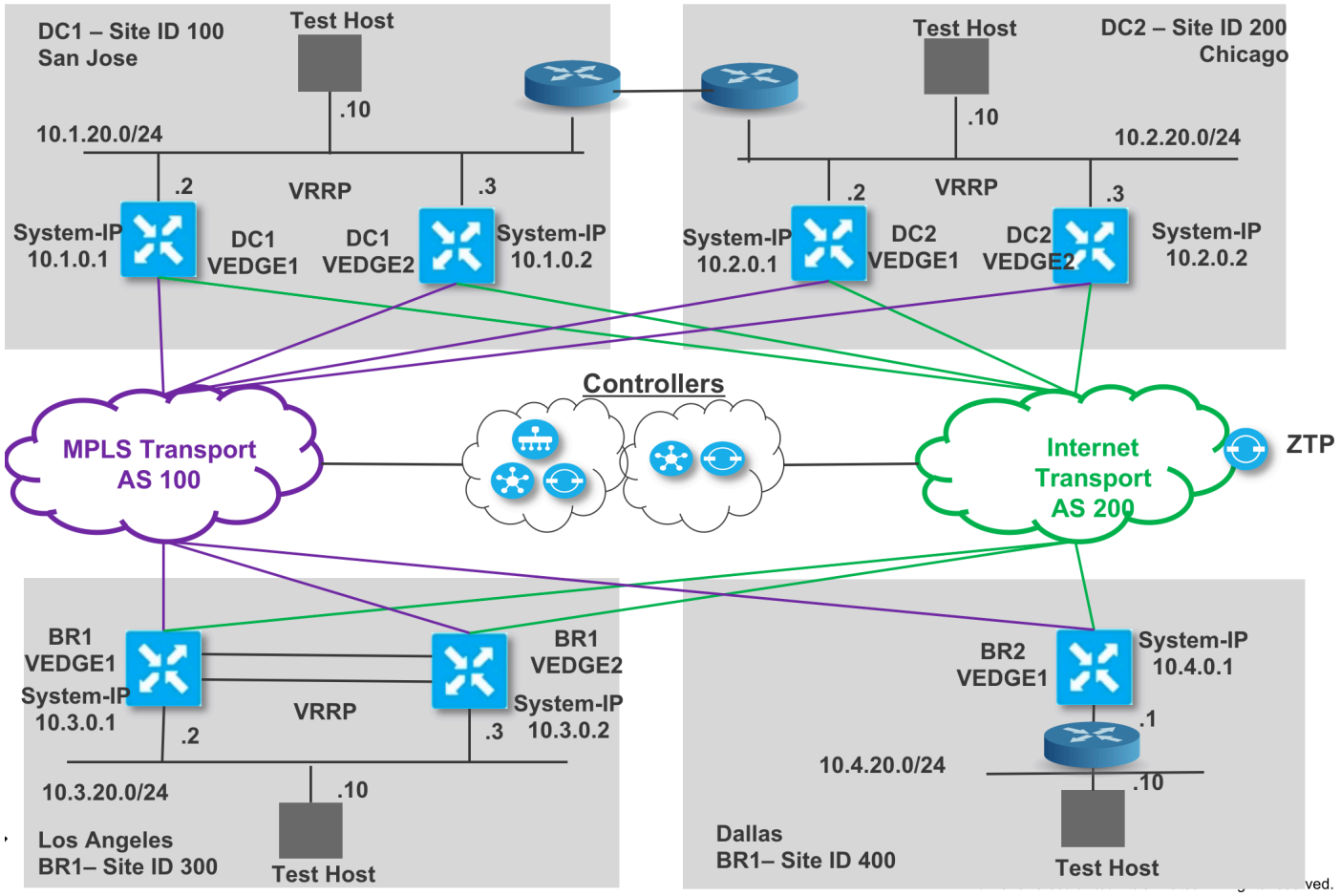
Introduction to Cisco SD-WAN (Viptela) Lab Guide

LABEN-2010

Lab Topology



Lab01 – Deploy vEdge in Branch 2 using ZTP

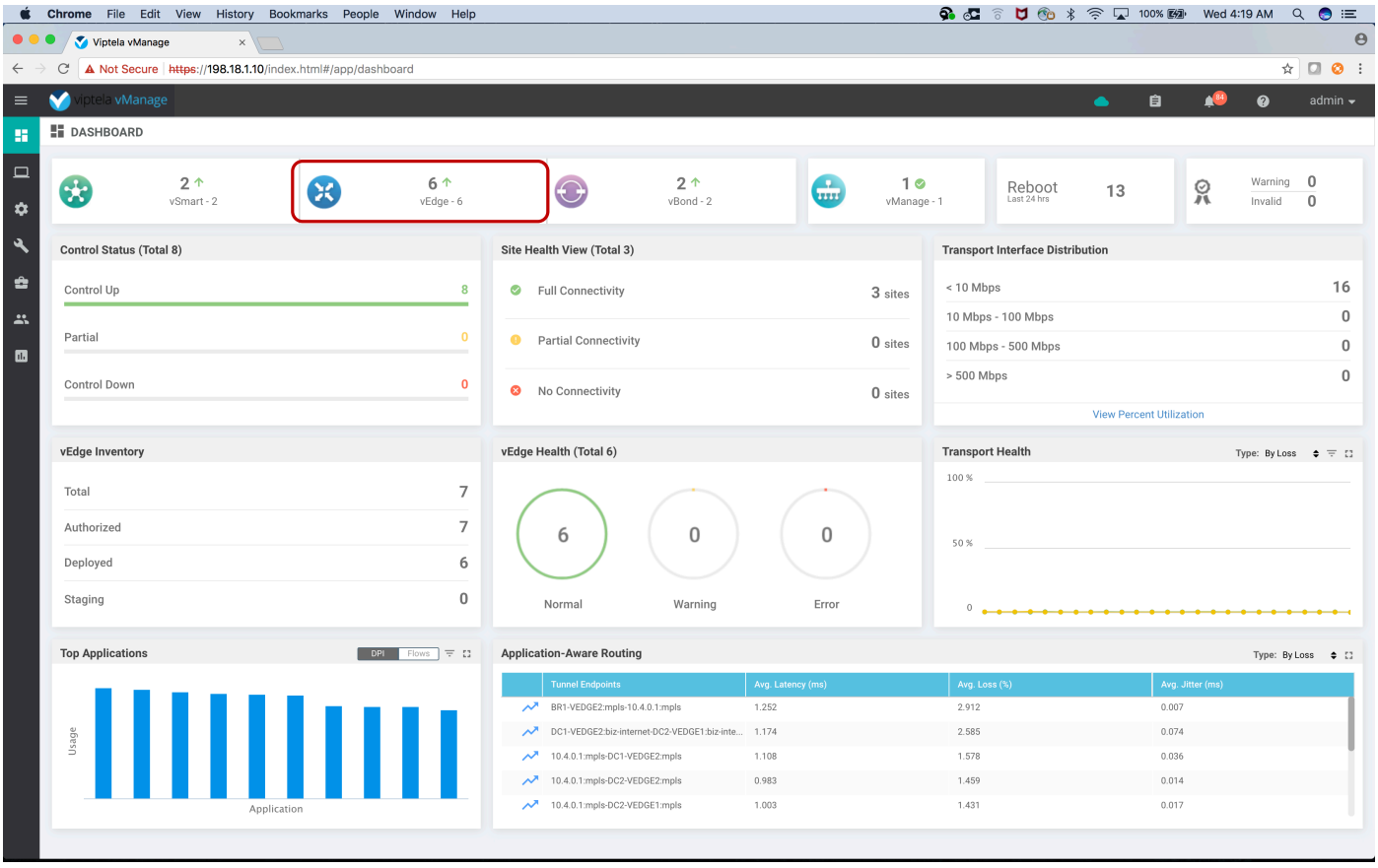
In this scenario we will bring up Branch 2 site using ZTP.

Steps

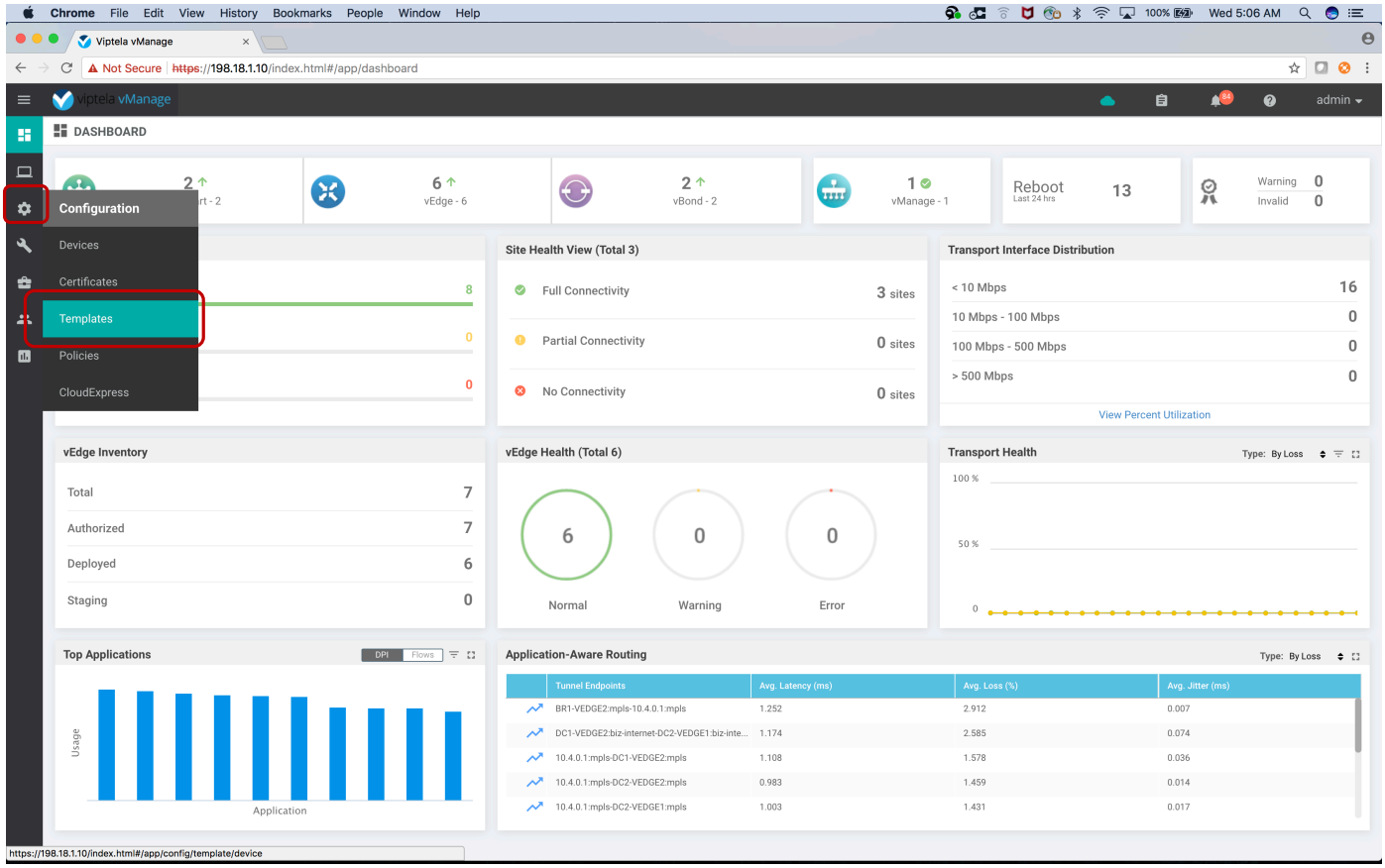
Deploy a Branch using vManage configuration template and Viptela's Zero Touch Provisioning (ZTP) service. ZTP process is simulated in this lab using default configuration from the factory for the vEdge in Branch 2.

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.



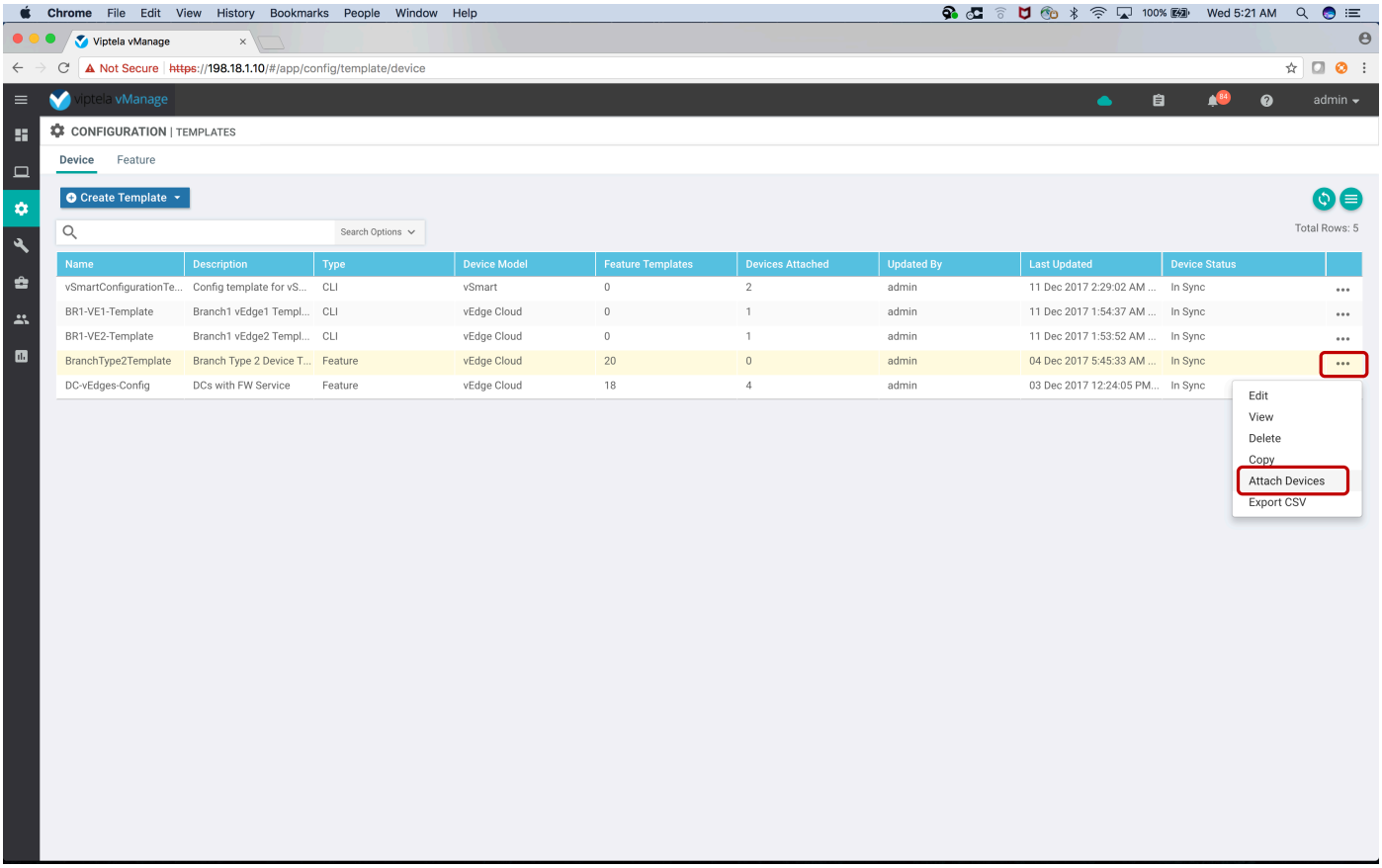
Click on “Configuration” icon and select “Templates” from the drop-down menu.



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.

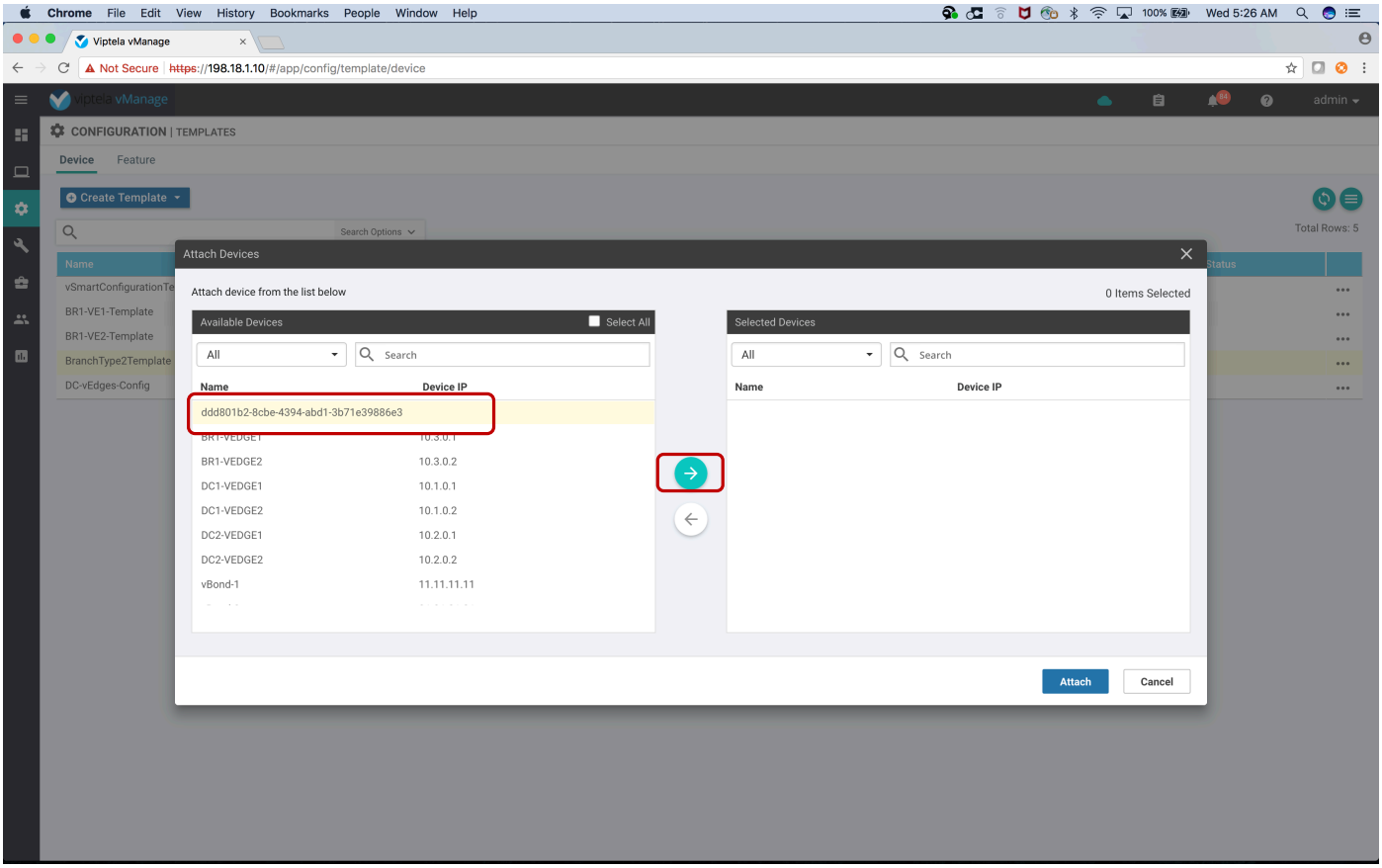
Click on the three dots (…) in the right most column and from the drop down select the option “Attach Devices”.



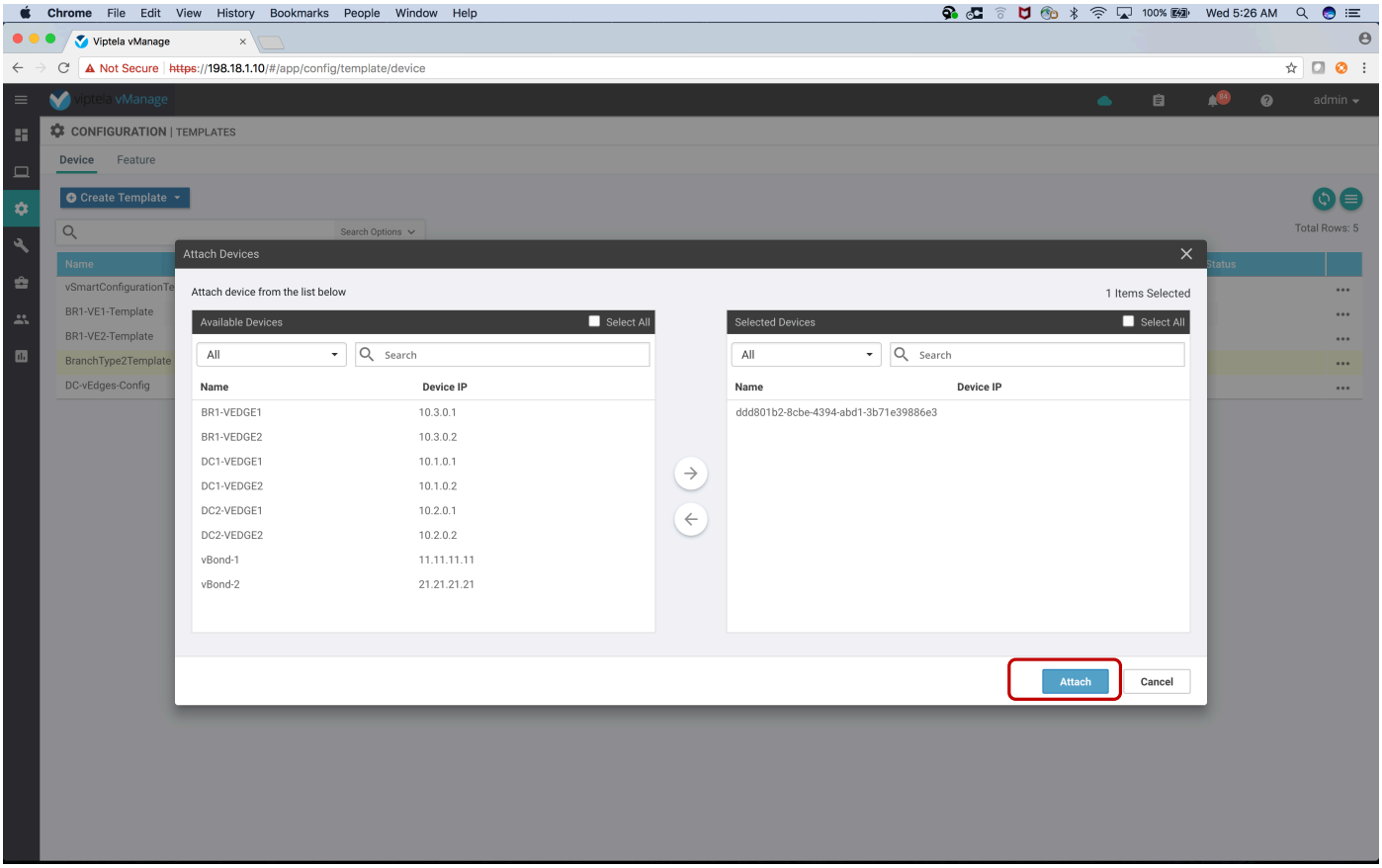
From the left pane labeled Available Devices find the device with chassis-id/UUID of `ddd801b2-8cbe-4394-abd1-3b71e39886e3.`

Select this device that has not been provisioned.

