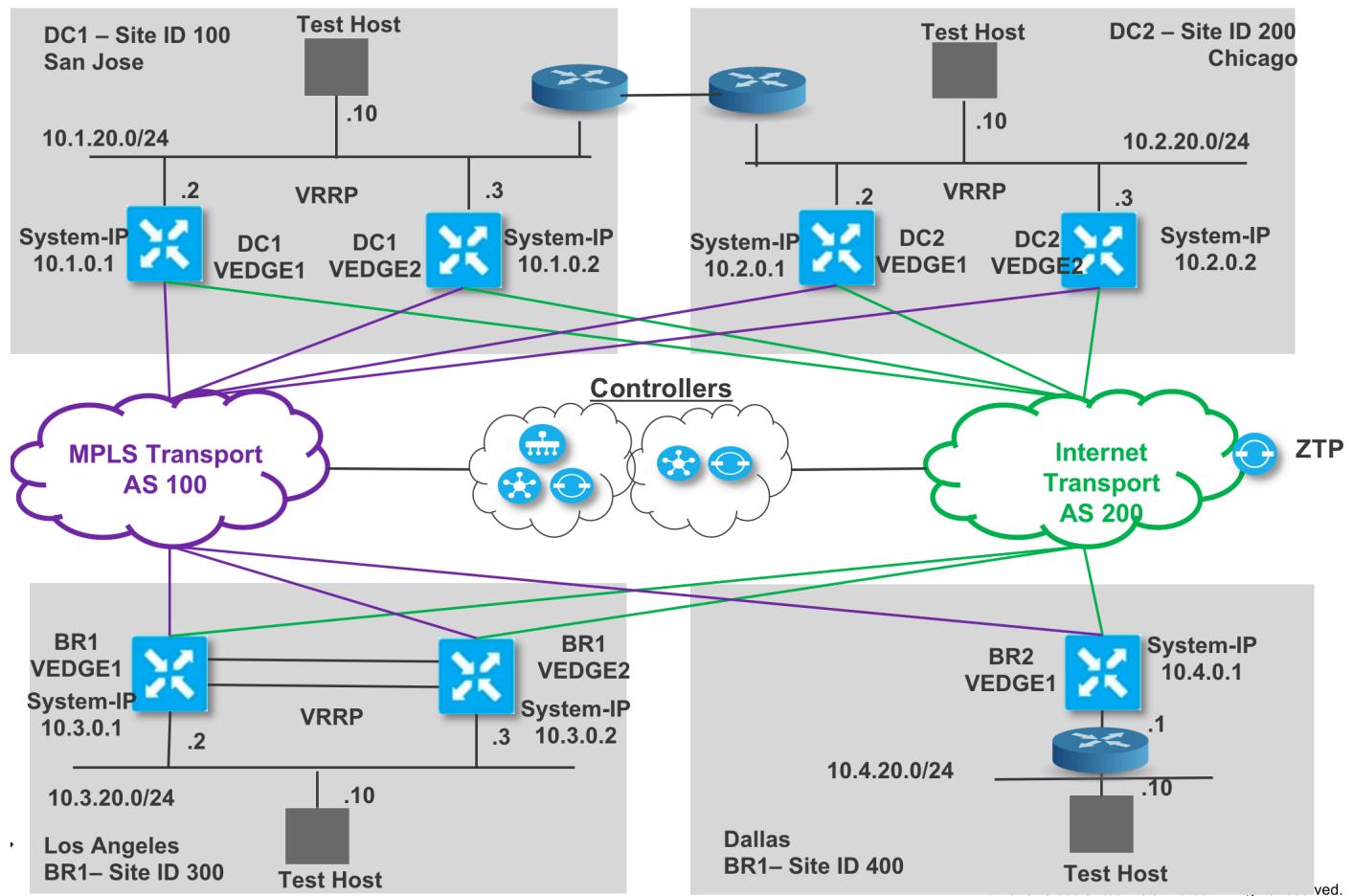


# Introduction to Cisco SD-WAN (Viptela) Lab Guide

LABEN-2010

<b>INTRODUCTION TO CISCO SD-WAN (VIPTELA)</b>	<b>LAB GUIDE</b>	<b>1</b>
<b>LAB01 – DEPLOY VEDGE IN BRANCH 2 USING ZTP</b>		<b>3</b>
STEPS.....		4
DPI .....		26
IPFIX Flow Records .....		26
Interface Stats .....		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

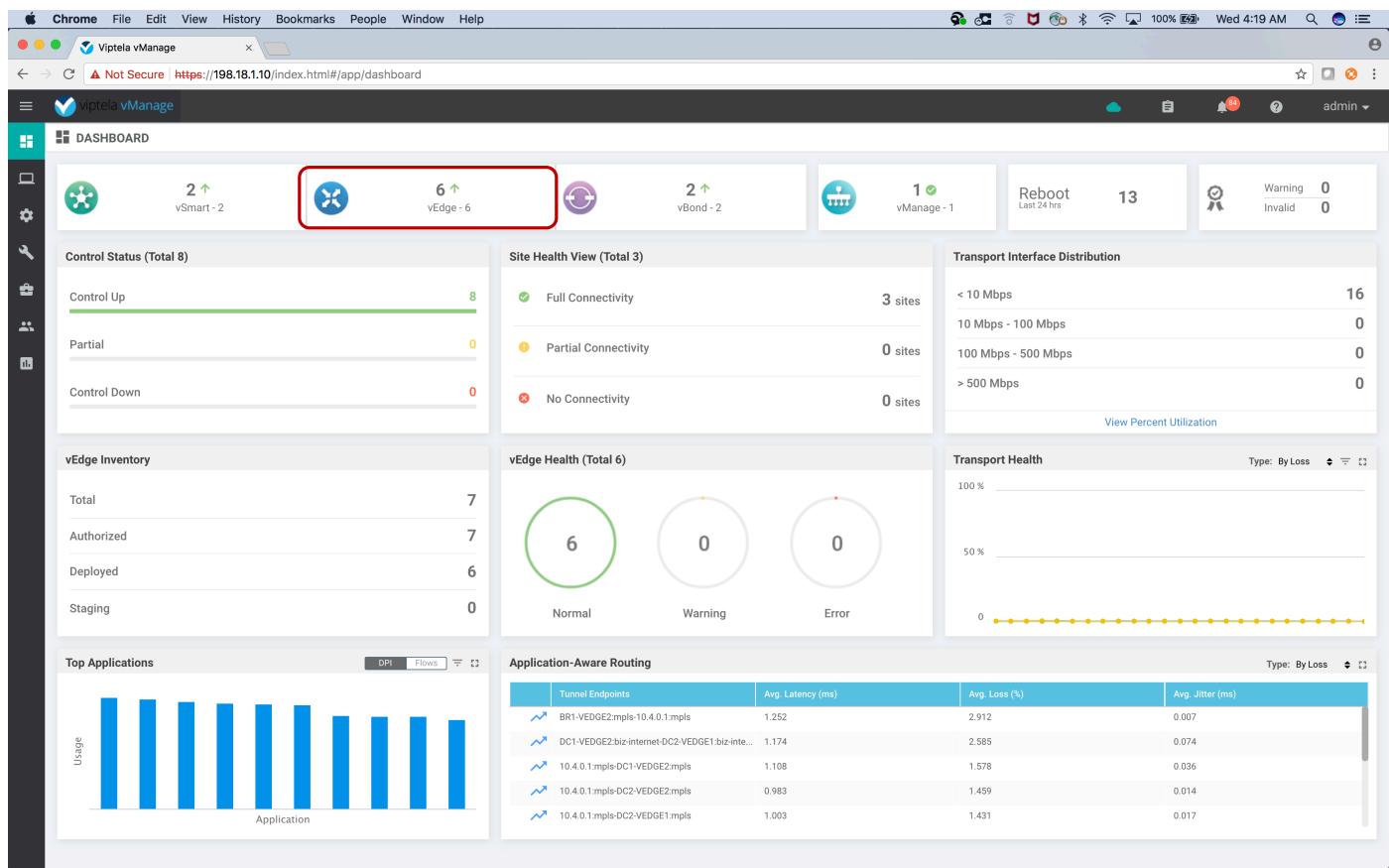
In this scenario we will bring up Branch 2 site using ZTP.

### Steps

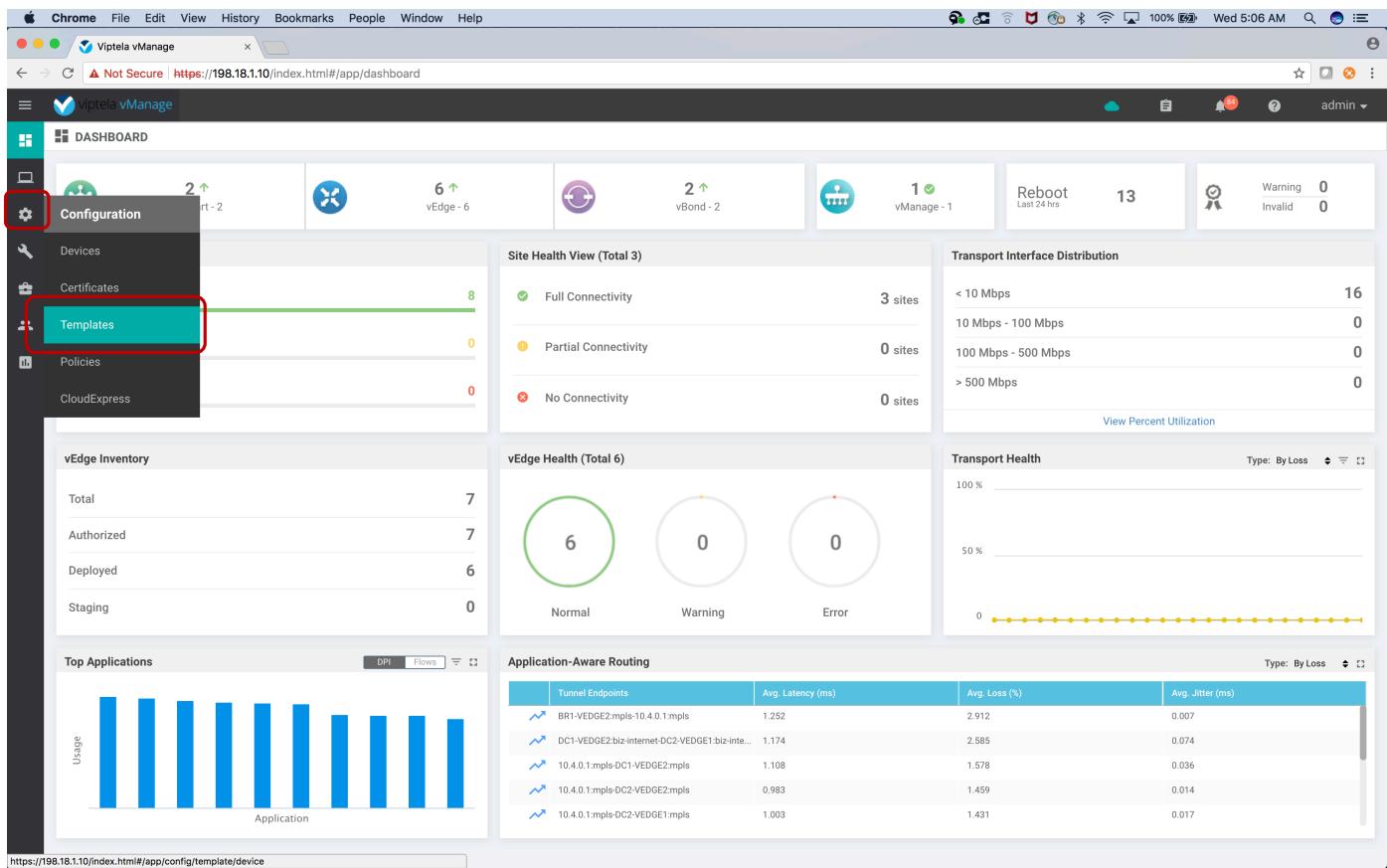
Deploy a Branch using vManage configuration template and Viptela's Zero Touch Provisioning (ZTP) service. ZTP process is simulated in this lab using default configuration from the factory for the vEdge in Branch 2.

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-VEDGE1 is still need to be provisioned via ZTP.



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

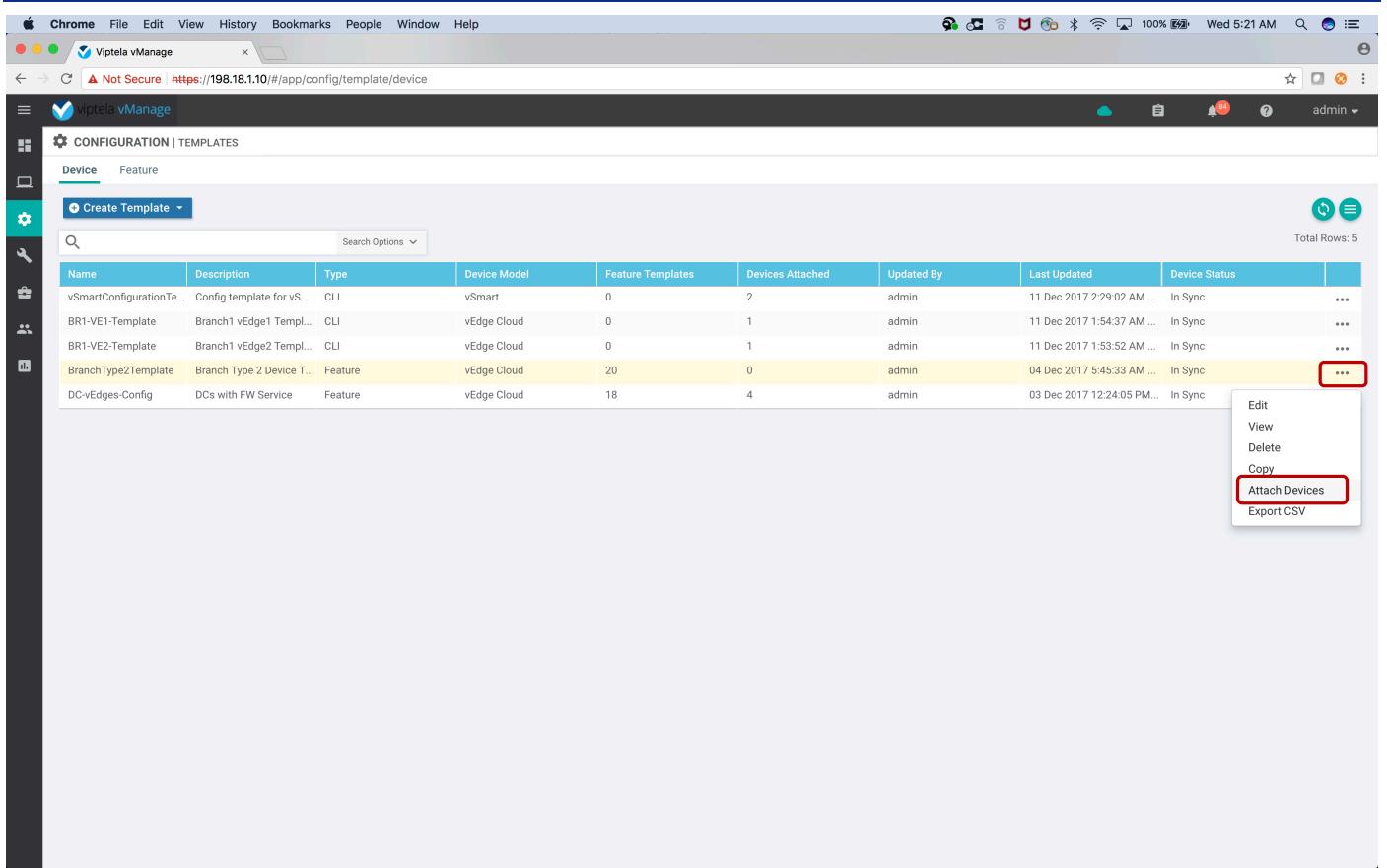


The screenshot shows the vManage dashboard with the Configuration menu open. The 'Templates' option is highlighted with a red box. The dashboard includes sections for Site Health View (Total 3), Transport Interface Distribution, vEdge Inventory, vEdge Health (Total 6), Application-Aware Routing, and Transport Health.

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 Cisco Viptela vManage interface. The top navigation bar includes 'File', 'Edit', 'View', 'History', 'Bookmarks', 'People', 'Window', and 'Help'. The title bar says 'Viptela vManage'. The main content area is titled 'CONFIGURATION | TEMPLATES' and has tabs for 'Device' and 'Feature'. A search bar and 'Search Options' dropdown are present. Below is a table with columns: Name, Description, Type, Device Model, Feature Templates, Devices Attached, Updated By, Last Updated, and Device Status. The table contains five rows. A context menu is open over the last row ('DC-vEdges-Config'), with options: Edit, View, Delete, Copy, Attach Devices (which is highlighted with a red box), and Export CSV.

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	...

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.

The screenshot shows the Cisco Viptela vManage web interface. The main menu bar includes Chrome, File, Edit, View, History, Bookmarks, People, Window, and Help. The title bar indicates the URL is <https://198.18.1.10/#/app/config/template/device>. The top right corner shows system status and the date and time: Wed 5:26 AM.

The left sidebar contains icons for Home, Configuration, Templates, Device, Feature, and Create Template. The main content area is titled "CONFIGURATION | TEMPLATES" and "Device".

A modal dialog box titled "Attach Devices" is open. It has two sections: "Available Devices" and "Selected Devices".

- Available Devices:** A table with columns "Name" and "Device IP". One row, "ddd801b2-8cbe-4394-abd1-3b71e39886e3", is highlighted with a red box. Other entries include BR1-VEDGE1, BR1-VEDGE2, DC1-VEDGE1, DC1-VEDGE2, DC2-VEDGE1, DC2-VEDGE2, and vBond-1.
- Selected Devices:** A table with columns "Name" and "Device IP". It is currently empty, indicated by "0 Items Selected".

Between the two tables is a central area with a blue arrow pointing right and a smaller blue arrow pointing left. Below the tables are "Attach" and "Cancel" buttons.

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

The screenshot shows the Cisco Viptela vManage web interface. The main menu bar includes Chrome, File, Edit, View, History, Bookmarks, People, Window, and Help. The title bar indicates the URL is <https://192.18.1.10/#/app/config/template/device>. A warning message 'Not Secure' is displayed. The left sidebar has icons for Home, Configuration, Monitoring, Analytics, and Support. The main content area is titled 'CONFIGURATION | TEMPLATES' and shows tabs for 'Device' and 'Feature'. A sub-menu 'Create Template' is open. A search bar and 'Search Options' dropdown are also present. The central part of the screen displays the 'Attach Devices' dialog. This dialog has two main sections: 'Available Devices' and 'Selected Devices'. The 'Available Devices' section lists the following items:

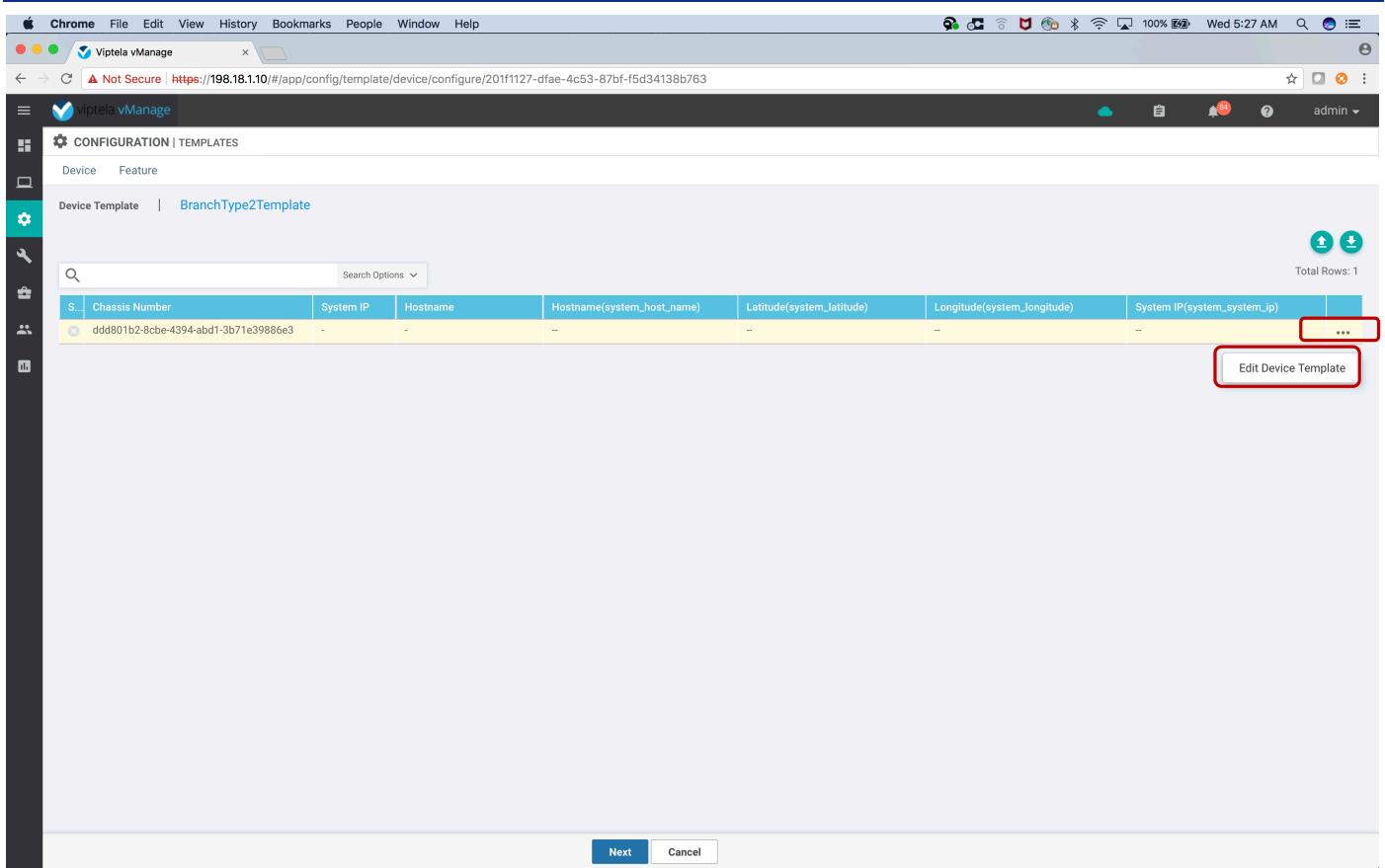
Name	Device IP
BR1-VEDGE1	10.3.0.1
BR1-VEDGE2	10.3.0.2
DC1-VEDGE1	10.1.0.1
DC1-VEDGE2	10.1.0.2
DC2-VEDGE1	10.2.0.1
DC2-VEDGE2	10.2.0.2
vBond-1	11.11.11.11
vBond-2	21.21.21.21

The 'Selected Devices' section shows one item selected:

Name	Device IP
ddd801b2-8cbe-4394-abd1-3b71e39886e3	

At the bottom of the dialog are 'Attach' and 'Cancel' buttons, with 'Attach' being highlighted by a red box.

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



The screenshot shows the Viptela vManage interface with the title "CONFIGURATION | TEMPLATES". The sub-page is "Device Template" under "BranchType2Template". A table lists a single device template entry:

S...	Chassis Number	System IP	Hostname	Hostname(system_host_name)	Latitude(system_latitude)	Longitude(system_longitude)	System IP(system_system_ip)	...
	ddd801b2-8cbe-4394-abd1-3b71e39886e3	-	-	-	-	-	-	<a href="#">Edit Device Template</a>

Total Rows: 1

At the bottom right of the table, there is a red box around the "Edit Device Template" button.

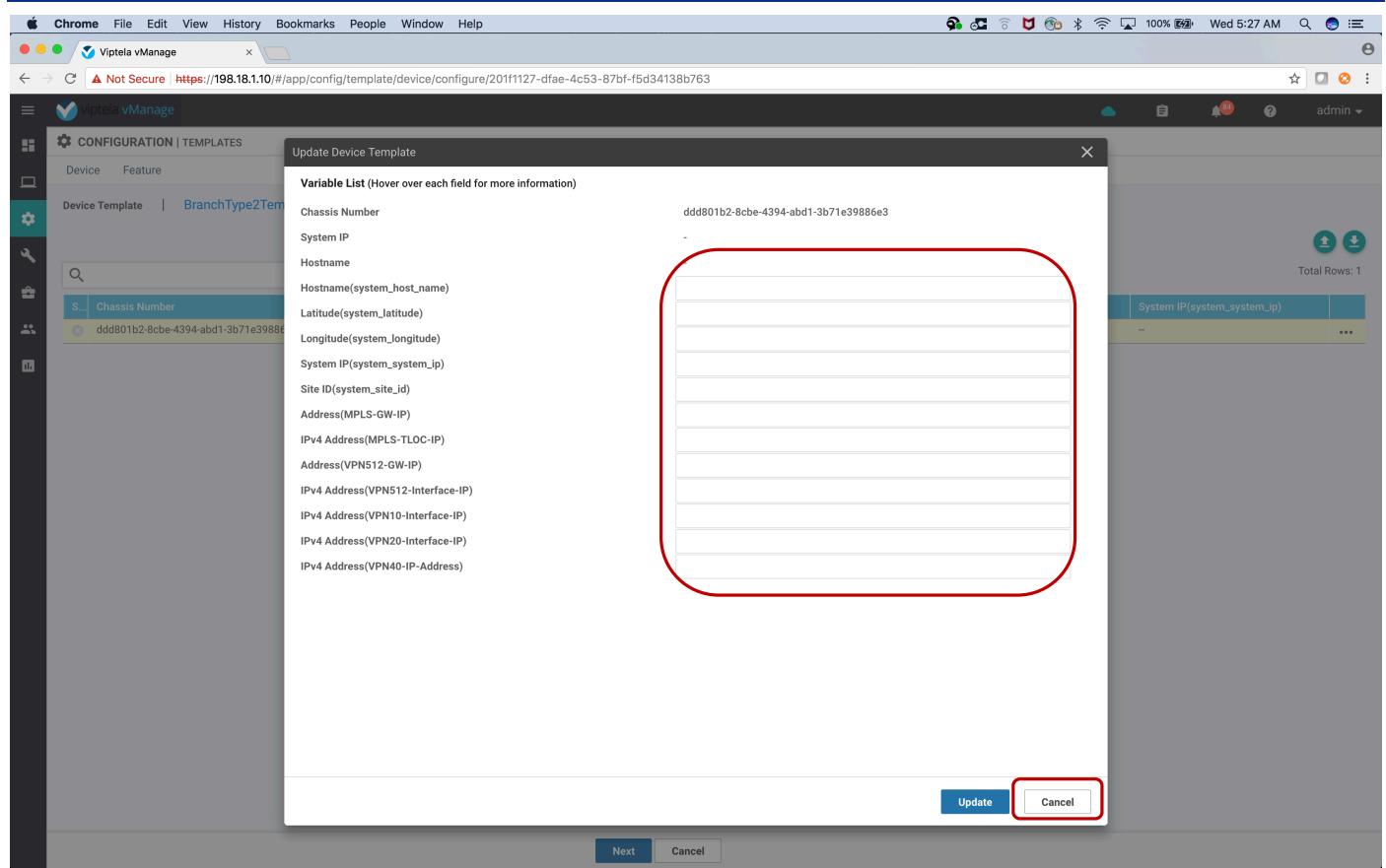
The “Edit Device Template” provides an option to update the variables values associated with the Branch2 vEdge.

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.



Chrome File Edit View History Bookmarks People Window Help

Viptela vManage

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

CONFIGURATION | TEMPLATES

Device Feature

Device Template | BranchType2Tem

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)

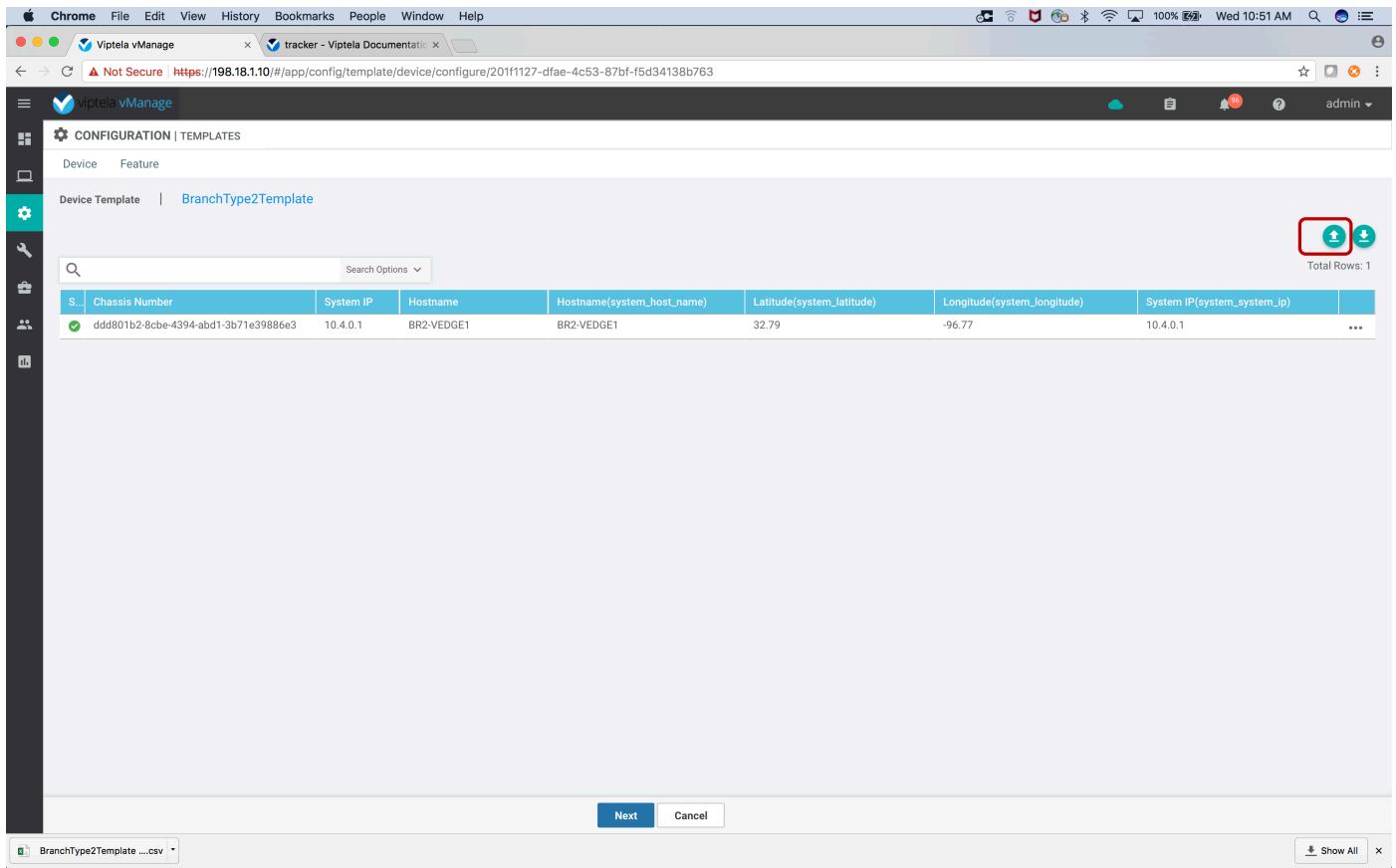
Total Rows: 1

System IP(system\_system\_ip)

Update Cancel

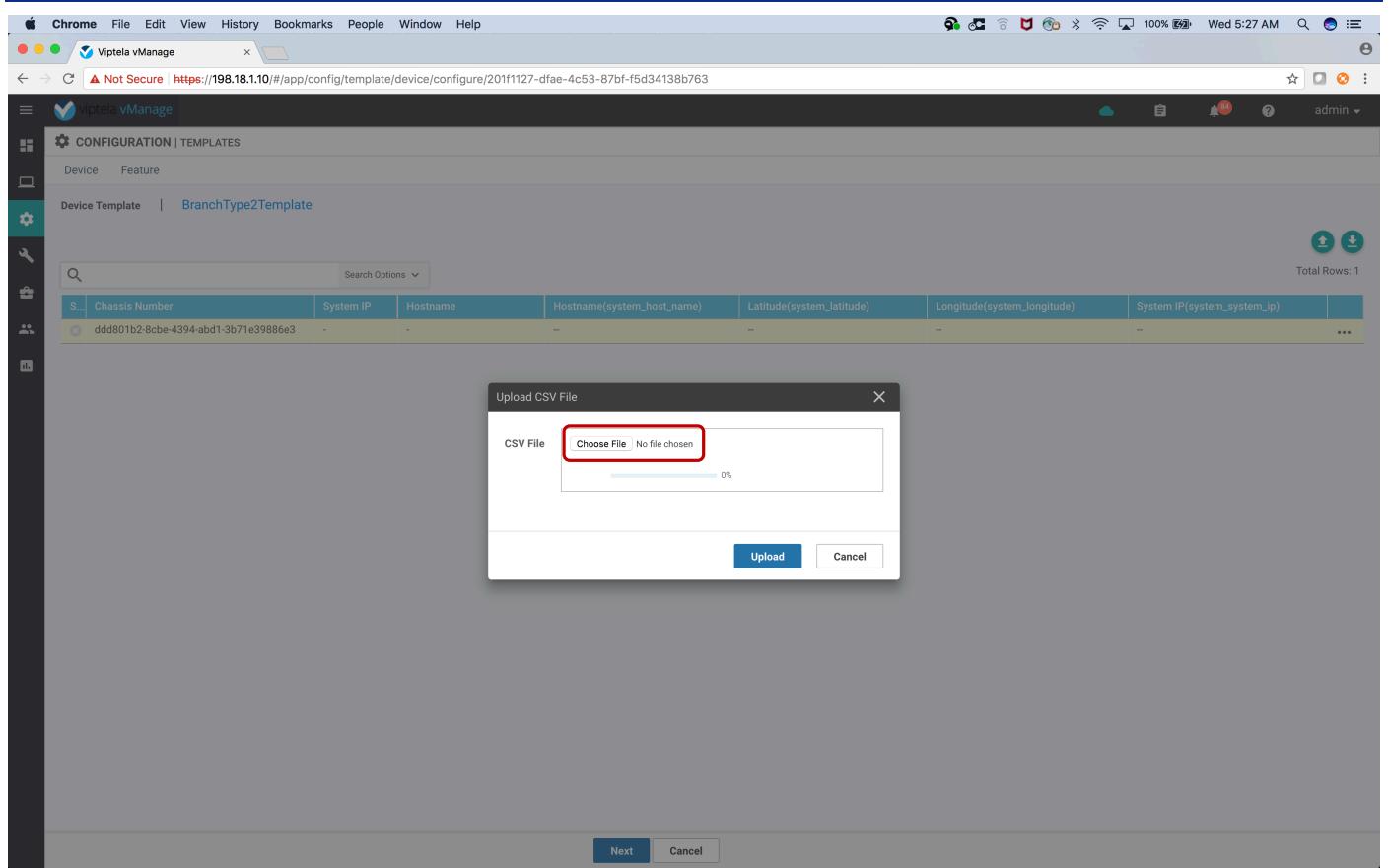
Next Cancel

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



The screenshot shows a browser window for 'Viptela vManage' with the URL <https://198.18.1.10/#/app/config/template/device/configure/201f1127-dfae-4c53-87bf-f5d34138b763>. The page title is 'tracker - Viptela Documentation'. The main content area is titled 'CONFIGURATION | TEMPLATES' and shows a table for 'Device Template' named 'BranchType2Template'. The table has columns: S., Chassis Number, System IP, Hostname, Hostname(system\_host\_name), Latitude(system\_latitude), Longitude(system\_longitude), System IP(system\_system\_ip), and a 'More' button. A single row is present with values: Chassis Number (ddd801b2-8cbe-4394-abd1-3b71e39886e3), System IP (10.4.0.1), Hostname (BR2-VEDGE1), Hostname(system\_host\_name) (BR2-VEDGE1), Latitude(system\_latitude) (32.79), Longitude(system\_longitude) (-96.77), System IP(system\_system\_ip) (10.4.0.1). The top right of the table area contains an 'Upload' icon (a blue circle with a white upward arrow) and a 'Download' icon (a green circle with a white downward arrow). Below the table are 'Next' and 'Cancel' buttons. At the bottom left is a dropdown menu showing 'BranchType2Template ....csv'. At the bottom right are 'Show All' and a close button.

Click on the “Choose File” button.



The screenshot shows a browser window for Viptela vManage. The URL is https://198.18.1.10/#/app/config/template/device/configure/201f1127-dfae-4c53-87bf-f5d34138b763. The page title is "Viptela vManage". The main navigation bar includes "File", "Edit", "View", "History", "Bookmarks", "People", "Window", and "Help". The top right corner shows system status: 100% battery, 5:27 AM, and user "admin".

The left sidebar has icons for Home, Devices, Features, Configuration, Templates, Scripts, and Help. The "TEMPLATES" section is selected.

The main content area is titled "CONFIGURATION | TEMPLATES" and shows "Device Template" and "BranchType2Template". A search bar and search options dropdown are present.

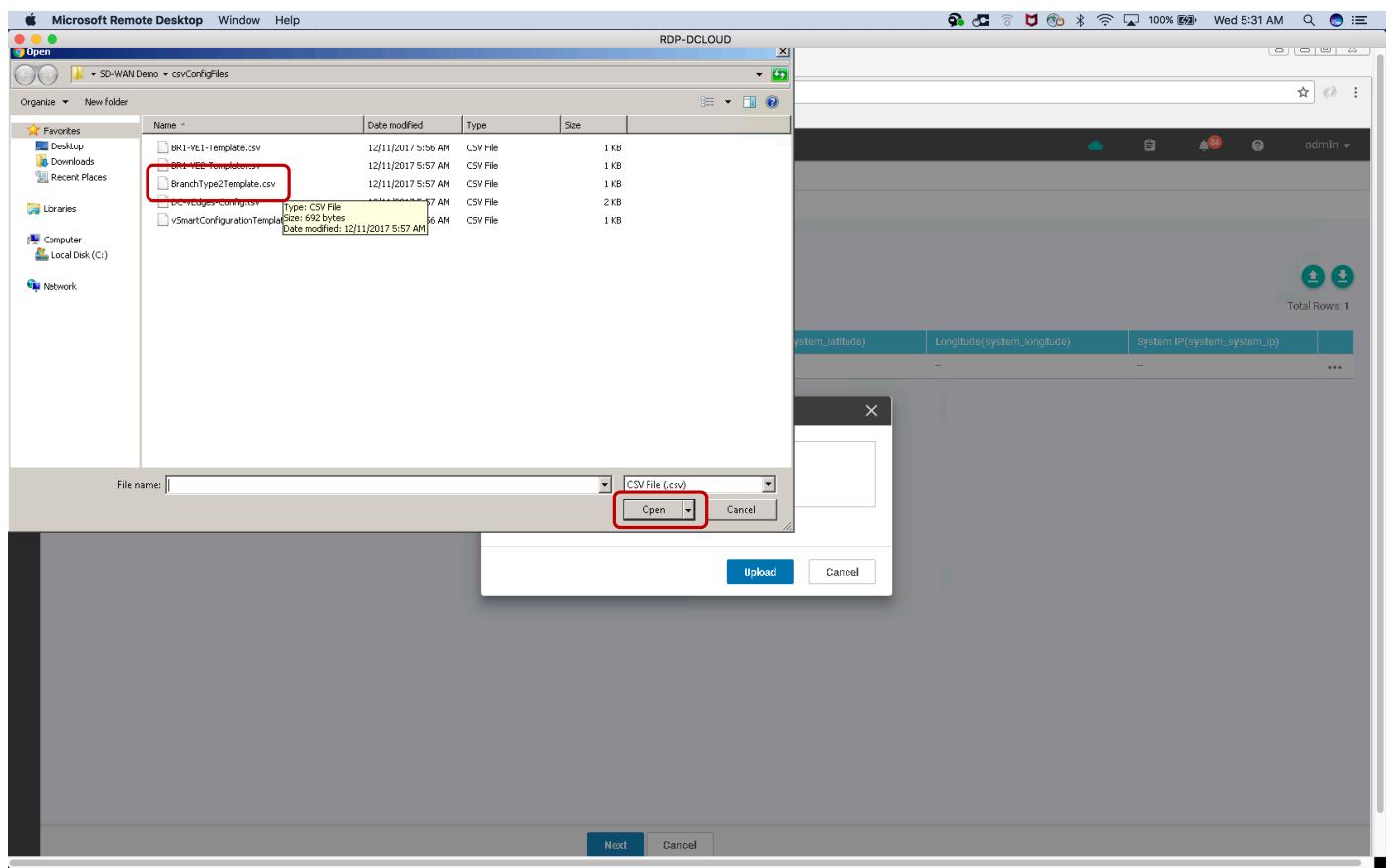
A table displays device configuration details:

S...	Chassis Number	System IP	Hostname	Hostname(system_host_name)	Latitude(system_latitude)	Longitude(system_longitude)	System IP(system_system_ip)
	ddd801b2-9cbe-4394-abd1-3b71e39886e3	-	-	-	-	-	-

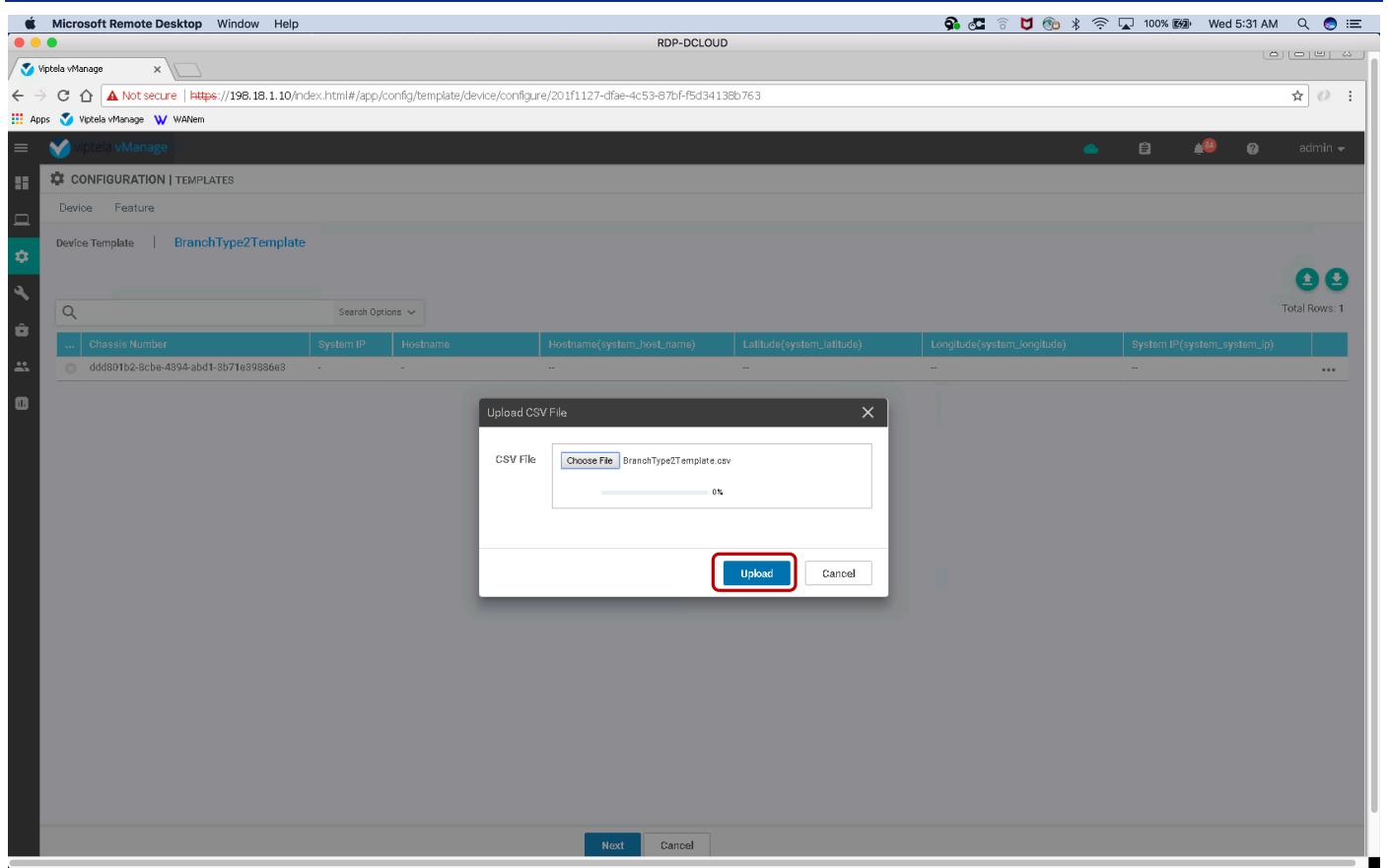
Total Rows: 1

An "Upload CSV File" dialog box is overlaid on the page. It contains a "CSV File" input field with a red box around the "Choose File" button, which displays "No file chosen". Below the input field is a progress bar at 0%. At the bottom are "Upload" and "Cancel" buttons.

