP.

The screenshot shows the Viptela vManage dashboard with the following key information:

- System Status:** vSmart - 2, vEdge - 6 (highlighted with a red box), vBond - 2, vManage - 1. Reboot status: Last 24 hrs, 13. Warnings: 0 Invalid.
- Control Status (Total 8):** Control Up: 8, Partial: 0, Control Down: 0.
- Site Health View (Total 3):** Full Connectivity: 3 sites, Partial Connectivity: 0 sites, No Connectivity: 0 sites.
- vEdge Inventory:** Total: 7, Authorized: 7, Deployed: 6, Staging: 0.
- vEdge Health (Total 6):** Normal: 6, Warning: 0, Error: 0.
- Transport Interface Distribution:** < 10 Mbps: 16, 10 Mbps - 100 Mbps: 0, 100 Mbps - 500 Mbps: 0, > 500 Mbps: 0.
- Transport Health:** Graph showing 100% health.
- Application-Aware Routing:**

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
BR1-VEEDGE2:mpls-10.4.0.1:mpls	1.252	2.912	0.007
DC1-VEEDGE2:biz-internet-DC2-VEEDGE1:biz-inte...	1.174	2.585	0.074
10.4.0.1:mpls-DC1-VEEDGE2:mpls	1.108	1.578	0.036
10.4.0.1:mpls-DC2-VEEDGE2:mpls	0.983	1.459	0.014
10.4.0.1:mpls-DC2-VEEDGE1:mpls	1.003	1.431	0.017
- Top Applications:** Bar chart showing usage for various applications.

Click on “Configuration” icon and select “Templates” from the drop-down menu.



Various templates are shown. Now we will select the template named BranchType2 for this remote site.

This preconfigured template is how a customer would setup a template to use in a process where they are rolling out new branches.

Click on the three dots (...) in the right most column and from the drop down select the option “Attach Devices”.

The screenshot shows the Viptela vManage web interface. The browser address bar indicates the URL is `https://198.18.1.10/#/app/config/template/device`. The page title is "CONFIGURATION | TEMPLATES". Below the title, there are tabs for "Device" and "Feature". A "Create Template" button is visible. A search bar with "Search Options" is present. The main content is a table with the following data:

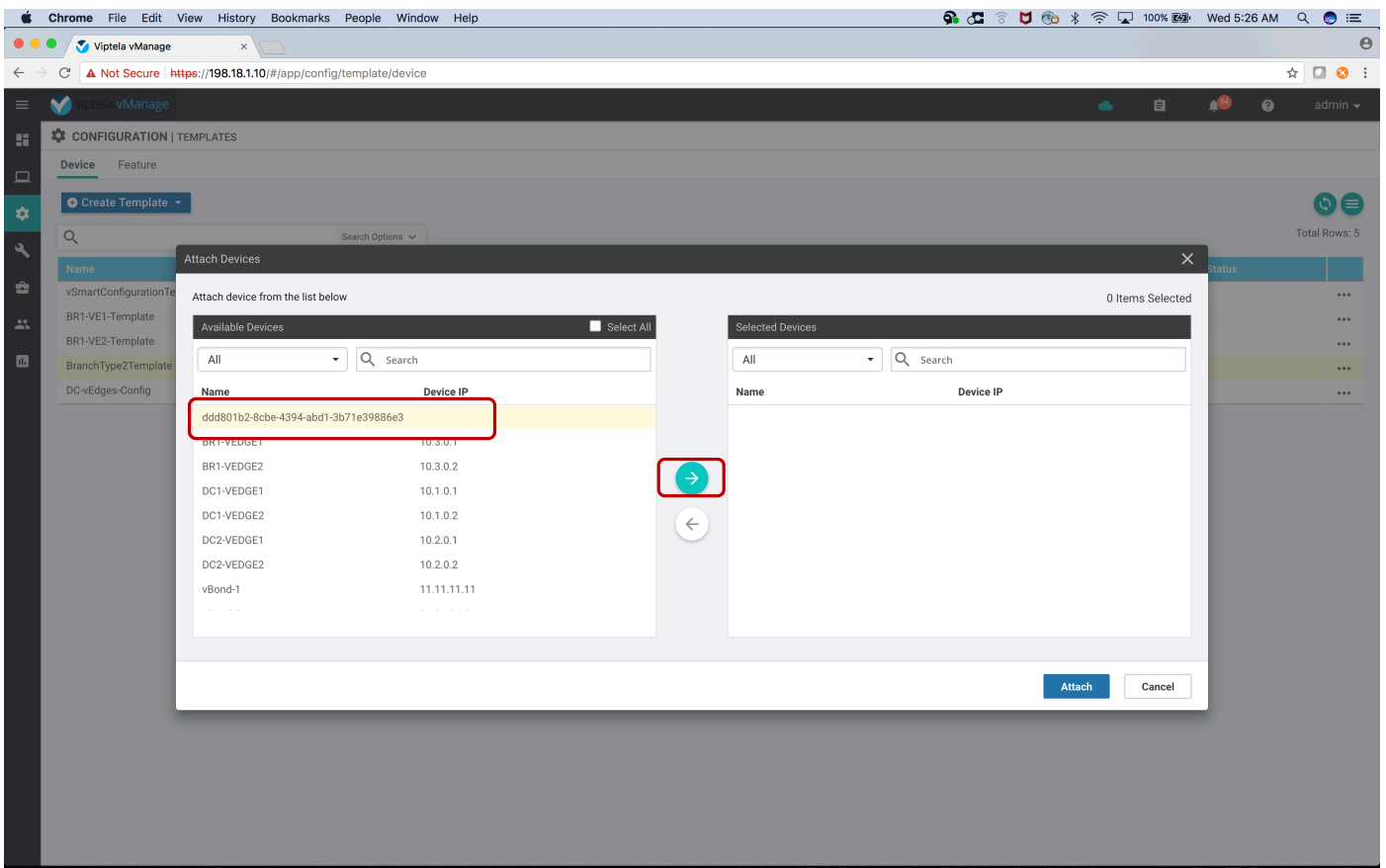
Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Device Status	
vSmartConfigurationTe...	Config template for vS...	CLI	vSmart	0	2	admin	11 Dec 2017 2:29:02 AM ...	In Sync	...
BR1-VE1-Template	Branch1 vEdge1 Templ...	CLI	vEdge Cloud	0	1	admin	11 Dec 2017 1:54:37 AM ...	In Sync	...
BR1-VE2-Template	Branch1 vEdge2 Templ...	CLI	vEdge Cloud	0	1	admin	11 Dec 2017 1:53:52 AM ...	In Sync	...
BranchType2Template	Branch Type 2 Device T...	Feature	vEdge Cloud	20	0	admin	04 Dec 2017 5:45:33 AM ...	In Sync	...
DC-vEdges-Config	DCs with FW Service	Feature	vEdge Cloud	18	4	admin	03 Dec 2017 12:24:05 PM...	In Sync	...

The context menu for the highlighted row includes the following options: Edit, View, Delete, Copy, Attach Devices (highlighted with a red box), and Export CSV.

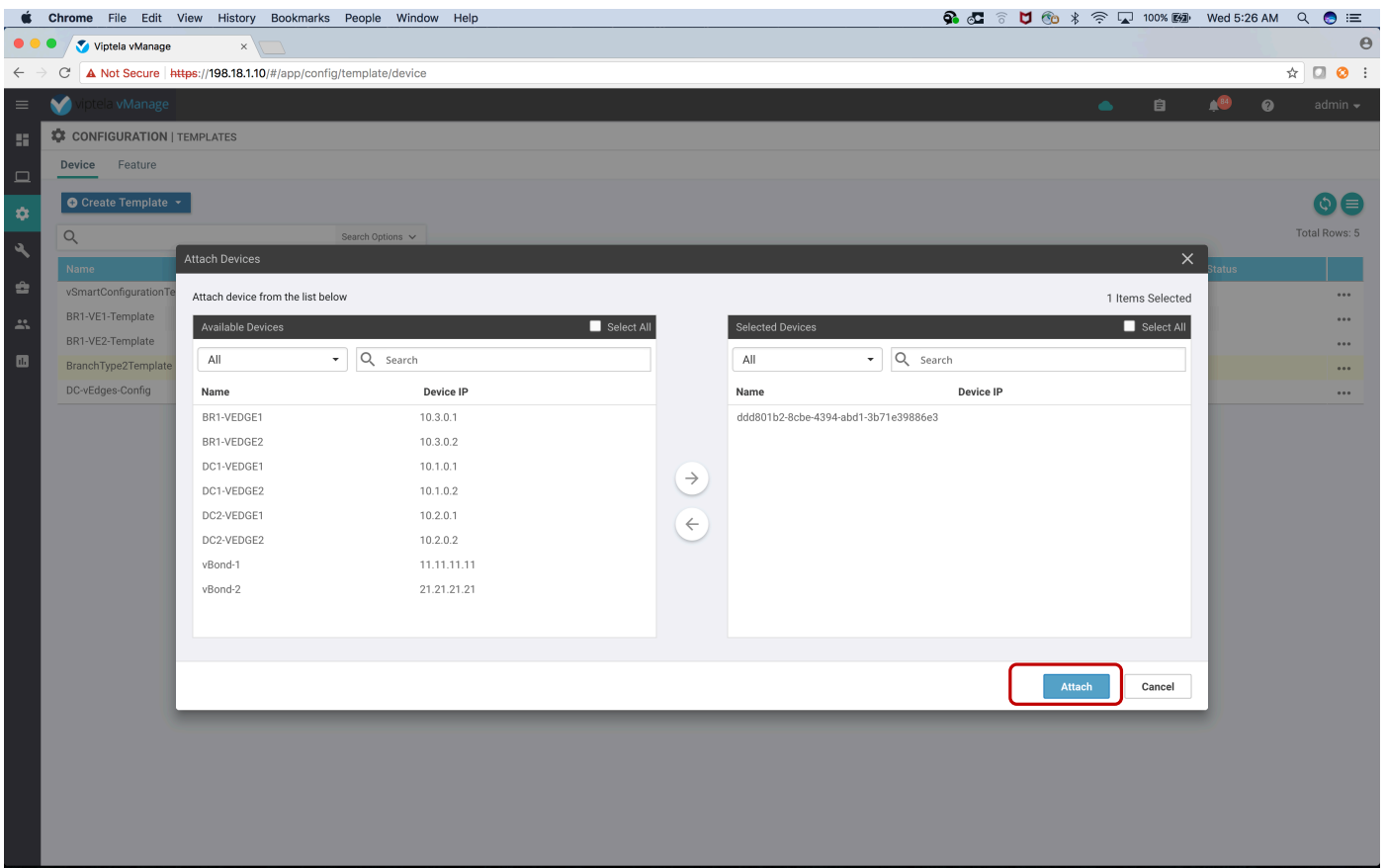
From the left pane labeled Available Devices find the device with chassis-id/UUID of `ddd801b2-8cbe-4394-abd1-3b71e39886e3`.

Select this device that has not been provisioned.

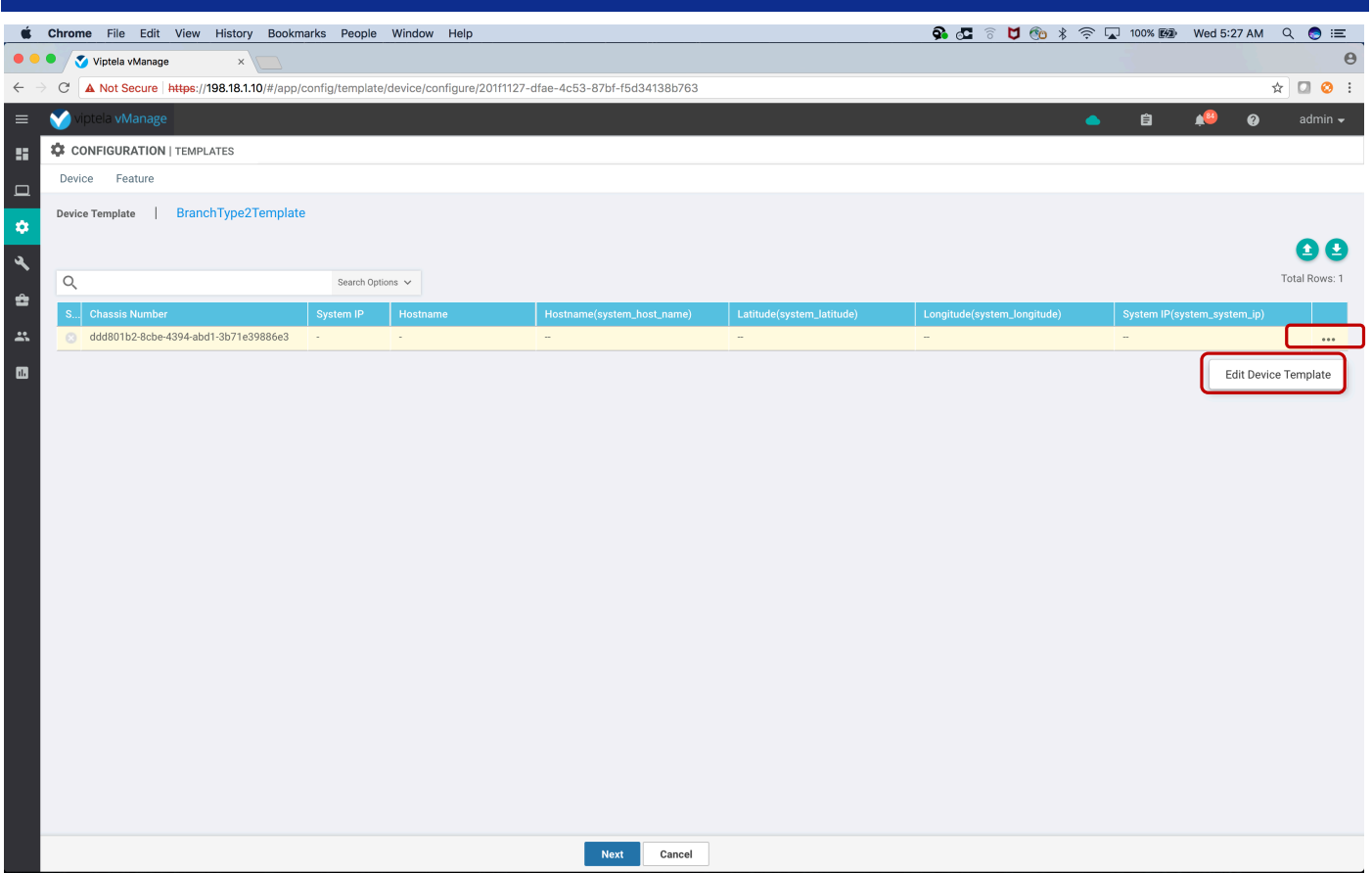
Move the selected device to the right pane labeled "Selected Devices" by clicking on the right arrow button.



Once the device is moved to the right pane, click on "Attach" button.



Click on the dots (...) in the right most column and select "Edit Device Template".



The “Edit Device Template” provides an option to update the variables values associated with the Branch2 vEdge.

One can fill this form out and click on “Update” button.

There is another method where one can upload a CSV file with the fields value already populated.

We will be using the method of CSV file in this demo.

Click the “Cancel” button to go back to the previous page.

Update Device Template

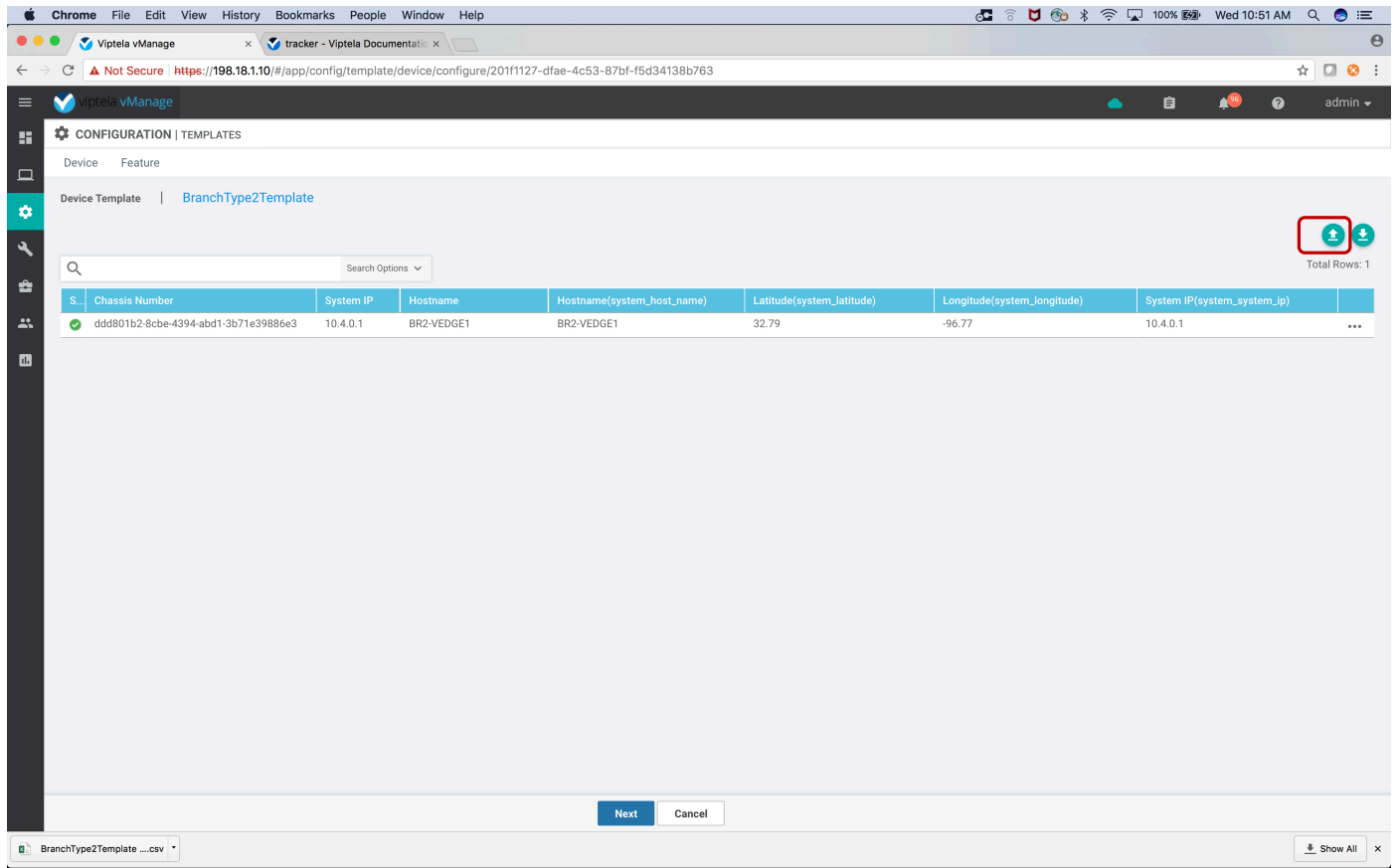
Variable List (Hover over each field for more information)

Chassis Number	ddd801b2-8cbe-4394-abd1-3b71e39886e3
System IP	-
Hostname	
Hostname(system_host_name)	
Latitude(system_latitude)	
Longitude(system_longitude)	
System IP(system_system_ip)	
Site ID(system_site_id)	
Address(MPLS-GW-IP)	
IPv4 Address(MPLS-TLOC-IP)	
Address(VPN512-GW-IP)	
IPv4 Address(VPN512-Interface-IP)	
IPv4 Address(VPN10-Interface-IP)	
IPv4 Address(VPN20-Interface-IP)	
IPv4 Address(VPN40-IP-Address)	

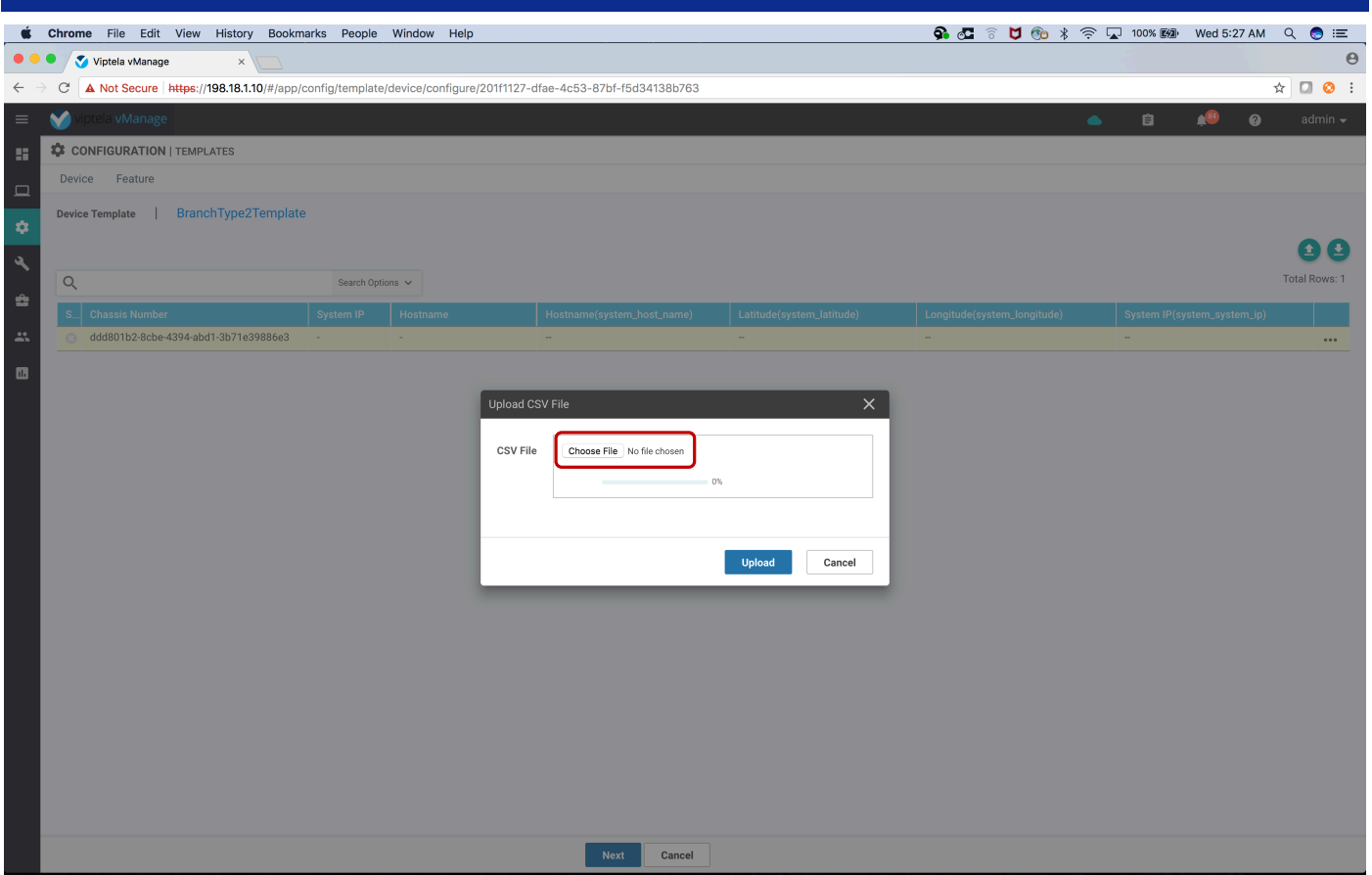
Update Cancel



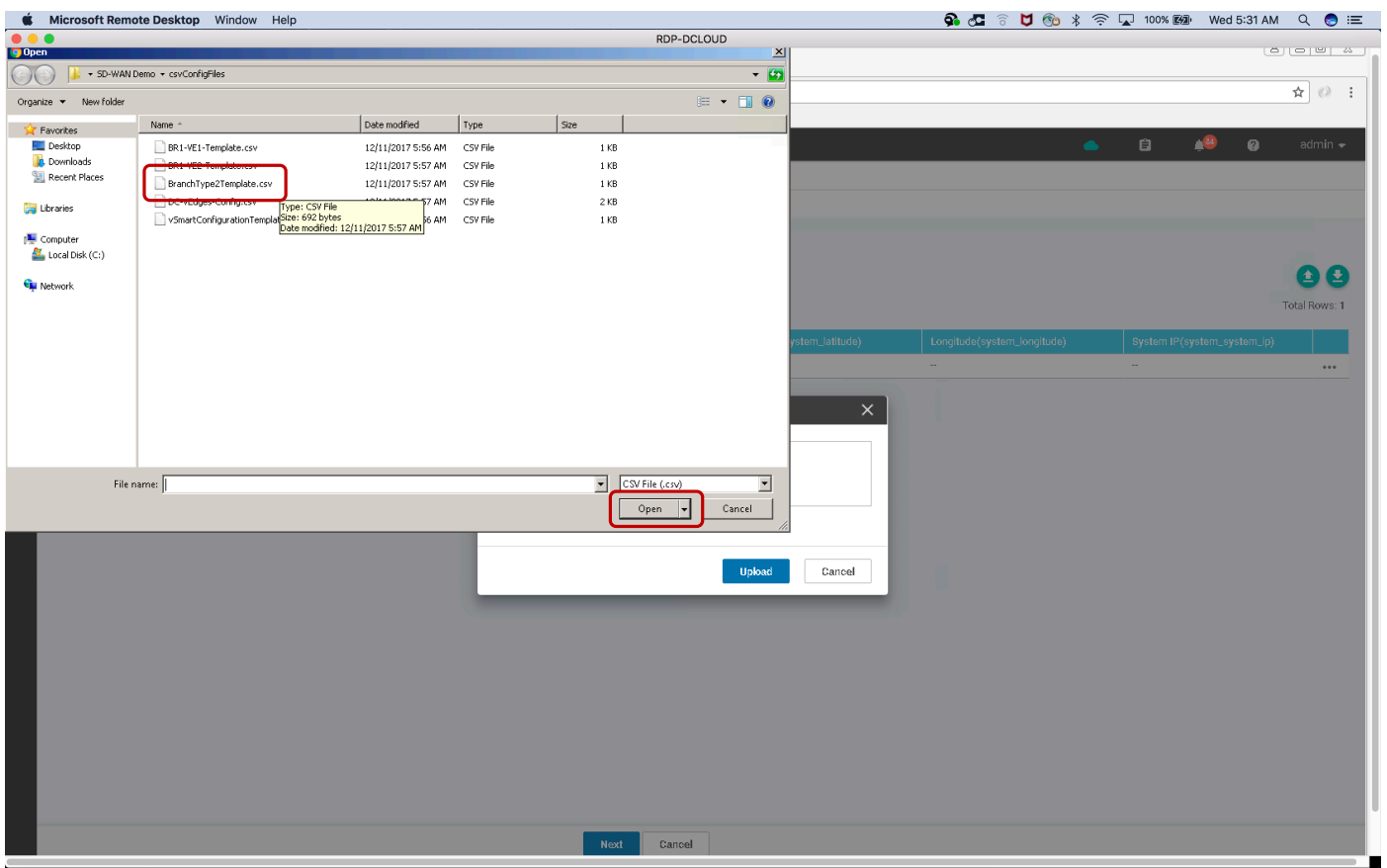
Click on the upload icon (  ) for uploading the CSV file.



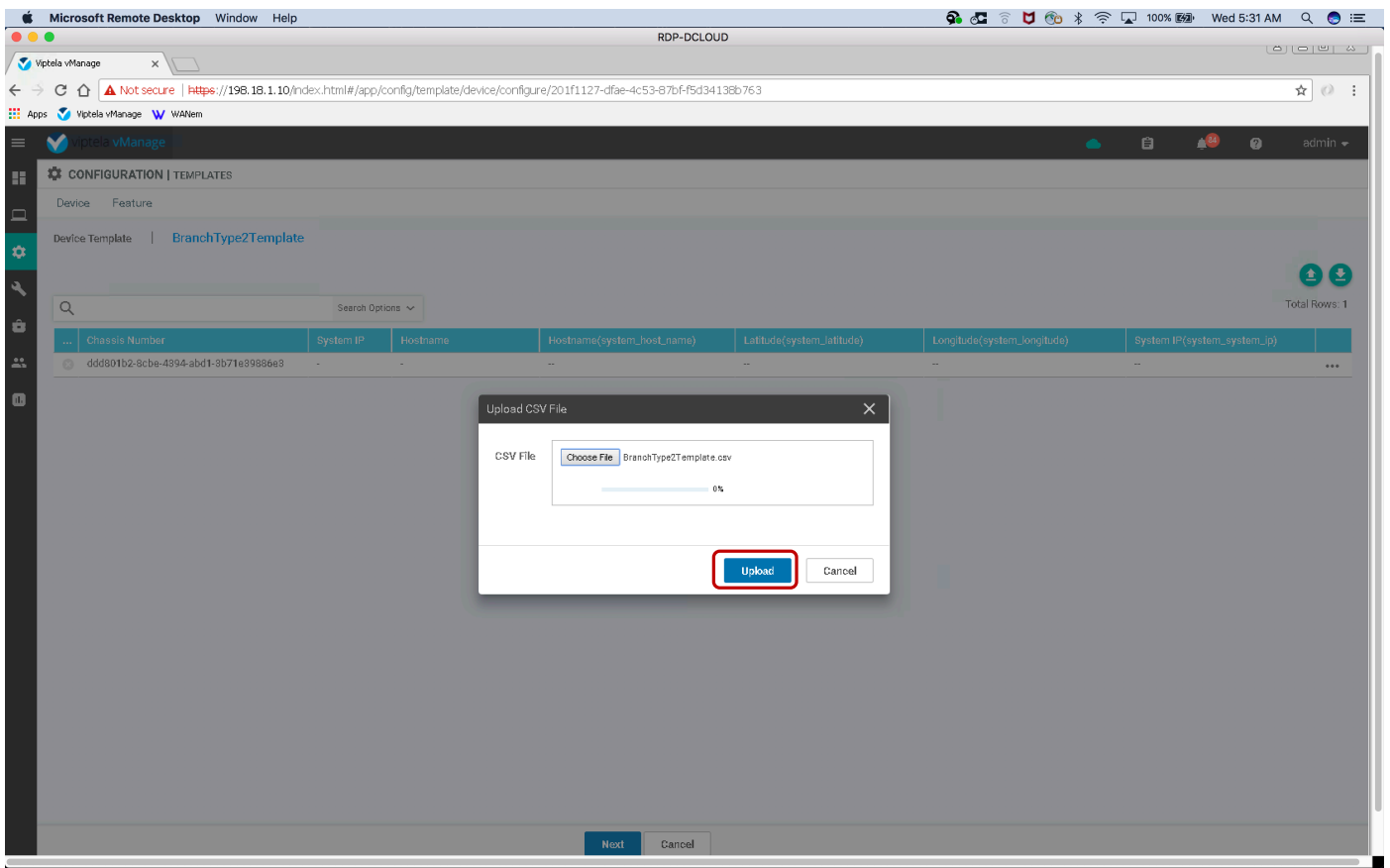
Click on the "Choose File" button.



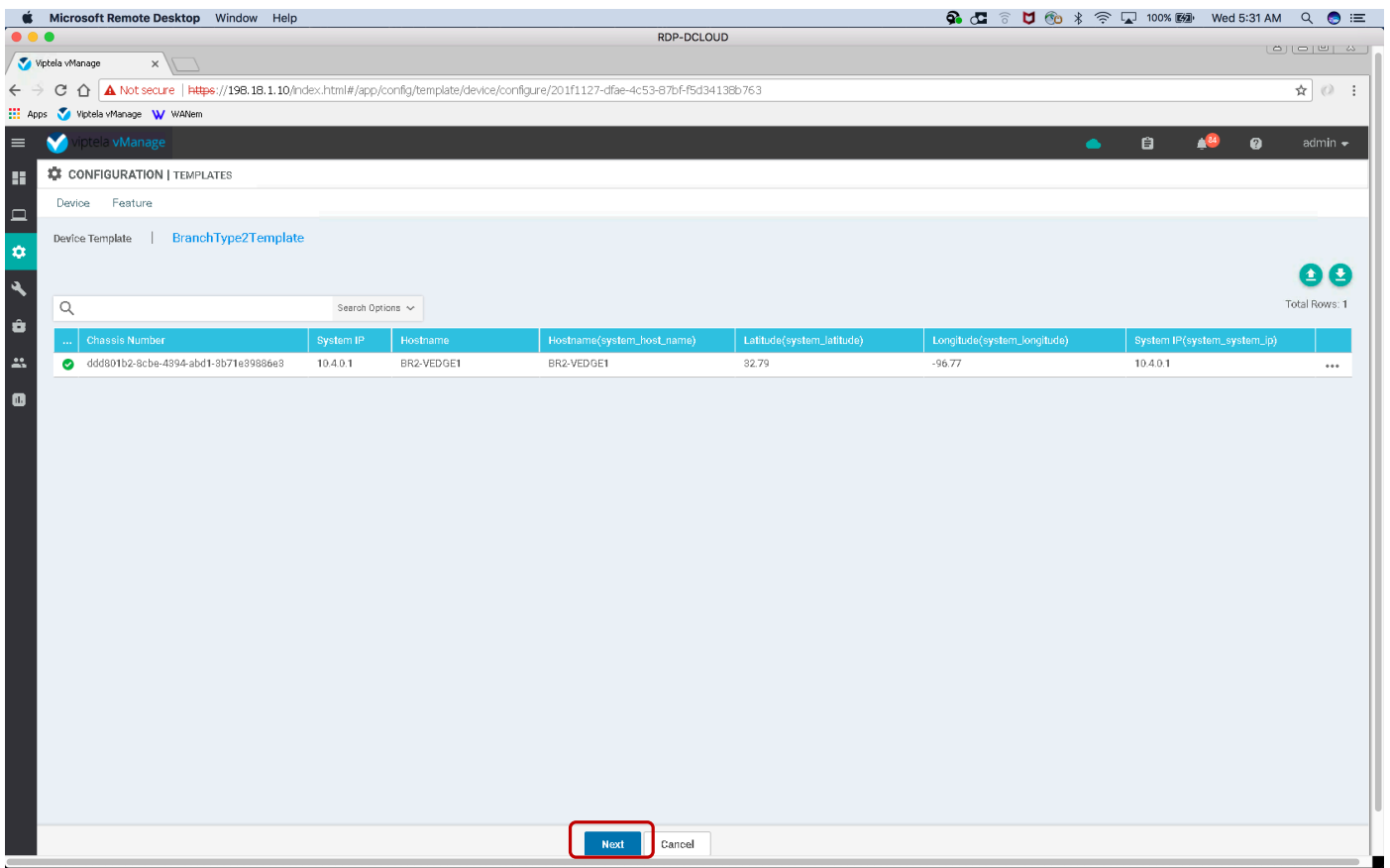
Prebuilt CSV file is located in the folder `\\Desktop\SD-WAN Demo\csvConfigFiles` on Workstation 1. The name of the file is "BranchType2Template.csv". In the popup window select the file `BranchType2Template.csv`. Click on the "Open" button.



On the next screen click on "Upload" button.



On the next screen, click on "Next" button. You will see the values for the variables are filled up based on the uploaded CSV file.



You may click on the tab in the left column with BR2-VEDGE1 label to see the full CLI configuration for validation.

Click on "Configure Devices".

Microsoft Remote Desktop Window Help RDP-DCLLOUD

Not secure https://198.18.1.10/index.html#/app/config/template/device/configure/201f1127-dfae-4c53-87bf-f5d34138b763

Viptela vManage admin

CONFIGURATION | TEMPLATES

'Configure' action will be applied to 1 device(s) attached to 1 device template(s).

Device Template	Total
BranchType2Template	1

Device List (Total: 1 devices)

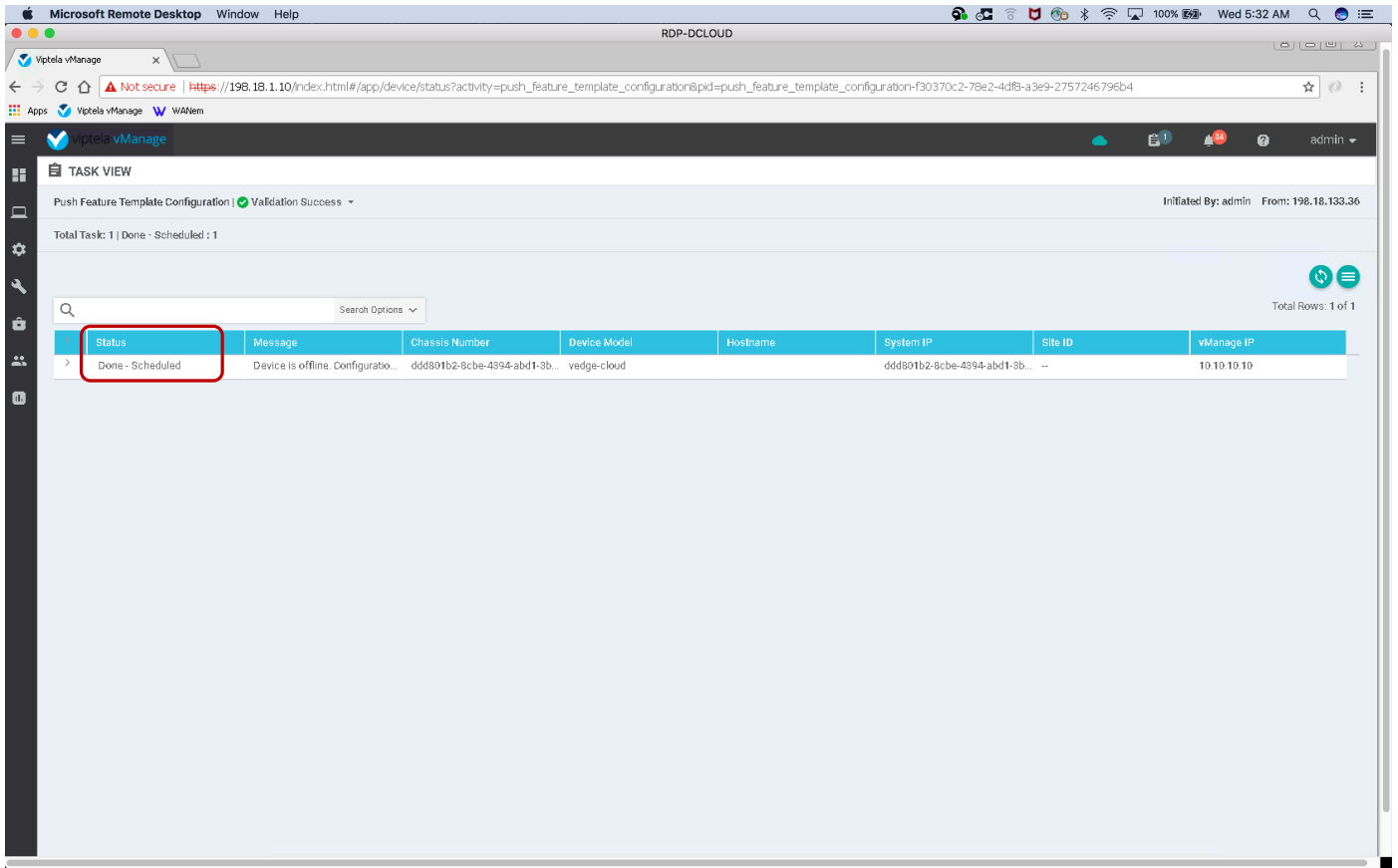
Filter/Search

ddid801b2-8cbe-4394-abd1-3b71a39886e3 BR2-VEGE110.4.0.1
--

```
bfd app-route poll-interval 5000
system
device-model vedge-cloud
host-name BR2-VEGE1
gps-location latitude 32.79
gps-location longitude -96.77
system-ip 10.4.0.1
domain-id 1
site-id 400
no route-consistency-check
organization-name "Cisco Sys1 - 19968"
vbond vbond.cisco.com port 12346
aaa
auth-order local radius tacacs
usergroup basic
task system read write
task interface read write
!
usergroup netadmin
!
usergroup operator
task system read
task interface read
task policy read
task routing read
task security read
!
user admin
password $6sIwK8Q==$wT21Ua985rE0PI6g8s14E6PA7wX@Nbgv/wh38F1C6sMdzRazdxorYYTLrL6syIG6qnlABTnrE96H3IKFQQRq1
!
logging
disk
enable
!
```

Back **Configure Devices** Cancel

Wait for few seconds till the device Status changes from “In Progress” to “Done – Scheduled”.