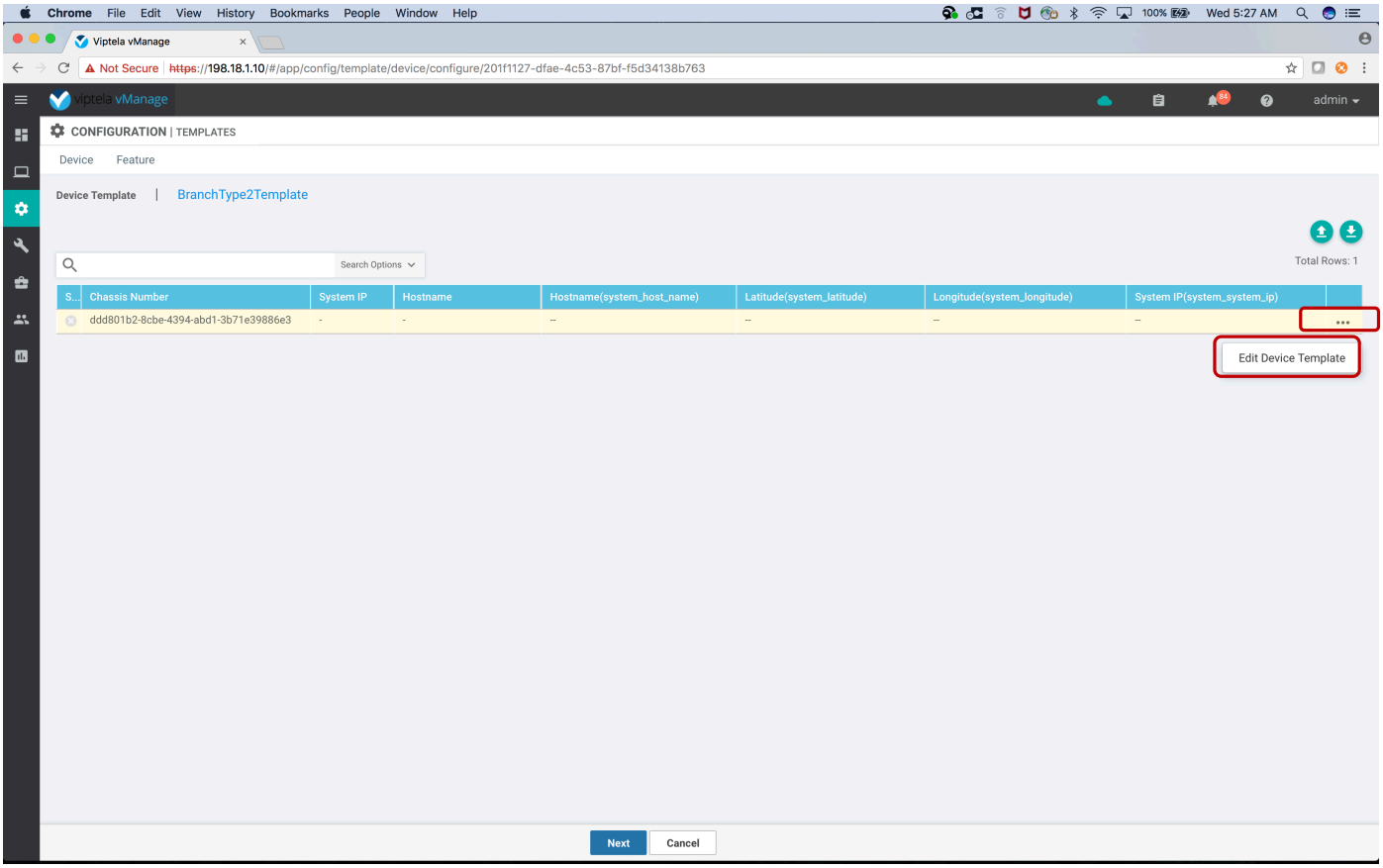
Move the selected device to the right pane labeled “Selected Devices” by clicking on the right arrow button.



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



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



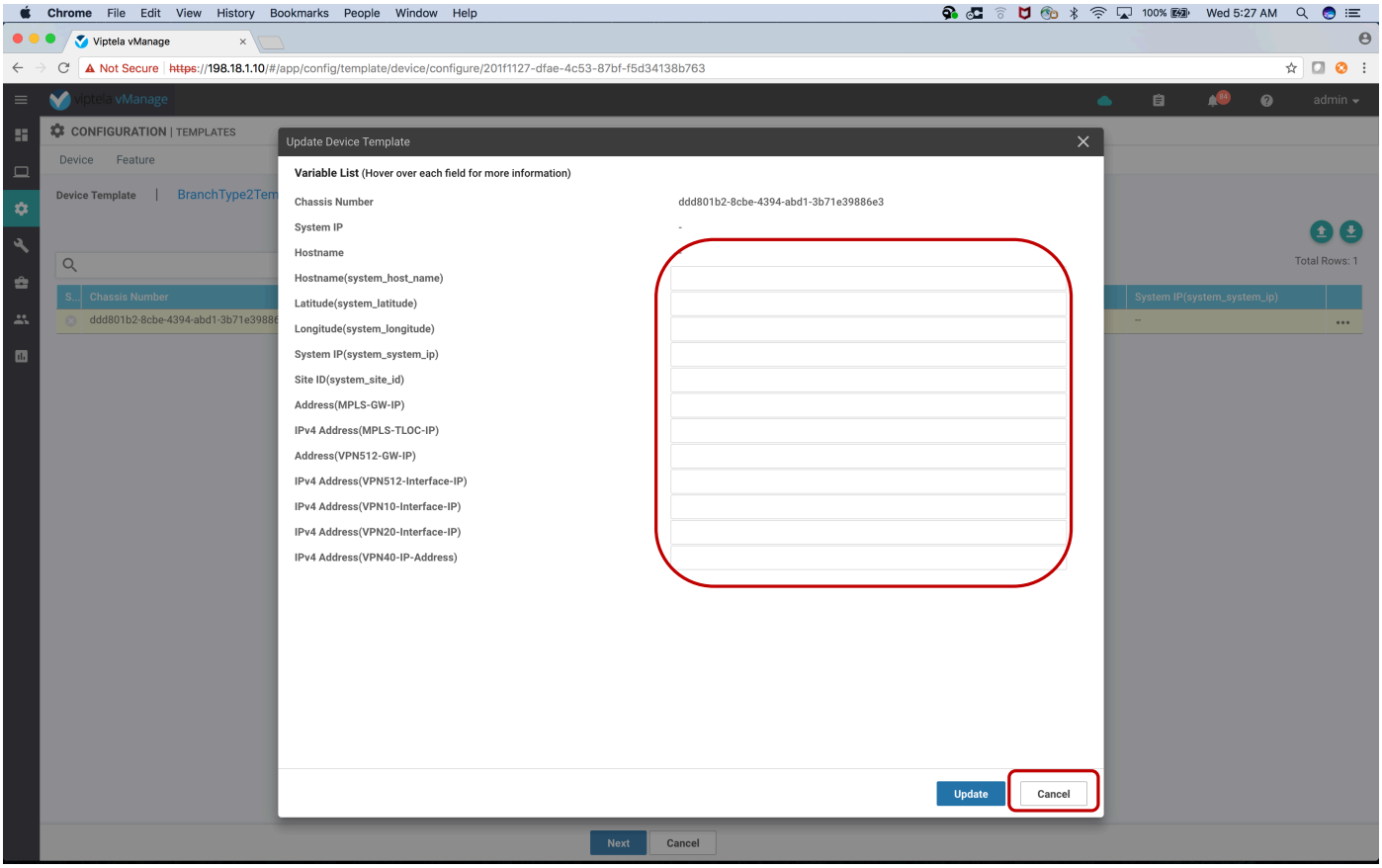
The “Edit Device Template” provides an option to update the variables values associated with the Branch2 vEdge.

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

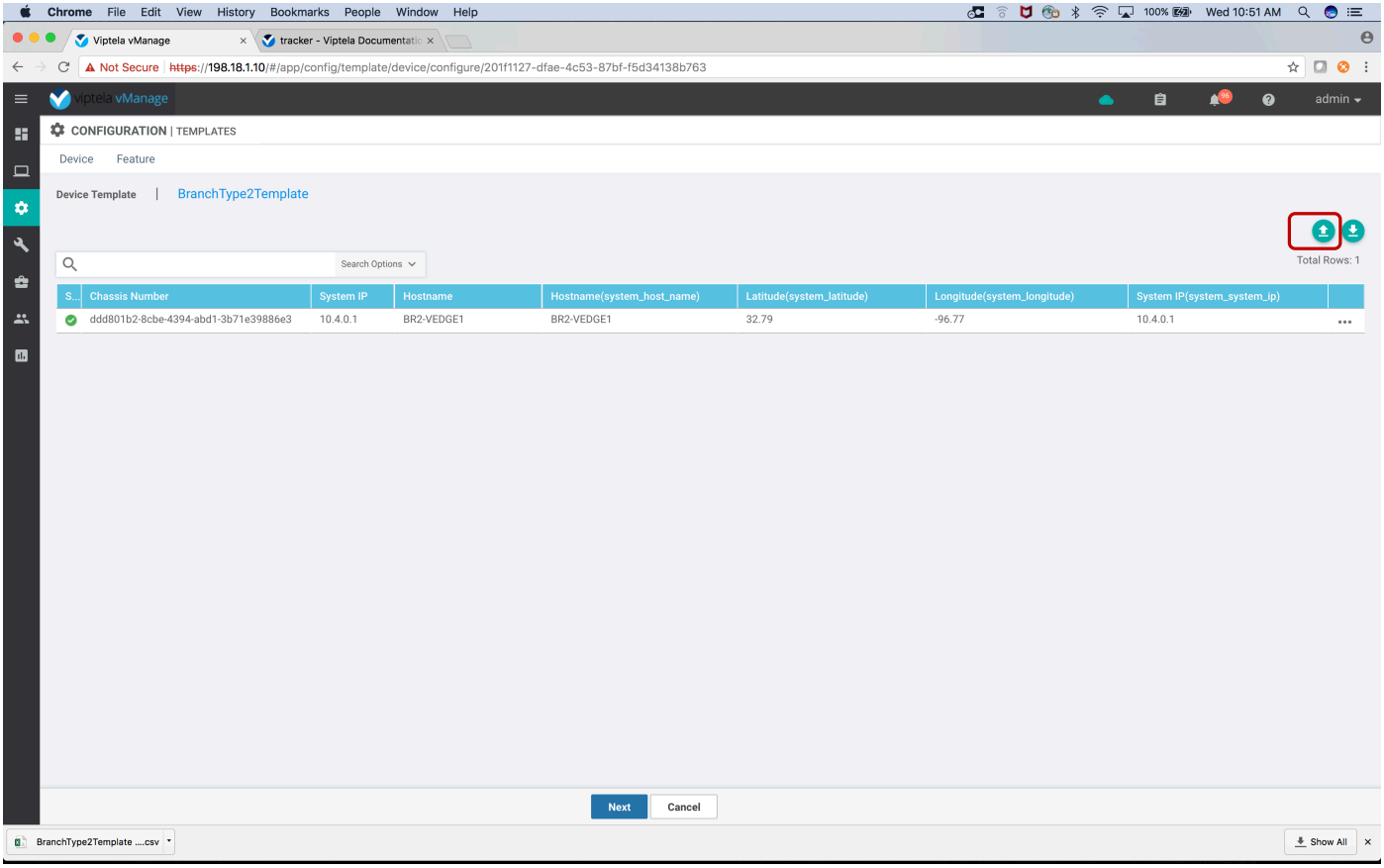
There is another method where one can upload a CSV file with the fields value already populated.

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

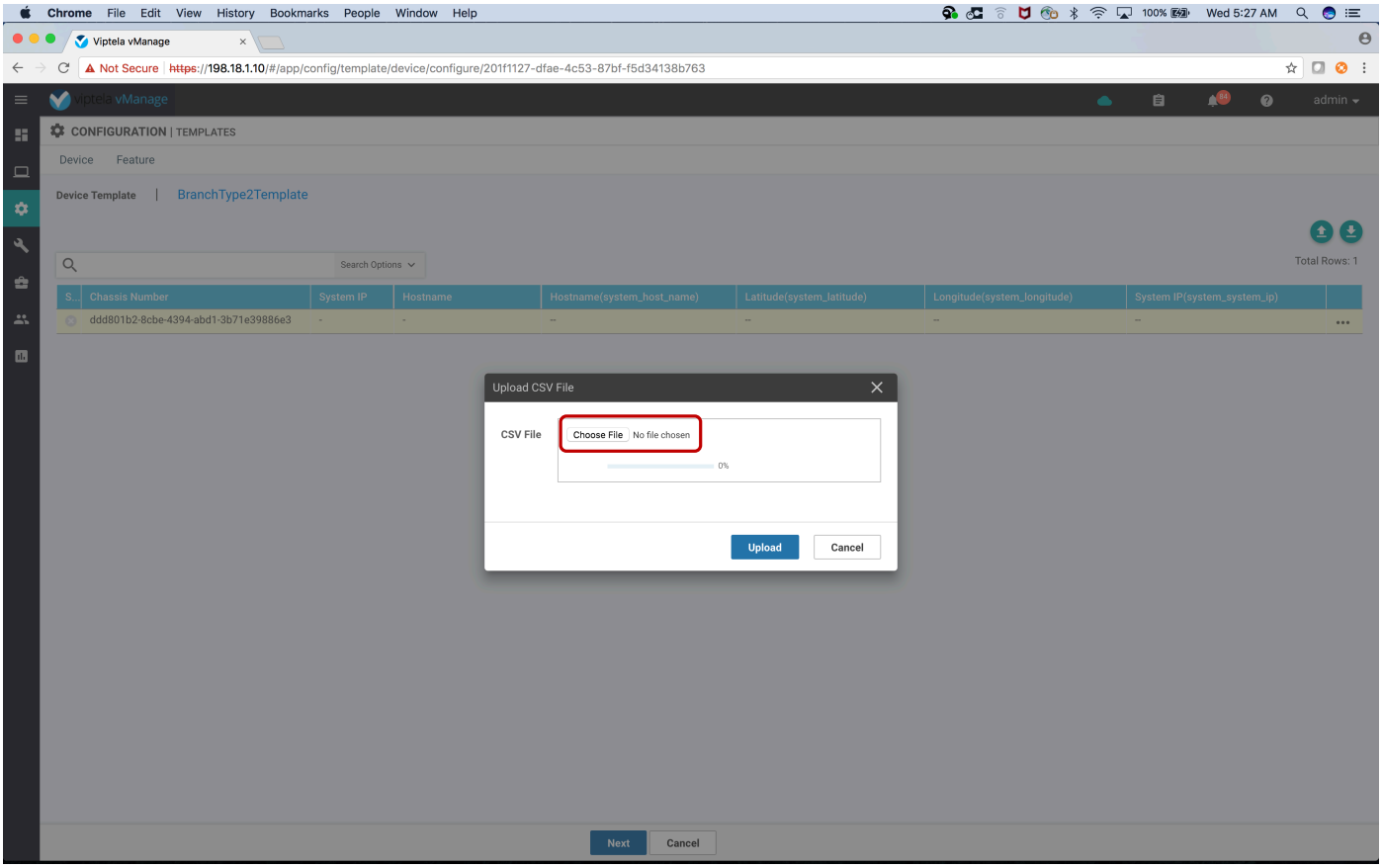
Click the “Cancel” button to go back to the previous page.



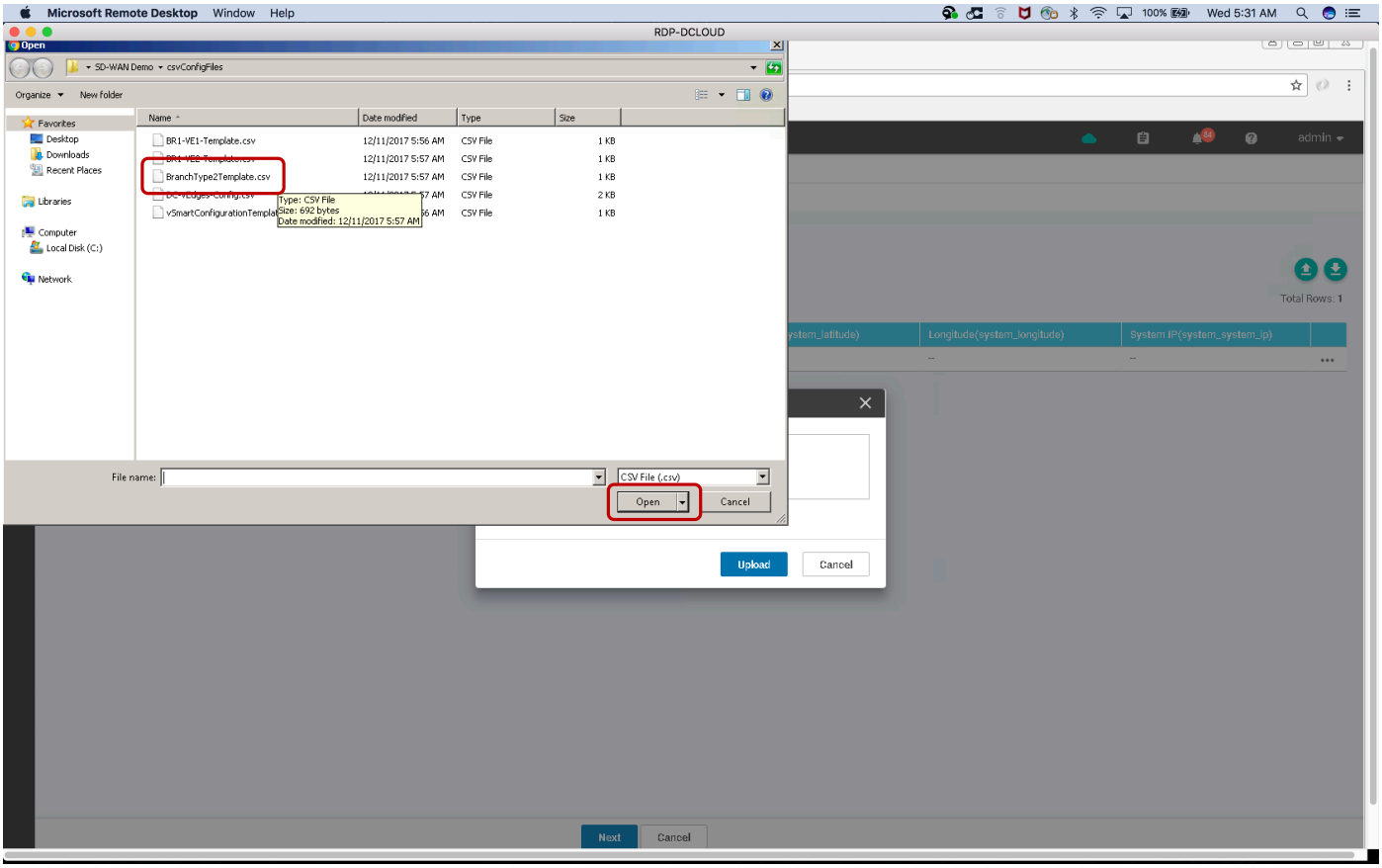
Click on the upload icon ( ) for uploading the CSV file.



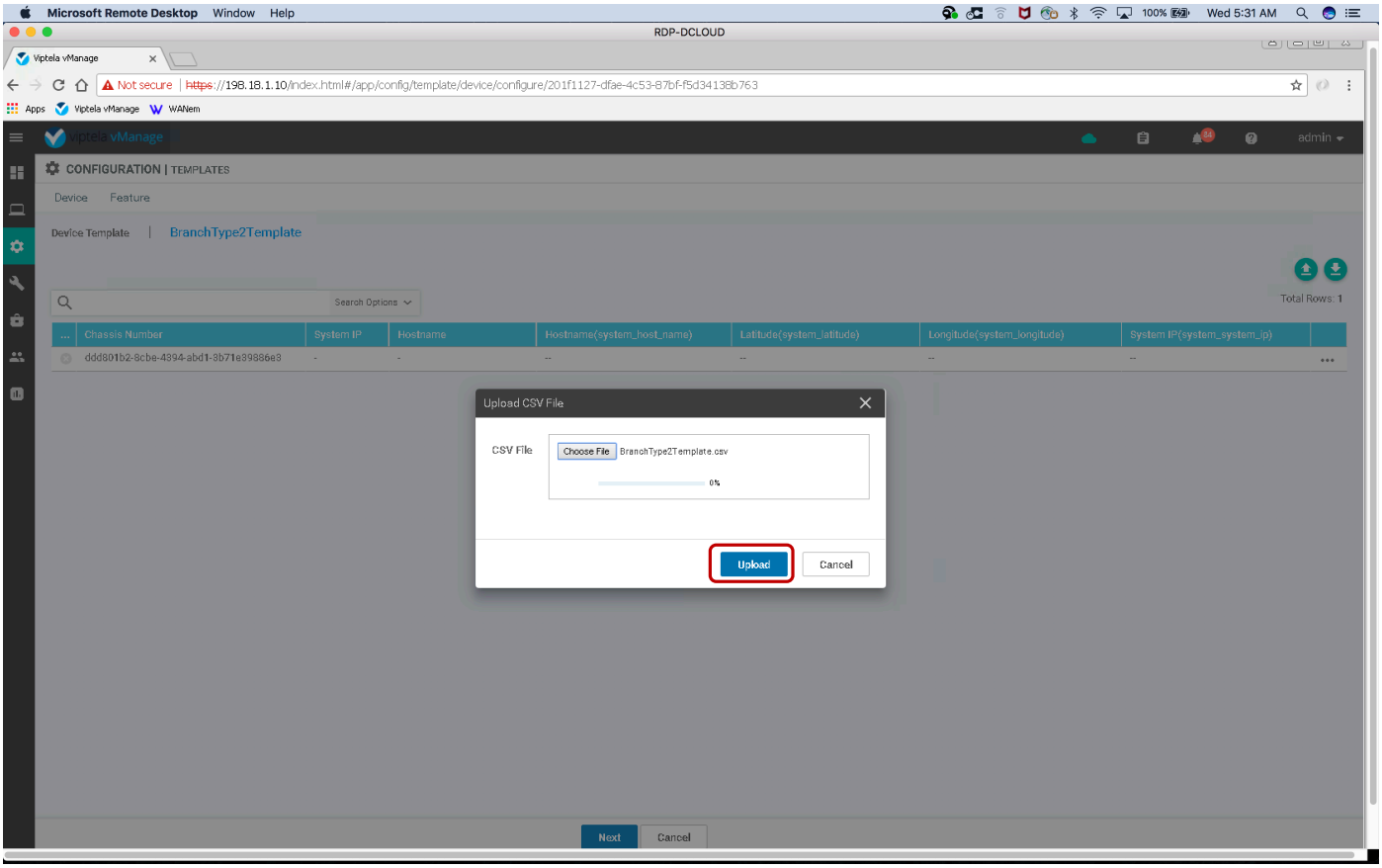
Click on the “Choose File” button.