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.



The screenshot shows a Microsoft Remote Desktop session for the Cisco dCloud environment. The main window is the Viptela vManage configuration interface, specifically the 'CONFIGURATION | TEMPLATES' section under 'Device Template'. A sub-section titled 'BranchType2Template' is selected. On the left, there's a sidebar with various icons. In the center, there's a table with columns: Chassis Number, System IP, Hostname, Hostname(system\_host\_name), Latitude(system\_latitude), Longitude(system\_longitude), and System IP(system\_system\_ip). One row is visible with the value 'ddd801b2-8cbe-4394-abd1-8b71e39886e3' in the Chassis Number column. Overlaid on the main window is a modal dialog titled 'Upload CSV File'. Inside the dialog, there's a 'CSV File' input field containing 'BranchType2Template.csv', a progress bar at 0%, and two buttons at the bottom: 'Upload' (which is highlighted with a red box) and 'Cancel'. At the very bottom of the screen, there are 'Next' and 'Cancel' buttons.

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.

Microsoft Remote Desktop Window Help RDP-DCLOUD

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

Apps Viptela vManage WANem

viptela vManage

CONFIGURATION | TEMPLATES

Device Feature

Device Template | BranchType2Template

Chassis Number	System IP	Hostname	Hostname(system_host_name)	Latitude(system_latitude)	Longitude(system_longitude)	System IP(system_system_ip)	...
ddd801b2-8cbe-4394-abd1-3b71e39886e3	10.4.0.1	BR2-VEDGE1	BR2-VEDGE1	32.79	-96.77	10.4.0.1	***

Total Rows: 1

Next Cancel

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”.

The screenshot shows a Microsoft Remote Desktop session for the Cisco dCloud platform. The title bar indicates the session is titled "RDP-DCLOUD". The main window is the "vManage" interface, specifically the "CONFIGURATION | TEMPLATES" section under "Device Template". A yellow message box at the top right states: "'Configure' action will be applied to 1 device(s) attached to 1 device template(s).".

The "BranchType2Template" tab is selected, showing a total of 1 device. The device list contains one entry: "ddc801c2-8cbe-4394-ab11-3671e39886e3 BR2-VEDGE1 0.4.0.1". This entry is highlighted with a red box.

The configuration pane displays the following CLI configuration:

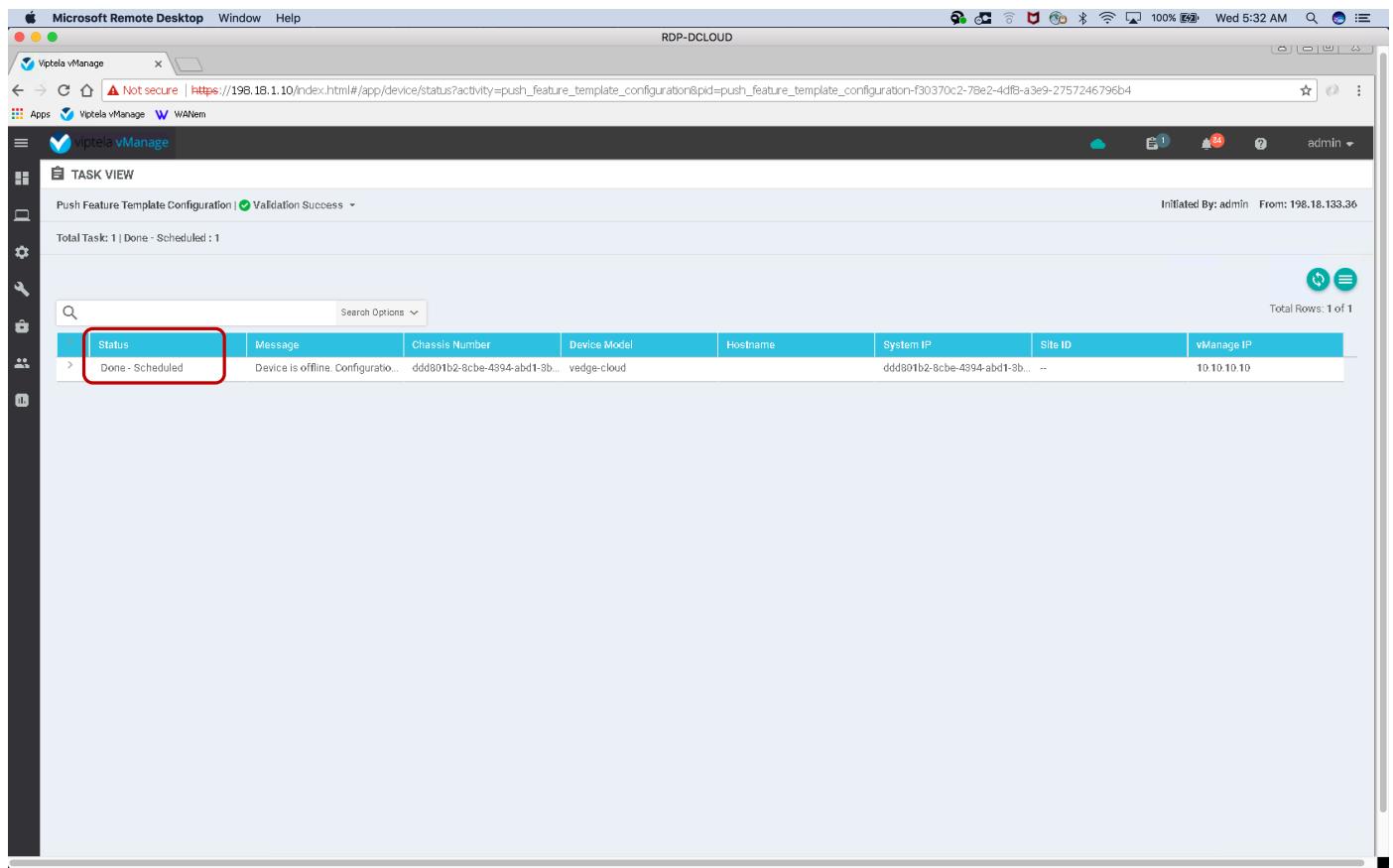
```

bfd app-route poll-interval 5000
system
device-model wedge-cloud
host-name BR2-VEDGE1
gps-location latitude 32.79
gps-location longitude -06.77
system-ip 10.4.0.1
domain-id
site-id 400
no route-consistency-check
organization-name "Cisco Sy1 - 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 $6$siuK8Q==$wT2lUa9B5rePI0gB8s14E6PAJdvXgNbgv/wj38F1C6sWdRazdxorYYTLrL6syIG6qnLABTrnE96HJ3KF6QRq1
!
logging
disk
enable
!

```

At the bottom of the configuration pane, there are "Back", "Configure Devices", and "Cancel" buttons. The "Configure Devices" button is highlighted with a red box.

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



The screenshot shows the vManage interface on an RDP session. The title bar indicates "Microsoft Remote Desktop" and "RDP-DCLOUD". The URL in the address bar is "https://198.18.1.10/index.html#/app/device/status?activity=push\_feature\_template\_configuration&pid=push\_feature\_template\_configuration-f30370c2-78e2-4df8-a3e9-275724679eb4". The main content area is titled "TASK VIEW" and displays a table of tasks. One task is listed with the following details:

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Done - Scheduled	Device is offline. Configuration... ddd801b2-8cbe-4394-abd1-8b...	vedge-cloud			ddd801b2-8cbe-4394-abd1-8b...	...	10.10.10.10

The "Status" column is highlighted with a red box. The status is currently "Done - Scheduled".

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

The screenshot shows the Viptela vManage dashboard with various sections:

- 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
- vEdge Inventory:**

Total	7
Authorized	7
Deployed	6
Staging	0
- vEdge Health (Total 6):**

Normal: 6
Warning: 0
Error: 0
- Transport Health:**

Type: By Loss
- Top Applications:**

Usage	Application
High	Application 1
High	Application 2
High	Application 3
Medium	Application 4
Medium	Application 5
Medium	Application 6
Medium	Application 7
Medium	Application 8
- Application-Aware Routing:**

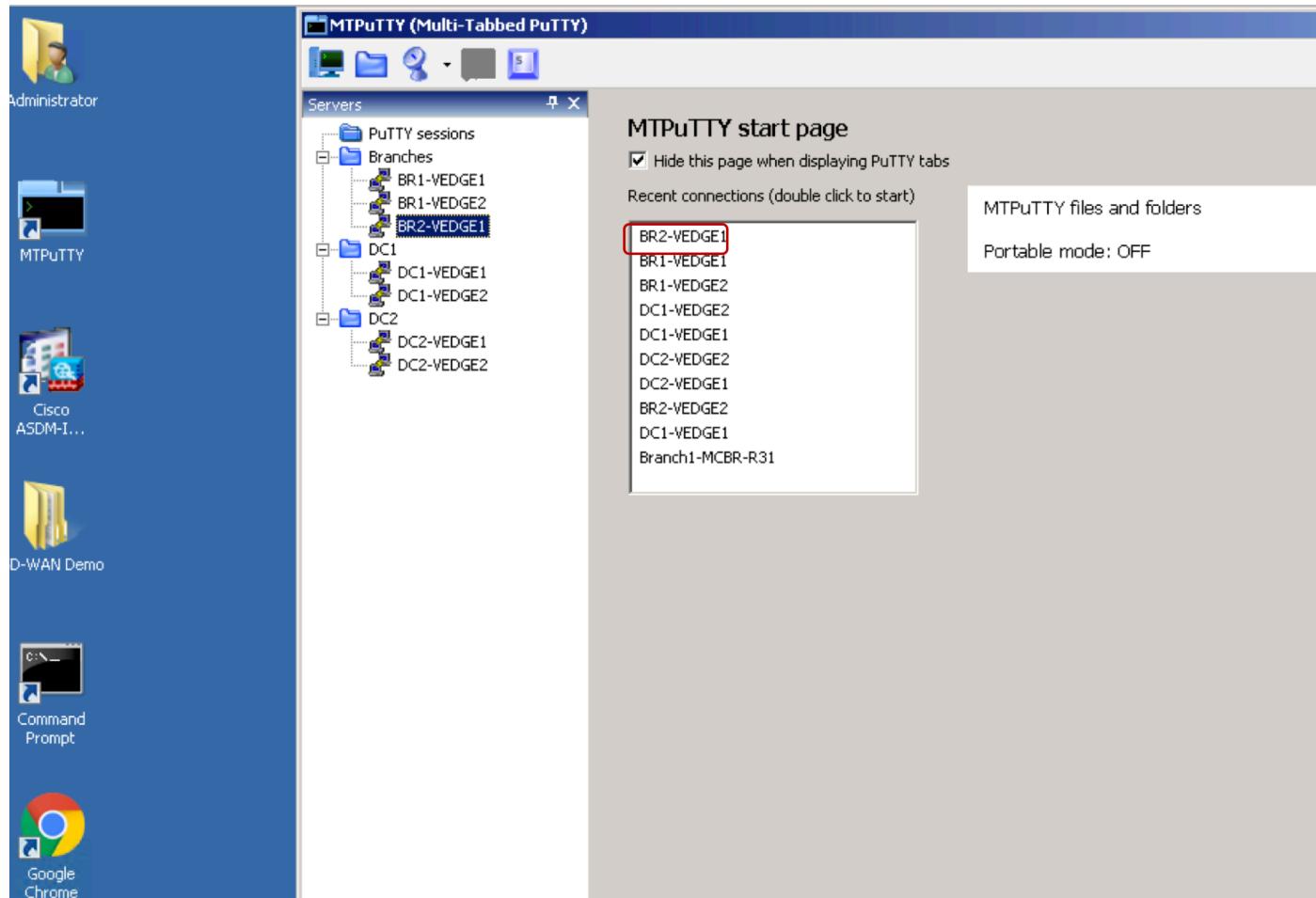
Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
BRI-VEDGE2.mpls-10.4.0.1.mpls	1.252	2.912	0.007
DC1-VEDGE2.biz-internet-DC2-VEDGE1.biz-inte...	1.174	2.585	0.074
10.4.0.1.mpls-DC1-VEDGE2.mpls	1.108	1.578	0.036
10.4.0.1.mpls-DC2-VEDGE2.mpls	0.983	1.459	0.014
10.4.0.1.mpls-DC2-VEDGE1.mpls	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.

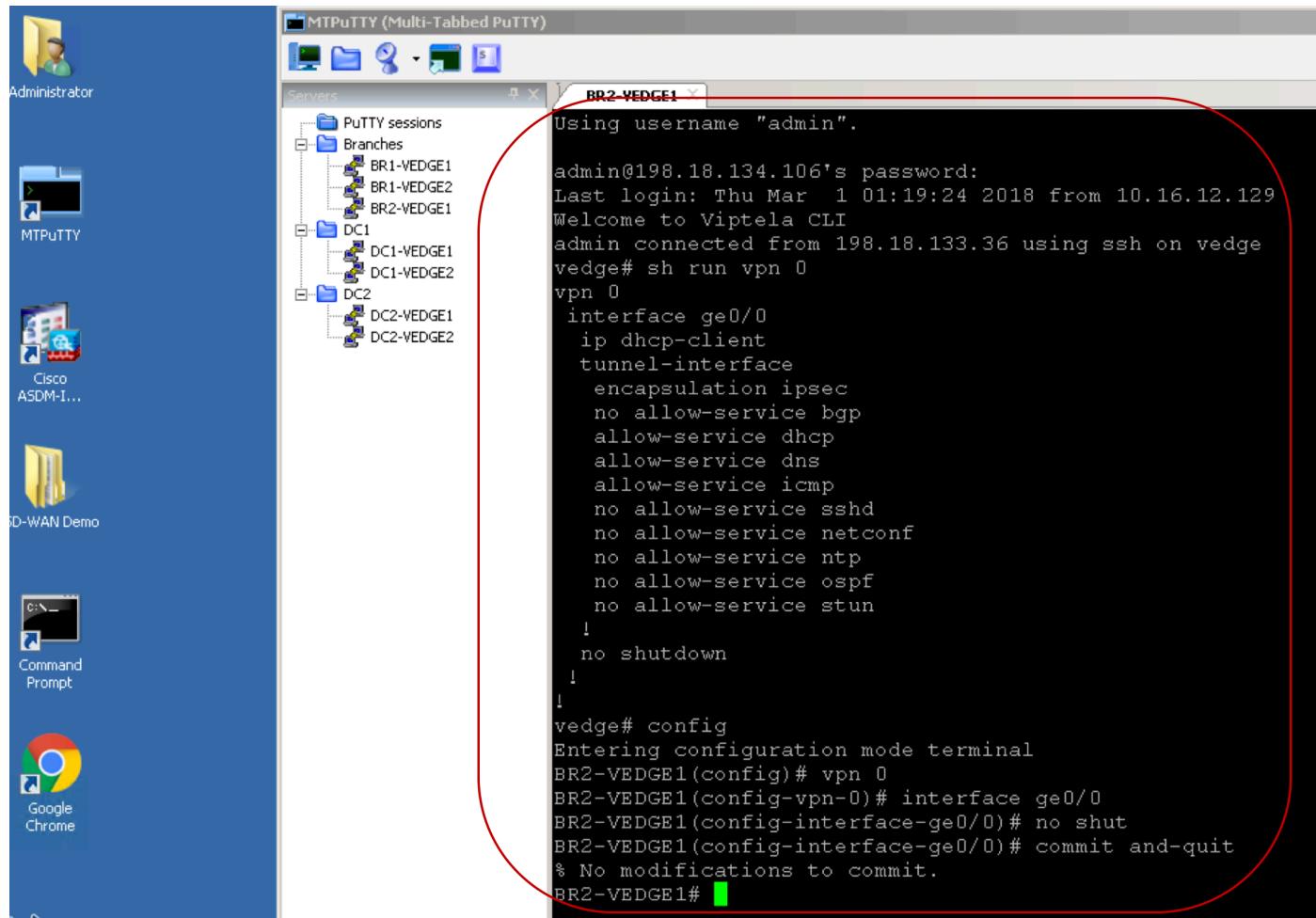
```
show run vpn 10
```

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.



```

Administrator
MTPuTTY
Cisco ASDM-I...
SD-WAN Demo
Command Prompt
Google Chrome

PuTTY (Multi-Tabbed PuTTY)
Servers BR2-VEDGE1
PuTTY sessions
Branches
  BR1-VEDGE1
    BR1-VEDGE2
    BR2-VEDGE1
  DC1
    DC1-VEDGE1
    DC1-VEDGE2
  DC2
    DC2-VEDGE1
    DC2-VEDGE2

Using username "admin".
admin@198.18.134.106's password:
Last login: Thu Mar  1 01:19:24 2018 from 10.16.12.129
Welcome to Viptela CLI
admin connected from 198.18.133.36 using ssh on vedge
vedge# sh run vpn 0
vpn 0
  interface ge0/0
    ip dhcp-client
    tunnel-interface
      encapsulation ipsec
      no allow-service bgp
      allow-service dhcp
      allow-service dns
      allow-service icmp
      no allow-service sshd
      no allow-service netconf
      no allow-service ntp
      no allow-service ospf
      no allow-service stun
    !
    no shutdown
  !
  !
vedge# config
Entering configuration mode terminal
BR2-VEDGE1(config)# vpn 0
BR2-VEDGE1(config-vpn-0)# interface ge0/0
BR2-VEDGE1(config-interface-ge0/0)# no shut
BR2-VEDGE1(config-interface-ge0/0)# commit and-quit
% No modifications to commit.
BR2-VEDGE1#

```

Issue the following command:

show run system

show run vpn 0

show run vpn 10

config t

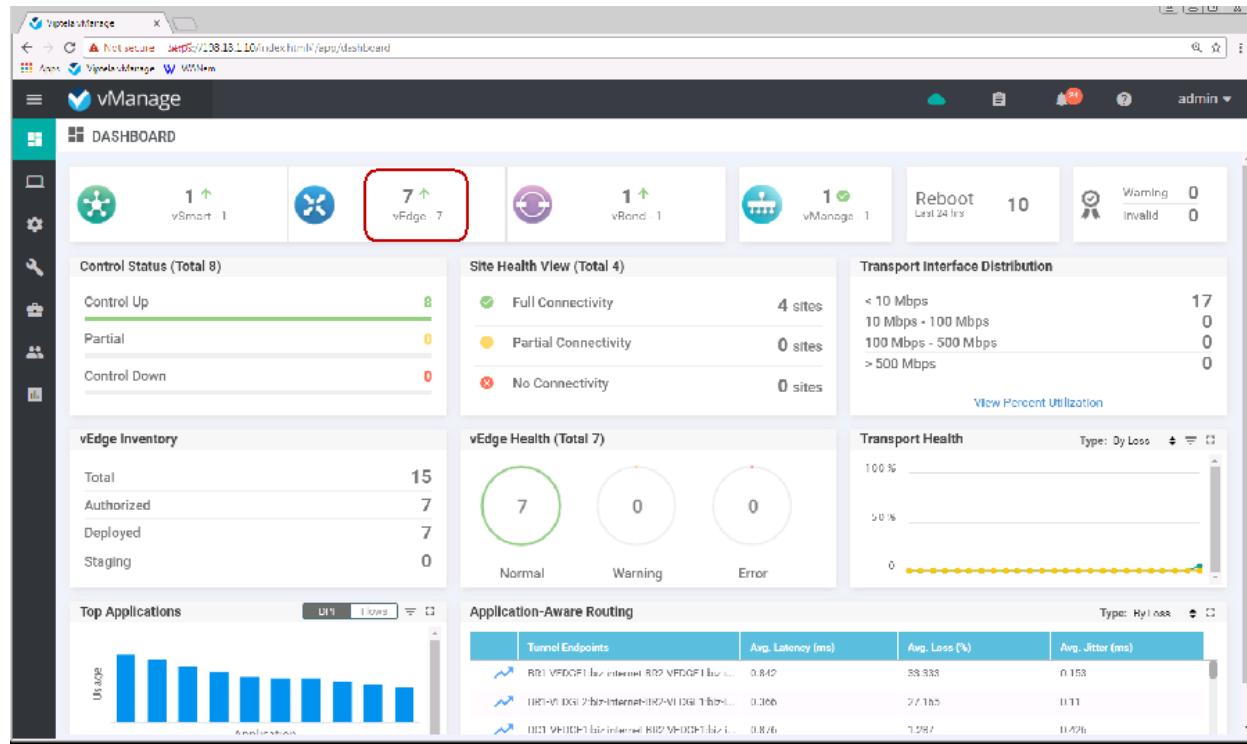
vpn 0

interface ge0/0

no shutdown

commit and-quit

Go back to the vManage dashboard. The BR2-VEDGE1 will come up and the dashboard will show total of 7 vEdges are operational.



Click on Monitor icon and then select Network.

The screenshot shows the vManage dashboard with the 'Network' section highlighted by a red box. The dashboard includes sections for Site Health View (Total 4), Transport Interface Distribution, vEdge Health (Total 7), Transport Health, Application-Aware Routing, and Top Applications. The 'Network' section also displays a list of devices with their status, system IP, and reachability.

Device	Status	System IP	Reachability
BR1-VEDGE1	reachable	10.3.0.1	reachable
BR1-VEDGE2	reachable	10.3.0.2	reachable
BR2-VEDGE1	reachable	10.4.0.1	reachable
DC1-VEDGE1	reachable	10.1.0.1	reachable
DC1-VEDGE2	reachable	10.1.0.2	reachable
DC2-VEDGE1	reachable	10.2.0.1	reachable
DC2-VEDGE2	reachable	10.2.0.2	reachable
vbond	reachable	11.11.11.11	reachable
vmanage	reachable	10.10.10.10	reachable
vsmart	reachable	12.12.12.12	reachable

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

The screenshot shows the 'MONITOR | NETWORK' page in vManage. The 'BR2-VEDGE1' entry in the list is highlighted with a red box. The page includes a search bar, filter dropdown, and a table with columns for Hostname, State, System IP, Reachability, Site ID, Device Model, BFD, Control, Version, Up Since, and Ch.

Hostname	State	System IP	Reachability	Site ID	Device Model	BFD	Control	Version	Up Since	Ch
BR1-VEDGE1	reachable	10.3.0.1	reachable	300	vEdge Cloud	9 (10)	3	17.1.1	12 Aug 2017 2:36:00 AM GMT	52a
BR1-VEDGE2	reachable	10.3.0.2	reachable	300	vEdge Cloud	9 (10)	3	17.1.1	12 Aug 2017 2:36:00 AM GMT	0e1
BR2-VEDGE1	reachable	10.4.0.1	reachable	400	vEdge Cloud	7 (12)	3	17.1.1	12 Aug 2017 2:36:00 AM GMT	ddd
DC1-VEDGE1	reachable	10.1.0.1	reachable	100	vEdge Cloud	9 (10)	3	17.1.1	12 Aug 2017 2:36:00 AM GMT	abd
DC1-VEDGE2	reachable	10.1.0.2	reachable	100	vEdge Cloud	9 (10)	3	17.1.1	12 Aug 2017 2:36:00 AM GMT	121
DC2-VEDGE1	reachable	10.2.0.1	reachable	200	vEdge Cloud	9 (10)	3	17.1.1	12 Aug 2017 2:36:00 AM GMT	9e7
DC2-VEDGE2	reachable	10.2.0.2	reachable	200	vEdge Cloud	9 (10)	3	17.1.1	12 Aug 2017 2:36:00 AM GMT	b82
vbond	reachable	11.11.11.11	reachable	-	vEdge Cloud (vBd...)	-	-	17.1.1	12 Aug 2017 2:36:00 AM GMT	abd
vmanage	reachable	10.10.10.10	reachable	10	vManage	-	0	17.1.1	12 Aug 2017 2:36:00 AM GMT	527
vsmart	reachable	12.12.12.12	reachable	10	vSmart	-	15	17.1.1	12 Aug 2017 2:36:00 AM GMT	10a

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

The screenshot shows the Cisco vManage web interface. The left sidebar has a 'Control Connections' link highlighted with a red box. The main content area displays two network topology diagrams and a table of control connections.

**Network Topologies:**

- vSmart Control Connections:** Shows three nodes: vSmart 2/2, vSmart 1/1, and vManage 1/1. They are interconnected via an 'mpls' node.
- vSmart 2/2:** Shows a connection between vSmart 2/2 and a 'biz-internet' node.

**Control Connections Table:**

Peer Type	Peer System IP	Peer Protocol	Private Port	Public Port	Controller Group ID	Last Update
mpls	--	--	--	--	--	--
vs smart	22.22.22.22	dtls	12446	12446	0	23 Dec 2017 2:29:10 PM HST
vs smart	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	--	--	--	--	--	--
vs smart	22.22.22.22	dtls	12446	12446	0	23 Dec 2017 2:29:10 PM HST
vs smart	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 interface. In the top navigation bar, the path is MONITOR > Network > Troubleshooting > Ping. The device selected is BR2-VEDGE1 (Site ID: 400, Device Model: vedge-cloud). The ping configuration includes Destination IP (198.18.133.21) and VPN (VPN - 10). The source interface is set to ge0/2 - ipv4 - 10.4.254.10. Probes are set to ICMP. The output section displays the results of an Nping session, showing transmitted and received packets, packet loss, round trip times, and a detailed log of ICMP echo requests and replies.

Summary	Output:
Packets Transmitted	<b>5</b>
Packets Received	<b>4</b>
Packet loss (%)	<b>20</b>
Round Trip Time	
Min (ms)	<b>0.032</b>
Max (ms)	<b>0.059</b>
Avg (ms)	<b>0.046</b>

```

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

The screenshot shows the vManage dashboard interface. Key sections include:

- Control Status (Total 8):** Control Up (8), 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:** Categories: < 10 Mbps (17), 10 Mbps - 100 Mbps (0), 100 Mbps - 500 Mbps (0), > 500 Mbps (0).
- vEdge Inventory:** Total (15), Authorized (7), Deployed (7), Staging (0).
- vEdge Health (Total 7):** Normal (7), Warning (0), Error (0).
- Transport Health:** Type: DelLoss, 100% utilization, 0 errors.
- Top Applications:** Legend: League, Application.
- Application-Aware Routing:** Tunnel Endpoints, Avg. Latency (ms), Avg. Loss (%), Avg. Jitter (ms). Examples include BR1-VEDGE1-ge0/0-ge0/1-mpls, BR1-VEDGE1-ge0/1-ge0/0-mpls, DM1-VCDC2mpls-DC2-VEDGE1-mpls, and BR1-VEDGE1-ge0/0-ge0/1-mpls.

## 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.

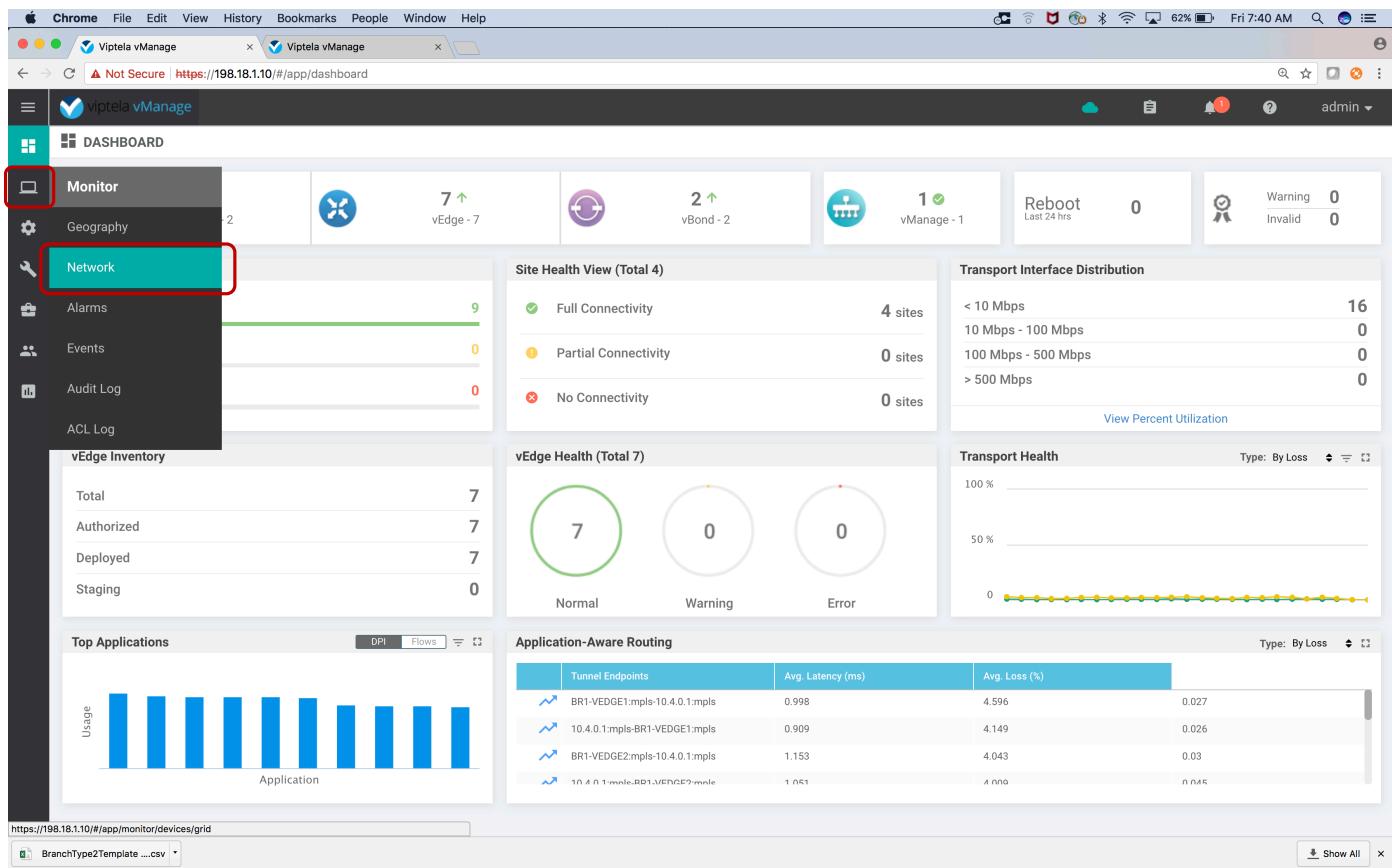
For corporate VPN 10, we will only advertise the Branches' routes to the DCs and not to other Branches. The DCs are advertising default routes and hence when a branch needs to talk to other branches, they will take the default to the DCs. The DC vEdges then route the traffic back to the other remote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



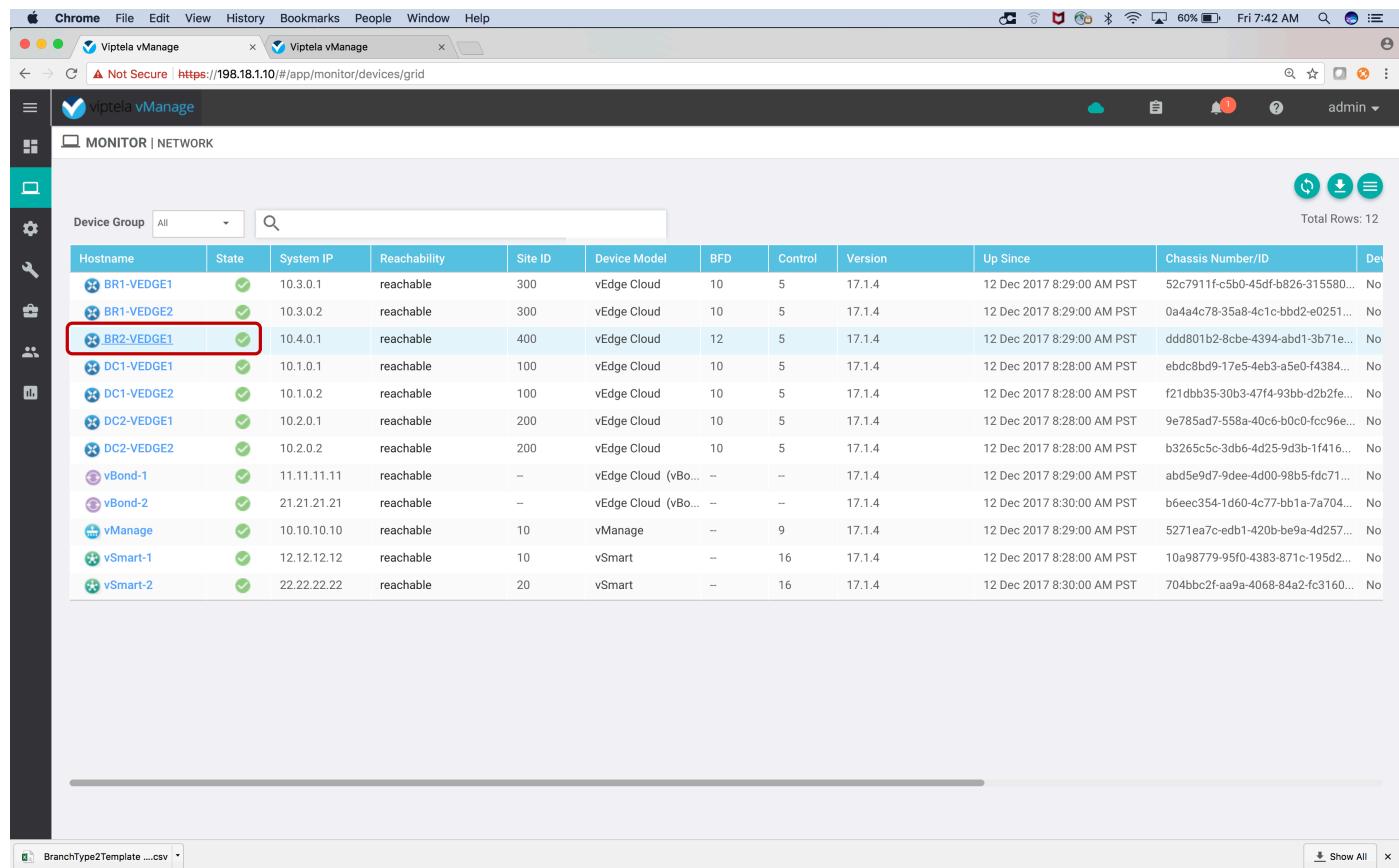
The screenshot shows the Viptela vManage dashboard with the following details:

- Monitor** icon is highlighted with a red box.
- Network** icon is highlighted with a red box.
- Geography**, **Events**, **Audit Log**, and **ACL Log** are also listed in the sidebar.
- vEdge Inventory** section shows:
 

Total	Authorized	Deployed	Staging
7	7	7	0
- Top Applications** section shows a bar chart of application usage.
- Site Health View (Total 4)** section shows:
 

Connectivity Status	Number of Sites
Full Connectivity	4 sites
Partial Connectivity	0 sites
No Connectivity	0 sites
- Transport Interface Distribution** section shows the count of interfaces for different bandwidth ranges.
- vEdge Health (Total 7)** section shows three circular dashboards for Normal (7), Warning (0), and Error (0) states.
- Transport Health** section shows a graph of transport utilization over time.
- Application-Aware Routing** section shows a table of tunnel endpoints with their average latency and loss percentages.

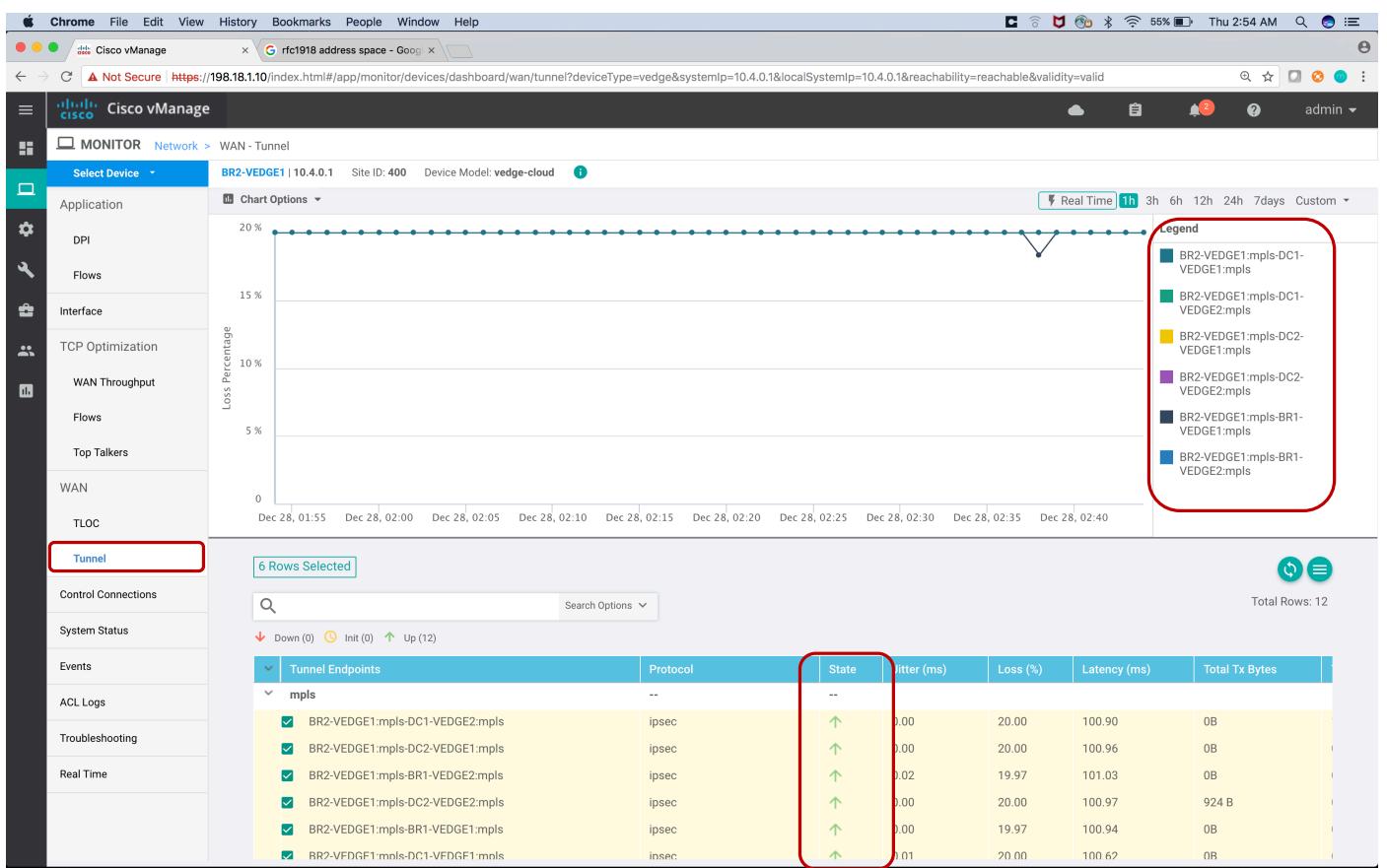
Find BR2-VEDGE1 and click on the name.



Hostname	State	System IP	Reachability	Site ID	Device Model	BFD	Control	Version	Up Since	Chassis Number/ID	Dev
BR1-VEDGE1	reachable	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	reachable	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
<b>BR2-VEDGE1</b>	reachable	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	reachable	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	reachable	10.1.0.2	reachable	100	vEdge Cloud	10	5	17.1.4	12 Dec 2017 8:28:00 AM PST	f21dbb35-30b3-47f4-93bd-d2b2fe...	No
DC2-VEDGE1	reachable	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	reachable	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	reachable	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	reachable	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	reachable	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	reachable	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	reachable	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).



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

Cisco vManage MONITOR Network > Troubleshooting Select Device BR2-EDGE1 | 10.4.0.1 Site ID: 400 Device Model: vedge-cloud

Data Stream' is disabled. Go to Settings page to enable Data Stream to use Debug Logs.

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

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 interface under the MONITOR > Troubleshooting > Traceroute section. The 'Select Device' dropdown is set to 'BR2-VEDGE1 | 10.4.0.1'. The 'Destination IP\*' field contains '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 traceroute command and its execution:

```

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 'Output' section also includes a network diagram showing the path from the source to the destination. The diagram shows a connection between two nodes: '10.4.0.1' and '10.3.0.2'. The link between them is labeled '3.13ms'. From '10.3.0.2', an arrow points to '10.3.0.21' (Branch1), which is labeled '4.27ms'.