Click on vManage dashboard icon. The dashboard icon will show that 6 vEdges are operational.

Chrome File Edit View History Bookmarks People Window Help  
Viptela vManage  
Not Secure https://198.18.1.10/index.html#/app/dashboard

admin

### DASHBOARD

2 ↑  
vSmart - 2

6 ↑  
vEdge - 6

2 ↑  
vBond - 2

1 ✓  
vManage - 1

Reboot 13  
Last 24 hrs

Warning 0  
Invalid 0

#### Control Status (Total 8)

Control Up	8
Partial	0
Control Down	0

#### Site Health View (Total 3)

Full Connectivity	3 sites
Partial Connectivity	0 sites
No Connectivity	0 sites

#### Transport Interface Distribution

< 10 Mbps	16
10 Mbps - 100 Mbps	0
100 Mbps - 500 Mbps	0
> 500 Mbps	0

[View Percent Utilization](#)

#### vEdge Inventory

Total	7
Authorized	7
Deployed	6
Staging	0

#### vEdge Health (Total 6)

6

Normal

0

Warning

0

Error

#### Transport Health

Type: By Loss

#### Top Applications

DPI Flows

#### Application-Aware Routing

Type: By Loss

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
BR1-VEGE2:mpls-10.4.0.1:mpls	1.252	2.912	0.007
DC1-VEGE2:biz-internet-DC2-VEGE1:biz-inte...	1.174	2.585	0.074
10.4.0.1:mpls-DC1-VEGE2:mpls	1.108	1.578	0.036
10.4.0.1:mpls-DC2-VEGE2:mpls	0.983	1.459	0.014
10.4.0.1:mpls-DC2-VEGE1:mpls	1.003	1.431	0.017

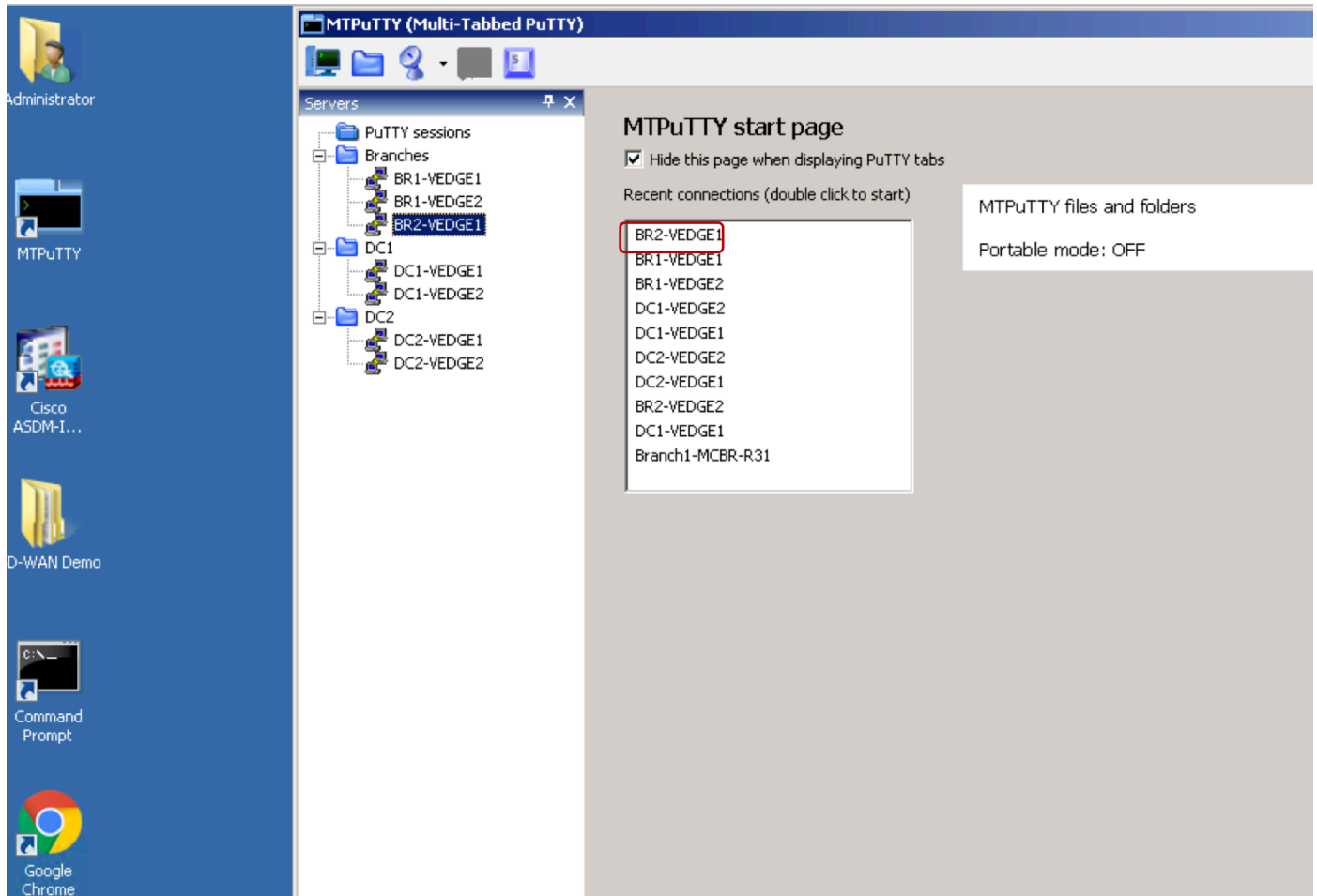


To simulate the device to be connected to the transport for ZTP, we will do “no shut” on the interface connected to Internet transport in the lab [interface ge0/0].

On the desktop of Wkst1 launch the MTPuTTY application.

Double click the BR2-VEDGE1 device.

You will be automatically logged in.



Issue the following commands to the BR2-vEdge1 CLI:

```
show run system
```

Note the default configuration for the system block with vbond pointing to ztp.viptela.com and no system-ip, site-id and organization name.

```
show run vpn 0
```

Note that the interface is in a shutdown state. This is the logical interface that the router uses to talk to the management and controller.

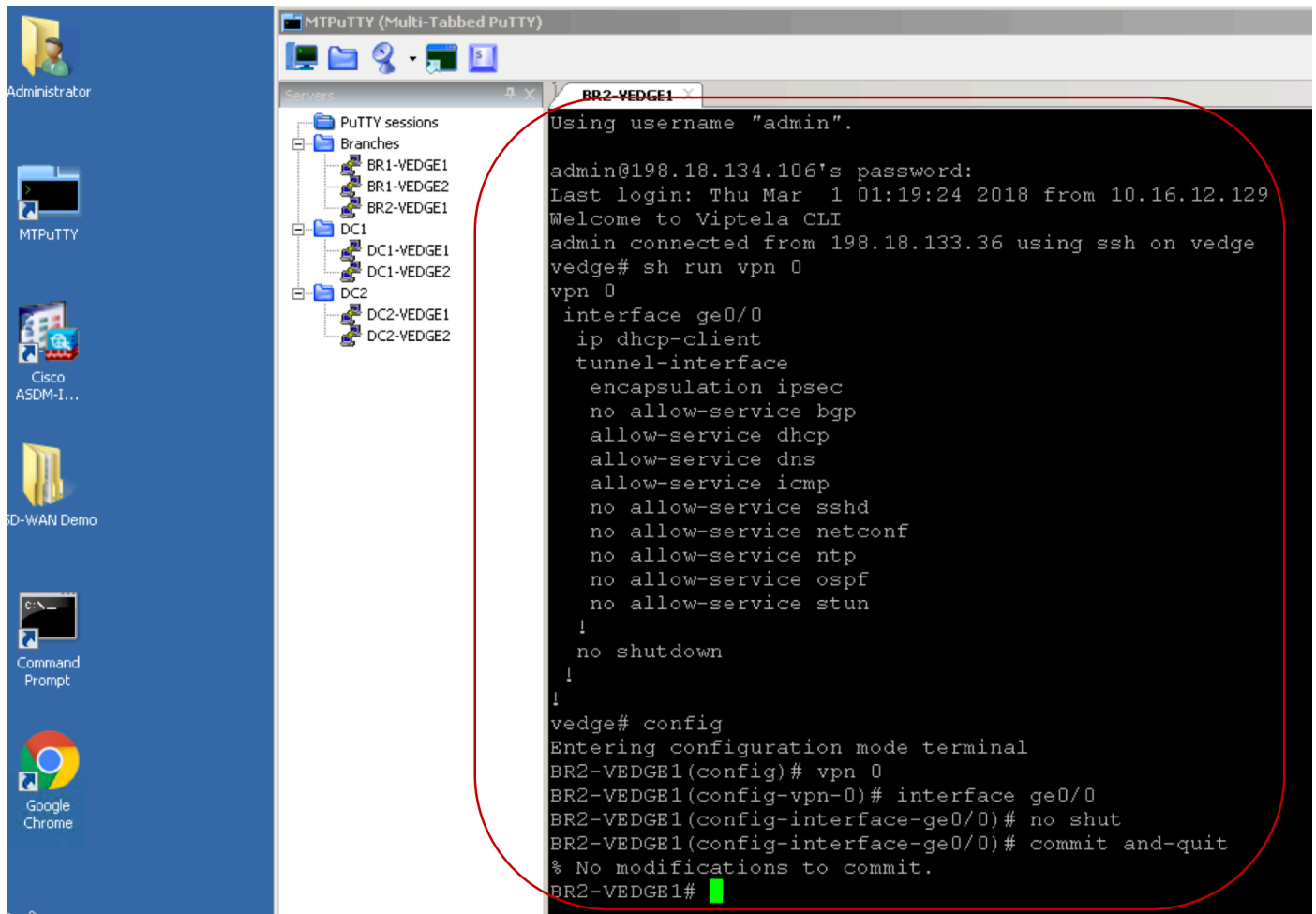
```
show run vpn 10
```

The interface is not found because the configuration has not been downloaded to the device yet for vpn 10, 20 and 40.

Now we will enable the interface so that the router can do the ZTP simulation.

```
config
vpn 0
interface ge0/0
no shut
commit and-quit
```

From the output, you will see that the device has default configuration for transport VPN 0 and no configuration for service/LAN side VPN 10.

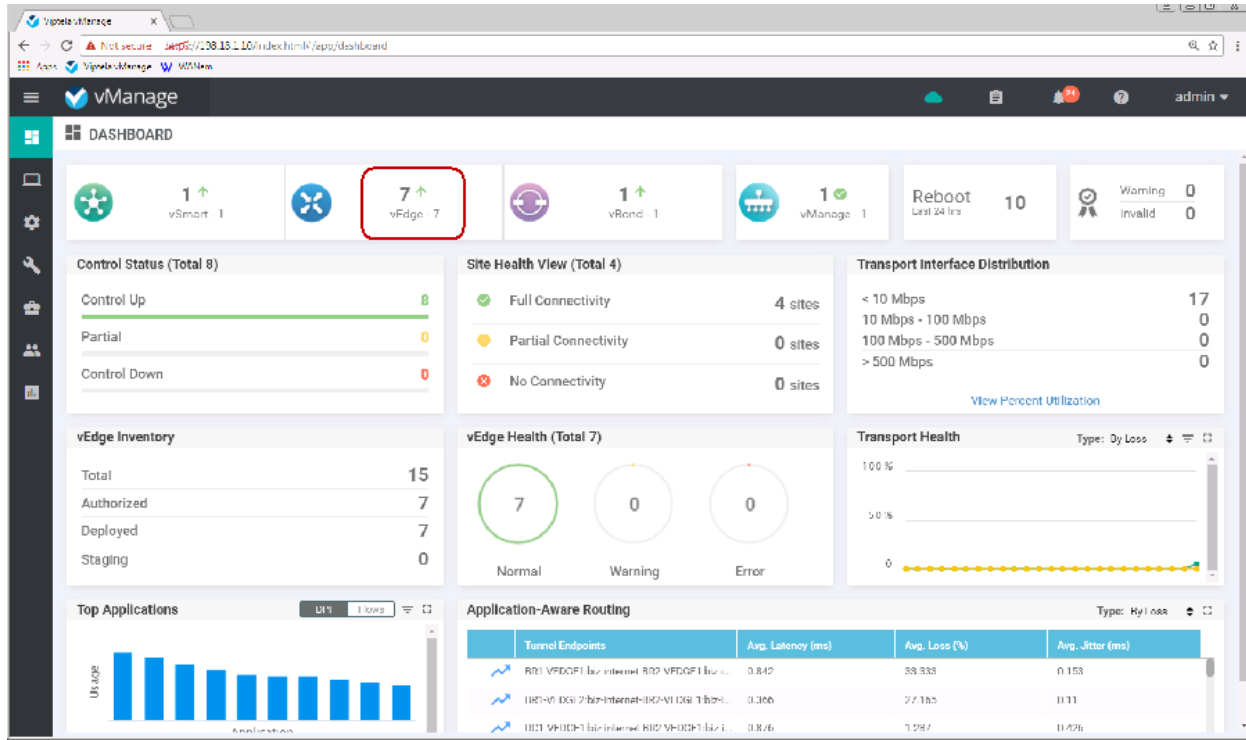


Issue the following command:

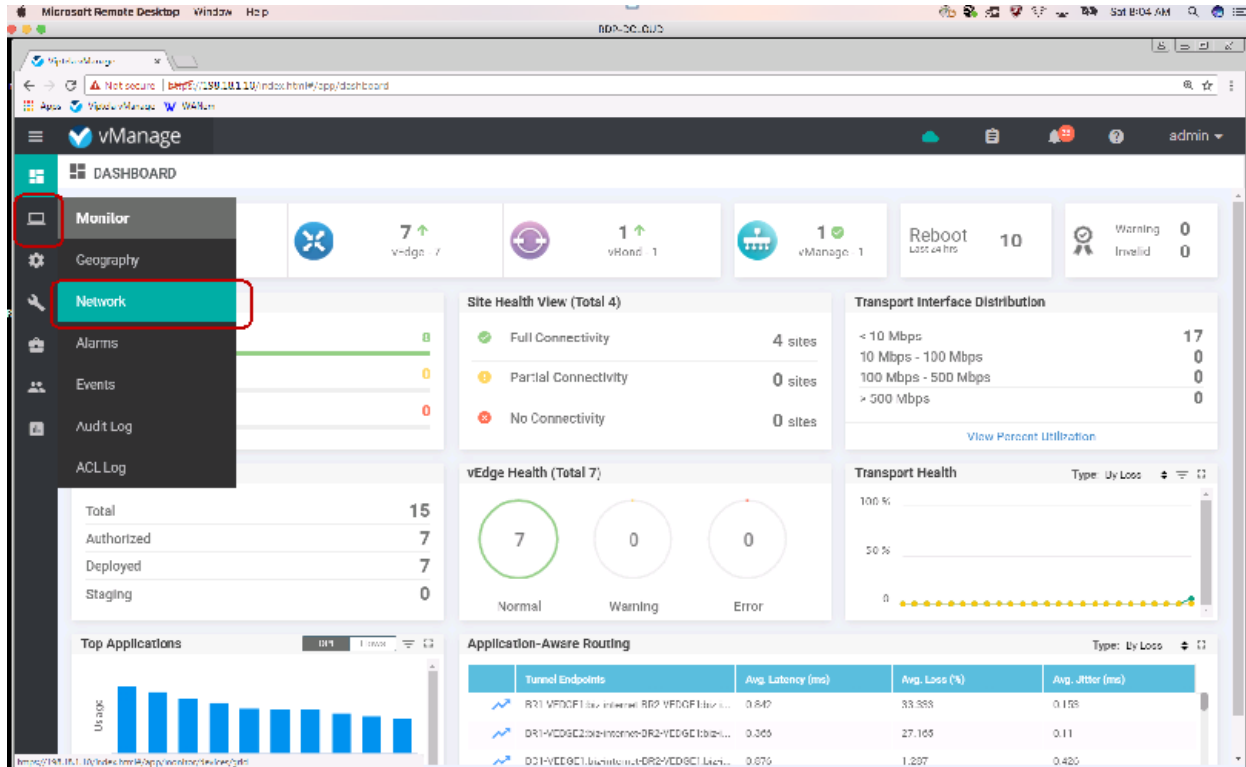
```

show run system
show run vpn 0
show run vpn 10
config t
vpn 0
interface ge0/0
no shutdown
commit and-quit
  
```

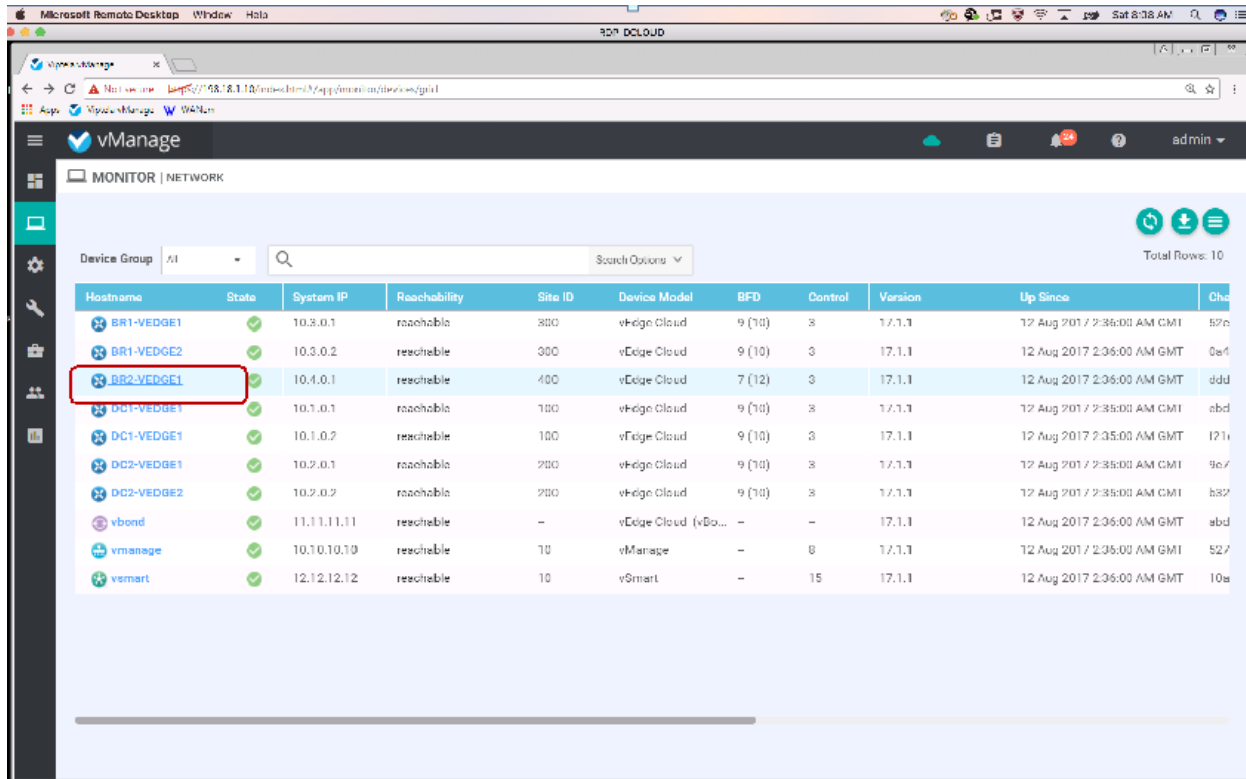
Go back to the vManage dashboard. The BR2-VEEDGE1 will come up and the dashboard will show total of 7 vEdges are operational.



Click on Monitor icon and then select Network.



Select BR2-VEDGE1 from the list. You will be taken to device dashboard for BR2-VEDGE2.

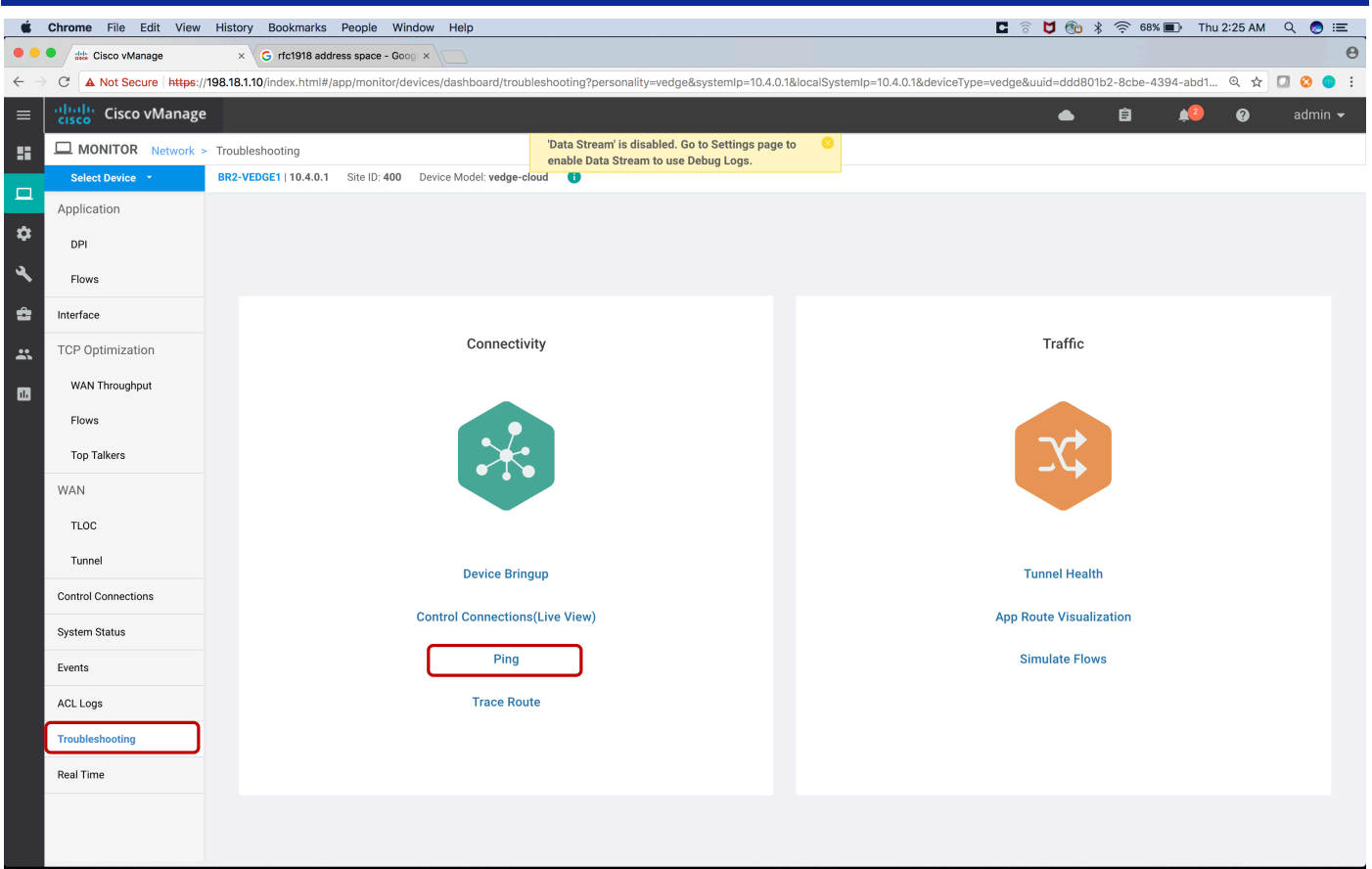


Click on Control Connections. Validate control sessions are established to vSmart and vManage.

The screenshot shows the Cisco vManage interface for device BR2-VEEDGE1. The 'Control Connections' section displays two network diagrams: one for 'mpls' and one for 'biz-internet'. Below the diagrams is a table listing the control connections.

Peer Type	Peer System IP	Peer Protocol	Private Port	Public Port	Controller Group ID	
mpls	--	--	--	--	--	--
vsmart	22.22.22.22	dtls	12446	12446	0	23 Dec 2017 2:29:10 PM HST
vsmart	12.12.12.12	dtls	12446	12446	0	23 Dec 2017 2:29:10 PM HST
vmanage	10.10.10.10	dtls	12446	12446	0	26 Dec 2017 5:32:54 AM HST
biz-internet	--	--	--	--	--	--
vsmart	22.22.22.22	dtls	12446	12446	0	23 Dec 2017 2:29:10 PM HST
vsmart	12.12.12.12	dtls	12446	12446	0	23 Dec 2017 2:29:10 PM HST

At this time, there is no policy defined for the overlay and hence we have full-mesh connectivity across all three VPNs (10, 20, 40). To validate the IP connectivity, from device dashboard click on "Troubleshooting" and then select "Ping" on the next screen.



Use the following IP addresses for validating IP connectivity.

Site	VPN 10 Test IP	VPN 20 Test IP	VPN 40 Test IP
DC1	198.18.133.21	10.1.20.10	N/A
DC2	10.2.0.21	10.2.20.10	N/A
Branch 1	10.3.0.10	10.3.20.10	10.3.40.10
Branch 2	10.4.0.10	10.4.20.10	10.4.40.10

Put in destination (198.18.133.21) for DC1, (10.2.0.21) for DC2, (10.3.0.10) for Branch 1 and (10.4.0.10) for Branch 2 in VPN 10. Select VPN 10 (the Corporate VPN) from the drop-down menu and select Source Interface from drop down menu. Click on Ping button.

The screenshot shows the Cisco vManage Troubleshooting interface. The configuration for a ping test is as follows:

- Destination IP\*: 198.18.133.21
- VPN: VPN - 10
- Source/Interface for VPN - 10: ge0/2 - ipv4 - 10.4.254.10
- Probes:  ICMP,  TCP,  UDP
- Source Port: [Empty]
- Destination Port: [Empty]
- Type Of Service: [Empty]
- Time To Live: [Empty]
- Don't Fragment:

The results of the ping test are shown in the Summary and Output sections:

Summary	
Packets Transmitted	5
Packets Received	4
Packet loss (%)	20
Round Trip Time	
Min (ms)	0.032
Max (ms)	0.059
Avg (ms)	0.046

**Output:**  
Nping in VPN 10  
Starting Nping 0.6.47 ( http://nmap.org/nping ) at 2017-12-28 12:29 UTC  
SENT (0.0246s) ICMP [10.4.254.10 > 198.18.133.21 Echo request (type=8/code=0) id=53579 seq=1] IP [ttl=64 id=33952 iplen=28 ]  
SENT (1.0248s) ICMP [10.4.254.10 > 198.18.133.21 Echo request (type=8/code=0) id=53579 seq=2] IP [ttl=64 id=33952 iplen=28 ]  
RCVD (1.0249s) ICMP [198.18.133.21 > 10.4.254.10 Echo reply (type=0/code=0) id=53579 seq=1] IP [ttl=63 id=62144 iplen=28 ]  
SENT (2.0260s) ICMP [10.4.254.10 > 198.18.133.21 Echo request (type=8/code=0) id=53579 seq=3] IP [ttl=64 id=33952 iplen=28 ]  
RCVD (2.0261s) ICMP [198.18.133.21 > 10.4.254.10 Echo reply (type=0/code=0) id=53579 seq=2] IP [ttl=63 id=62384 iplen=28 ]  
SENT (3.0271s) ICMP [10.4.254.10 > 198.18.133.21 Echo request (type=8/code=0) id=53579 seq=4] IP [ttl=64 id=33952 iplen=28 ]  
RCVD (3.0273s) ICMP [198.18.133.21 > 10.4.254.10 Echo reply (type=0/code=0) id=53579 seq=3] IP [ttl=63 id=62518 iplen=28 ]  
SENT (4.0280s) ICMP [10.4.254.10 > 198.18.133.21 Echo request (type=8/code=0) id=53579 seq=5] IP [ttl=64 id=33952 iplen=28 ]  
RCVD (4.0281s) ICMP [198.18.133.21 > 10.4.254.10 Echo reply (type=0/code=0) id=53579 seq=4] IP [ttl=63 id=62726 iplen=28 ]  
Max rtt: 0.059ms | Min rtt: 0.032ms | Avg rtt: 0.046ms  
Raw packets sent: 5 (140B) | Rcvd: 4 (112B) | Lost: 1 (20.00%)  
Nping done: 1 IP address pinged in 4.04 seconds

From the device dashboard, one can view application flows, IPFIX flow records, interface stats and others from the device dashboard.

## DPI

Click on DPI from the device dashboard.

## IPFIX Flow Records

From device dashboard click on “Flows” and will see the IPFIX flow records.

## Interface Stats

From the device dashboard click on “Interfaces” to see utilization of the links on the vEdge.

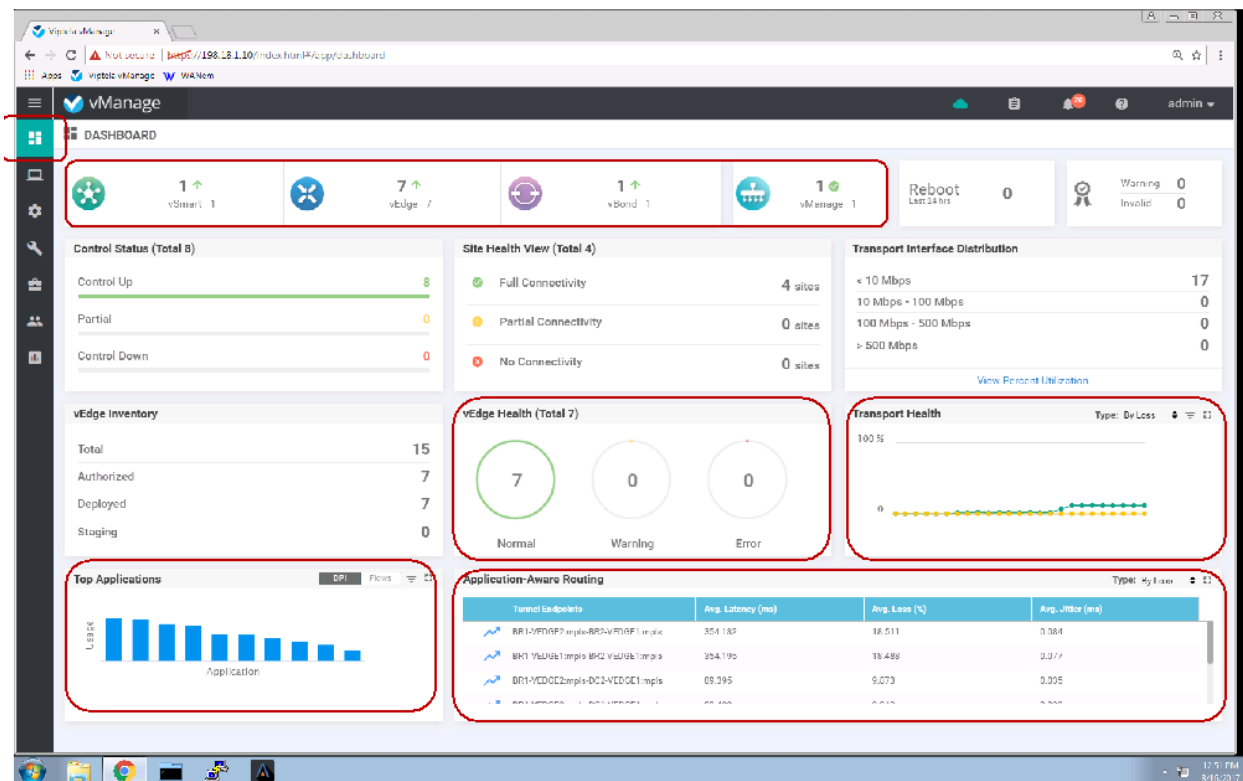
Below is the table showing how the interfaces are mapped to different functions on different devices.



VEDGES	Internet TLOC	MPLS TLOC	VPN10 Interface	VPN20 Interface	VPN40 Interface
DC VEDGES	ge0/2	ge0/1	ge0/0	ge0/3	N/A
BR1-VEDGE1	ge0/1	ge0/0	ge0/3	ge0/4	ge0/5
BR1-VEDGE2	ge0/0	ge0/2	ge0/3	ge0/4	ge0/5
BR2-VEDGE1	ge0/0	ge0/1	ge0/2	ge0/3	ge0/4

Click on the vManage dashboard icon:

- Up/Down Status of ALL Viptela components
- vEdge Health
- Applications/Flow Visibility
- Transport Health Visibility



# Lab 02 - Strict Hub-n-Spoke Topology

Enterprise may not need a full mesh topology and would like to have a pure Hub-n-Spoke IPsec/BFD topology. A simple policy activation will convert full mesh connectivity to Strict Hub-n-Spoke.

In this case we will create a fabric with IPsec tunnels only getting established between the spokes and the DCs. Based on policy we will not establish any IPsec tunnels between the Branches.

For corporate VPN 10, we will only advertise the Branches' routes to the DCs and not to other Branches. The DCs are advertising default routes and hence when a branch needs to talk to other branches, they will take the default to the DCs. The DC vEdges then route the traffic back to the other remote Branches.

For PCI/IOT segment (VPN 20), we will advertise the routes between the Branches by setting the next-hop pointing to the DCs TLOCs. This is being done to provide Hub-n-Spoke communication between the Branches through the DCs as there is no default route being advertised from the DCs.

For guest WiFi VPN 40, we don't need any communication between the branches. We will restrict the route exchange between sites for VPN 40. There will be only one static default route in VPN 40 providing direct internet access.

## Steps

Go to vManage dashboard. Click on the Monitor icon and click on "Network" from the drop down.

The screenshot shows the Viptela vManage dashboard. The 'Monitor' menu is open, and 'Network' is selected. The dashboard displays various health and performance metrics:

- Dashboard Summary:** 7 vEdge, 2 vBond, 1 vManage, 0 Reboot, 0 Warning/Invalid.
- Site Health View (Total 4):** Full Connectivity (4 sites), Partial Connectivity (0 sites), No Connectivity (0 sites).
- Transport Interface Distribution:** < 10 Mbps (16), 10 Mbps - 100 Mbps (0), 100 Mbps - 500 Mbps (0), > 500 Mbps (0).
- vEdge Health (Total 7):** 7 Normal, 0 Warning, 0 Error.
- Transport Health:** Line graph showing 100% health.
- Top Applications:** Bar chart showing usage for various applications.
- Application-Aware Routing:** Table showing tunnel endpoints, latency, and loss.

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)
BR1-VEGE1:mpls-10.4.0.1:mpls	0.998	4.596
10.4.0.1:mpls-BR1-VEGE1:mpls	0.909	4.149
BR1-VEGE2:mpls-10.4.0.1:mpls	1.153	4.043
10.4.0.1:mpls-BR1-VEGE2:mpls	1.051	4.000

Find BR2-VEDGE1 and click on the name.

The screenshot shows the Viptela vManage interface in a Chrome browser window. The page title is 'MONITOR | NETWORK'. A search bar is present above a table of devices. The table has 12 columns: Hostname, State, System IP, Reachability, Site ID, Device Model, BFD, Control, Version, Up Since, and Chassis Number/ID. The row for 'BR2-VEDGE1' is highlighted with a red box. Below the table, there is a download button for a CSV file named 'BranchType2Template ...csv' and a 'Show All' button.

Hostname	State	System IP	Reachability	Site ID	Device Model	BFD	Control	Version	Up Since	Chassis Number/ID	De
BR1-VEDGE1	✓	10.3.0.1	reachable	300	vEdge Cloud	10	5	17.1.4	12 Dec 2017 8:29:00 AM PST	52c7911f-c5b0-45df-b826-315580...	No
BR1-VEDGE2	✓	10.3.0.2	reachable	300	vEdge Cloud	10	5	17.1.4	12 Dec 2017 8:29:00 AM PST	0a4a4c78-35a8-4c1c-bbd2-e0251...	No
BR2-VEDGE1	✓	10.4.0.1	reachable	400	vEdge Cloud	12	5	17.1.4	12 Dec 2017 8:29:00 AM PST	ddd801b2-8cbe-4394-abd1-3b71e...	No
DC1-VEDGE1	✓	10.1.0.1	reachable	100	vEdge Cloud	10	5	17.1.4	12 Dec 2017 8:28:00 AM PST	ebdc8bd9-17e5-4eb3-a5e0-f4384...	No
DC1-VEDGE2	✓	10.1.0.2	reachable	100	vEdge Cloud	10	5	17.1.4	12 Dec 2017 8:28:00 AM PST	f21dbb35-30b3-47f4-93bb-d2b2fe...	No
DC2-VEDGE1	✓	10.2.0.1	reachable	200	vEdge Cloud	10	5	17.1.4	12 Dec 2017 8:28:00 AM PST	9e785ad7-558a-40c6-b0c0-fcc96e...	No
DC2-VEDGE2	✓	10.2.0.2	reachable	200	vEdge Cloud	10	5	17.1.4	12 Dec 2017 8:28:00 AM PST	b3265c5c-3db6-4d25-9d3b-1f416...	No
vBond-1	✓	11.11.11.11	reachable	-	vEdge Cloud (vBo...	-	-	17.1.4	12 Dec 2017 8:29:00 AM PST	abd5e9d7-9dee-4d00-98b5-fdc71...	No
vBond-2	✓	21.21.21.21	reachable	-	vEdge Cloud (vBo...	-	-	17.1.4	12 Dec 2017 8:30:00 AM PST	b6eec354-1d60-4c77-bb1a-7a704...	No
vManage	✓	10.10.10.10	reachable	10	vManage	-	9	17.1.4	12 Dec 2017 8:29:00 AM PST	5271ea7c-edb1-420b-be9a-4d257...	No
vSmart-1	✓	12.12.12.12	reachable	10	vSmart	-	16	17.1.4	12 Dec 2017 8:28:00 AM PST	10a98779-95f0-4383-871c-195d2...	No
vSmart-2	✓	22.22.22.22	reachable	20	vSmart	-	16	17.1.4	12 Dec 2017 8:30:00 AM PST	704bbc2f-aa9a-4068-84a2-fc3160...	No

Select Tunnels from the left column.

The next screen shows IPSec tunnels are established to the DCs and the remote Branch-1 (full mesh).

The screenshot displays the Cisco vManage interface for monitoring a WAN Tunnel. The top section shows a line chart of Loss Percentage (0% to 20%) over time (Dec 28, 01:55 to 02:40). A legend on the right lists tunnel endpoints with their corresponding colors. The bottom section shows a table of tunnel endpoints with 6 rows selected. The 'State' column is highlighted with a red box.