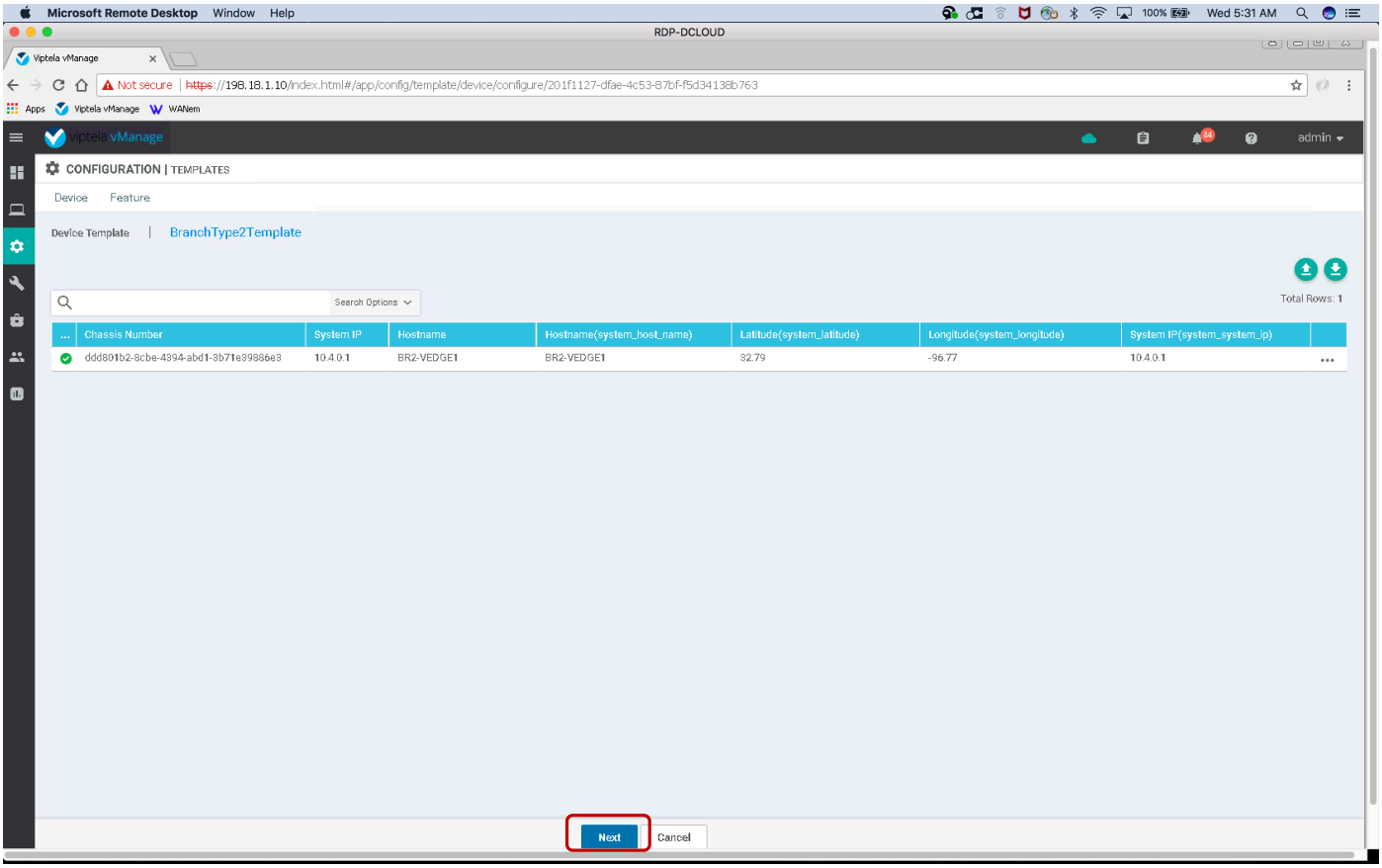
Prebuilt CSV file is located in the folder \Desktop\SD-WAN Demo\csvConfigFiles on Workstation 1. The name of the file is “BranchType2Template.csv”. In the popup window select the file BranchType2Template.csv. Click on the “Open” button.



On the next screen click on “Upload” button.

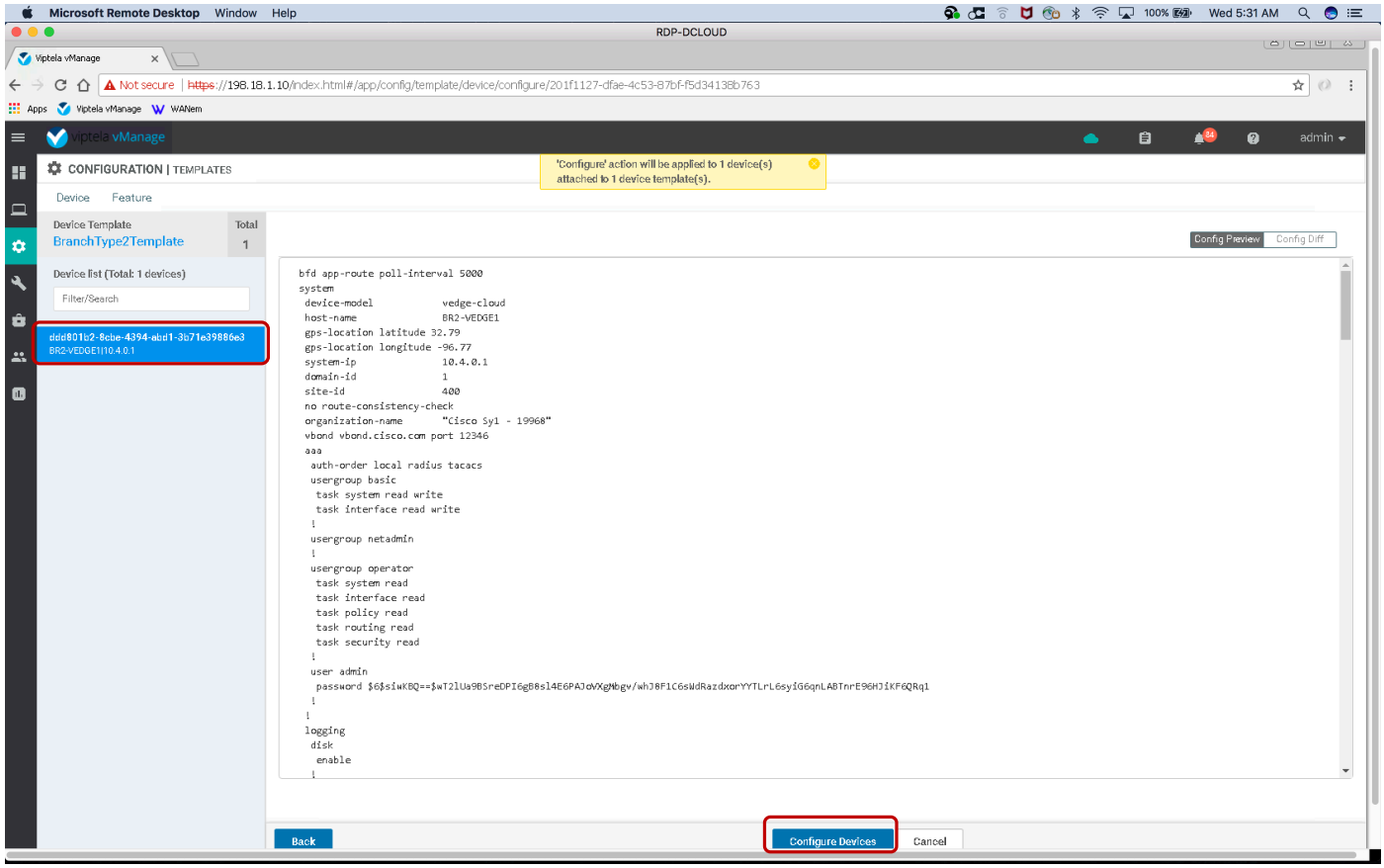


On the next screen, click on “Next” button. You will see the values for the variables are filled up based on the uploaded CSV file.

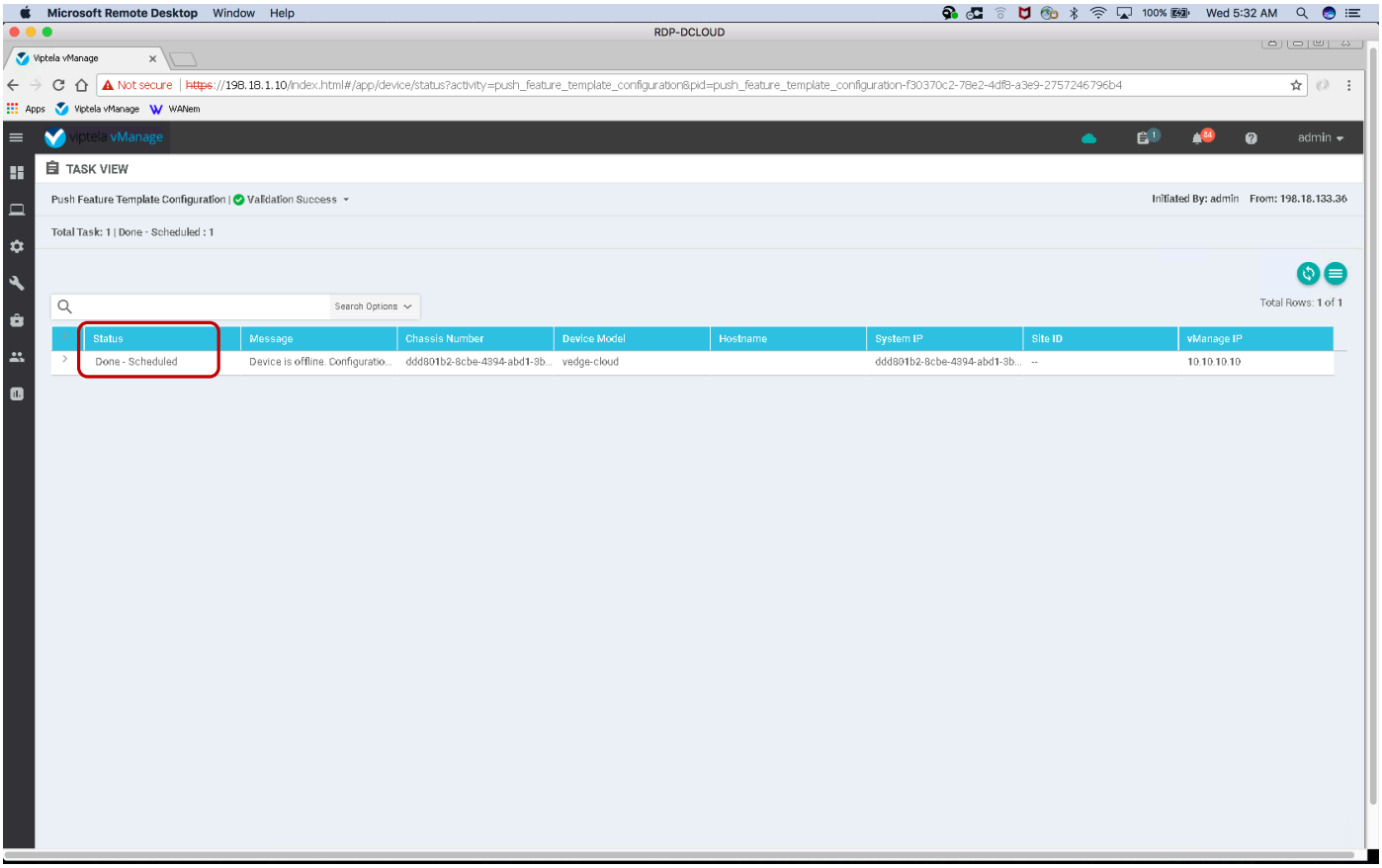


You may click on the tab in the left column with BR2-VEDGE1 label to see the full CLI configuration for validation.

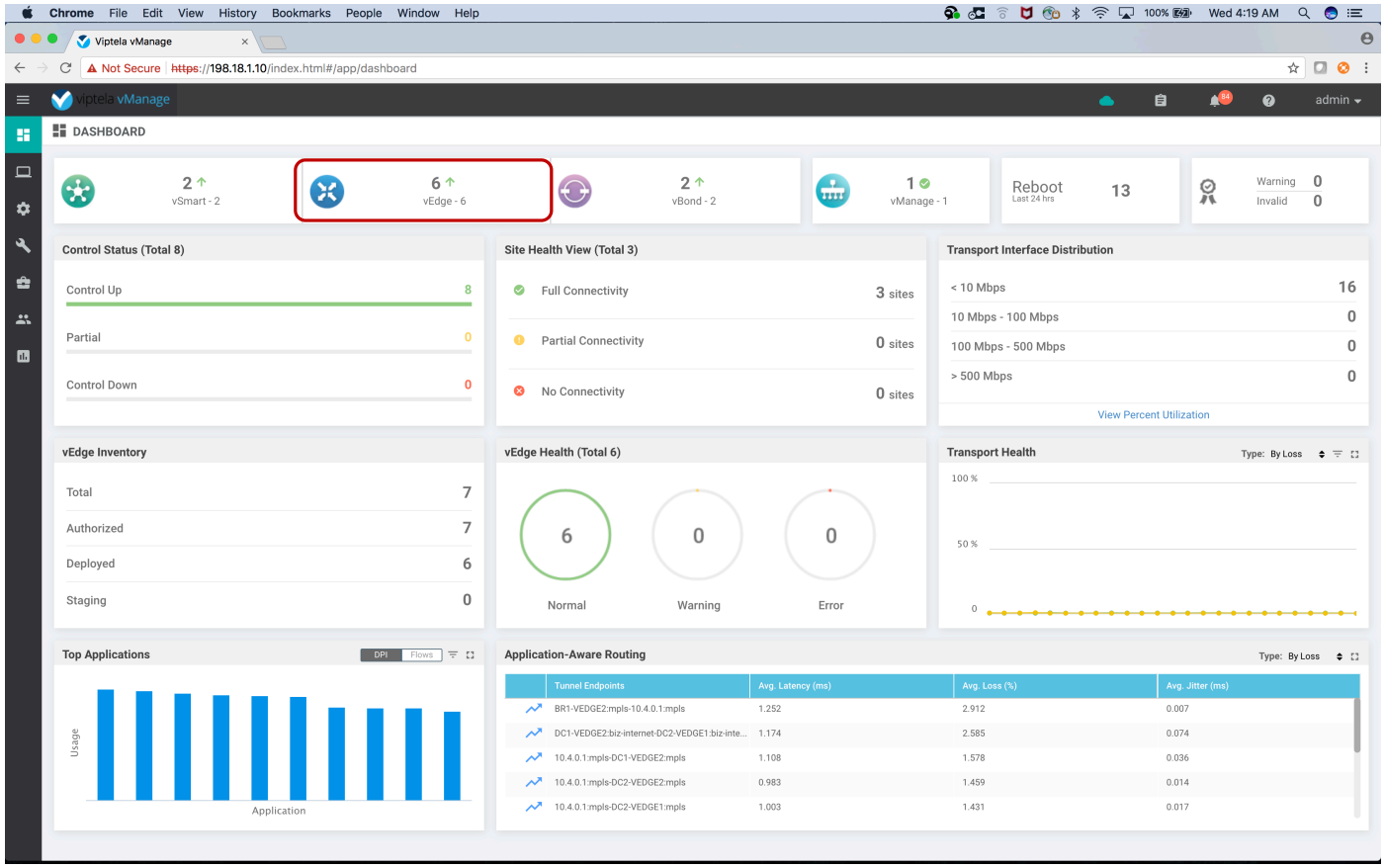
Click on “Configure Devices”.



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



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

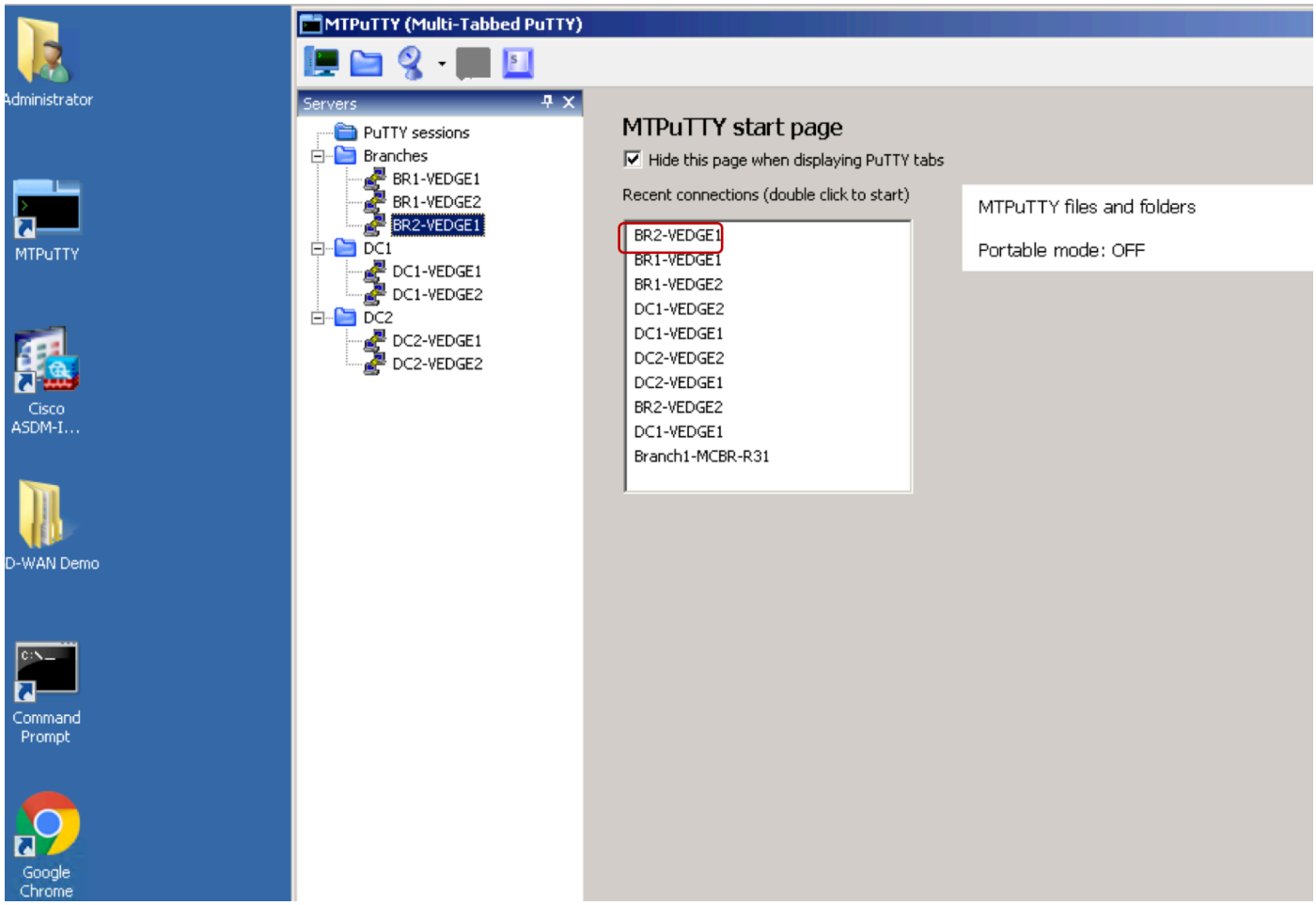


To simulate the device to be connected to the transport for ZTP, we will do “no shut” on the interface connected to Internet transport in the lab [interface ge0/0].

On the desktop of Wkst1 launch the MTPutty application.

Double click the BR2-VEDGE1 device.

You will be automatically logged in.