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. In the top navigation bar, the URL is 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&uuid=ddd801b2-8cbe-.... The title bar says "Cisco vManage". The main content area is titled "MONITOR Network > Troubleshooting > Traceroute". A dropdown menu "Select Device" is open, with "BR2-EDGE1" highlighted. Below it, a list of devices includes "BR1-EDGE1", "BR2-EDGE2", "DC1-EDGE1", "DC1-EDGE2", "DC2-EDGE1", and "DC2-EDGE2". The "BR1-EDGE1" entry is also highlighted with a red box. To the right, there is a "Traceroute for VPN - 10" section with a "Start" button. A network diagram shows a path from 10.3.0.21 to 10.4.0.21, with a hop labeled "4.27ms".

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 monitoring and troubleshooting. The top navigation bar includes 'Cisco vManage' and 'rfc1918 address space - Google'. The main menu has 'MONITOR' selected under 'Network > Troubleshooting > Traceroute'. A device 'BR1-VEDGE1 | 10.3.0.1' is selected, with 'Site ID: 300' and 'Device Model: vedge-cloud'. The 'VPN' tab is active. The 'Destination IP\*' field contains '10.4.0.10', the 'VPN' dropdown shows 'VPN - 10', and the 'Source/Interface for VPN - 10' dropdown shows 'ge0/3 - ipv4 - 10.3.0.2'. The 'Start' button is highlighted with a red box. The 'Output' section displays the traceroute command and its execution:

```
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 'Output' section also contains a network diagram showing the path from the source interface 'ge0/3 - ipv4 - 10.3.0.2' to the destination '10.4.0.10' through intermediate nodes '10.4.254.10' and '10.4.254.254'. The diagram includes latency values: 2.33ms between the source and the first hop, 4.18ms between the two hops, and 3.93ms between the second hop and the destination.

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

Destination IP\*  
10.4.20.10

VPN  
VPN - 20

Source/Interface for VPN - 20  
ge0/4 - ipv4 - 10.3.20.2

**Start**

**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
```

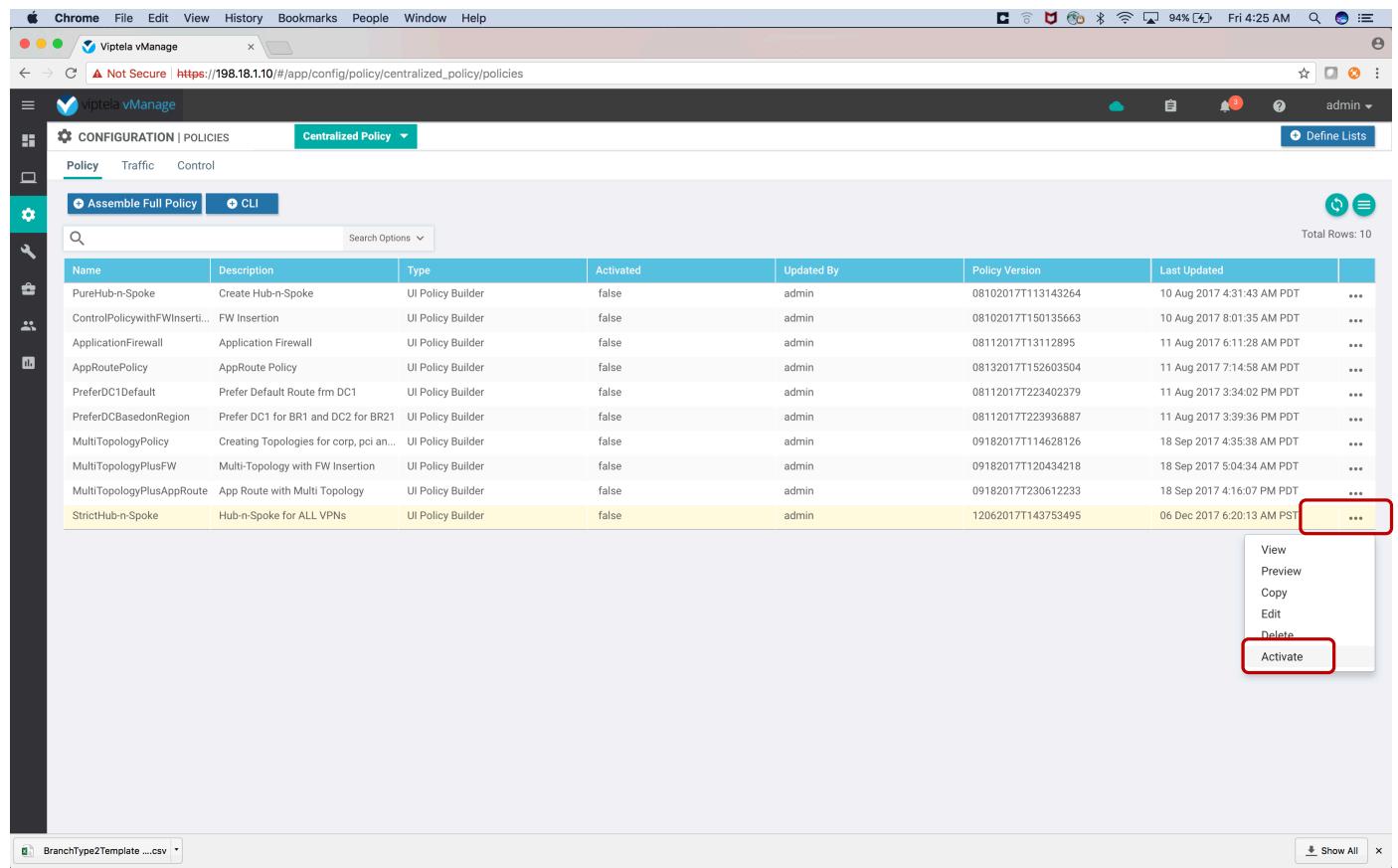
ge0/4 - ipv4 - 10.3.20.2  
2.42ms  
10.4.20.1  
4.36ms  
10.4.20.10

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

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

- Site Health View (Total 4):**
  - Full Connectivity: 4 sites
  - Partial Connectivity: 0 sites
  - No Connectivity: 0 sites
- Transport Interface Distribution:**
  - < 10 Mbps: 17 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:** Shows utilization levels at 100%, 50%, and 0%.
- Application-Aware Routing:** Shows top applications and their usage.

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



Name	Description	Type	Activated	Updated By	Policy Version	Last Updated	Actions
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 3:54:02 PM PDT	...
PreferDCBasedonRegion	Prefer DC1 for BR1 and DC2 for BR21	UI Policy Builder	false	admin	08112017T223936887	11 Aug 2017 3:59:36 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	...
<b>StrictHub-n-Spoke</b>	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 interface with the 'Centralized Policy' tab selected. A modal window 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 modal 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
ControlPolicywithFWInsert...	FW Insertion	UI Policy Builder	false	admin	08102017T150135663
ApplicationFirewall	Application Firewall				08112017T13112895
AppRoutePolicy	AppRoute Policy				08132017T152603504
PreferDC1Default	Prefer Default Route frm DC1				08112017T223402379
PreferDCBasedonRegion	Prefer DC1 for BR1 and DC2 for...				08112017T223936887
MultiTopologyPolicy	Creating Topologies for corp, p...				09182017T114628126
MultiTopologyPlusFW	Multi-Topology with FW Insertion				09182017T120434218
MultiTopologyPlusAppRoute	App Route with Multi Topology				09182017T230612233
StrictHub-n-Spoke	Hub-n-Spoke for ALL VPNs	UI Policy Builder	false	admin	12152017T134720152

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.

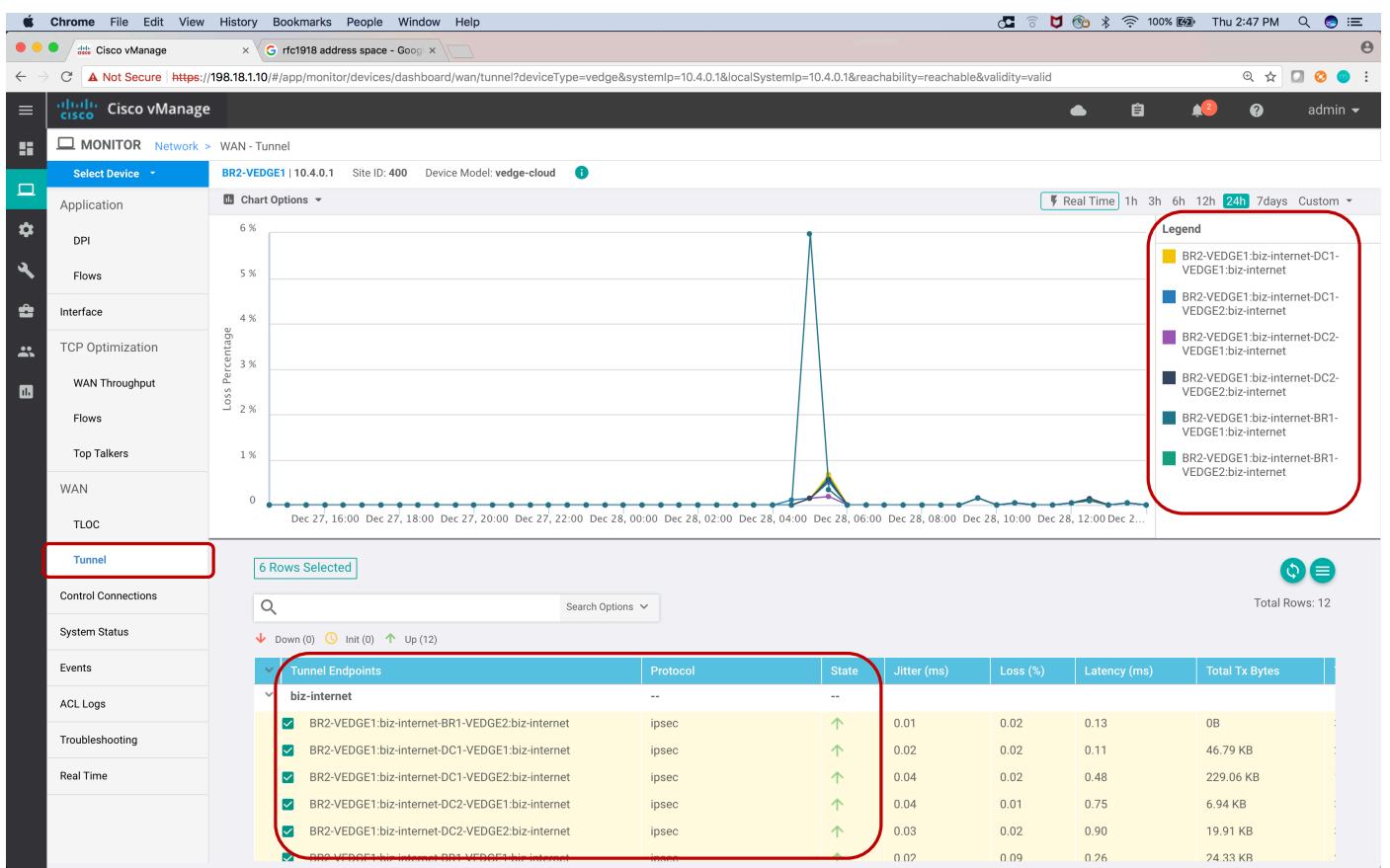
The screenshot shows a browser window for 'Viptela vManage' with the URL [https://198.18.1.10/#/app/device/status?activity=vsmart\\_policy\\_config&pid=vsmart\\_policy\\_config-c0508fb0-3b99-4c90-ab07-4c503554fab7](https://198.18.1.10/#/app/device/status?activity=vsmart_policy_config&pid=vsmart_policy_config-c0508fb0-3b99-4c90-ab07-4c503554fab7). The page displays a 'TASK VIEW' section with a table showing two successful tasks:

Status	Message	Hostname	System IP	Site ID	Site
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

A red box highlights the first row in the table.

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.

The screenshot shows the Cisco vManage interface with the following details:

- Destination IP\***: 10.3.0.21 (highlighted with a red box)
- VPN**: VPN - 10 (highlighted with a red box)
- Source/Interface for VPN - 10**: ge0/2 - ipv4 - 10.4.254.10 (highlighted with a red box)
- Start** button (highlighted with a red box)

**Output** section:

```

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** section:

```

graph LR
    A[ge0/2 - ipv4 - 10.4.254.10] -- "2.53ms" --> B((198.18.133.212))
    B -- "4.40ms" --> C((10.3.0.2))
    C -- "5.71ms" --> D[10.3.0.21]
  
```

The diagram illustrates the traceroute path from the source interface (ge0/2) to the destination IP (10.3.0.21). The first hop is to 198.18.133.212 (198.18.133.212) with a latency of 2.53ms. The second hop is to 10.3.0.2 (10.3.0.2) with a latency of 4.40ms. The final hop is to the destination 10.3.0.21 with a latency of 5.71ms.

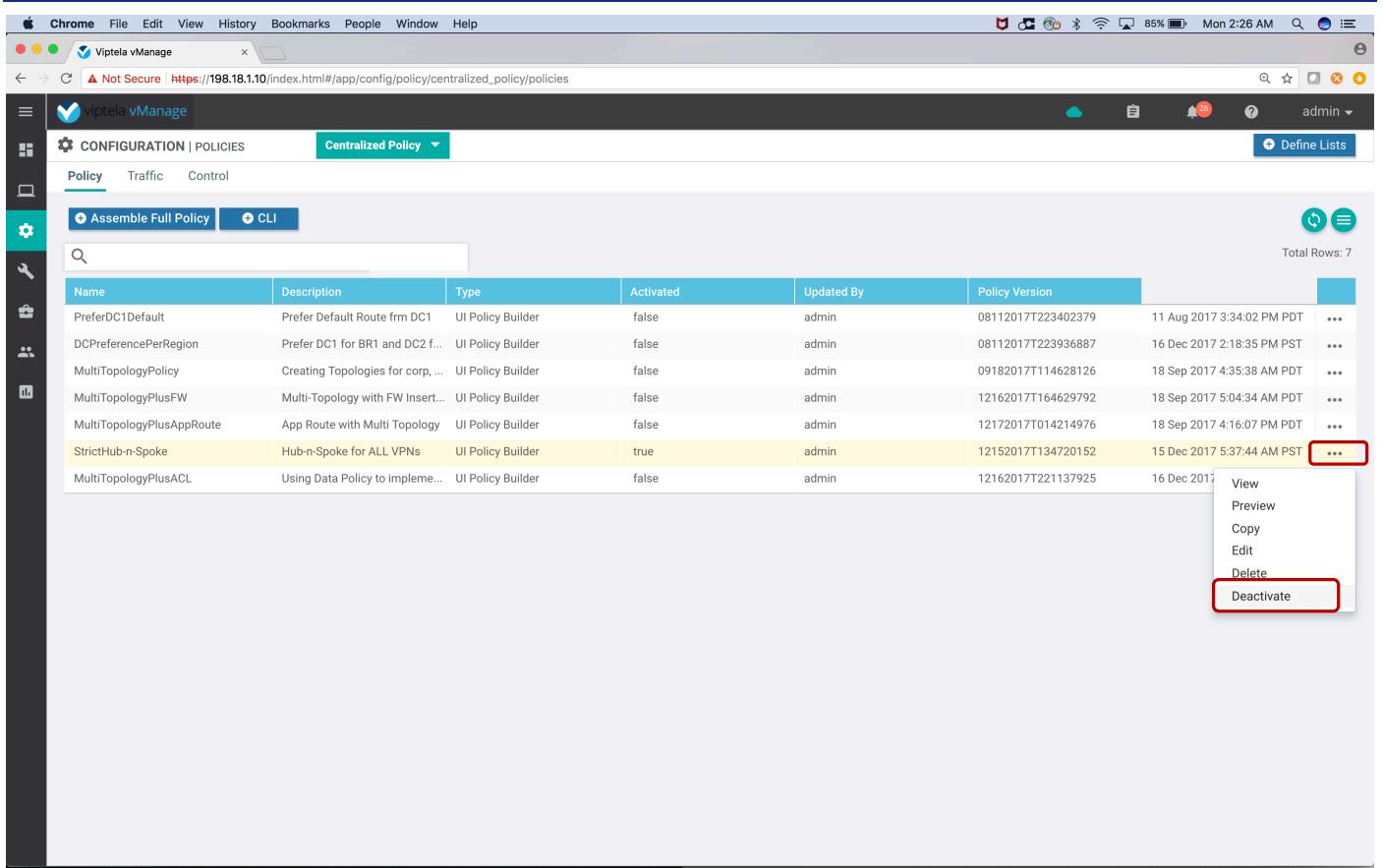
Traceroute from BR2 to BR1 in VPN 20. Use destination IP of 10.3.20.10 in VPN 20.

The screenshot shows the Cisco vManage interface with the following details:

- Header:** Cisco vManage, Not Secure, https://198.18.1.10/#/app/monitor/devices/dashboard/troubleshooting/traceroute?personality=vedge&systemIp=10.4.0.1&localSystemIp=10.4.0.1&deviceType=vedge&uuid=ddd801b2-8cbe-4394-abd..., admin.
- Breadcrumbs:** MONITOR > Troubleshooting > Traceroute
- Form Fields:**
  - Destination IP\*: 10.3.20.10
  - VPN: VPN - 20
  - Source/Interface for VPN - 20: ge0/3 - ipv4 - 10.4.20.1
- Start Button:** A red box highlights the "Start" button at the top right of the form.
- Output Section:**

```
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
```
- Diagram:** A network diagram showing the traceroute path. It starts at 10.3.20.10, goes through 10.1.20.3 (2.69ms), and then 10.3.20.2 (4.63ms). The total round trip time is 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 web interface. The top navigation bar includes links for Chrome, File, Edit, View, History, Bookmarks, People, Window, and Help. The title bar indicates the URL is [Not Secure https://198.18.1.10/index.html#/app/config/policy/centralized\\_policy/policies](https://198.18.1.10/index.html#/app/config/policy/centralized_policy/policies). The main content area is titled "CONFIGURATION | POLICIES" and "Centralized Policy". Below this, there are tabs for Policy, Traffic, and Control, with "Policy" selected. Two buttons are visible: "Assemble Full Policy" and "CLI". A search bar is present above a table. The table has columns: Name, Description, Type, Activated, Updated By, Policy Version, and a timestamp. The table contains 7 rows. A context menu is open over the last row, listing options: View, Preview, Copy, Edit, Delete, and Deactivate. 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

Click on “Deactivate” button.

The screenshot shows the Viptela vManage web interface. The main page displays a table of policies under the 'Centralized Policy' tab. One policy, 'StrictHub-n-Spoke', is selected and highlighted in yellow. A modal dialog box titled 'Deactivate Policy' is overlaid on the page. The dialog contains the message: 'Policy will be removed from the following vSmart. 12.12.12.12, 22.22.22.22'. Below this, a question is posed: '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	Date	Action
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 Inte...				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 VPNs				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.

The screenshot shows a web browser window for 'Viptela vManage' with the URL [https://198.18.1.10/index.html#/app/device/status?activity=vsmart\\_policy\\_config&pid=vsmart\\_policy\\_config-457bf2e5-330a-4aeb-839b-e5f3a1c855ad](https://198.18.1.10/index.html#/app/device/status?activity=vsmart_policy_config&pid=vsmart_policy_config-457bf2e5-330a-4aeb-839b-e5f3a1c855ad). The page displays a 'TASK VIEW' section for 'Push vSmart Policy'. It shows two successful tasks: 'Done Removing policy to vsmart.' for vSmart-1 and vSmart-2. The 'Status' column for these tasks is highlighted with a red box.

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-VEDGE1 and Click on “Real Time” tab. In the dialogue box, search for “ip routes”. Select the “IP Routes” from pull down menu.

The screenshot shows the Cisco vManage web interface. The left sidebar has a 'Real Time' tab highlighted with a red box. The main content area shows a 'Device Options' dropdown with 'ip routes' typed in, and 'IP Routes' is highlighted with a red box. Below the dropdown is a search bar and a 'Search Options' button. At the bottom of the page, it says 'No data available' and 'Total Rows: 0'.

On the next pop-up select “Show Filters”.

The screenshot shows the Cisco vManage interface in a web browser. The title bar indicates the URL is [Not Secure https://198.18.1.10/index.html#/app/monitor/devices/dashboard/details?systemIp=10.4.0.1&localSystemIp=10.4.0.1&option=IP%20Routes](https://198.18.1.10/index.html#/app/monitor/devices/dashboard/details?systemIp=10.4.0.1&localSystemIp=10.4.0.1&option=IP%20Routes). The top navigation bar includes links for Chrome, File, Edit, View, History, Bookmarks, People, Window, and Help. The system status bar at the top right shows battery level at 56%, signal strength, and the date and time as Mon 1:35 AM.

The main interface is titled "Cisco vManage" and has a "MONITOR Network > Real Time" section. On the left, a sidebar menu 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, and Real Time. The "Real Time" option is currently selected.

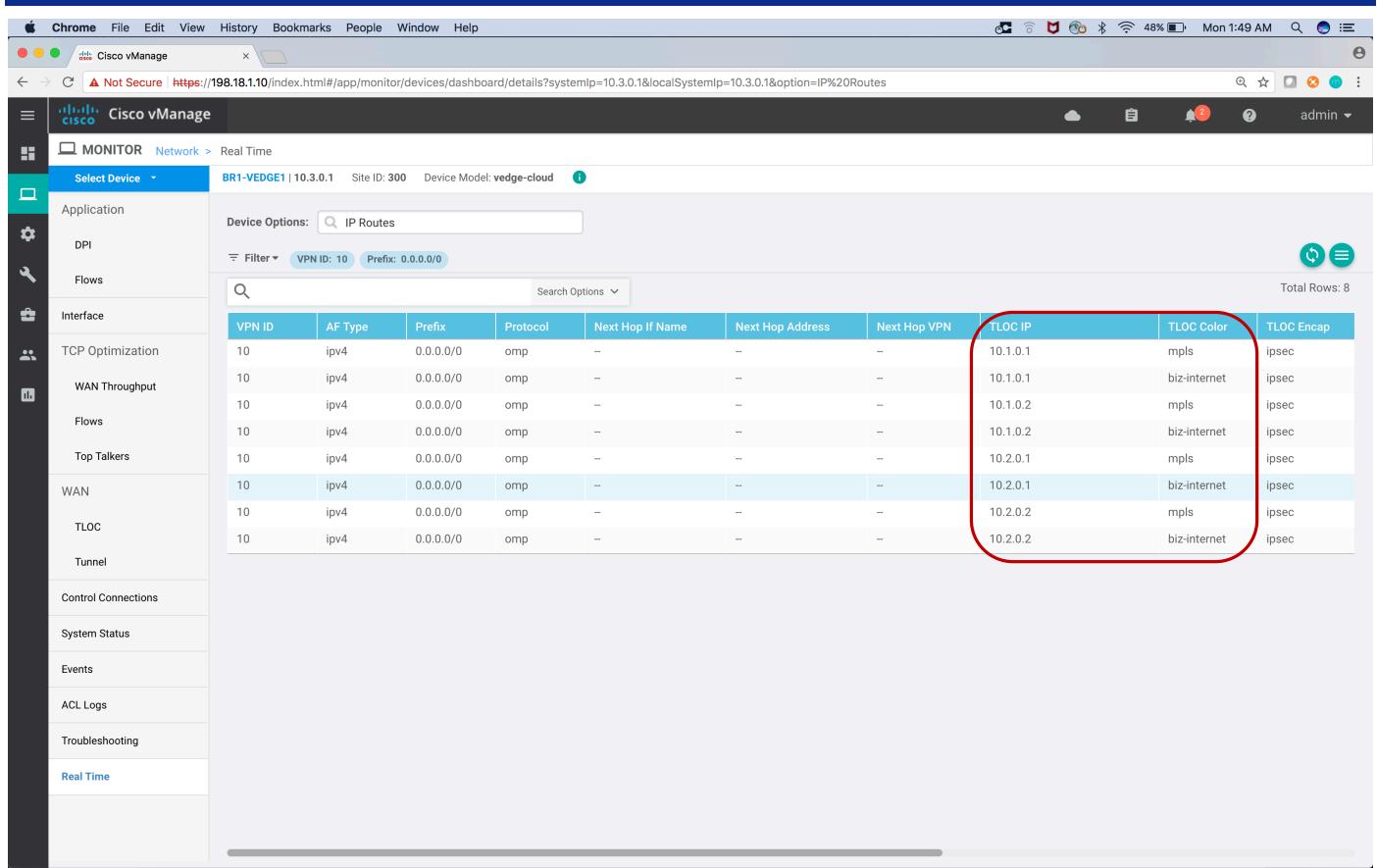
In the center, under the "Real Time" section, there is a "Device Options" search bar with the placeholder "IP Routes" and a "Filter" button. A modal dialog box titled "Select Filter" is displayed in the foreground, containing the instruction "Choose filters to display data faster." and two buttons: "Show Filters" (highlighted with a red border) and "Do Not Filter".

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

The screenshot shows the Cisco vManage interface in a web browser. The top navigation bar includes links for Chrome, File, Edit, View, History, Bookmarks, People, Window, and Help. A message bar at the top right indicates "Not Secure" and the URL "https://198.18.1.10/index.html#/app/monitor/devices/dashboard/details?systemIp=10.4.0.1&localSystemIp=10.4.0.1&option=IP%20Routes". The main header "Cisco vManage" has a "Real Time" dropdown. The left sidebar lists various monitoring categories 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 "Real Time" category is currently selected. The main content area displays a table of IP routes for device "BR2-VEDGE1" (Site ID: 400, Device Model: wedge-cloud). The table has columns: Next Hop Address, Next Hop VPN, TLOC IP, TLOC Color, and TLOC Encap. A modal dialog box is overlaid on the table, showing filters for "VPN ID: 10" and "Prefix: 0.0.0.0". The "Search" button in the dialog is highlighted with a red box.

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

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

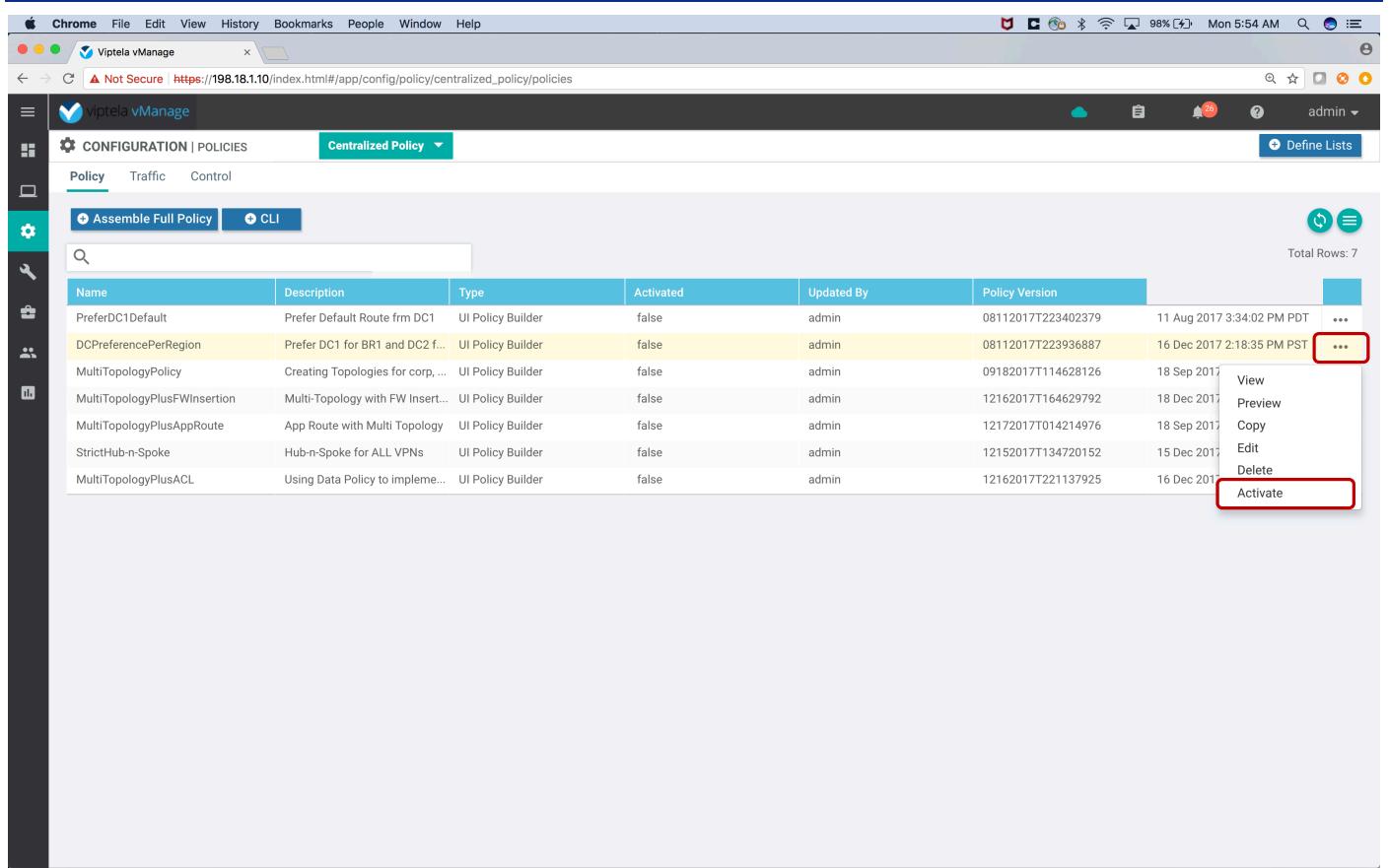


The screenshot shows the Cisco vManage interface for device BR1-VEDGE1. The left sidebar lists various monitoring categories. The main pane displays 'IP Routes' for VPN ID 10. A red circle highlights the last row of the table, which corresponds to the configuration shown in the previous slide.

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”.

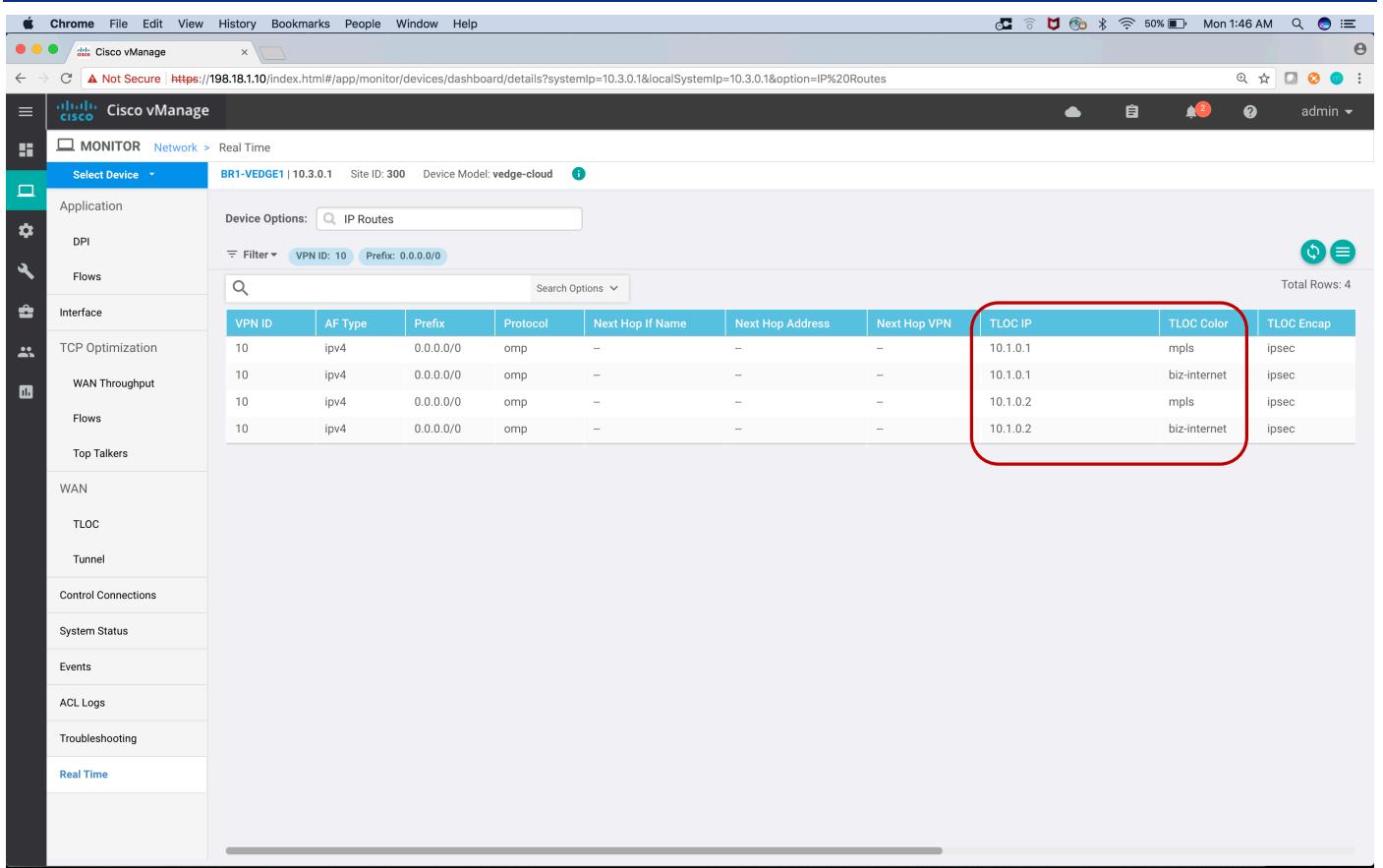


The screenshot shows the Viptela vManage web interface. The top navigation bar includes links for Chrome, File, Edit, View, History, Bookmarks, People, Window, Help, and a status bar showing 98% battery, Mon 5:54 AM, and a search bar. The main title is "Viptela vManage". The left sidebar has icons for Home, Configuration, Policies, Traffic, Control, and Help.

The central 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 Modified. The last column includes actions: View, Preview, Copy, Edit, Delete, and Activate. The "Activate" button for the "MultiTopologyPlusACL" policy is highlighted with a red box.

Name	Description	Type	Activated	Updated By	Policy Version	Last Modified	Action
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	<a href="#">View</a>
MultiTopologyPlusFWInsertion	Multi-Topology with FW Insert...	UI Policy Builder	false	admin	12162017T164629792	18 Dec 2017	<a href="#">Preview</a>
MultiTopologyPlusAppRoute	App Route with Multi Topology	UI Policy Builder	false	admin	12172017T014214976	18 Sep 2017	<a href="#">Copy</a>
StrictHub-n-Spoke	Hub-n-Spoke for ALL VPNs	UI Policy Builder	false	admin	12152017T134720152	15 Dec 2017	<a href="#">Edit</a>
MultiTopologyPlusACL	Using Data Policy to impleme...	UI Policy Builder	false	admin	12162017T221137925	16 Dec 2017	<a href="#">Delete</a>
							<a href="#">Activate</a>

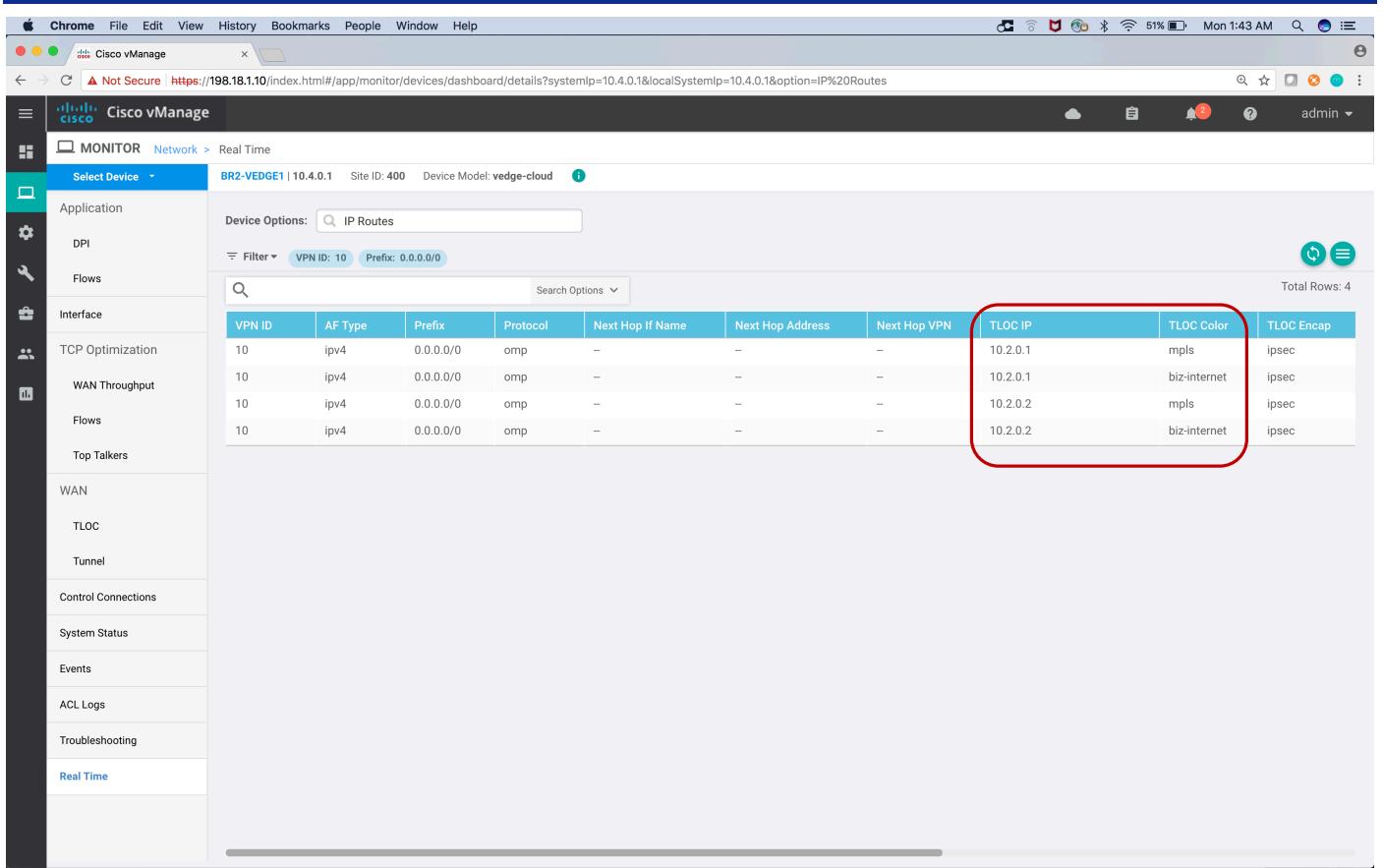
Once the policy has been successfully being pushed to the vSmarts, go to the Device dashboard for BR1-VEGDE1 and get the default route in VPN 10. You will see the route installed is pointing to DC1 as the preferred path.



The screenshot shows the Cisco vManage interface for device BR1-VEDGE1. The left sidebar lists various monitoring categories like Application, DPI, Flows, and Interface. The main pane displays 'IP Routes' for VPN ID 10, with a total of 4 rows. The table columns are: VPN ID, AF Type, Prefix, Protocol, Next Hop If Name, Next Hop Address, Next Hop VPN, TLOC IP, TLOC Color, and TLOC Encap. The TLOC IP column is 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	--	--	--	10.1.0.1	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 device BR2-EDGE1. The left sidebar has 'Real Time' selected under 'MONITOR'. The main area displays a table of IP Routes. A red box highlights the last four rows of the table, which correspond to the entries in the following table:

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.

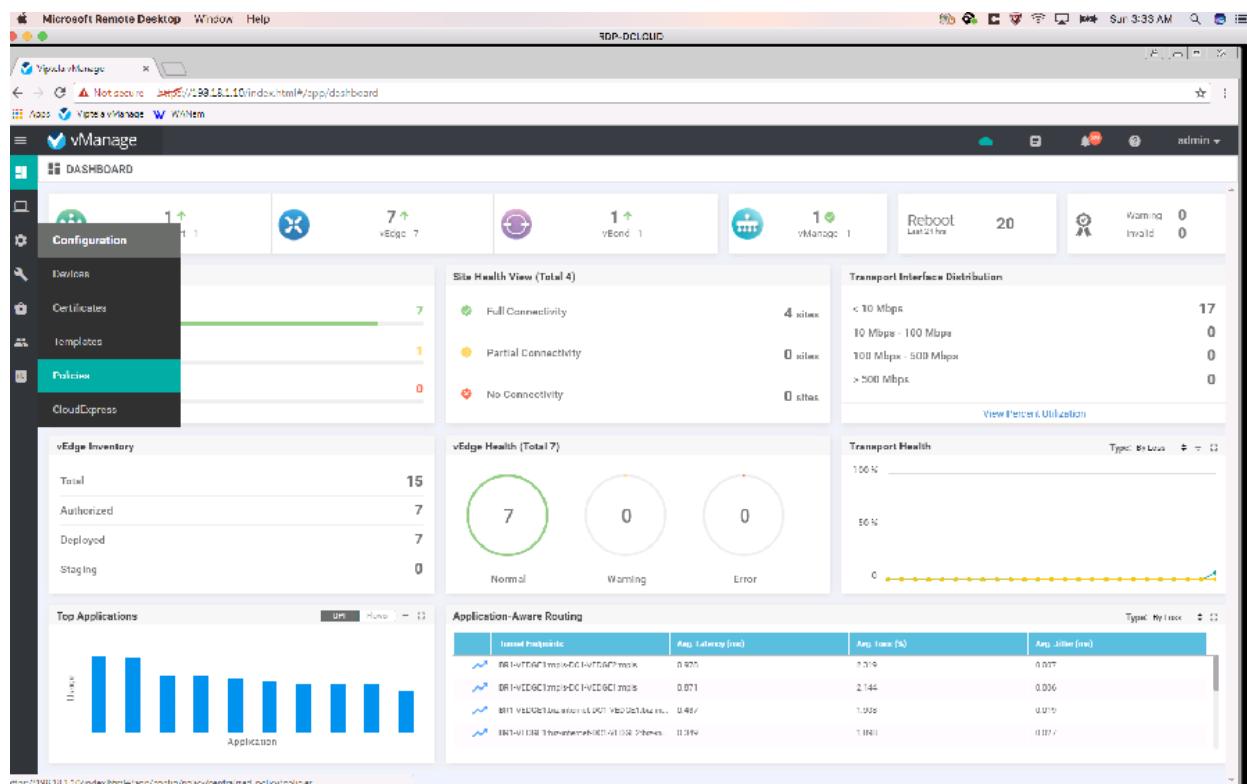
## Lab 04 - Service (FW) Insertion

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.

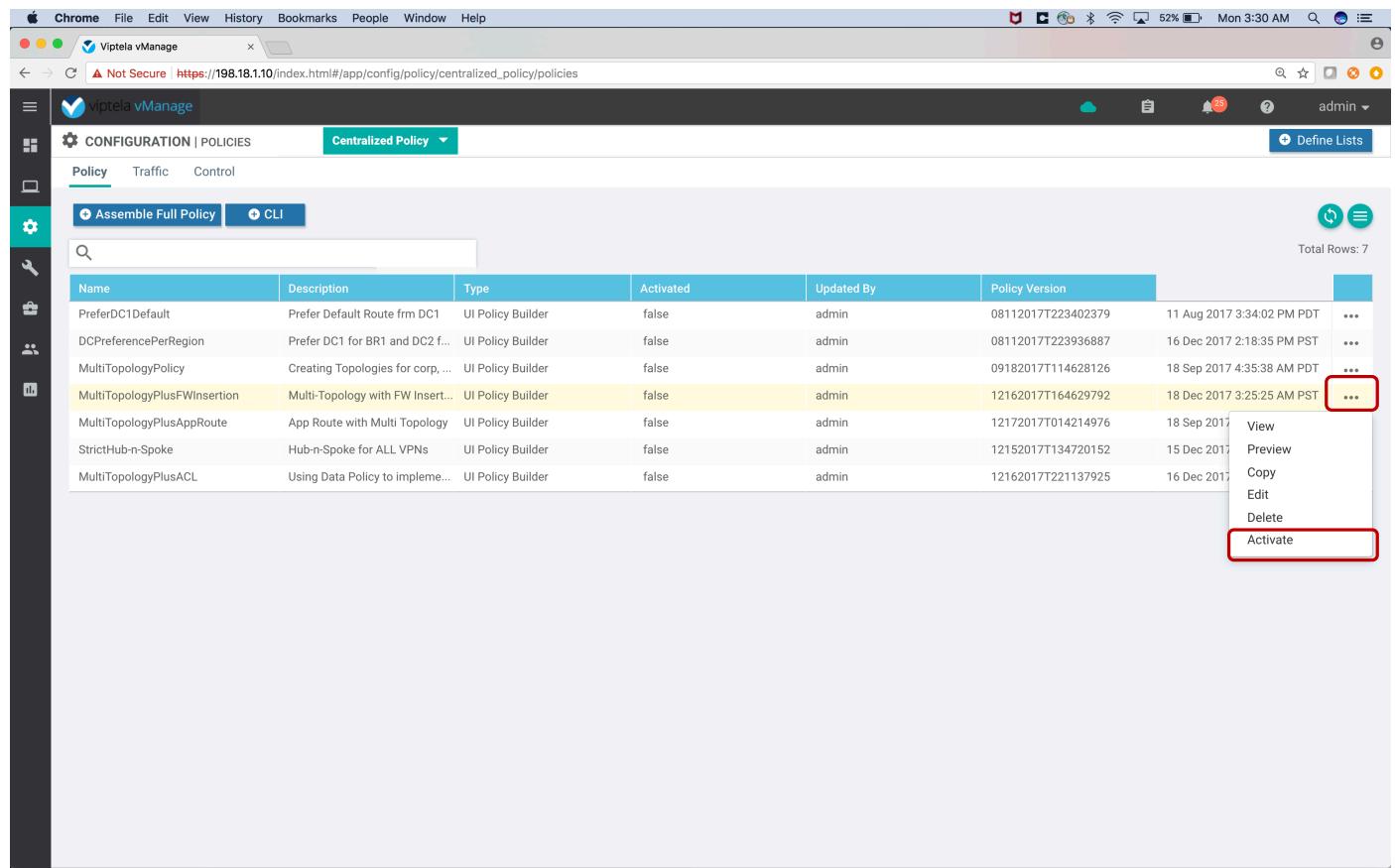
Using Cisco SD-WAN, services can be deployed anywhere in the network and based on policies redirect flows/site-traffic through those services.

### Steps

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



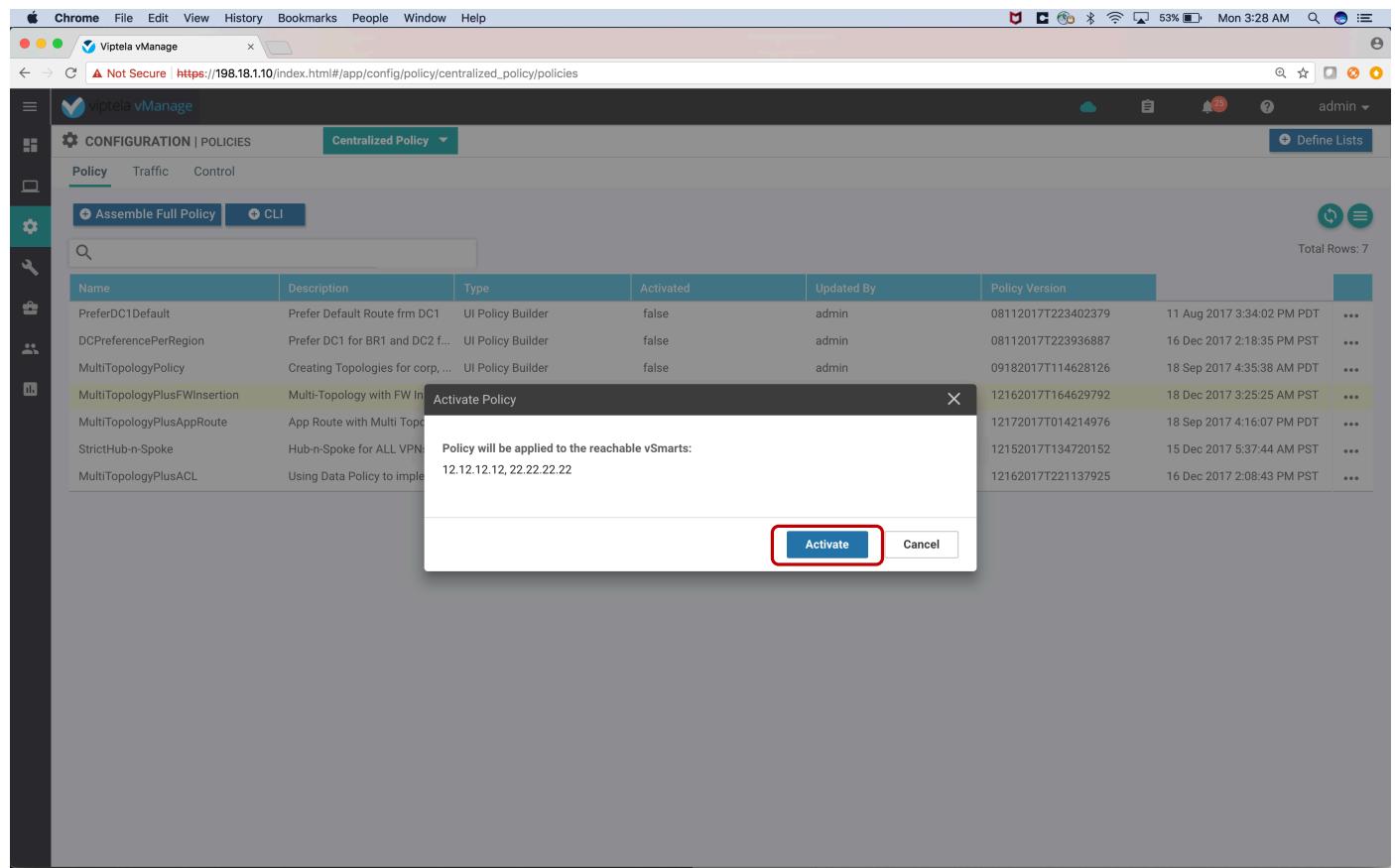
Activate the policy named “MultiTopologyPlusFWInsertion”.



The screenshot shows the Viptela vManage web interface with the URL [https://198.18.1.10/index.html#/app/config/policy/centralized\\_policy/policies](https://198.18.1.10/index.html#/app/config/policy/centralized_policy/policies). The page displays a list of policies under the 'Centralized Policy' tab. The 'Policy' tab is selected. A search bar is present at the top. The table has columns: Name, Description, Type, Activated, Updated By, Policy Version, and Actions. The 'Actions' column includes options like '...', 'View', 'Preview', 'Copy', 'Edit', 'Delete', and 'Activate'. The 'MultiTopologyPlusFWInsertion' policy is highlighted with a yellow background and a red box surrounds its '...' menu option. A second red box highlights the 'Activate' button in the 'Actions' column for this row.

Name	Description	Type	Activated	Updated By	Policy Version	Actions
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 View
StrictHub-n-Spoke	Hub-n-Spoke for ALL VPNs	UI Policy Builder	false	admin	12152017T134720152	15 Dec 2017 Preview
MultiTopologyPlusACL	Using Data Policy to impleme...	UI Policy Builder	false	admin	12162017T221137925	16 Dec 2017 Copy Edit Delete

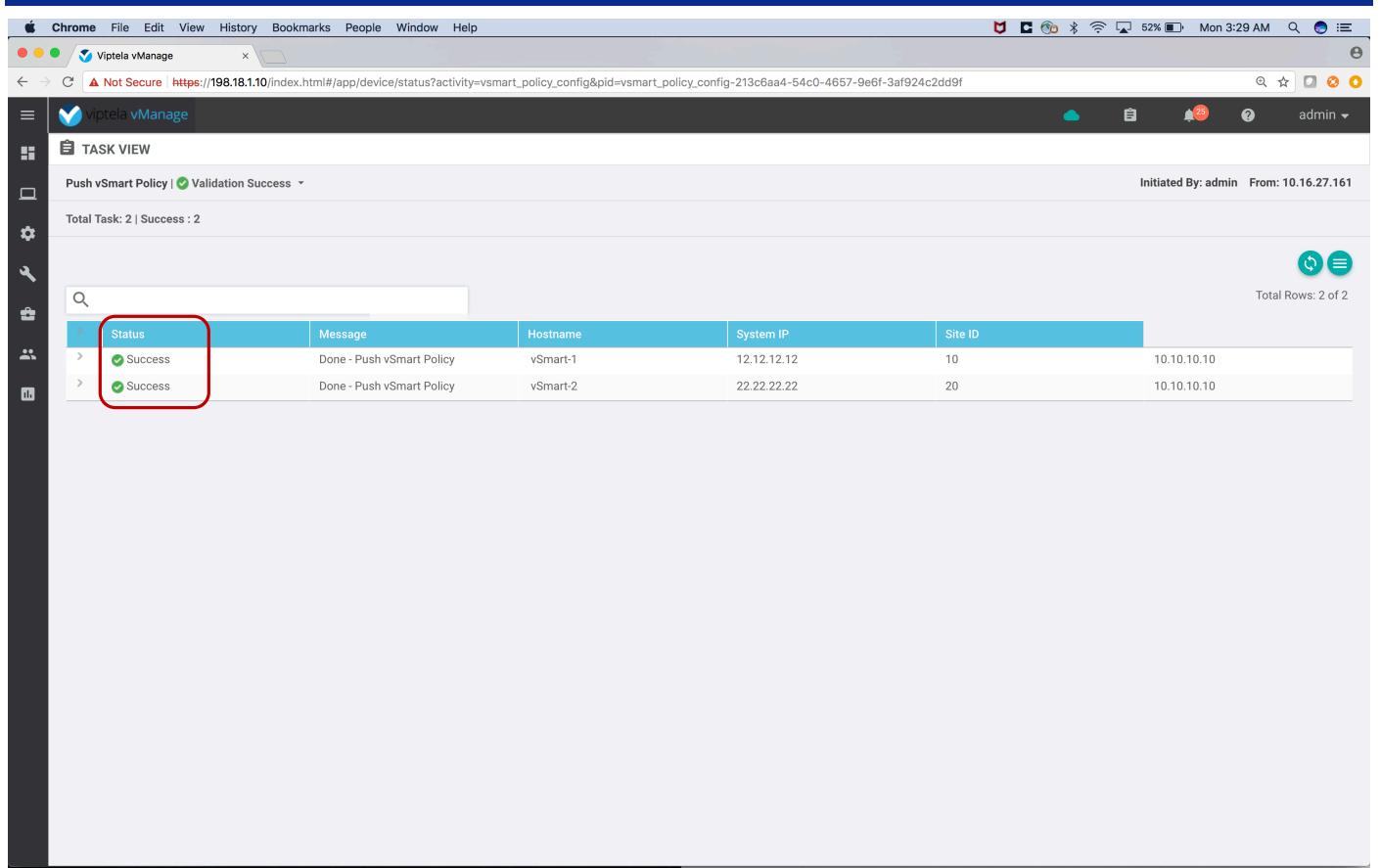
Click on “Activate” button.



The screenshot shows the Viptela vManage web interface. The main page displays a table of policies, with one row selected. A modal dialog box titled "Activate Policy" is overlaid on the page. The dialog contains the message "Policy will be applied to the reachable vSmarts:" followed by the IP addresses "12.12.12.12, 22.22.22.22". At the bottom of the dialog are two buttons: "Activate" (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
DCPreferencePerRegion	Prefer DC1 for BR1 and DC2 f...	UI Policy Builder	false	admin	08112017T223936887
MultiTopologyPolicy	Creating Topologies for corp, ...	UI Policy Builder	false	admin	09182017T114628126
MultiTopologyPlusFWInsertion	Multi-Topology with FW Insertion	Activate Policy			12162017T164629792
MultiTopologyPlusAppRoute	App Route with Multi Topology				12172017T014214976
StrictHub-n-Spoke	Hub-n-Spoke for ALL VPNs				12152017T134720152
MultiTopologyPlusACL	Using Data Policy to implement				12162017T221137925

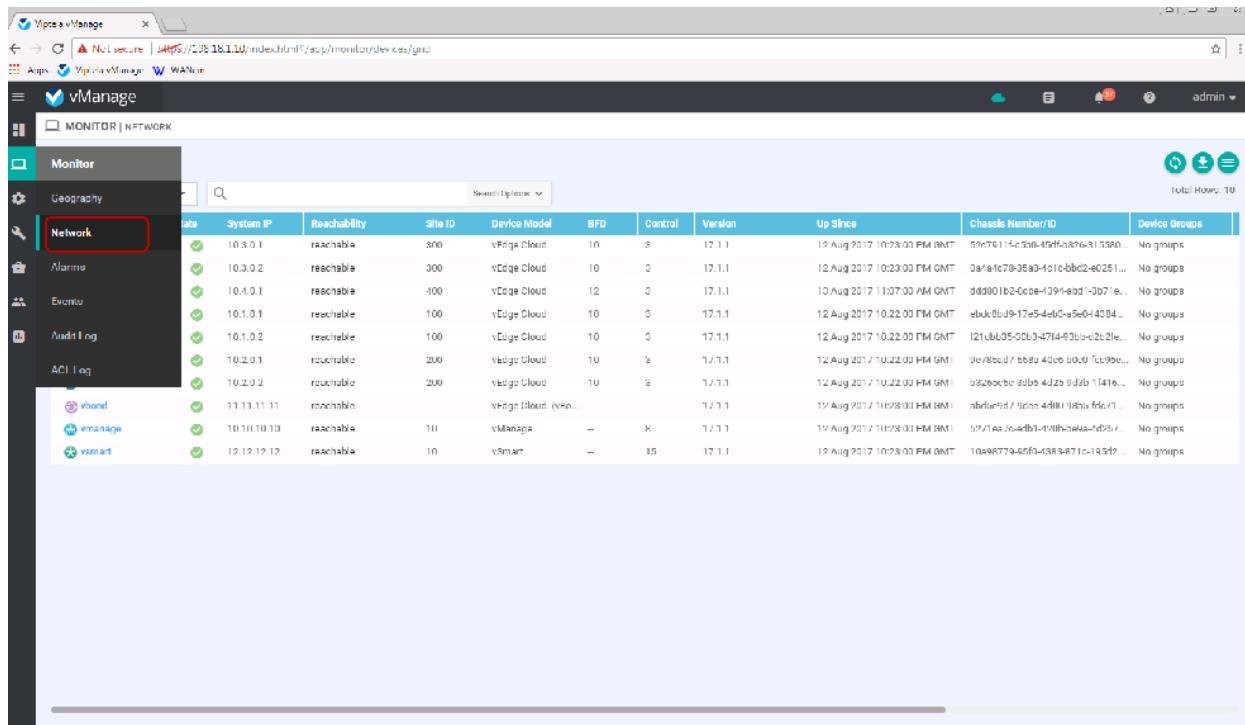
Wait till the policy is successfully pushed to the vSmarts.



The screenshot shows the Viptela vManage interface with a task view titled "Push vSmart Policy | Validation Success". It displays two successful tasks: "Done - Push vSmart Policy" for vSmart-1 and vSmart-2. The "Status" column is highlighted with a red box.

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

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



The screenshot shows the Viptela vManage interface with the "Monitor" tab selected. Under the "Network" section, a table lists various devices. The "Network" tab is highlighted with a red box.

Name	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 10:28:00 PM GMT	59c7e114c59a-45f0-1026-811580...	No groups
10.3.0.2	reachable	300	vEdge Cloud	10	3	17.1.1		12 Aug 2017 10:23:00 PM GMT	0aef1c79-35a0-401c-bbc2-e0251...	No groups
10.4.0.1	reachable	400	vEdge Cloud	12	3	17.1.1		13 Aug 2017 11:07:00 AM GMT	dd9801b2-0cc8-4391-e0d1-3b71e...	No groups
10.1.0.1	reachable	100	vEdge Cloud	10	3	17.1.1		12 Aug 2017 10:22:00 PM GMT	e6bcb019-17e5-46c0-a5e0-43584...	No groups
10.1.0.2	reachable	100	vEdge Cloud	10	3	17.1.1		12 Aug 2017 10:22:00 PM GMT	d21ab1b5-50b3-47f4-93b0-c212e...	No groups
10.2.0.1	reachable	200	vEdge Cloud	10	3	17.1.1		12 Aug 2017 10:22:00 PM GMT	9e18ec77-bbb8-42ce-0000-7c99e...	No groups
10.2.0.2	reachable	200	vEdge Cloud	10	3	17.1.1		12 Aug 2017 10:22:00 PM GMT	b268e6bc-dabb-442b-9d3b-14161...	No groups
11.11.11.11	reachable	vManage	vManage	—	3	17.1.1		12 Aug 2017 11:29:01 PM GMT	a8f45ed7-9e05-4d00-98b1-fde71...	No groups
10.10.10.10	reachable	10	vSmart	—	15	17.1.1		12 Aug 2017 10:28:01 PM GMT	597aee7c-acdb-49fb-9a6a-4d5b7...	No groups
12.12.12.12	reachable	10	vSmart	—	15	17.1.1		12 Aug 2017 10:28:00 PM GMT	10a96772-45f0-1383-871c-1a95d...	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 under the MONITOR tab. In the left sidebar, the Troubleshooting option is highlighted with a red box. The main panel displays the Connectivity Tools - Traceroute configuration. 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 - 10.4.254.0. The Traceroute button is selected. Below the configuration, the Output section shows the traceroute command and its execution results. A network diagram on the right illustrates the path from the source to the destination, with each hop labeled with its IP address and latency values.