Tunnel Endpoints	Protocol	State	Jitter (ms)	Loss (%)	Latency (ms)	Total Tx Bytes
BR2-VEGGE1.mpls-DC1-VEGGE2.mpls	ipsec	↑	0.00	20.00	100.90	0B
BR2-VEGGE1.mpls-DC2-VEGGE2.mpls	ipsec	↑	0.00	20.00	100.96	0B
BR2-VEGGE1.mpls-BR1-VEGGE2.mpls	ipsec	↑	0.02	19.97	101.03	0B
BR2-VEGGE1.mpls-DC2-VEGGE2.mpls	ipsec	↑	0.00	20.00	100.97	924 B
BR2-VEGGE1.mpls-BR1-VEGGE1.mpls	ipsec	↑	0.00	19.97	100.94	0B
BR2-VFDGF1.mpls-DC1-VFDGF1.mpls	insec	↑	0.01	20.00	100.62	0B

From the device dashboard select “Troubleshooting” and then select “Traceroute”.


Chrome File Edit View History Bookmarks People Window Help  
Cisco vManage rfc1918 address space - Google  
Not Secure https://198.18.1.10/index.html#/app/monitor/devices/dashboard/troubleshooting?personality=vedge&systemip=10.4.0.1&localSystemip=10.4.0.1&deviceType=vedge&uuid=ddd801b2-8cbe-4394-abd1... admin

MONITOR Network > Troubleshooting  
Data Stream' is disabled. Go to Settings page to enable Data Stream to use Debug Logs.

Select Device BR2-VEDGE1 | 10.4.0.1 Site ID: 400 Device Model: vedge-cloud

- Application
- DPI
- Flows
- Interface
- TCP Optimization
- WAN Throughput
- Flows
- Top Talkers
- WAN
- TLOC
- Tunnel
- Control Connections
- System Status
- Events
- ACL Logs
- Troubleshooting**
- Real Time

### Connectivity




Device Bringup

Control Connections(Live View)

Ping

Trace Route

### Traffic



Tunnel Health

App Route Visualization

Simulate Flows

Select Traceroute using the radio button. Put in 10.3.0.21 as the destination IP for Branch1 in VPN 10. Select VPN 10 and source interface from the drop-down menu. And click on Start button.

The screenshot shows the Cisco vManage Traceroute interface. The configuration fields are: Destination IP\* (10.3.0.21), VPN (VPN - 10), and Source/Interface for VPN - 10 (Choose/Reset selections). The Start button is highlighted. The Output section shows the following text:

```
Traceroute -m 15 -w 1 10.3.0.21 in VPN 10
traceroute to 10.3.0.21 (10.3.0.21), 15 hops max, 60 byte packets
 1 10.3.0.2 (10.3.0.2) 2.610 ms 3.347 ms 3.432 ms
 2 10.3.0.21 (10.3.0.21) 4.136 ms 4.290 ms 4.370 ms
```

The diagram shows a direct connection between 10.4.0.1 and 10.3.0.21 with a latency of 4.27ms. A hop of 3.13ms is also shown between 10.4.0.1 and 10.3.0.2.

It shows direct connectivity between the Branch1 (10.3.0.21) and Branch2.

Do the same for VPN 20 with Destination IP in Branch-1 of 10.3.20.10.

Do the same by selecting from Branch1. Click on Select Device and select BR1-VEDGE1.

The screenshot shows the Cisco vManage interface for Troubleshooting > Traceroute. The breadcrumb navigation is MONITOR > Network > Troubleshooting > Traceroute. The current device is BR2-VEGE1 | 10.4.0.1 | Site ID: 400 | Device Model: vedge-cloud. The interface includes a 'Select Device' dropdown menu, a search bar, and a table of devices. The table lists several vEdge Cloud devices across different sites. The device BR2-VEGE1 is highlighted in blue. The main area shows a traceroute path to 10.3.0.21 with a delay of 4.27ms. A 'Start' button is visible in the top right corner of the main area.

Device Group	Search	Device	Model	Version
All				
BR1-VEGE1		10.3.0.1   Site ID: 300	vEdge Cloud	Version: 17.2.2
BR1-VEGE2		10.3.0.2   Site ID: 300	vEdge Cloud	Version: 17.2.2
BR2-VEGE1		10.4.0.1   Site ID: 400	vEdge Cloud	Version: 17.2.2
DC1-VEGE1		10.1.0.1   Site ID: 100	vEdge Cloud	Version: 17.2.2
DC1-VEGE2		10.1.0.2   Site ID: 100	vEdge Cloud	Version: 17.2.2
DC2-VEGE1		10.2.0.1   Site ID: 200	vEdge Cloud	Version: 17.2.2
DC2-VEGE2		10.2.0.2   Site ID: 200	vEdge Cloud	Version: 17.2.2

Select Traceroute, put in destination IP of 10.4.0.21, select VPN 10 and select source interface. Then click the Start button. You see additional hop because of additional CSR (router) in Branch 2.

The screenshot shows the Cisco vManage interface for configuring a traceroute. The 'Destination IP\*' is set to 10.4.0.10, the 'VPN' is set to VPN-10, and the 'Source/Interface for VPN-10' is set to ge0/3 - ipv4 - 10.3.0.2. A 'Start' button is visible. The 'Output' section displays the following text:

```
Traceroute -m 15 -w 1 -s 10.3.0.2 10.4.0.10 in VPN 10
traceroute to 10.4.0.10 (10.4.0.10), 15 hops max, 60 byte
packets
 1 10.4.254.10 (10.4.254.10) 2.184 ms 2.340 ms 2.457 ms
 2 10.4.254.254 (10.4.254.254) 3.971 ms 3.992 ms 4.584 ms
 3 10.4.0.10 (10.4.0.10) 3.805 ms 3.910 ms 4.078 ms
```

The diagram shows a path starting from the source interface 'ge0/3 - ipv4 - 10.3.0.2' with a delay of 2.33ms to the first hop '10.4.254.10', then 4.18ms to the second hop '10.4.254.254', and finally 3.93ms to the destination '10.4.0.10'.

Do the same for VPN 20 by traceroute to the test host in VPN 20.



The screenshot shows the Cisco vManage interface for a Traceroute operation. The browser address bar shows the URL: `https://198.18.1.10/#/app/monitor/devices/dashboard/troubleshooting/traceroute?personality=vedge&systemIp=10.3.0.1&localSystemIp=10.3.0.1&deviceType=vedge&uid=52c7911f-c5b0-45df-b826-...`

The interface includes the following elements:

- Navigation:** MONITOR > Network > Troubleshooting > Traceroute
- Device Information:** Select Device: BR1-VEDGE1 | 10.3.0.1 | Site ID: 300 | Device Model: vedge-cloud
- Configuration Fields:**
  - Destination IP\*: 10.4.20.10
  - VPN: VPN - 20
  - Source/Interface for VPN - 20: ge0/4 - ipv4 - 10.3.20.2
- Advanced Options:** A "Start" button is visible.
- Output:**

```
Traceroute -m 15 -w 1 -s 10.3.20.2 10.4.20.10 in VPN 20
traceroute to 10.4.20.10 (10.4.20.10), 15 hops max, 60 byte packets
 1 10.4.20.1 (10.4.20.1) 2.028 ms 2.559 ms 2.674 ms
 2 10.4.20.10 (10.4.20.10) 4.216 ms 4.228 ms 4.628 ms
```
- Diagram:** A path diagram showing the route from the source interface `ge0/4 - ipv4 - 10.3.20.2` to the destination IP `10.4.20.1` (2.42ms) and then to the final destination `10.4.20.10` (4.36ms).

Go to vManage dashboard and go to Configuration and select Policies.

The screenshot shows the Cisco vManage dashboard interface. At the top, there's a navigation bar with 'vManage' and 'admin' user. Below it is a 'DASHBOARD' section with several key metrics: Configuration (1 up), vEdge (7 up), vCloud (1 up), vManage (1 up), Reboot (20), Warning (0), and Invalid (0). A sidebar on the left contains navigation options: Configuration, Devices, Certificates, Templates, Policies (highlighted with a red box), and CloudExpress. The main dashboard area is divided into several sections:

- Site Health View (Total 4):** Shows connectivity status: Full Connectivity (4 sites), Partial Connectivity (0 sites), and No Connectivity (0 sites).
- Transport Interface Distribution:** A bar chart showing interface speeds: < 10 Mbps (17), 10 Mbps - 100 Mbps (0), 100 Mbps - 500 Mbps (0), and > 500 Mbps (0).
- vEdge Inventory:** A table showing: Total (15), Authorized (7), Deployed (7), and Staging (0).
- vEdge Health (Total 7):** Three gauges for Normal (7), Warning (0), and Error (0).
- Transport Health:** A line graph showing health over time, with a 'Type: By Loss' filter.
- Top Applications:** A bar chart showing usage for various applications.
- Application-Aware Routing:** A table with columns: Tunnel Outcomes, Avg. Latency (ms), Avg. Loss (%), and Avg. Jitter (ms).
 

Tunnel Outcomes	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
BR1-VL201-1mp1-DC1-VLDG21mp1	0.970	2.219	0.007
BR1-VEDGE1-1mp1-DC1-VEDGE11mp1	0.371	2.144	0.005
BR1-VEDGE1-1mp1-DC1-VEDGE11mp1	0.407	1.500	0.015
BR1-VEDGE1-1mp1-DC1-VEDGE11mp1	0.340	1.698	0.027

Click in the right most column of the policy named StrictHub-n-Spoke. From pull down click on Activate.

The screenshot shows the Viptela vManage web interface. The main content area displays a table of policies under the 'Centralized Policy' tab. The table has columns for Name, Description, Type, Activated, Updated By, Policy Version, and Last Updated. The 'StrictHub-n-Spoke' policy is highlighted in yellow. A context menu is open over the three-dot menu icon in the last column of this row, with the 'Activate' option selected and highlighted by a red box.

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated	
PureHub-n-Spoke	Create Hub-n-Spoke	UI Policy Builder	false	admin	08102017T113143264	10 Aug 2017 4:31:43 AM PDT	...
ControlPolicywithFWinserti...	FW Insertion	UI Policy Builder	false	admin	08102017T150135663	10 Aug 2017 8:01:35 AM PDT	...
ApplicationFirewall	Application Firewall	UI Policy Builder	false	admin	08112017T13112895	11 Aug 2017 6:11:28 AM PDT	...
AppRoutePolicy	AppRoute Policy	UI Policy Builder	false	admin	08132017T152603504	11 Aug 2017 7:14:58 AM PDT	...
PreferDC1Default	Prefer Default Route frm DC1	UI Policy Builder	false	admin	08112017T223402379	11 Aug 2017 3:34:02 PM PDT	...
PreferDCBasedonRegion	Prefer DC1 for BR1 and DC2 for BR21	UI Policy Builder	false	admin	08112017T223936887	11 Aug 2017 3:39:36 PM PDT	...
MultiTopologyPolicy	Creating Topologies for corp, pci an...	UI Policy Builder	false	admin	09182017T114628126	18 Sep 2017 4:35:38 AM PDT	...
MultiTopologyPlusFW	Multi-Topology with FW Insertion	UI Policy Builder	false	admin	09182017T120434218	18 Sep 2017 5:04:34 AM PDT	...
MultiTopologyPlusAppRoute	App Route with Multi Topology	UI Policy Builder	false	admin	09182017T230612233	18 Sep 2017 4:16:07 PM PDT	...
StrictHub-n-Spoke	Hub-n-Spoke for ALL VPNs	UI Policy Builder	false	admin	12062017T143753495	06 Dec 2017 6:20:13 AM PST	...

Click on Activate button on the pop-up.

The screenshot shows the Viptela vManage web interface. At the top, there's a navigation bar with 'CONFIGURATION | POLICIES' and a dropdown menu for 'Centralized Policy'. Below this, there are tabs for 'Policy', 'Traffic', and 'Control'. A search bar and 'Total Rows: 10' are visible. The main area contains a table of policies. A dialog box titled 'Activate Policy' is open, displaying the message: 'Policy will be applied to the reachable vSmarts: 12.12.12.12, 22.22.22.22'. The 'Activate' button in the dialog is highlighted with a red box.

Name	Description	Type	Activated	Updated By	Policy Version	
PureHub-n-Spoke	Create Hub-n-Spoke	UI Policy Builder	false	admin	08102017T113143264	10 Aug 2017 4:31:43 AM PDT ...
ControlPolicywithFWinsert...	FW Insertion	UI Policy Builder	false	admin	08102017T1150135663	10 Aug 2017 8:01:35 AM PDT ...
ApplicationFirewall	Application Firewall				08112017T113112895	11 Aug 2017 6:11:28 AM PDT ...
AppRoutePolicy	AppRoute Policy				08132017T1152603504	11 Aug 2017 7:14:58 AM PDT ...
PreferDC1Default	Prefer Default Route frm DC1				08112017T1223402379	11 Aug 2017 3:34:02 PM PDT ...
PreferDCBasedonRegion	Prefer DC1 for BR1 and DC2 for...				08112017T1223936887	11 Aug 2017 3:39:36 PM PDT ...
MultiTopologyPolicy	Creating Topologies for corp, p...				09182017T114628126	18 Sep 2017 4:35:38 AM PDT ...
MultiTopologyPlusFW	Multi-Topology with FW Insertion				09182017T1120434218	18 Sep 2017 5:04:34 AM PDT ...
MultiTopologyPlusAppRoute	App Route with Multi Topology				09182017T1230612233	18 Sep 2017 4:16:07 PM PDT ...
StrictHub-n-Spoke	Hub-n-Spoke for ALL VPNs	UI Policy Builder	false	admin	12152017T1134720152	15 Dec 2017 5:37:44 AM PST ...

Wait until the policy activation Status changes to Success. The policy will be applied to vSmart controllers. vSmart will push the policies to the appropriate vEdge routers.

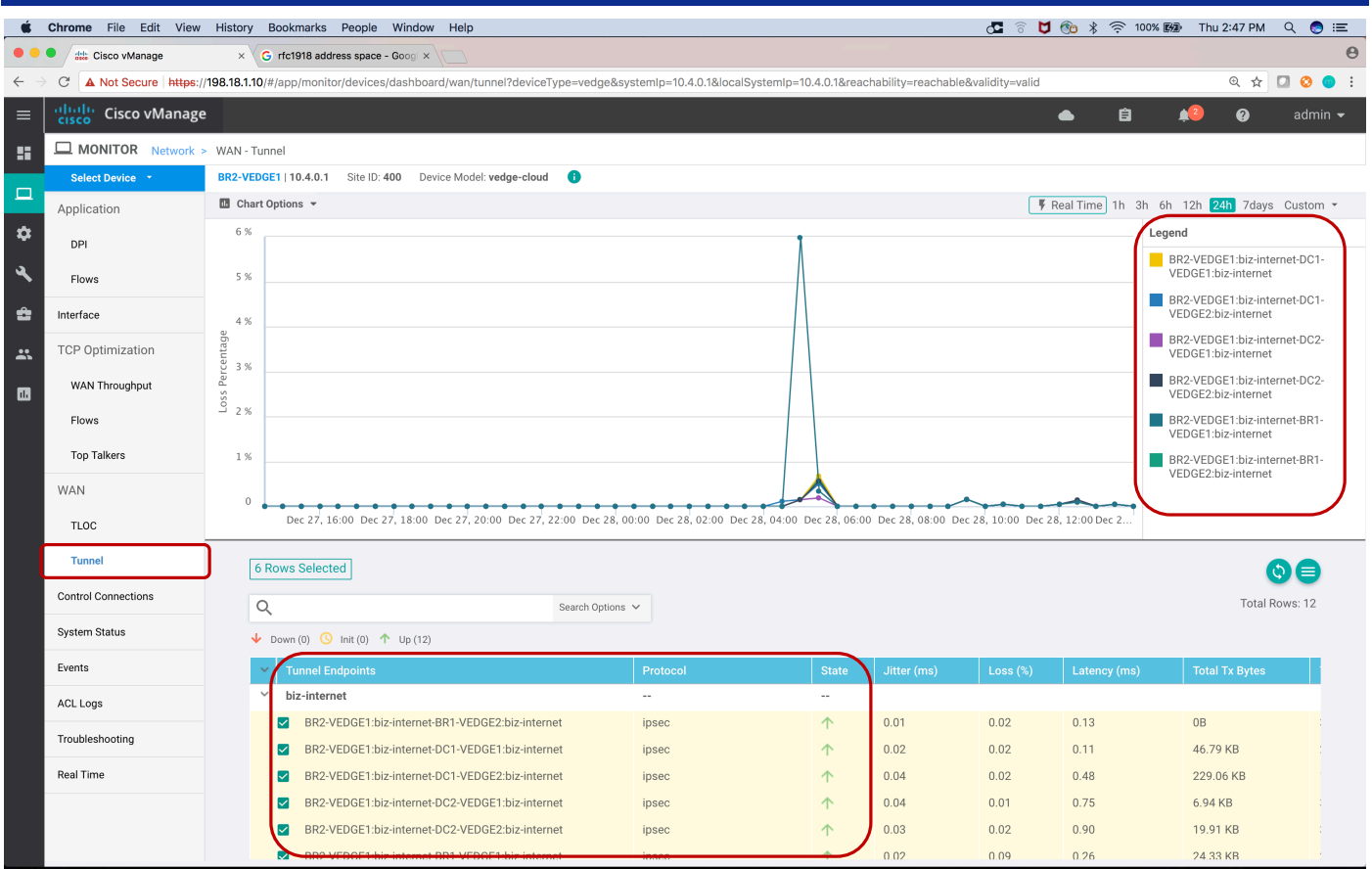
The screenshot shows the Viptela vManage web interface. The main content area is titled 'TASK VIEW' and displays a task named 'Push vSmart Policy' with a status of 'Validation Success'. Below this, it shows 'Total Task: 2 | Success : 2'. A table lists the task details:

Status	Message	Hostname	System IP	Site ID	
Success	Done - Push vSmart Policy	vSmart-1	12.12.12.12	10	10.10.10.10
Success	Done - Push vSmart Policy	vSmart-2	22.22.22.22	20	10.10.10.10

The 'Status' column in the table is highlighted with a red box. The interface also includes a search bar, a 'Total Rows: 2 of 2' indicator, and a 'Show All' button at the bottom right.

Validate Strict Hub-n-Spoke topology by going to device dashboard.

Look at the Tunnel setup between the Branches and DCs only.



Traceroute from Branch-2 and Branch-1 in VPN10 and VPN20.

Traceroute from BR2 to BR1. Use destination IP of 10.3.0.21 in VPN 10.

Destination IP\* 10.3.0.21

VPN VPN - 10

Source/Interface for VPN - 10 ge0/2 - ipv4 - 10.4.254.10

Start

Output

Traceroute -m 15 -w 1 -s 10.4.254.10 10.3.0.21 in VPN 10  
traceroute to 10.3.0.21 (10.3.0.21), 15 hops max, 60 byte packets

1 198.18.133.212 (198.18.133.212) 2.139 ms 2.713 ms 2.723 ms

2 10.3.0.2 (10.3.0.2) 4.273 ms 4.377 ms 4.550 ms

3 10.3.0.21 (10.3.0.21) 5.596 ms 5.722 ms 5.815 ms

Diagram: ge0/2 - ipv4 - 10.4.254.10 (2.53ms) -> 198.18.133.212 (4.40ms) -> 10.3.0.2 (5.71ms) -> 10.3.0.21

Traceroute from BR2 to BR1 in VPN 20. Use destination IP of 10.3.20.10 in VPN 20.

**Destination IP\*** 10.3.20.10

**VPN** VPN - 20

**Source/Interface for VPN - 20** ge0/3 - ipv4 - 10.4.20.1

**Start**

**Output**

```
Traceroute -m 15 -w 1 -s 10.4.20.1 10.3.20.10 in VPN 20
traceroute to 10.3.20.10 (10.3.20.10), 15 hops max, 60 byte packets
 1 10.1.20.3 (10.1.20.3) 2.177 ms 2.934 ms 2.955 ms
 2 10.3.20.2 (10.3.20.2) 4.551 ms 4.596 ms 4.739 ms
 3 10.3.20.10 (10.3.20.10) 5.135 ms 5.252 ms 5.286 ms
```

Network Diagram:

- Source: ge0/3 - ipv4 - 10.4.20.1
- Hop 1: 10.1.20.3 (2.69ms)
- Hop 2: 10.3.20.2 (4.63ms)
- Destination: 10.3.20.10 (5.22ms)

Deactivate the policy. From main dashboard select Configuration then Policies and select the StrictHub-n-Spoke policy and Deactivate.



The screenshot shows the Viptela vManage interface for configuring centralized policies. A table lists several policies, with the 'StrictHub-n-Spoke' policy highlighted in yellow. A context menu is open for this policy, and the 'Deactivate' option is highlighted with a red box.

Name	Description	Type	Activated	Updated By	Policy Version		
PreferDC1Default	Prefer Default Route frm DC1	UI Policy Builder	false	admin	08112017T223402379	11 Aug 2017 3:34:02 PM PDT	...
DCPreferencePerRegion	Prefer DC1 for BR1 and DC2 f...	UI Policy Builder	false	admin	08112017T223936887	16 Dec 2017 2:18:35 PM PST	...
MultiTopologyPolicy	Creating Topologies for corp, ...	UI Policy Builder	false	admin	09182017T114628126	18 Sep 2017 4:35:38 AM PDT	...
MultiTopologyPlusFW	Multi-Topology with FW Insert...	UI Policy Builder	false	admin	12162017T164629792	18 Sep 2017 5:04:34 AM PDT	...
MultiTopologyPlusAppRoute	App Route with Multi Topology	UI Policy Builder	false	admin	12172017T014214976	18 Sep 2017 4:16:07 PM PDT	...
StrictHub-n-Spoke	Hub-n-Spoke for ALL VPNs	UI Policy Builder	true	admin	12152017T134720152	15 Dec 2017 5:37:44 AM PST	...
MultiTopologyPlusACL	Using Data Policy to impleme...	UI Policy Builder	false	admin	12162017T221137925	16 Dec 2017	...

- View
- Preview
- Copy
- Edit
- Delete
- Deactivate

Click on "Deactivate" button.

The screenshot shows the Viptela vManage web interface. A modal dialog box titled "Deactivate Policy" is open, displaying the following text:

Policy will be removed from the following vSmart.  
12.12.12.12, 22.22.22.22

Would you like to remove policy from reachable vSmarts?

At the bottom of the dialog are two buttons: "Deactivate" (highlighted with a red box) and "Cancel".

Name	Description	Type	Activated	Updated By	Policy Version	
PreferDC1Default	Prefer Default Route frm DC1	UI Policy Builder	false	admin	08112017T223402379	11 Aug 2017 3:34:02 PM PDT ...
DCPreferencePerRegion	Prefer DC1 for BR1 and DC2 f...	UI Policy Builder	false	admin	08112017T223936887	16 Dec 2017 2:18:35 PM PST ...
MultiTopologyPolicy	Creating Topologies for co				09182017T114628126	18 Sep 2017 4:35:38 AM PDT ...
MultiTopologyPlusFW	Multi-Topology with FW In				12162017T164629792	18 Sep 2017 5:04:34 AM PDT ...
MultiTopologyPlusAppRoute	App Route with Multi Topo				12172017T014214976	18 Sep 2017 4:16:07 PM PDT ...
StrictHub-n-Spoke	Hub-n-Spoke for ALL VPN				12152017T134720152	15 Dec 2017 5:37:44 AM PST ...
MultiTopologyPlusACL	Using Data Policy to imple				12162017T221137925	16 Dec 2017 2:08:43 PM PST ...

Wait till the policy is successfully removed from the vSmarts.

Chrome File Edit View History Bookmarks People Window Help

Viptela vManage

Not Secure https://198.18.1.10/index.html#/app/device/status?activity=vsmart\_policy\_config&pid=vsmart\_policy\_config-457bf2e5-330a-4aeb-839b-e5f3a1c855ad

admin

### TASK VIEW

Push vSmart Policy | Validation Success - Initiated By: admin From: 10.16.27.161

Total Task: 2 | Success : 2

Search:

Total Rows: 2 of 2

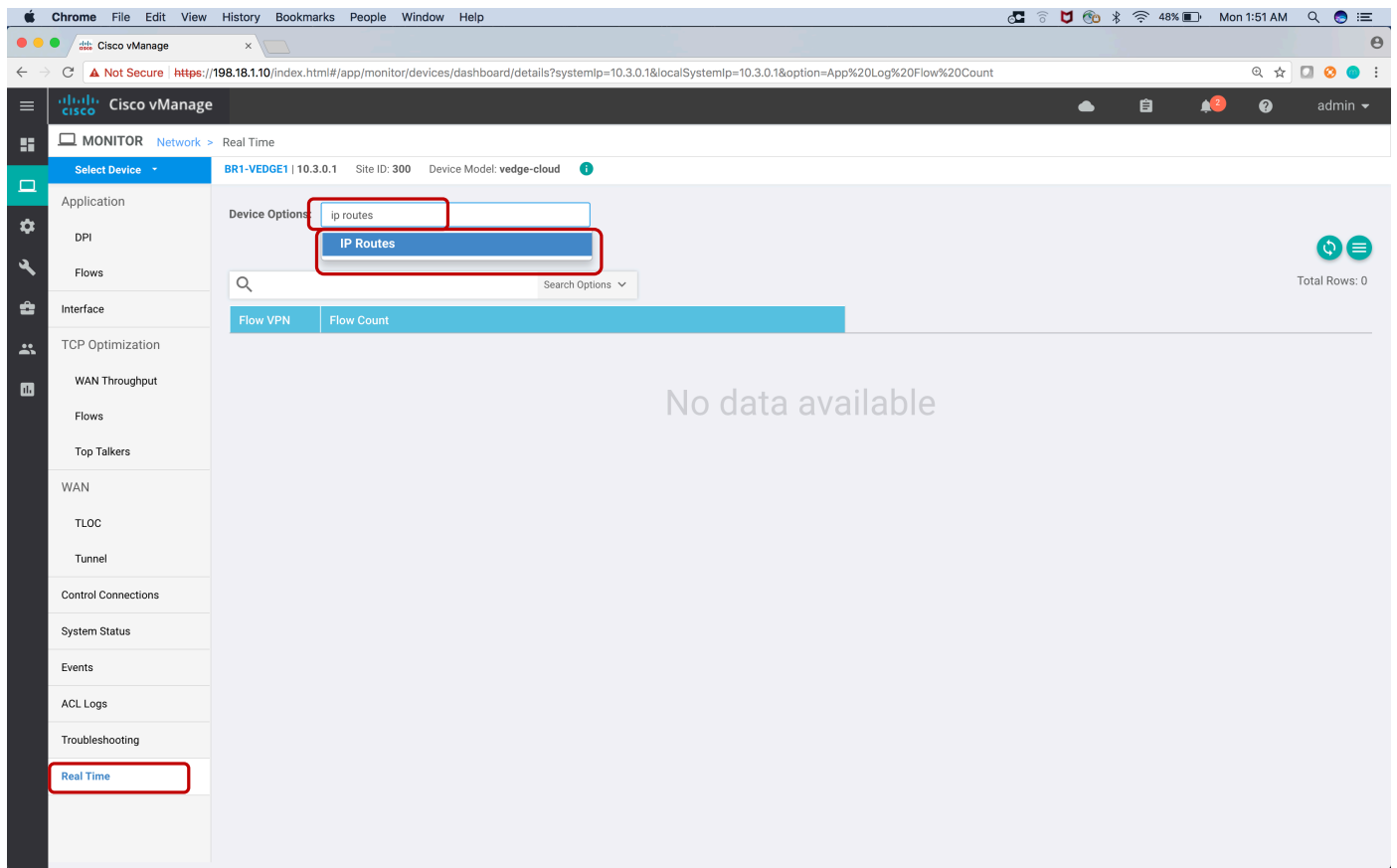
Status	Message	Hostname	System IP	Site ID	
Success	Done Removing policy to vsmart.	vSmart-1	12.12.12.12	10	10.10.10.10
Success	Done Removing policy to vsmart.	vSmart-2	22.22.22.22	20	10.10.10.10

# Lab 03 - Prefer Data Center DC1 and DC2 for Different Set of Branches for Regional Internet Exit

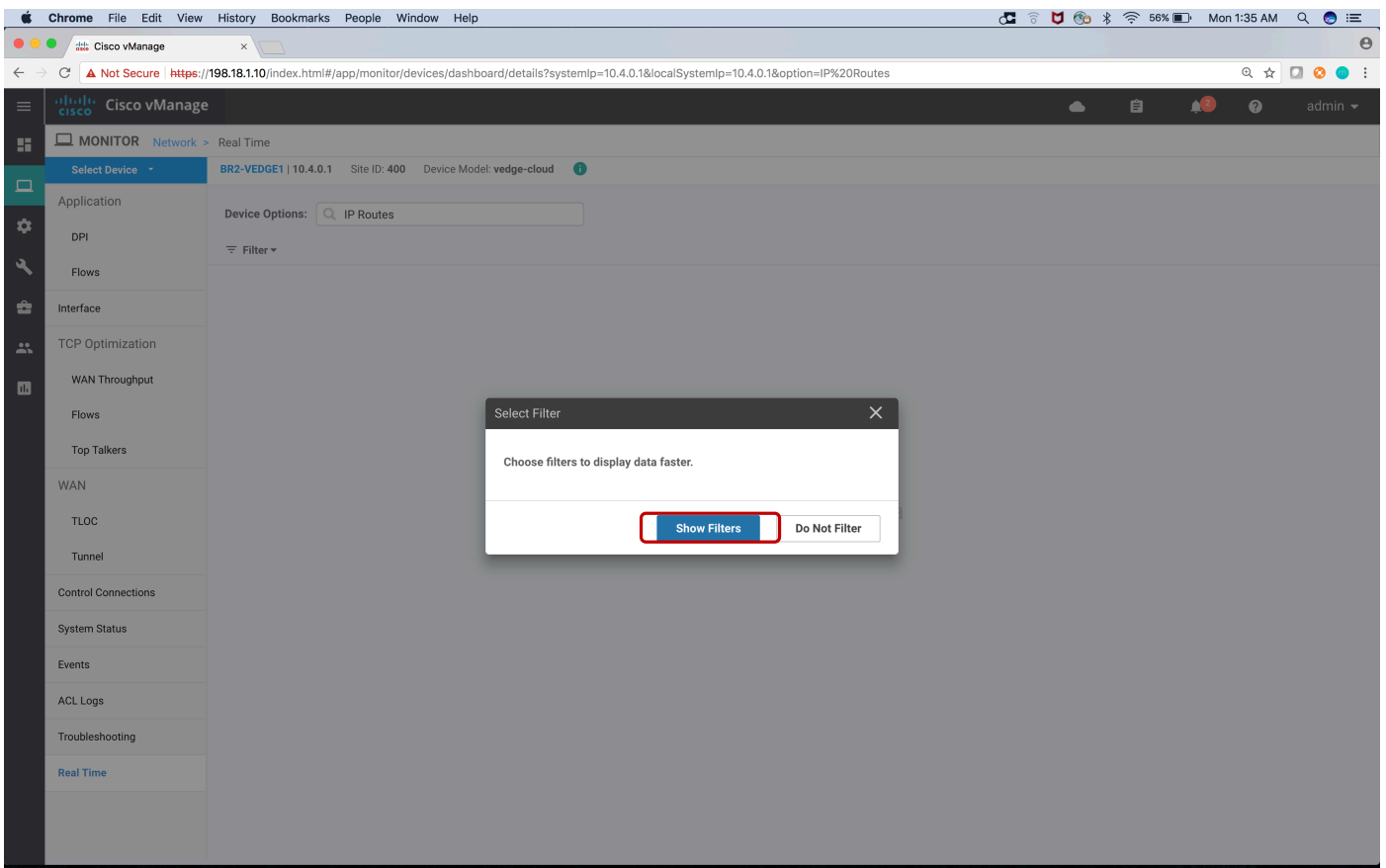
In some cases, the Enterprise may want different Branches to take different Regional Exits to the Internet on the same Overlay. Let's say in this case the customer wants DC1 the preferred exit for Branch 1 and DC2 is the preferred exit for Branch 2.

## Steps

Go to Device dashboard for BR1-VEEDGE1 and Click on "Real Time" tab. In the dialogue box, search for "ip routes". Select the "IP Routes" from pull down menu.



On the next pop-up select "Show Filters".



On the next screen put in value of 10 for VPN and 0.0.0.0/0 (default) for prefix.

Device Options: IP Routes

Filter VPN ID: 10 Prefix: 0.0.0.0/0

VPN ID: 10

AF Type: Select AF Type

Prefix: 0.0.0.0/0

Protocol: Select Protocol

Reset All Search Close

VPN ID	Next Hop Address	Next Hop VPN	TLOC IP	TLOC Color	TLOC Encap
10	--	--	10.1.0.1	mpls	ipsec
10	--	--	10.1.0.1	biz-internet	ipsec
10	--	--	10.1.0.2	mpls	ipsec
10	--	--	10.1.0.2	biz-internet	ipsec
10	--	--	10.2.0.1	mpls	ipsec
10	--	--	10.2.0.1	biz-internet	ipsec
10	--	--	10.2.0.2	mpls	ipsec
10	--	--	10.2.0.2	biz-internet	ipsec

The next screen will show default route being load-shared across the two DCs.

The screenshot shows the Cisco vManage interface for monitoring IP routes on device BR1-VEDGE1. The table below represents the data shown in the interface:

VPN ID	AF Type	Prefix	Protocol	Next Hop If Name	Next Hop Address	Next Hop VPN	TLOC IP	TLOC Color	TLOC Encap
10	ipv4	0.0.0.0/0	omp	--	--	--	10.1.0.1	mpls	ipsec
10	ipv4	0.0.0.0/0	omp	--	--	--	10.1.0.1	biz-internet	ipsec
10	ipv4	0.0.0.0/0	omp	--	--	--	10.1.0.2	mpls	ipsec
10	ipv4	0.0.0.0/0	omp	--	--	--	10.1.0.2	biz-internet	ipsec
10	ipv4	0.0.0.0/0	omp	--	--	--	10.2.0.1	mpls	ipsec
10	ipv4	0.0.0.0/0	omp	--	--	--	10.2.0.1	biz-internet	ipsec
10	ipv4	0.0.0.0/0	omp	--	--	--	10.2.0.2	mpls	ipsec
10	ipv4	0.0.0.0/0	omp	--	--	--	10.2.0.2	biz-internet	ipsec

Go to BR2-VEDGE1 device dashboard and it will show the same for the default.

Activate the policy named "DCPreferencePerRegion".

The screenshot shows the Viptela vManage interface for configuring policies. The table below lists several policies, with 'DCPreferencePerRegion' highlighted in yellow. A context menu is open over the actions column for this policy, showing options: View, Preview, Copy, Edit, Delete, and Activate. The 'Activate' option is highlighted with a red box.

Name	Description	Type	Activated	Updated By	Policy Version	
PreferDC1Default	Prefer Default Route frm DC1	UI Policy Builder	false	admin	08112017T223402379	11 Aug 2017 3:34:02 PM PDT
DCPreferencePerRegion	Prefer DC1 for BR1 and DC2 f...	UI Policy Builder	false	admin	08112017T223936887	16 Dec 2017 2:18:35 PM PST
MultiTopologyPolicy	Creating Topologies for corp, ...	UI Policy Builder	false	admin	09182017T114628126	18 Sep 2017
MultiTopologyPlusFWinsertion	Multi-Topology with FW Insert...	UI Policy Builder	false	admin	12162017T164629792	18 Dec 2017
MultiTopologyPlusAppRoute	App Route with Multi Topology	UI Policy Builder	false	admin	12172017T014214976	18 Sep 2017
StrictHub-n-Spoke	Hub-n-Spoke for ALL VPNs	UI Policy Builder	false	admin	12152017T134720152	15 Dec 2017
MultiTopologyPlusACL	Using Data Policy to impleme...	UI Policy Builder	false	admin	12162017T221137925	16 Dec 2017

Once the policy has been successfully being pushed to the vSmarts, go to the Device dashboard for BR1-VEGDE1 and get the default route in VPN 10. You will see the route installed is pointing to DC1 as the preferred path.



The screenshot shows the Cisco vManage interface for monitoring IP routes on device BR1-VEDGE1. The table below displays the route information:

VPN ID	AF Type	Prefix	Protocol	Next Hop If Name	Next Hop Address	Next Hop VPN	TLOC IP	TLOC Color	TLOC Encap
10	ipv4	0.0.0.0/0	omp	--	--	--	10.1.0.1	mpls	ipsec
10	ipv4	0.0.0.0/0	omp	--	--	--	10.1.0.1	biz-internet	ipsec
10	ipv4	0.0.0.0/0	omp	--	--	--	10.1.0.2	mpls	ipsec
10	ipv4	0.0.0.0/0	omp	--	--	--	10.1.0.2	biz-internet	ipsec

The same is shown on BR2-VEDGE1 where the preferred datacenter is DC2.

The screenshot shows the Cisco vManage interface for monitoring IP routes on a device. The interface includes a navigation sidebar on the left with options like Application, DPI, Flows, Interface, TCP Optimization, WAN Throughput, Flows, Top Talkers, WAN, TLOC, Tunnel, Control Connections, System Status, Events, ACL Logs, Troubleshooting, and Real Time. The main content area displays a table of IP routes with the following columns: VPN ID, AF Type, Prefix, Protocol, Next Hop If Name, Next Hop Address, Next Hop VPN, TLOC IP, TLOC Color, and TLOC Encap. The table contains four rows of data, and the last three columns (TLOC IP, TLOC Color, and TLOC Encap) are highlighted with a red box.

VPN ID	AF Type	Prefix	Protocol	Next Hop If Name	Next Hop Address	Next Hop VPN	TLOC IP	TLOC Color	TLOC Encap
10	ipv4	0.0.0.0/0	omp	--	--	--	10.2.0.1	mpls	ipsec
10	ipv4	0.0.0.0/0	omp	--	--	--	10.2.0.1	biz-internet	ipsec
10	ipv4	0.0.0.0/0	omp	--	--	--	10.2.0.2	mpls	ipsec
10	ipv4	0.0.0.0/0	omp	--	--	--	10.2.0.2	biz-internet	ipsec

Deactivate the policy.