Issue the following commands to the BR2-vEdge1 CLI:

```
show run system
```

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

```
show run vpn 0
```

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

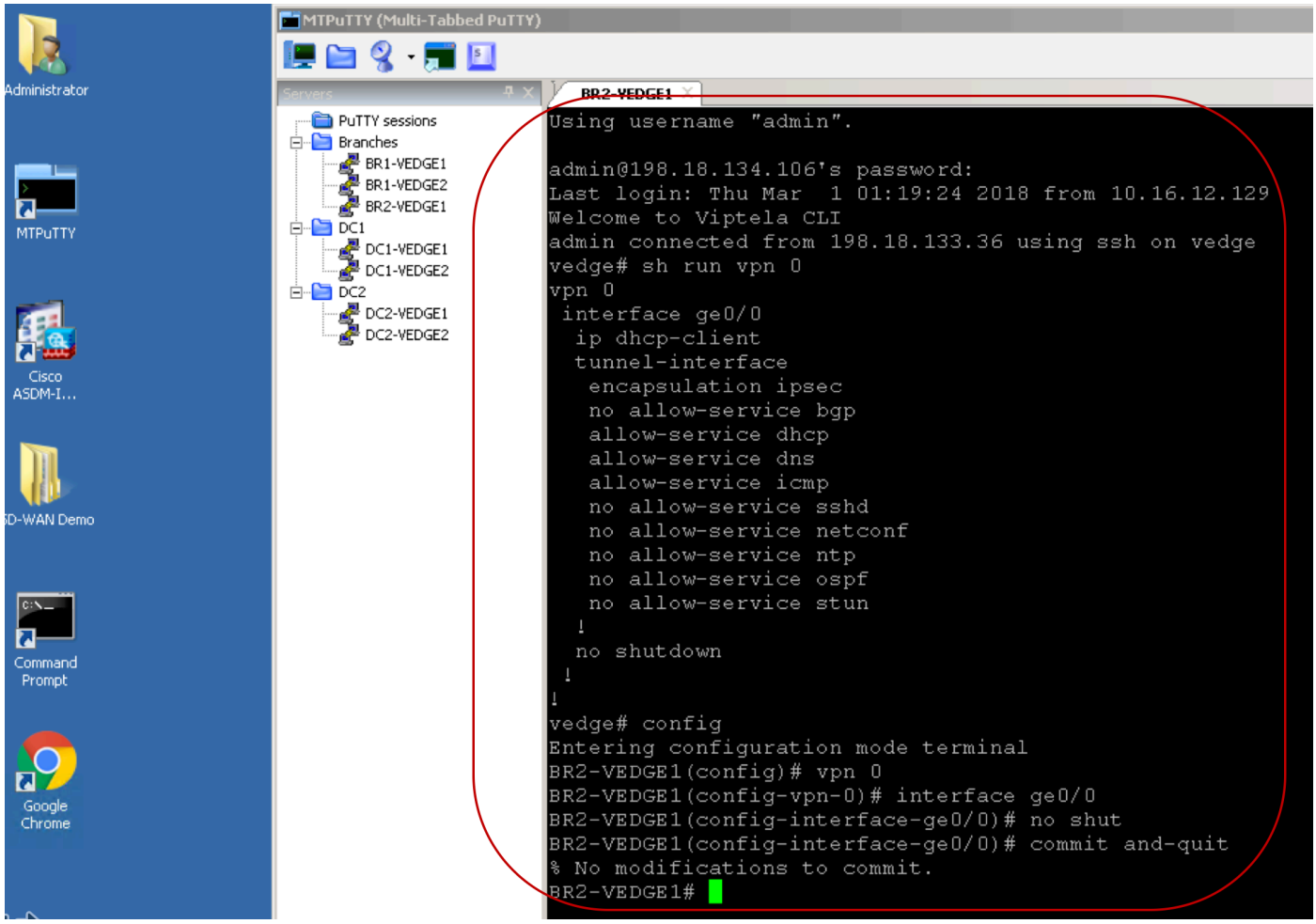
```
show run vpn 10
```

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

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

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

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



Issue the following command:

show run system

show run vpn 0

show run vpn 10

config t

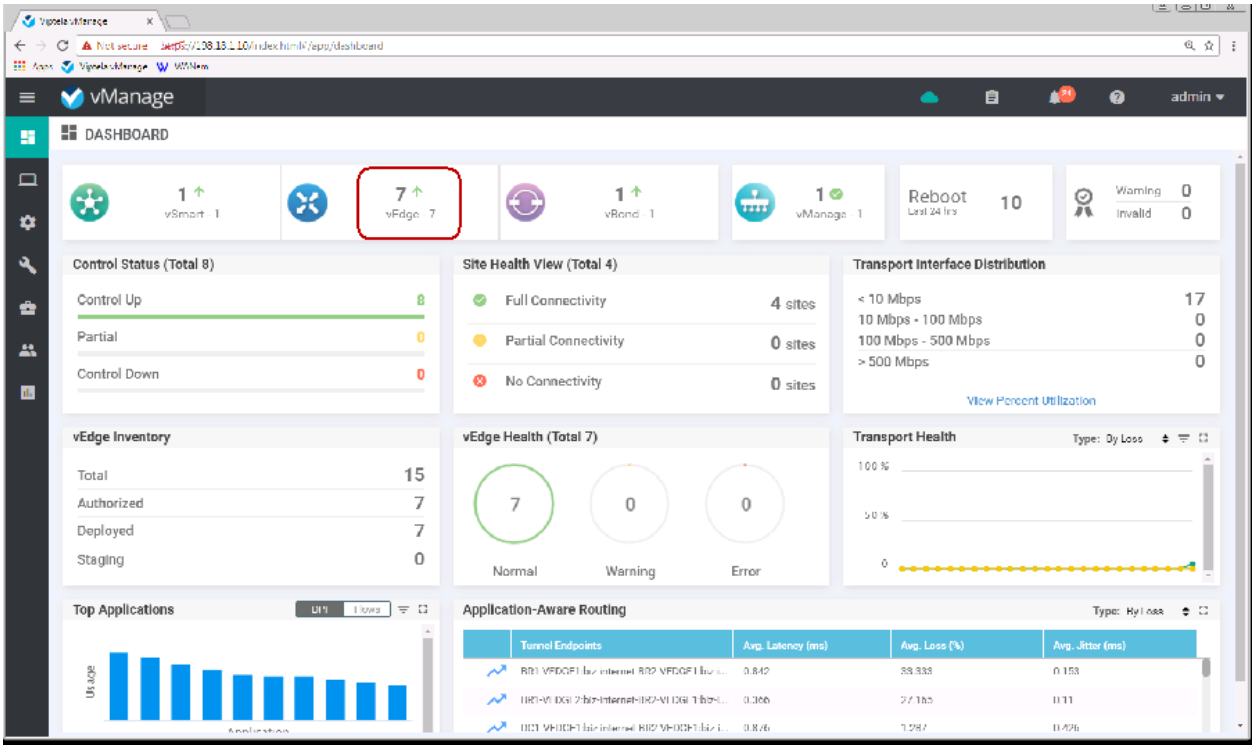
vpn 0

interface ge0/0

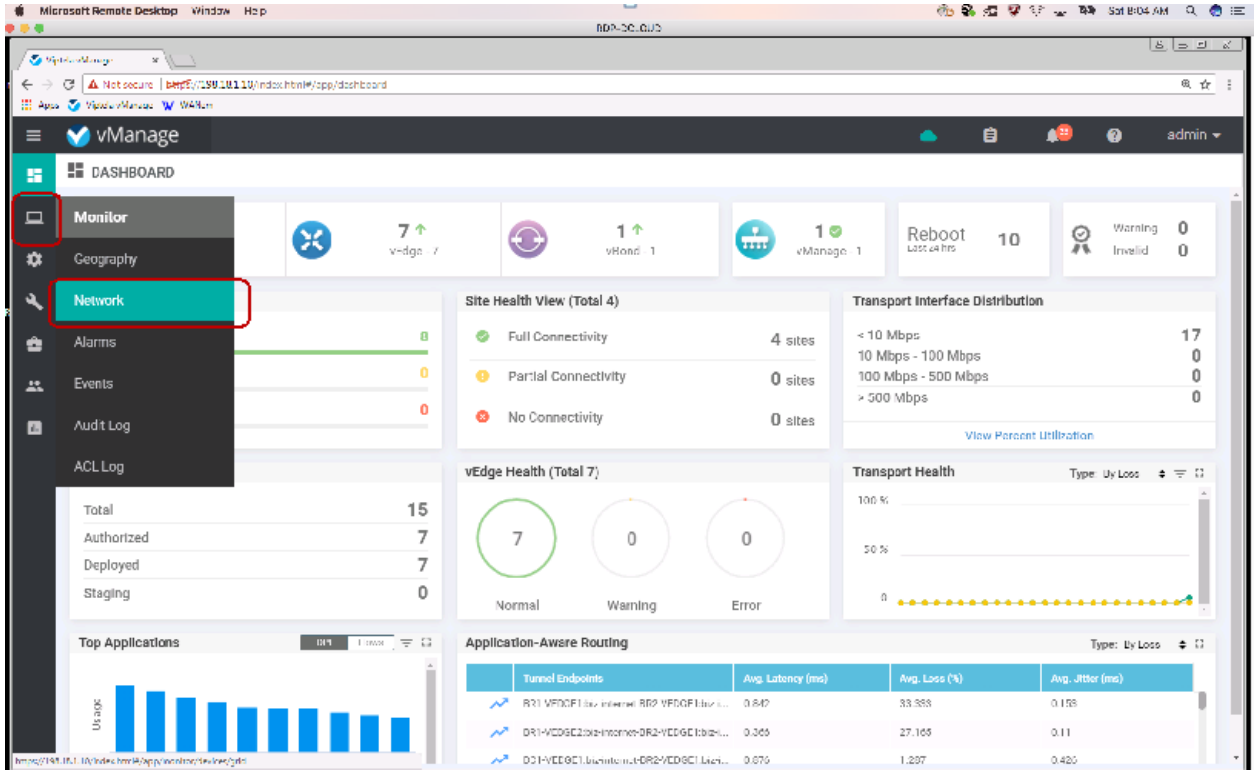
no shutdown

commit and-quit

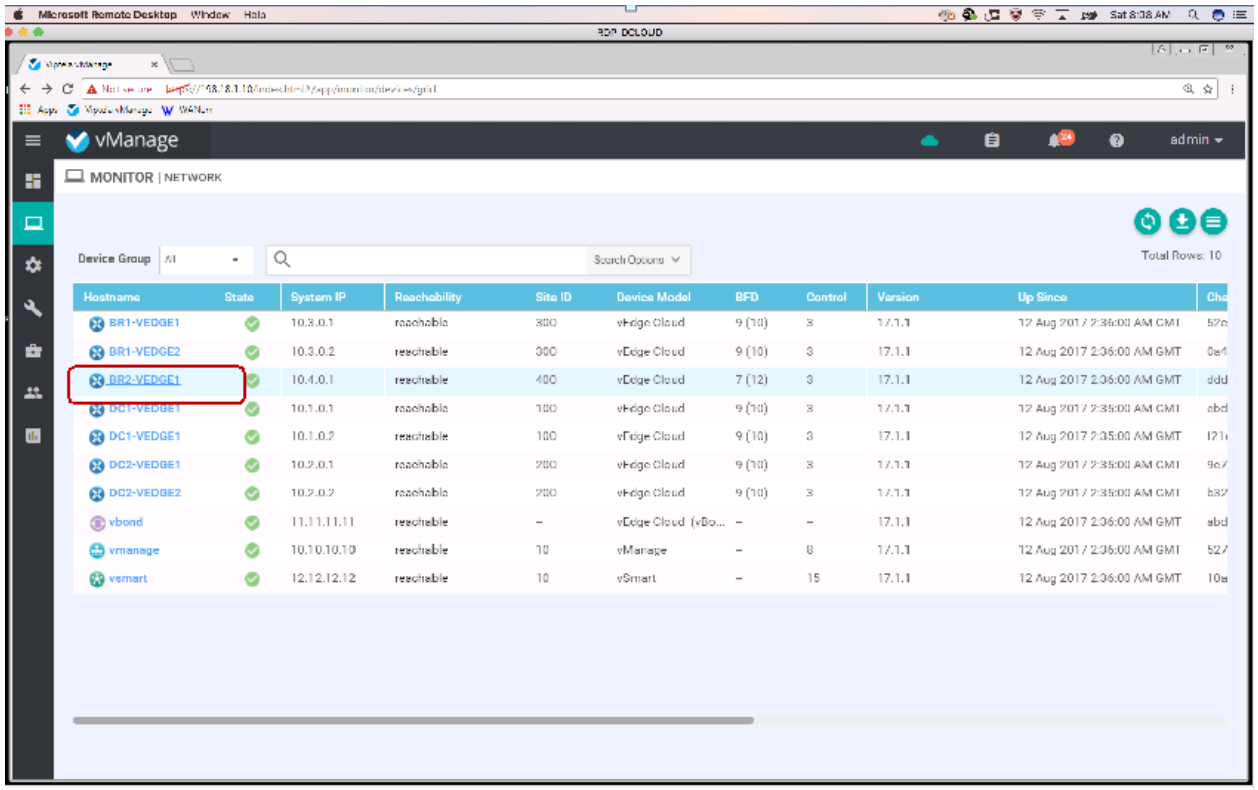
Go back to the vManage dashboard. The BR2-VEDGE1 will come up and the dashboard will show total of 7 vEdges are operational.



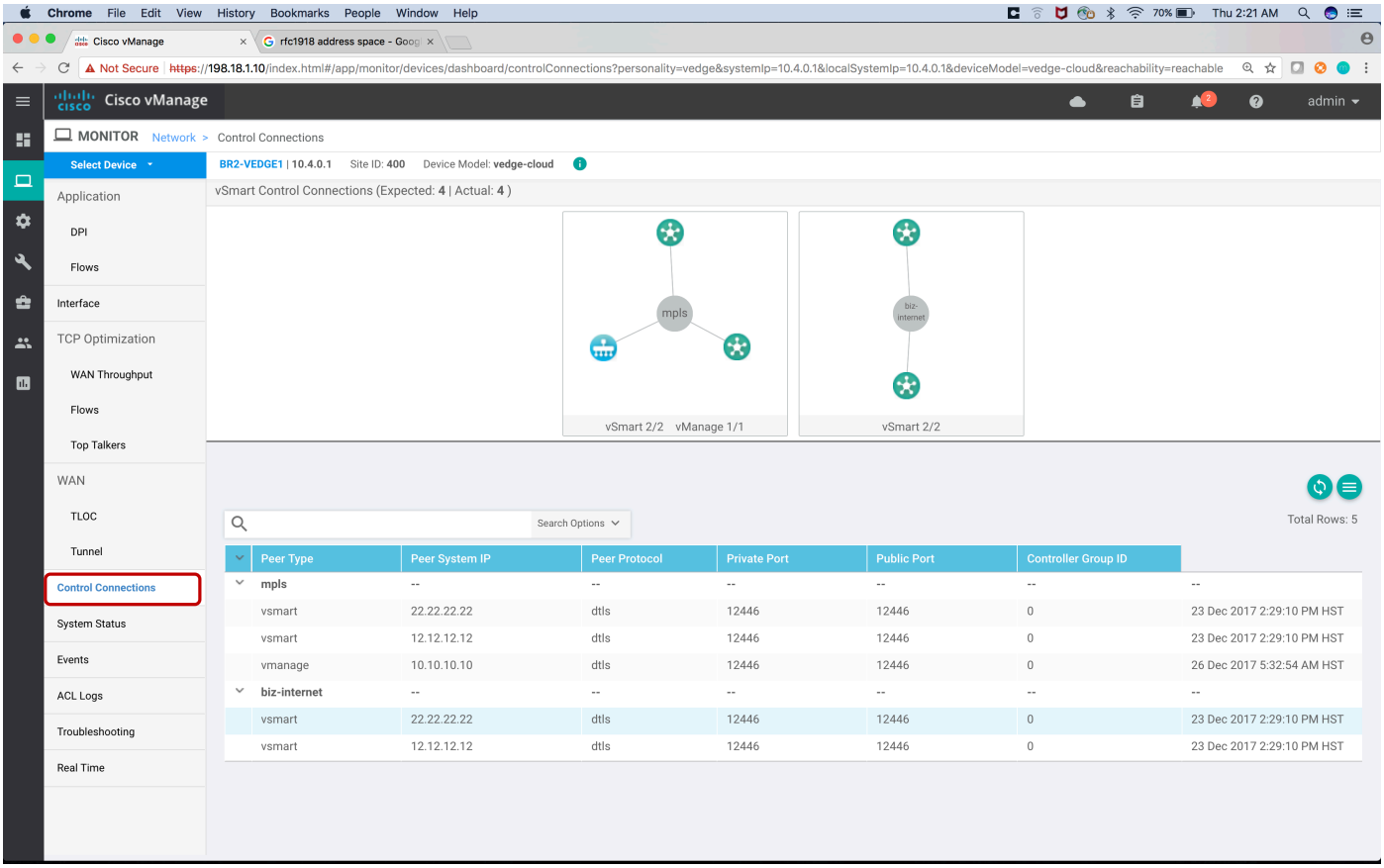
Click on Monitor icon and then select Network.



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

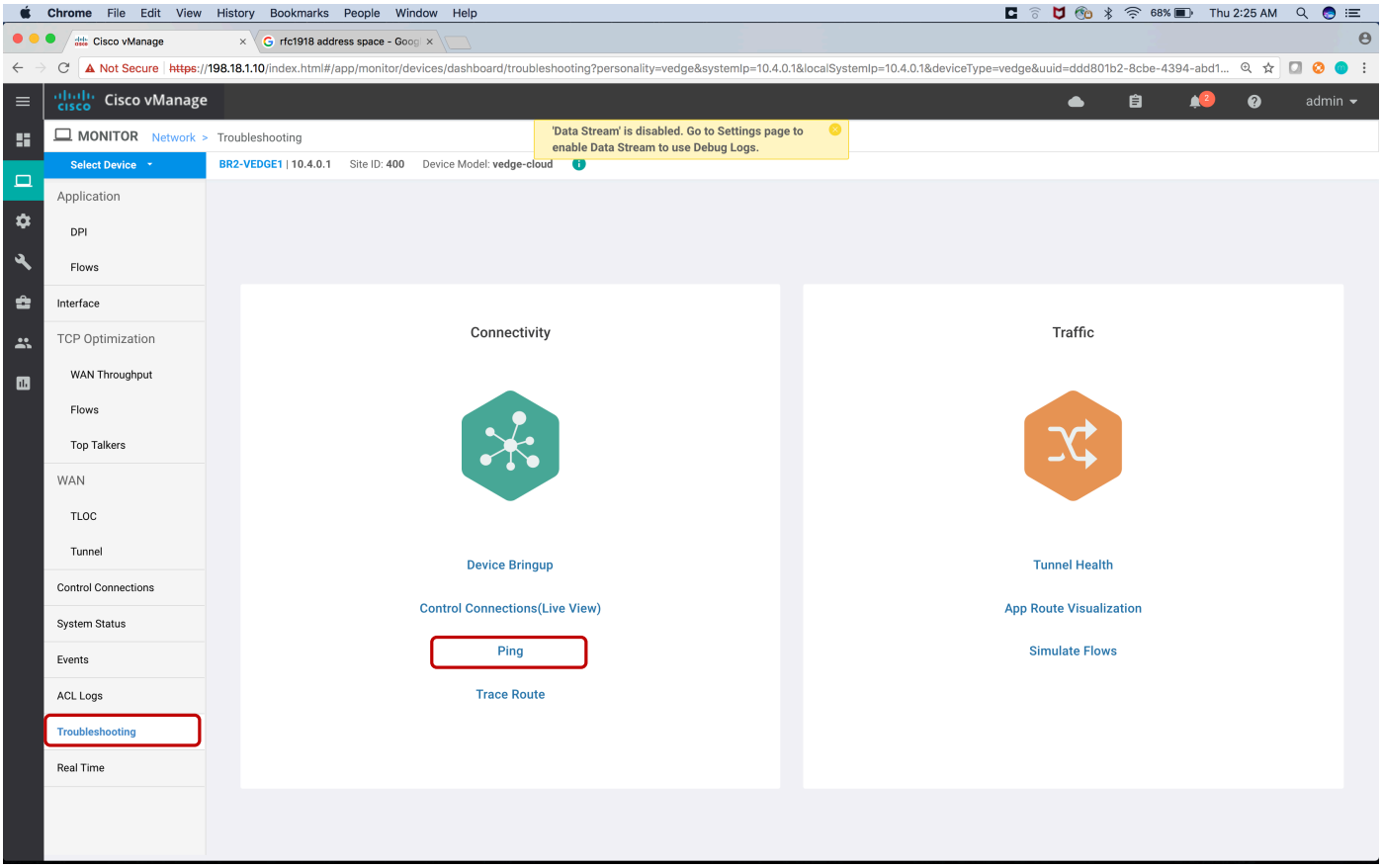


Click on Control Connections. Validate control sessions are established to vSmart and vManage.



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.

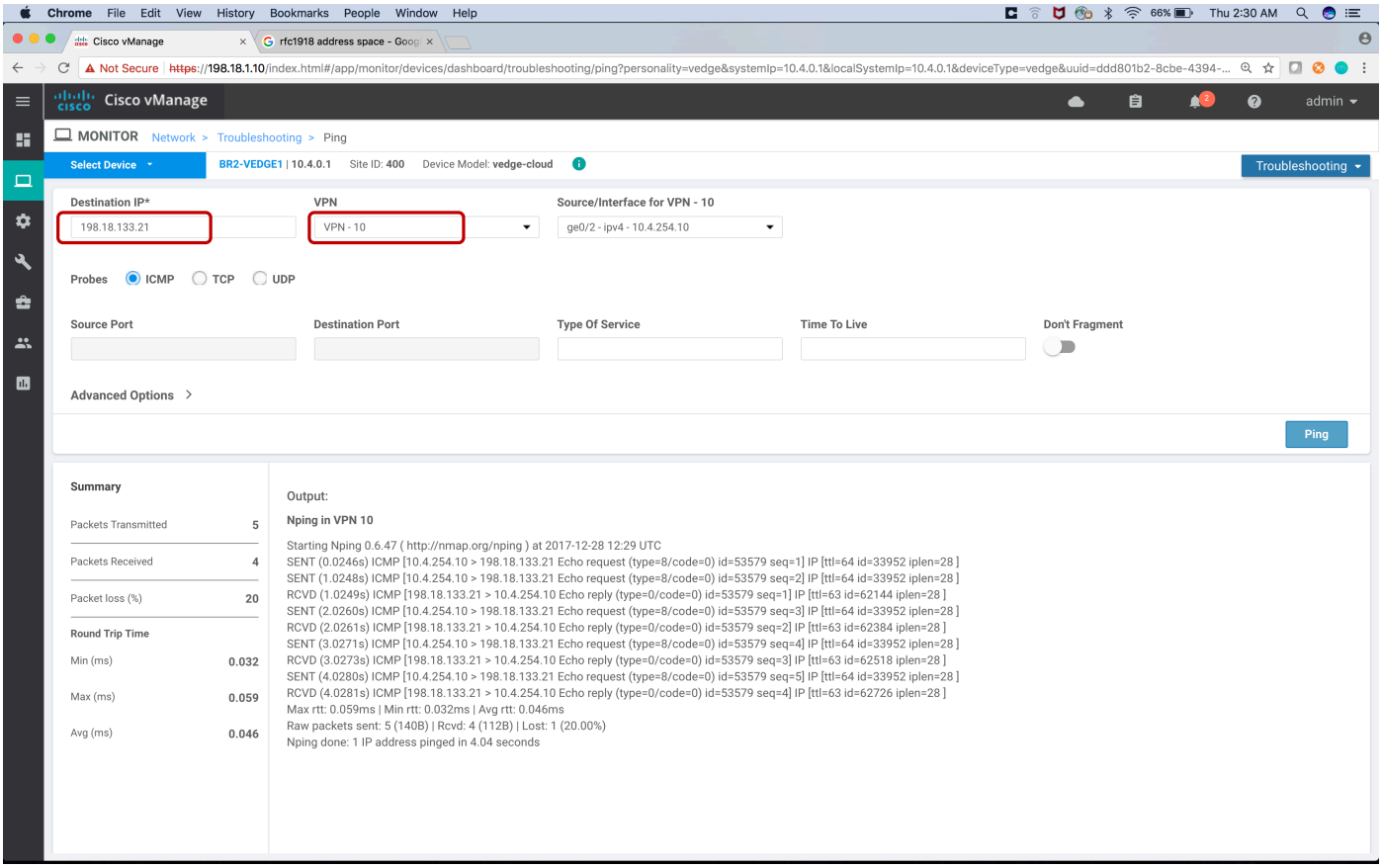


Use the following IP addresses for validating IP connectivity.