```

traceroute -m 15 -w 1 > 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

```

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

The screenshot shows the Viptela vManage interface under the MONITOR tab. In the Connectivity Tools section, the Traceroute option is selected. The destination IP is set to 10.4.0.21, the VPN is set to VPN - 10, and the source/interface is set to ge0/3 - ipv4 - 10.3.0.2. The Start button is highlighted with a red box. The Troubleshooting link in the left sidebar is also highlighted with a red box.

**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

```

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.

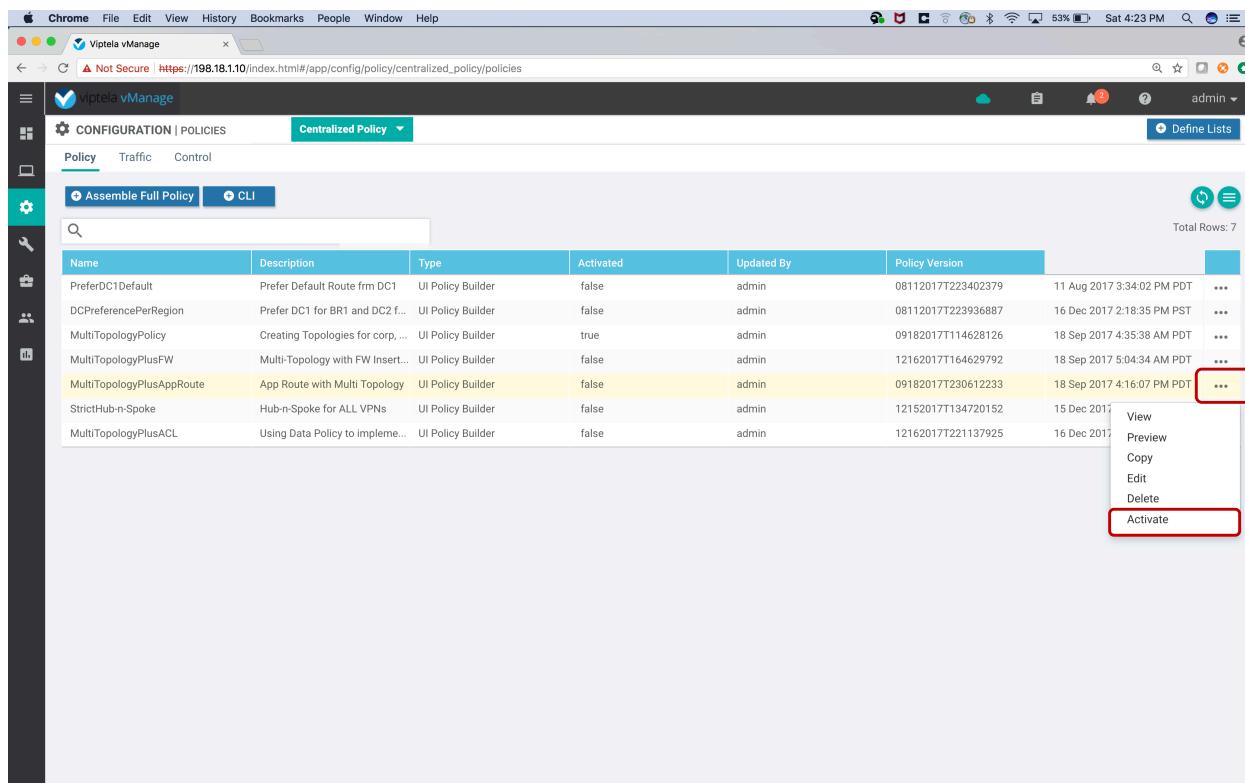
In this demonstration, some of the applications have SLAs defined and are pinned to the MPLS (interface ge0/0 on BR2-VEDGE1). Some applications are pinned to the internet transport (interface ge0/1 on BR2-VEDGE1).

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”.



Name	Description	Type	Activated	Updated By	Policy Version	Date	Action Buttons
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	true	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	09182017T230612233	18 Sep 2017 4:16:07 PM PDT	...
StrictHub-n-Spoke	Hub-n-Spoke for ALL VPNs	UI Policy Builder	false	admin	12152017T134720152	15 Dec 2017	<span style="border: 1px solid #ccc; padding: 2px;">View</span>
MultiTopologyPlusACL	Using Data Policy to impleme...	UI Policy Builder	false	admin	12162017T221137925	16 Dec 2017	<span style="border: 1px solid #ccc; padding: 2px;">Preview</span>

Click on the “Activate” button.

The screenshot shows the 'Centralized Policy' configuration page in the Viptela vManage interface. A modal dialog box is overlaid on the page, prompting the user to activate a policy. The dialog contains the message: 'Policy will be applied to the reachable vSmarts: 12.12.12.12, 22.22.22.22'. At the bottom of the dialog are two buttons: 'Activate' (highlighted with a red box) and 'Cancel'.

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

The screenshot shows the 'Task View' page in the Viptela vManage interface. It displays the results of a task to push vSmart Policy. The table has columns: Status, Message, Hostname, System IP, and Site ID. There are two rows, both of which show a green checkmark icon and the status 'Success'. The 'Status' column is highlighted with a red box. The table shows a total of 2 tasks initiated by admin from 10.16.45.97.

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

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.

	Domain ID	Device groups	Vbond	Timezone	Latitude	Longitude
1	["No groups"]	vbond.cisco.com	UTC	32.79	-96.77	16 Dec 2017 3:53...

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.

Screenshot of Cisco vManage interface showing App Routes Statistics for device BR2-VEDGE. The search bar contains "biz-internet". A red circle highlights the search bar and the results table.

**Device Options:** App Routes Statistics

**Search Results:**

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	0,1,2,3,4	1	5
12346	10.3.0.1	biz-internet	biz-internet	0	0	0	0,1,2,3,4	2	5
12346	10.3.0.1	biz-internet	biz-internet	0	0	0	0,1,2,3,4	3	5
12346	10.3.0.1	biz-internet	biz-internet	0	0	0	0,1,2,3,4	4	5
12346	10.3.0.1	biz-internet	biz-internet	0	0	0	0,1,2,3,4	5	5
65368	10.3.0.2	biz-internet	biz-internet	0	0	0	0,1,2,3,4	0	5
65368	10.3.0.2	biz-internet	biz-internet	0	0	0	0,1,2,3,4	1	5
65368	10.3.0.2	biz-internet	biz-internet	0	0	0	0,1,2,3,4	2	5
65368	10.3.0.2	biz-internet	biz-internet	0	0	0	0,1,2,3,4	3	5
65368	10.3.0.2	biz-internet	biz-internet	0	0	0	0,1,2,3,4	4	5
12346	10.1.0.1	biz-internet	biz-internet	0	0	0	0,1,2,3,4	0	5
12346	10.1.0.1	biz-internet	biz-internet	0	0	0	0,1,2,3,4	1	5
12346	10.1.0.1	biz-internet	biz-internet	0	0	0	0,1,2,3,4	2	5
12346	10.1.0.1	biz-internet	biz-internet	0	0	0	0,1,2,3,4	3	5
12346	10.1.0.1	biz-internet	biz-internet	0	0	0	0,1,2,3,4	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.

Screenshot of Cisco vManage interface showing App Routes Statistics for device BR2-VEDGE. The search bar contains "mpls". A red circle highlights the search bar and the results table.

**Device Options:** App Routes Statistics

**Search Results:**

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	0,1,2,3,4	1	5
12366	10.3.0.2	mpls	mpls	0	1	0	0,1,2,3,4	2	5
12366	10.3.0.2	mpls	mpls	0	1	0	0,1,2,3,4	3	5
12366	10.3.0.2	mpls	mpls	0	1	0	0,1,2,3,4	4	5
12366	10.3.0.2	mpls	mpls	0	1	0	0,1,2,3,4	5	5
12346	10.3.0.1	mpls	mpls	0	0	0	0,1,2,3,4	0	5
12346	10.3.0.1	mpls	mpls	0	0	0	0,1,2,3,4	1	5
12346	10.3.0.1	mpls	mpls	0	0	0	0,1,2,3,4	2	5
12346	10.3.0.1	mpls	mpls	0	0	0	0,1,2,3,4	3	5
12346	10.3.0.1	mpls	mpls	0	0	0	0,1,2,3,4	4	5
12346	10.3.0.1	mpls	mpls	0	0	0	0,1,2,3,4	5	5
12346	10.1.0.1	mpls	mpls	0	0	0	0,1,2,3,4	0	5
12346	10.1.0.1	mpls	mpls	0	0	0	0,1,2,3,4	1	5
12346	10.1.0.1	mpls	mpls	0	0	0	0,1,2,3,4	2	5
12346	10.1.0.1	mpls	mpls	0	0	0	0,1,2,3,4	3	5
12346	10.1.0.1	mpls	mpls	0	0	0	0,1,2,3,4	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 used for the defined flow based on policies and transport performance measurements.

The screenshot shows the Cisco vManage interface with the following details:

- Header:** Chrome browser window, Not Secure, 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..., admin user.
- Left Sidebar:** MONITOR > Troubleshooting. Sub-options include Application, DPI, Flows, Interface, TCP Optimization, WAN Throughput, Flows, Top Talkers, WAN, TLOC, Tunnel, Control Connections, System Status, Events, ACL Logs, and Troubleshooting (which is highlighted with a red box).
- Central Content:**
  - Connectivity:** Shows a green hexagonal icon with a network graph.
  - Traffic:** Shows an orange hexagonal icon with a double-headed arrow.
  - Device Bringup:** Control Connections(Live View)
  - Ping:**
  - Trace Route:**
  - Tunnel Health:**
  - App Route Visualization:**
  - Simulate Flows:** A red box highlights this button.

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.

The screenshot shows the Cisco vManage interface with the following details:

- 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
- Protocol\***: 1
- Source Port**: (empty)
- Destination Port**: (empty)
- DSCP**: 46
- Path**: Tunnel (radio button selected)
- Advanced Options** (dropdown menu open)
- Output:** A network diagram showing traffic from a laptop icon to a switch icon labeled "10.4.0.1". The switch then connects to a box labeled "→ mpls" and "← mpls". To the right of the switch is a box labeled "Remote System IP Encapsulation" and "10.3.0.1 IPSec".
- Buttons:** Troubleshooting, Simulate (highlighted with a red box).

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.

The screenshot shows the WANem interface with several configuration sections for different interfaces:

- Interface: eth4**: Bandwidth(BW) dropdown is set to "Choose BW", Other, and "Specify BW(Kbps)" is 0. Delay is 0.
- Interface: eth3**: Bandwidth(BW) dropdown is set to "Choose BW", Other, and "Specify BW(Kbps)" is 0. Delay is 0.
- Interface: eth2**: Bandwidth(BW) dropdown is set to "Choose BW", Other, and "Specify BW(Kbps)" is 0. Delay is 100 ms. This row has a red box around the "Delay" section and another red box around the "Delay time(ms)" input field.
- Interface: eth1**: Bandwidth(BW) dropdown is set to "Choose BW", Other, and "Specify BW(Kbps)" is 0. Delay is 0.
- Interface: eth0**: Bandwidth(BW) dropdown is set to "Choose BW", Other, and "Specify BW(Kbps)" is 0. Delay is 0.

At the bottom, there are buttons for "Apply settings", "Reset settings", "Refresh settings", and a checkbox for "Display commands only, do not execute them". A "Check current status" button is also present.

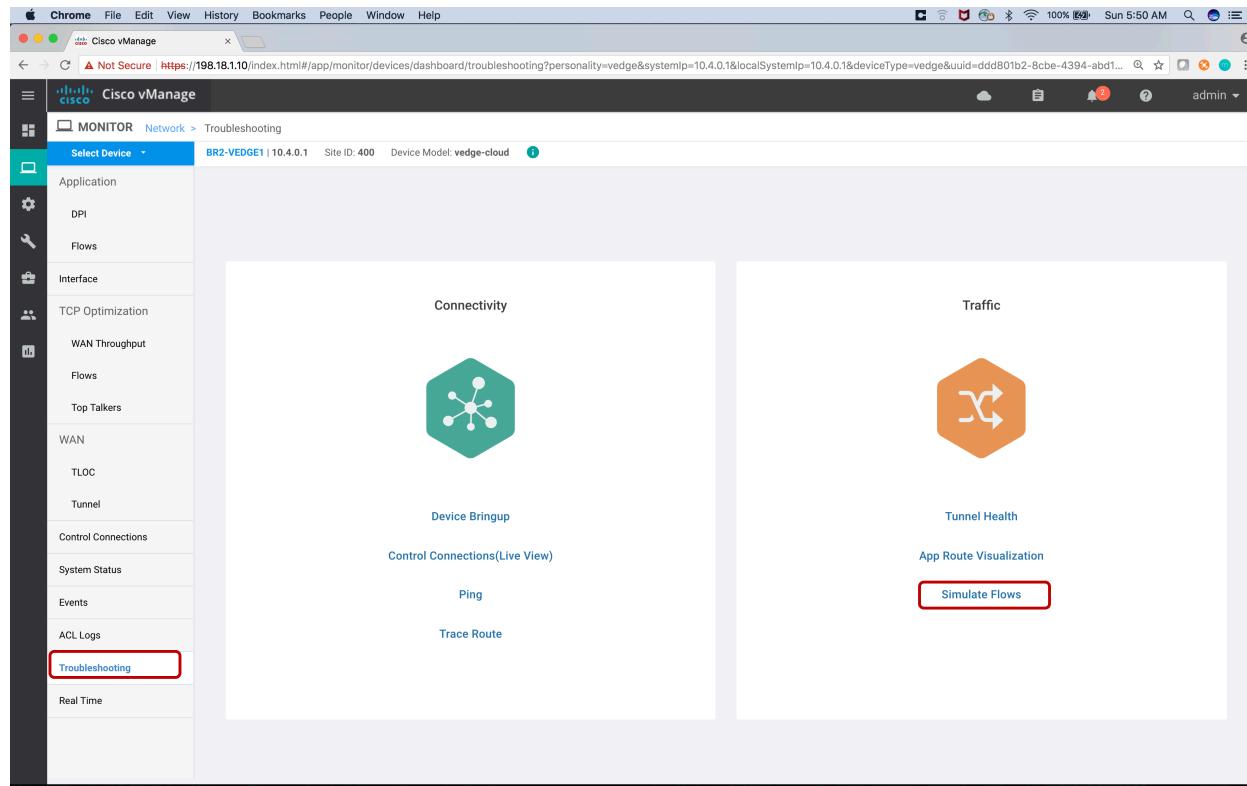
Go back to the vManage's device dashboard and look for App Route Statistics under “Real Time”.

You will observe high latency on MPLS IPSec Tunnels with no change on Internet tunnels.

The screenshot shows the Cisco vManage device dashboard under the "Real Time" section. The left sidebar lists various monitoring categories. The main area displays "App Route Statistics" for device BR2-VEDGE1. A search bar at the top contains "mpls". A filter dropdown below it is set to "App Routes Statistics". A large red circle highlights the entire table of results, which includes columns for Local System IP, Local Color, Remote Color, Mean Loss, Mean Latency, Mean Jitter, SLA Class Index, Index, Total Packets, Loss, and Average Latency. The table shows multiple entries for MPLS tunnels, all with high mean latency values (e.g., 101, 100, 101 ms).

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”.



The screenshot shows the Cisco vManage interface with the following details:

- Header:** Chrome browser window, Cisco vManage tab, 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..., admin user.
- Left Sidebar (Select Device):** MONITOR, Network > Troubleshooting. Options include Application, DPI, Flows, Interface, TCP Optimization, WAN Throughput, Flows, Top Talkers, WAN, TLOC, Tunnel, Control Connections, System Status, Events, ACL Logs, and Troubleshooting (highlighted with a red box).
- Central Area:**
  - Connectivity:** Device Bringup icon (green hexagon with network nodes).
  - Traffic:** Tunnel Health icon (orange hexagon with arrows).
  - Control Connections (Live View):** Ping icon (blue hexagon with a ping ball), Trace Route icon (grey hexagon with a route path).
  - App Route Visualization:** Simulate Flows button (red box).

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.

Not Secure https://198.18.1.10/index.html#/app/monitor/devices/dashboard/troubleshooting/simulate\_flows?personality=vedge&systemIp=10.4.0.1&deviceType=vedge&uid=ddd801b2-8c...

MONITOR Network > Troubleshooting > Simulate Flows

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

Troubleshooting

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

Advanced Options

Protocol\*  
1

Source Port

Destination Port

DSCP  
46

All Paths

Simulate

Output:

Total next hops: 1 | IPSec : 1

Network Diagram:

```

graph LR
    Laptop((Laptop)) --> Router((10.4.0.1))
    Router --> Destination[10.3.0.1]
    Router -- "biz-internet" --> Destination
    Router -- "Remote System IP Encapsulation" --> Destination
  
```

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.

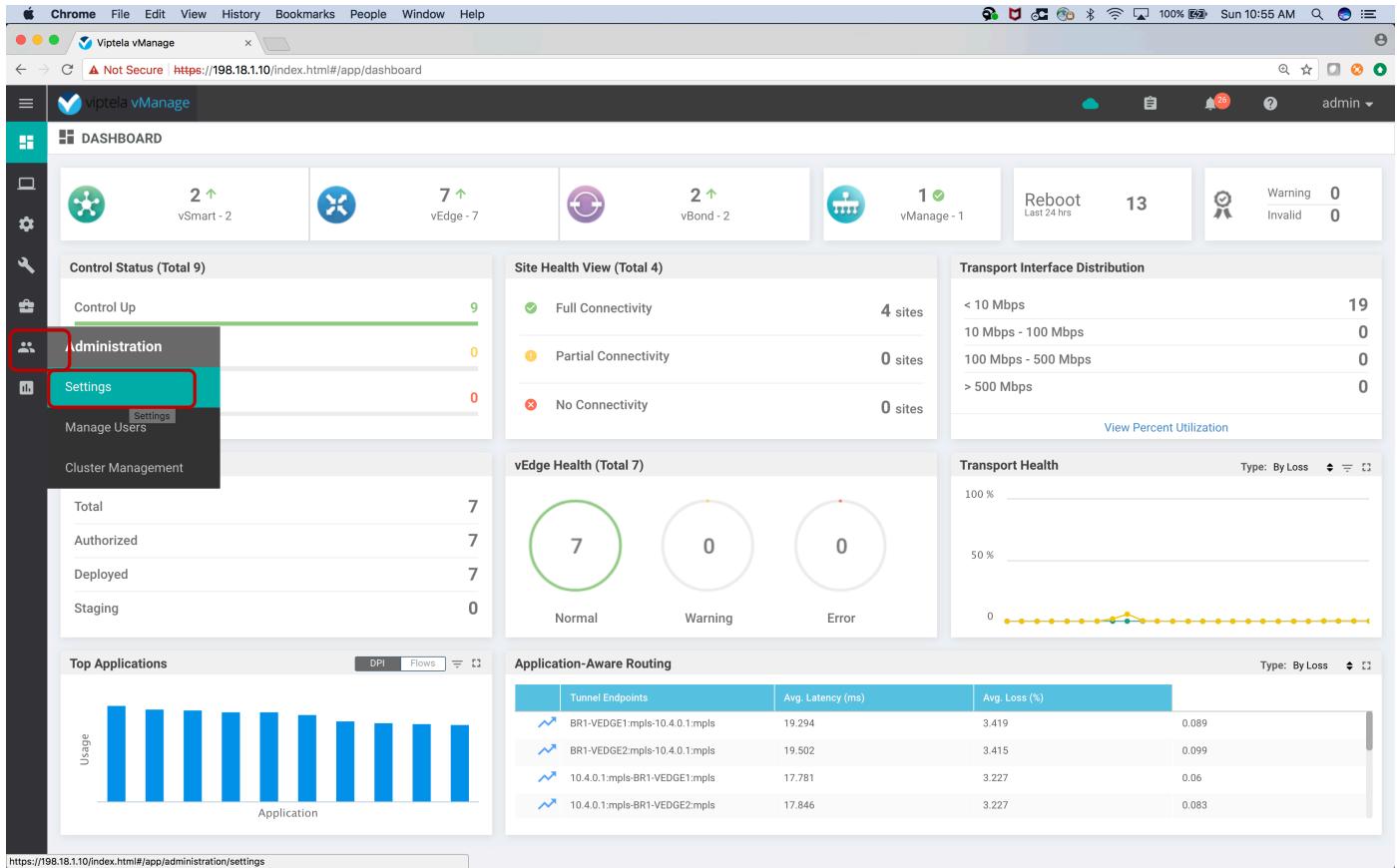
Cisco SD-WAN provides a method to run application probes for each one of these applications and compute the Viptela Quality of Experience (vQoE) score for each one of the paths (DIA or regional Hub/DC internet exits). vEdge routers then based on vQoE scores to pick the best optimal path for a given SaaS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

- Control Status (Total 9):**
  - Control Up: 9
  - Administration: 0
  - Settings: 0
- Site Health View (Total 4):**

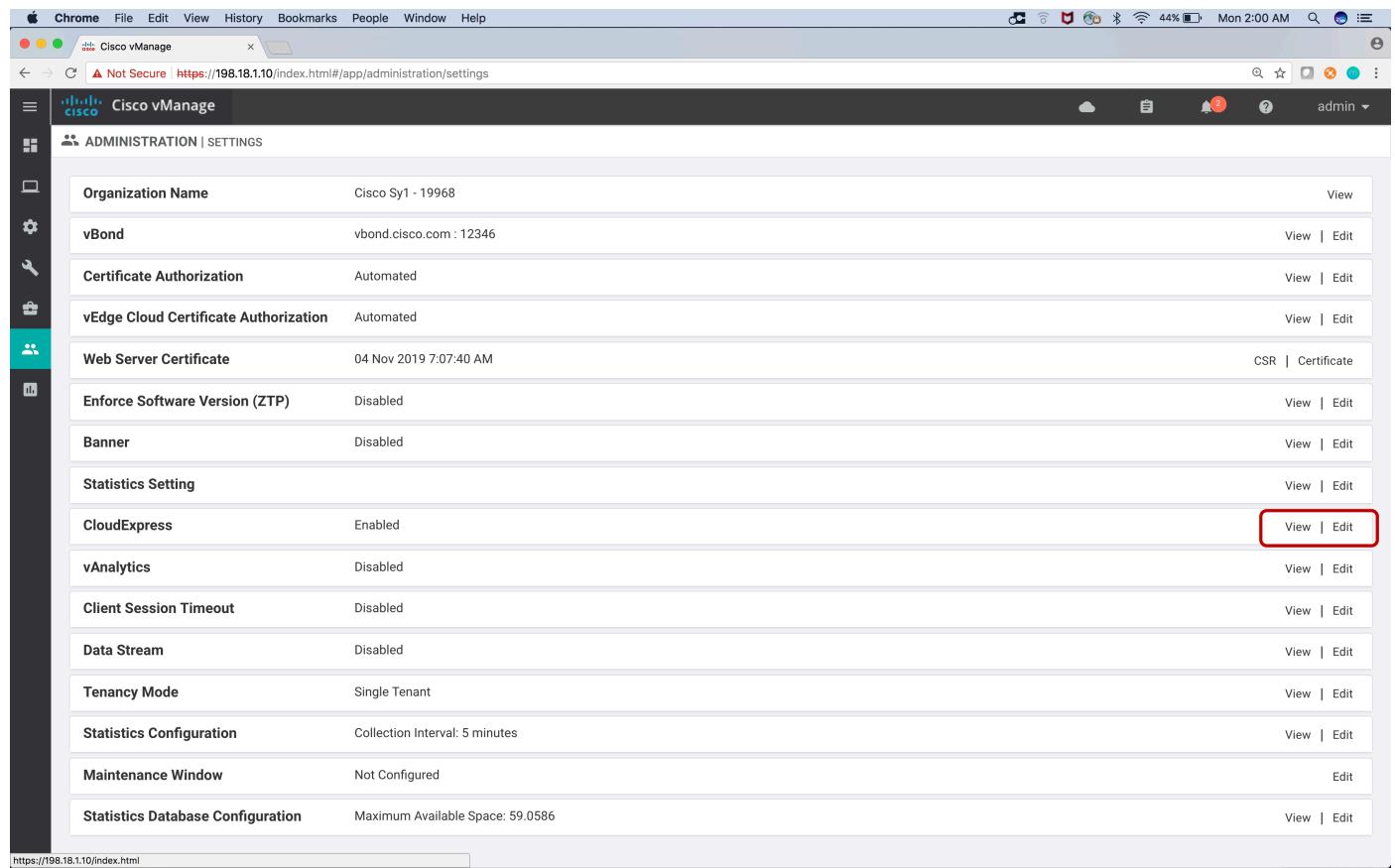
Status	Count
Full Connectivity	4 sites
Partial Connectivity	0 sites
No Connectivity	0 sites
- Transport Interface Distribution:**

Bandwidth Range	Count
< 10 Mbps	19
10 Mbps - 100 Mbps	0
100 Mbps - 500 Mbps	0
> 500 Mbps	0
- vEdge Health (Total 7):**

Status	Count
Normal	7
Warning	0
Error	0
- Transport Health:** A line chart showing transport utilization over time, currently at 100%.
- Application-Aware Routing:**

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)
BR1-EDGE1:mpls-10.4.0.1:mpls	19.294	3.419
BR1-EDGE2:mpls-10.4.0.1:mpls	19.502	3.415
10.4.0.1:mpls-BR1-EDGE1:mpls	17.781	3.227
10.4.0.1:mpls-BR1-EDGE2:mpls	17.846	3.227

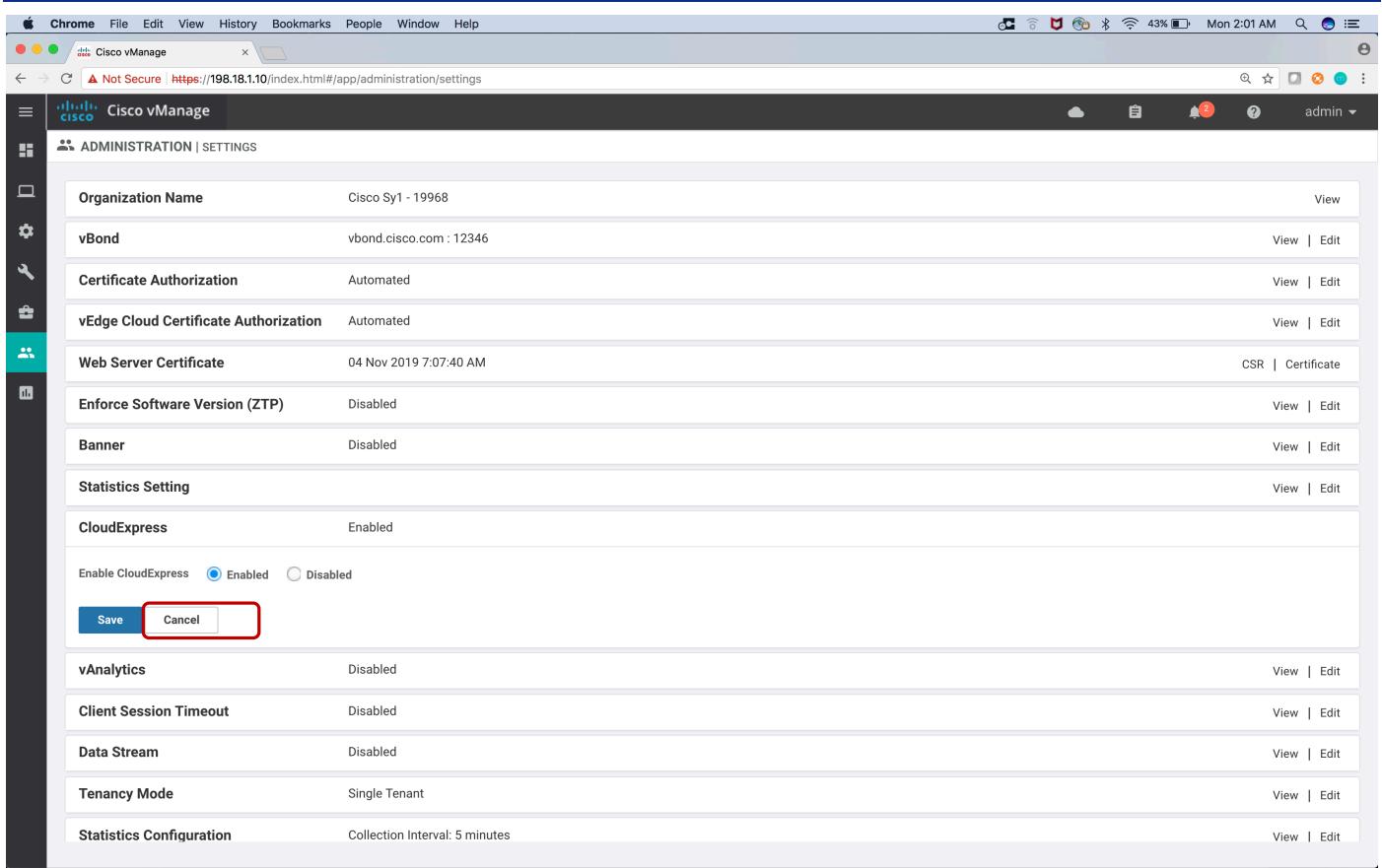
Click on “Edit” for CloudExpress.