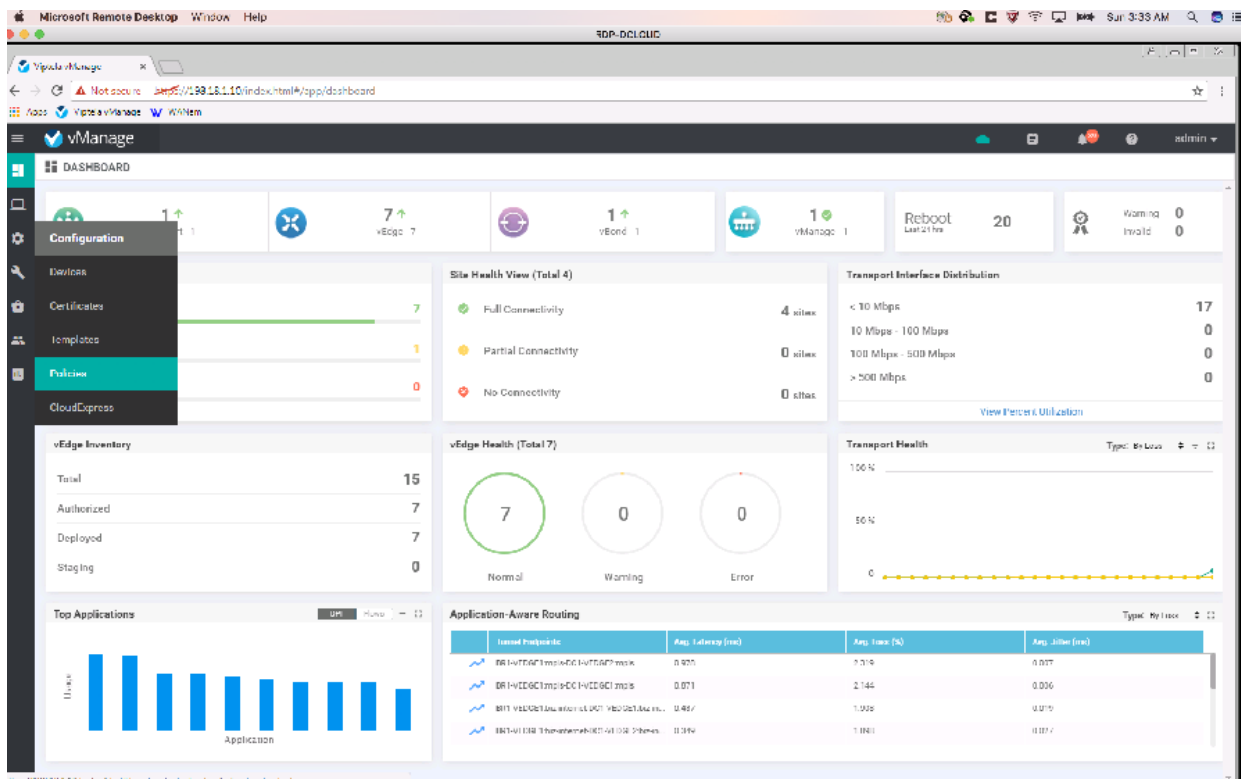
# Lab 04 - Service (FW) Insertion

When new branches are added, the enterprise may want initially that direct branch to branch communication go through a firewall in their DC or Colo/Regional facility hosting those services.

Using Cisco SD-WAN, services can be deployed anywhere in the network and based on policies redirect flows/site-traffic through those services.

## Steps

Go to vManage dashboard and go to Configuration and select Policies.

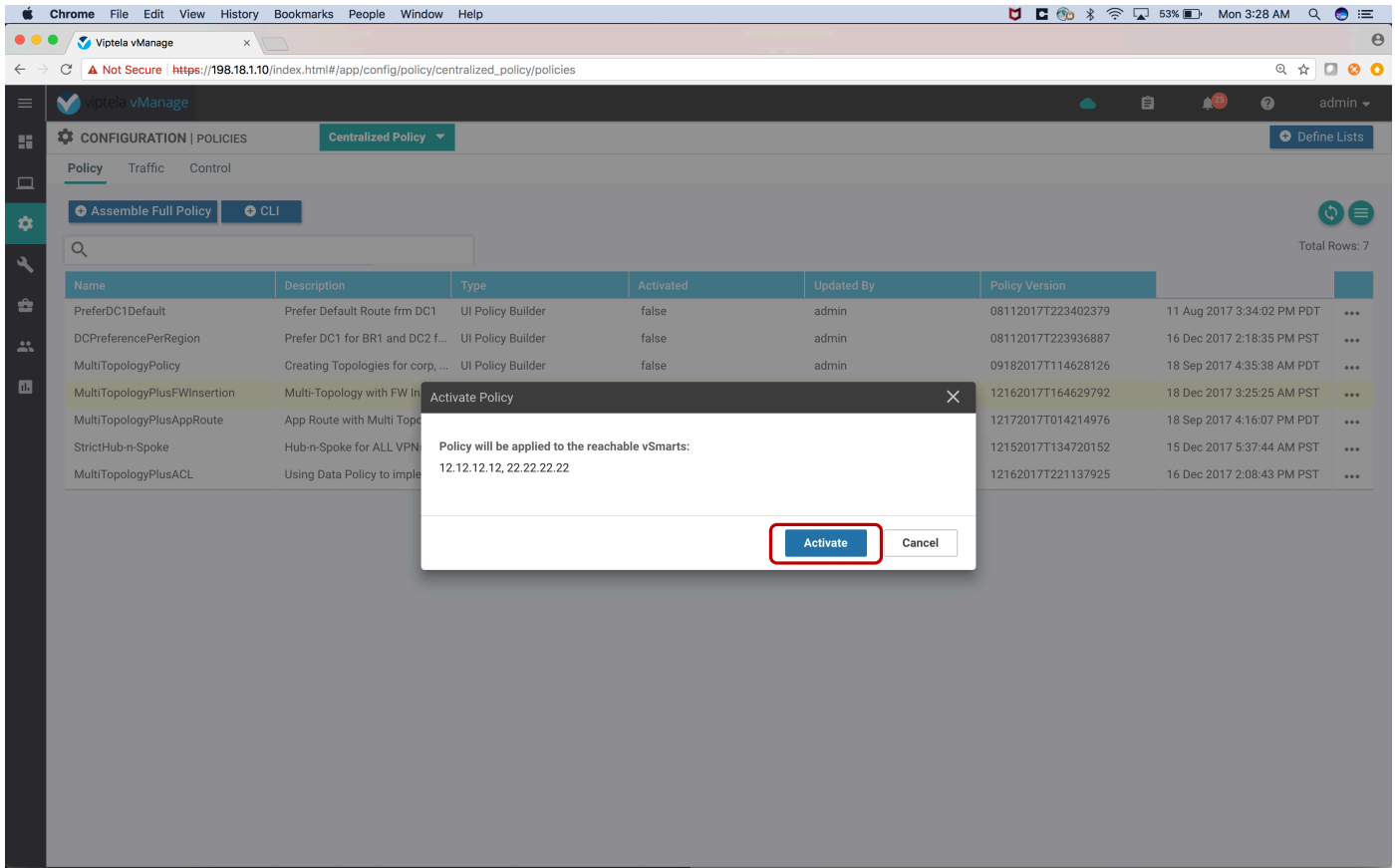


Activate the policy named "MultiTopologyPlusFWInsertion".

The screenshot shows the Viptela vManage web interface. The main content area displays a table of policies under the 'CONFIGURATION | POLICIES' section. The table has columns for Name, Description, Type, Activated, Updated By, and Policy Version. The 'MultiTopologyPlusFWInsertion' policy is highlighted in yellow. A context menu is open over the actions column for this policy, showing options: View, Preview, Copy, Edit, Delete, and Activate. The 'Activate' option is highlighted with a red box.

Name	Description	Type	Activated	Updated By	Policy Version	
PreferDC1Default	Prefer Default Route frm DC1	UI Policy Builder	false	admin	08112017T223402379	11 Aug 2017 3:34:02 PM PDT ...
DCPreferencePerRegion	Prefer DC1 for BR1 and DC2 f...	UI Policy Builder	false	admin	08112017T223936887	16 Dec 2017 2:18:35 PM PST ...
MultiTopologyPolicy	Creating Topologies for corp, ...	UI Policy Builder	false	admin	09182017T114628126	18 Sep 2017 4:35:38 AM PDT ...
MultiTopologyPlusFWInsertion	Multi-Topology with FW Insert...	UI Policy Builder	false	admin	12162017T164629792	18 Dec 2017 3:25:25 AM PST ...
MultiTopologyPlusAppRoute	App Route with Multi Topology	UI Policy Builder	false	admin	12172017T014214976	18 Sep 2017 ...
StrictHub-n-Spoke	Hub-n-Spoke for ALL VPNs	UI Policy Builder	false	admin	12152017T134720152	15 Dec 2017 ...
MultiTopologyPlusACL	Using Data Policy to impleme...	UI Policy Builder	false	admin	12162017T221137925	16 Dec 2017 ...

Click on “Activate” button.



Wait till the policy is successfully pushed to the vSmarts.

**TASK VIEW**  
Push vSmart Policy | Validation Success - Initiated By: admin From: 10.16.27.161  
Total Task: 2 | Success : 2

Status	Message	Hostname	System IP	Site ID	
Success	Done - Push vSmart Policy	vSmart-1	12.12.12.12	10	10.10.10.10
Success	Done - Push vSmart Policy	vSmart-2	22.22.22.22	20	10.10.10.10

Total Rows: 2 of 2

Go to Device Dashboard for BR2-VEDGE1. Go to Monitor then select Network. Click on BR2-VEDGE1.

**MONITOR | NETWORK**

State	System IP	Reachability	Site ID	Device Model	BFD	Control	Version	Up Since	Chassis Number/ID	Device Groups
✓	10.3.0.1	reachable	300	vEdge Cloud	10	3	17.1.1	12 Aug 2017 10:23:00 PM GMT	59c79114c32ab454f5a876312560	No groups
✓	10.3.0.2	reachable	300	vEdge Cloud	10	3	17.1.1	12 Aug 2017 10:23:00 PM GMT	0af91c79-35a9-101c-bb62-60251...	No groups
✓	10.4.0.1	reachable	400	vEdge Cloud	12	3	17.1.1	10 Aug 2017 11:07:00 AM GMT	d83901b2-6c9e-1391-a0d1-3d71e...	No groups
✓	10.1.0.1	reachable	100	vEdge Cloud	10	3	17.1.1	12 Aug 2017 10:22:00 PM GMT	ebdc8b39-17e5-4eb0-a5e044504...	No groups
✓	10.1.0.2	reachable	100	vEdge Cloud	10	3	17.1.1	12 Aug 2017 10:22:00 PM GMT	121b4b05-02b3-4714-63b3-c2121e...	No groups
✓	10.2.0.1	reachable	200	vEdge Cloud	10	3	17.1.1	12 Aug 2017 10:22:00 PM GMT	9e795ed7-555a-420b-b000-1cc99e...	No groups
✓	10.2.0.2	reachable	200	vEdge Cloud	10	3	17.1.1	12 Aug 2017 10:22:00 PM GMT	b526e0e0-82bb-4d2b-93db-7141e...	No groups
✓	11.11.11.11	reachable		vEdge Cloud (Veo...			17.1.1	17 Aug 2017 11:09:00 PM GMT	ab4d1e5d7-560a-4d81-935a-fde07...	No groups
✓	10.10.10.10	reachable	100	vManage	-	3	17.1.1	17 Aug 2017 11:09:00 PM GMT	5771ea-2ca4b1-478b3a5a-4db37...	No groups
✓	12.12.12.12	reachable	10	vSmart	-	15	17.1.1	12 Aug 2017 10:23:00 PM GMT	10a46779-40f0-4383-871c-195d...	No groups

Go to Troubleshooting and then do traceroute to 10.3.0.21 in VPN 10. You could see traffic going through FW (198.18.130.1 or 10.2.0.1) sitting in DC1 and DC2 respectively.

The screenshot shows the Viptela vManage interface for device BR2-VEDGE1. The 'Connectivity Tools' section has 'Traceroute' selected. The configuration is as follows:

- Destination IP\*: 10.3.0.21
- VPN: VPN - 10
- Source/Interface for VPN - 10: ge0/2 - ipv4 - 10.4.254.0

The 'Start' button is highlighted. The 'Output' section shows the following results:

```
Traceroute -m 15 -w 1 -s 10.4.254.10 10.3.0.21 in VPN 10
traceroute to 10.3.0.21 (10.3.0.21), 15 hops max, 60 byte packets
 1 10.2.0.211 (10.2.0.211) 3.552 ms 4.532 ms 4.634 ms
 2 10.2.0.1 (10.2.0.1) 5.022 ms 5.332 ms 5.431 ms
 3 10.2.0.212 (10.2.0.212) 5.920 ms 6.168 ms 6.568 ms
 4 10.3.0.2 (10.3.0.2) 6.888 ms 7.357 ms 7.441 ms
 5 10.3.0.21 (10.3.0.21) 7.807 ms 8.041 ms 8.117 ms
```

The diagram shows the path from the source interface ge0/2 - ipv4 - 10.4.254.10 through hops 10.2.0.211, 10.2.0.1, 10.2.0.212, and 10.3.0.2 to the destination 10.3.0.21. Round trip times are shown above each hop: 4.24ms, 5.26ms, 6.22ms, 7.23ms, and 7.99ms.

Repeat the same with BR1-VEDGE1. Do traceroute to the destination IP of 10.4.0.21.

**Connectivity Tools** | **Traceroute**

Destination IP\*: 10.4.0.21 | VPN: VPN-10 | Source/Interface for VPN - 10: ge0/3-ipv4-10.3.0.2

**Advanced Options** > **Start**

**Output**

```
Traceroute -m 15 -w 1 -s 10.3.0.2 10.4.0.21 in VPN 10
traceroute to 10.4.0.21 (10.4.0.21), 15 hops max, 60
byte packets
 1 10.2.0.211 (10.2.0.211) 1.987 ms 2.098 ms 3.099 ms
 2 10.2.0.1 (10.2.0.1) 3.916 ms 3.952 ms 3.972 ms
 3 10.2.0.212 (10.2.0.212) 4.043 ms 4.065 ms 4.082 ms
 4 10.4.254.10 (10.4.254.10) 5.227 ms 5.433 ms 5.568
ms
 5 10.4.254.254 (10.4.254.254) 6.091 ms 6.203 ms
7.016 ms
 6 10.4.0.21 (10.4.0.21) 8.359 ms 6.816 ms 7.787 ms
```

**Network Diagram:** ge0/3-ipv4-10.3.0.2 (Source) → 10.2.0.211 (2.39ms) → 10.2.0.1 (3.95ms) → 10.2.0.212 (4.06ms) → 10.4.254.10 (5.41ms) → 10.4.254.254 (6.44ms) → 10.4.0.21 (7.65ms)

Deactivate the policy named "MultiTopologyPlusFWInsertion".



# Lab 06 - Application Aware Routing

SD-WAN provides a fast deployment model for flexible topologies; any circuit type can be deployed and SD-WAN will provide the ability to direct different types of traffic over different types of link.

Video can be transmitted over the internet, while mission critical applications are sent over MPLS as long as the circuits satisfy certain SLAs for the applications in question. This provides path diversity and high availability as well as the ability to use transports in an intelligent fashion.

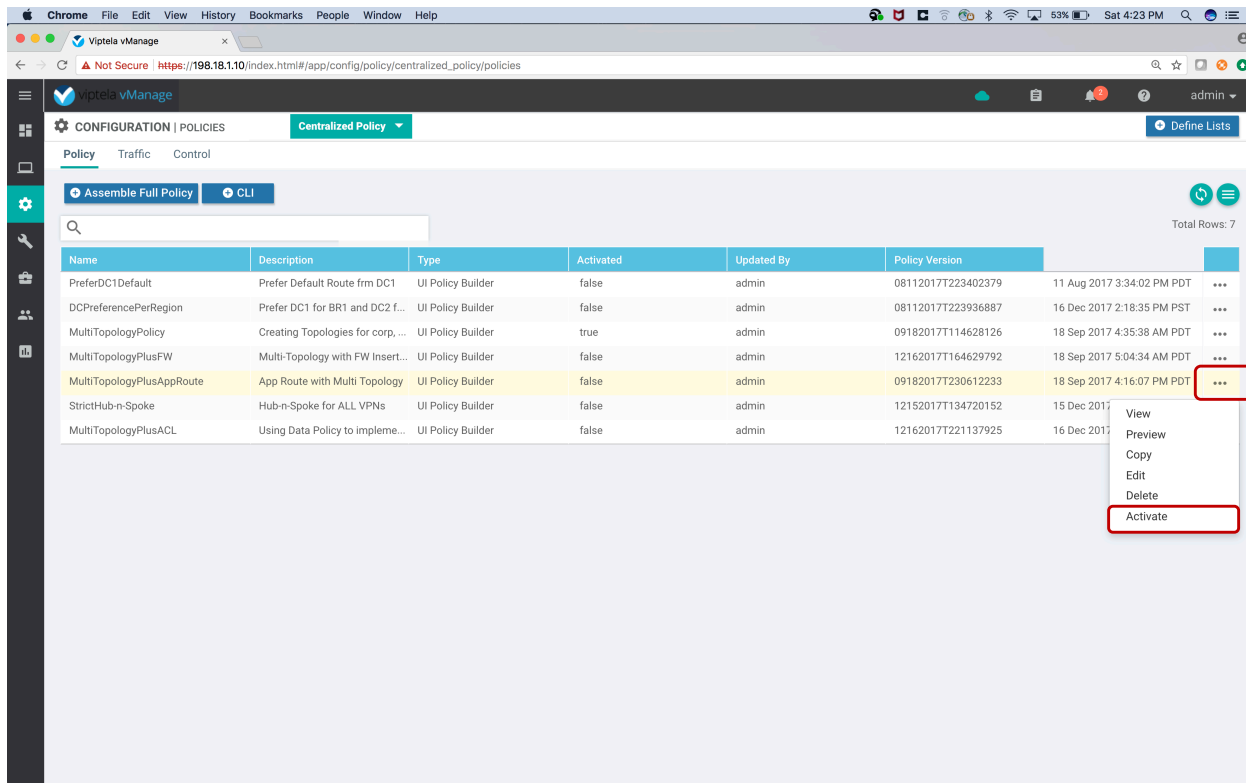
In this demonstration, some of the applications have SLAs defined and are pinned to the MPLS (interface ge0/0 on BR2-VEDGE1). Some applications are pinned to the internet transport (interface ge0/1 on BR2-VEDGE1).

The policy is applied to ALL sites, so the policy has impact on all the traffic received and sent by BR2-VEDGE1. More traffic is received than sent by the BR2-VEDGE1. Look at the traffic received by BR2-VEDGE1 on mpls interface (ge0/0) and internet interface (ge0/1).

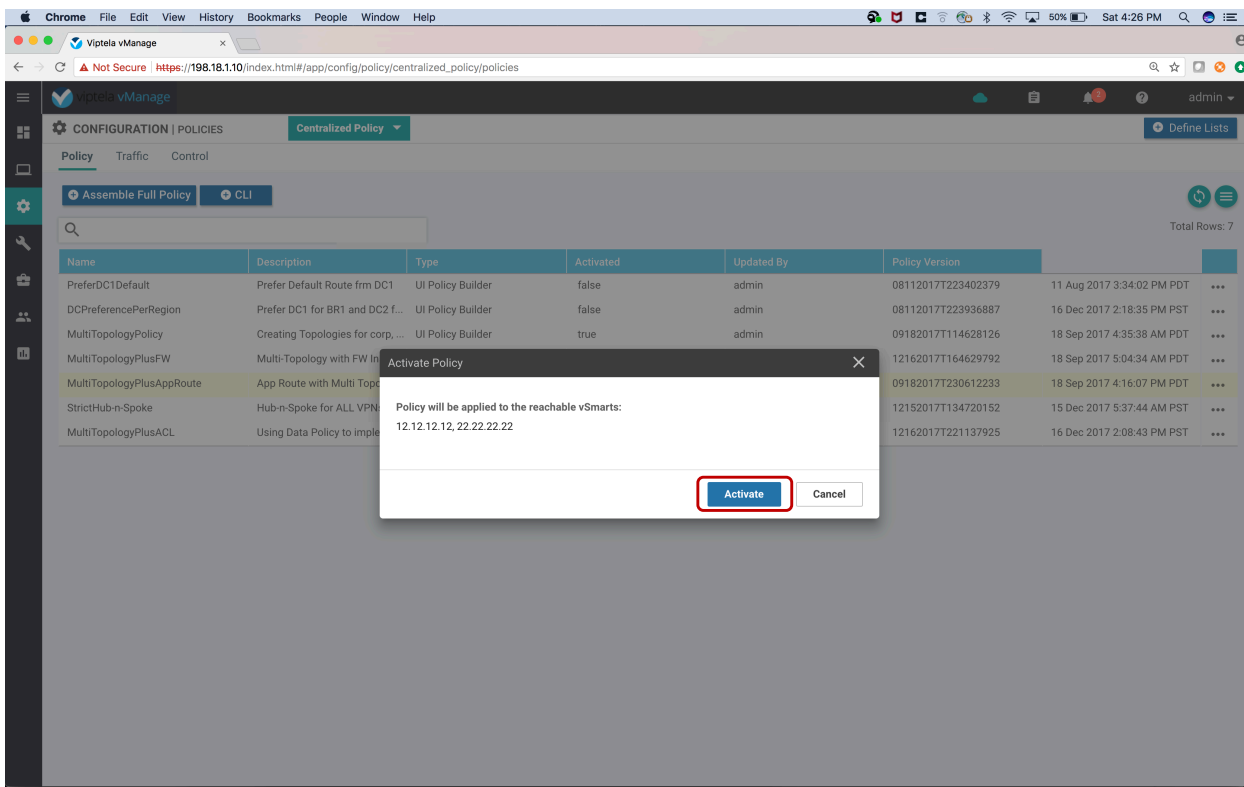
You would observe traffic received switch from mpls interface to internet interface after the latency impairment on MPLS transport.

## Steps

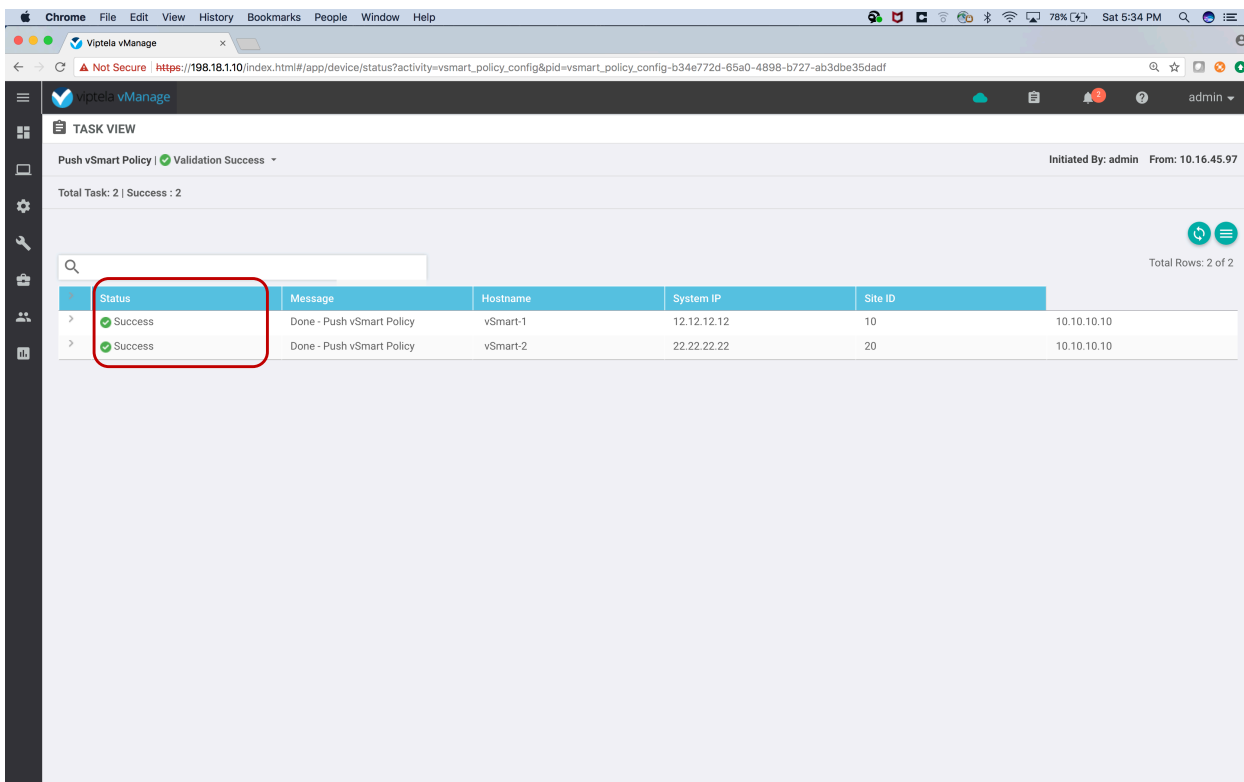
Go to the Policy configuration page, and activate the Application Aware Routing policy named “MultiTopologyPlusAppRoute”.



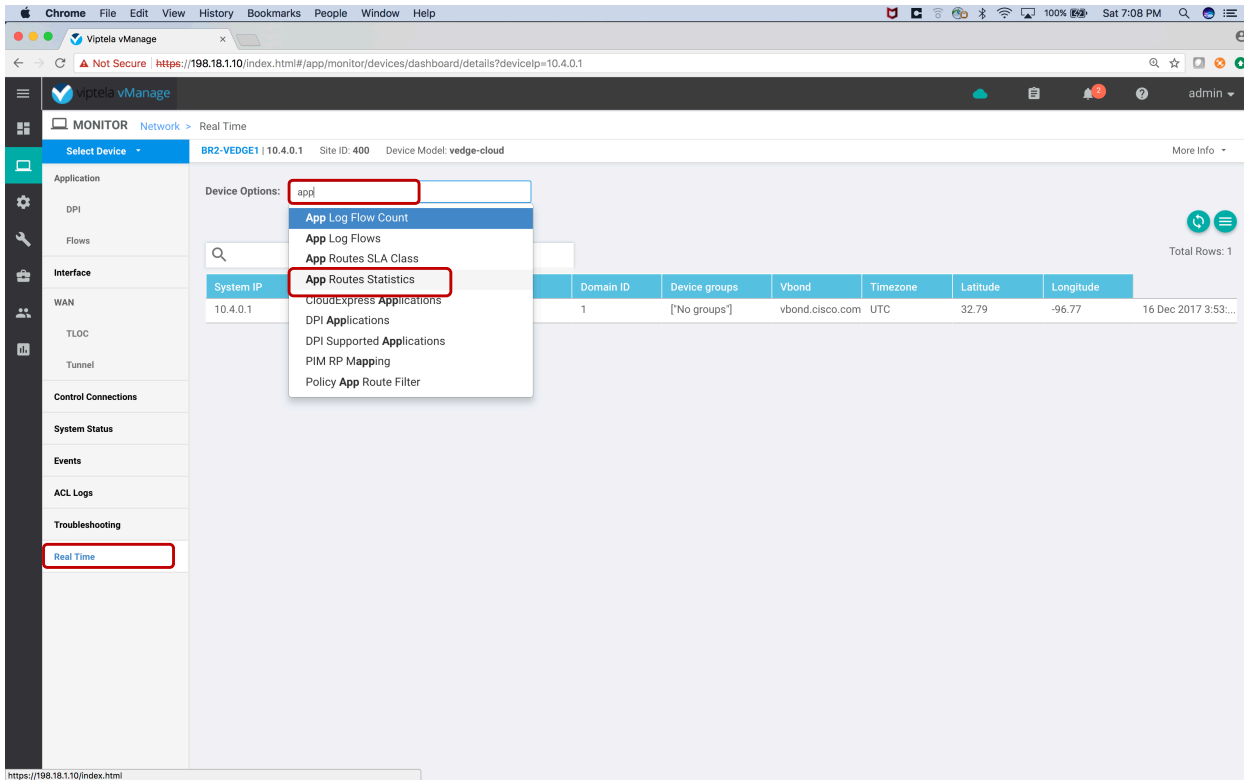
Click on the “Activate” button.



Wait till the policy is successfully pushed to both the vSmarts.



To see the current performance measurement on both the transports, go to device dashboard for BR2-VEDGE1. Click on “Real Time” tab. Search for “App Routes Statistics” and select it.



Scroll to the right and you will see the columns showing latency, loss and jitter for each of the tunnels on MPLS and Internet. The values (at or close to zero) are much lower than the SLA definitions defined for the app-route policies.

To view the tunnels statistics on internet transport, type in “biz-internet” in the search column and hit return.

The screenshot shows the Cisco vManage interface for device BR2-VEDGE1. The 'Device Options' field is set to 'App Routes Statistics'. The search filter is 'biz-internet'. The table below displays statistics for various flows.

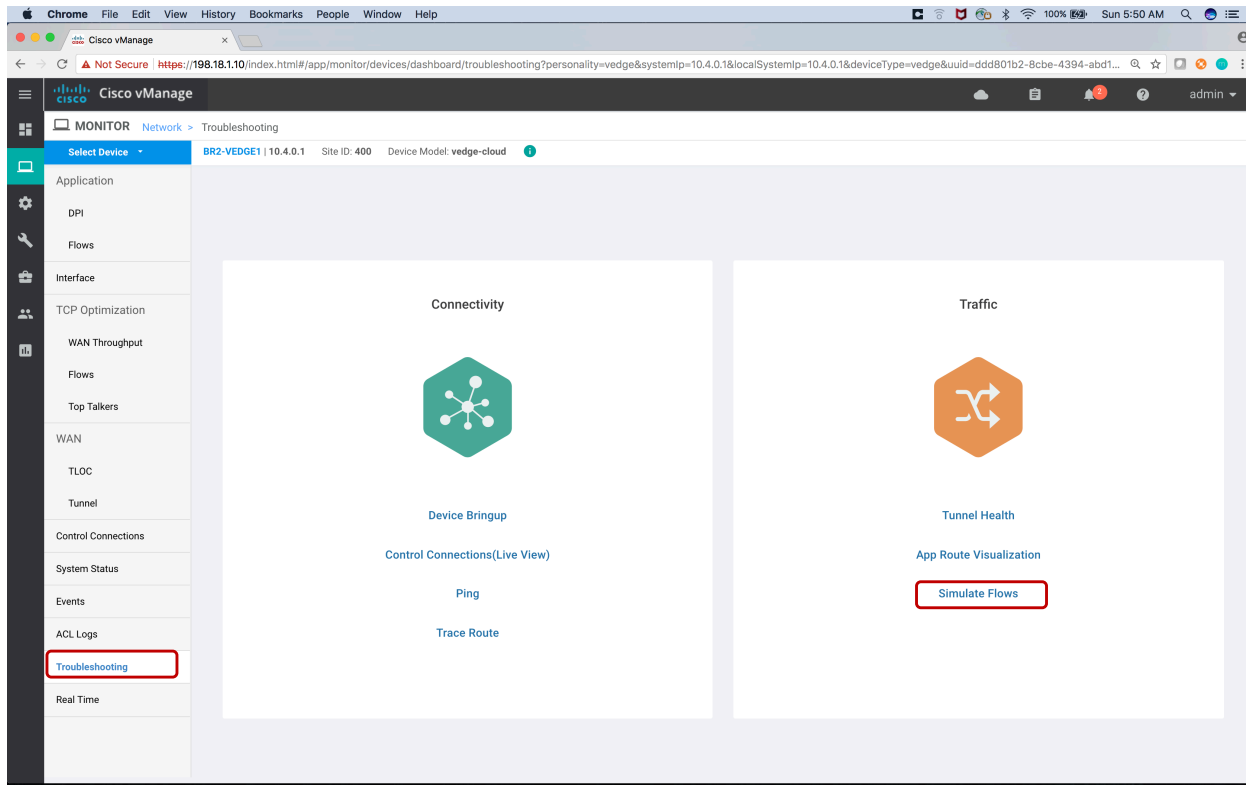
Destination Port	Remote System Ip	Local Color	Remote Color	Mean Loss	Mean Latency	Mean Jitter	SLA Class Index	Index	Total Packets
12346	10.3.0.1	biz-internet	biz-internet	0	0	0	0,1,2,3,4	0	5
12346	10.3.0.1	biz-internet	biz-internet	0	0	0	0,2,3,4	1	5
12346	10.3.0.1	biz-internet	biz-internet	0	0	0	0,2,3,4	2	5
12346	10.3.0.1	biz-internet	biz-internet	0	0	0	0,2,3,4	3	5
12346	10.3.0.1	biz-internet	biz-internet	0	0	0	0,2,3,4	4	5
12346	10.3.0.1	biz-internet	biz-internet	0	0	0	0,2,3,4	5	5
65368	10.3.0.2	biz-internet	biz-internet	0	0	0	0,2,3,4	0	5
65368	10.3.0.2	biz-internet	biz-internet	0	0	0	0,2,3,4	1	5
65368	10.3.0.2	biz-internet	biz-internet	0	0	0	0,2,3,4	2	5
65368	10.3.0.2	biz-internet	biz-internet	0	0	0	0,2,3,4	3	5
65368	10.3.0.2	biz-internet	biz-internet	0	0	0	0,2,3,4	4	5
65368	10.3.0.2	biz-internet	biz-internet	0	0	0	0,2,3,4	5	5
12346	10.1.0.1	biz-internet	biz-internet	0	0	0	0,2,3,4	0	5
12346	10.1.0.1	biz-internet	biz-internet	0	0	0	0,2,3,4	1	5
12346	10.1.0.1	biz-internet	biz-internet	0	0	0	0,2,3,4	2	5
12346	10.1.0.1	biz-internet	biz-internet	0	0	0	0,2,3,4	3	5
12346	10.1.0.1	biz-internet	biz-internet	0	0	0	0,2,3,4	4	5
12346	10.1.0.1	biz-internet	biz-internet	0	0	0	0,1,2,3,4	5	5
12346	10.1.0.2	biz-internet	biz-internet	0	1	0	0,1,2,3,4	0	5

To view the tunnels statistics on internet transport, type in "mpls" in the search column and hit return.

The screenshot shows the Cisco vManage interface for device BR2-VEDGE1. The 'Device Options' field is set to 'App Routes Statistics'. The search filter is 'mpls'. The table below displays statistics for various flows.

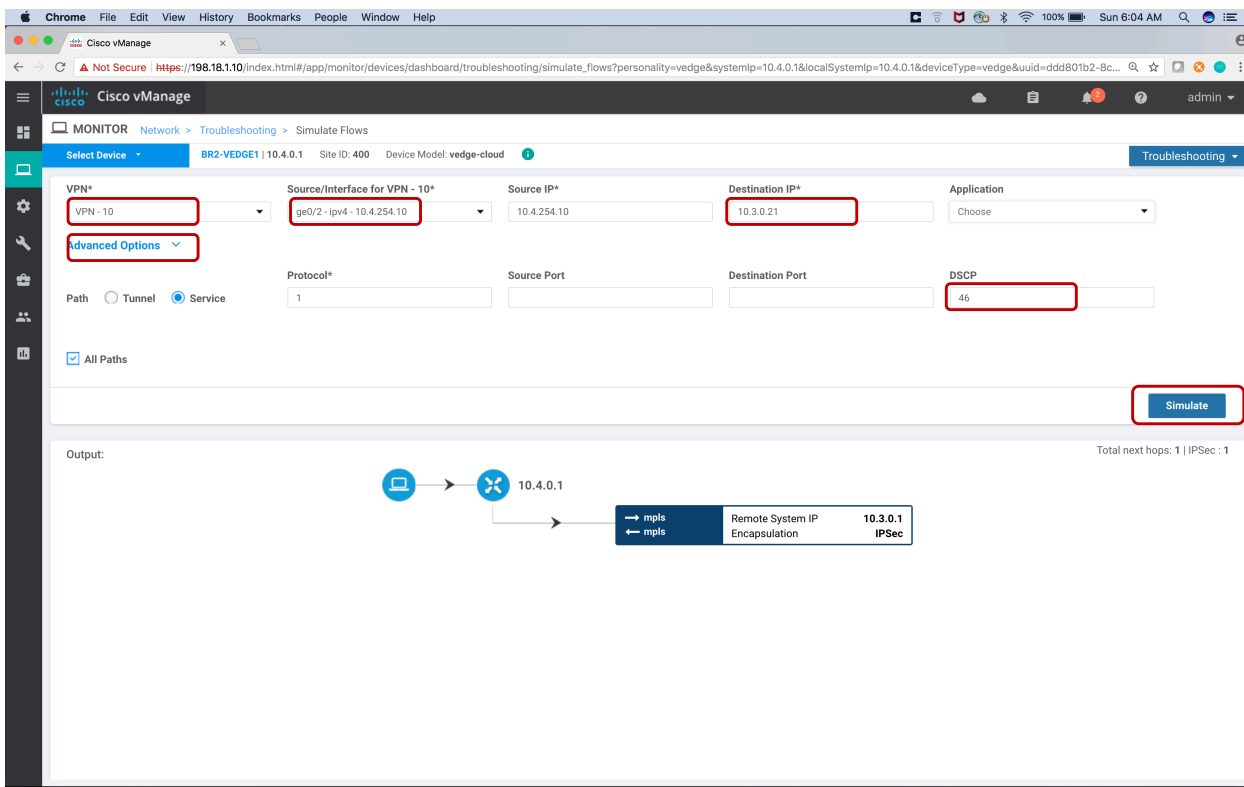
Destination Port	Remote System Ip	Local Color	Remote Color	Mean Loss	Mean Latency	Mean Jitter	SLA Class Index	Index	Total Packets
12366	10.3.0.2	mpls	mpls	0	1	0	0,1,2,3,4	0	5
12366	10.3.0.2	mpls	mpls	0	1	0	0,2,3,4	1	5
12366	10.3.0.2	mpls	mpls	0	1	0	0,2,3,4	2	5
12366	10.3.0.2	mpls	mpls	0	1	0	0,2,3,4	3	5
12366	10.3.0.2	mpls	mpls	0	1	0	0,2,3,4	4	5
12366	10.3.0.2	mpls	mpls	0	1	0	0,2,3,4	5	5
12346	10.3.0.1	mpls	mpls	0	0	0	0,2,3,4	0	5
12346	10.3.0.1	mpls	mpls	0	0	0	0,2,3,4	1	5
12346	10.3.0.1	mpls	mpls	0	0	0	0,2,3,4	2	5
12346	10.3.0.1	mpls	mpls	0	0	0	0,2,3,4	3	5
12346	10.3.0.1	mpls	mpls	0	0	0	0,2,3,4	4	5
12346	10.3.0.1	mpls	mpls	0	0	0	0,2,3,4	5	5
12346	10.1.0.1	mpls	mpls	0	0	0	0,2,3,4	0	5
12346	10.1.0.1	mpls	mpls	0	0	0	0,2,3,4	1	5
12346	10.1.0.1	mpls	mpls	0	0	0	0,2,3,4	2	5
12346	10.1.0.1	mpls	mpls	0	0	0	0,2,3,4	3	5
12346	10.1.0.1	mpls	mpls	0	0	0	0,2,3,4	4	5
12346	10.1.0.1	mpls	mpls	0	0	0	0,1,2,3,4	5	5
12346	10.1.0.2	mpls	mpls	0	0	0	0,1,2,3,4	0	5

Click on the “Troubleshooting” tab and then click on “Simulate Flows”. This will provide simulation on what IPSec tunnels will be used for the defined flow based on policies and transport performance measurements.



Select VPN 10, then select the source interface, put in 10.3.0.21 as the destination address, then click on “Advanced Options”, then put in DSCP value of 46 and click on “Simulate” button.

It shows the traffic class with DSCP of 46 will go over MPLS as the transport meets the SLA (latency 50msec) and is the preferred transport of choice for that traffic.