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.



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

DPI

Click on DPI from the device dashboard.

IPFIX Flow Records

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

Interface Stats

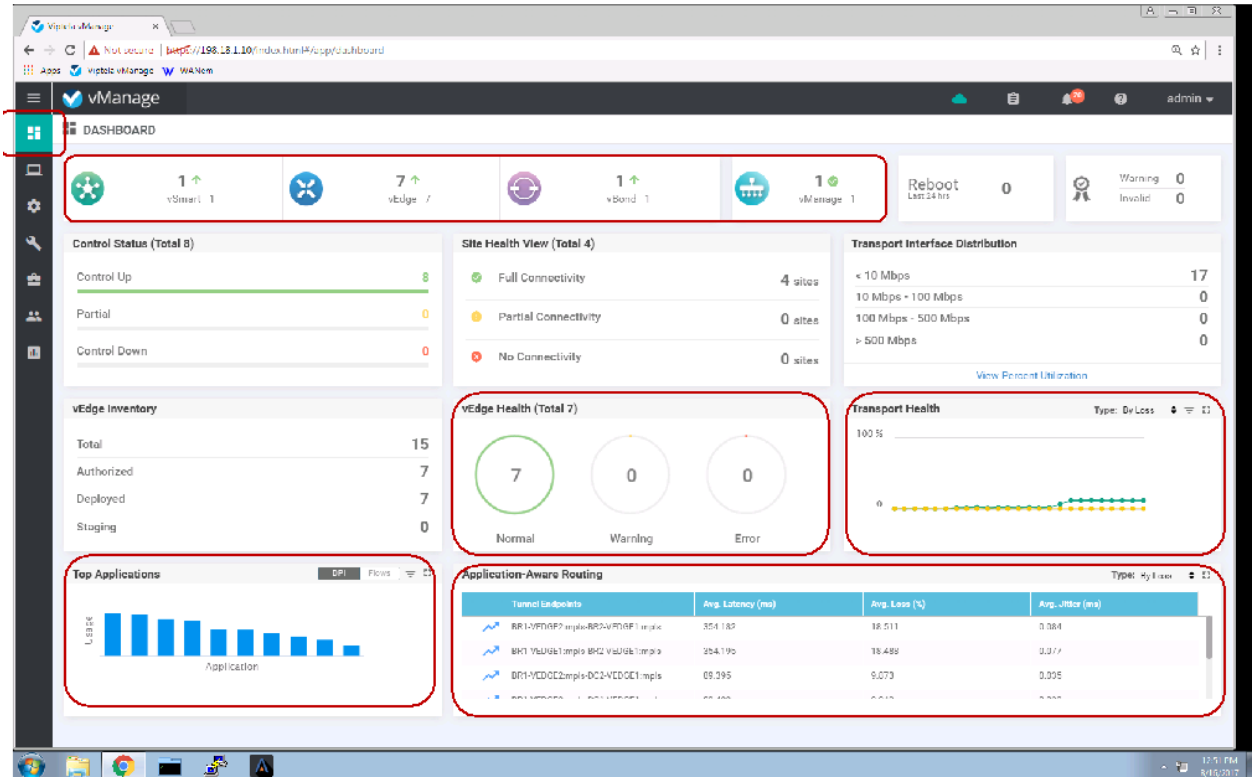
From the device dashboard click on “Interfaces” to see utilization of the links on the vEdge.

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

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

Click on the vManage dashboard icon:

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



Lab 02 - Strict Hub-n-Spoke Topology

Enterprise may not need a full mesh topology and would like to have a pure Hub-n-SpokeIPSec/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.

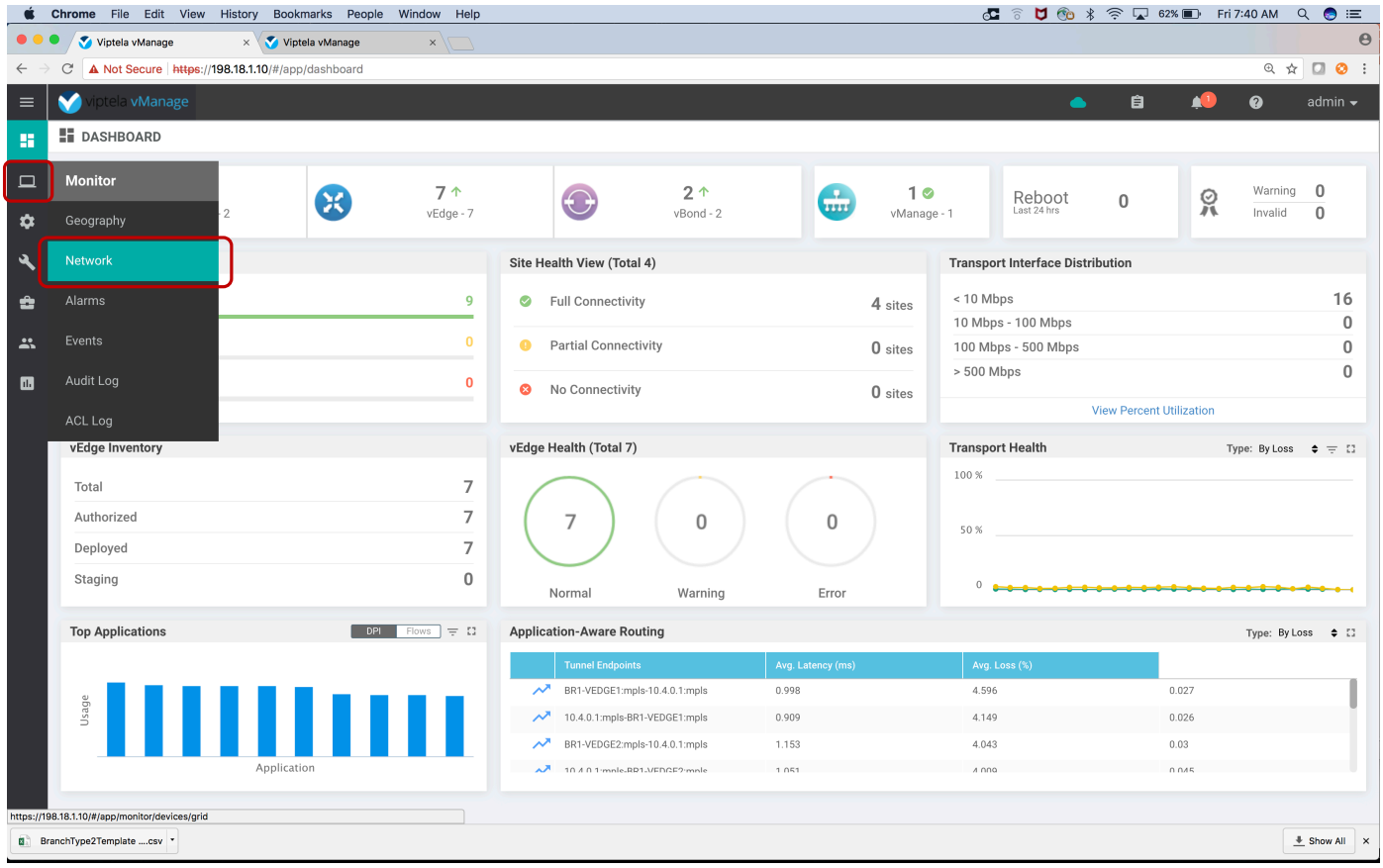
For corporate VPN 10, we will only advertise the Branches' routes to the DCs and not to other Branches. The DCs are advertising default routes and hence when a branch needs to talk to other branches, they will take the default to the DCs. The DC vEdges then route the traffic back to the other remote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

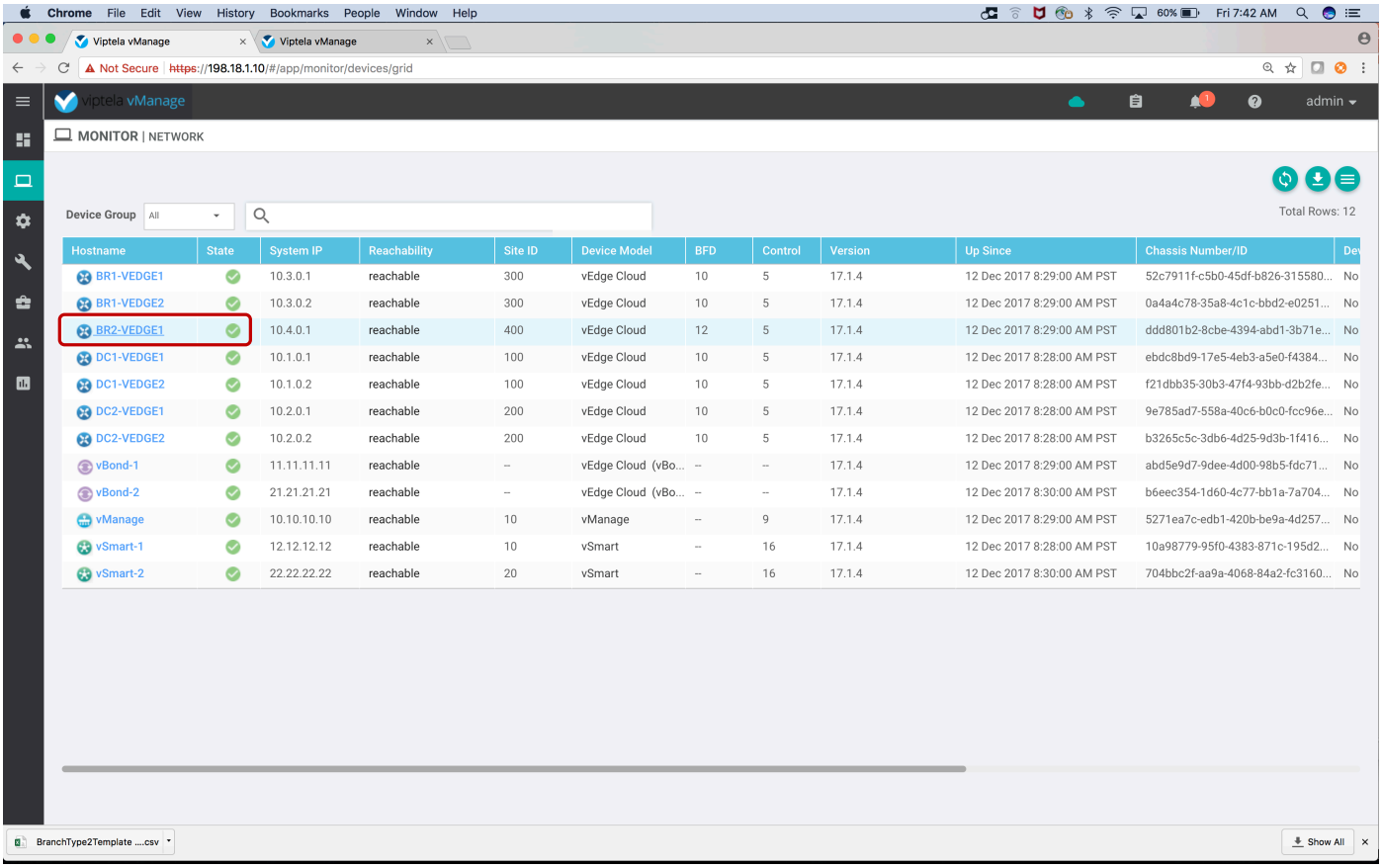
For guest WiFi VPN 40, we don't need any communication between the branches. We will restrict the route exchange between sites for VPN 40. There will be only one static default route in VPN 40 providing direct internet access.

Steps

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

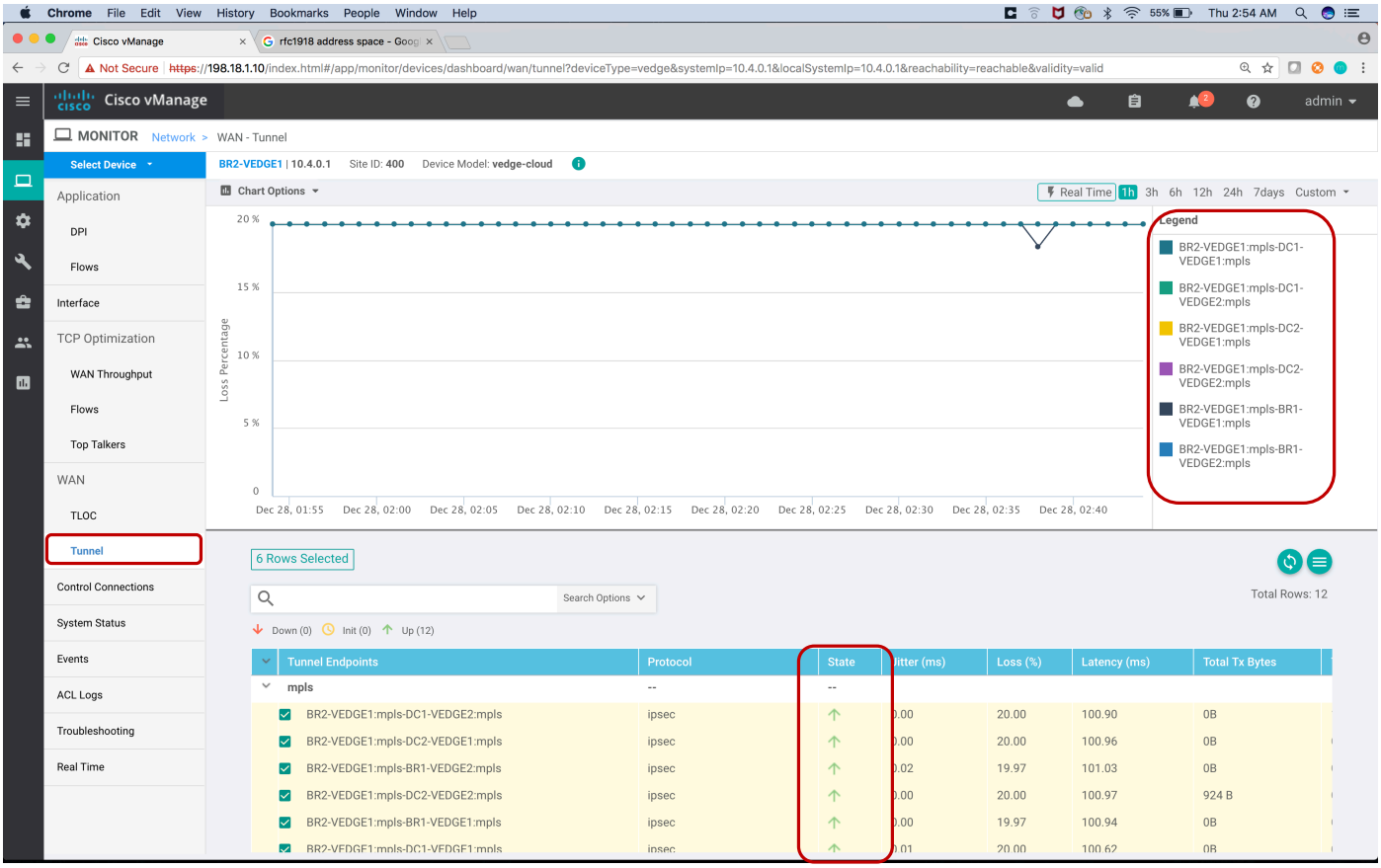


Find BR2-VEDGE1 and click on the name.

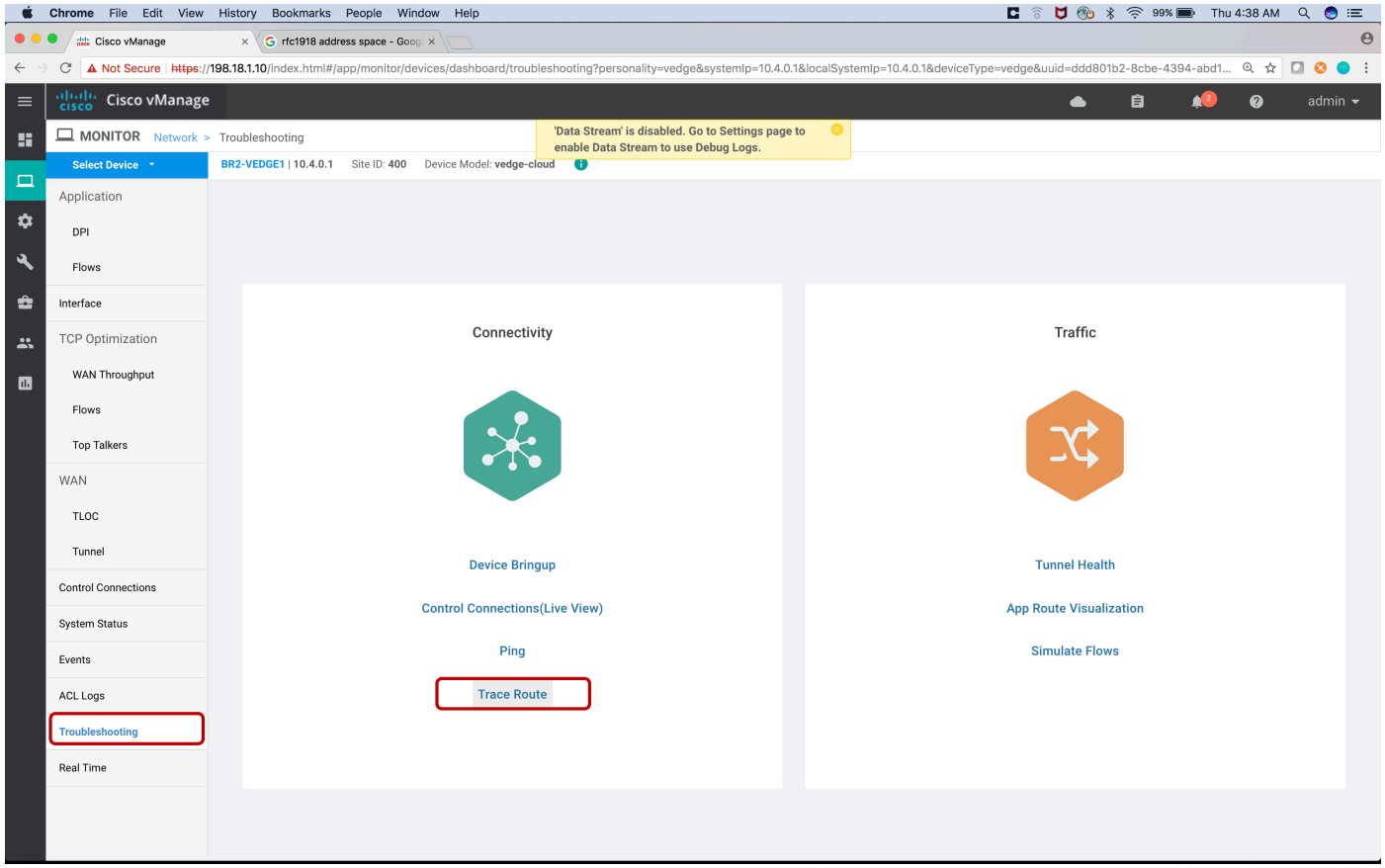


Select Tunnels from the left column.

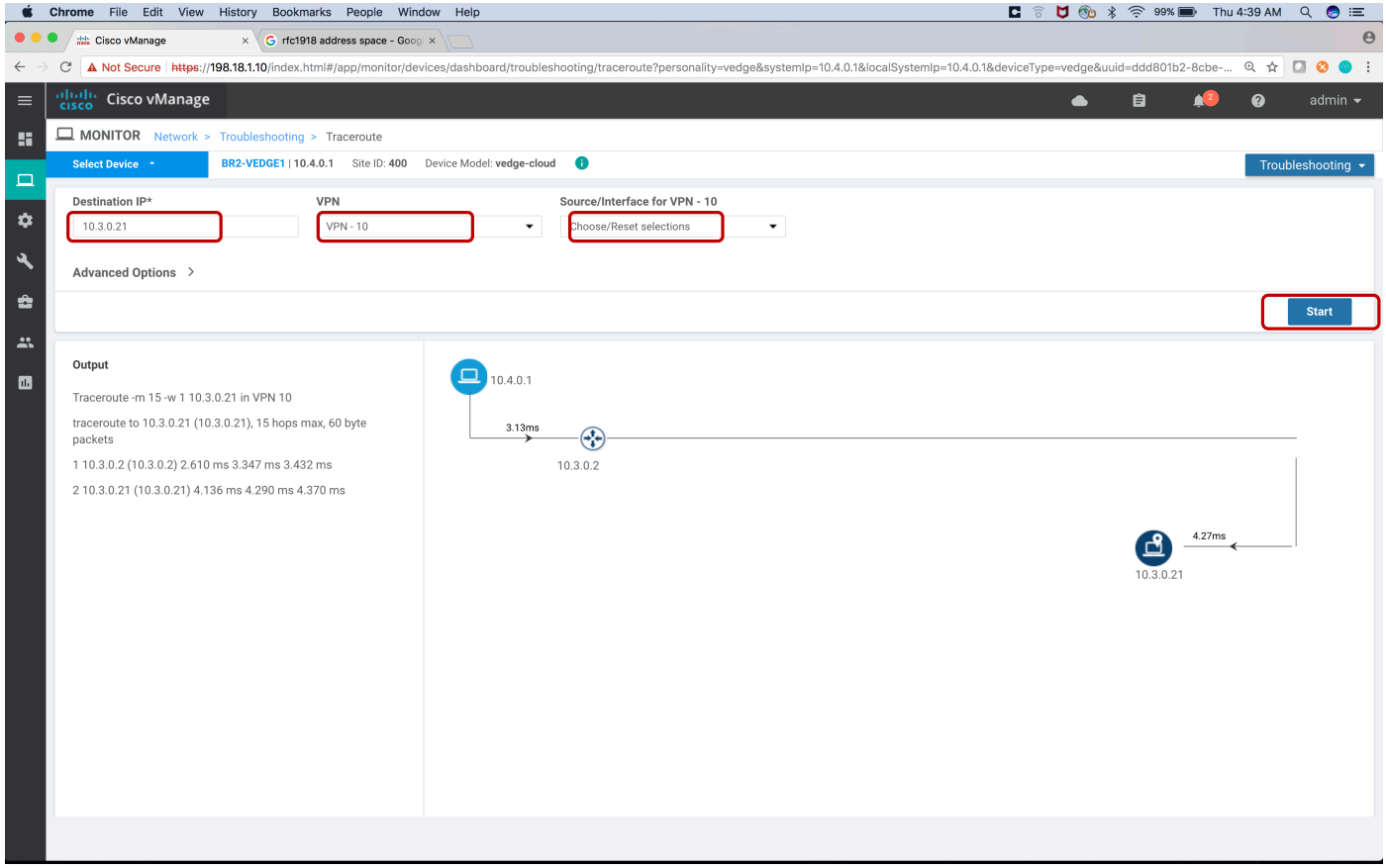
The next screen shows IPSec tunnels are established to the DCs and the remote Branch-1 (full mesh).