The screenshot shows the Cisco vManage Administration Settings page. The left sidebar has icons for Home, Network, Configuration, Monitoring, Devices, and People. The main content area is titled "ADMINISTRATION | SETTINGS". A table lists various configuration items with "View" and "Edit" links. The "CloudExpress" row is highlighted with a red box around its "Edit" link.

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

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



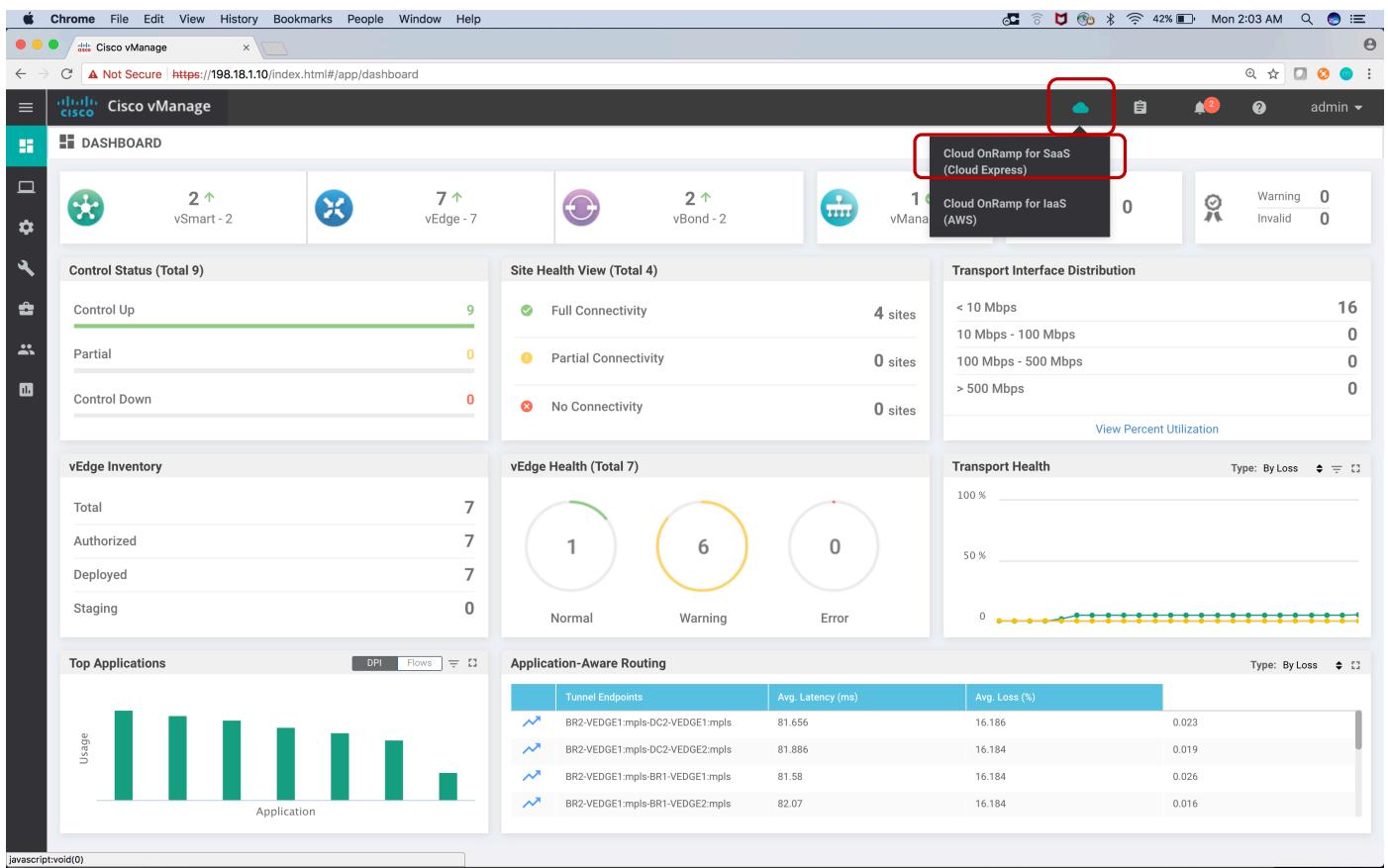
The screenshot shows the Cisco vManage Administration Settings page. On the left, there is a sidebar with icons for Home, Devices, Configuration, Monitoring, Analytics, and Support. The main content area is titled "ADMINISTRATION | SETTINGS". It lists various configuration options with "View" and "Edit" links:

- Organization Name:** Cisco Sy1 - 19968
- vBond:** vbond.cisco.com : 12346
- Certificate Authorization:** Automated
- vEdge Cloud Certificate Authorization:** Automated
- Web Server Certificate:** 04 Nov 2019 7:07:40 AM (CSR | Certificate)
- Enforce Software Version (ZTP):** Disabled
- Banner:** Disabled
- Statistics Setting:** View | Edit
- CloudExpress:** Enabled
- Enable CloudExpress:**  Enabled  Disabled
- vAnalytics:** Disabled
- Client Session Timeout:** Disabled
- Data Stream:** Disabled
- Tenancy Mode:** Single Tenant
- Statistics Configuration:** Collection Interval: 5 minutes (View | Edit)

At the bottom of the configuration section, there are "Save" and "Cancel" buttons, with "Save" being highlighted.

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).



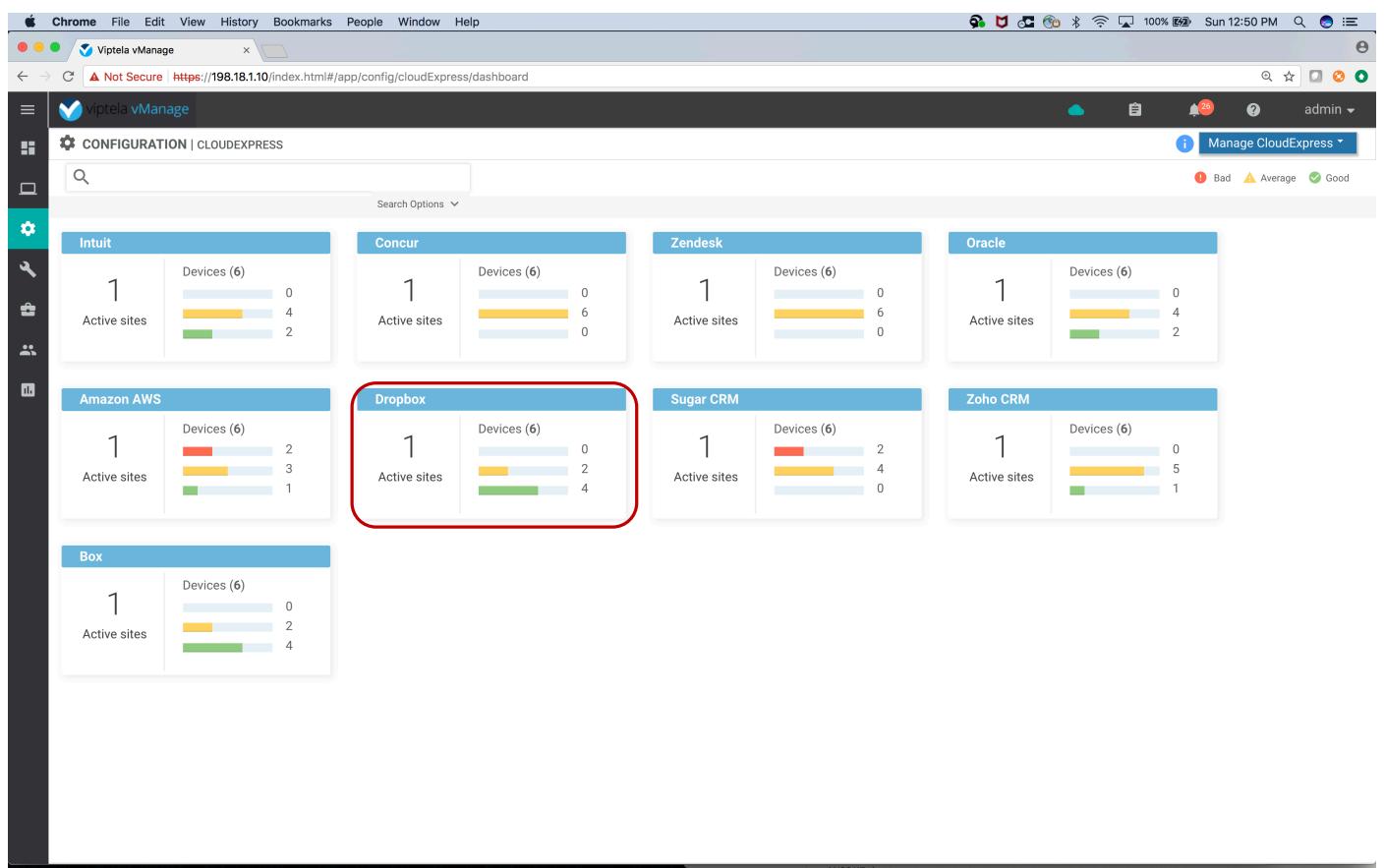
The screenshot shows the Cisco vManage dashboard with several key components:

- Control Status (Total 9):** Shows Control Up (9), Partial (0), and Control Down (0).
- vEdge Inventory:** Total 7, including Authorized (7), Deployed (7), and Staging (0).
- Top Applications:** A bar chart showing application usage.
- Site Health View (Total 4):** Shows Full Connectivity (4 sites), Partial Connectivity (0 sites), and No Connectivity (0 sites).
- Transport Interface Distribution:** Categories: < 10 Mbps (16), 10 Mbps - 100 Mbps (0), 100 Mbps - 500 Mbps (0), > 500 Mbps (0).
- vEdge Health (Total 7):** Shows 1 Normal, 6 Warning, and 0 Error.
- Transport Health:** A graph showing percent utilization over time.
- Application-Aware Routing:** A table showing Tunnel Endpoints, Avg. Latency (ms), and Avg. Loss (%).

A specific callout highlights the **Cloud OnRamp for SaaS (Cloud Express)** section, which includes a status icon and a link to "Cloud OnRamp for IaaS (AWS)".

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

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

Viptela vManage

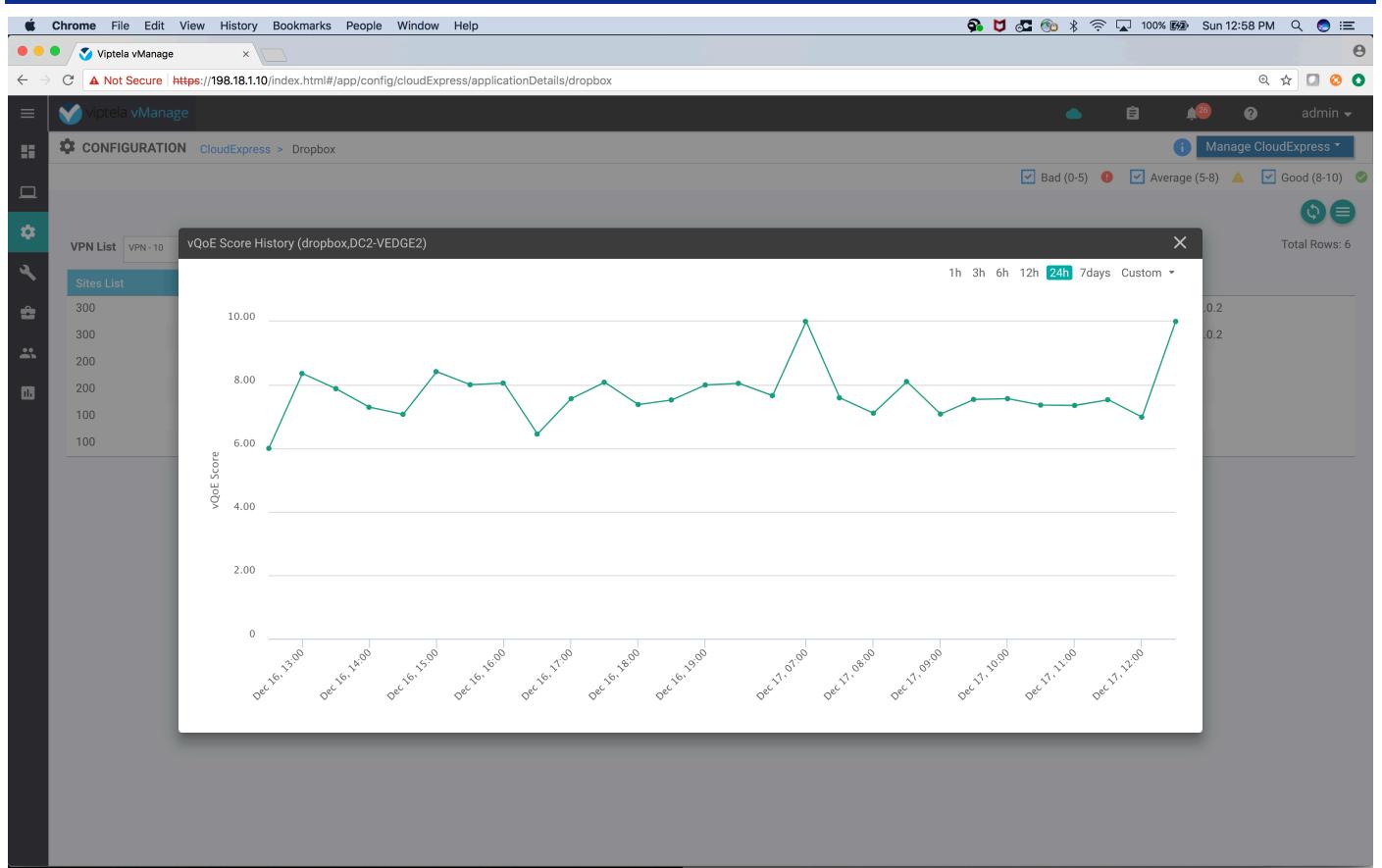
CONFIGURATION CloudExpress > Dropbox

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
300	BR1-VEDGE2	✓	10.0 ↗	gateway	N/A
200	DC2-VEDGE2	✓	10.0 ↗	local	ge0/2
200	DC2-VEDGE1	⚠	6.0 ↗	local	ge0/2
100	DC1-VEDGE2	✓	10.0 ↗	local	ge0/2
100	DC1-VEDGE1	⚠	6.0 ↗	local	ge0/2



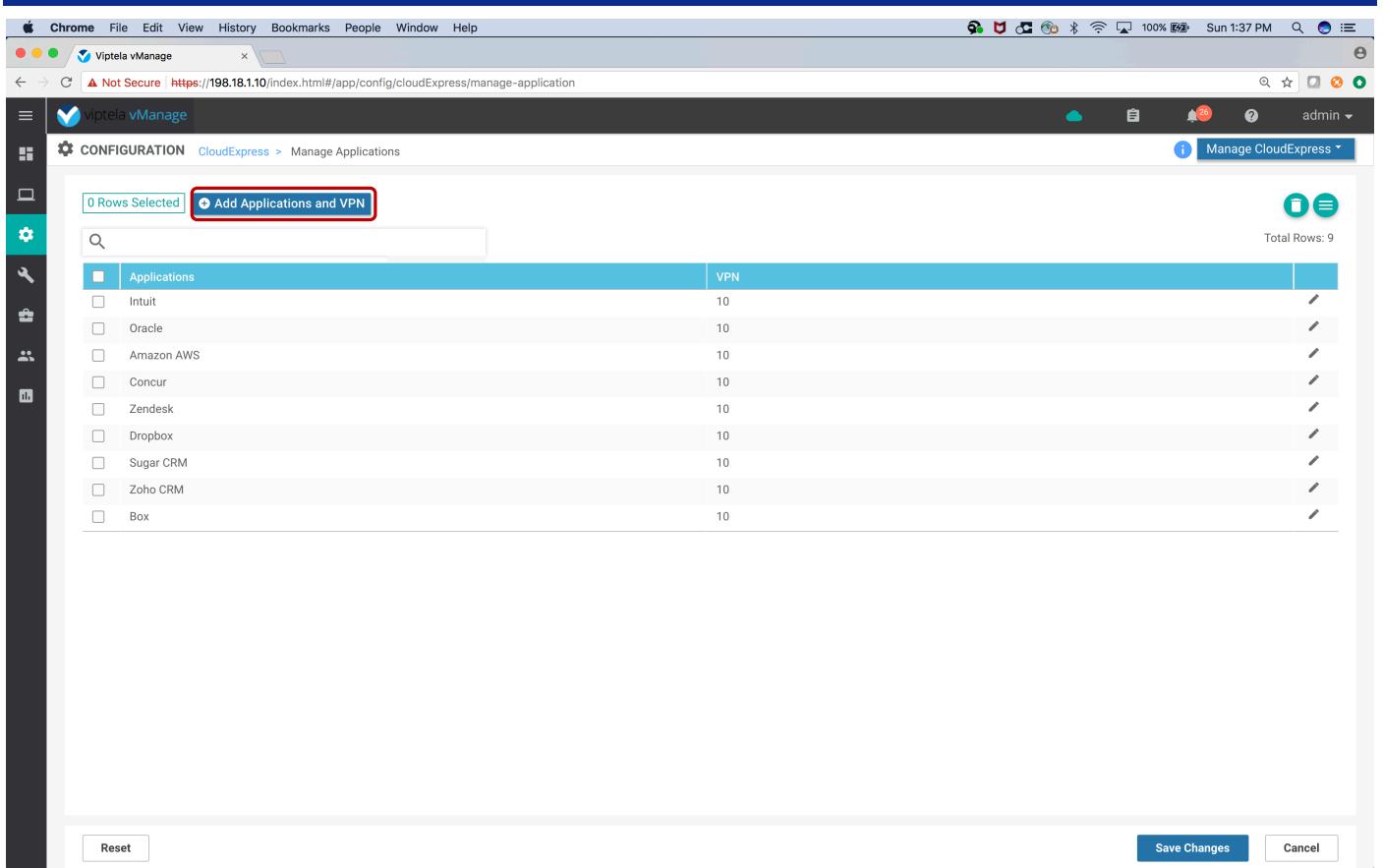
To add in a new application to the list go to CloudExpress dashboard. Click on the “Manage CloudExpress” pull down and select “Applications”.

The screenshot shows the Cisco vManage Cloud Express dashboard. At the top right, there is a red box around the "Manage CloudExpress" button, which has a dropdown menu with the following options: Applications (highlighted with a red box), Client Sites, Gateways, and Direct Internet Access(DIA) Sites.

The main area displays various application configurations in cards:

- Intuit**: Active sites: 1, Devices (6): 0 (blue), 3 (yellow), 3 (green).
- Concur**: Active sites: 1, Devices (6): 0 (blue), 2 (yellow), 4 (green).
- Zendesk**: Active sites: 1, Devices (6): 0 (blue), 5 (yellow), 1 (green).
- Oracle**: Active sites: 1, Devices (6): 0 (blue), 3 (yellow), 3 (green).
- Amazon AWS**: Active sites: 1, Devices (6): 0 (blue), 6 (yellow), 0 (green).
- Dropbox**: Active sites: 1, Devices (6): 0 (blue), 3 (yellow), 3 (green).
- Sugar CRM**: Active sites: 1, Devices (6): 3 (red), 3 (yellow), 0 (green).
- Zoho CRM**: Active sites: 1, Devices (6): 0 (blue), 4 (yellow), 2 (green).
- Box**: Active sites: 1, Devices (6): 0 (blue), 1 (yellow), 5 (green).

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



The screenshot shows a web browser window for Viptela vManage. The title bar says "Viptela vManage". The address bar shows "Not Secure https://198.18.1.10/index.html#/app/config/cloudExpress/manage-application". The main content area is titled "CONFIGURATION CloudExpress > Manage Applications". A sub-header "Manage Applications" is visible. On the left, there's a sidebar with various icons. The main table has columns "Applications" and "VPN". The table lists several applications with a value of 10 for the VPN column. At the bottom right of the table are "Save Changes" and "Cancel" buttons.

Applications	VPN
Intuit	10
Oracle	10
Amazon AWS	10
Concur	10
Zendesk	10
Dropbox	10
Sugar CRM	10
Zoho CRM	10
Box	10

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

The screenshot shows the Cisco Viptela vManage interface. The main window displays a list of applications under the heading 'CONFIGURATION' > 'CloudExpress' > 'Manage Applications'. A modal dialog box is overlaid on the screen, titled 'Add Applications & VPN'. In the 'Applications' field, the text 'office' is entered, and 'Office 365' is listed as a suggestion. The 'VPN' field is empty. At the bottom of the modal are 'Add' and 'Cancel' buttons. The background shows a list of applications including Intuit, Oracle, Amazon AWS, Concur, Zendesk, Dropbox, Sugar CRM, Zoho CRM, and Box. The total number of rows is 9.

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

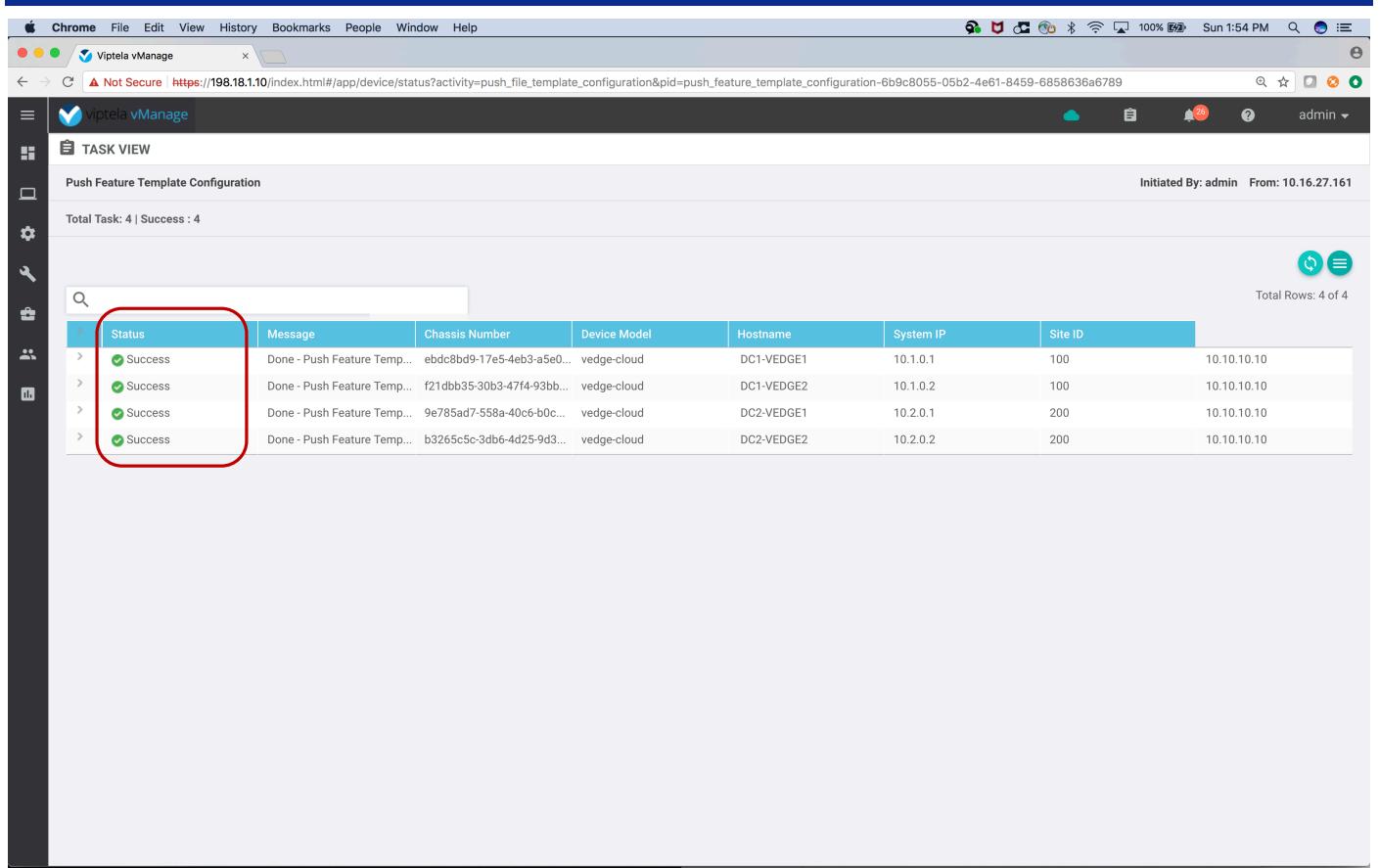
The screenshot shows a web browser window for 'Viptela vManage' on a Mac OS X system. The title bar includes the Cisco logo, the event details ('Cisco live! 6–9 March 2018 • Melbourne, Australia'), and the page title ('Not Secure https://198.18.1.10/index.html#/app/config/cloudExpress/manage-application'). The main content area is titled 'CONFIGURATION' and 'CloudExpress > Manage Applications'. A table lists various applications (Intuit, Oracle, Amazon AWS, Concur, Zendesk, Dropbox, Sugar CRM, Zoho CRM, Box) with their corresponding VPN values (all set to 10). A modal dialog titled 'Add Applications & VPN' is displayed, containing fields for 'Applications' (with 'Office 365' selected) and 'VPN' (set to 10). The 'Add' button in the dialog is highlighted with a red rectangle. At the bottom of the main screen, there are 'Save Changes' and 'Cancel' buttons.

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

The screenshot shows the Viptela vManage interface with the title bar "Viptela vManage". The URL in the address bar is "Not Secure https://198.18.1.10/index.html#/app/config/cloudExpress/manage-application". The main content area is titled "CONFIGURATION CloudExpress > Manage Applications". A table lists various applications with their corresponding VPN values. The "Save Changes" button at the bottom right is highlighted with a red box.

Applications	VPN
Intuit	10
Oracle	10
Amazon AWS	10
Concur	10
Zendesk	10
Dropbox	10
Sugar CRM	10
Zoho CRM	10
Box	10
Google Apps	10

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



The screenshot shows the Viptela vManage interface with a task titled "Push Feature Template Configuration". The task has been initiated by "admin" from IP "10.16.27.161" and has completed 4 tasks successfully. A red box highlights the "Status" column of the task table, which shows four entries all marked as "Success".

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 “Diresct Internet Access (DIA) Sites”.

The screenshot shows the Cisco vManage Cloud Express dashboard. On the left, there's a sidebar with icons for Home, Applications, Client Sites, Gateways, and Direct Internet Access. The main area displays a grid of application configurations. Each configuration card includes a title, the number of active sites (e.g., 1), and a bar chart showing device counts across three categories. A red box highlights the 'Manage CloudExpress' dropdown menu, which contains four options: Applications, Client Sites, Gateways, and Direct Internet Access(DIA) Sites. The 'Direct Internet Access(DIA) Sites' option is also highlighted with a red box.

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

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.

The screenshot shows the Viptela vManage interface with the 'CONFIGURATION' tab selected. In the 'CloudExpress > Manage DIA' section, there is a button labeled 'Attach DIA Sites' which is highlighted with a red box. Below this, a modal dialog box titled 'Attach DIA Sites' is displayed. The dialog has two main sections: 'Available Sites' on the left and 'Selected Sites' on the right. The 'Available Sites' section shows a table with columns 'Site List' and 'Devices'. One row is selected, showing '400' in the Site List and 'BR2-VEDGE1' in the Devices column. This row is also highlighted with a red box. Between the two sections is a central area with a right-pointing arrow button, which is also highlighted with a red box. At the bottom of the dialog, there are 'Attach' and 'Cancel' buttons.

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

The screenshot shows the Viptela vManage interface with the title bar "viptela vManage". The main menu includes "File", "Edit", "View", "History", "Bookmarks", "People", "Window", and "Help". The address bar indicates a non-secure connection to "https://198.18.1.10/index.html#/app/config/cloudExpress/manage-dia". The navigation bar shows "CONFIGURATION" and "CloudExpress > Manage DIA". The main content area displays a table with columns "Site List" and "Devices". A modal dialog box titled "Attach DIA Sites" is open, containing two tables: "Available Sites" and "Selected Sites". The "Selected Sites" table has one row: "400 BR2-VEDGE1". At the bottom of the dialog, there is a link "Add interfaces to selected sites(optional)" highlighted with a red box, followed by "Attach" and "Cancel" buttons.

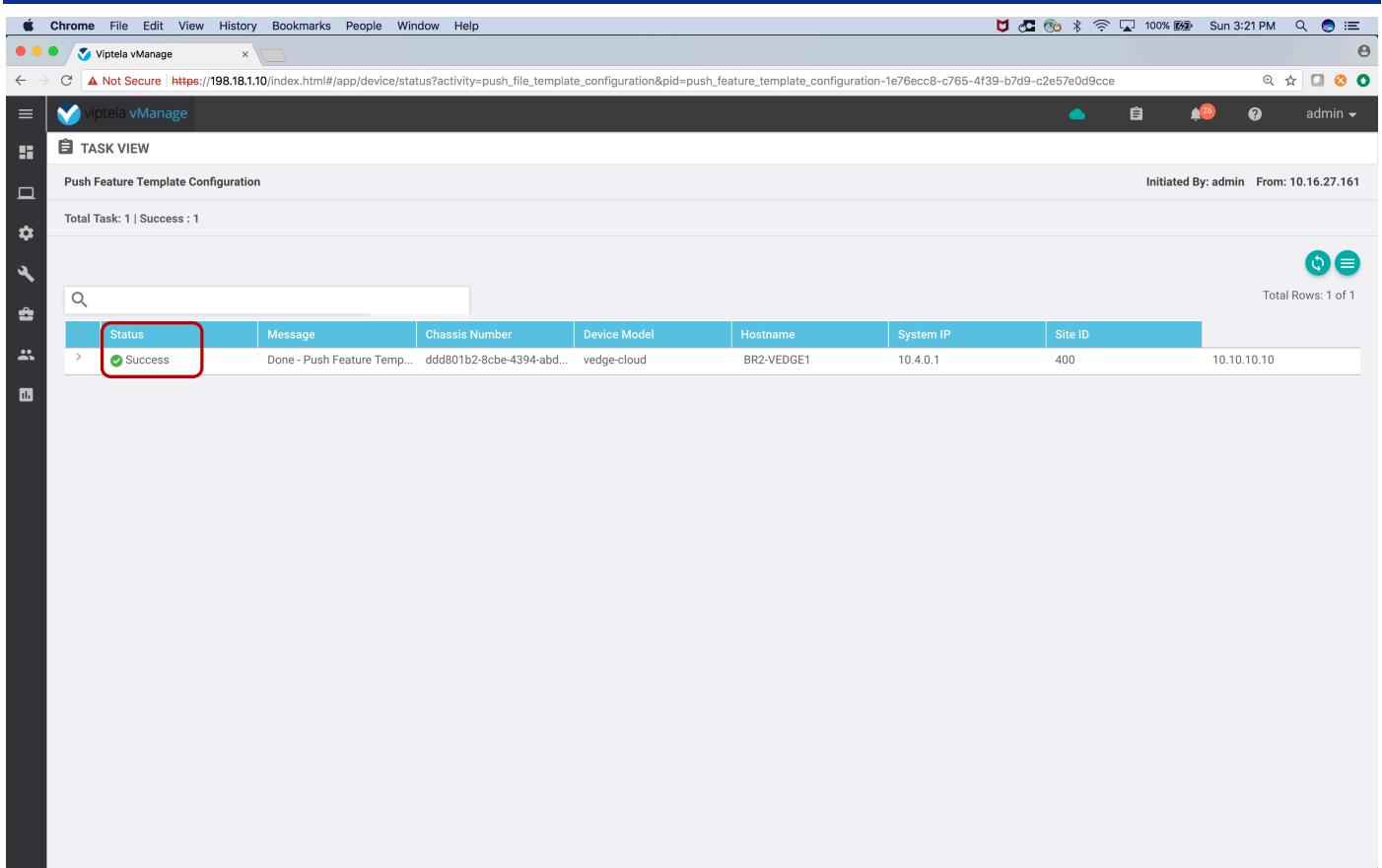
Click in the box “Select Interfaces”, select ge0/0 (internet) interface on BR2-VEDGE1. Then click on “Save Changes” button.

The screenshot shows the Viptela vManage web interface. The main navigation bar includes 'File', 'Edit', 'View', 'History', 'Bookmarks', 'People', 'Window', and 'Help'. The title bar indicates the URL is [Not Secure https://198.18.1.10/index.html#/app/config/cloudExpress/manage-dia](https://198.18.1.10/index.html#/app/config/cloudExpress/manage-dia). The top right corner shows system status (100% battery, Sun 3:20 PM) and user 'admin'. The left sidebar has icons for Home, Devices, Configuration, Monitoring, and Support. The main content area is titled 'CONFIGURATION' > 'CloudExpress' > 'Manage DIA'. A sub-menu bar at the top of the content area includes 'Attach DIA Sites', 'Detach DIA Sites', and 'Edit DIA Sites'. Below this is a search bar and a table header 'Devices in sync'. A modal dialog box is open, titled 'Attach DIA Sites' with 'Site ID: 400'. It contains two sections: 'vEdges' and 'Interfaces'. Under 'vEdges', there is one entry: '10.4.0.1'. Under 'Interfaces', a dropdown menu titled 'Select Interfaces...' lists five options: 'ge0/2', 'ge0/0' (which is highlighted with a red box), 'ge0/3', 'ge0/4', and 'ge0/5'. At the bottom of the dialog are three buttons: 'Back', 'Save Changes' (which is highlighted with a red box), and 'Cancel'. The status bar at the bottom of the browser window shows the URL <https://198.18.1.10/index.html>.

Click on the “Attach” button.

The screenshot shows the Viptela vManage interface with the title bar "vManage" and the URL "https://198.18.1.10/index.html#/app/config/cloudExpress/manage-dia". The main menu bar includes "File", "Edit", "View", "History", "Bookmarks", "People", "Window", and "Help". The top right corner shows system status: 100% battery, Sun 3:20 PM, and a user "admin". The left sidebar has icons for Home, Devices, Site, Configuration, and Help. The main content area is titled "CONFIGURATION" > "CloudExpress" > "Manage DIA". A sub-menu "Manage CloudExpress" is visible. Below this, there are buttons for "Attach DIA Sites", "Detach DIA Sites", and "Edit DIA Sites". A modal dialog box titled "Attach DIA Sites" is open. It contains two tables: "Available Sites" (empty) and "Selected Sites" (containing row 400 with device BR2-VEDGE1). There are "Search" fields and "Site List" and "Devices" columns. At the bottom of the dialog are "Attach" and "Cancel" buttons, with "Attach" being highlighted by a red box.

Wait till the CloudExpress configuration push to BR2-VEDGE1 succeeds.



The screenshot shows a browser window for 'Viptela vManage' with the URL [https://198.18.1.10/index.html#/app/device/status?activity=push\\_file\\_template\\_configuration&pid=push\\_feature\\_template\\_configuration-1e76ecc8-c765-4f39-b7d9-c2e57e0d9cce](https://198.18.1.10/index.html#/app/device/status?activity=push_file_template_configuration&pid=push_feature_template_configuration-1e76ecc8-c765-4f39-b7d9-c2e57e0d9cce). The page displays a table titled 'Push Feature Template Configuration' with one row. The row contains the following data:

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

A red box highlights the 'Status' column header. The status message 'Success' is also highlighted with a red box. The table has a total of 1 row.

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.

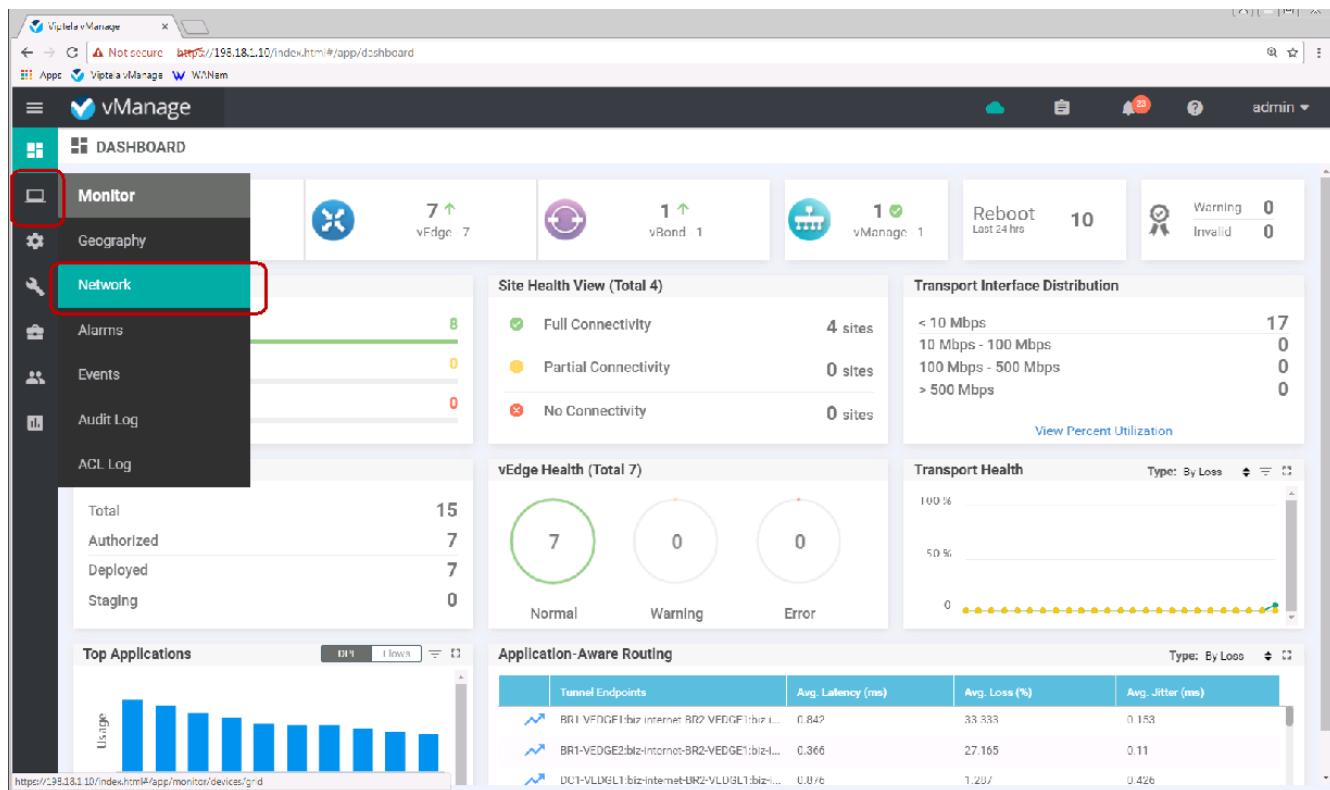
Corporate VPN 10 – Full Mesh

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.