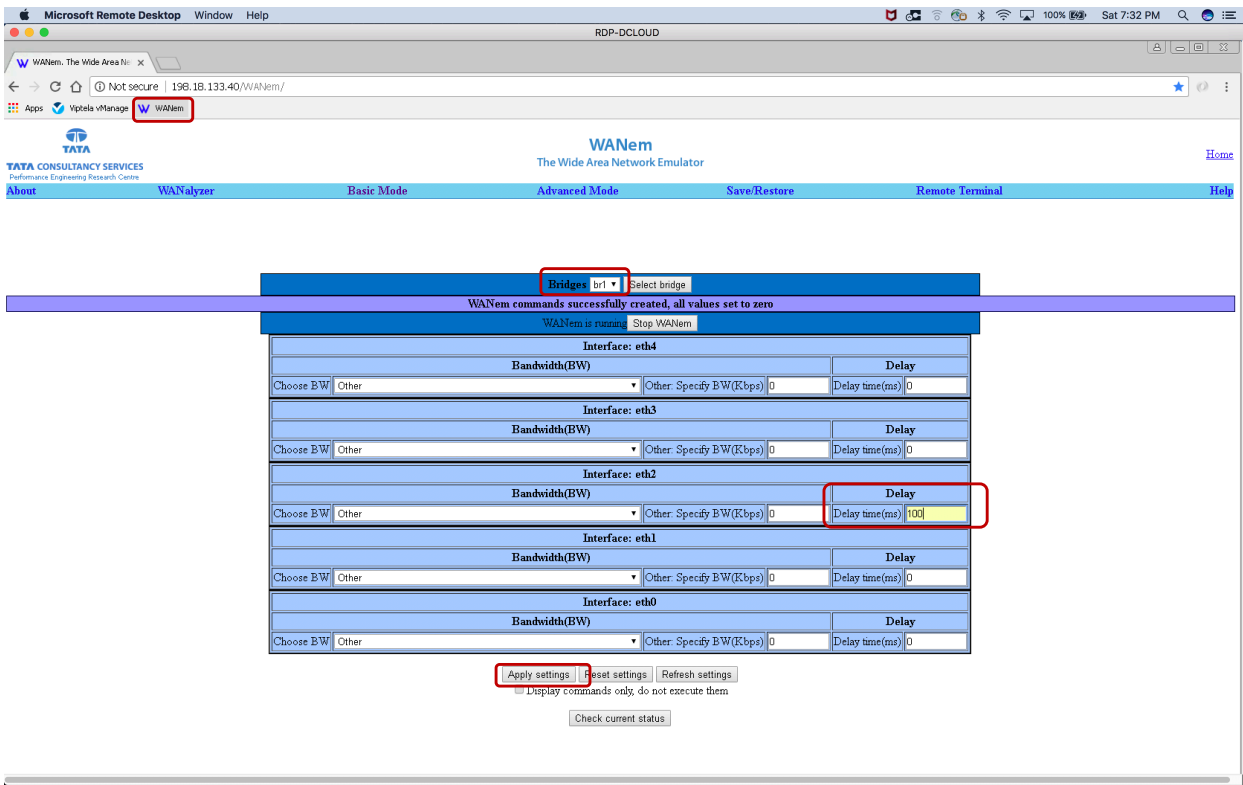


Go to the Chrome browser and click on the “WANem” (Wan Emulator) bookmark.

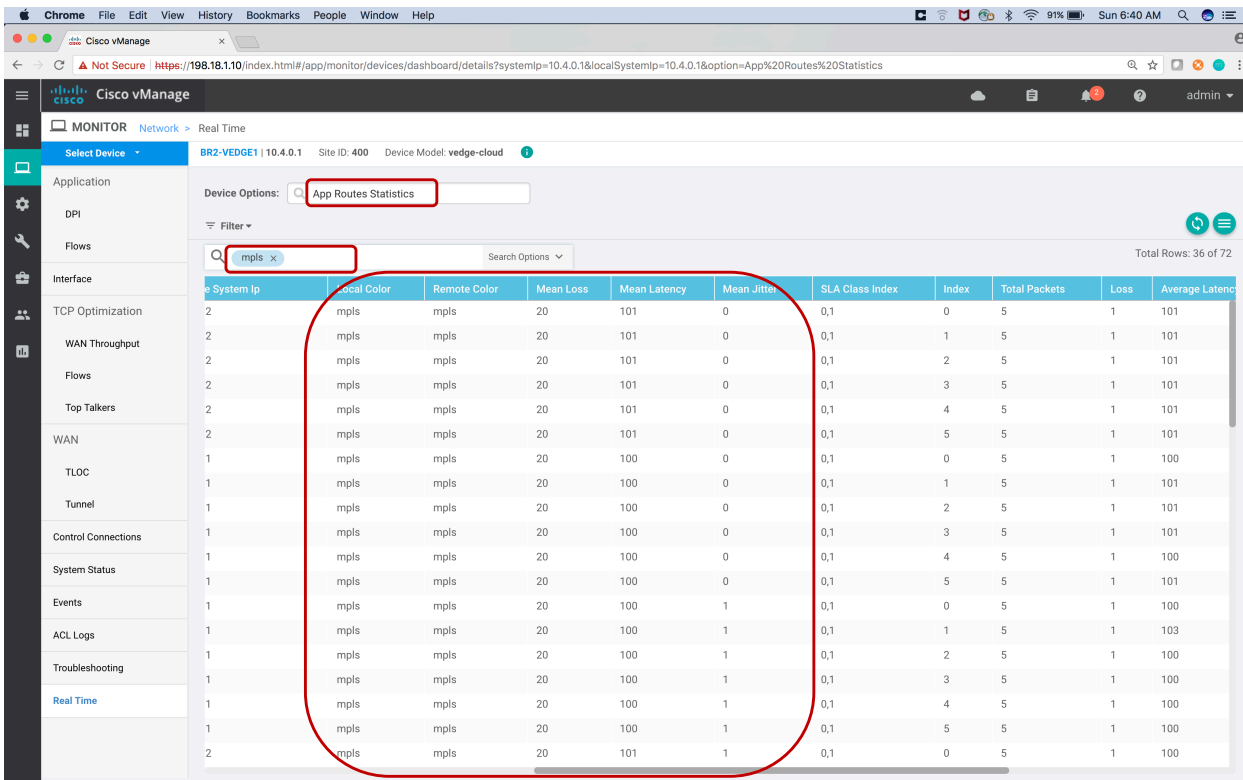
On the page select Bridge “br1” which is connected to the MPLS transport.

Put in a value of 100 msec for delay for “interface 2” which will introduce latency of 100msec on BR2-VEDGE1 on MPLS.

Then click on “Apply Settings” button.

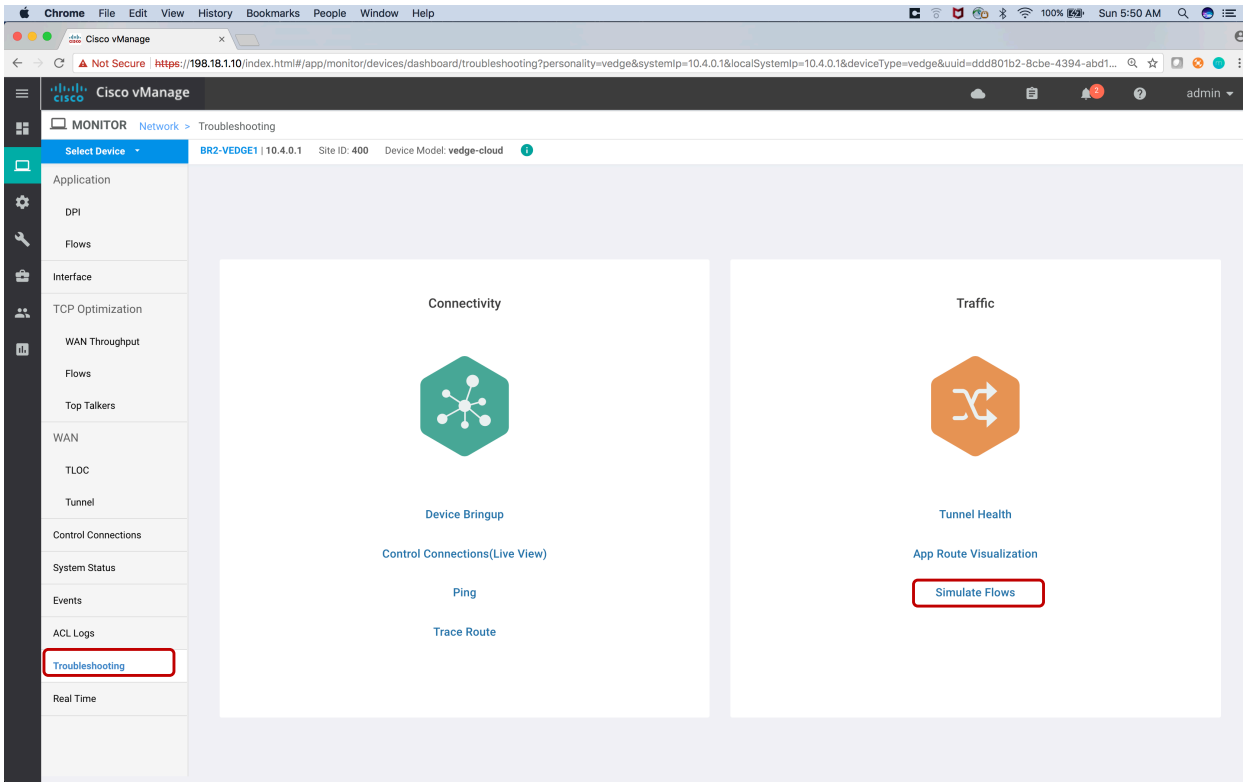


Go back to the vManage's device dashboard and look for App Route Statistics under "Real Time". You will observe high latency on MPLS IPsec Tunnels with no change on Internet tunnels.



The policy has an SLA definition of up to 5% packet loss and 50 msec latency for voice / video applications (DSCP 46) with preferred path of MPLS.

Go to device dashboard and select “Troubleshooting” and then select “Simulate Flows”.



Select VPN 10, then select the source interface, put in 10.3.0.21 as the destination address, then click on “Advanced Options”, then put in DSCP value of 46 and click on “Simulate” button.

It shows the traffic class with DSCP of 46 will go over Internet as the transport meets the SLA (latency 50msec) requirement and the MPLS path is not taken.



The screenshot shows the Cisco vManage web interface for configuring a simulated flow. The page is titled "MONITOR Network > Troubleshooting > Simulate Flows". The selected device is "BR2-VEDGE1 | 10.4.0.1" with Site ID: 400 and Device Model: vedge-cloud. The configuration fields are as follows:

- VPN\*: VPN - 10
- Source/Interface for VPN - 10\*: ge0/2 - ipv4 - 10.4.254.10
- Source IP\*: 10.4.254.10
- Destination IP\*: 10.3.0.21
- Application: Choose
- Path: Tunnel (unselected), Service (selected)
- Protocol\*: 1
- Source Port: (empty)
- Destination Port: (empty)
- DSCP: 46
- All Paths:

A "Simulate" button is located at the bottom right of the configuration area. Below the configuration is an "Output" section showing a network diagram with a laptop icon connected to a router icon labeled "10.4.0.1". An arrow points from the router to a box representing the remote system:

→ biz-internet	Remote System IP	10.3.0.1
← biz-internet	Encapsulation	IPSec

Total next hops: 1 | IPSec: 1

Remove latency from the WAN Emulation tool.

Deactivate the app-route policy from vManage GUI.

# Lab 07 - Cloud OnRamp for SaaS (CloudExpress)

Enterprises are increasingly make use of SaaS applications including Office365, Salesforce, Dropbox, Google Applications etc. Primary method of connecting to these applications is through internet direct from the Branch using Direct internet Access (DIA) or internet access provided from regional Hub or DC locations. A Branch may have multiple DIA exits as well.

The user experience is impacted by the loss, latency and jitter experienced on these internet exits. In the past, the connectivity to SaaS application was static in nature and never accounted for the application performance and/or user experience based on real time performance profile of these paths.

Cisco SD-WAN provides a method to run application probes for each one of these applications and compute the Viptela Quality of Experience (vQoE) score for each one of the paths (DIA or regional Hub/DC internet exits). vEdge routers then based on vQoE scores to pick the best optimal path for a given SaaS application.

## Steps

CloudExpress is off by default in Cisco SD-WAN. All aspects, including configurations and visibility, are provided from vManage.

The first step to enable CloudExpress is to enable it in vManage Settings. For this demo, it is already enabled for the two DCs and Branch-1.

From vManage Dashboard go to "Administration" -> "Settings"

The screenshot shows the vManage vManage dashboard. The left sidebar contains a navigation menu with 'Administration' and 'Settings' highlighted in red. The main dashboard area displays various system health and performance metrics:

- Control Status (Total 9):** Control Up: 9, Control Down: 0, Partial Connectivity: 0, No Connectivity: 0.
- Site Health View (Total 4):** Full Connectivity: 4 sites, Partial Connectivity: 0 sites, No Connectivity: 0 sites.
- Transport Interface Distribution:** < 10 Mbps: 19 sites, 10 Mbps - 100 Mbps: 0 sites, 100 Mbps - 500 Mbps: 0 sites, > 500 Mbps: 0 sites.
- vEdge Health (Total 7):** Normal: 7, Warning: 0, Error: 0.
- Transport Health:** Line graph showing health percentage over time.
- Top Applications:** Bar chart showing usage for various applications.
- Application-Aware Routing:** Table showing tunnel endpoints, average latency, and average loss.

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)
BR1-VEGE1:mpls-10.4.0.1:mpls	19.294	3.419
BR1-VEGE2:mpls-10.4.0.1:mpls	19.502	3.415
10.4.0.1:mpls-BR1-VEGE1:mpls	17.781	3.227
10.4.0.1:mpls-BR1-VEGE2:mpls	17.846	3.227

Click on “Edit” for CloudExpress.


The screenshot shows the Cisco vManage Administration Settings page. The 'CloudExpress' setting is highlighted with a red box. The table below lists various settings and their values.

Setting Name	Value	Actions
Organization Name	Cisco Sy1 - 19968	View
vBond	vbond.cisco.com : 12346	View   Edit
Certificate Authorization	Automated	View   Edit
vEdge Cloud Certificate Authorization	Automated	View   Edit
Web Server Certificate	04 Nov 2019 7:07:40 AM	CSR   Certificate
Enforce Software Version (ZTP)	Disabled	View   Edit
Banner	Disabled	View   Edit
Statistics Setting		View   Edit
CloudExpress	Enabled	View   Edit
vAnalytics	Disabled	View   Edit
Client Session Timeout	Disabled	View   Edit
Data Stream	Disabled	View   Edit
Tenancy Mode	Single Tenant	View   Edit
Statistics Configuration	Collection Interval: 5 minutes	View   Edit
Maintenance Window	Not Configured	Edit
Statistics Database Configuration	Maximum Available Space: 59.0586	View   Edit

Here you would “Enable” the service and save it. Press “Cancel” to exit out.

The screenshot displays the Cisco vManage Administration Settings page. The page is titled "ADMINISTRATION | SETTINGS" and lists various configuration items. The "CloudExpress" section is expanded, showing "Enable CloudExpress" with "Enabled" selected. A red box highlights the "Cancel" button. The "Save" button is also visible.

Configuration Item	Value	Actions
Organization Name	Cisco Sy1 - 19968	View
vBond	vbond.cisco.com : 12346	View   Edit
Certificate Authorization	Automated	View   Edit
vEdge Cloud Certificate Authorization	Automated	View   Edit
Web Server Certificate	04 Nov 2019 7:07:40 AM	CSR   Certificate
Enforce Software Version (ZTP)	Disabled	View   Edit
Banner	Disabled	View   Edit
Statistics Setting		View   Edit
CloudExpress	Enabled	
Enable CloudExpress	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Save	Cancel	
vAnalytics	Disabled	View   Edit
Client Session Timeout	Disabled	View   Edit
Data Stream	Disabled	View   Edit
Tenancy Mode	Single Tenant	View   Edit
Statistics Configuration	Collection Interval: 5 minutes	View   Edit

Go to CloudExpress Dashboard by clicking on the Cloud OnRamp icon (  ) and select "Cloud OnRamp for SaaS (Cloud Express)".

Or go to Configuration -> Cloud OnRamp for SaaS (CloudExpress).

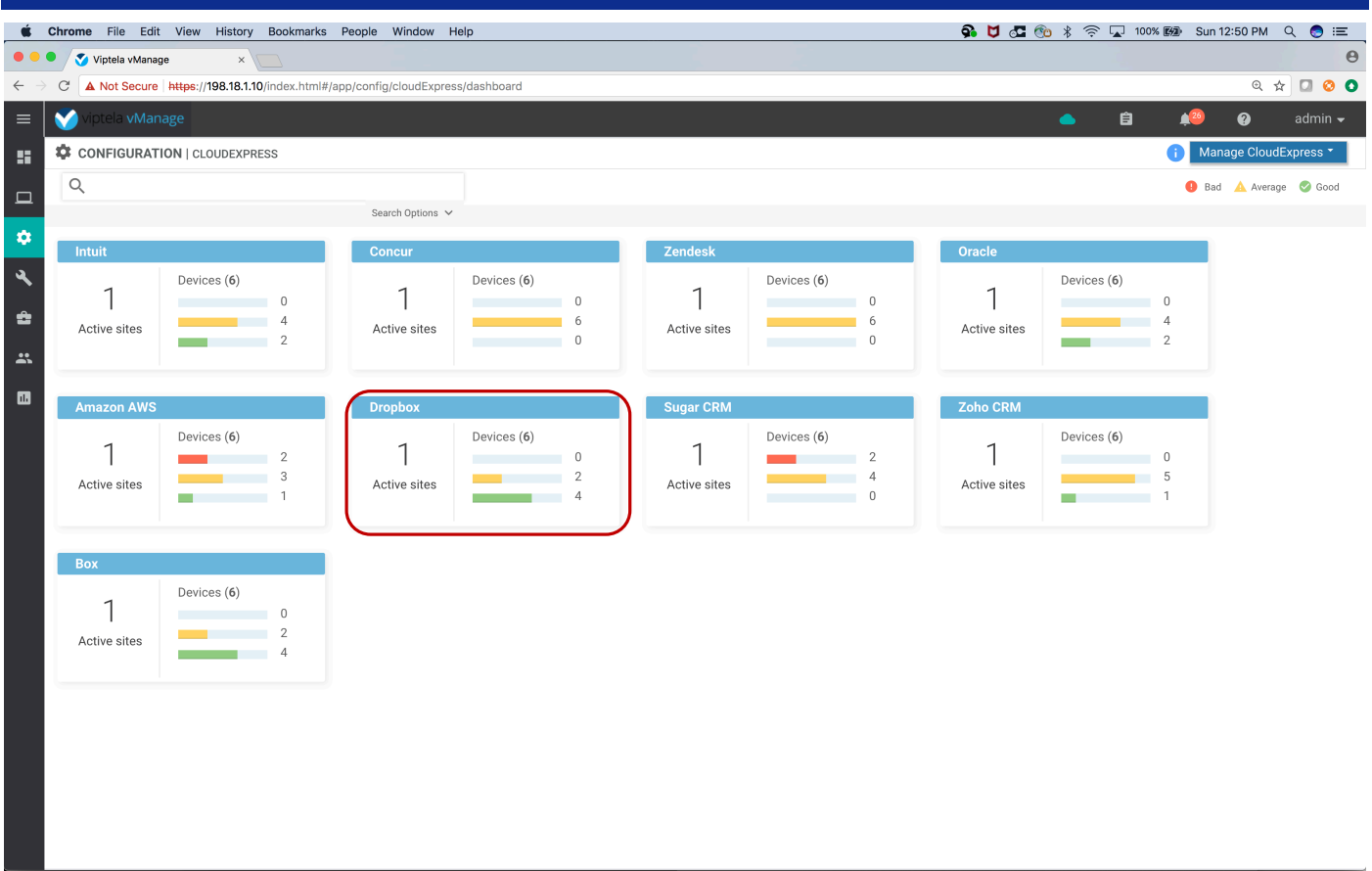
The screenshot shows the Cisco vManage dashboard with the following sections:

- Dashboard Summary:** vSmart - 2, vEdge - 7, vBond - 2, vManage - 1, Cloud OnRamp for SaaS (Cloud Express) - 0, Cloud OnRamp for IaaS (AWS) - 0, Warning - 0, Invalid - 0.
- Control Status (Total 9):** Control Up: 9, Partial: 0, Control Down: 0.
- Site Health View (Total 4):** Full Connectivity: 4 sites, Partial Connectivity: 0 sites, No Connectivity: 0 sites.
- Transport Interface Distribution:** < 10 Mbps: 16, 10 Mbps - 100 Mbps: 0, 100 Mbps - 500 Mbps: 0, > 500 Mbps: 0.
- vEdge Inventory:** Total: 7, Authorized: 7, Deployed: 7, Staging: 0.
- vEdge Health (Total 7):** Normal: 1, Warning: 6, Error: 0.
- Transport Health:** Type: By Loss. Line graph showing 0% loss.
- Top Applications:** Bar chart showing usage for various applications.
- Application-Aware Routing:** Table with columns: Tunnel Endpoints, Avg. Latency (ms), Avg. Loss (%).

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)
BR2-VEEDGE1.mpls-DC2-VEEDGE1.mpls	81.656	16.186
BR2-VEEDGE1.mpls-DC2-VEEDGE2.mpls	81.886	16.184
BR2-VEEDGE1.mpls-BR1-VEEDGE1.mpls	81.58	16.184
BR2-VEEDGE1.mpls-BR1-VEEDGE2.mpls	82.07	16.184

CloudExpress dashboard will show you all the applications that are enabled for CloudExpress, number of sites and number of devices.

Click on one of the application's tab to view details for that application.



The application dashboard shows the list of devices and the reported Viptela Quality of Experience (vQoE) score for the application.

Click on the graph icon to get historical vQoE score graph for that particular device.

Chrome File Edit View History Bookmarks People Window Help

Viptela vManage

Not Secure https://198.18.1.10/index.html#/app/config/cloudExpress/applicationDetails/dropbox

admin

CONFIGURATION CloudExpress > Dropbox

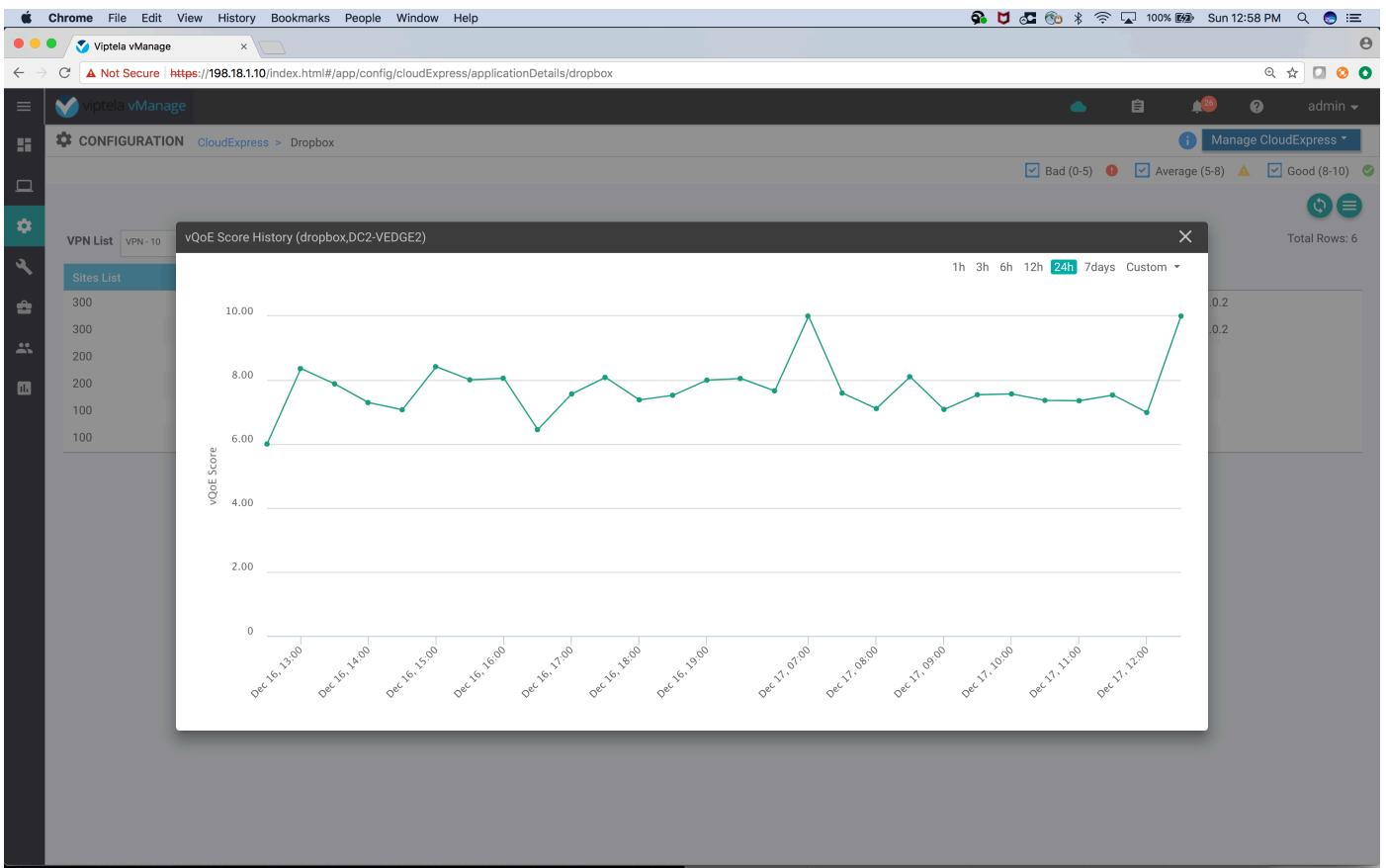
Manage CloudExpress

Bad (0-5) Average (5-8) Good (8-10)

VPN List VPN-10

Total Rows: 6

Sites List	Hostname	vQoE Status	vQoE Score	DIA Status	Selected Interface	
300	BR1-VEDGE1	✓	10.0	gateway	N/A	10.1.0.2
300	BR1-VEDGE2	✓	10.0	gateway	N/A	10.1.0.2
200	DC2-VEDGE2	✓	10.0	local	ge0/2	N/A
200	DC2-VEDGE1	⚠	6.0	local	ge0/2	N/A
100	DC1-VEDGE2	✓	10.0	local	ge0/2	N/A
100	DC1-VEDGE1	⚠	6.0	local	ge0/2	N/A



To add in a new application to the list go to CloudExpress dashboard. Click on the “Manage CloudExpress” pull down and select “Applications”.



The screenshot shows the Viptela vManage CloudExpress dashboard. The browser address bar indicates the URL is <https://198.18.1.10/index.html#/app/config/cloudExpress/dashboard>. The dashboard title is "CONFIGURATION | CLOUDEXPRESS". A search bar is present at the top. A dropdown menu is open, showing options: "Applications", "Client Sites", "Gateways", and "Direct Internet Access(DIA) Sites". The main content area displays several application tiles, each with a count of "1" and "Active sites", and a bar chart for "Devices (6)".

Application	Active sites	Devices (6)
Intuit	3	0, 3, 3
Concur	2	0, 2, 4
Zendesk	5	0, 5, 1
Oracle	3	0, 3, 3
Amazon AWS	6	0, 6, 0
Dropbox	3	0, 3, 3
Sugar CRM	3	3, 3, 0
Zoho CRM	4	0, 4, 2
Box	1	0, 1, 5

On the next page click on the “Add Applications and VPNs” button.

0 Rows Selected **Add Applications and VPN**

Search

Total Rows: 9

Applications	VPN
<input type="checkbox"/> Intuit	10
<input type="checkbox"/> Oracle	10
<input type="checkbox"/> Amazon AWS	10
<input type="checkbox"/> Concur	10
<input type="checkbox"/> Zendesk	10
<input type="checkbox"/> Dropbox	10
<input type="checkbox"/> Sugar CRM	10
<input type="checkbox"/> Zoho CRM	10
<input type="checkbox"/> Box	10

Reset Save Changes Cancel

Type in "office" in the applications box and select "Office 365" in the drop down.

The screenshot shows the Viptela vManage interface. At the top, there is a navigation bar with 'CONFIGURATION', 'CloudExpress', and 'Manage Applications'. Below this is a table with columns for 'Applications' and 'VPN'. The table contains the following data:

Applications	VPN
<input type="checkbox"/> Intuit	10
<input type="checkbox"/> Oracle	10
<input type="checkbox"/> Amazon AWS	10
<input type="checkbox"/> Concur	
<input type="checkbox"/> Zendesk	
<input type="checkbox"/> Dropbox	
<input type="checkbox"/> Sugar CRM	
<input type="checkbox"/> Zoho CRM	
<input type="checkbox"/> Box	

An 'Add Applications & VPN' dialog box is open in the center. It has two main sections: 'Applications' and 'VPN'. In the 'Applications' section, a dropdown menu is open, showing 'Office 365' selected. In the 'VPN' section, the number '10' is entered. Below the 'VPN' field, there is a red 'Required' label. At the bottom of the dialog, there are 'Add' and 'Cancel' buttons. The 'Add' button is highlighted in blue.

Enter Corporate VPN number (10) and click “Add” button.

The screenshot shows the Viptela vManage web interface. At the top, there is a navigation bar with 'CONFIGURATION', 'CloudExpress', and 'Manage Applications'. Below this is a table with columns for 'Applications' and 'VPN'. A modal dialog titled 'Add Applications & VPN' is open in the center. The dialog contains two input fields: 'Applications' with the value 'Office 365' and 'VPN' with the value '10'. The 'Add' button at the bottom of the dialog is highlighted with a red box. In the background, a table lists various applications and their corresponding VPN values.

Applications	VPN
<input type="checkbox"/> Intuit	10
<input type="checkbox"/> Oracle	10
<input type="checkbox"/> Amazon AWS	10
<input type="checkbox"/> Concur	
<input type="checkbox"/> Zendesk	
<input type="checkbox"/> Dropbox	
<input type="checkbox"/> Sugar CRM	
<input type="checkbox"/> Zoho CRM	
<input type="checkbox"/> Box	

Save the changes by clicking the “Save Changes” button.

0 Rows Selected | Add Applications and VPN

Search

Total Rows: 10

Applications	VPN	
<input type="checkbox"/> Intuit	10	/
<input type="checkbox"/> Oracle	10	/
<input type="checkbox"/> Amazon AWS	10	/
<input type="checkbox"/> Concur	10	/
<input type="checkbox"/> Zendesk	10	/
<input type="checkbox"/> Dropbox	10	/
<input type="checkbox"/> Sugar CRM	10	/
<input type="checkbox"/> Zoho CRM	10	/
<input type="checkbox"/> Box	10	/
<input type="checkbox"/> Google Apps	10	/

Reset | Save Changes | Cancel

Wait till the new application (goggle apps) configuration of the devices is successful.

The screenshot shows the vManage interface with a 'TASK VIEW' for 'Push Feature Template Configuration'. The task was initiated by 'admin' from '10.16.27.161'. It shows 'Total Task: 4 | Success: 4'. A table lists the results for four devices, with the 'Status' column highlighted by a red box. The table columns are: Status, Message, Chassis Number, Device Model, Hostname, System IP, and Site ID.

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID
Success	Done - Push Feature Temp...	ebdc8bd9-17e5-4eb3-a5e0...	vedge-cloud	DC1-VEDGE1	10.1.0.1	100
Success	Done - Push Feature Temp...	f21dbb35-30b3-47f4-93bb...	vedge-cloud	DC1-VEDGE2	10.1.0.2	100
Success	Done - Push Feature Temp...	9e785ad7-558a-40c6-b0c...	vedge-cloud	DC2-VEDGE1	10.2.0.1	200
Success	Done - Push Feature Temp...	b3265c5c-3db6-4d25-9d3...	vedge-cloud	DC2-VEDGE2	10.2.0.2	200

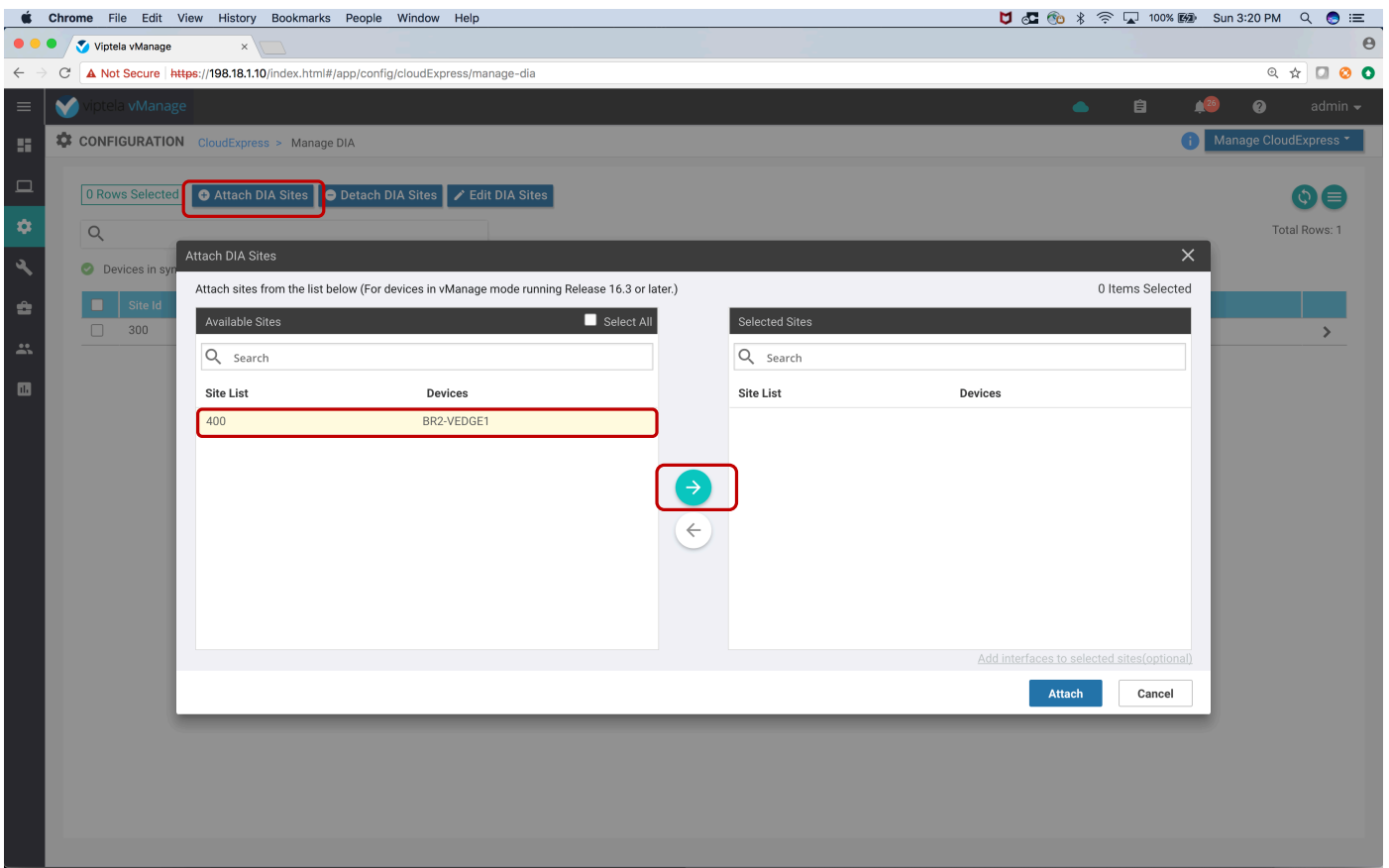
In order to configure the BR2-VEDGE1 as the CloudExpress DIA sites, go to CloudExpress dashboard.

Click on "Manage CloudExpress" button and select "Diresect Internet Access (DIA) Sites".

The screenshot shows the Viptela vManage CloudExpress dashboard. The page title is 'CONFIGURATION | CLOUDEXPRESS'. A search bar is at the top. A dropdown menu for 'Manage CloudExpress' is open, showing options: Applications, Client Sites, Gateways, and Direct Internet Access(DIA) Sites. The dashboard displays a grid of application configurations, each with a '1' in a box, 'Active sites', and a bar chart for 'Devices (6)'. The applications shown are Intuit, Concur, Zendesk, Oracle, Amazon AWS, Dropbox, Sugar CRM, Zoho CRM, Office 365, Box, and Goto Meeting.

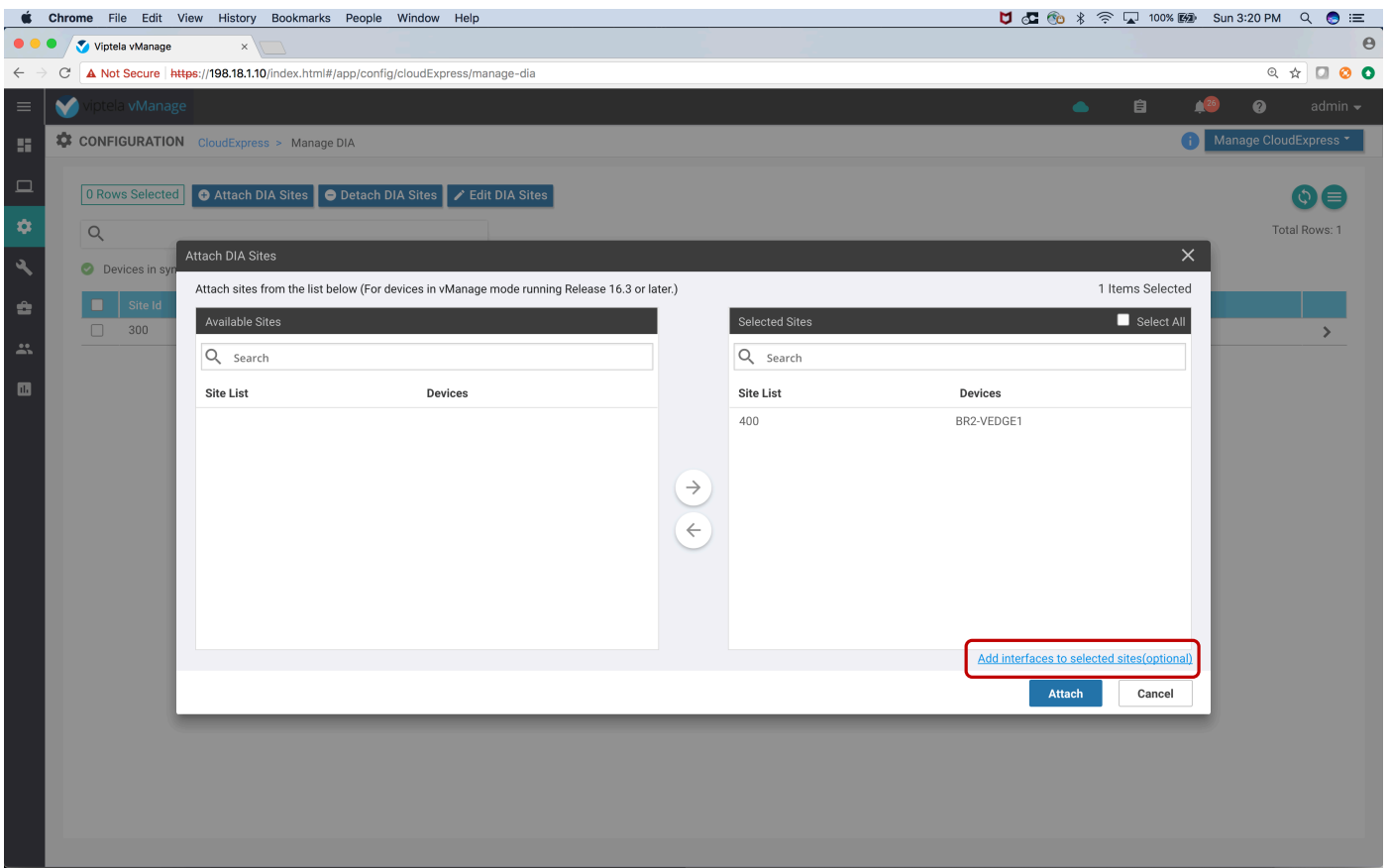
Application	Active sites	Devices (6)
Intuit	6	0
Concur	6	0
Zendesk	6	0
Oracle	5	1
Amazon AWS	4	2
Dropbox	6	0
Sugar CRM	2	4
Zoho CRM	6	0
Office 365	6	0
Box	6	0
Goto Meeting	5	1

Click on the “Attach DIA Sites” button. On the next pop-up, select BR2-VEDGE1 and Click the right arrow key to move the device in right hand column.