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



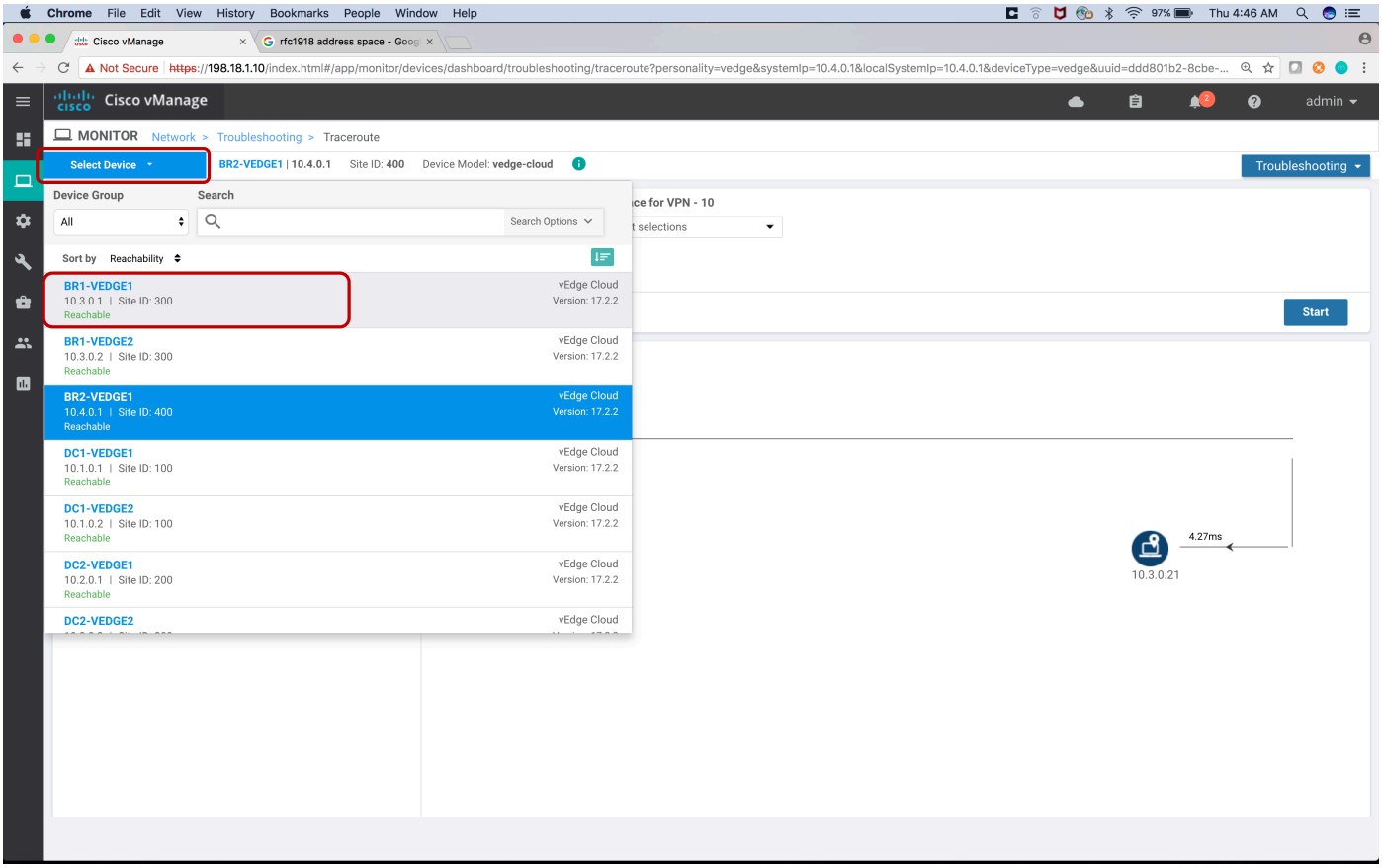
Select Traceroute using the radio button. Put in 10.3.0.21 as the destination IP for Branch1 in VPN 10. Select VPN 10 and source interface from the drop-down menu. And click on Start button.



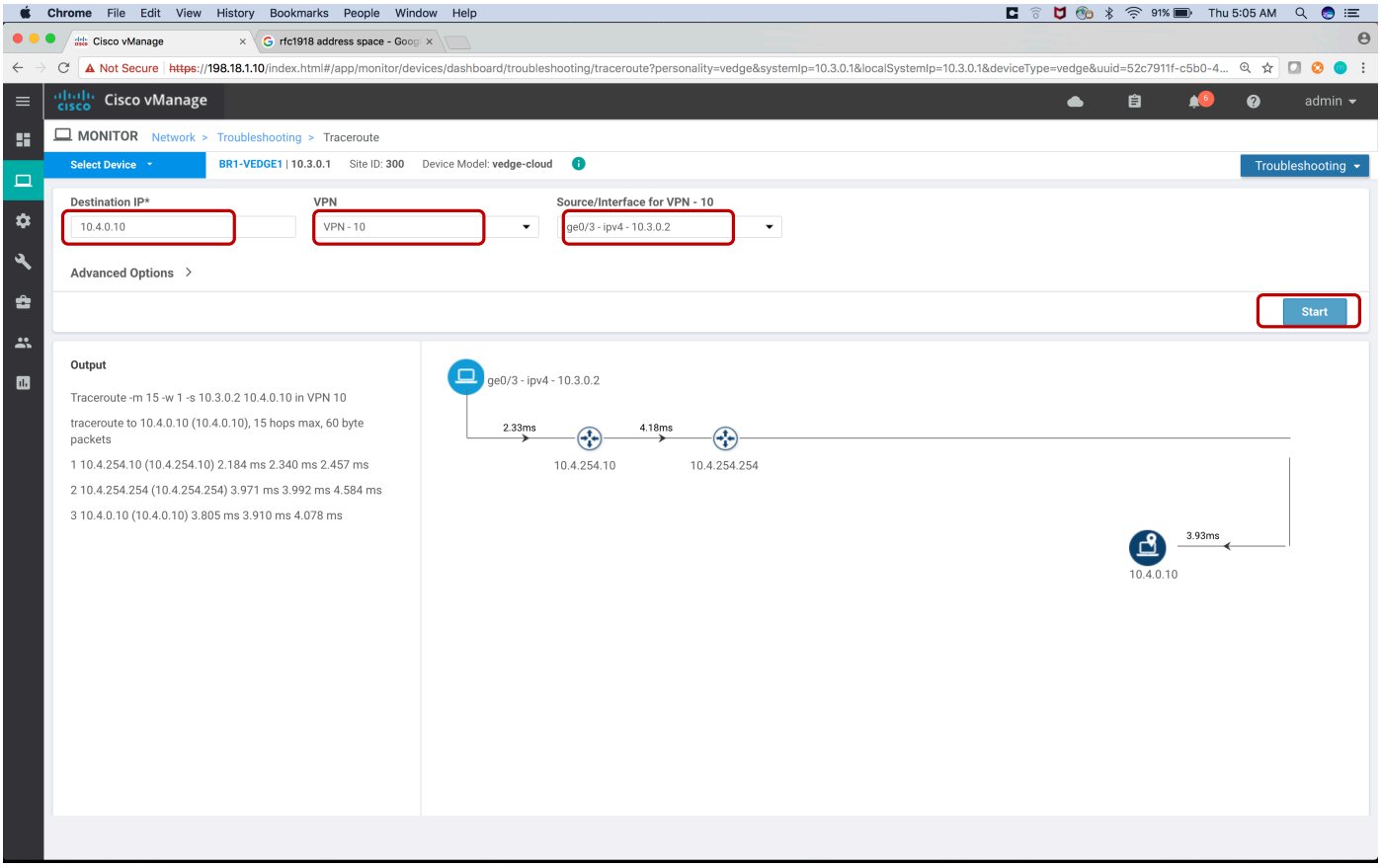
It shows direct connectivity between the Branch1 (10.3.0.21) and Branch2.

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

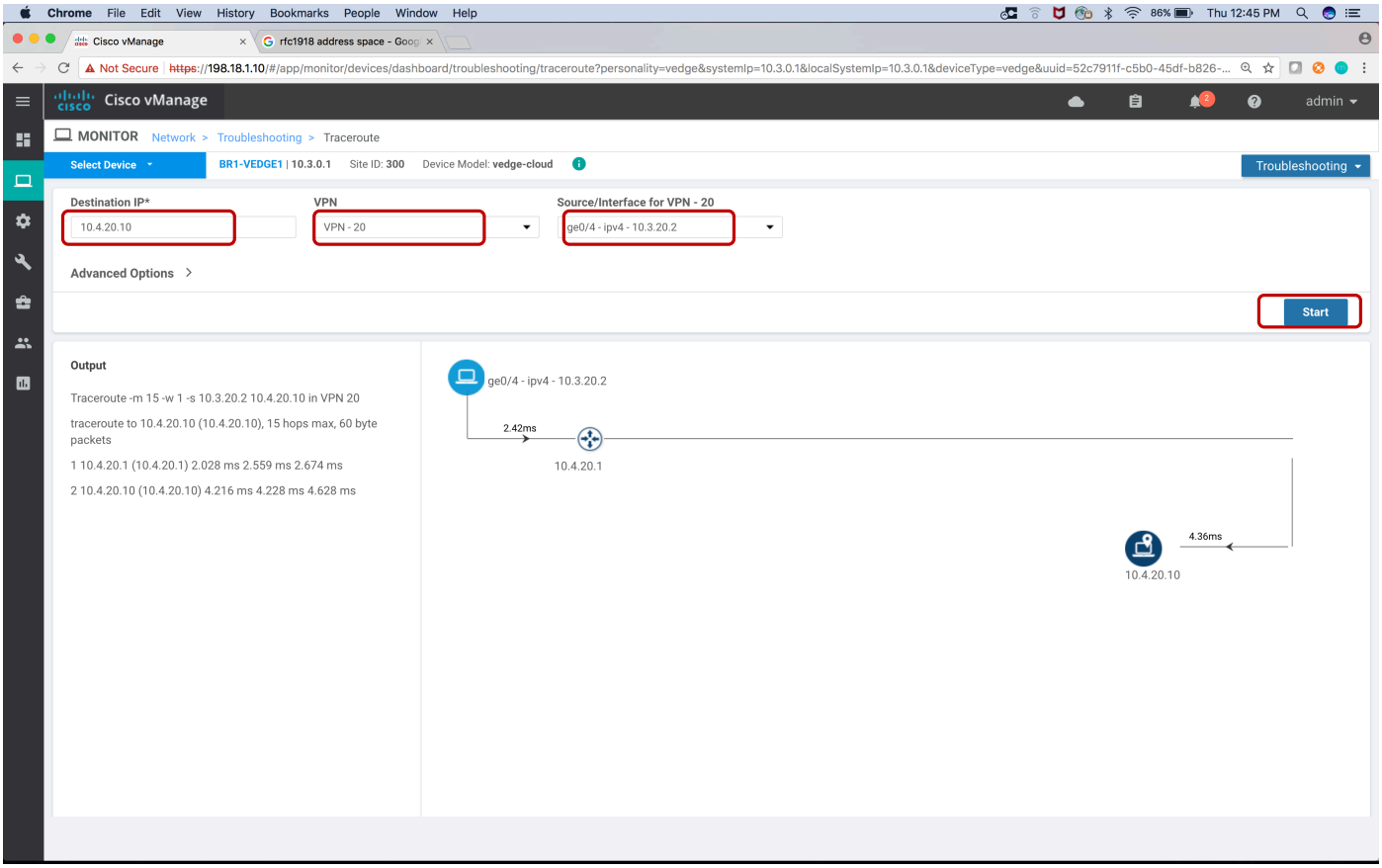
Do the same by selecting from Branch1. Click on Select Device and select BR1-VEDGE1.



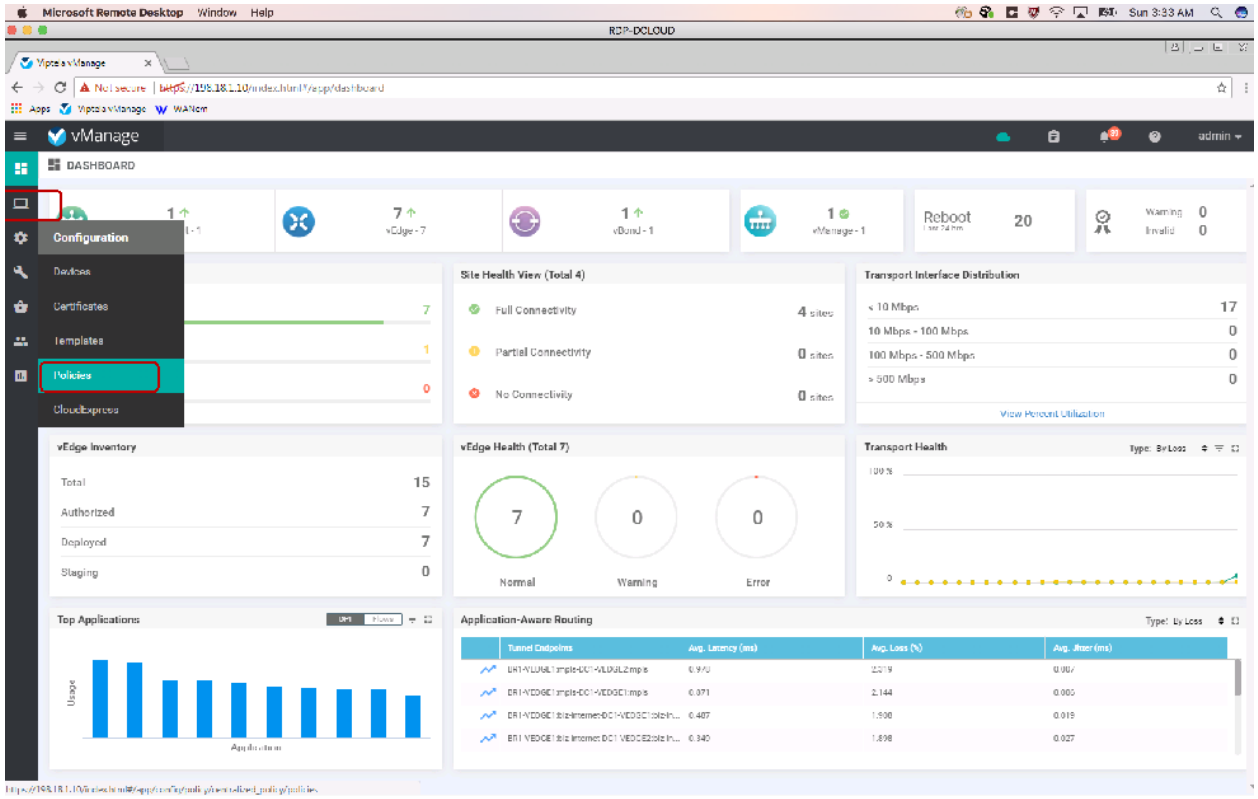
Select Traceroute, put in destination IP of 10.4.0.21, select VPN 10 and select source interface. Then click the Start button. You see additional hop because of additional CSR (router) in Branch 2.



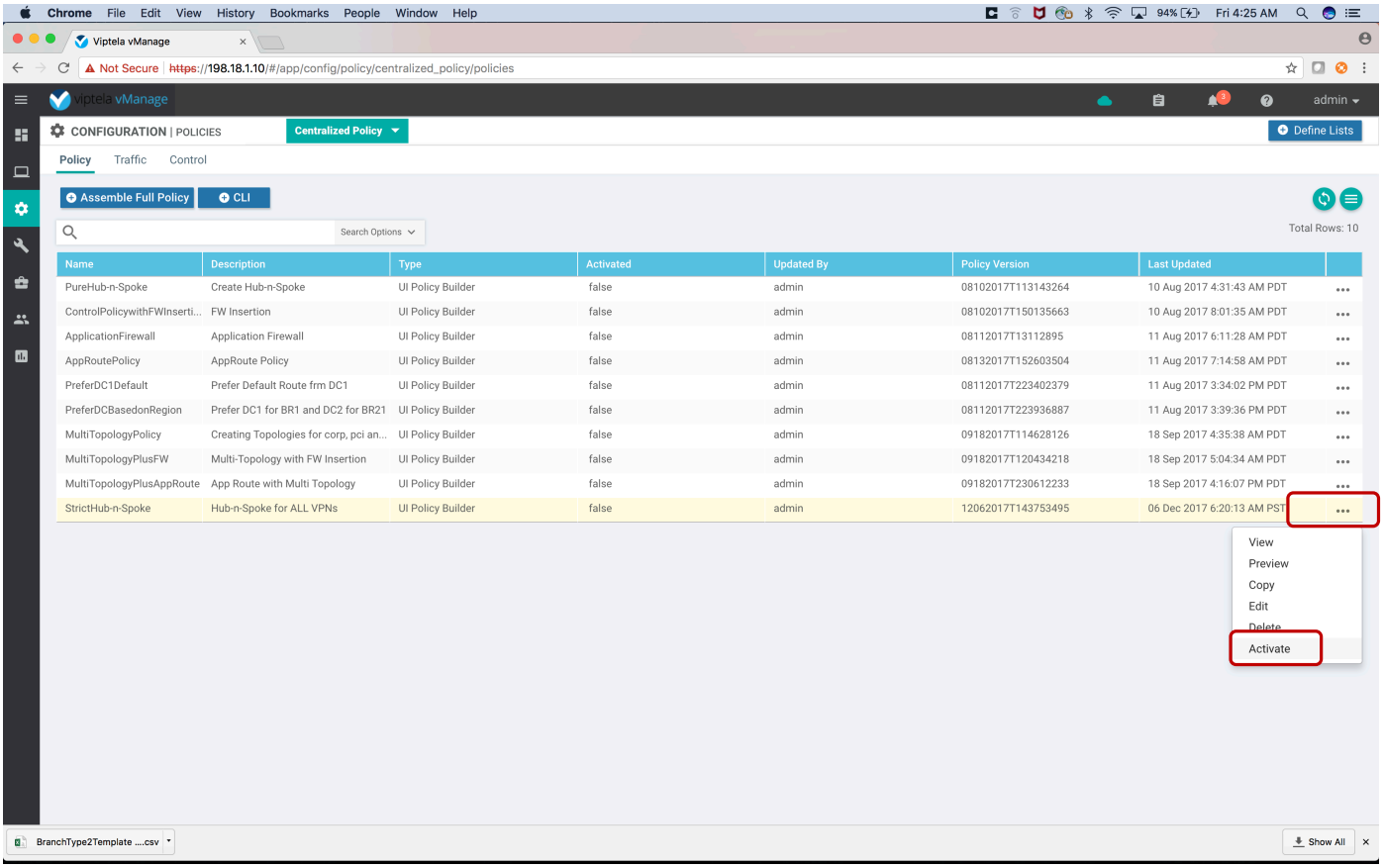
Do the same for VPN 20 by traceroute to the test host in VPN 20.