The screenshot shows the vManage interface for monitoring network devices. The left sidebar has icons for Home, Devices, Troubleshooting, and Reports. The main area is titled 'MONITOR | NETWORK' and displays a table of devices. The table columns are: Hostname, State, System IP, Reachability, Site ID, Device Model, BFD, Control, Version, Up Since, and Ch. A search bar and a 'Search Options' dropdown are at the top of the table. The device 'BR2-VEDGE1' is highlighted with a red box. The table data is as follows:

Hostname	State	System IP	Reachability	Site ID	Device Model	BFD	Control	Version	Up Since	Ch
BR1-VEDGE1	reachable	10.3.0.1	reachable	300	vEdge Cloud	8	3	17.1.1	12 Aug 2017 2:36:00 AM GMT	52c
BR1-VEDGE2	reachable	10.3.0.2	reachable	300	vEdge Cloud	8	3	17.1.1	12 Aug 2017 2:36:00 AM GMT	5a4
BR2-VEDGE1	unreachable	10.4.0.1	unreachable	400	vEdge Cloud	--	--	17.1.1	09 Aug 2017 7:39:00 PM GMT	ddd
DC1-VEDGE1	reachable	10.1.0.1	reachable	100	vEdge Cloud	8	3	17.1.1	12 Aug 2017 2:35:00 AM GMT	ebd
DC1-VEDGE2	reachable	10.1.0.2	reachable	100	vEdge Cloud	8	3	17.1.1	12 Aug 2017 2:35:00 AM GMT	f21
DC2-VEDGE1	reachable	10.2.0.1	reachable	200	vEdge Cloud	8	3	17.1.1	12 Aug 2017 2:35:00 AM GMT	9e7
DC2-VEDGE2	reachable	10.2.0.2	reachable	200	vEdge Cloud	8	3	17.1.1	12 Aug 2017 2:35:00 AM GMT	b32
vbond	reachable	11.11.11.11	reachable	—	vEdge Cloud (vB0...)	—	—	17.1.1	12 Aug 2017 2:36:00 AM GMT	abd
vmanage	reachable	10.10.10.10	reachable	10	vManage	—	7	17.1.1	12 Aug 2017 2:36:00 AM GMT	52f
vsmart	reachable	12.12.12.12	reachable	10	vSmart	--	10	17.1.1	12 Aug 2017 2:36:00 AM GMT	10a

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

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

Data Stream' is disabled. Go to Settings page to enable Data Stream to use Debug Logs.

Cisco vManage MONITOR Network > Troubleshooting Select Device BR2-EDGE1 | 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

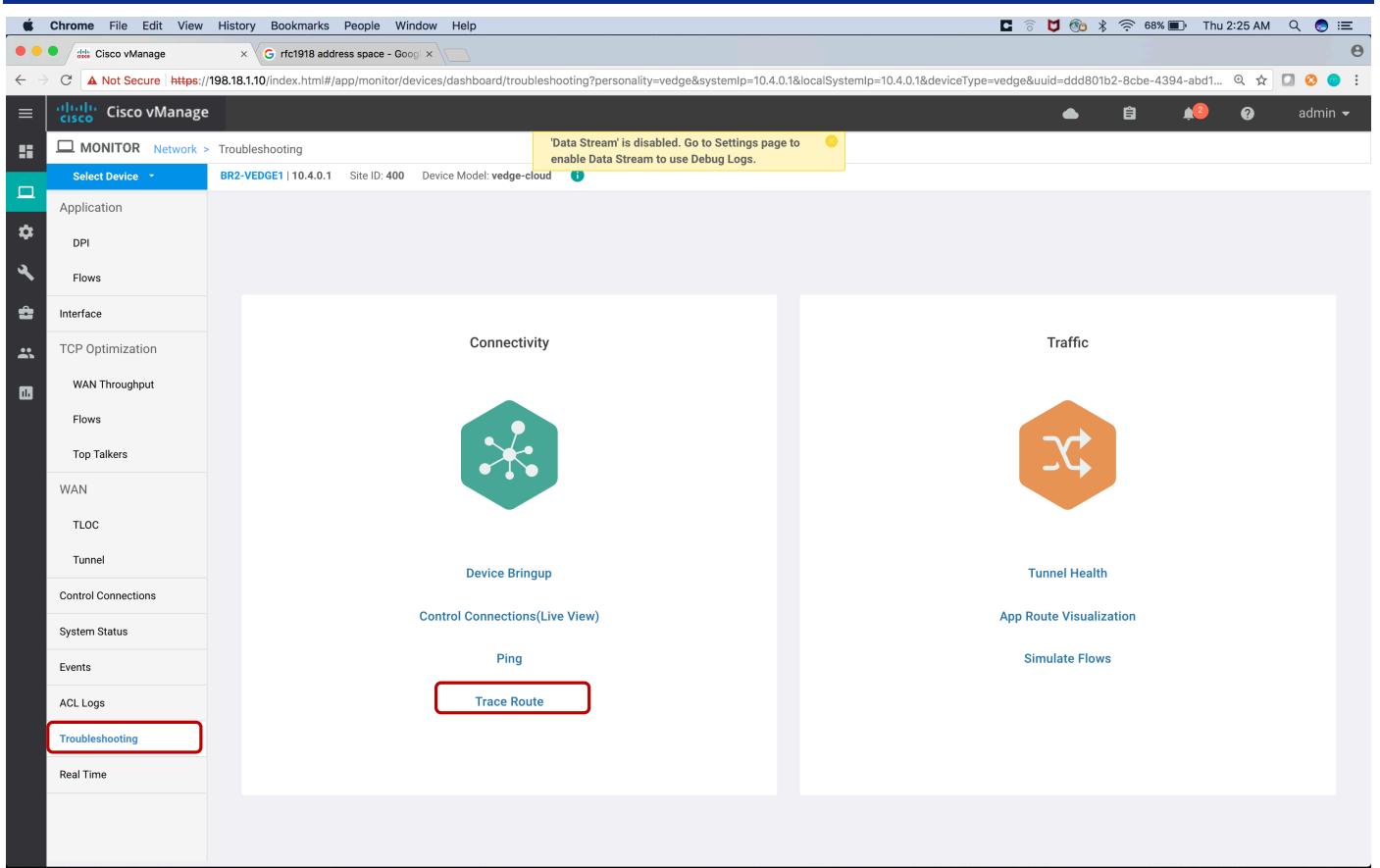
Connectivity (BR2-EDGE1)  
Traffic (BR2-EDGE1)

Device Bringup (BR2-EDGE1)  
Tunnel Health (BR2-EDGE1)

Control Connections (Live View) (BR2-EDGE1)  
App Route Visualization (BR2-EDGE1)

Ping (BR2-EDGE1)  
Trace Route (BR2-EDGE1)

Simulate Flows (BR2-EDGE1)



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 in a Chrome browser window. The URL is 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&uuid=ddd801b2-8cbe-... . The user is logged in as 'admin'. The 'Select Device' dropdown is set to 'BR2-VEDGE1 | 10.4.0.1'. The 'Destination IP\*' field contains '10.3.0.21', the 'VPN' dropdown is set to 'VPN - 10', and the 'Source/Interface for VPN - 10' dropdown has 'Choose/Reset selections'. A red box highlights the 'Start' button. The 'Output' section shows the traceroute command used: Traceroute -m 15 -w 1 10.3.0.21 in VPN 10. The results show two hops: 1 10.3.0.2 (10.3.0.2) 2.610 ms 3.347 ms 3.432 ms and 2 10.3.0.21 (10.3.0.21) 4.136 ms 4.290 ms 4.370 ms. Below the output is a network diagram showing a path from 10.4.0.1 to 10.3.0.2, then to 10.3.0.21, with a total round trip time of 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.

The screenshot shows the Cisco vManage web interface. At the top, there's a navigation bar with links like Chrome, File, Edit, View, History, Bookmarks, People, Window, Help, and a search bar. The title bar says "Cisco vManage". Below the title bar, it shows "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&uuid=ddd801b2-8cbe-...". The user is logged in as "admin".

In the main content area, the path "MONITOR > Network > Troubleshooting > Traceroute" is selected. A "Select Device" dropdown shows "BR2-VEDGE1 | 10.4.0.1 Site ID: 400 Device Model: vedge-cloud". The "Destination IP\*" field contains "10.3.20.10", the "VPN" field contains "VPN - 20", and the "Source/Interface for VPN - 20" field contains "ge0/3 - ipv4 - 10.4.20.1". A red box highlights the "Start" button.

The "Output" section displays the traceroute command and its results:

```
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
```

Below the output is a network diagram showing a path from "ge0/3 - ipv4 - 10.4.20.1" to "10.3.20.2" (via a switch icon) and then to "10.3.20.10". The link between the first two nodes is labeled "2.64ms" and the link between the second and third nodes is labeled "4.01ms".

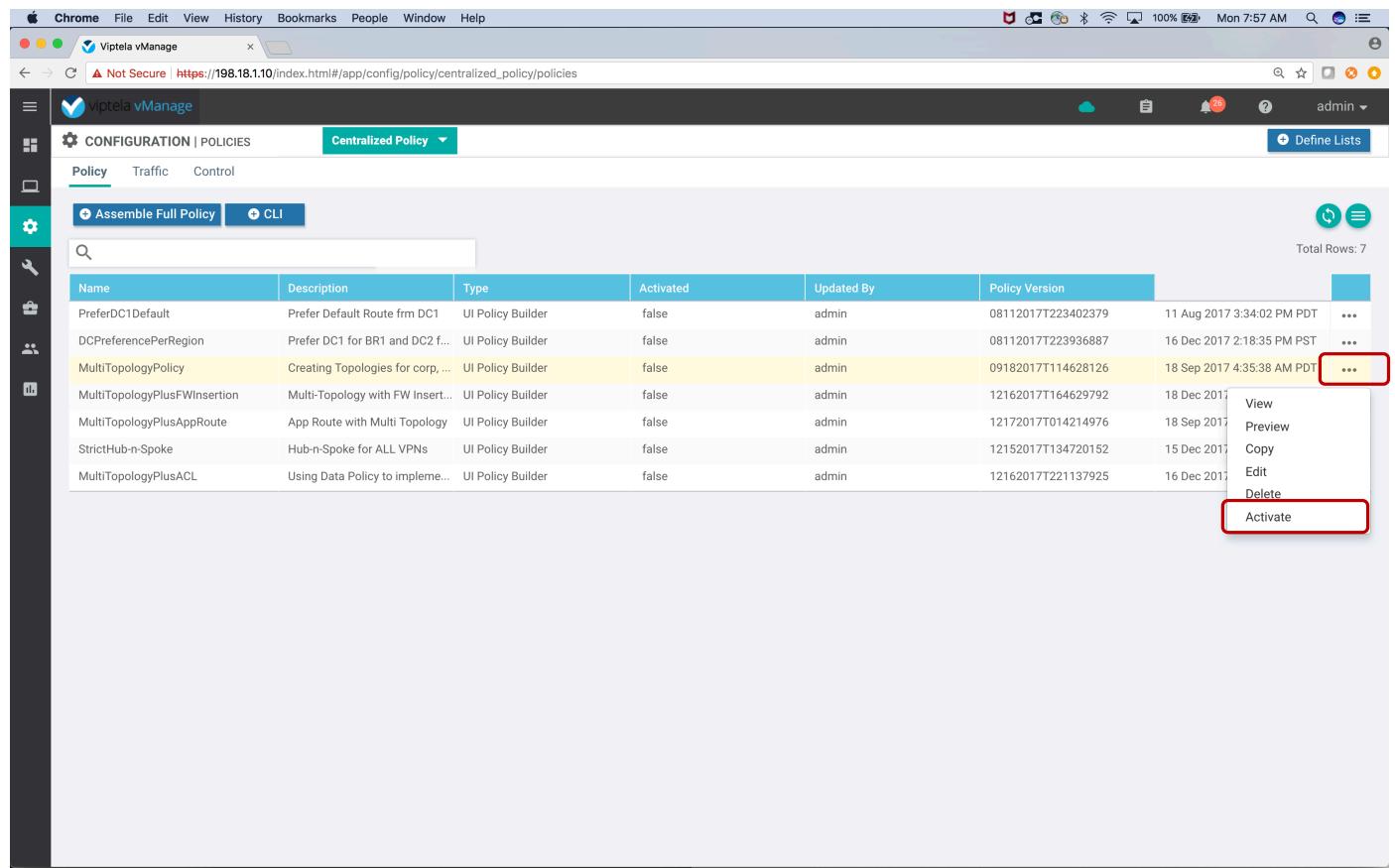
Go to vManage dashboard and go to Configuration and select Policies.

The screenshot shows the vManage dashboard with the following sections:

- Site Health View (Total 4):**
  - Full Connectivity: 4 sites
  - Partial Connectivity: 0 sites
  - No Connectivity: 0 sites
- Transport Interface Distribution:**

Transport Interface Range	Count
< 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:** Shows three horizontal bars representing 100%, 50%, and 0% utilization.
- Application-Aware Routing:**
  - Top Applications:** Bar chart showing usage for various applications.
  - Tunnel Endpoints:** Table showing latency, loss, jitter, and type for five entries.

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



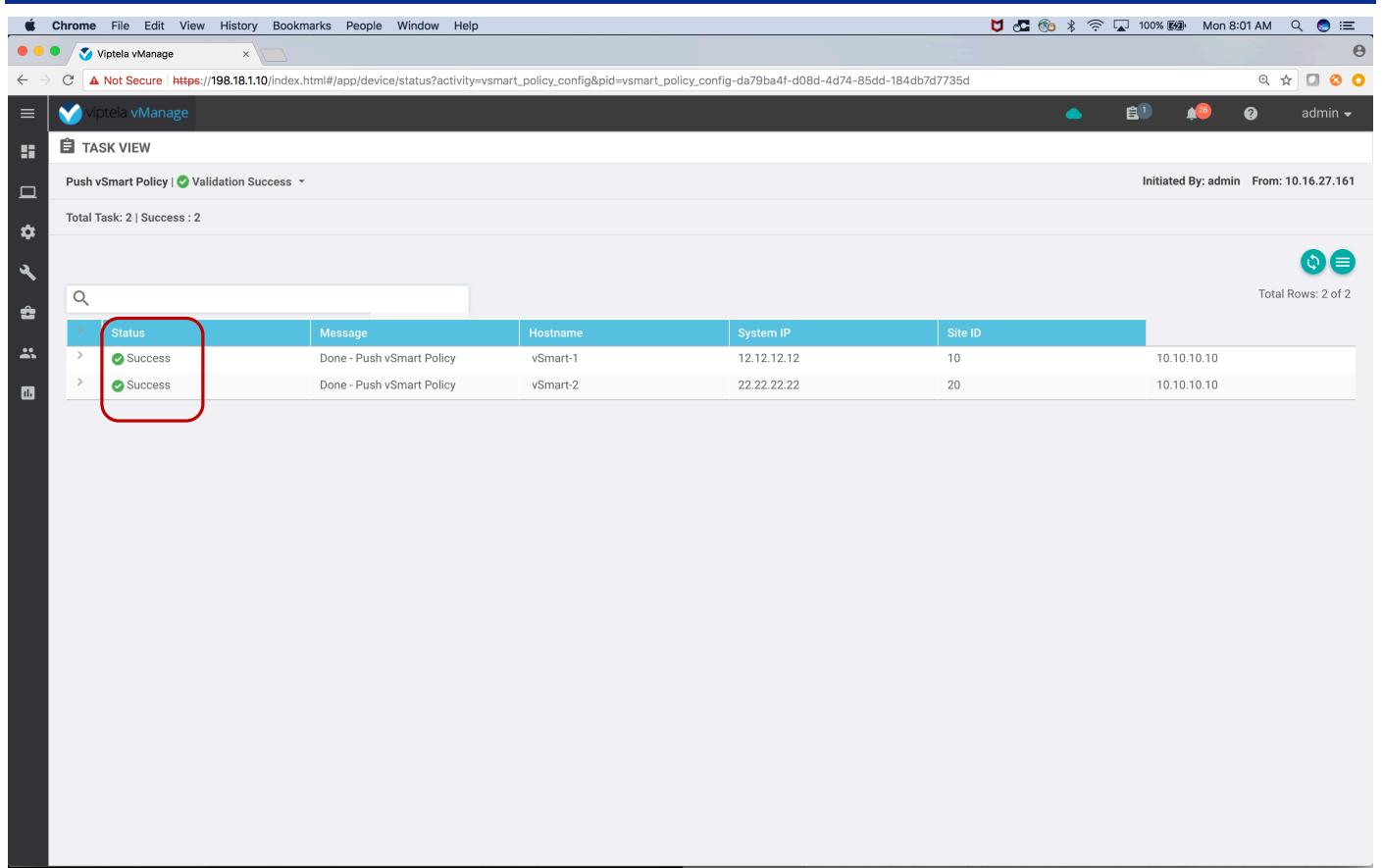
Name	Description	Type	Activated	Updated By	Policy Version	Date	Action
PreferDC1Default	Prefer Default Route frm DC1	UI Policy Builder	false	admin	08112017T223402379	11 Aug 2017 3:34:02 PM PDT	...
DCPreferencePerRegion	Prefer DC1 for BR1 and DC2 f...	UI Policy Builder	false	admin	08112017T223936887	16 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	<a href="#">View</a>
MultiTopologyPlusAppRoute	App Route with Multi Topology	UI Policy Builder	false	admin	12172017T014214976	18 Sep 2017	<a href="#">Preview</a>
StrictHub-n-Spoke	Hub-n-Spoke for ALL VPNs	UI Policy Builder	false	admin	12152017T134720152	15 Dec 2017	<a href="#">Copy</a>
MultiTopologyPlusACL	Using Data Policy to impleme...	UI Policy Builder	false	admin	12162017T221137925	16 Dec 2017	<a href="#">Edit</a> <a href="#">Delete</a>

Click on “Activate” button on the pop-up.

The screenshot shows the Viptela vManage web interface. The top navigation bar includes links for Chrome, File, Edit, View, History, Bookmarks, People, Window, and Help. The title bar shows "Viptela vManage". The main content area is titled "CONFIGURATION | POLICIES" and "Centralized Policy". Below this, there are tabs for Policy, Traffic, and Control, with "Assemble Full Policy" selected. A search bar is present above a table listing seven policies. The table columns include Name, Description, Type, Activated, Updated By, Policy Version, and Last Modified. The "MultiTopologyPolicy" row is highlighted. A modal dialog box titled "Activate Policy" is overlaid on the page, containing the message "Policy will be applied to the reachable vSmarts: 12.12.12.12, 22.22.22.22" and two buttons: "Activate" (highlighted with a red border) and "Cancel".

Name	Description	Type	Activated	Updated By	Policy Version	Last Modified
PreferDC1Default	Prefer Default Route from DC1	UI Policy Builder	false	admin	08112017T223402379	11 Aug 2017 3:34:02 PM PDT
DCPreferencePerRegion	Prefer DC1 for BR1 and DC2 for BR2	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 Insertion	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 4:16:07 PM PDT
StrictHub-n-Spoke	Hub-n-Spoke for ALL VPNs	UI Policy Builder	false	admin	12152017T134720152	15 Dec 2017 5:37:44 AM PST
MultiTopologyPlusACL	Using Data Policy to implement	UI Policy Builder	false	admin	12162017T221137925	16 Dec 2017 2:08:43 PM PST

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



The screenshot shows the vManage interface with the title "viptela vManage". The main area is titled "TASK VIEW" and displays a table of tasks. The table has columns: Status, Message, Hostname, System IP, and Site ID. There are two rows, both marked as "Success". A red box highlights the "Status" column header. The table shows:

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

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-VEDGE1.

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

The screenshot shows the vManage dashboard interface. The left sidebar has a red box around the 'Network' option under the 'Monitor' category. The main area displays various monitoring statistics and charts.

**Site Health View (Total 4)**

Connectivity Status	Number of Sites
Full Connectivity	4 sites
Partial Connectivity	0 sites
No Connectivity	0 sites

**Transport Interface Distribution**

Bandwidth Range	Count
< 10 Mbps	17
10 Mbps - 100 Mbps	0
100 Mbps - 500 Mbps	0
> 500 Mbps	0

**vEdge Health (Total 7)**

Status	Count
Normal	7
Warning	0
Error	0

**Transport Health**

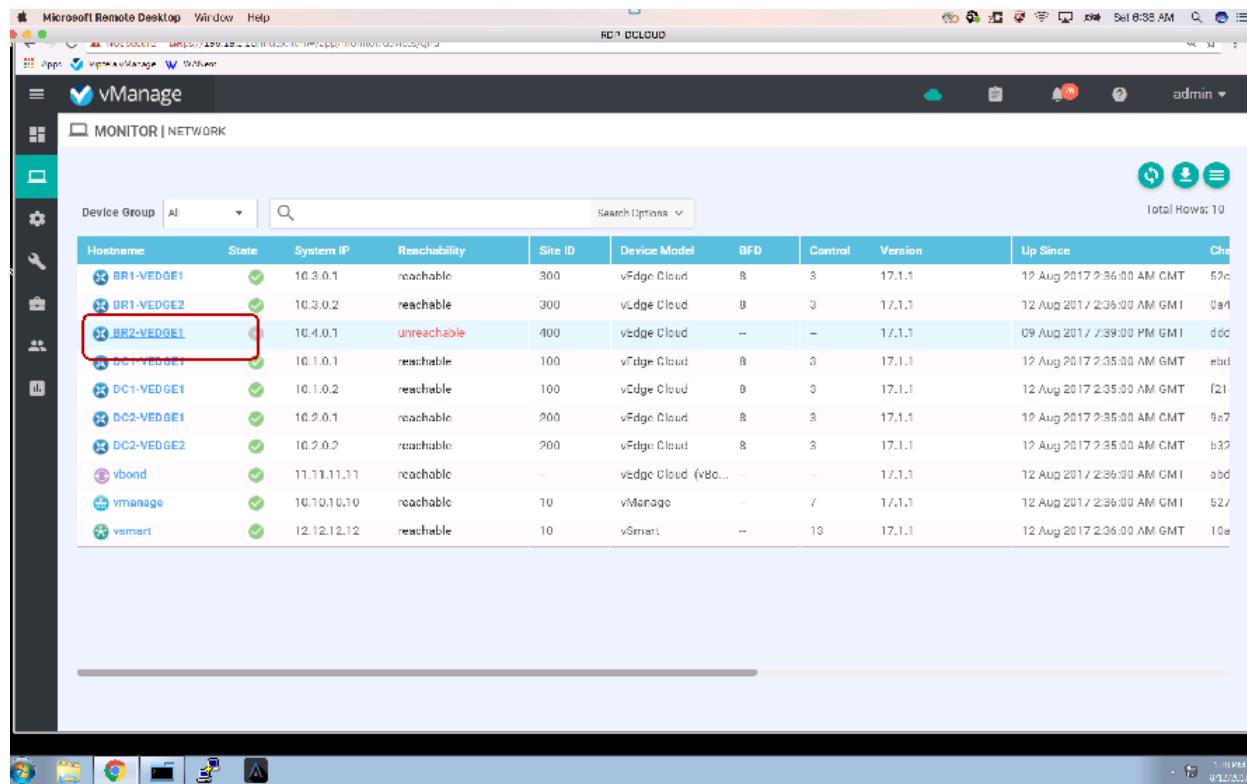
Type: By Loss

**Application-Aware Routing**

Type: By Loss

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
BRI-VEDGE1:biz-Internet-BR2-VEDGE1:biz...	0.842	33.333	0.153
BRI-VEDGE2:biz-Internet-BR2-VEDGE1:biz4...	0.366	27.165	0.11
DC1-VLDGL1:biz-Internet-BR2-VLDGL1:biz4...	0.876	1.297	0.426

Find BR2-VEDGE1 and click on the name.



The screenshot shows the vManage interface on a Microsoft Remote Desktop session. The title bar says "Microsoft Remote Desktop" and "vManage". The main window is titled "MONITOR | NETWORK" and displays a table of devices. The table has columns: Hostname, State, System IP, Reachability, Site ID, Device Model, BFD, Control, Version, Up Since, and Ch. A red box highlights the row for "BR2-VEDGE1", which has a system IP of 10.4.0.1 and a reachability status of "unreachable". Other devices listed include BR1-VEDGE1, BR1-VEDGE2, DC1-VEDGE1, DC1-VEDGE2, DC2-VEDGE1, DC2-VEDGE2, vbond, vmanage, and vsmart. The interface includes a left sidebar with icons for Home, Devices, Troubleshooting, and Reports, and a top navigation bar with various icons.

Hostname	State	System IP	Reachability	Site ID	Device Model	BFD	Control	Version	Up Since	Ch
BR1-VEDGE1	green	10.3.0.1	reachable	300	vEdge Cloud	8	3	17.1.1	12 Aug 2017 2:36:00 AM GMT	52c
BR1-VEDGE2	green	10.3.0.2	reachable	300	vEdge Cloud	8	3	17.1.1	12 Aug 2017 2:36:00 AM GMT	5a4
BR2-VEDGE1	grey	10.4.0.1	unreachable	400	vEdge Cloud	--	--	17.1.1	09 Aug 2017 7:39:00 PM GMT	ddd
DC1-VEDGE1	green	10.1.0.1	reachable	100	vEdge Cloud	8	3	17.1.1	12 Aug 2017 2:35:00 AM GMT	ebd
DC1-VEDGE2	green	10.1.0.2	reachable	100	vEdge Cloud	8	3	17.1.1	12 Aug 2017 2:35:00 AM GMT	f21
DC2-VEDGE1	green	10.2.0.1	reachable	200	vEdge Cloud	8	3	17.1.1	12 Aug 2017 2:35:00 AM GMT	9e7
DC2-VEDGE2	green	10.2.0.2	reachable	200	vEdge Cloud	8	3	17.1.1	12 Aug 2017 2:35:00 AM GMT	b32
vbond	green	11.11.11.11	reachable	—	vEdge Cloud (vbond)	—	—	17.1.1	12 Aug 2017 2:36:00 AM GMT	abd
vmanage	green	10.10.10.10	reachable	10	vManage	—	7	17.1.1	12 Aug 2017 2:36:00 AM GMT	52f
vsmart	green	12.12.12.12	reachable	10	vSmart	--	10	17.1.1	12 Aug 2017 2:36:00 AM GMT	10a

Select Troubleshooting from the left column. Then select “Traceroute”.

The screenshot shows the Cisco vManage web interface. The top navigation bar includes links for Chrome, File, Edit, View, History, Bookmarks, People, Window, and Help. The address bar shows a warning: "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...". The title bar says "Cisco vManage". The main header "Cisco vManage" has a "MONITOR Network > Troubleshooting" dropdown. A sidebar on the left lists various troubleshooting categories: Application, DPI, Flows, Interface, TCP Optimization, WAN Throughput, Flows, Top Talkers, WAN, TLOC, Tunnel, Control Connections, System Status, Events, ACL Logs, and Troubleshooting. The "Troubleshooting" link is highlighted with a red box. The main content area is divided into two sections: "Connectivity" (with a green hexagon icon) and "Traffic" (with an orange hexagon icon). Under Connectivity, there are "Device Bringup" (with a green hexagon icon), "Control Connections(Live View)" (with a green hexagon icon), "Ping" (with a green hexagon icon), and "Trace Route" (which is highlighted with a red box). Under Traffic, there are "Tunnel Health" (with an orange hexagon icon), "App Route Visualization" (with an orange hexagon icon), and "Simulate Flows" (with an orange hexagon icon).

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.

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 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
```

ge0/2 - ipv4 - 10.4.254.10 → 10.3.0.2 → 10.3.0.21 (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

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&uuid=ddd801b2-8cbe-... Sat 4:35 AM

Cisco vManage 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 10.1.20.3 (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
```

The diagram illustrates the traceroute path. It starts with a source host icon labeled "ge0/3 - ipv4 - 10.4.20.1". An arrow points to the first router, "10.1.20.3", with a label "2.54ms". Another arrow points to the second router, "10.3.20.2", with a label "4.46ms". A final arrow points to the destination host, "10.3.20.10", with a label "5.34ms".

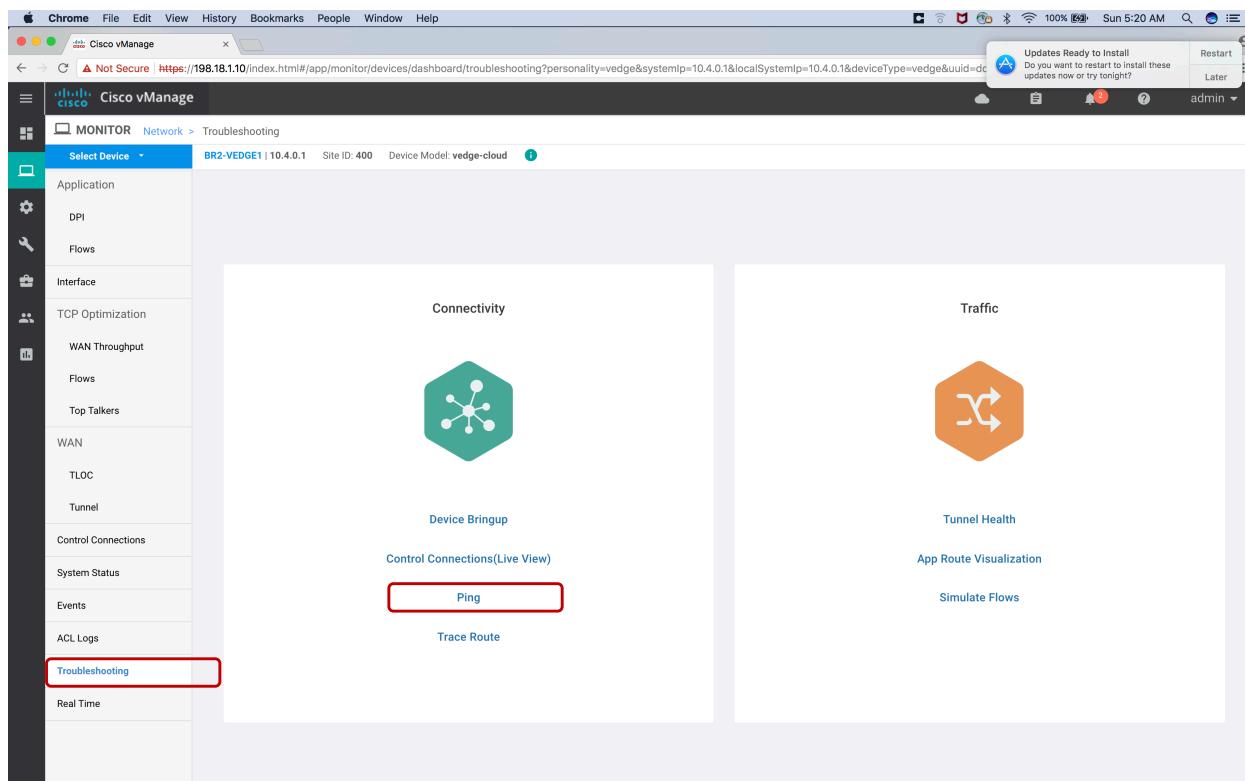
# Lab 09 - Application Firewalling using Centralized Policies

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.

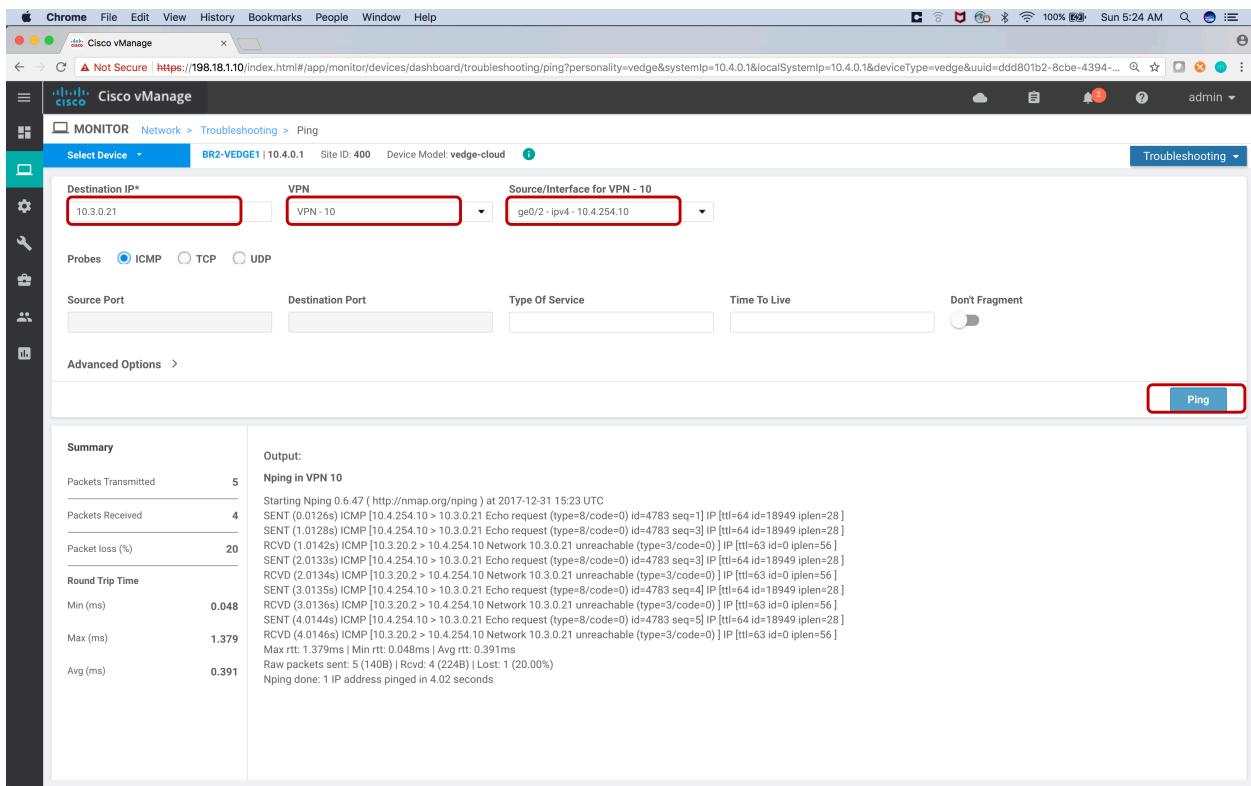
This policy will be implemented as a centralized data policy where based on source and destination prefix match, traffic between BR1 and BR2 is dropped. More granular matches can be done to limit certain applications and allow other applications to flow between the Branches.

## 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).



The screenshot shows the Cisco vManage interface under the MONITOR > Troubleshooting > Ping section. The device selected is BR2-VEDGE1 (10.4.0.1). The destination IP is set to 10.3.0.21, the VPN is set to VPN - 10, and the source/Interface is set to ge0/2 - ipv4 - 10.4.254.10. The 'Ping' button is highlighted with a red box.

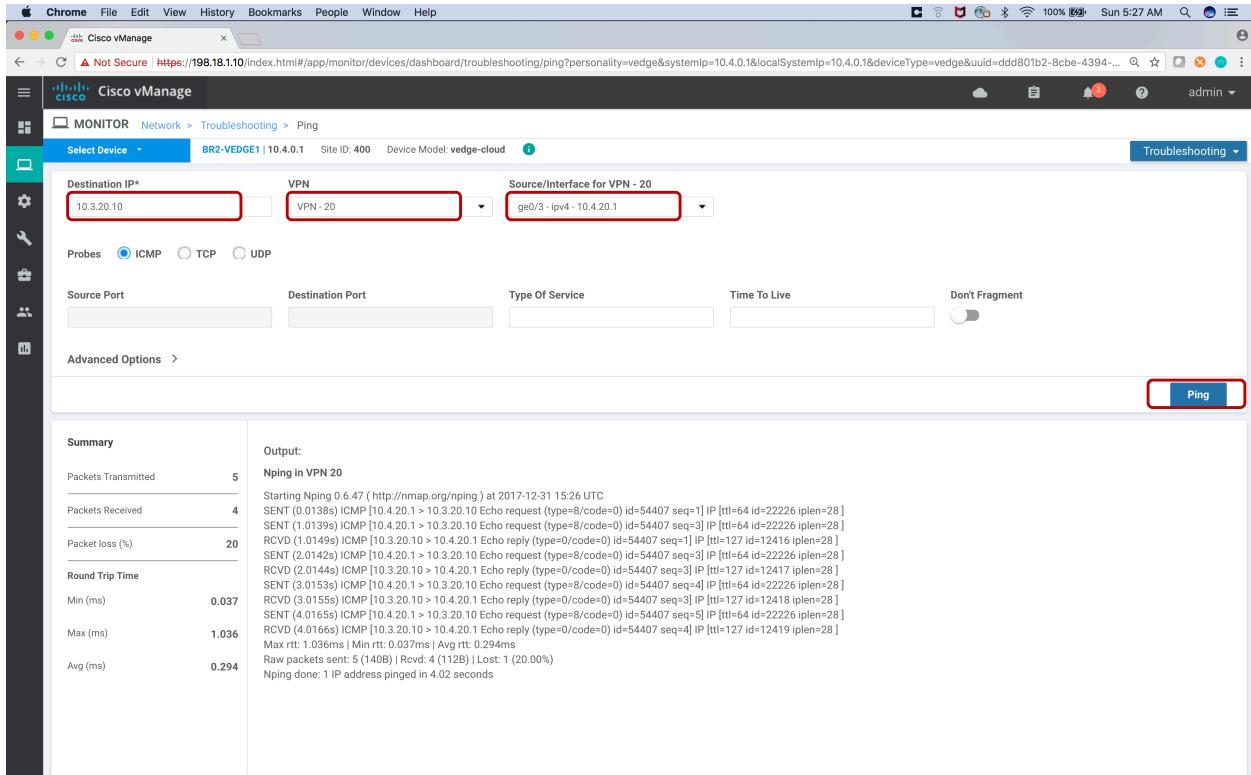
**Summary**

	Output:
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 (4.0145s) 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).



The screenshot shows the Cisco vManage interface under the MONITOR > Troubleshooting > Ping section. The device selected is BR2-VEDGE1 (10.4.0.1). The destination IP is set to 10.3.20.10, the VPN is set to VPN - 20, and the source/Interface is set to ge0/3 - ipv4 - 10.4.20.1. The 'Ping' button is highlighted with a red box.