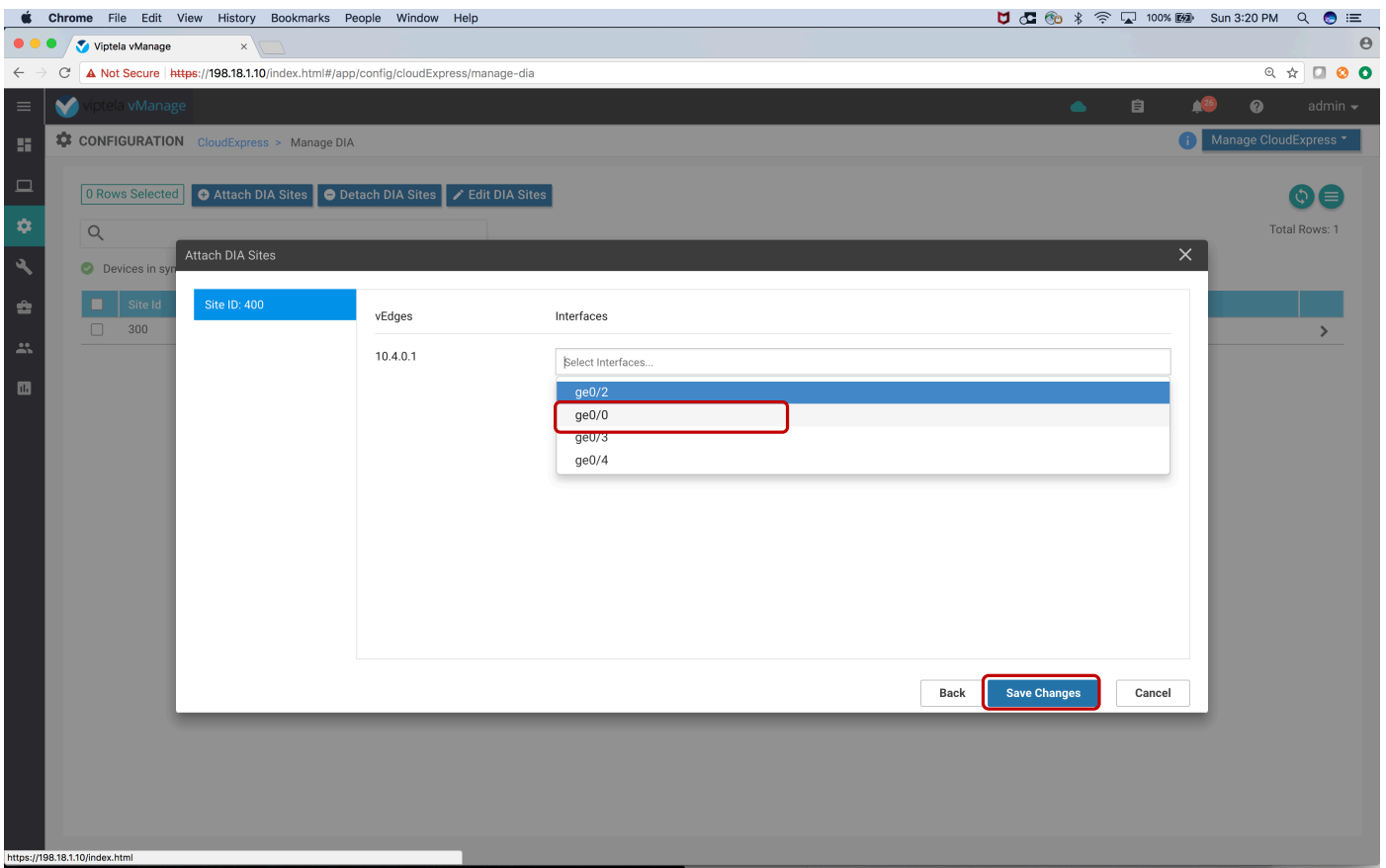


Click on the link “Add interfaces to selected Sites”.

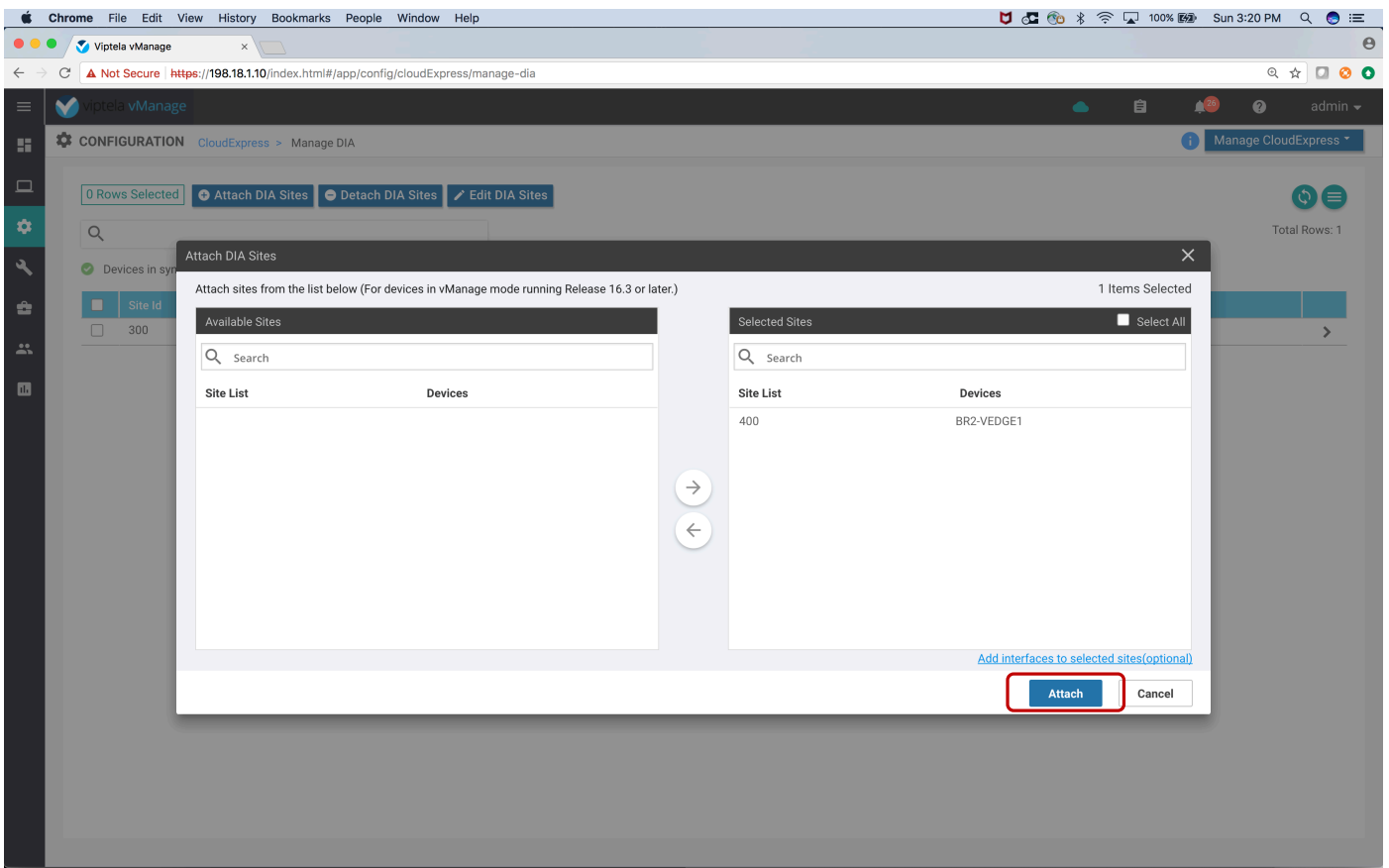




Click in the box “Select Interfaces”, select ge0/0 (internet) interface on BR2-VEEDGE1. Then click on “Save Changes” button.



Click on the “Attach” button.



Wait till the CloudExpress configuration push to BR2-VEEDGE1 succeeds.

The screenshot shows the Viptela vManage interface. The main heading is "TASK VIEW" with a sub-heading "Push Feature Template Configuration". It indicates the task was initiated by "admin" from "10.16.27.161". Below this, it shows "Total Task: 1 | Success : 1". A table displays the task details:

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	
Success	Done - Push Feature Temp...	ddd801b2-8cbe-4394-abd...	vedge-cloud	BR2-VEDGE1	10.4.0.1	400	10.10.10.10

Go back to CloudExpress dashboard and you will see the new application (O365) and the new site (site400) has been provisioned and is operational.

# Lab 08 - Multi-Topology/Different Topologies Per VPN

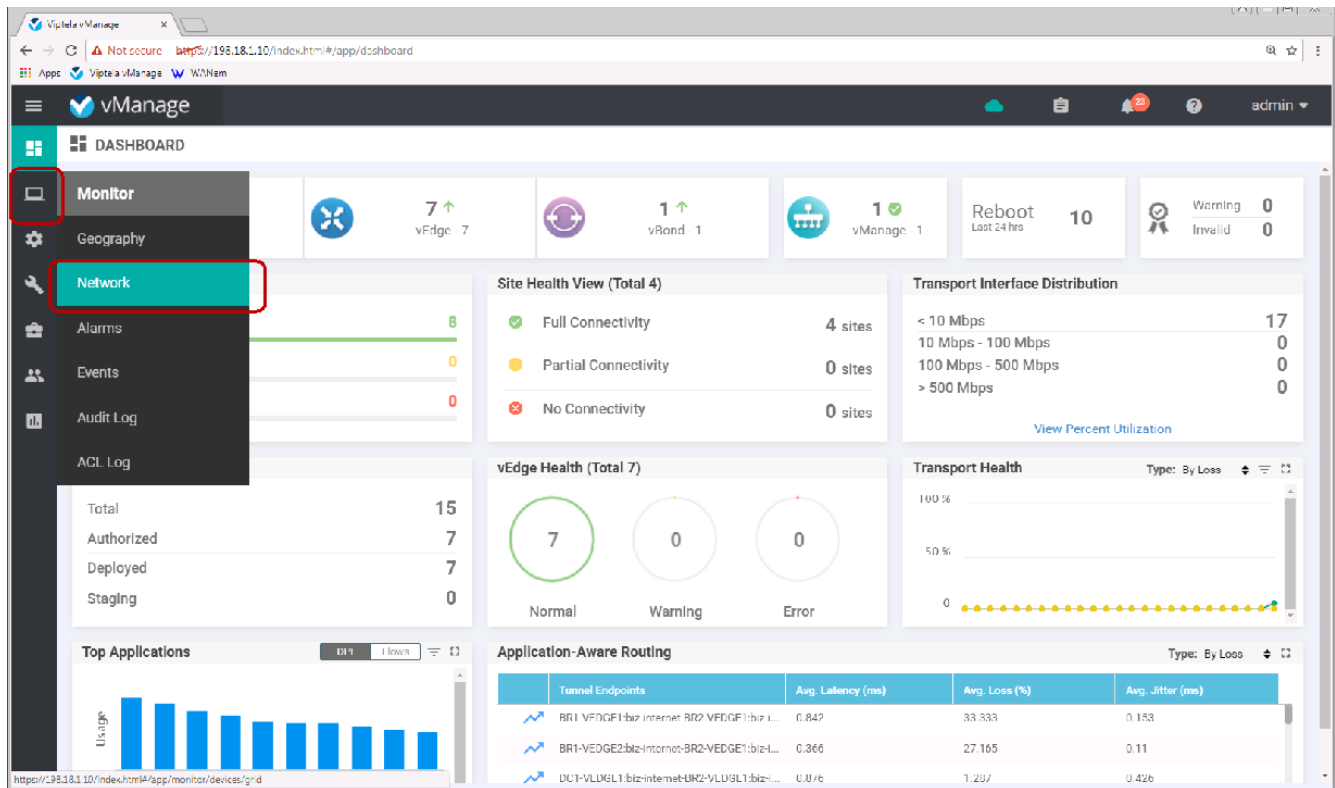
Enterprises may have multiple VPN segments and may need different connectivity models/topologies. The default in Cisco SD-WAN is to have full mesh for all VPNs. In scenario 2 we demonstrated how you can restrict ALL VPNs to be Hub-n-Spoke.

In this scenario, we will demonstrate the following topologies for different VPNs using policies.

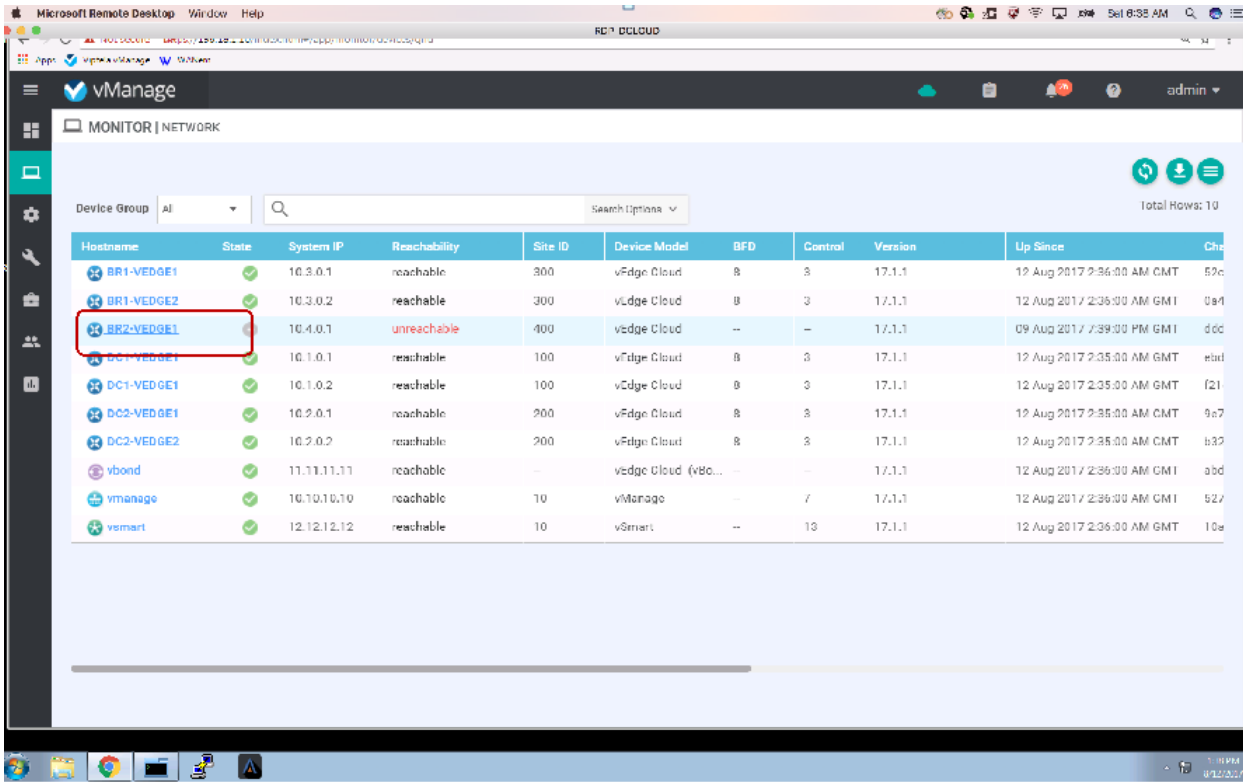
- Corporate VPN 10 – Full Mesh
- PCI/IOT VPN 20 – Hub-n-Spoke
- GuestWiFi VPN 40 – DIA ONLY in Branches

## Steps

Go to vManage dashboard. Click on the Monitor icon and click on Network from the drop down.



Find BR2-VEDGE1 and click on the name.



Select Troubleshooting from the left column and then select "Traceroute" option.

The screenshot shows the Cisco vManage web interface. At the top, there is a navigation bar with 'MONITOR' and 'Network > Troubleshooting'. A yellow warning banner states: "'Data Stream' is disabled. Go to Settings page to enable Data Stream to use Debug Logs.' Below the navigation bar, a sidebar on the left lists various monitoring categories: Application, DPI, Flows, Interface, TCP Optimization, WAN Throughput, Flows, Top Talkers, WAN, TLOC, Tunnel, Control Connections, System Status, Events, ACL Logs, Troubleshooting (highlighted with a red box), and Real Time. The main content area is divided into two columns: 'Connectivity' and 'Traffic'. The 'Connectivity' column contains a green hexagonal icon with a network diagram, followed by the text 'Device Bringup', 'Control Connections(Live View)', 'Ping', and a red-bordered button labeled 'Trace Route'. The 'Traffic' column contains an orange hexagonal icon with a network diagram, followed by the text 'Tunnel Health', 'App Route Visualization', and 'Simulate Flows'. The browser's address bar shows the URL: 'https://198.18.1.10/index.html#/app/monitor/devices/dashboard/troubleshooting?personality=vedge&systemip=10.4.0.1&localSystemip=10.4.0.1&deviceType=vedge&uuid=ddd801b2-8cbe-4394-abd1...'

Put in 10.3.0.21 as the destination IP. Select VPN 10 from drop down menu. And click on “Start” button. It shows direct path between Branch1 and Branch2 for VPN 10.

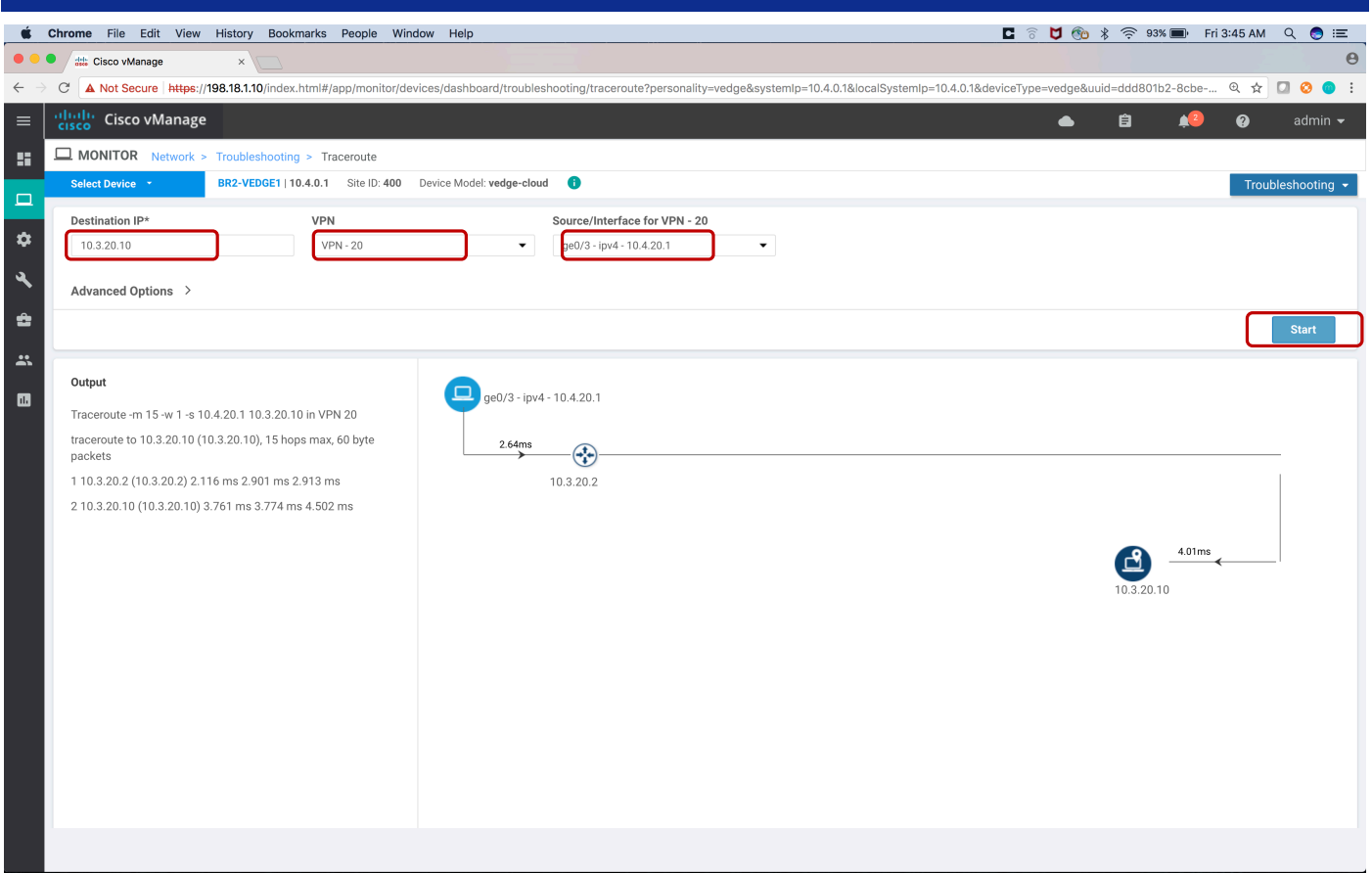
The screenshot shows the Cisco vManage interface for a Traceroute operation. The 'Destination IP\*' field is set to 10.3.0.21, the 'VPN' dropdown is set to VPN - 10, and the 'Source/Interface for VPN - 10' dropdown is set to Choose/Reset selections. A red box highlights the 'Start' button. The 'Output' section displays the following text:

```
Traceroute -m 15 -w 1 10.3.0.21 in VPN 10
traceroute to 10.3.0.21 (10.3.0.21), 15 hops max, 60 byte packets
 1 10.3.0.2 (10.3.0.2) 2.610 ms 3.347 ms 3.432 ms
 2 10.3.0.21 (10.3.0.21) 4.136 ms 4.290 ms 4.370 ms
```

The diagram shows a direct connection between 10.4.0.1 and 10.3.0.21. The path is: 10.4.0.1 (3.13ms) -> 10.3.0.2 -> 10.3.0.21 (4.27ms).

Do the same for VPN 20. This time the destination IP would be 10.3.20.10 and VPN would be 20. It shows direct connectivity between Branch1 and Branch2 for VPN 20.





Chrome File Edit View History Bookmarks People Window Help

Cisco vManage

Not Secure https://198.18.1.10/index.html#/app/monitor/devices/dashboard/troubleshooting/traceroute?personality=vedge&systemip=10.4.0.1&localSystemip=10.4.0.1&deviceType=vedge&uid=ddd801b2-8cbe-...

Cisco vManage

MONITOR Network > Troubleshooting > Traceroute

Select Device BR2-VEDGE1 | 10.4.0.1 Site ID: 400 Device Model: vedge-cloud Troubleshooting

Destination IP\* 10.3.20.10 VPN VPN - 20 Source/Interface for VPN - 20 ge0/3 - ipv4 - 10.4.20.1

Advanced Options > Start

Output

Traceroute -m 15 -w 1 -s 10.4.20.1 10.3.20.10 in VPN 20  
traceroute to 10.3.20.10 (10.3.20.10), 15 hops max, 60 byte packets

```
1 10.3.20.2 (10.3.20.2) 2.116 ms 2.901 ms 2.913 ms
2 10.3.20.10 (10.3.20.10) 3.761 ms 3.774 ms 4.502 ms
```

ge0/3 - ipv4 - 10.4.20.1

2.64ms

10.3.20.2

4.01ms

10.3.20.10

Go to vManage dashboard and go to Configuration and select Policies.

The screenshot shows the Cisco vManage dashboard interface. At the top, there's a navigation bar with 'vManage' and a user profile 'admin'. Below this is a 'DASHBOARD' section with several key metrics: Configuration (1 up, 1 down), vEdge (7 up, 7 down), vCloud (1 up, 1 down), vManage (1 up, 1 down), a Reboot timer (20), and Warning/Invalid counts (0 each). A left-hand navigation menu is visible, with 'Policies' highlighted in red. The main dashboard area contains several widgets: 'Site Health View (Total 4)' showing connectivity status (Full, Partial, No Connectivity); 'Transport Interface Distribution' showing bandwidth usage across different ranges; 'vEdge Inventory' showing counts for Total, Authorized, Deployed, and Staging; 'vEdge Health (Total 7)' with three status gauges (Normal: 7, Warning: 0, Error: 0); 'Transport Health' with a line graph; 'Top Applications' with a bar chart; and 'Application-Aware Routing' with a table of tunnel endpoints.

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
BR1-VL201-mp1-DC1-ALDUL2mps	0.970	2.219	0.007
BR1-VEDGE1-mp1-DC1-VEDGE1mps	0.371	2.144	0.005
BR1-VEDGE1-mp1-DC1-VEDGE1mps	0.407	1.500	0.015
BR1-VEDGE1-mp1-DC1-VEDGE1mps	0.340	1.698	0.027

Click in the right most column of the policy named "MultiTopologyPolicy". From pull down click on "Activate".

The screenshot shows the Viptela vManage interface. The main content area displays a table of policies under the 'Centralized Policy' tab. The table has columns for Name, Description, Type, Activated, Updated By, and Policy Version. The 'MultiTopologyPolicy' row is highlighted in yellow. A context menu is open over the rightmost column of this row, showing options: View, Preview, Copy, Edit, Delete, and Activate. The 'Activate' option is highlighted with a red box.

Name	Description	Type	Activated	Updated By	Policy Version	
PreferDC1Default	Prefer Default Route firm DC1	UI Policy Builder	false	admin	08112017T223402379	11 Aug 2017 3:34:02 PM PDT
DCPreferencePerRegion	Prefer DC1 for BR1 and DC2 f...	UI Policy Builder	false	admin	08112017T223936887	16 Dec 2017 2:18:35 PM PST
MultiTopologyPolicy	Creating Topologies for corp, ...	UI Policy Builder	false	admin	09182017T114628126	18 Sep 2017 4:35:38 AM PDT
MultiTopologyPlusFWInsertion	Multi-Topology with FW Insert...	UI Policy Builder	false	admin	12162017T164629792	18 Dec 2017
MultiTopologyPlusAppRoute	App Route with Multi Topology	UI Policy Builder	false	admin	12172017T014214976	18 Sep 2017
StrictHub-n-Spoke	Hub-n-Spoke for ALL VPNs	UI Policy Builder	false	admin	12152017T134720152	15 Dec 2017
MultiTopologyPlusACL	Using Data Policy to impleme...	UI Policy Builder	false	admin	12162017T221137925	16 Dec 2017

Click on "Activate" button on the pop-up.

The screenshot shows the Viptela vManage web interface. The browser address bar displays `https://198.18.1.10/index.html#/app/config/policy/centralized_policy/policies`. The page title is "CONFIGURATION | POLICIES" and the sub-tab is "Centralized Policy". A table lists several policies, with the "MultiTopologyPolicy" row highlighted. A modal dialog box titled "Activate Policy" is open, displaying the message: "Policy will be applied to the reachable vSmarts: 12.12.12.12, 22.22.22.22". The dialog has "Activate" and "Cancel" buttons, with "Activate" highlighted by a red box.

Name	Description	Type	Activated	Updated By	Policy Version	
PreferDC1Default	Prefer Default Route frm DC1	UI Policy Builder	false	admin	08112017T223402379	11 Aug 2017 3:34:02 PM PDT ...
DCPreferencePerRegion	Prefer DC1 for BR1 and DC2 f...	UI Policy Builder	false	admin	08112017T223936887	16 Dec 2017 2:18:35 PM PST ...
MultiTopologyPolicy	Creating Topologies for corp...	UI Policy Builder	false	admin	09182017T114628126	18 Sep 2017 4:35:38 AM PDT ...
MultiTopologyPlusFWInsertion	Multi-Topology with FW In...				12162017T1164629792	18 Dec 2017 3:25:25 AM PST ...
MultiTopologyPlusAppRoute	App Route with Multi Topo...				12172017T014214976	18 Sep 2017 4:16:07 PM PDT ...
StrictHub-n-Spoke	Hub-n-Spoke for ALL VPN...				12152017T1134720152	15 Dec 2017 5:37:44 AM PST ...
MultiTopologyPlusACL	Using Data Policy to imple...				12162017T221137925	16 Dec 2017 2:08:43 PM PST ...

Wait until the policy has been successfully pushed to the vSmarts. Activation Status would change to "Success".

The screenshot shows the vManage vTask View interface. At the top, it displays 'TASK VIEW' and 'Push vSmart Policy | Validation Success'. Below this, it indicates 'Total Task: 2 | Success : 2'. A table lists the task details:

Status	Message	Hostname	System IP	Site ID	
Success	Done - Push vSmart Policy	vSmart-1	12.12.12.12	10	10.10.10.10
Success	Done - Push vSmart Policy	vSmart-2	22.22.22.22	20	10.10.10.10

The 'Status' column in the table is highlighted with a red box. The interface also shows a search bar and 'Total Rows: 2 of 2'.

To validate full mesh for VPN 10 and Hub-n-Spoke for VPN 20, go to the dashboard for BR2-VEGGE1.

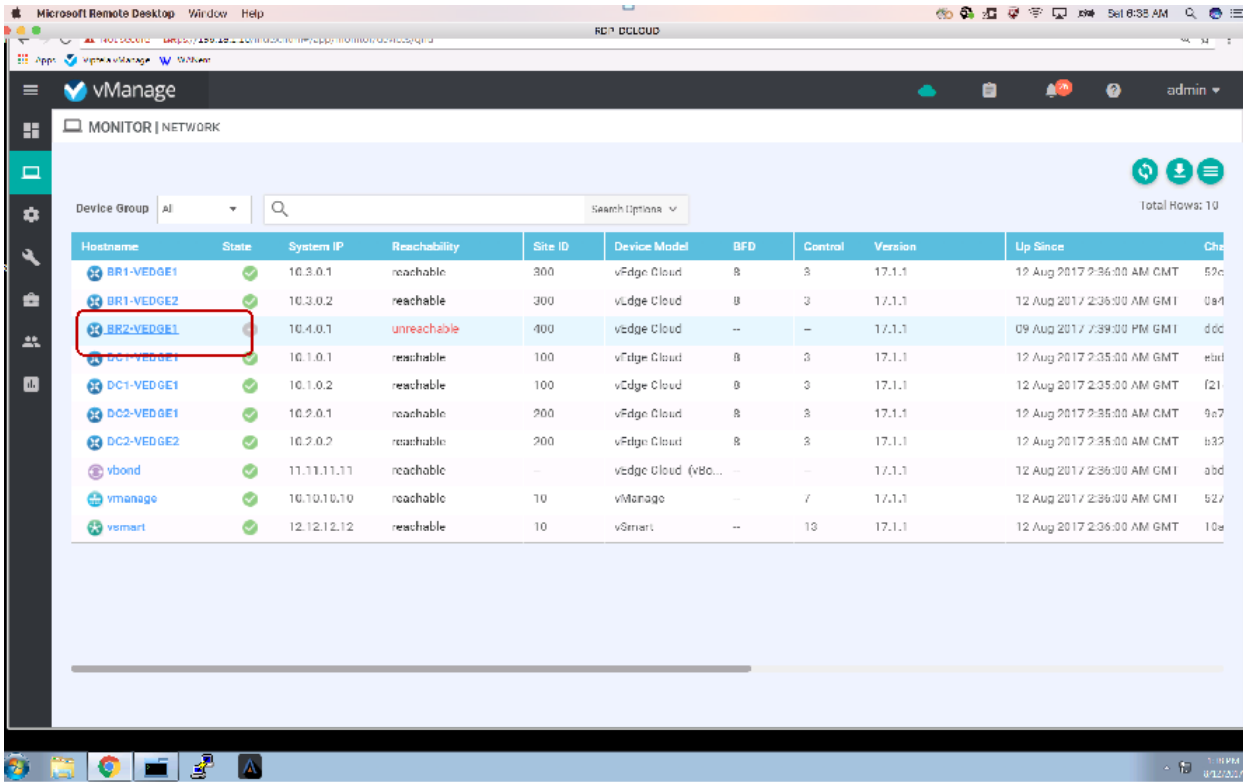
Go to vManage dashboard. Click on the Monitor icon and click on Network from the drop down.

The screenshot displays the Cisco vManage dashboard interface. The left sidebar contains navigation options: Monitor, Geography, Network, Alarms, Events, Audit Log, and ACL Log. The main dashboard area includes several key performance indicators (KPIs) and detailed views:

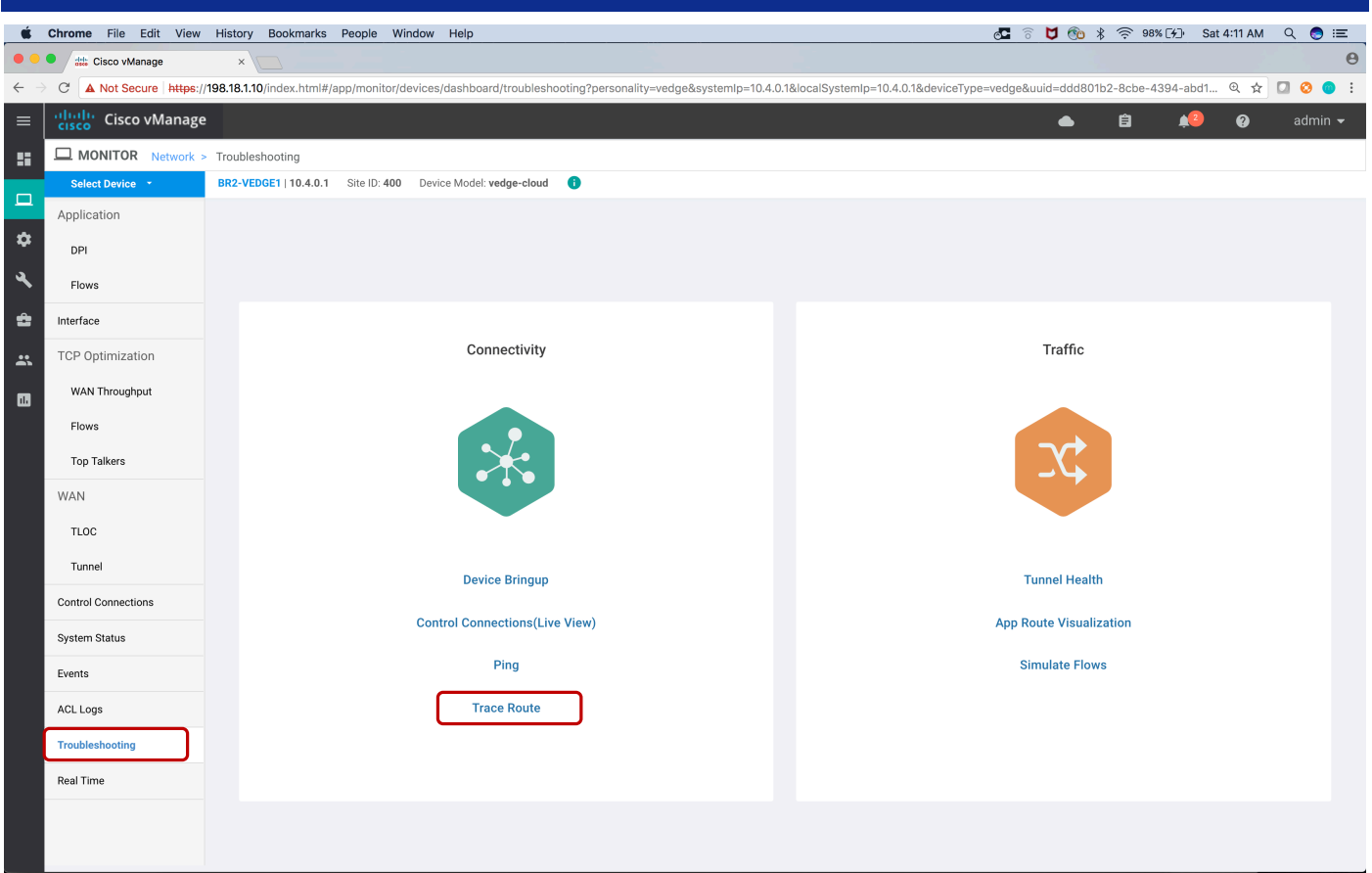
- Summary KPIs:** vEdge: 7 (up arrow), vBond: 1 (up arrow), vManage: 1 (checkmark), Reboot Last 24 hrs: 10, Warning Invalid: 0.
- Site Health View (Total 4):**
  - Full Connectivity: 4 sites
  - Partial Connectivity: 0 sites
  - No Connectivity: 0 sites
- Transport Interface Distribution:**
  - < 10 Mbps: 17
  - 10 Mbps - 100 Mbps: 0
  - 100 Mbps - 500 Mbps: 0
  - > 500 Mbps: 0
- vEdge Health (Total 7):**
  - Normal: 7
  - Warning: 0
  - Error: 0
- Transport Health:** A line graph showing health percentage over time, currently at 100%.
- Top Applications:** A bar chart showing usage for various applications.
- Application-Aware Routing:** A table showing routing metrics for different tunnel endpoints.

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
RR1-VFDGF1.biz-internet-BR2-VFDGF1.biz-I...	0.842	33.333	0.153
BR1-VEGE2.biz-internet-BR2-VEGE1.biz-I...	0.366	27.165	0.11
DC1-VLDGL1.biz-internet-UK2-VLDGL1.biz-I...	0.876	1.207	0.426

Find BR2-VEDGE1 and click on the name.



Select Troubleshooting from the left column. Then select "Traceroute".



Put in 10.3.0.21 as the destination IP.

Select VPN 10 from drop down menu and click on "Start" button.

It shows direct path between Branch1 and Branch2 for VPN 10.



The screenshot shows the Cisco vManage Troubleshooting Traceroute configuration page. The Destination IP is set to 10.3.0.21, the VPN is set to VPN-10, and the Source/Interface for VPN-10 is set to ge0/2 - ipv4 - 10.4.254.10. The Start button is highlighted. The output shows the following traceroute results:

```
Traceroute -m 15 -w 1 -s 10.4.254.10 10.3.0.21 in VPN 10
traceroute to 10.3.0.21 (10.3.0.21), 15 hops max, 60 byte packets
 1 10.3.0.2 (10.3.0.2) 2.033 ms 2.902 ms 2.935 ms
 2 10.3.0.21 (10.3.0.21) 3.923 ms 3.937 ms 4.389 ms
```

The diagram shows a path from the source interface ge0/2 - ipv4 - 10.4.254.10 to 10.3.0.2 with a delay of 2.62ms, and then to 10.3.0.21 with a delay of 4.08ms.

Do the same for VPN 20.

This time the destination IP would be 10.3.20.10 and VPN would be 20.

It shows connectivity between Branch1 and Branch2 for VPN 20 through the DC.

Chrome File Edit View History Bookmarks People Window Help

Cisco vManage

Not Secure https://198.18.1.10/index.html#/app/monitor/devices/dashboard/troubleshooting/traceroute?personality=vedge&systemip=10.4.0.1&localSystemip=10.4.0.1&deviceType=vedge&uid=ddd801b2-8cbe-...