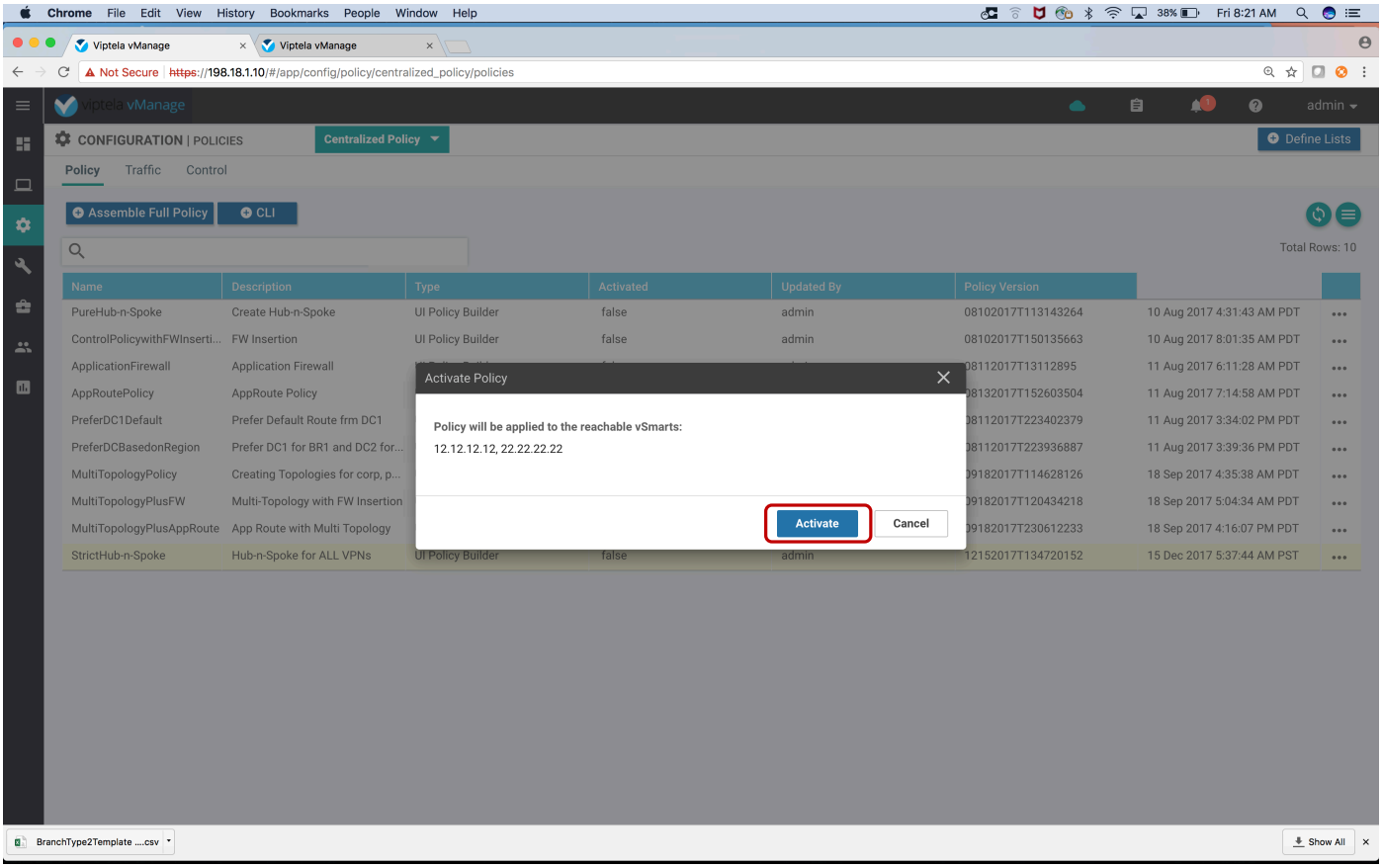
Go to vManage dashboard and go to Configuration and select Policies.



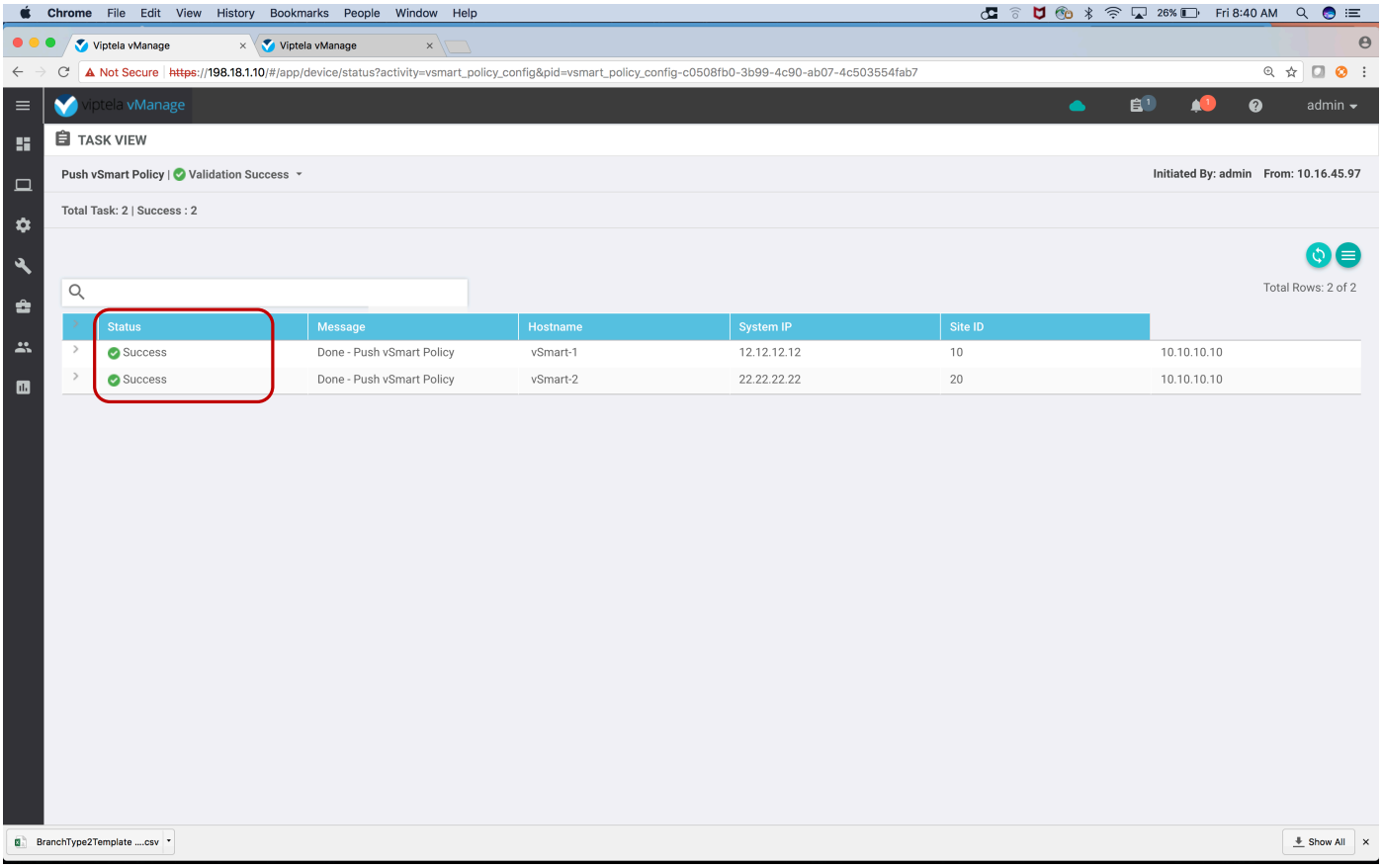
Click in the right most column of the policy named StrictHub-n-Spoke. From pull down click on Activate.



Click on Activate button on the pop-up.

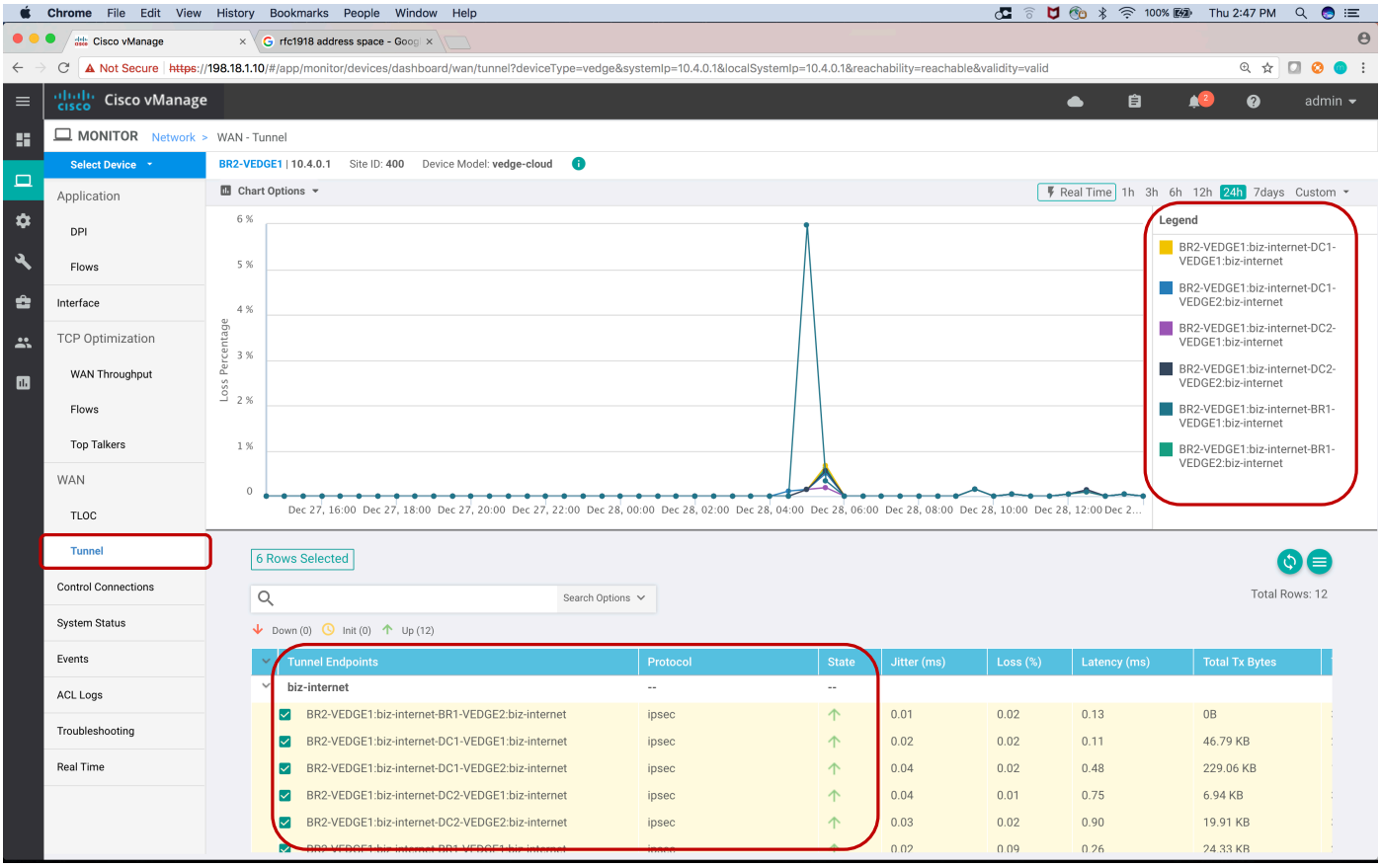


Wait until the policy activation Status changes to Success. The policy will be applied to vSmart controllers. vSmart will push the policies to the appropriate vEdge routers.



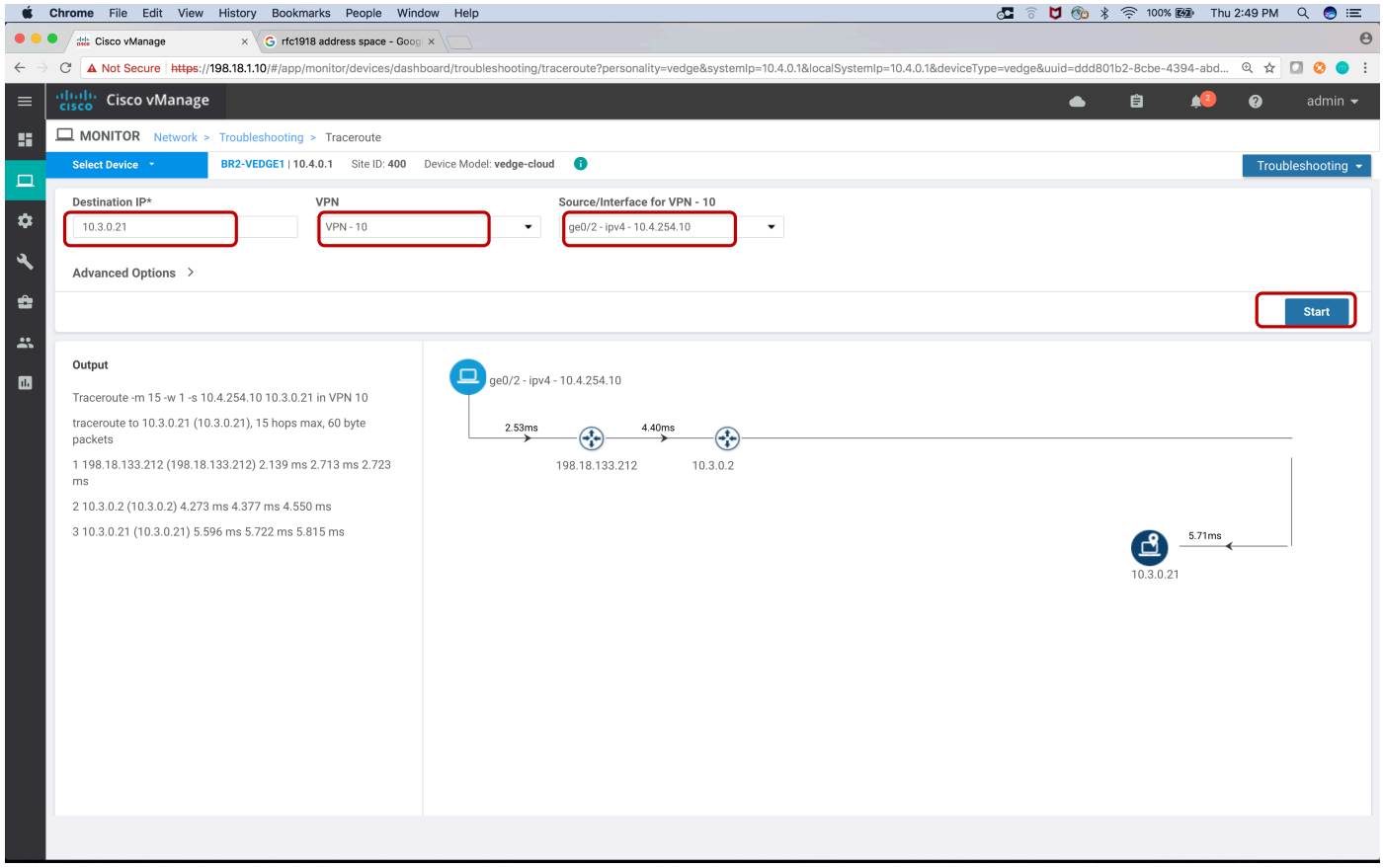
Validate Strict Hub-n-Spoke topology by going to device dashboard.

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

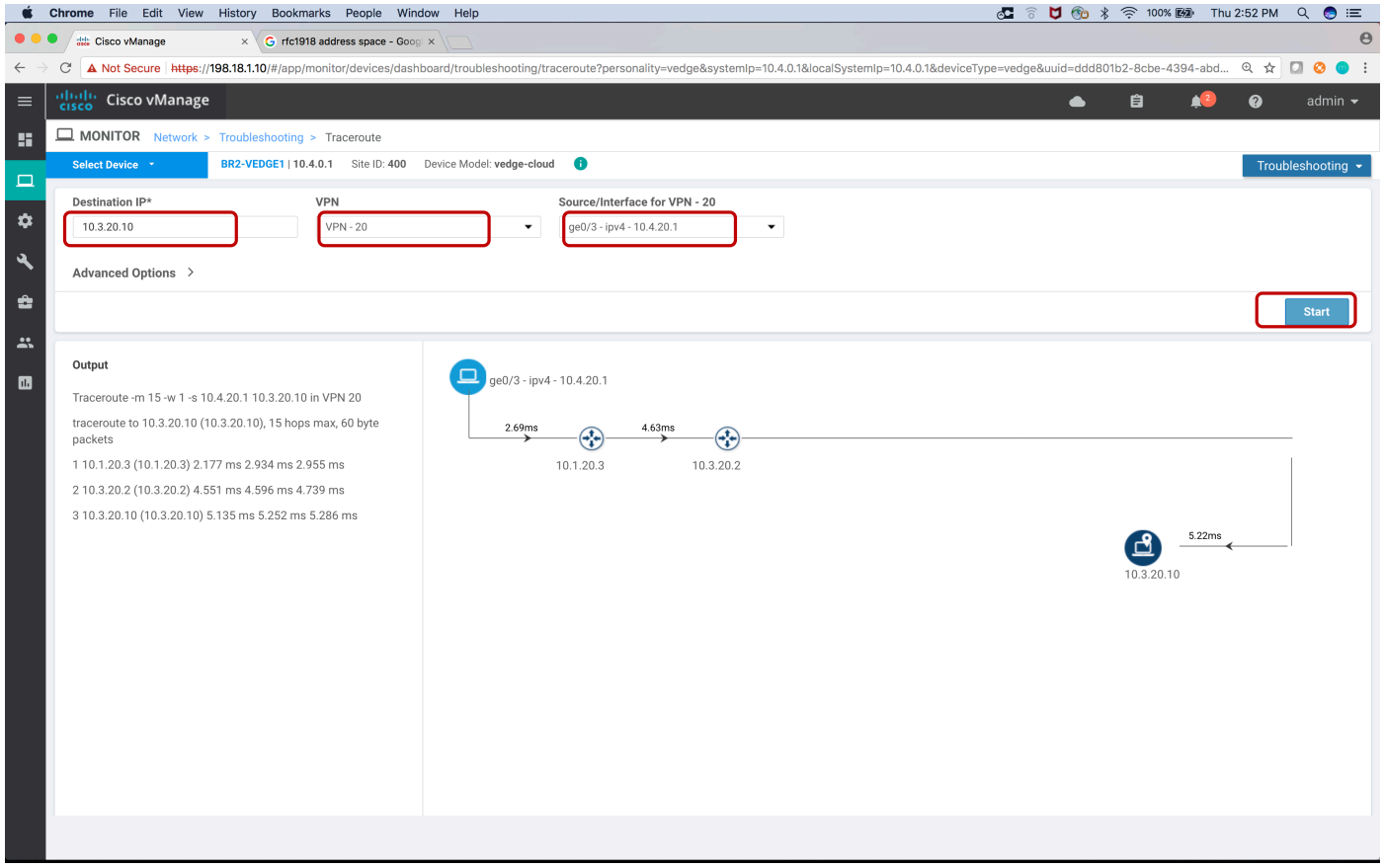


Traceroute from Branch-2 and Branch-1 in VPN10 and VPN20.

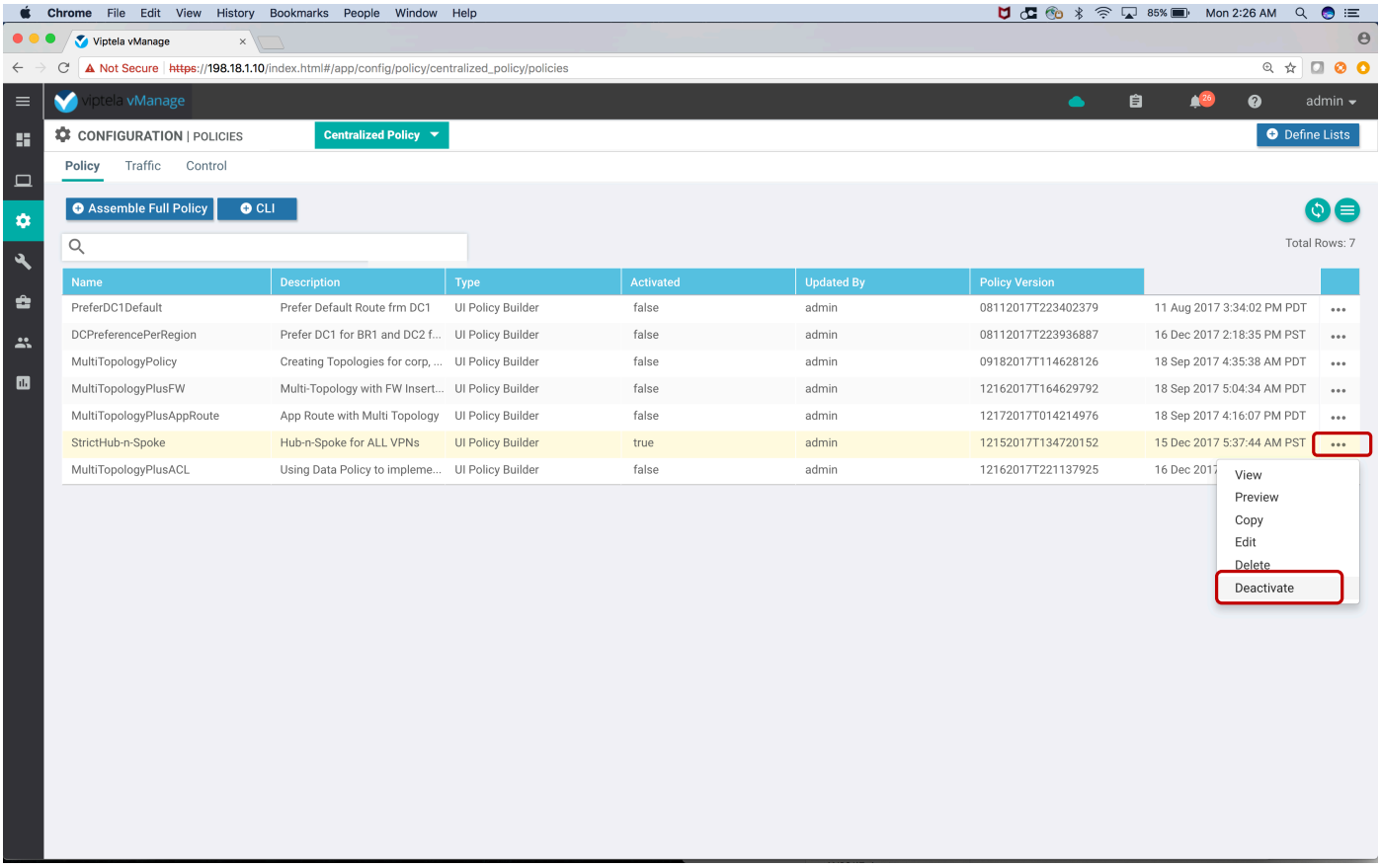
Traceroute from BR2 to BR1. Use destination IP of 10.3.0.21 in VPN 10.