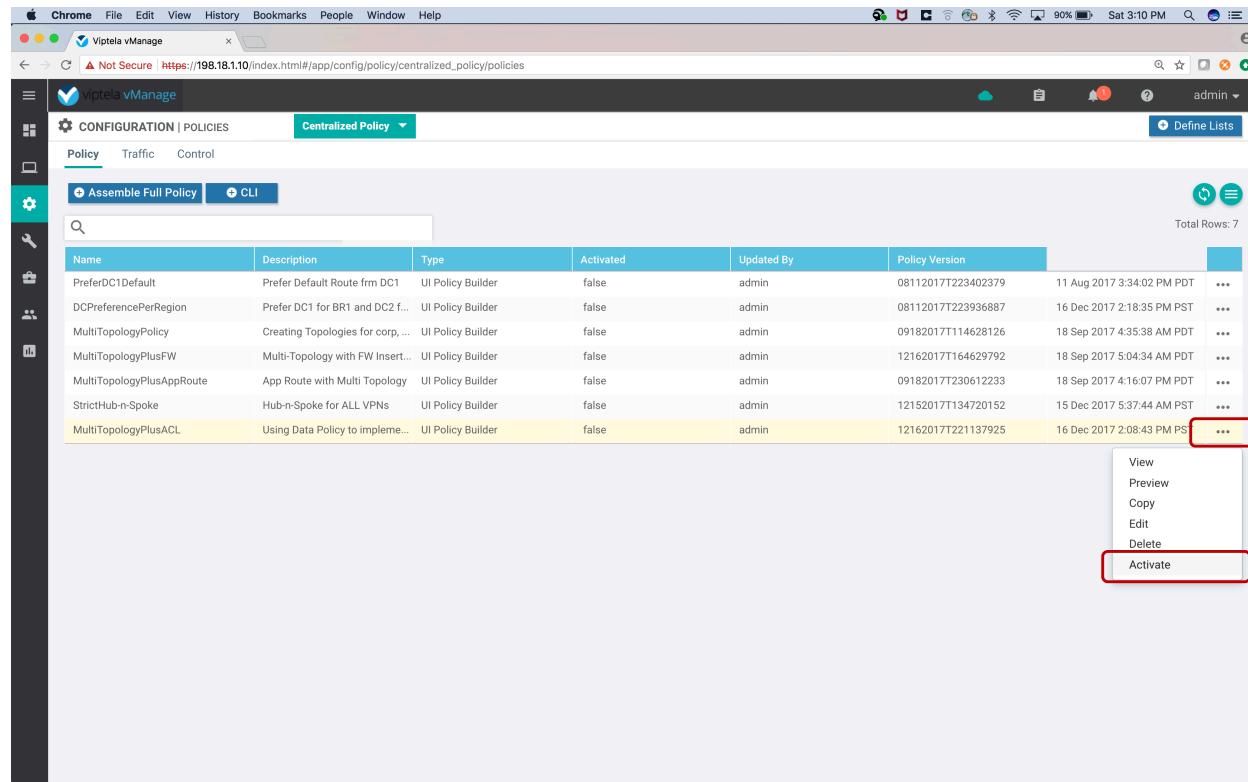
**Summary**

	Output:
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:**

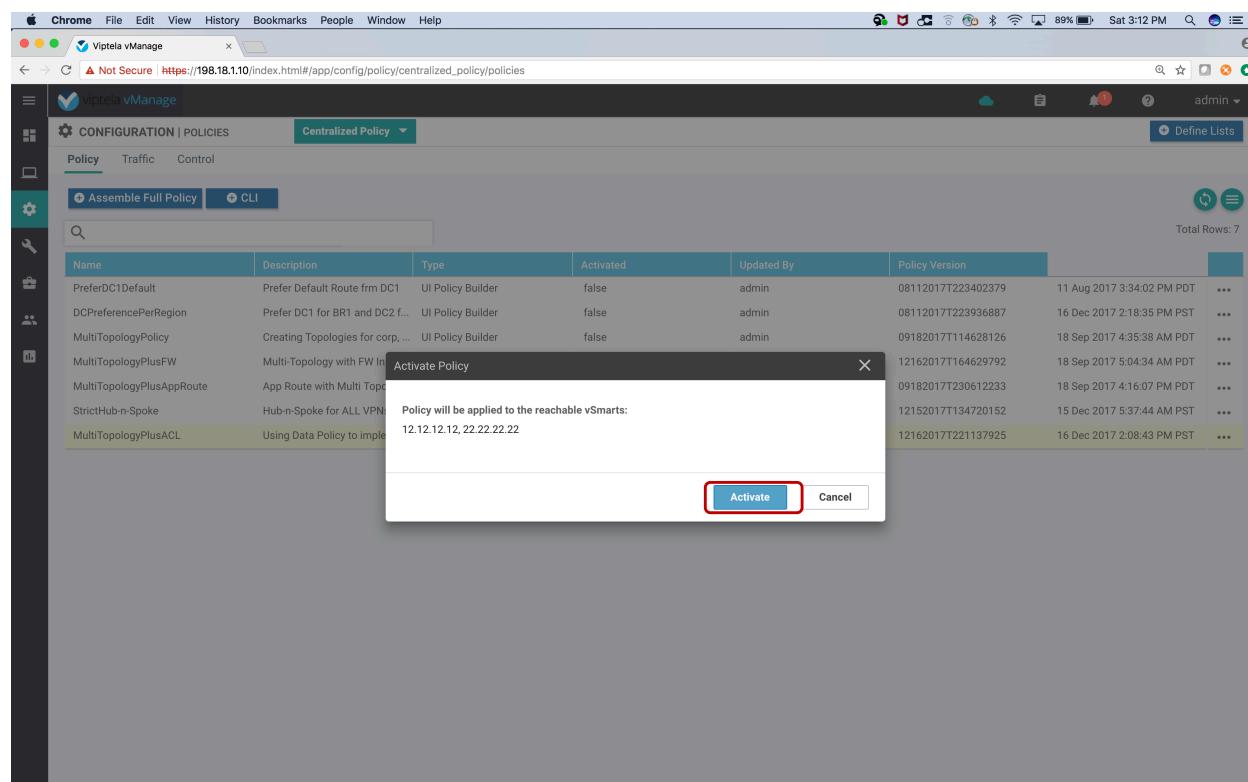
```
Nping in VPN 20
Starting Nping 0.6.47 ( http://nmap.org/nping ) at 2017-12-31 15:26 UTC
SENT (0.0138s) ICMP [10.4.20.1 > 10.3.20.10 Echo request (type=8/code=0) id=54407 seq=1] IP [ttl=64 id=22226 iplen=28]
SENT (1.0139s) ICMP [10.4.20.1 > 10.3.20.10 Echo request (type=8/code=0) id=54407 seq=3] IP [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=4] 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”.



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 ...	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	09182017T230612233	18 Sep 2017 4:16:07 PM PDT
StrictHub-n-Spoke	Hub-n-Spoke for ALL VPNs	UI Policy Builder	false	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 2:08:43 PM PST

Click the “Activate” button.



Activate Policy

Policy will be applied to the reachable vSmarts:

12.12.12.12, 22.22.22.22

**Activate**   **Cancel**

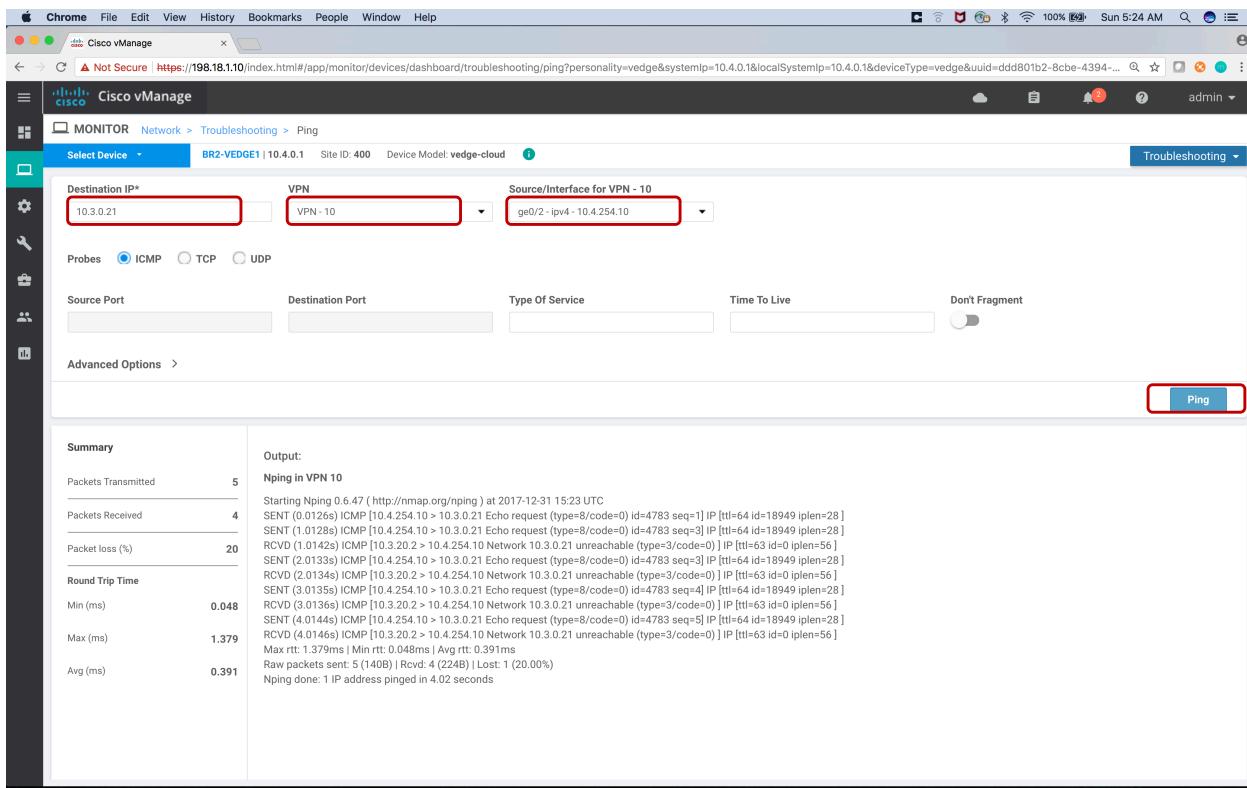
Wait till the policy is pushed successfully pushed to both the vSmarts.

The screenshot shows a browser window for 'Viptela vManage' at the URL [https://198.18.1.10/index.html#/app/device/status?activity=vsmart\\_policy\\_config&pid=vsmart\\_policy\\_config-2275154c-97ab-4862-acc6-8a8a255909be](https://198.18.1.10/index.html#/app/device/status?activity=vsmart_policy_config&pid=vsmart_policy_config-2275154c-97ab-4862-acc6-8a8a255909be). The title bar indicates 'Not Secure'. The main interface shows a 'TASK VIEW' section with the message 'Push vSmart Policy | Validation Success'. It displays a table with two rows, both marked as 'Success'. The table columns are Status, Message, Hostname, System IP, and Site ID. The first row corresponds to vSmart-1 and the second to vSmart-2. A red box highlights the 'Status' column header in the table.

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

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 interface under the MONITOR > Troubleshooting > Ping section. The device selected is BR2-VEDGE1 (Site ID: 400, Device Model: vedge-cloud). The configuration for the ping test is as follows:

- Destination IP\*: 10.3.0.20.1
- VPN: VPN - 10
- Source/Interface for VPN - 10: ge0/2 - ipv4 - 10.4.254.10
- Probes: ICMP (selected)
- Source Port, Destination Port, Type Of Service, Time To Live, and Don't Fragment options are present but not explicitly set.
- Advanced Options button is visible.
- Ping button is highlighted with a red border.

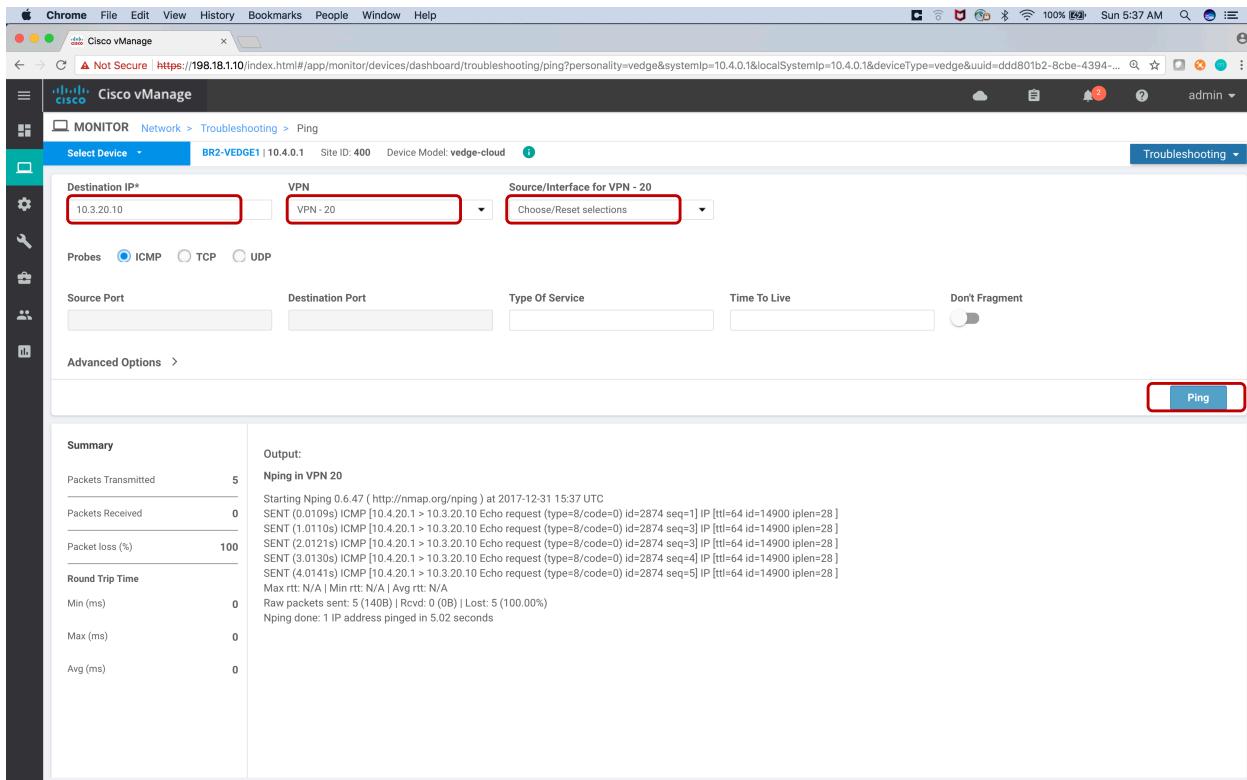
The summary table shows the results of the ping test:

Summary		Output:
Packets Transmitted	5	Nping in VPN 10
Packets Received	4	Starting Nping 0.6.47 ( http://nmap.org/nping ) at 2017-12-31 15:23 UTC
Packet loss (%)	20	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]
Round Trip Time		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]
Min (ms)	0.048	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]
Max (ms)	1.379	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]
Avg (ms)	0.391	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]

The output log shows the ICMP echo requests and responses between the vedge and the host in Branch3.

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 interface under the MONITOR > Troubleshooting > Ping section. The device selected is BR2-VEDGE1 (Site ID: 400, Device Model: vedge-cloud). The configuration for the ping test 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, Destination Port, Type Of Service, Time To Live, and Don't Fragment options are present but not explicitly set.
- Advanced Options button is visible.
- Ping button is highlighted with a red border.

The summary table shows the results of the ping test:

Summary		Output:
Packets Transmitted	5	Nping in VPN 20
Packets Received	0	Starting Nping 0.6.47 ( http://nmap.org/nping ) at 2017-12-31 15:37 UTC
Packet loss (%)	100	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]
Round Trip Time		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]
Min (ms)	0	SENT (2.0111s) 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]
Max (ms)	0	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]
Avg (ms)	0	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]

The output log shows the ICMP echo requests being sent from the vedge but failing to receive any responses, indicating a blocked connection.

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.

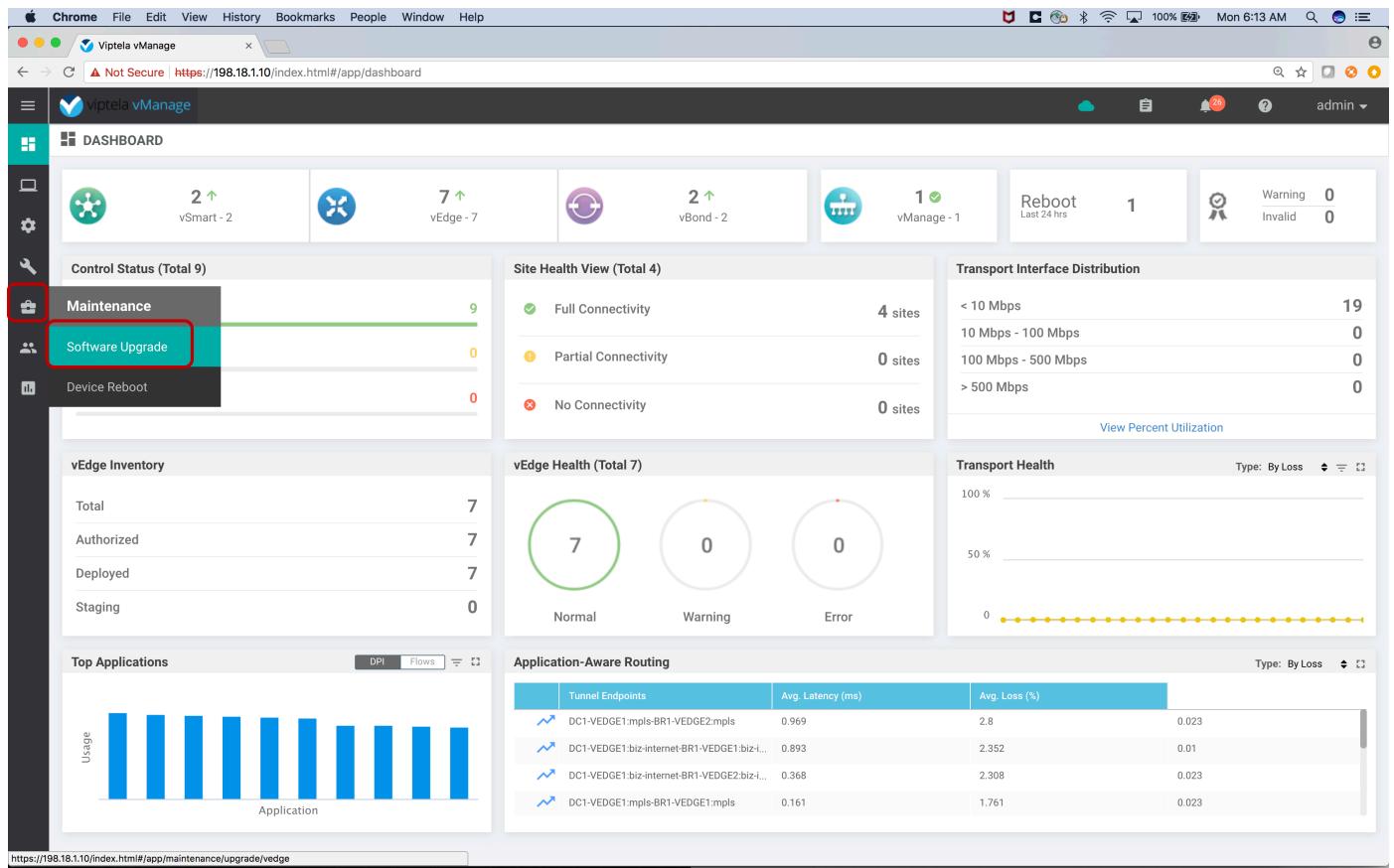
Methodology for upgrading the Cisco SD-WAN

- 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 with the following details:

- Maintenance:**
  - Software Upgrade** (highlighted with a red box)
  - Device Reboot**
- Control Status (Total 9):**
  - Maintenance**: 9
  - Software Upgrade**: 0
  - Device Reboot**: 0
- Site Health View (Total 4):**
  - Full Connectivity**: 4 sites
  - Partial Connectivity**: 0 sites
  - No Connectivity**: 0 sites
- Transport Interface Distribution:**

Bandwidth Range	Count
< 10 Mbps	19
10 Mbps - 100 Mbps	0
100 Mbps - 500 Mbps	0
> 500 Mbps	0
- vEdge Inventory:**

Status	Count
Total	7
Authorized	7
Deployed	7
Staging	0
- vEdge Health (Total 7):**

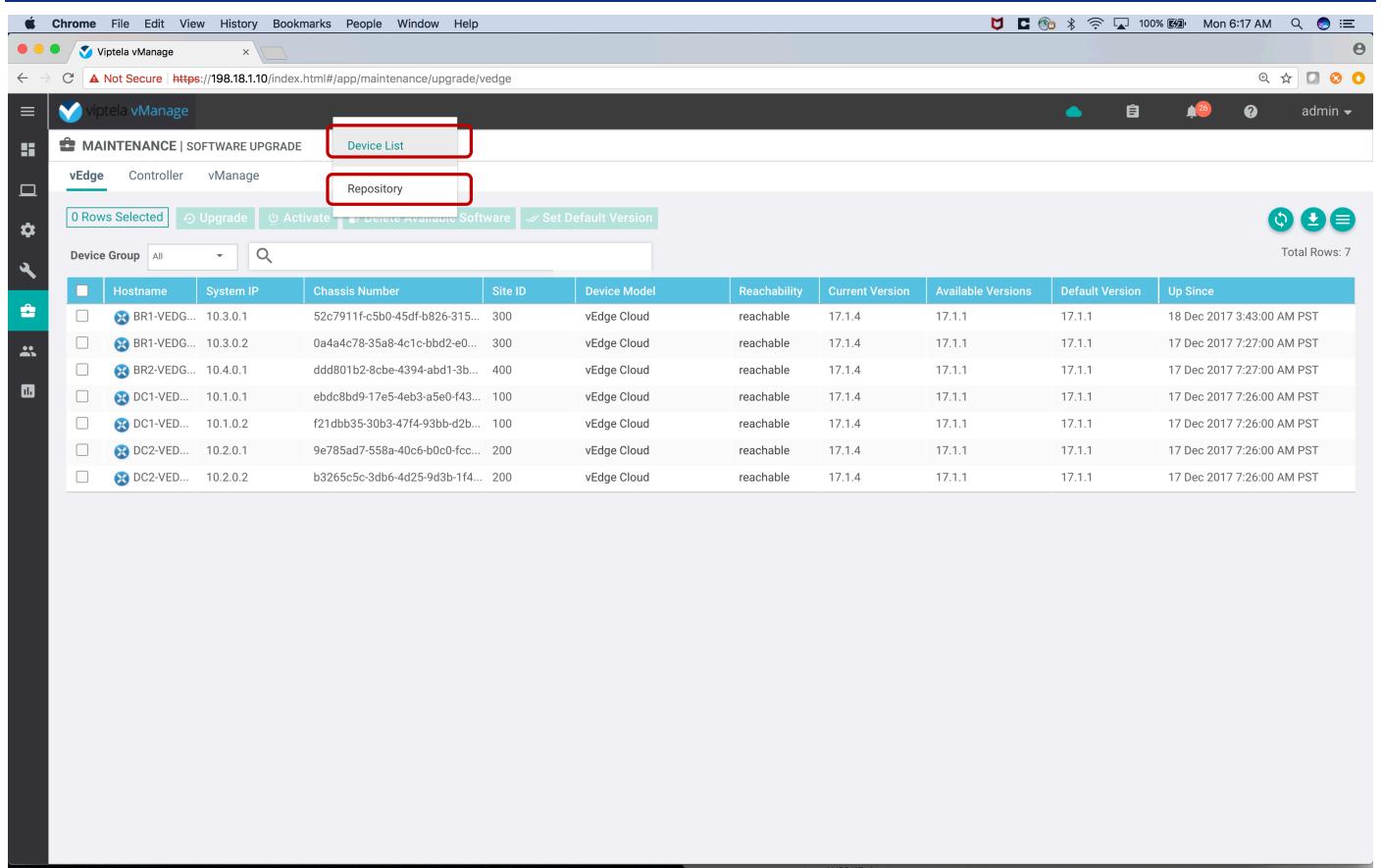
Status	Count
Normal	7
Warning	0
Error	0
- Transport Health:**

Type: By Loss

Graph showing transport utilization over time.
- Application-Aware Routing:**

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)
DC1-VEDGE1.mpls-BR1-VEDGE2.mpls	0.969	2.8
DC1-VEDGE1.biz-internet-BR1-VEDGE1.biz.i...	0.893	2.352
DC1-VEDGE1.biz-internet-BR1-VEDGE2.biz.i...	0.368	2.308
DC1-VEDGE1.mpls-BR1-VEDGE1.mpls	0.161	1.761

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



The screenshot shows the Viptela vManage software upgrade interface. At the top, there's a navigation bar with links like Chrome, File, Edit, View, History, Bookmarks, People, Window, Help, and a search bar indicating 'Not Secure https://198.18.1.10/index.html#/app/maintenance/upgrade/vedge'. Below the header, the main title is 'MAINTENANCE | SOFTWARE UPGRADE' with tabs for 'Device List' (highlighted with a red box) and 'Repository' (also highlighted with a red box). A toolbar below these tabs includes buttons for 'Upgrade', 'Activate', 'Delete Available Software', and 'Set Default Version'. On the left, a sidebar contains icons for Home, Devices, Network, Security, and Analytics. The central part of the screen displays a table titled 'Device Group' with a single row selected. The table columns are: Hostname, System IP, Chassis Number, Site ID, Device Model, Reachability, Current Version, Available Versions, Default Version, and Up Since. The data in the table is as follows:

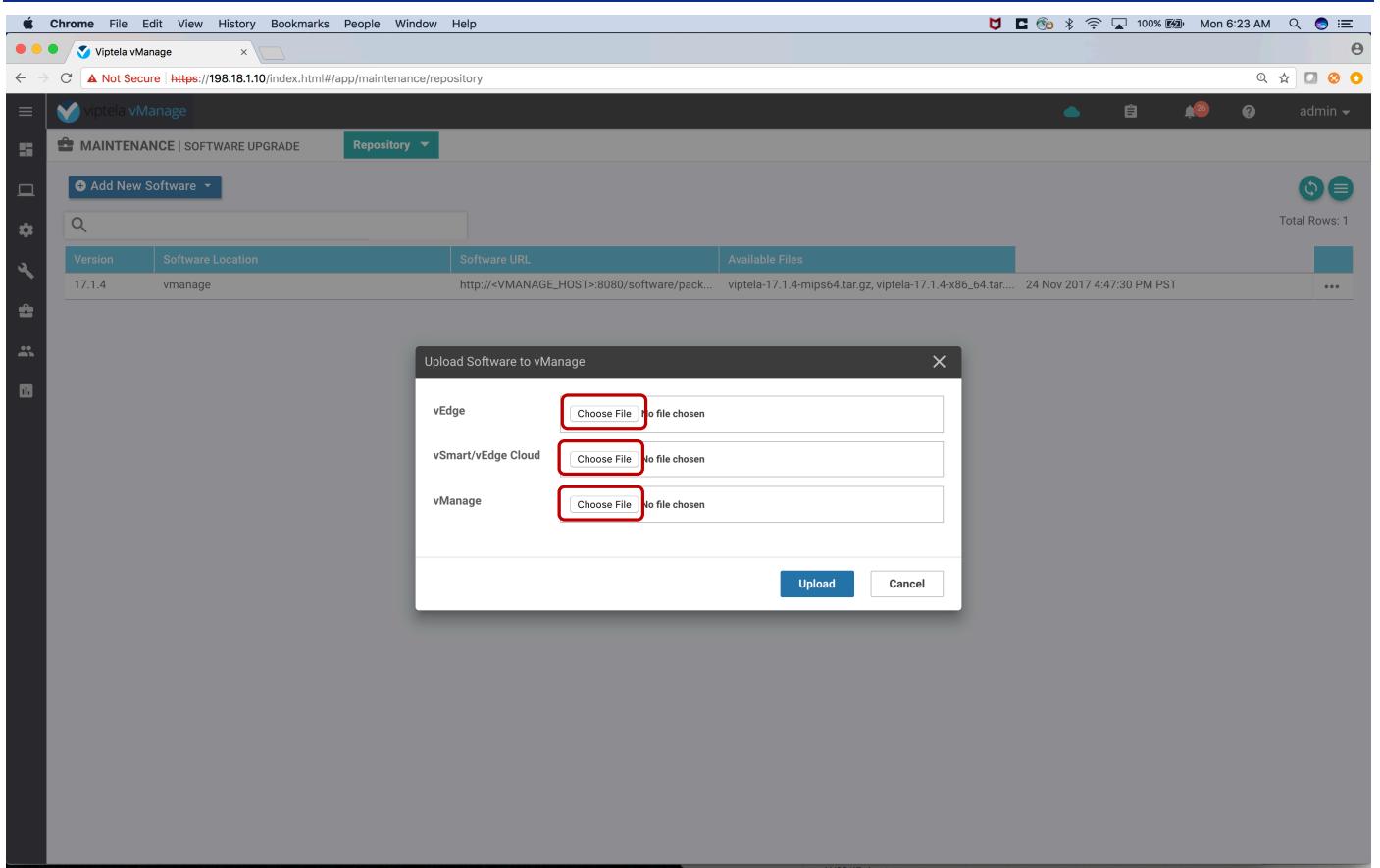
	Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability	Current Version	Available Versions	Default Version	Up Since
<input type="checkbox"/>	BR1-VEDG...	10.3.0.1	52c7911f-c5b0-45df-b826-315...	300	vEdge Cloud	reachable	17.1.4	17.1.1	17.1.1	18 Dec 2017 3:43:00 AM PST
<input type="checkbox"/>	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.

The screenshot shows a web browser window for 'Viptela vManage' on a Mac OS X desktop. The title bar indicates it's not secure (https://198.18.1.10/index.html#/app/maintenance/repository). The main content area is titled 'MAINTENANCE | SOFTWARE UPGRADE' and 'Repository'. A red box highlights the 'Add New Software' button. Below it, a table lists one item: 'vManage' (Version 17.1.4, Software Location 'vmanage'). The table has columns for Version, Software Location, Software URL, Available Files, and Date. The date shown is 24 Nov 2017 4:47:30 PM PST. A 'Total Rows: 1' message is visible on the right. The left sidebar contains various icons for system management.

Version	Software Location	Software URL	Available Files	Date
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

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



The screenshot shows the Cisco vManage web interface. The top navigation bar includes 'File', 'Edit', 'View', 'History', 'Bookmarks', 'People', 'Window', and 'Help'. The title bar says 'Viptela vManage'. A message 'Not Secure https://198.18.1.10/index.html#/app/maintenance/repository' is displayed. The main content area has a sidebar with icons for 'MAINTENANCE | SOFTWARE UPGRADE', 'Repository', and other management functions. The 'Repository' tab is selected, showing a table with one row:

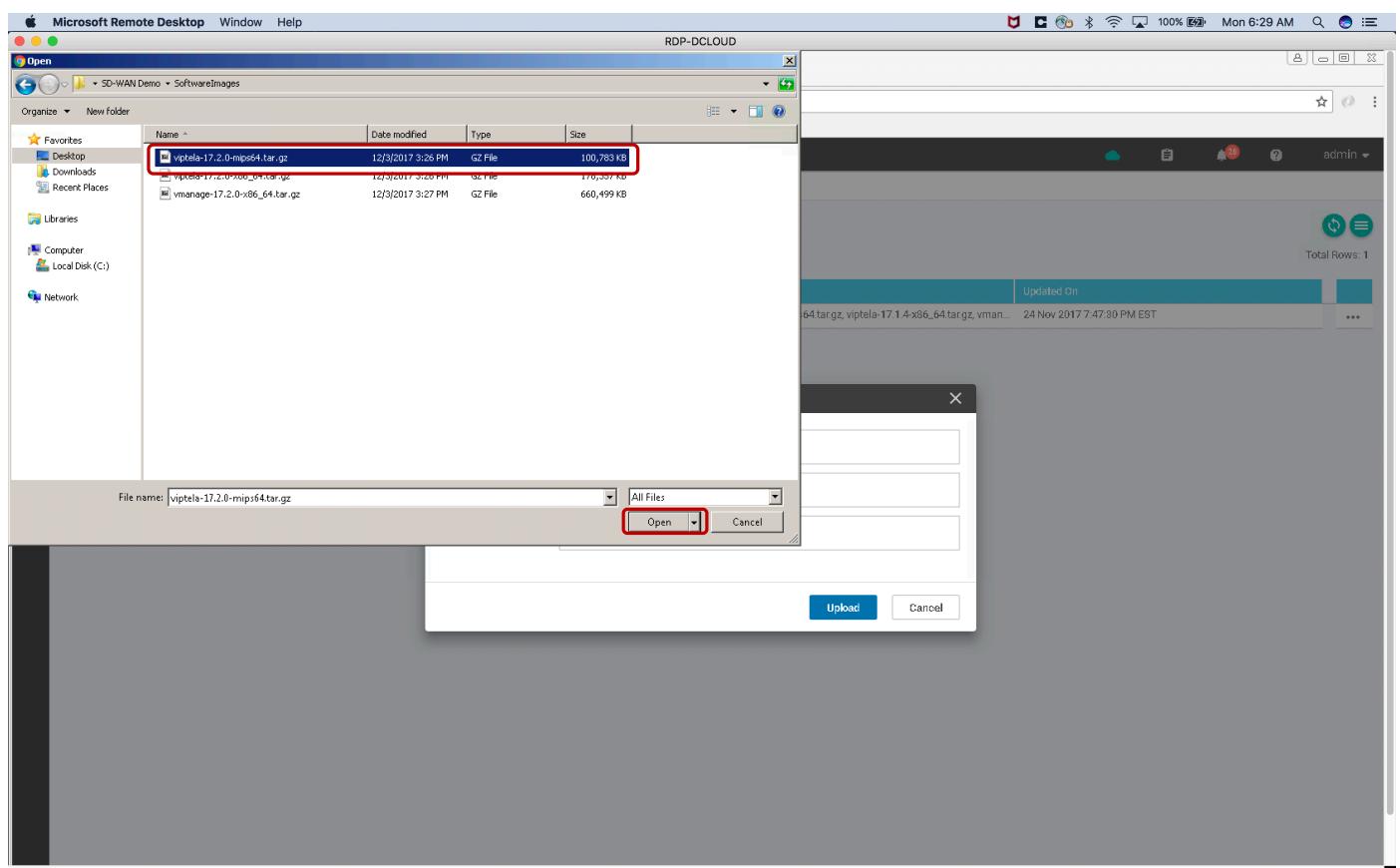
Version	Software Location	Software URL	Available Files	Date
17.1.4	vmanage	http://<VMANAGE_HOST>:8080/software/pack...	viptela-17.1.4-mips64.tar.gz, viptela-17.1.4-x86_64.tar...	24 Nov 2017 4:47:30 PM PST

A modal dialog box titled 'Upload Software to vManage' is open in the center. It lists three categories: 'vEdge', 'vSmart/vEdge Cloud', and 'vManage'. Each category has a 'Choose File' button with the message 'No file chosen'. At the bottom of the dialog are 'Upload' and 'Cancel' buttons.

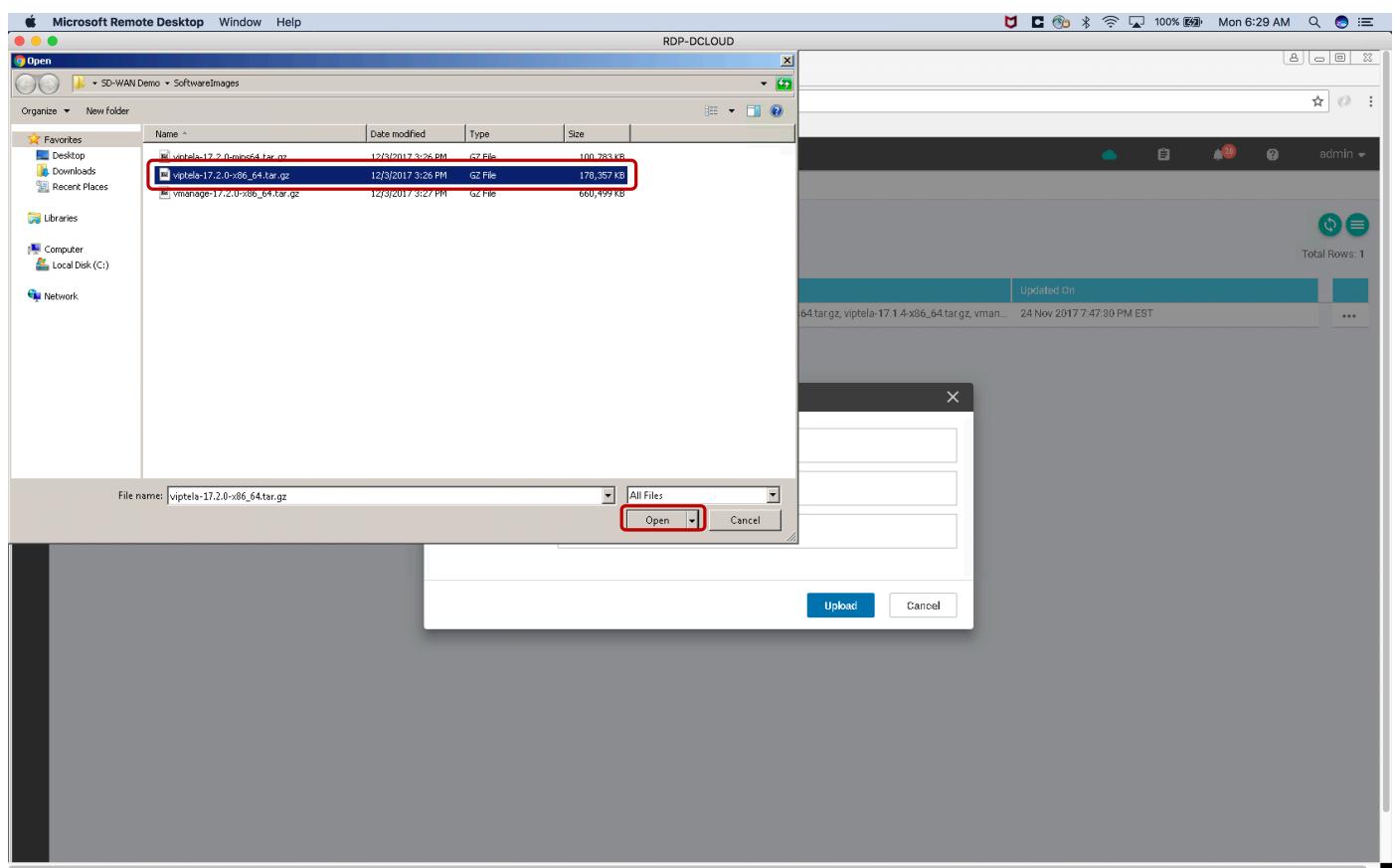
The software images are in the folder \Desktop\SD-WAN Demo\SoftwareImages.

Select the following files for each and click on “Open” tab.

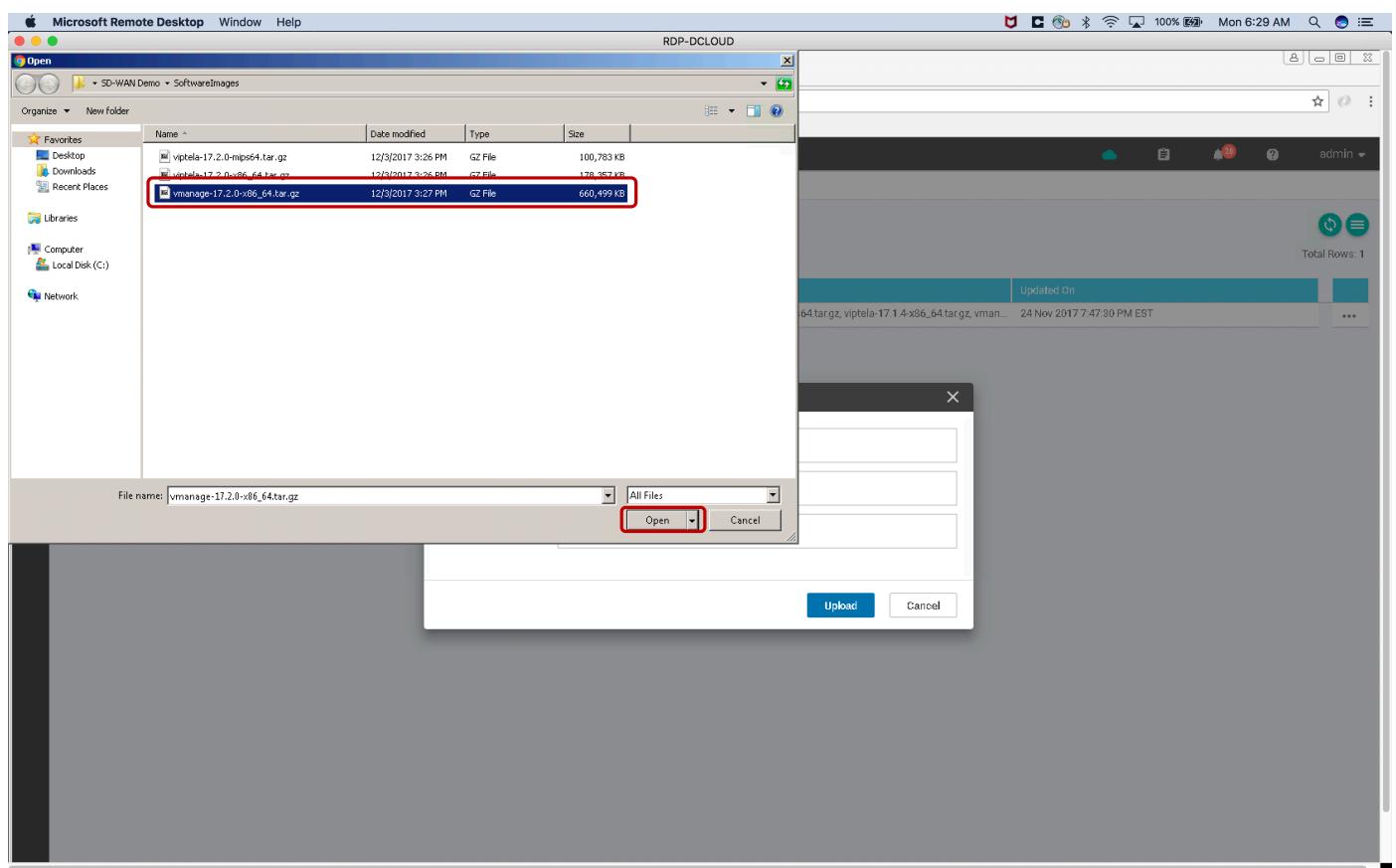
For vEdge (select the mips file):



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



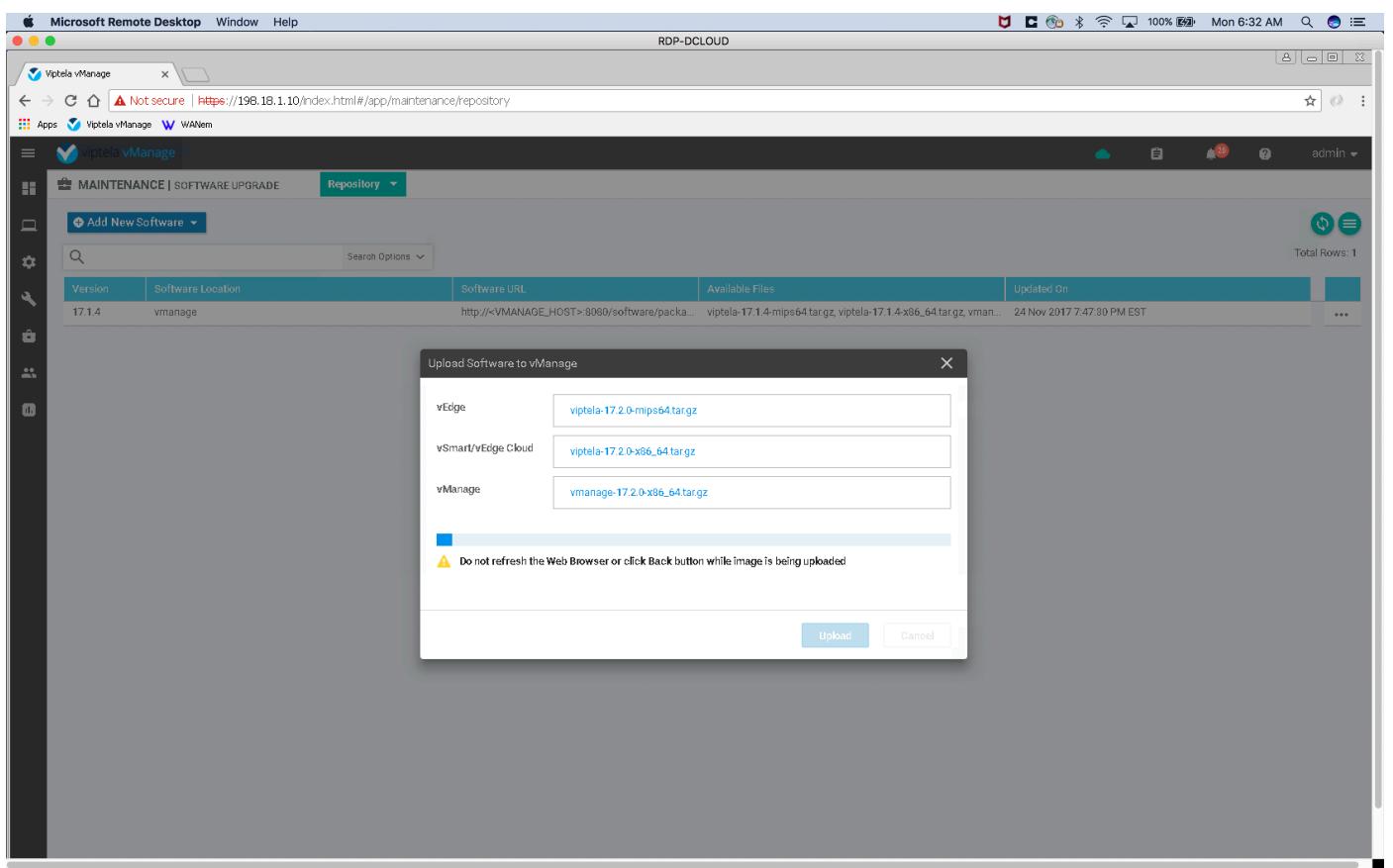
For vManage (select vManage file):



On the next screen, click on Update.

The screenshot shows a Microsoft Remote Desktop session for 'RDP-DCLOUD'. The browser window is titled 'Viptela vManage' and displays the 'MAINTENANCE | SOFTWARE UPGRADE' page. A modal dialog box titled 'Upload Software to vManage' is open, prompting for software files for vEdge, vSmart/vEdge Cloud, and vManage. The 'vEdge' field contains 'Choose File viptela-17.2.0-mips64.tar.gz'. The 'vSmart/vEdge Cloud' field contains 'Choose File viptela-17.2.0-x86\_64.targz'. The 'vManage' field contains 'Choose File vmanage-17.2.0-x86\_64.targz'. The 'Upload' button at the bottom of the modal is highlighted with a red box.

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



The screenshot shows a Microsoft Remote Desktop session for 'RDP-DCLOUD'. The browser window is titled 'Viptela vManage' and displays the 'MAINTENANCE | SOFTWARE UPGRADE' page. The 'Repository' tab is selected. A table lists one software entry:

Version	Software Location	Software URL	Available Files	Updated On
17.1.4	vmanage	http://<VMANAGE_HOST>:8080/software/packa...	vptela-17.1.4-mips64.targz, vptela-17.1.4-x86_64.targz, vman...	24 Nov 2017 7:47:30 PM EST

A modal window titled 'Upload Software to vManage' is overlaid on the page. It contains three dropdown menus corresponding to the categories in the table: vEdge, vSmart/vEdge Cloud, and vManage. Each menu lists the same three files: vptela-17.2.0-mips64.targz, vptela-17.2.0-x86\_64.targz, and vmange-17.2.0-x86\_64.targz. At the bottom of the modal, there is a warning message: 'Do not refresh the Web Browser or click Back button while image is being uploaded'.

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

The screenshot shows a Microsoft Remote Desktop session for the Cisco vManage application. The title bar indicates the session is titled "RDP-DCLOUD". The main window displays the "MAINTENANCE | SOFTWARE UPGRADE" section under the "Repository" tab. A green success message at the top right states "Software images uploaded successfully". Below this, a table lists two software versions:

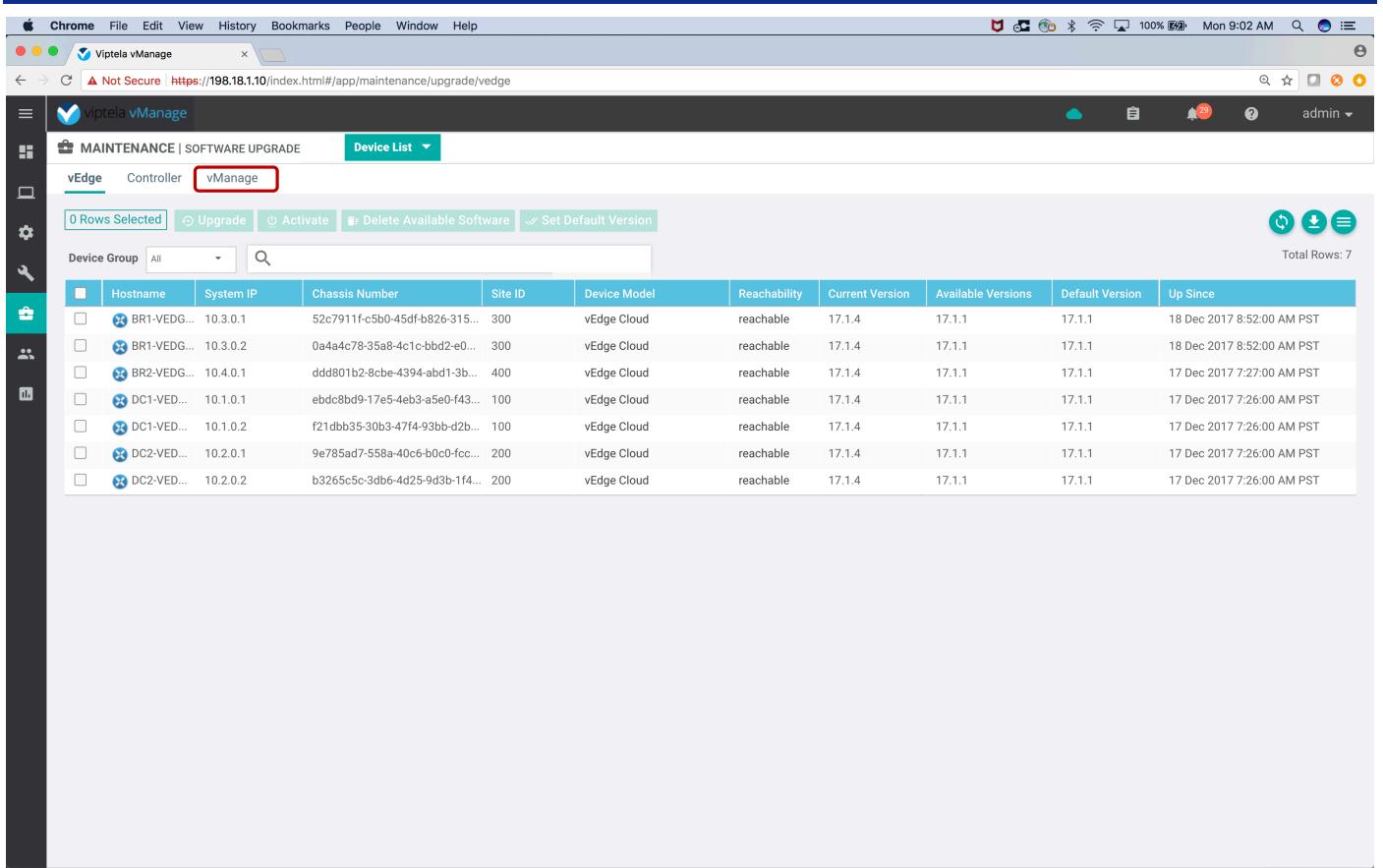
Version	Software Location	Software URL	Available Files	Updated On
17.2.0	vmanage	http://<VMANAGE_HOST>:8080/software/packa... http://<VMANAGE_HOST>:8080/software/packa...	viptela-17.2.0-mips64.targz, viptela-17.2.0-x86_64.targz, vman...	18 Dec 2017 9:33:18 AM EST
17.1.4	vmanage	http://<VMANAGE_HOST>:8080/software/packa... http://<VMANAGE_HOST>:8080/software/packa...	viptela-17.1.4-mips64.targz, viptela-17.1.4-x86_64.targz, vman...	24 Nov 2017 7:47:30 PM EST

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