Cisco vManage admin

MONITOR Network > Troubleshooting > Traceroute

Select Device BR2-VEDGE1 | 10.4.0.1 Site ID: 400 Device Model: vedge-cloud Troubleshooting

Destination IP\* 10.3.20.10 VPN VPN - 20 Source/Interface for VPN - 20 ge0/3 - ipv4 - 10.4.20.1

Advanced Options > Start

Output

Traceroute -m 15 -w 1 -s 10.4.20.1 10.3.20.10 in VPN 20  
traceroute to 10.3.20.10 (10.3.20.10), 15 hops max, 60 byte packets

1	10.1.20.3 (10.1.20.3)	1.948 ms	2.834 ms	2.847 ms
2	10.3.20.2 (10.3.20.2)	4.281 ms	4.499 ms	4.613 ms
3	10.3.20.10 (10.3.20.10)	5.331 ms	5.341 ms	5.362 ms

```
graph LR; S[ge0/3 - ipv4 - 10.4.20.1] -- 2.54ms --> H1((10.1.20.3)); H1 -- 4.46ms --> H2((10.3.20.2)); H2 -- 5.34ms --> D[10.3.20.10];
```

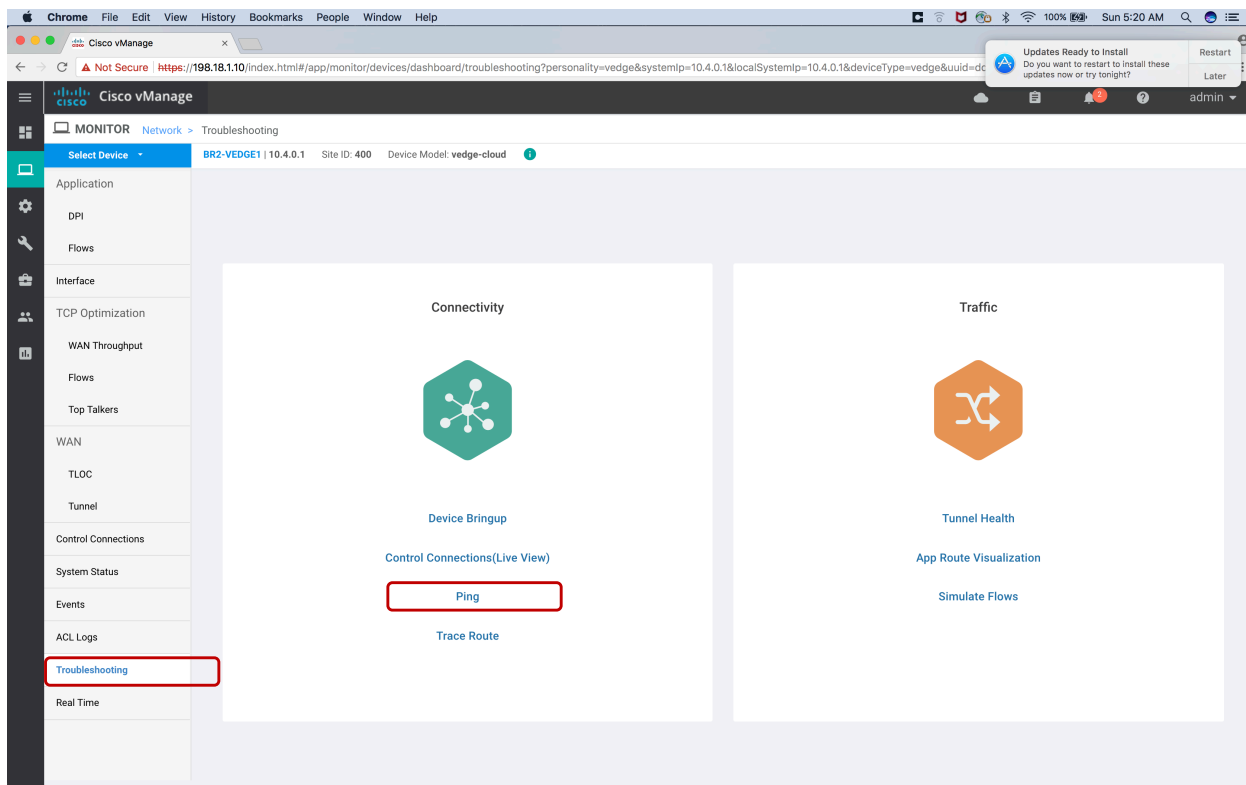
# Lab 09 - Application Firewalling using Centralized Policies

There are cases where an enterprise would like to implement security/packet filtering policy on demand based on network anomalies and/or business requirements. In this scenario we don't want the PCI segment (VPN 20) in Branch1 and Branch2 to be able to communicate with each other. We do want the PCI segment to talk to the servers in the DCs.

This policy will be implemented as a centralized data policy where based on source and destination prefix match, traffic between BR1 and BR2 is dropped. More granular matches can be done to limit certain applications and allow other applications to flow between the Branches.

## Steps

Go to the device dashboard for BR2-VEDGE1 and click "Troubleshooting" tab. Then select "Ping".



Validate connectivity from BR2-VEDGE1 to the test host in Branch3 in VPN 10 (10.3.0.21).

**Destination IP\*** 10.3.0.21 **VPN** VPN - 10 **Source/Interface for VPN - 10** ge0/2 - ipv4 - 10.4.254.10

Probes  ICMP  TCP  UDP

Source Port Destination Port Type Of Service Time To Live Dont Fragment

**Ping**

Summary	
Packets Transmitted	5
Packets Received	4
Packet loss (%)	20
Round Trip Time	
Min (ms)	0.048
Max (ms)	1.379
Avg (ms)	0.391

**Output:**  
Nping in VPN 10  
Starting Nping 0.6.47 ( http://nmap.org/nping ) at 2017-12-31 15:23 UTC  
SENT (0.0126s) ICMP [10.4.254.10 > 10.3.0.21 Echo request (type=8/code=0) id=4783 seq=1] IP [ttl=64 id=18949 iplen=28]  
SENT (1.0128s) ICMP [10.4.254.10 > 10.3.0.21 Echo request (type=8/code=0) id=4783 seq=3] IP [ttl=64 id=18949 iplen=28]  
RCVD (1.0142s) ICMP [10.3.20.2 > 10.4.254.10 Network 10.3.0.21 unreachable (type=3/code=0) ] IP [ttl=63 id=0 iplen=56]  
SENT (2.0133s) ICMP [10.4.254.10 > 10.3.0.21 Echo request (type=8/code=0) id=4783 seq=3] IP [ttl=64 id=18949 iplen=28]  
RCVD (2.0134s) ICMP [10.3.20.2 > 10.4.254.10 Network 10.3.0.21 unreachable (type=3/code=0) ] IP [ttl=63 id=0 iplen=56]  
SENT (3.0135s) ICMP [10.4.254.10 > 10.3.0.21 Echo request (type=8/code=0) id=4783 seq=4] IP [ttl=64 id=18949 iplen=28]  
RCVD (3.0136s) ICMP [10.3.20.2 > 10.4.254.10 Network 10.3.0.21 unreachable (type=3/code=0) ] IP [ttl=63 id=0 iplen=56]  
SENT (4.0144s) ICMP [10.4.254.10 > 10.3.0.21 Echo request (type=8/code=0) id=4783 seq=5] IP [ttl=64 id=18949 iplen=28]  
RCVD (4.0146s) ICMP [10.3.20.2 > 10.4.254.10 Network 10.3.0.21 unreachable (type=3/code=0) ] IP [ttl=63 id=0 iplen=56]  
Max rtt: 1.379ms | Min rtt: 0.048ms | Avg rtt: 0.391ms  
Raw packets sent: 5 (140B) | Rcvd: 4 (224B) | Lost: 1 (20.00%)  
Nping done: 1 IP address pinged in 4.02 seconds

Validate connectivity from BR2-VEDGE1 to the test host in Branch3 in VPN 20 (10.3.20.10).

**Destination IP\*** 10.3.20.10 **VPN** VPN - 20 **Source/Interface for VPN - 20** ge0/3 - ipv4 - 10.4.20.1

Probes  ICMP  TCP  UDP

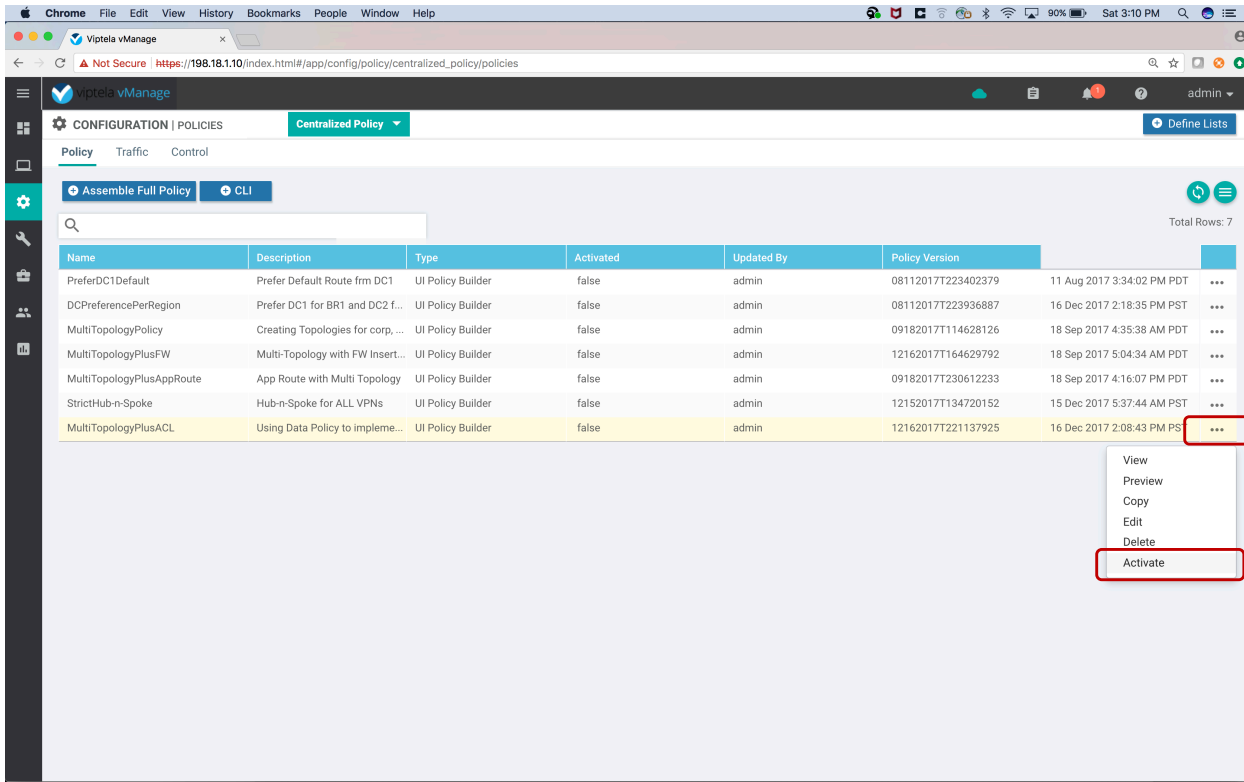
Source Port Destination Port Type Of Service Time To Live Dont Fragment

**Ping**

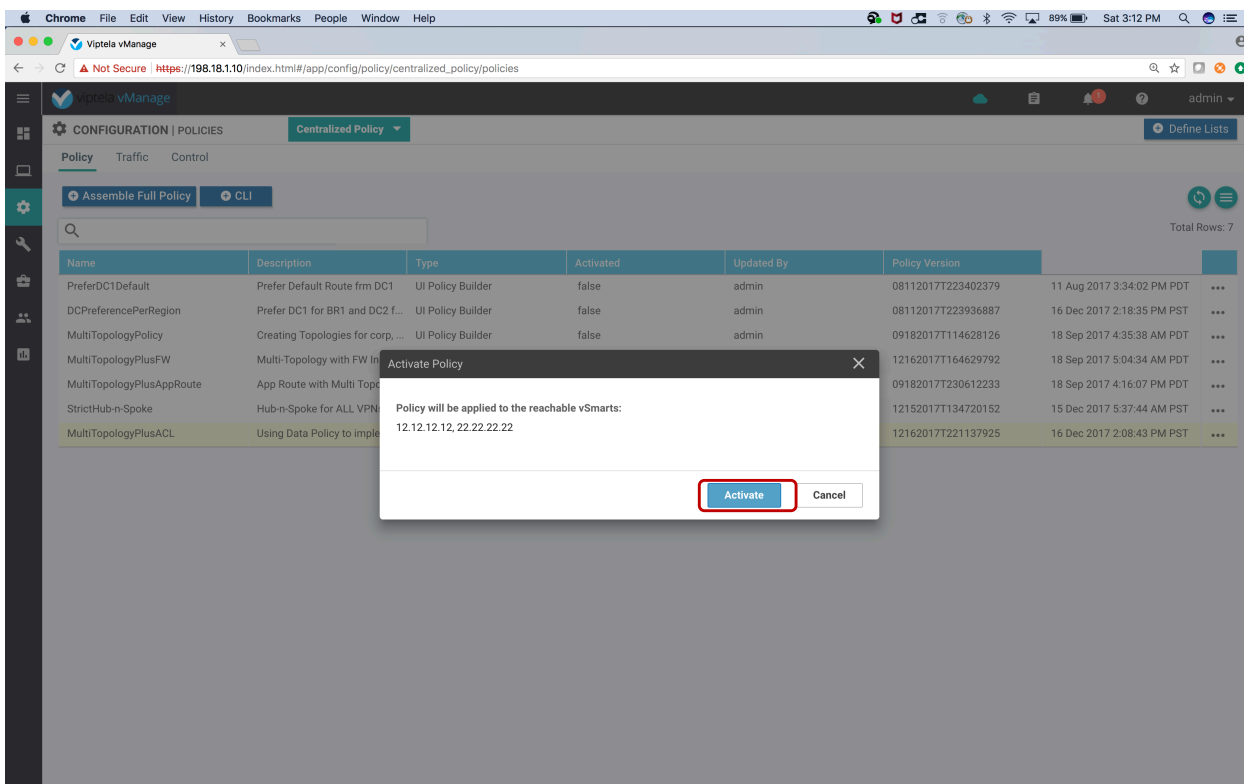
Summary	
Packets Transmitted	5
Packets Received	4
Packet loss (%)	20
Round Trip Time	
Min (ms)	0.037
Max (ms)	1.036
Avg (ms)	0.294

**Output:**  
Nping in VPN 20  
Starting Nping 0.6.47 ( http://nmap.org/nping ) at 2017-12-31 15:26 UTC  
SENT (0.0138s) ICMP [10.4.20.1 > 10.3.20.10 Echo request (type=8/code=0) id=54407 seq=1] IP [ttl=64 id=22226 iplen=28]  
SENT (1.0139s) ICMP [10.4.20.1 > 10.3.20.10 Echo request (type=8/code=0) id=54407 seq=3] IP [ttl=64 id=22226 iplen=28]  
RCVD (1.0149s) ICMP [10.3.20.10 > 10.4.20.1 Echo reply (type=0/code=0) id=54407 seq=1] IP [ttl=127 id=12416 iplen=28]  
SENT (2.0142s) ICMP [10.4.20.1 > 10.3.20.10 Echo request (type=8/code=0) id=54407 seq=3] IP [ttl=64 id=22226 iplen=28]  
RCVD (2.0144s) ICMP [10.3.20.10 > 10.4.20.1 Echo reply (type=0/code=0) id=54407 seq=3] IP [ttl=127 id=12417 iplen=28]  
SENT (3.0153s) ICMP [10.4.20.1 > 10.3.20.10 Echo request (type=8/code=0) id=54407 seq=4] IP [ttl=64 id=22226 iplen=28]  
RCVD (3.0155s) ICMP [10.3.20.10 > 10.4.20.1 Echo reply (type=0/code=0) id=54407 seq=3] IP [ttl=127 id=12418 iplen=28]  
SENT (4.0165s) ICMP [10.4.20.1 > 10.3.20.10 Echo request (type=8/code=0) id=54407 seq=5] IP [ttl=64 id=22226 iplen=28]  
RCVD (4.0166s) ICMP [10.3.20.10 > 10.4.20.1 Echo reply (type=0/code=0) id=54407 seq=4] IP [ttl=127 id=12419 iplen=28]  
Max rtt: 1.036ms | Min rtt: 0.037ms | Avg rtt: 0.294ms  
Raw packets sent: 5 (140B) | Rcvd: 4 (112B) | Lost: 1 (20.00%)  
Nping done: 1 IP address pinged in 4.02 seconds

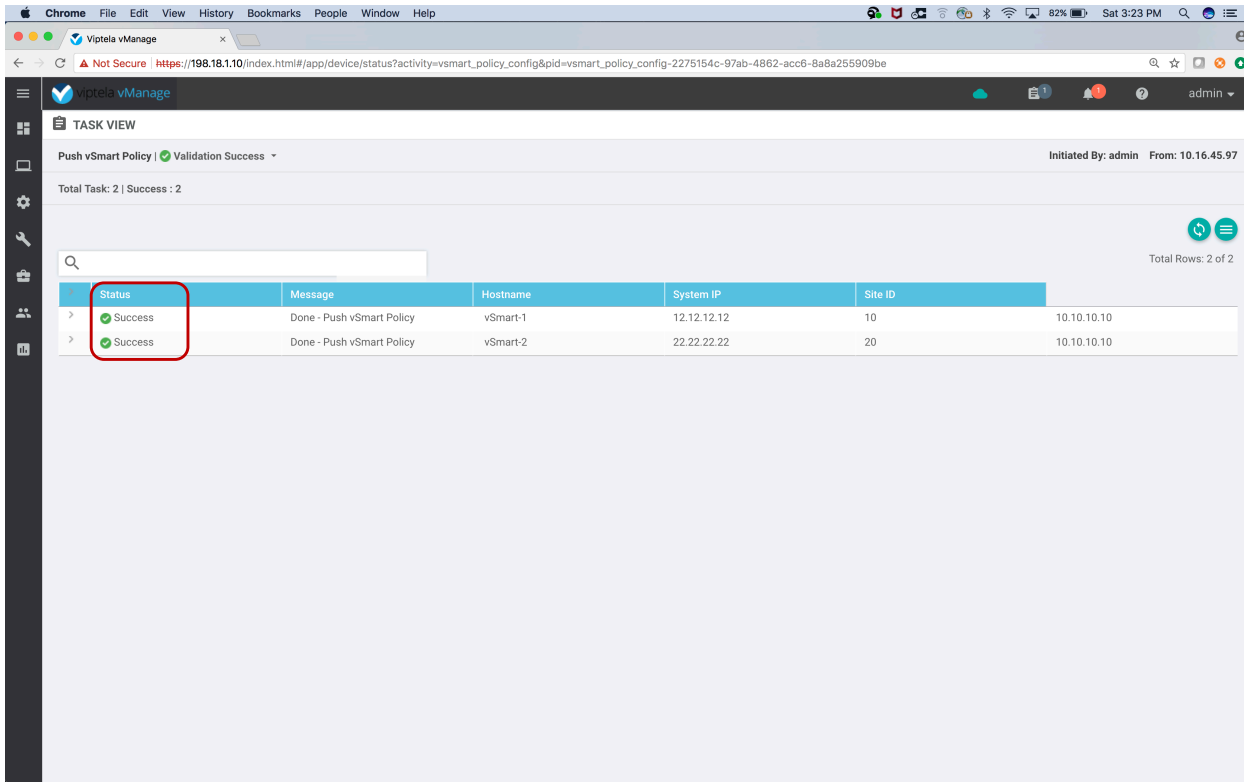
Activate the policy named “MultiTopologyPlusACL”.



Click the “Activate” button.



Wait till the policy is pushed successfully pushed to both the vSmarts.



Go to device dashboard for BR2-VEDGE1 and Click on "Troubleshooting" tab.

Then repeat the ping test to the host in Branch1 in VPN 10.

The screenshot shows the Cisco vManage Troubleshooting interface for device BR2-VEG1E1. The configuration is as follows:

- Destination IP\*: 10.3.0.21
- VPN: VPN - 10
- Source/Interface for VPN - 10: ge0/2 - ipv4 - 10.4.254.10
- Probes: ICMP (selected)
- Source Port: (empty)
- Destination Port: (empty)
- Type Of Service: (empty)
- Time To Live: (empty)
- Don't Fragment: (disabled)

The **Ping** button is highlighted with a red box. The output shows a successful ping with 5 packets transmitted and 4 received.

Summary	
Packets Transmitted	5
Packets Received	4
Packet loss (%)	20
Round Trip Time	
Min (ms)	0.048
Max (ms)	1.379
Avg (ms)	0.391

**Output:**  
Nping in VPN 10  
Starting Nping 0.6.47 ( http://nmap.org/nping ) at 2017-12-31 15:23 UTC  
SENT (0.0126s) ICMP [10.4.254.10 > 10.3.0.21 Echo request (type=8/code=0) id=4783 seq=1] IP [ttl=64 id=18949 iplen=28]  
SENT (1.0128s) ICMP [10.4.254.10 > 10.3.0.21 Echo request (type=8/code=0) id=4783 seq=3] IP [ttl=64 id=18949 iplen=28]  
RCVD (1.0142s) ICMP [10.3.20.2 > 10.4.254.10 Network 10.3.0.21 unreachable (type=3/code=0) ] IP [ttl=63 id=0 iplen=56]  
SENT (2.0133s) ICMP [10.4.254.10 > 10.3.0.21 Echo request (type=8/code=0) id=4783 seq=3] IP [ttl=64 id=18949 iplen=28]  
RCVD (2.0134s) ICMP [10.3.20.2 > 10.4.254.10 Network 10.3.0.21 unreachable (type=3/code=0) ] IP [ttl=63 id=0 iplen=56]  
SENT (3.0135s) ICMP [10.4.254.10 > 10.3.0.21 Echo request (type=8/code=0) id=4783 seq=4] IP [ttl=64 id=18949 iplen=28]  
RCVD (3.0136s) ICMP [10.3.20.2 > 10.4.254.10 Network 10.3.0.21 unreachable (type=3/code=0) ] IP [ttl=63 id=0 iplen=56]  
SENT (4.0144s) ICMP [10.4.254.10 > 10.3.0.21 Echo request (type=8/code=0) id=4783 seq=5] IP [ttl=64 id=18949 iplen=28]  
RCVD (4.0146s) ICMP [10.3.20.2 > 10.4.254.10 Network 10.3.0.21 unreachable (type=3/code=0) ] IP [ttl=63 id=0 iplen=56]  
Raw rtt: 1.379ms | Min rtt: 0.048ms | Avg rtt: 0.391ms  
Raw packets sent: 5 (140B) | Rcvd: 4 (224B) | Lost: 1 (20.00%)  
Nping done: 1 IP address pinged in 4.02 seconds

Do a ping test to the Host in Branch3 in VPN 20 (10.3.20.10).

The ping will fail due to centralized ACL blocking communication between the branches for PCI/IOT segment.

The screenshot shows the Cisco vManage Troubleshooting interface for device BR2-VEG1E1. The configuration is as follows:

- Destination IP\*: 10.3.20.10
- VPN: VPN - 20
- Source/Interface for VPN - 20: Choose/Reset selections
- Probes: ICMP (selected)
- Source Port: (empty)
- Destination Port: (empty)
- Type Of Service: (empty)
- Time To Live: (empty)
- Don't Fragment: (disabled)

The **Ping** button is highlighted with a red box. The output shows a failed ping with 5 packets transmitted and 0 received.

Summary	
Packets Transmitted	5
Packets Received	0
Packet loss (%)	100
Round Trip Time	
Min (ms)	0
Max (ms)	0
Avg (ms)	0

**Output:**  
Nping in VPN 20  
Starting Nping 0.6.47 ( http://nmap.org/nping ) at 2017-12-31 15:37 UTC  
SENT (0.0109s) ICMP [10.4.20.1 > 10.3.20.10 Echo request (type=8/code=0) id=2874 seq=1] IP [ttl=64 id=14900 iplen=28]  
SENT (1.0110s) ICMP [10.4.20.1 > 10.3.20.10 Echo request (type=8/code=0) id=2874 seq=3] IP [ttl=64 id=14900 iplen=28]  
SENT (2.0121s) ICMP [10.4.20.1 > 10.3.20.10 Echo request (type=8/code=0) id=2874 seq=3] IP [ttl=64 id=14900 iplen=28]  
SENT (3.0130s) ICMP [10.4.20.1 > 10.3.20.10 Echo request (type=8/code=0) id=2874 seq=4] IP [ttl=64 id=14900 iplen=28]  
SENT (4.0141s) ICMP [10.4.20.1 > 10.3.20.10 Echo request (type=8/code=0) id=2874 seq=5] IP [ttl=64 id=14900 iplen=28]  
Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A  
Raw packets sent: 5 (140B) | Rcvd: 0 (0B) | Lost: 5 (100.00%)  
Nping done: 1 IP address pinged in 5.02 seconds

Deactivate the policy named "MultiTopologyPlusACL".



## Upgrading Software on Cisco SD-WAN

Cisco SD-WAN provides a simple process of upgrading the software on ALL components from vManage.

Software version on the vEdges has to be equal or lower than the controllers.

Methodology for upgrading the Cisco SD-WAN

- 1- Upgrade the vManage
- 2- Then upgrade the vBonds/vSmarts
- 3- Then upgrade the vEdges

### Steps

Go to vManage Dashboard.

Click on “Maintenance” icon and select “Software Upgrade” from the pull-down.

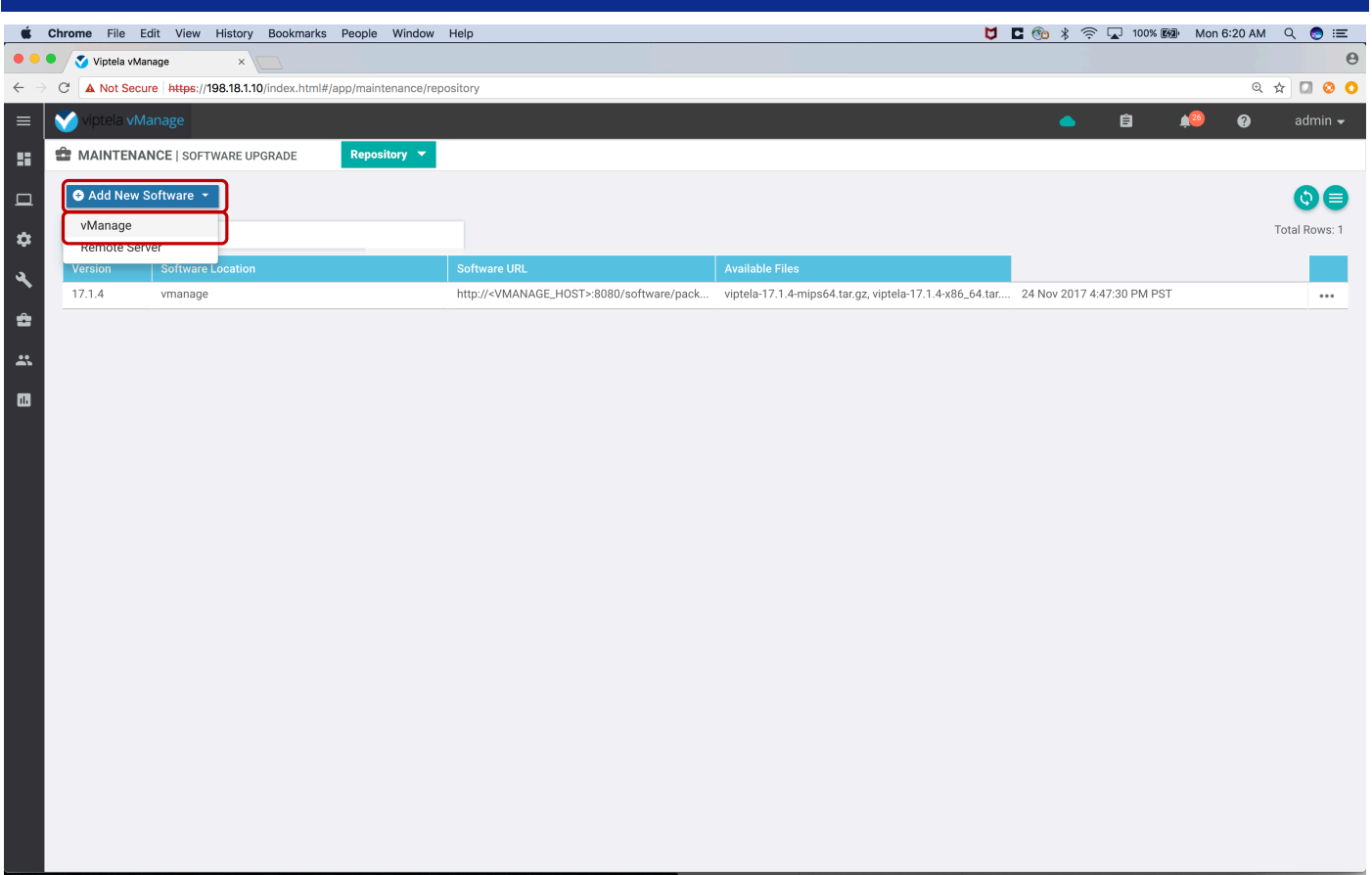
The screenshot shows the vManage dashboard interface. The 'Maintenance' menu is open, and 'Software Upgrade' is highlighted. The dashboard includes various status cards for vSmart, vEdge, vBond, and vManage, along with Site Health View, Transport Interface Distribution, vEdge Inventory, vEdge Health, and Application-Aware Routing sections.

Click on “Device List” and then select “Repository”.

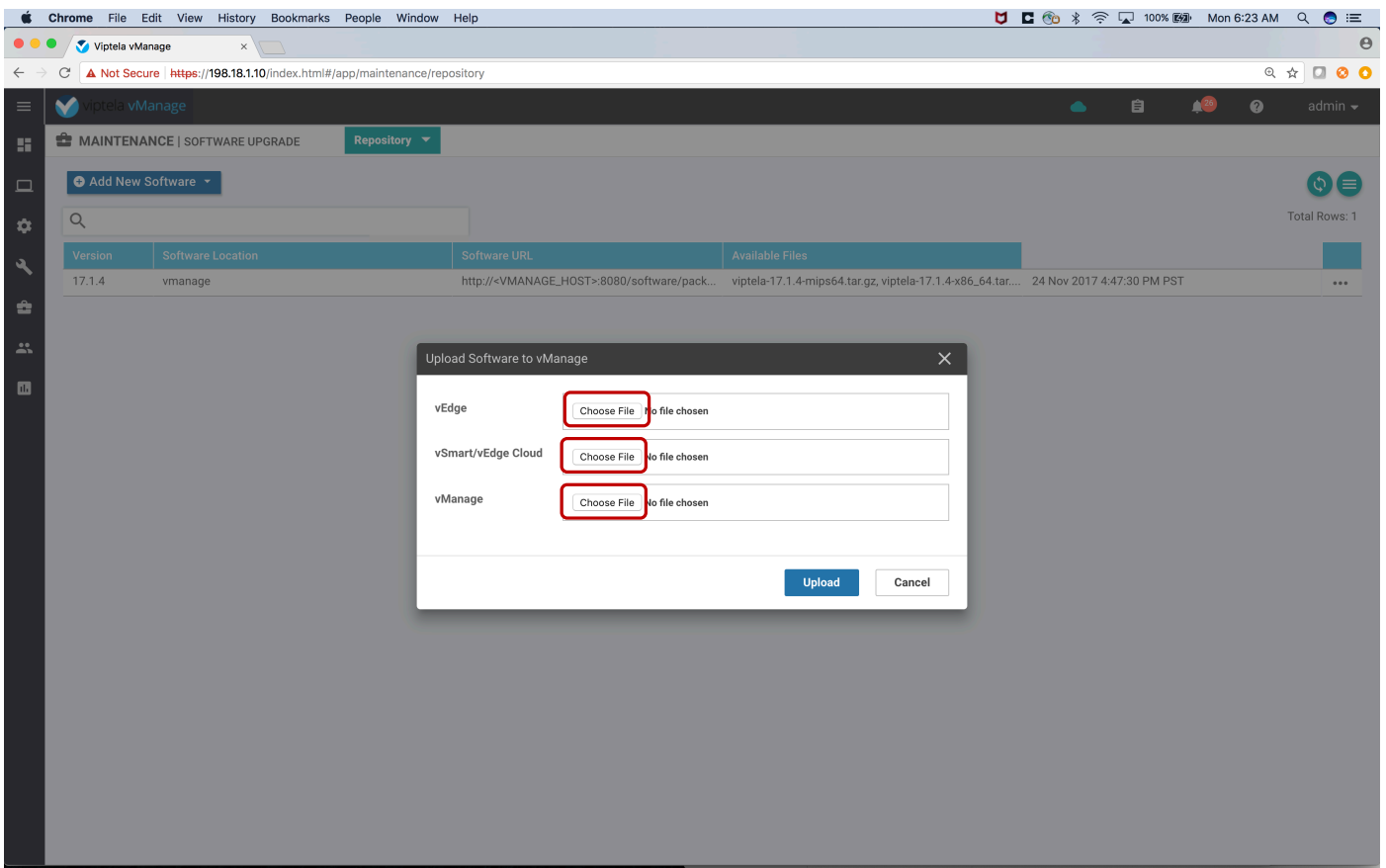
The screenshot shows the vManage vEdge Software Upgrade interface. The top navigation bar includes 'Device List' and 'Repository' tabs, both highlighted with red boxes. Below the navigation bar, there are buttons for 'Upgrade', 'Activate', 'Delete Available Software', and 'Set Default Version'. A search bar is present for the device group. The main content area displays a table of vEdge devices.

	Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability	Current Version	Available Versions	Default Version	Up Since
<input type="checkbox"/>	BR1-VEDG...	10.3.0.1	52c7911f-c5b0-45df-b826-315...	300	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	18 Dec 2017 3:43:00 AM PST
<input type="checkbox"/>	BR1-VEDG...	10.3.0.2	0a4a4c78-35a8-4c1c-bbd2-e0...	300	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:27:00 AM PST
<input type="checkbox"/>	BR2-VEDG...	10.4.0.1	ddd801b2-8cbe-4394-abd1-3b...	400	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:27:00 AM PST
<input type="checkbox"/>	DC1-VED...	10.1.0.1	ebdc8bd9-17e5-4eb3-a5e0-f43...	100	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:26:00 AM PST
<input type="checkbox"/>	DC1-VED...	10.1.0.2	f21dbb35-30b3-47f4-93bb-d2b...	100	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:26:00 AM PST
<input type="checkbox"/>	DC2-VED...	10.2.0.1	9e785ad7-558a-40c6-b0c0-fcc...	200	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:26:00 AM PST
<input type="checkbox"/>	DC2-VED...	10.2.0.2	b3265c5c-3db6-4d25-9d3b-1f4...	200	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:26:00 AM PST

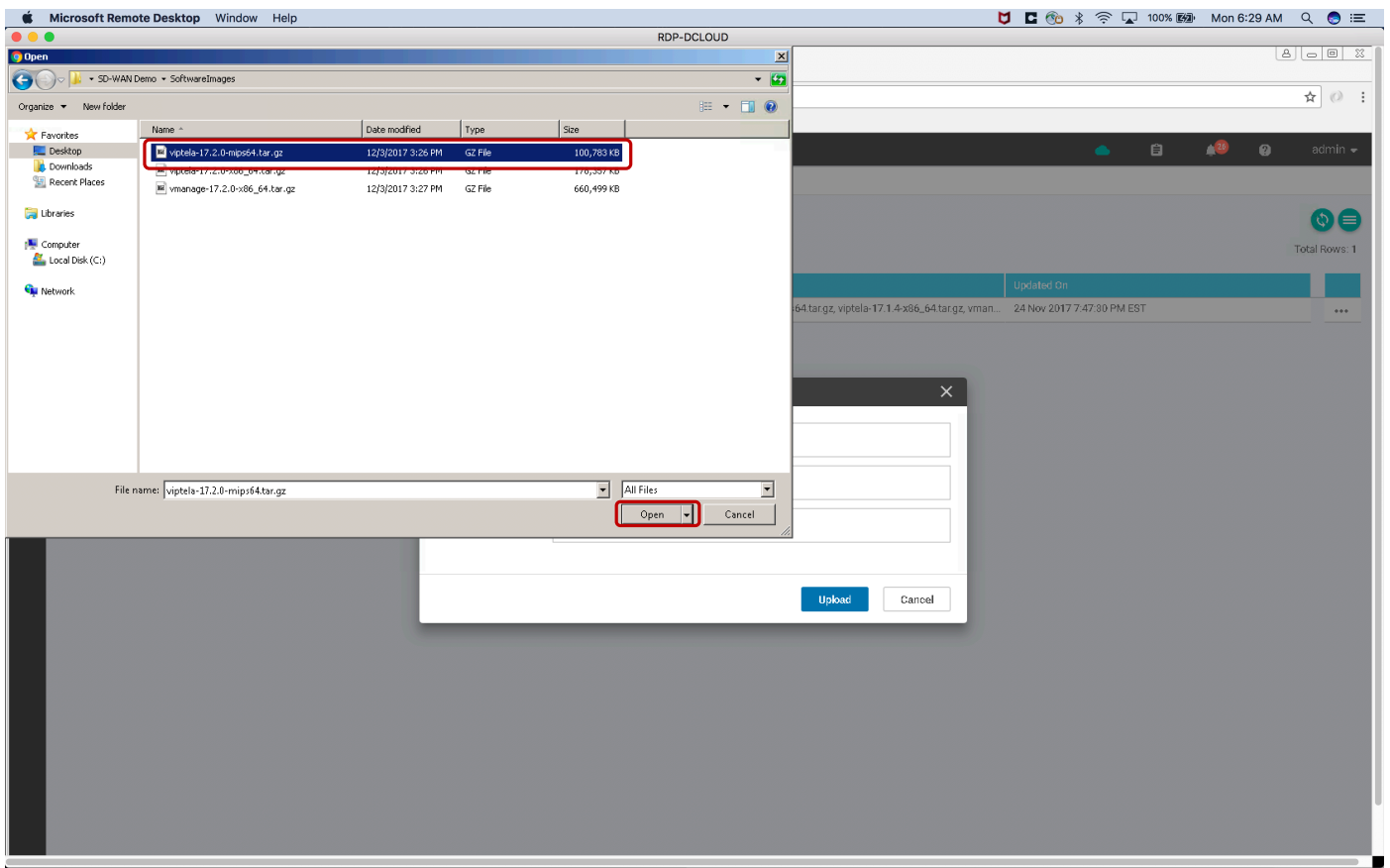
Click on “Add New Software” and then select “vManage”.  
This is to upload software to vManage rather than rely on an external server.