The screenshot shows a web browser window for Viptela vManage. The title bar says "Viptela vManage". The address bar shows "Not Secure https://198.18.1.10/index.html#/app/maintenance/repository". The main interface has a sidebar with icons for Home, Devices, Configuration, Monitoring, Analytics, and Help. The top navigation bar includes "Device List" (highlighted with a red box), "Repository", and "Total Rows: 2". A search bar is present. The main content area is a table with the following data:

Version	Software Location	Software URL	Available Files	Date	Action
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 Viptela vManage interface for a software upgrade. The top navigation bar includes 'File', 'Edit', 'View', 'History', 'Bookmarks', 'People', 'Window', and 'Help'. The title bar says 'Viptela vManage'. The address bar shows 'Not Secure https://198.18.1.10/index.html#/app/maintenance/upgrade/vedge'. The main content area has a header 'MAINTENANCE | SOFTWARE UPGRADE' and a sub-header 'Device List'. A filter dropdown shows 'vEdge' selected. Below is a table with columns: Hostname, System IP, Chassis Number, Site ID, Device Model, Reachability, Current Version, Available Versions, Default Version, and Up Since. The table lists seven devices, all of which are reachable and have version 17.1.4. The 'Up Since' column shows dates from Dec 2017 to Jan 2018. At the bottom of the table is a green 'Upgrade' button.

	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 software upgrade interface. At the top, there's a navigation bar with links like Chrome, File, Edit, View, History, Bookmarks, People, Window, Help, and a search bar indicating 'Not Secure https://198.18.1.10/index.html#/app/maintenance/upgrade/vmanage'. Below the header, the title 'MAINTENANCE | SOFTWARE UPGRADE' and 'Device List' are visible. A toolbar below the title includes buttons for Upgrade (highlighted with a red box), Activate, Delete Available Software, and Set Default Version. On the left, a sidebar has icons for vEdge, Controller, and vManage. The main area displays a table with one row of 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

Total Rows: 1

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

The screenshot shows the Viptela vManage software upgrade interface. The main window displays a device list with one entry: vManage (IP 10.10.10.10). A modal dialog titled "Software Upgrade" is overlaid on the main window. The dialog contains a warning message: "Backup of data volume is highly recommended before upgrading vManage." Below the message, there is a "Version" dropdown menu with two options: "17.2.0" (which is selected and highlighted with a red box) and "17.1.4". At the bottom of the dialog are two buttons: "Upgrade" (highlighted with a red box) and "Cancel".

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

The screenshot shows a web browser window for 'viptela vManage' with the URL [https://198.18.1.10/index.html#/app/device/status?activity=software\\_install&pid=software\\_install~41df2ead-8912-4a3c-a325-c990c1aba87f](https://198.18.1.10/index.html#/app/device/status?activity=software_install&pid=software_install~41df2ead-8912-4a3c-a325-c990c1aba87f). The page title is 'vManage'. The top navigation bar includes 'File', 'Edit', 'View', 'History', 'Bookmarks', 'People', 'Window', and 'Help'. The status bar shows '100% 100% Mon 9:13 AM'. The main content area is titled 'TASK VIEW' and displays a table of software installation tasks. The table has columns: Status, Message, Hostname, System IP, Site ID, Device Type, and Device Model. One row is shown: 'Success' (green icon), 'Done - Software Install', 'vManage', '10.10.10.10', '10', 'vManage', 'vManage'. A search bar and a refresh/cancel icon are at the top of the table. The bottom right corner of the table says 'Total Rows: 1 of 1'. The left sidebar contains icons for Home, Devices, Network, Security, Applications, and Help.

	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.

The screenshot shows the Viptela vManage software upgrade interface. The top navigation bar includes 'File', 'Edit', 'View', 'History', 'Bookmarks', 'People', 'Window', and 'Help'. The address bar shows 'Not Secure https://198.18.1.10/index.html#/app/maintenance/upgrade/vmanage'. The main header has 'vManage' selected in a dropdown menu. Below the header, there are tabs for 'MAINTENANCE | SOFTWARE UPGRADE' and 'Device List'. A sub-header indicates 'vEdge Controller vManage'. There are buttons for 'Upgrade', 'Activate' (which is highlighted with a red box), 'Delete Available Software', and 'Set Default Version'. A search bar and a device group filter ('All') are also present. The main content area displays a table with one row of data:

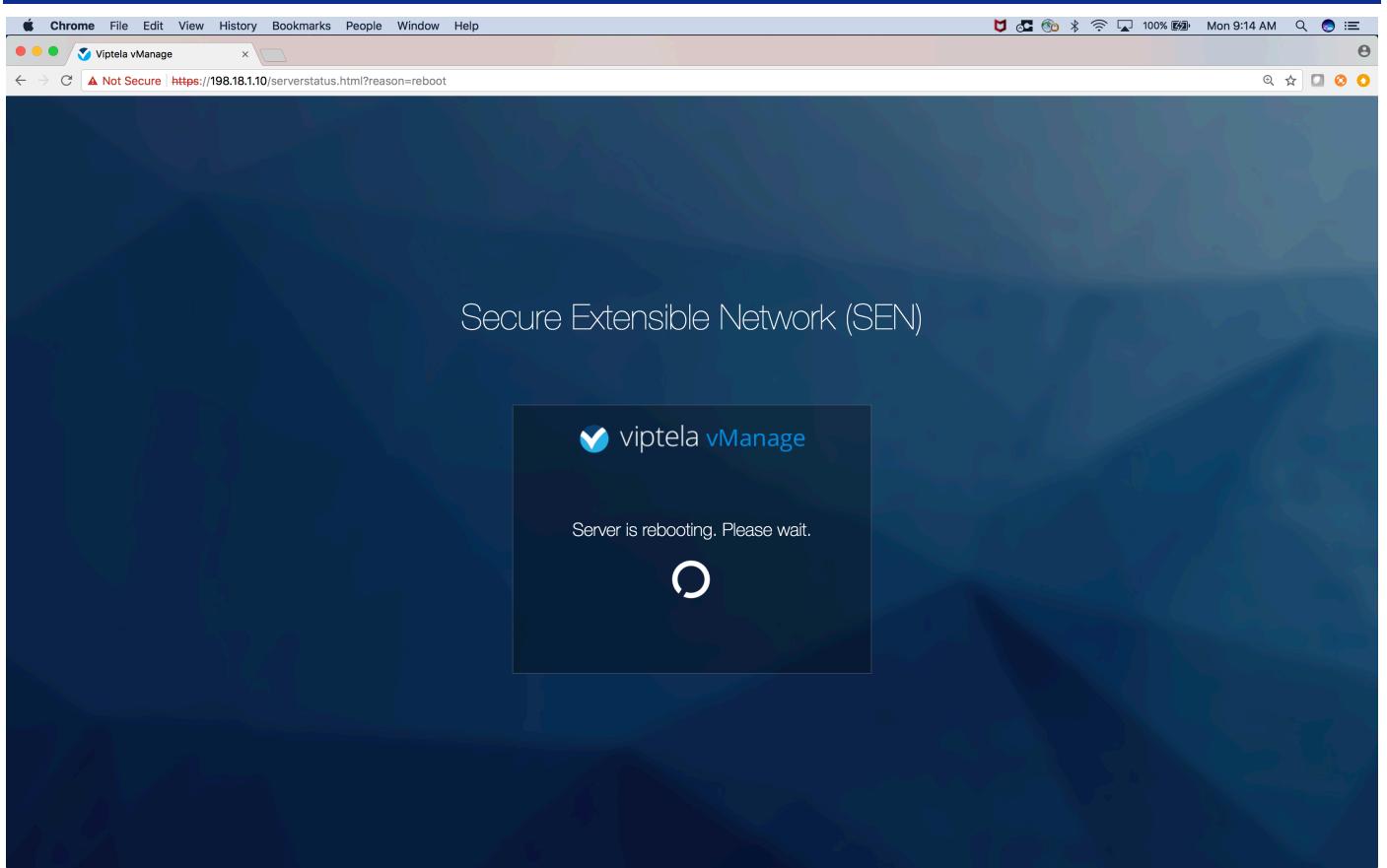
Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability	Current Version	Available Versions	Default Version	
vManage	10.10.10.10	5271ea7c-edb1-420b-be9a-4d...	10	vManage	reachable	17.1.4	17.1.1 17.1.3 17.2.0	17.1.1	17 Dec 2017 7:27:00 AM PST

Total Rows: 1

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

The screenshot shows the Cisco Viptela vManage software upgrade interface. At the top, there's a navigation bar with links like Chrome, File, Edit, View, History, Bookmarks, People, Window, Help, and a search bar indicating the URL is <https://198.18.1.10/index.html#/app/maintenance/upgrade/vmanage>. The main area is titled "MAINTENANCE | SOFTWARE UPGRADE" and shows a "Device List" for "vManage". A table lists one device: vManage (IP 10.10.10.10). Below the table is a "Device Group" dropdown set to "All". A modal dialog box titled "Activate Software" is displayed, containing a warning message: "Activating new version of software on vManage requires a reboot, which will log out all active clients and bring down all control connections." It also shows the selected "Version" as "17.2.0" and two buttons: "Activate" (highlighted with a red box) and "Cancel".

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 right, there is a user menu with 'admin' and a dropdown. A red box highlights the 'About' link in this dropdown menu. The dashboard includes sections for Control Status, Site Health View, Transport Interface Distribution, vEdge Inventory, vEdge Health, Transport Health, Top Applications, and Application-Aware Routing.

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 with the following key components:

- Control Status (Total 9):** Shows Control Up (9), Partial, and Control Down.
- vEdge Inventory:** Shows Total, Authorized, Deployed, and Staging.
- Top Applications:** A bar chart showing Usage by Application.
- Site Health View (Total 4 sites):** Shows Full Connectivity.
- Transport Interface Distribution:** A table showing interface speeds: < 10 Mbps (19), 10 Mbps - 100 Mbps (0), 100 Mbps - 500 Mbps (0), and 500+ Mbps (0).
- Application-Aware Routing:** A table showing Tunnel Endpoints, Avg. Latency (ms), and Avg. Loss (%). The data is as follows:

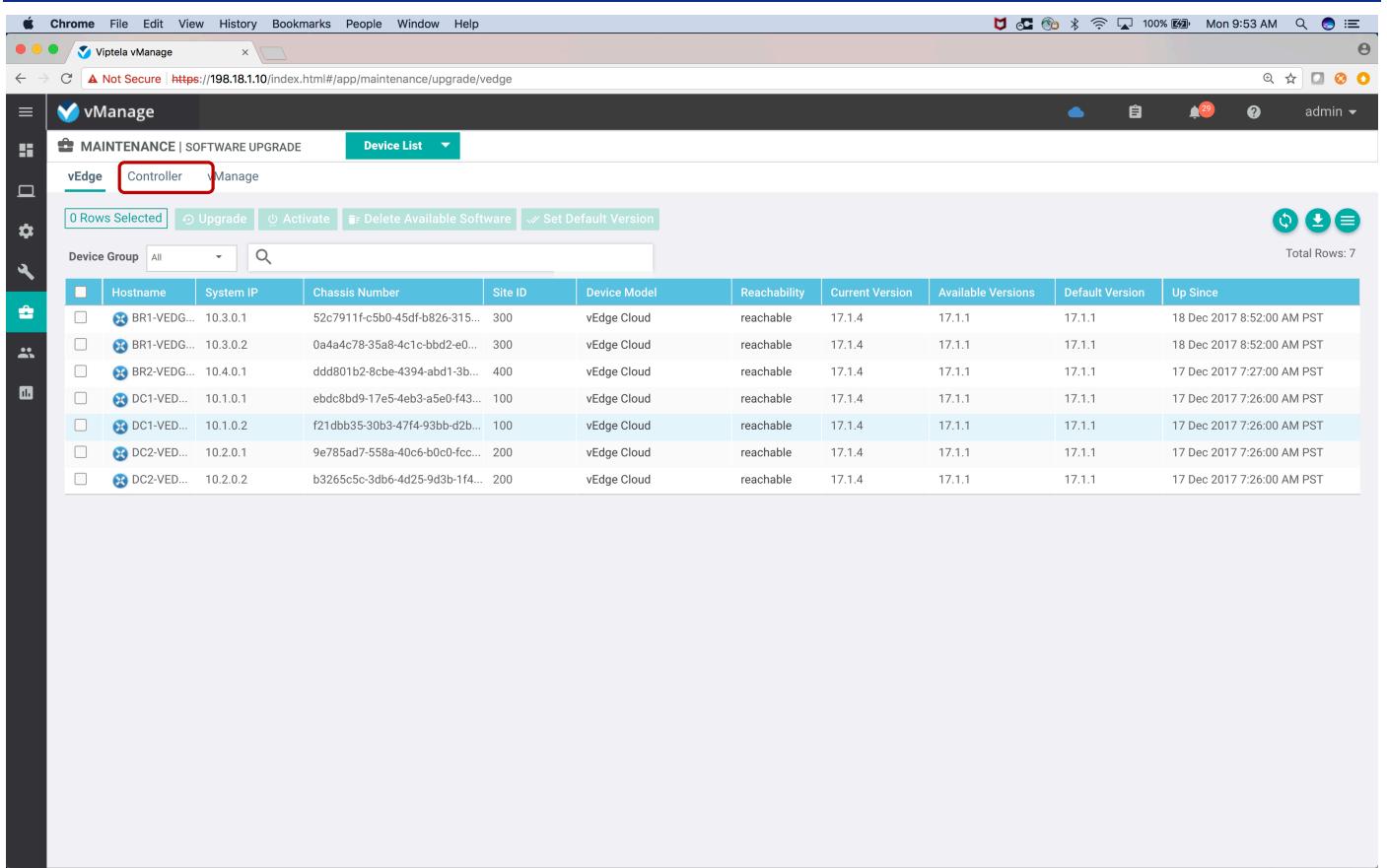
Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)
DC1-VEDGE1:mpls-BR1-VEDGE2:mpls	0.956	2.705
DC1-VEDGE1:biz-internet-BR1-VEDGE2:biz-l...	0.394	2.257
DC1-VEDGE1:biz-internet-BR1-VEDGE1:biz-l...	0.946	1.987
DC1-VEDGE1:mpls-BR1-VEDGE1:mpls	0.368	1.472

A modal dialog box is displayed in the center of the screen, containing the following information:

- Viptela vManage
- 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.

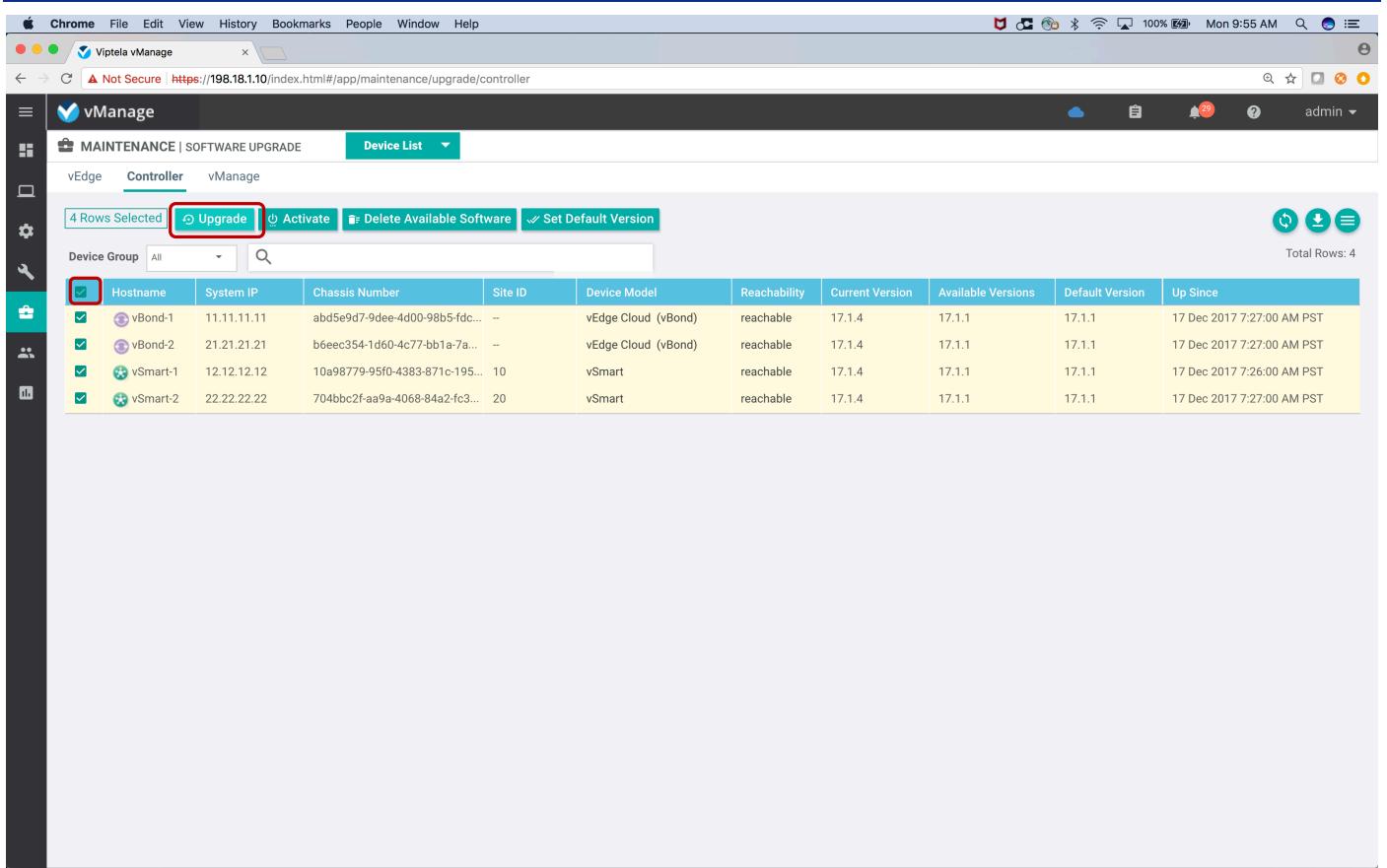
Go to Software Upgrade page and Click on “Controllers” to upgrade vBonds and vSmarts.



The screenshot shows the Viptela vManage interface for maintenance and software upgrade. The main title is "MAINTENANCE | SOFTWARE UPGRADE". A red box highlights the "Controller" tab in the navigation bar. Below it, there are buttons for "Upgrade", "Activate", "Delete Available Software", and "Set Default Version". The table lists seven vEdge controllers with their details:

	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 Viptela vManage interface for maintenance and software upgrade. The top navigation bar includes Chrome, File, Edit, View, History, Bookmarks, People, Window, Help, and a status bar indicating 100% battery, Mon 9:55 AM, and admin.

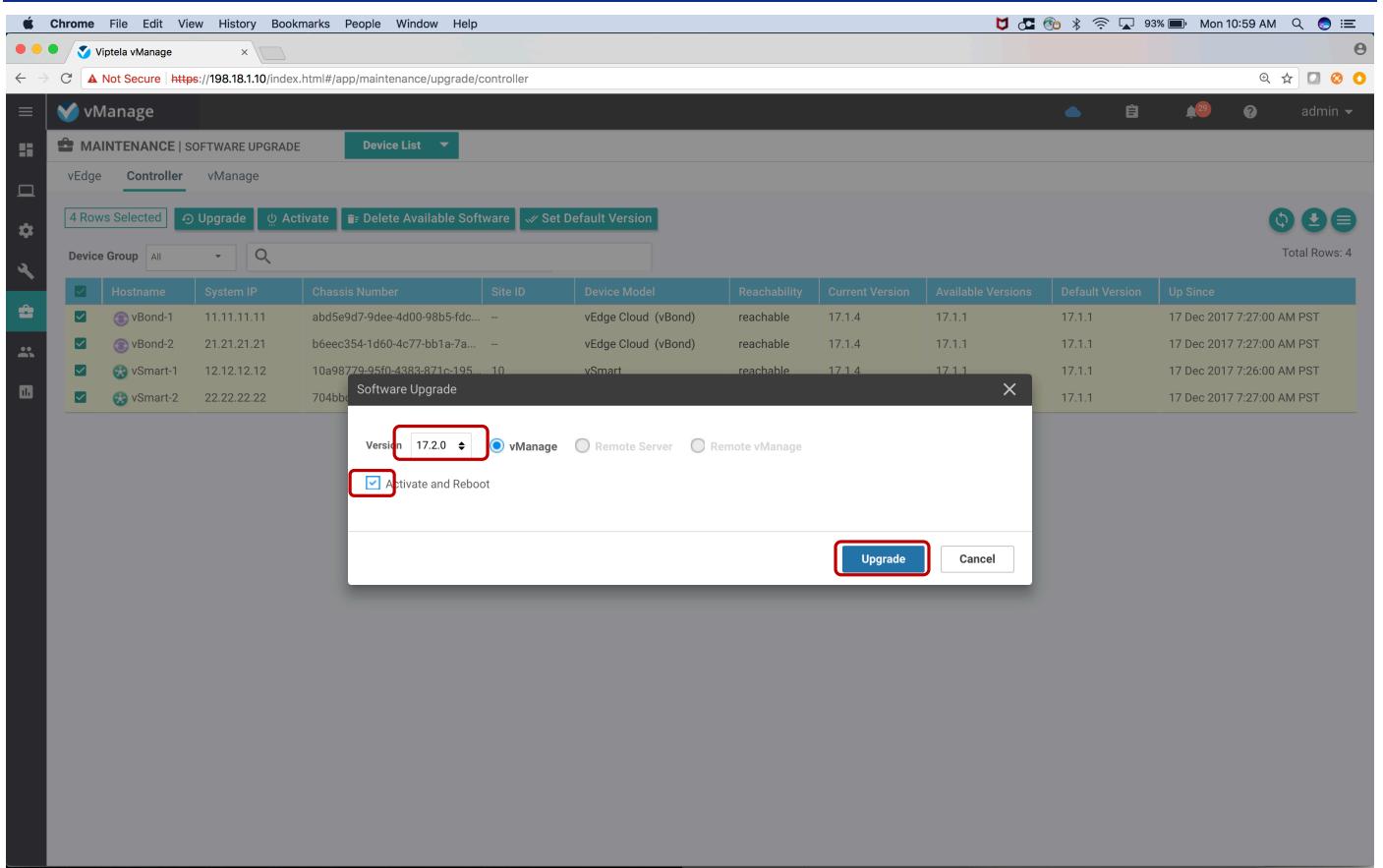
The main title is "vManage" and the sub-section is "MAINTENANCE | SOFTWARE UPGRADE". The "Device List" tab is selected. The left sidebar has icons for vEdge, Controller, vManage, and other management functions.

In the center, a table lists four devices selected for upgrade:

Device Group	Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability	Current Version	Available Versions	Default Version	Up Since
All	vBond-1	11.11.11.11	ab5e9d7-9dee-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	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
	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

At the top of the table, there are buttons for "Upgrade" (highlighted with a red box), "Activate", "Delete Available Software", and "Set Default Version". A message at the bottom right says "Total Rows: 4".

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

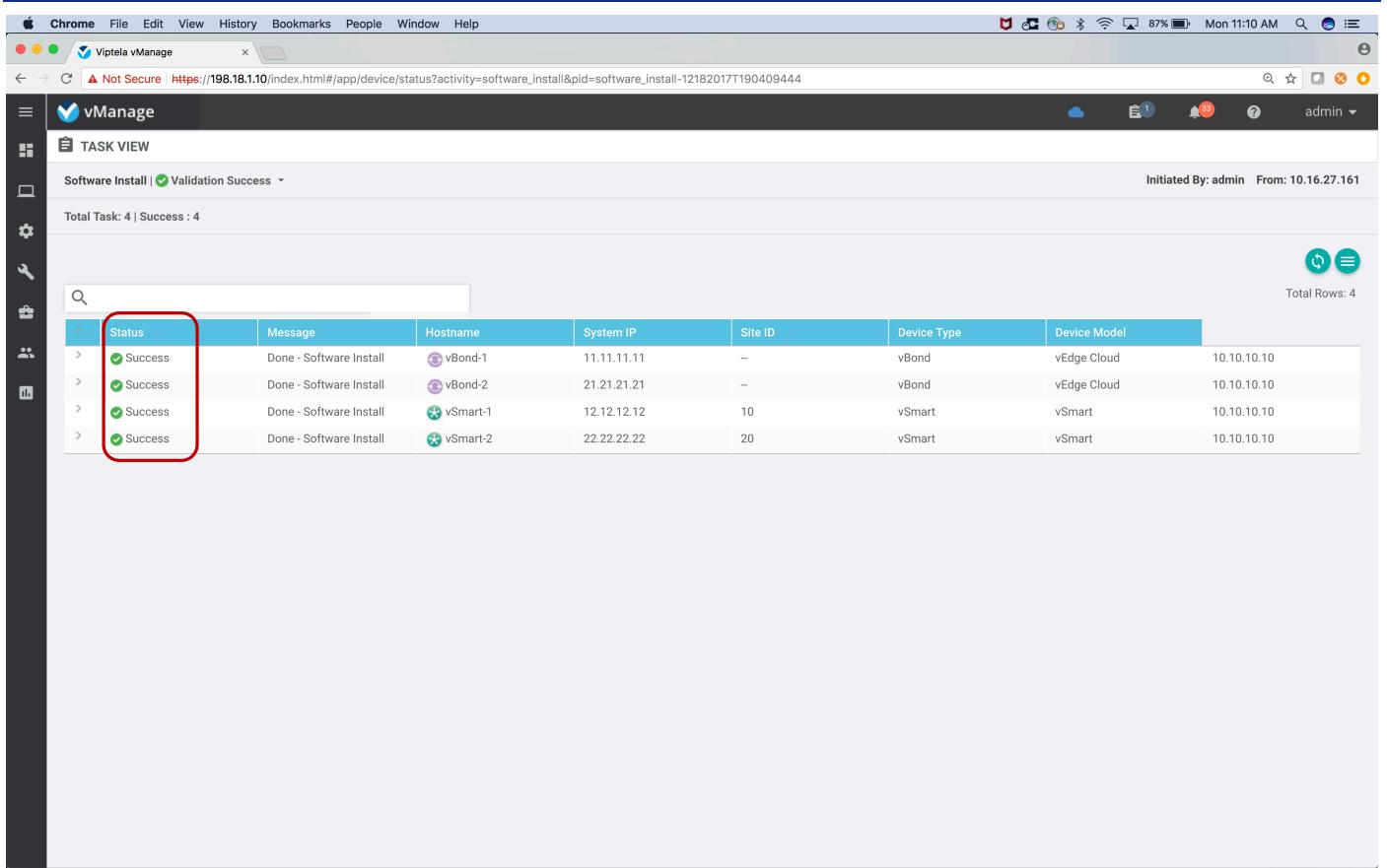


The screenshot shows the vManage software upgrade interface. A modal dialog box is open, prompting for the target version (17.2.0), deployment method (vManage), and whether to activate and reboot the devices. The 'Activate and Reboot' checkbox is checked. The background table lists four devices: vBond-1, vBond-2, vSmart-1, and vSmart-2, all marked for selection.

Device Group	Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability	Current Version	Available Versions	Default Version	Up Since
All	vBond-1	11.11.11.11	ab5e9d7-9dee-4d00-98b5-fdc...	--	vEdge Cloud (vBond)	reachable	17.1.4	17.1.1	17.1.1	17 Dec 2017 7:27:00 AM PST
All	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
All	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
All	vSmart-2	22.22.22.22	70bb...	--	vSmart	reachable	17.1.4	17.1.1	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.

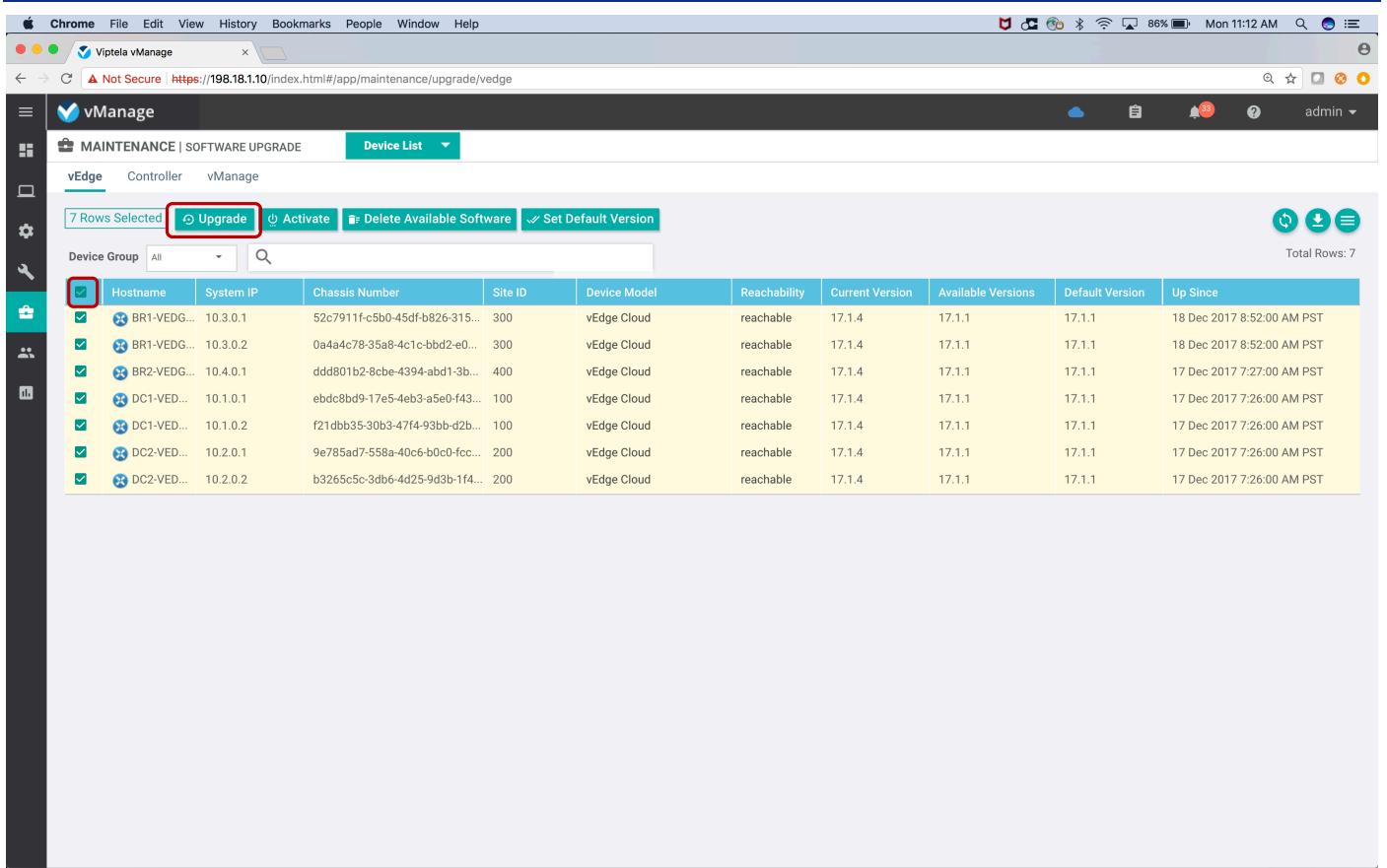


The screenshot shows the Cisco vManage interface with a successful software install task. The task details are as follows:

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

A red box highlights the 'Status' column header and the first four rows of the table.

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.

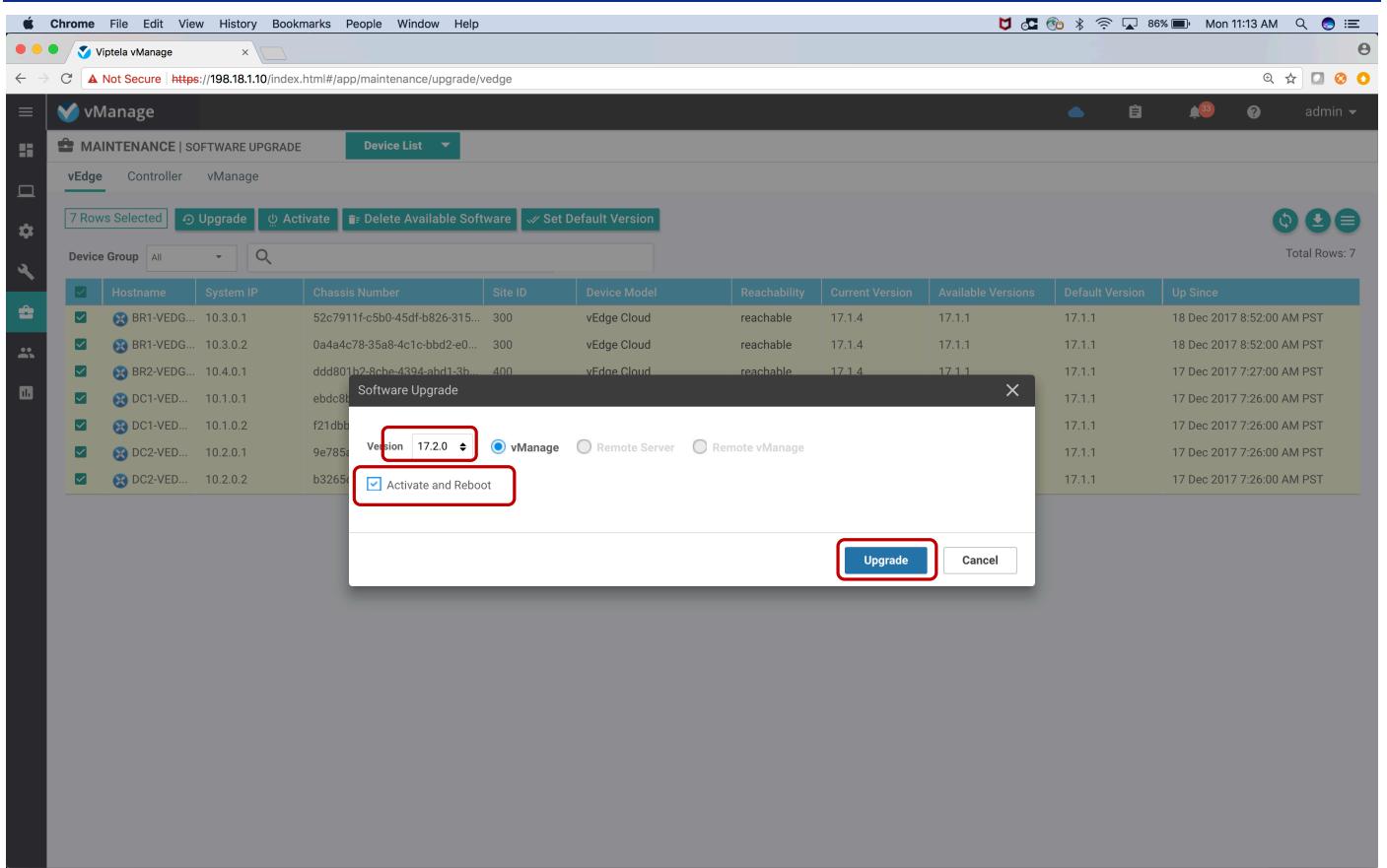


The screenshot shows the vManage interface for maintenance and software upgrade. A list of vEdge devices is displayed, with checkboxes checked for all seven devices. The 'Upgrade' button is highlighted with a red box.

Device Group	Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability	Current Version	Available Versions	Default Version	Up Since
	BRI-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
	BRI-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	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
	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
	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
	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
	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 Cisco vManage interface for maintenance and software upgrade. A modal dialog titled "Software Upgrade" is open over a table of devices. The table lists seven vEdges with their details like Hostname, System IP, Chassis Number, Site ID, Device Model, Reachability, Current Version, Available Versions, Default Version, and Up Since. The "vEdge" tab is selected in the navigation bar. The "Upgrade" button in the toolbar 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	ddd801b2-8che-4394-abd1-3b...	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

The "Software Upgrade" dialog contains the following fields:

- Version: 17.2.0 (dropdown menu)
- Target: vManage (radio button selected)
- Remote Server (radio button)
- Remote vManage (radio button)
- Activate and Reboot
- 
- 

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)