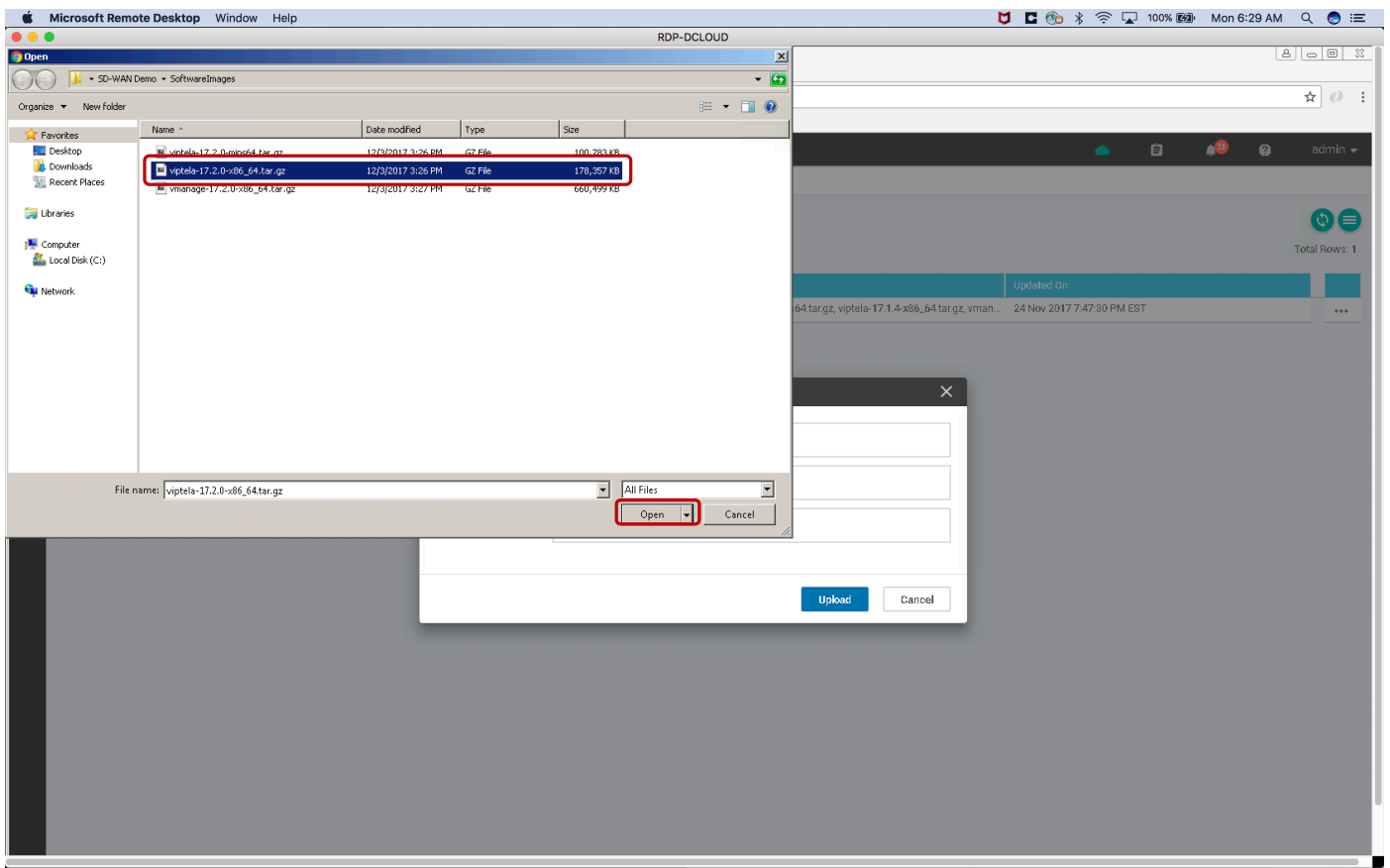
Click on choose file for vEdges, vSmart/vBond/vEdge Cloud and vManage.



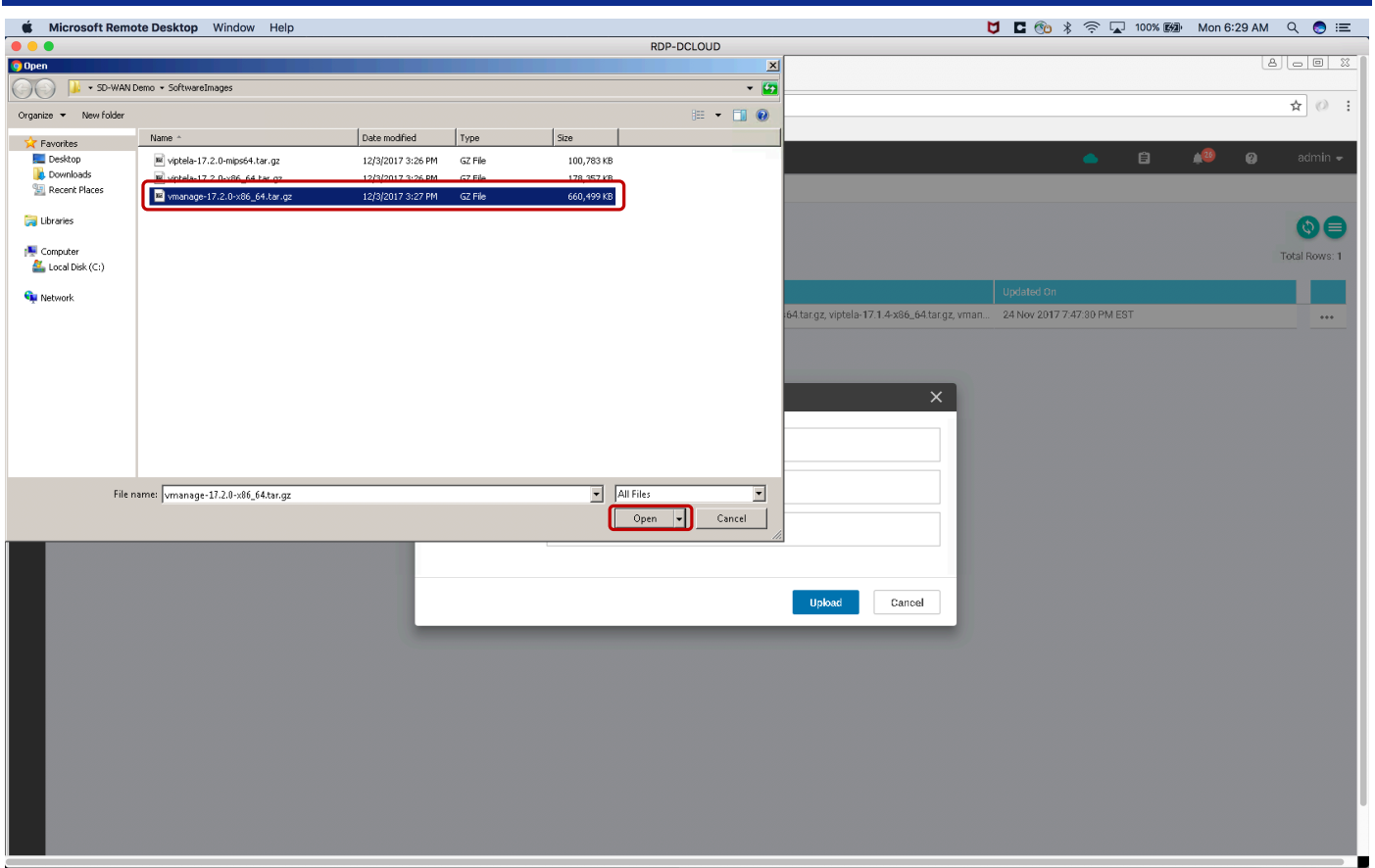
The software images are in the folder `\Desktop\SD-WAN Demo\SoftwareImages`.  
Select the following files for each and click on “Open” tab.  
For vEdge (select the mips file):



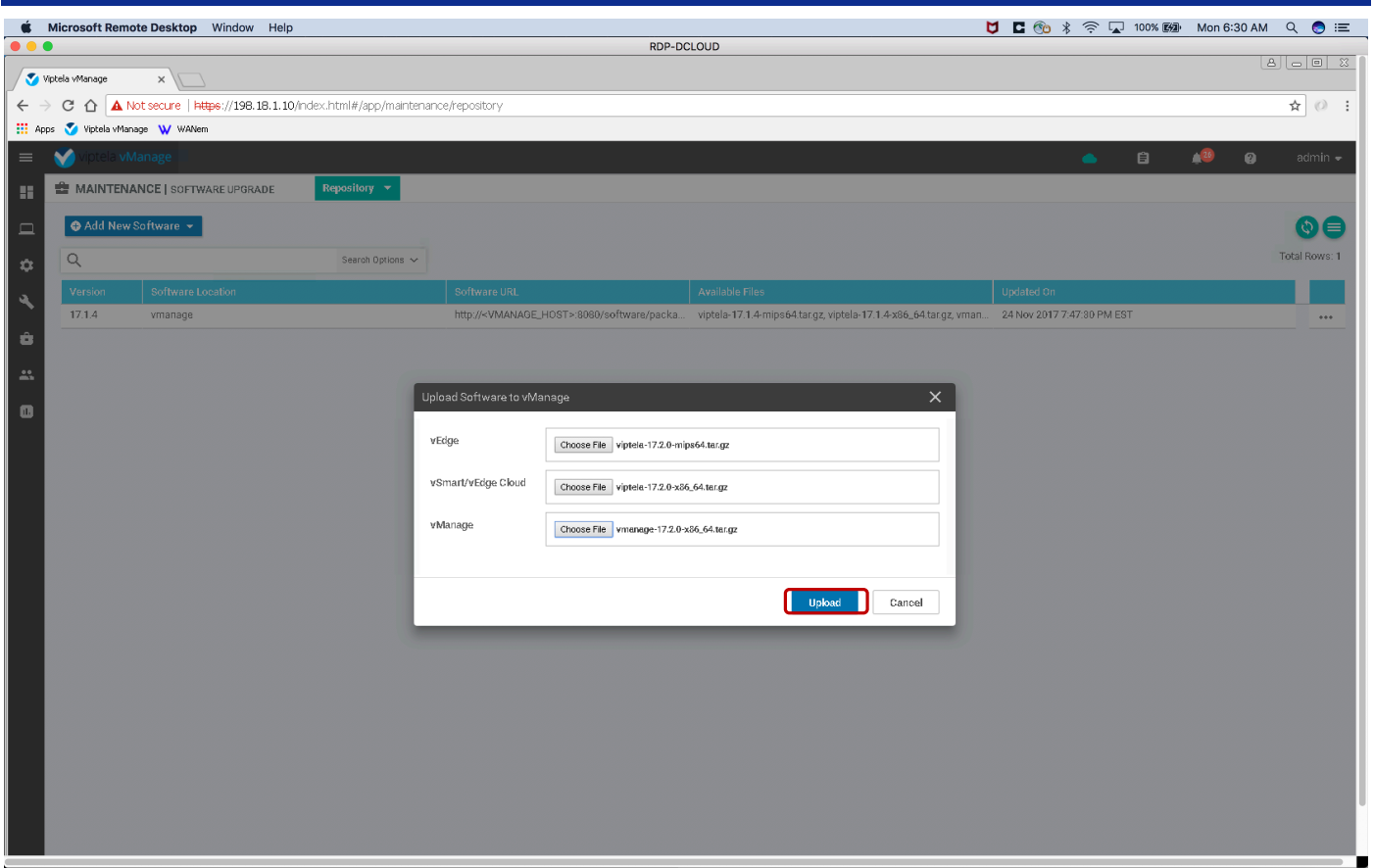
For vSmart/vEdge Cloud (Select the x86 file):



For vManage (select vmanage file):

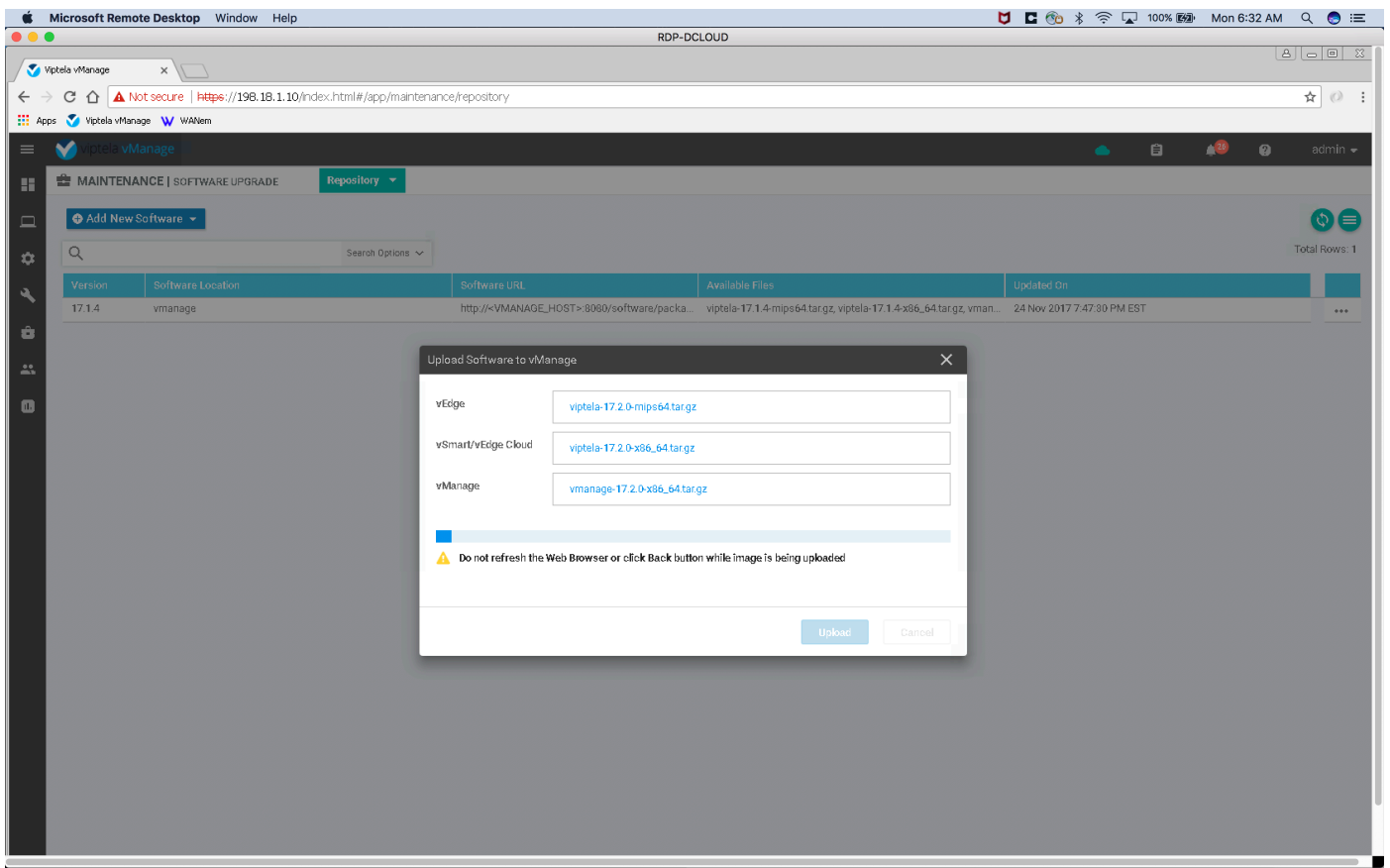


On the next screen, click on Update.

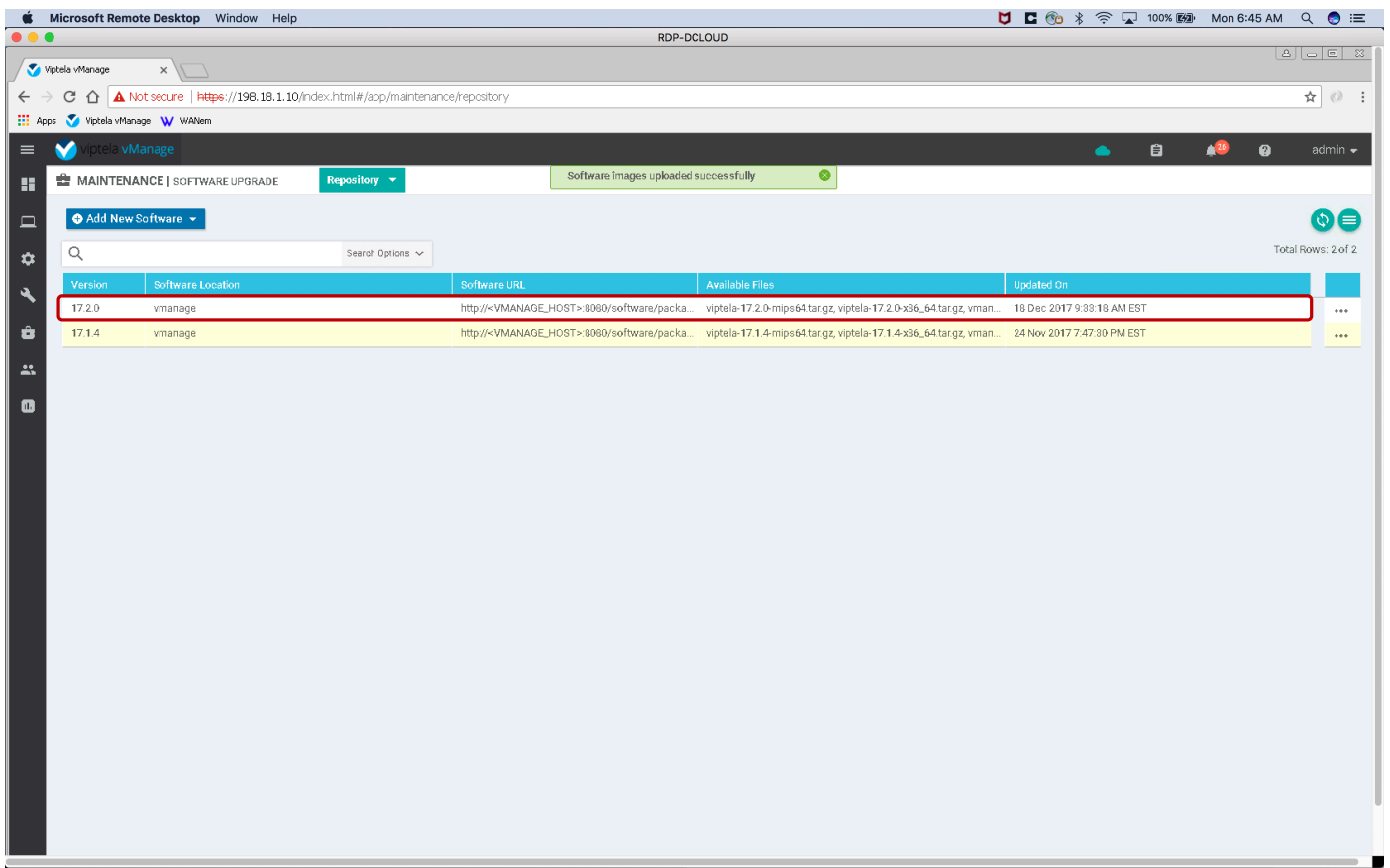


The upload will start and will take some time. Do not refresh the browser or try to go back.





Once the upload completes, the 17.2.0 image will show up in the repository.



Click on “Device List” or go through “Maintenance” -> “Software Upgrade”.

The screenshot shows the Viptela vManage maintenance repository page. The page title is 'MAINTENANCE | SOFTWARE UPGRADE'. There is a search bar and a 'Total Rows: 2' indicator. A table lists the available software versions:

Version	Software Location	Software URL	Available Files	
17.2.0	vmanage	http://<VMANAGE_HOST>:8080/software/pack...	viptela-17.2.0-mips64.tar.gz, viptela-17.2.0-x86_64.tar...	18 Dec 2017 6:33:18 AM PST
17.1.4	vmanage	http://<VMANAGE_HOST>:8080/software/pack...	viptela-17.1.4-mips64.tar.gz, viptela-17.1.4-x86_64.tar...	24 Nov 2017 4:47:30 PM PST

First, upgrade vManage.  
Click on vManage tab.

The screenshot shows the vManage web interface for software upgrades. The breadcrumb navigation is MAINTENANCE | SOFTWARE UPGRADE. The 'vManage' tab is selected. Below the navigation, there are buttons for 'Upgrade', 'Activate', 'Delete Available Software', and 'Set Default Version'. A table lists 7 vEdge Cloud devices with columns for Hostname, System IP, Chassis Number, Site ID, Device Model, Reachability, Current Version, Available Versions, Default Version, and Up Since. The 'Upgrade' button is highlighted with a red box.

	Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability	Current Version	Available Versions	Default Version	Up Since
<input type="checkbox"/>	BR1-VEDG...	10.3.0.1	52c7911f-c5b0-45df-b826-315...	300	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	18 Dec 2017 8:52:00 AM PST
<input type="checkbox"/>	BR1-VEDG...	10.3.0.2	0a4a4c78-35a8-4c1c-bbd2-e0...	300	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	18 Dec 2017 8:52:00 AM PST
<input type="checkbox"/>	BR2-VEDG...	10.4.0.1	ddd801b2-8cbe-4394-abd1-3b...	400	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:27:00 AM PST
<input type="checkbox"/>	DC1-VED...	10.1.0.1	ebdc8bd9-17e5-4eb3-a5e0-f43...	100	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:26:00 AM PST
<input type="checkbox"/>	DC1-VED...	10.1.0.2	f21dbb35-30b3-47f4-93bb-d2b...	100	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:26:00 AM PST
<input type="checkbox"/>	DC2-VED...	10.2.0.1	9e785ad7-558a-40c6-b0c0-fcc...	200	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:26:00 AM PST
<input type="checkbox"/>	DC2-VED...	10.2.0.2	b3265c5c-3db6-4d25-9d3b-1f4...	200	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:26:00 AM PST

Click on the “Upgrade” button.

The screenshot shows the Viptela vManage web interface for software upgrades. At the top, there are navigation tabs for 'vEdge', 'Controller', and 'vManage'. Below these are action buttons: 'Upgrade' (highlighted with a red box), 'Activate', 'Delete Available Software', and 'Set Default Version'. A search bar for 'Device Group' is present. The main content area features a table with the following data:

Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability	Current Version	Available Versions	Default Version	
vManage	10.10.10.10	5271ea7c-edb1-420b-be9a-4d...	10	vManage	reachable	17.1.4	17.1.1 17.1.3	17.1.1	17 Dec 2017 7:27:00 AM PST

In the pop-up, click on version field and select 17.2.0. Then click on “Upgrade” button.

The screenshot shows the vManage web interface in a Chrome browser. The page title is 'MAINTENANCE | SOFTWARE UPGRADE'. Below the title, there are buttons for 'Upgrade', 'Activate', 'Delete Available Software', and 'Set Default Version'. A table lists the device details for 'vManage'. A modal dialog titled 'Software Upgrade' is displayed in the foreground. The dialog contains a warning icon and the text: 'Backup of data volume is highly recommended before upgrading vManage.' Below this, there are radio buttons for 'Version', 'vManage', and 'Remote Server'. The 'Version' dropdown menu is open, showing '17.2.0' as the selected option. At the bottom right of the dialog, there are 'Upgrade' and 'Cancel' buttons.

Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability	Current Version	Available Versions	Default Version	
vManage	10.10.10.10	5271ea7c-edb1-420b-be9a-4d...	10	vManage	reachable	17.1.4	17.1.1 17.1.3	17.1.1	17 Dec 2017 7:27:00 AM PST

The vManage will install the new version. Wait till it is finished uploading the image.

Chrome File Edit View History Bookmarks People Window Help

Viptela vManage

Not Secure https://198.18.1.10/index.html#/app/device/status?activity=software\_install&pid=software\_install-41df2ead-8912-4a3c-a325-c990c1aba87f

Viptela vManage admin

### TASK VIEW

Software Install | Validation Success Initiated By: admin From: 10.16.27.161

Total Task: 1 | Success : 1

Search

Total Rows: 1 of 1

Status	Message	Hostname	System IP	Site ID	Device Type	Device Model
Success	Done - Software Install	vManage	10.10.10.10	10	vManage	vManage

Go to software upgrade page and click on “vManage” tab. Then click on “Activate” button.

MAINTENANCE | SOFTWARE UPGRADE

vEdge Controller **vManage**

Upgrade Activate Delete Available Software Set Default Version

Device Group: All

Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability	Current Version	Available Versions	Default Version	
vManage	10.10.10.10	5271ea7c-edb1-420b-be9a-4d...	10	vManage	reachable	17.1.4	17.1.1 17.1.3 17.2.0	17.1.1	17 Dec 2017 7:27:00 AM PST

Click on the version field and select 17.2.0. Click on “Activate”.

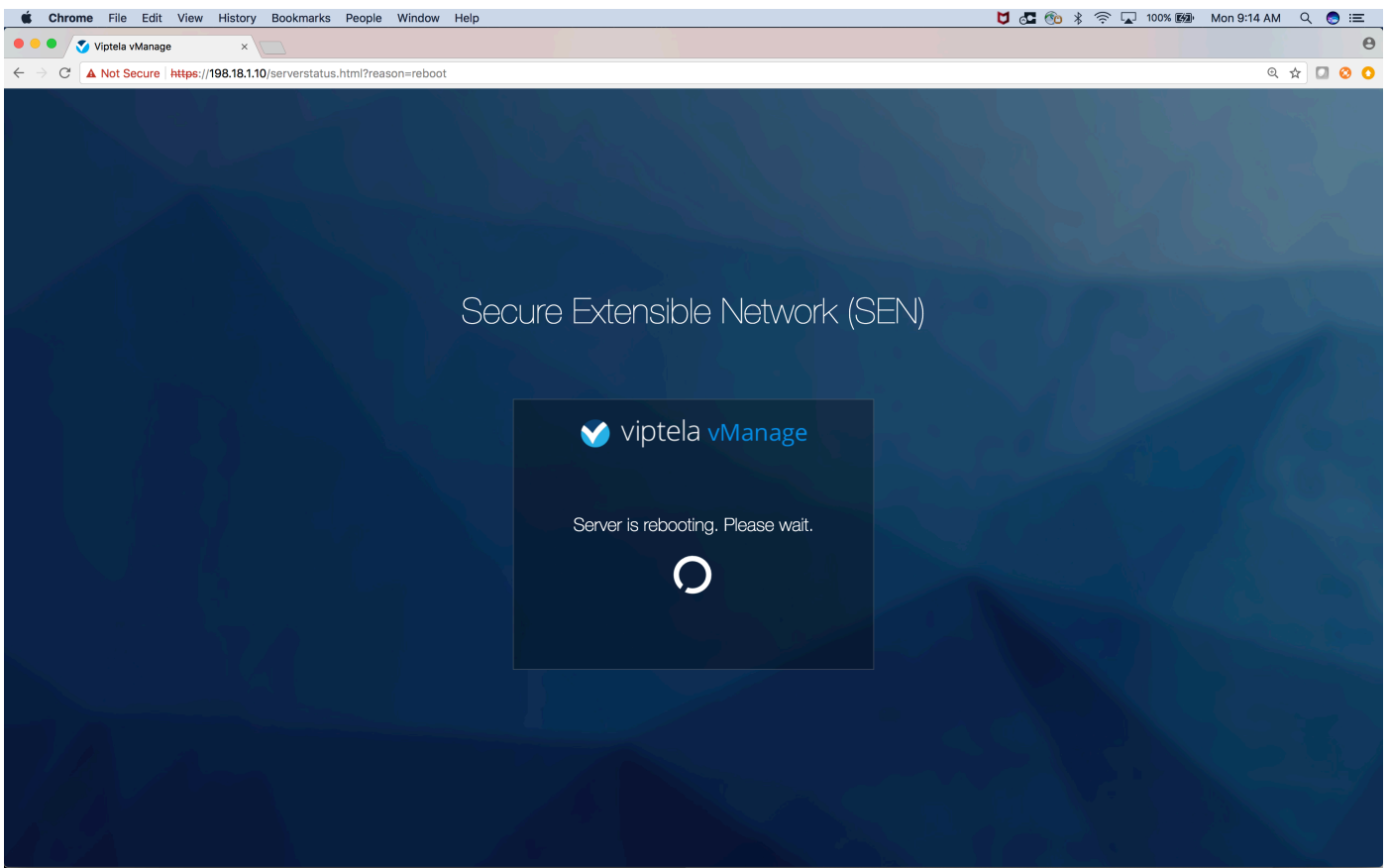


The screenshot shows the vManage web interface in a Chrome browser. The browser address bar shows a URL starting with `https://198.18.1.10/`. The interface has a dark sidebar on the left and a main content area. The main content area is titled "MAINTENANCE | SOFTWARE UPGRADE" and includes a "Device List" dropdown. Below this, there are tabs for "vEdge" and "Controller", with "vManage" selected. A row of action buttons includes "Upgrade", "Activate", "Delete Available Software", and "Set Default Version". A "Device Group" dropdown is set to "All". A table lists device information:

Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability	Current Version	Available Versions	Default Version	
vManage	10.10.10.10	5271ea7c-edb1-420b-be9a-4d...	10	vManage	reachable	17.1.4	17.1.1 17.1.3 17.2.0	17.1.1	17 Dec 2017 7:27:00 AM PST

An "Activate Software" dialog box is open in the center. It contains a warning icon and the text: "Activating new version of software on vManage requires a reboot, which will log out all active clients and bring down all control connections." Below this, there is a "Version" dropdown menu currently set to "17.2.0". At the bottom of the dialog are "Activate" and "Cancel" buttons.

The vManage will reboot and you will lose the session to vManage.



It will take few minutes to reboot. Once the vManage is back on-line, log back in again to vManage portal. To validate the current version on vManage, click on the icon with ? and then click on “About” in the pull down menu.

The screenshot shows the vManage dashboard interface. At the top, there's a navigation bar with the vManage logo and a user profile 'admin'. Below this is a 'DASHBOARD' section with several summary cards: vSmart - 2, vEdge - 7, vBond - 2, and vManage - 1. A 'Reboot' status is also visible. A help pop-up menu is open in the top right corner, showing 'Dashboard Help', 'Help', and 'About' options. The main dashboard area is divided into several sections: 'Control Status (Total 9)' with a bar chart showing 9 Control Up, 0 Partial, and 0 Control Down; 'Site Health View (Total 4)' with 4 sites showing Full Connectivity, 0 Partial, and 0 No Connectivity; 'Transport Interface Distribution' with a bar chart showing 19 sites with < 10 Mbps, 0 with 10-100 Mbps, 0 with 100-500 Mbps, and 0 with > 500 Mbps; 'vEdge Inventory' with 7 Total, 7 Authorized, 7 Deployed, and 0 Staging; 'vEdge Health (Total 7)' with 7 Normal, 0 Warning, and 0 Error; 'Transport Health' with a line graph showing 100% health; 'Top Applications' with a bar chart; and 'Application-Aware Routing' with a table of tunnel endpoints.

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)
DC1-VEGE1.mpls-BR1-VEGE2.mpls	0.956	2.705
DC1-VEGE1.biz-internet-BR1-VEGE2.biz-l...	0.394	2.257
DC1-VEGE1.biz-internet-BR1-VEGE1.biz-l...	0.946	1.987
DC1-VEGE1.mpls-BR1-VEGE1.mpls	0.368	1.472

The pop-up should show the current version of vManage as 17.2.0. Click on “OK” button to close the pop-up.

The screenshot shows the Viptela vManage dashboard interface. A modal dialog box is open in the center, displaying the following information:

- Viptela vManage logo
- Platform Version: 17.2.0
- Application Version: 17.2.0
- Server: vManage
- Copyright (c) 2017, Viptela, Inc. All rights reserved.
- Timestamp: 2017-12-18 17:41:15,149
- Time zone: UTC
- An "OK" button is highlighted with a red box.

The background dashboard includes sections for Control Status (Total 9), Site Health View (Total 4), Transport Interface Distribution, vEdge Inventory, Top Applications, and Application-Aware Routing. The Application-Aware Routing table is partially visible below:

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)
DC1-VEDGE1.mpls-BR1-VEDGE2.mpls	0.956	2.705
DC1-VEDGE1.biz-internet-BR1-VEDGE2.biz...	0.394	2.257
DC1-VEDGE1.biz-internet-BR1-VEDGE1.biz...	0.946	1.987
DC1-VEDGE1.mpls-BR1-VEDGE1.mpls	0.368	1.472

Go to Software Upgrade page and Click on “Controllers” to upgrade vBonds and vSmarts.

The screenshot shows the vManage interface for software upgrades. The 'Controller' tab is selected, and a table displays the following data:

	Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability	Current Version	Available Versions	Default Version	Up Since
<input type="checkbox"/>	BR1-VEDG...	10.3.0.1	52c7911f-c5b0-45df-b826-315...	300	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	18 Dec 2017 8:52:00 AM PST
<input type="checkbox"/>	BR1-VEDG...	10.3.0.2	0a4a4c78-35a8-4c1c-bbd2-e0...	300	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	18 Dec 2017 8:52:00 AM PST
<input type="checkbox"/>	BR2-VEDG...	10.4.0.1	ddd801b2-8cbe-4394-abd1-3b...	400	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:27:00 AM PST
<input type="checkbox"/>	DC1-VED...	10.1.0.1	ebdc8bd9-17e5-4eb3-a5e0-f43...	100	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:26:00 AM PST
<input type="checkbox"/>	DC1-VED...	10.1.0.2	f21dbb35-30b3-47f4-93bb-d2b...	100	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:26:00 AM PST
<input type="checkbox"/>	DC2-VED...	10.2.0.1	9e785ad7-558a-40c6-b0c0-fcc...	200	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:26:00 AM PST
<input type="checkbox"/>	DC2-VED...	10.2.0.2	b3265c5c-3db6-4d25-9d3b-1f4...	200	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:26:00 AM PST

Click on the top Select button to select all the controllers. Controllers can be upgraded one at a time manually as well. The click on “Upgrade”.

The screenshot shows the vManage web interface for software upgrades. The browser address bar shows the URL `https://198.18.1.10/index.html#/app/maintenance/upgrade/controller`. The page title is "MAINTENANCE | SOFTWARE UPGRADE". Below the title, there are tabs for "vEdge", "Controller", and "vManage". A toolbar contains buttons for "Upgrade" (highlighted with a red box), "Activate", "Delete Available Software", and "Set Default Version". Below the toolbar is a search bar for "Device Group" and a "Total Rows: 4" indicator. A table lists four devices with columns for Hostname, System IP, Chassis Number, Site ID, Device Model, Reachability, Current Version, Available Versions, Default Version, and Up Since.

	Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability	Current Version	Available Versions	Default Version	Up Since
<input checked="" type="checkbox"/>	vBond-1	11.11.11.11	abd5e9d7-9dee-4d00-98b5-fdc...	--	vEdge Cloud (vBond)	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:27:00 AM PST
<input checked="" type="checkbox"/>	vBond-2	21.21.21.21	b6eec354-1d60-4c77-bb1a-7a...	--	vEdge Cloud (vBond)	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:27:00 AM PST
<input checked="" type="checkbox"/>	vSmart-1	12.12.12.12	10a98779-95f0-4383-871c-195...	10	vSmart	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:26:00 AM PST
<input checked="" type="checkbox"/>	vSmart-2	22.22.22.22	704bbc2f-aa9a-4068-84a2-fc3...	20	vSmart	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:27:00 AM PST

Select 17.2.0 from the version field. Check mark the “Activate and Reboot” option. Then click on “Upgrade” button.

The screenshot shows the vManage interface for a software upgrade. The main table lists four devices: vBond-1, vBond-2, vSmart-1, and vSmart-2. A 'Software Upgrade' dialog box is open, showing the 'Version' dropdown set to 17.2.0, the 'vManage' radio button selected, and the 'Activate and Reboot' checkbox checked. The 'Upgrade' button is highlighted with a red box.

Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability	Current Version	Available Versions	Default Version	Up Since
vBond-1	11.11.11.11	abd5e9d7-9dee-4d00-98b5-fdc...	--	vEdge Cloud (vBond)	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:27:00 AM PST
vBond-2	21.21.21.21	b6eec354-1d60-4c77-bb1a-7a...	--	vEdge Cloud (vBond)	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:27:00 AM PST
vSmart-1	12.12.12.12	10a9877e-95fn-4984-871c-195...	10	vSmart	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:26:00 AM PST
vSmart-2	22.22.22.22	704bb...						17.1.1	17 Dec 2017 7:27:00 AM PST

vManage will download the code and will activate the new version by rebooting the devices. This may take some time.

When the controllers are upgraded successfully, the status column will show it.

The screenshot shows the vManage interface with a 'TASK VIEW' for 'Software Install'. The status is 'Validation Success'. The table below lists the installation details for four devices, all of which are marked as 'Success'.

Status	Message	Hostname	System IP	Site ID	Device Type	Device Model	
Success	Done - Software Install	vBond-1	11.11.11.11	--	vBond	vEdge Cloud	10.10.10.10
Success	Done - Software Install	vBond-2	21.21.21.21	--	vBond	vEdge Cloud	10.10.10.10
Success	Done - Software Install	vSmart-1	12.12.12.12	10	vSmart	vSmart	10.10.10.10
Success	Done - Software Install	vSmart-2	22.22.22.22	20	vSmart	vSmart	10.10.10.10

Now the vEdges are left for upgrade. Go to the Software Upgrade page and select ALL the vEdges. Individual or a sub-group of vEdges can be upgraded at a given time. Click on “Upgrade” button.



7 Rows Selected **Upgrade** **Activate** **Delete Available Software** **Set Default Version**

Device Group: All

<input checked="" type="checkbox"/>	Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability	Current Version	Available Versions	Default Version	Up Since
<input checked="" type="checkbox"/>	BR1-VEDG...	10.3.0.1	52c7911f-c5b0-45df-b826-315...	300	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	18 Dec 2017 8:52:00 AM PST
<input checked="" type="checkbox"/>	BR1-VEDG...	10.3.0.2	0a4a4c78-35a8-4c1c-bbd2-e0...	300	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	18 Dec 2017 8:52:00 AM PST
<input checked="" type="checkbox"/>	BR2-VEDG...	10.4.0.1	ddd801b2-8cbe-4394-abd1-3b...	400	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:27:00 AM PST
<input checked="" type="checkbox"/>	DC1-VED...	10.1.0.1	ebdc8bd9-17e5-4eb3-a5e0-f43...	100	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:26:00 AM PST
<input checked="" type="checkbox"/>	DC1-VED...	10.1.0.2	f21dbb35-30b3-47f4-93bb-d2b...	100	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:26:00 AM PST
<input checked="" type="checkbox"/>	DC2-VED...	10.2.0.1	9e785ad7-558a-40c6-b0c0-fcc...	200	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:26:00 AM PST
<input checked="" type="checkbox"/>	DC2-VED...	10.2.0.2	b3265c5c-3db6-4d25-9d3b-1f4...	200	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:26:00 AM PST

In the pop-up window select 17.2.0 as the version required, check mark the “Activate and Reboot” option. Then click the “Upgrade” button.

[Important: This process may take a long time to download the image to the vEdge Routers. One may decide to upgrade one or two vEdges]

The screenshot shows the vManage interface for a software upgrade. A table lists 7 vEdge devices with columns for Hostname, System IP, Chassis Number, Site ID, Device Model, Reachability, Current Version, Available Versions, Default Version, and Up Since. A 'Software Upgrade' dialog box is open, showing 'Version 17.2.0' selected, 'vManage' as the source, and the 'Activate and Reboot' checkbox checked. The 'Upgrade' button is highlighted with a red box.

Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability	Current Version	Available Versions	Default Version	Up Since
BR1-VEDG...	10.3.0.1	52c7911f-c5b0-45df-b826-315...	300	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	18 Dec 2017 8:52:00 AM PST
BR1-VEDG...	10.3.0.2	0a4a4c78-35a8-4c1c-bbd2-e0...	300	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	18 Dec 2017 8:52:00 AM PST
BR2-VEDG...	10.4.0.1	ddd801h29bbs-439fabr12h...	400	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:27:00 AM PST
DC1-VED...	10.1.0.1	ebdc8...						17.1.1	17 Dec 2017 7:26:00 AM PST
DC1-VED...	10.1.0.2	f21dbb...						17.1.1	17 Dec 2017 7:26:00 AM PST
DC2-VED...	10.2.0.1	9e785...						17.1.1	17 Dec 2017 7:26:00 AM PST
DC2-VED...	10.2.0.2	b3265...						17.1.1	17 Dec 2017 7:26:00 AM PST

Once the vEdges are successfully upgraded, the screen will show the status on the screen.



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)