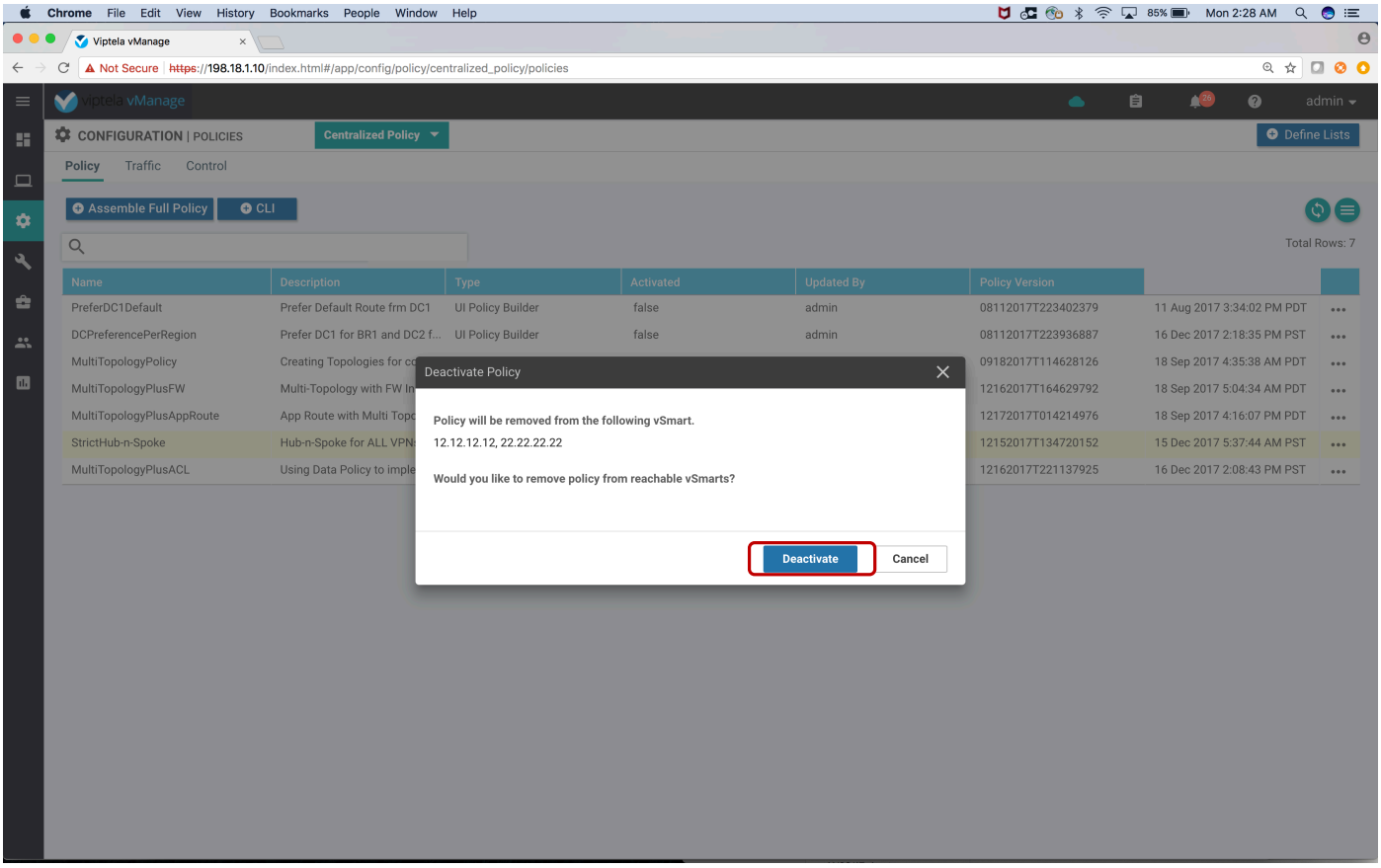
Traceroute from BR2 to BR1 in VPN 20. Use destination IP of 10.3.20.10 in VPN 20.



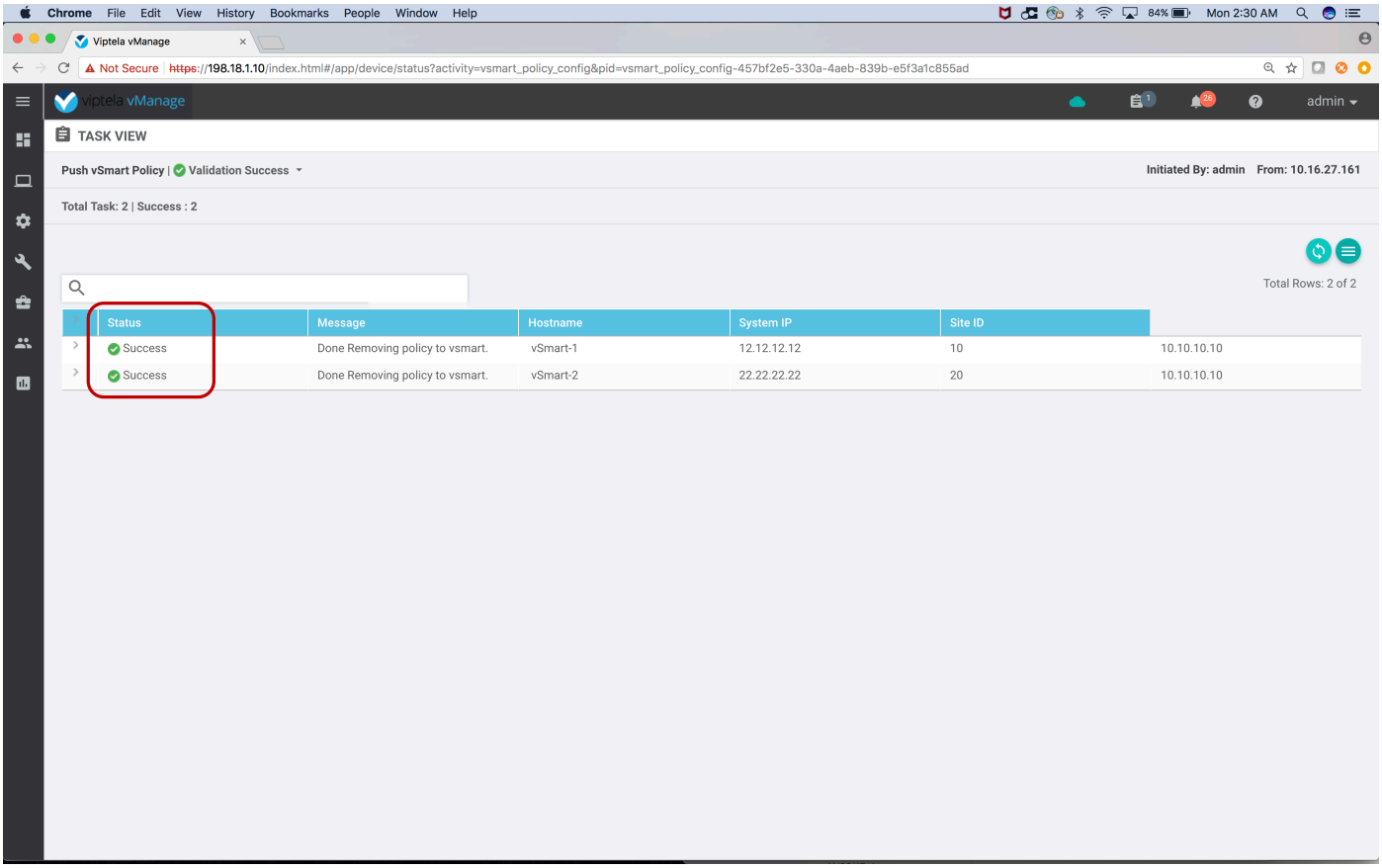
Deactivate the policy. From main dashboard select Configuration then Policies and select the StrictHub-n-Spoke policy and Deactivate.



Click on “Deactivate” button.



Wait till the policy is successfully removed from the vSmarts.



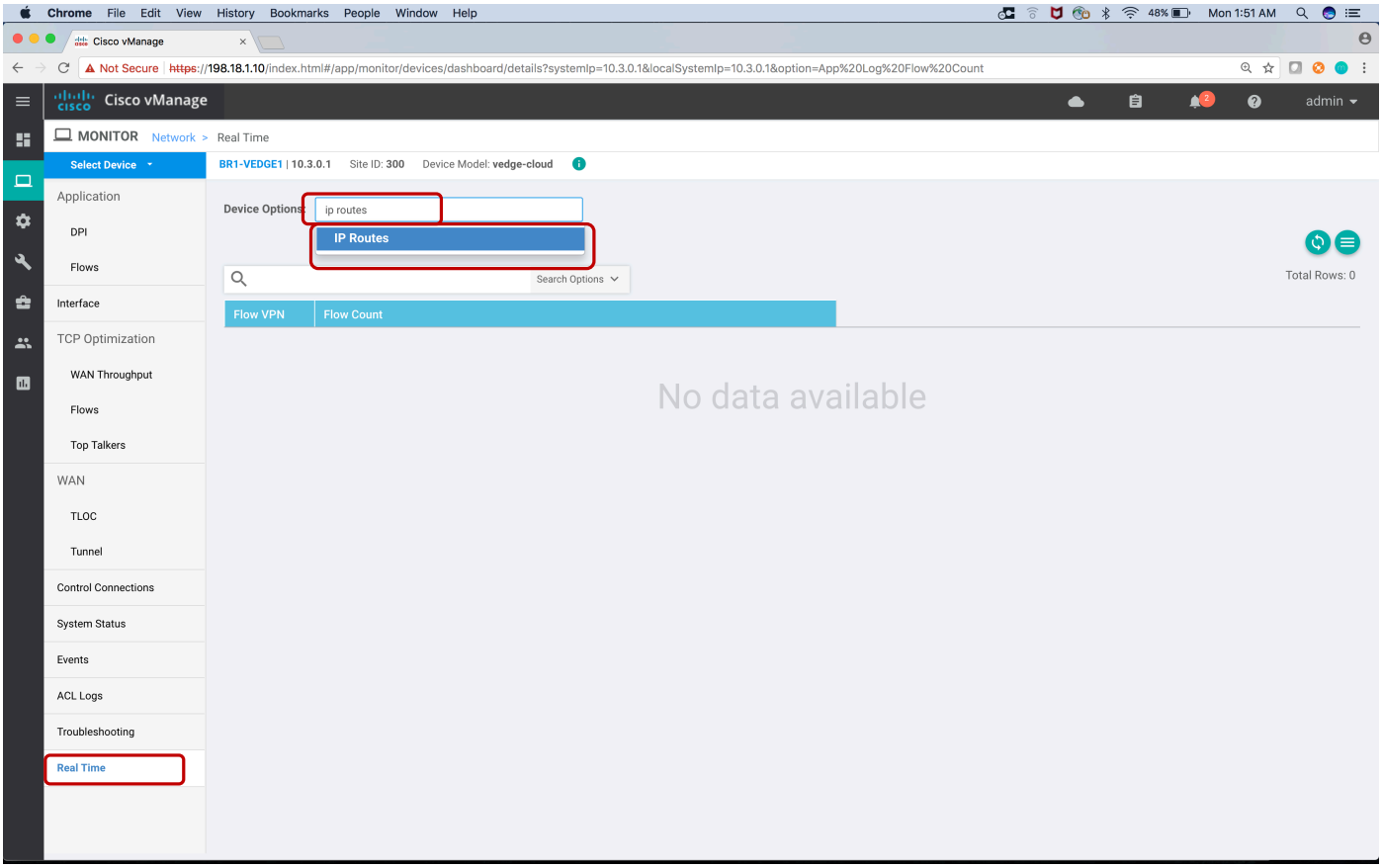
Lab 03 - Prefer Data Center DC1 and DC2 for Different Set of Branches for Regional Internet Exit

In some cases, the Enterprise may want different Branches to take different Regional Exits to the Internet on the same Overlay.

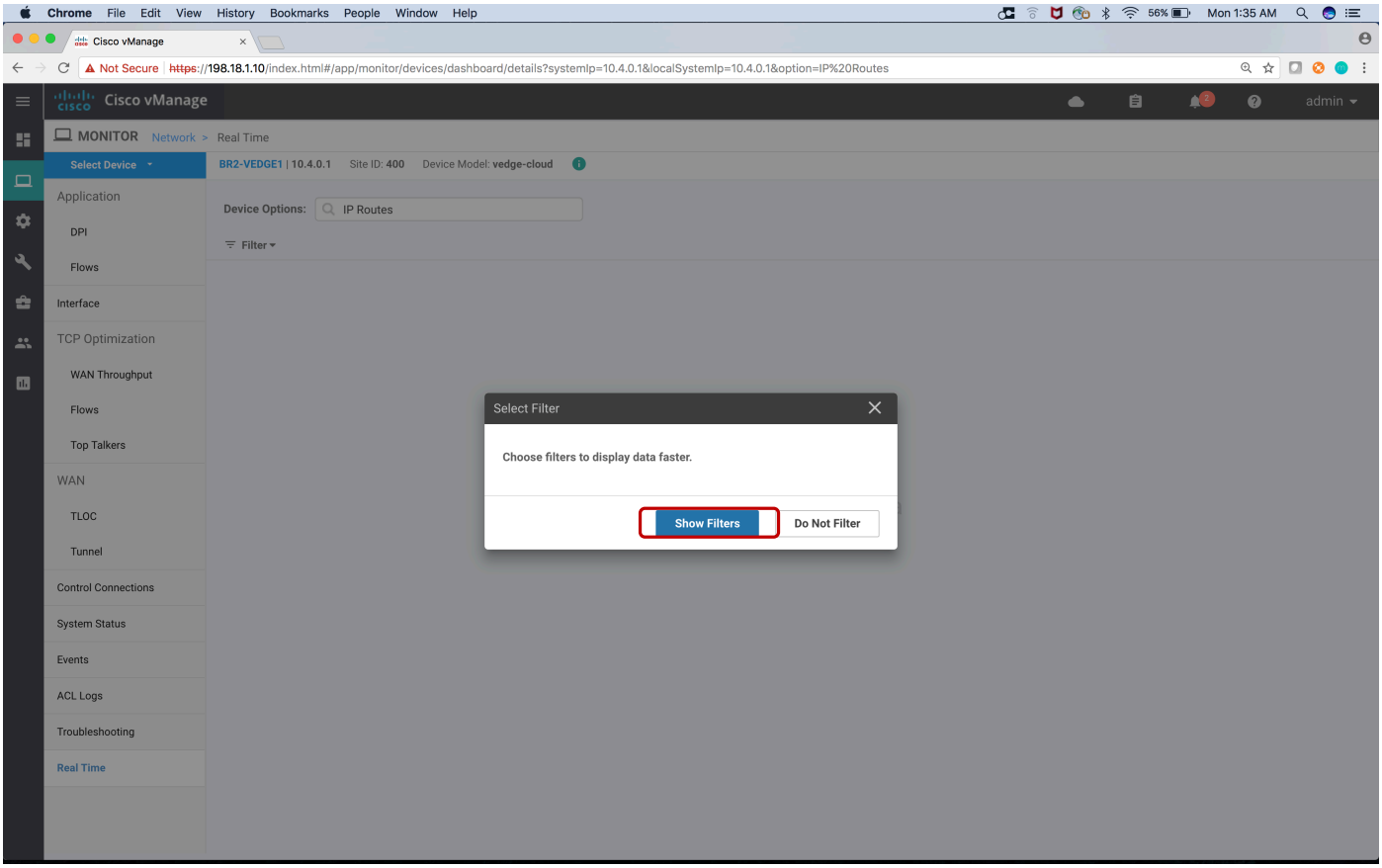
Let's say in this case the customer wants DC1 the preferred exit for Branch 1 and DC2 is the preferred exit for Branch 2.

Steps

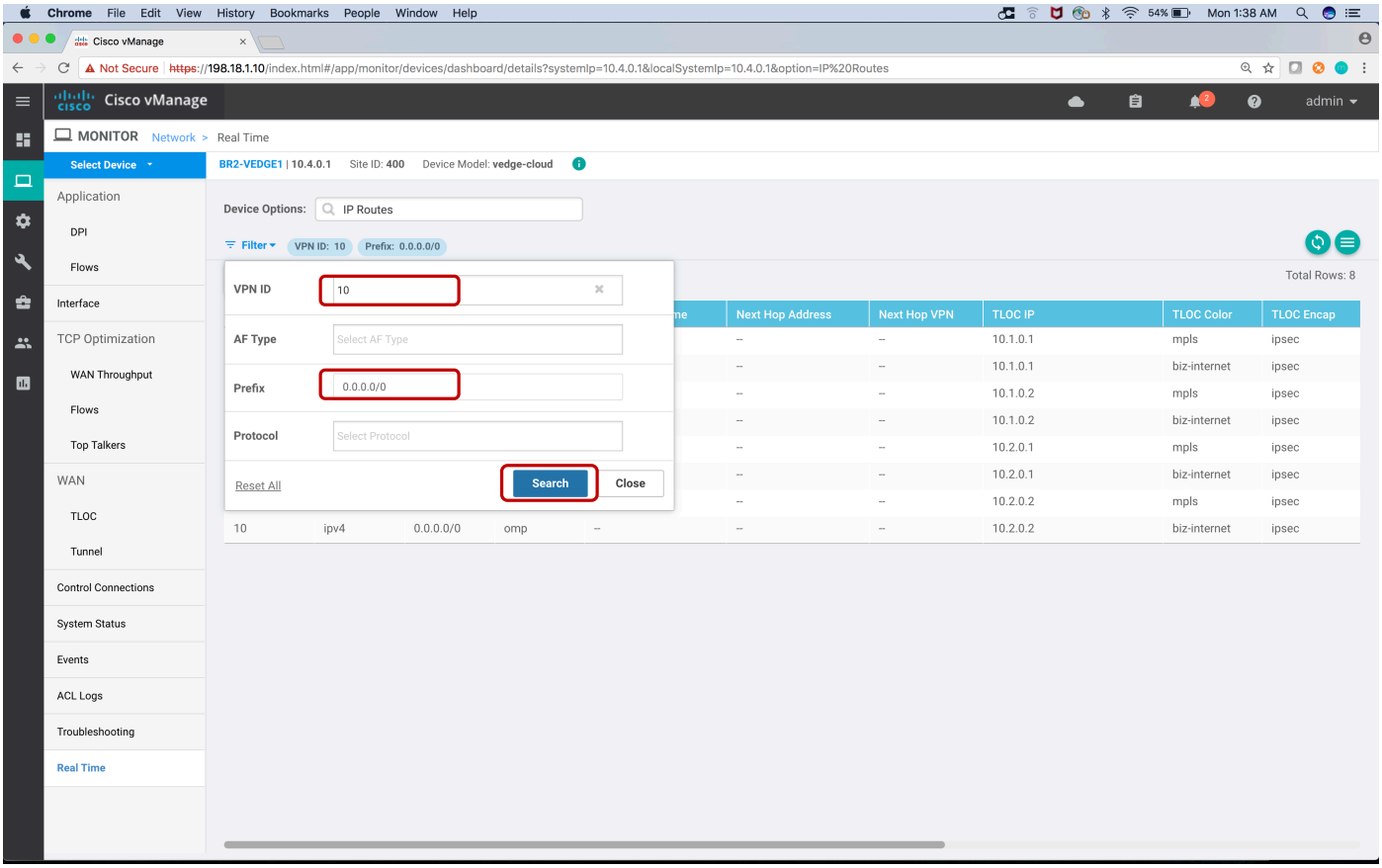
Go to Device dashboard for BR1-VEDGE1 and Click on "Real Time" tab. In the dialogue box, search for "ip routes". Select the "IP Routes" from pull down menu.



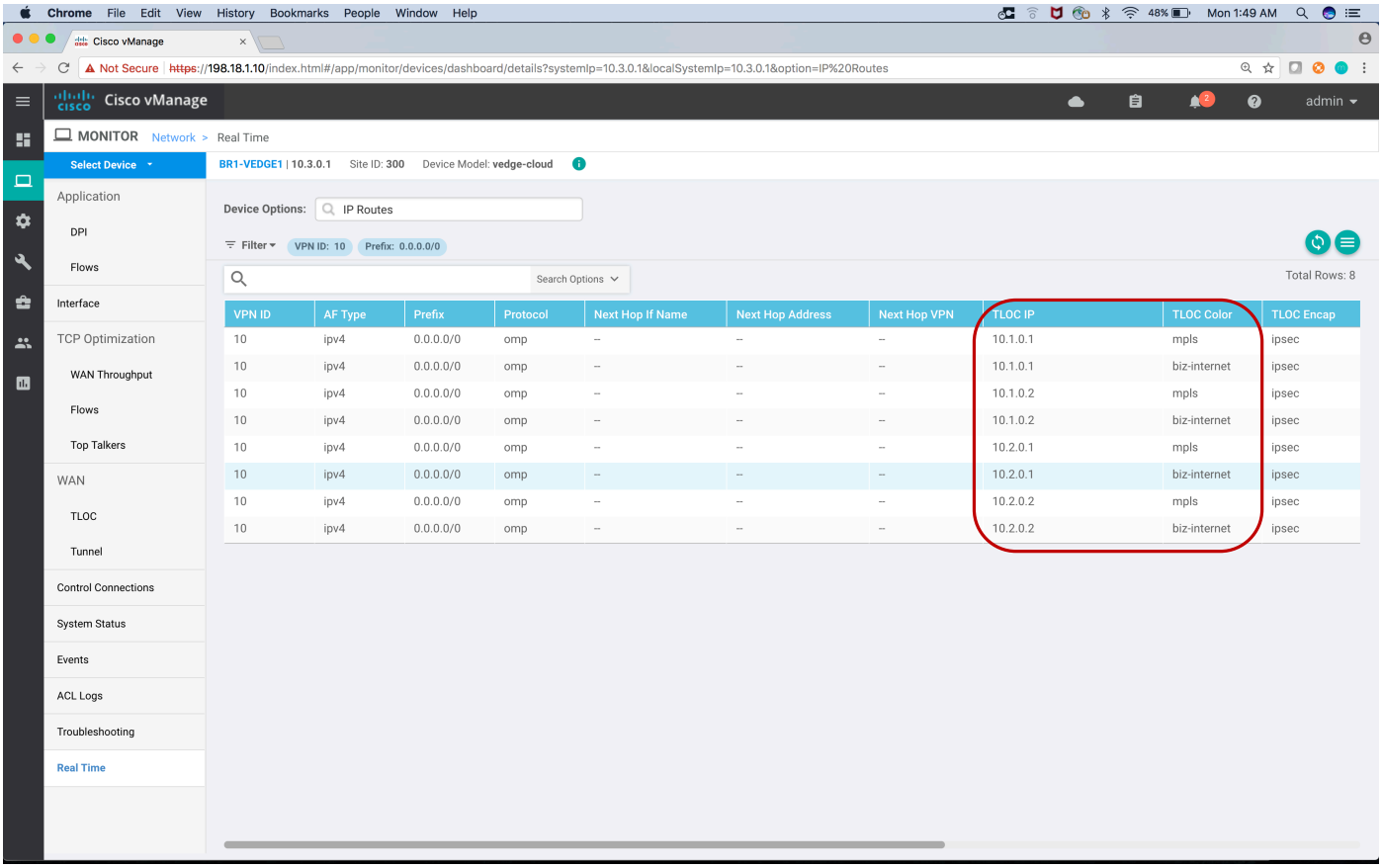
On the next pop-up select "Show Filters".



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

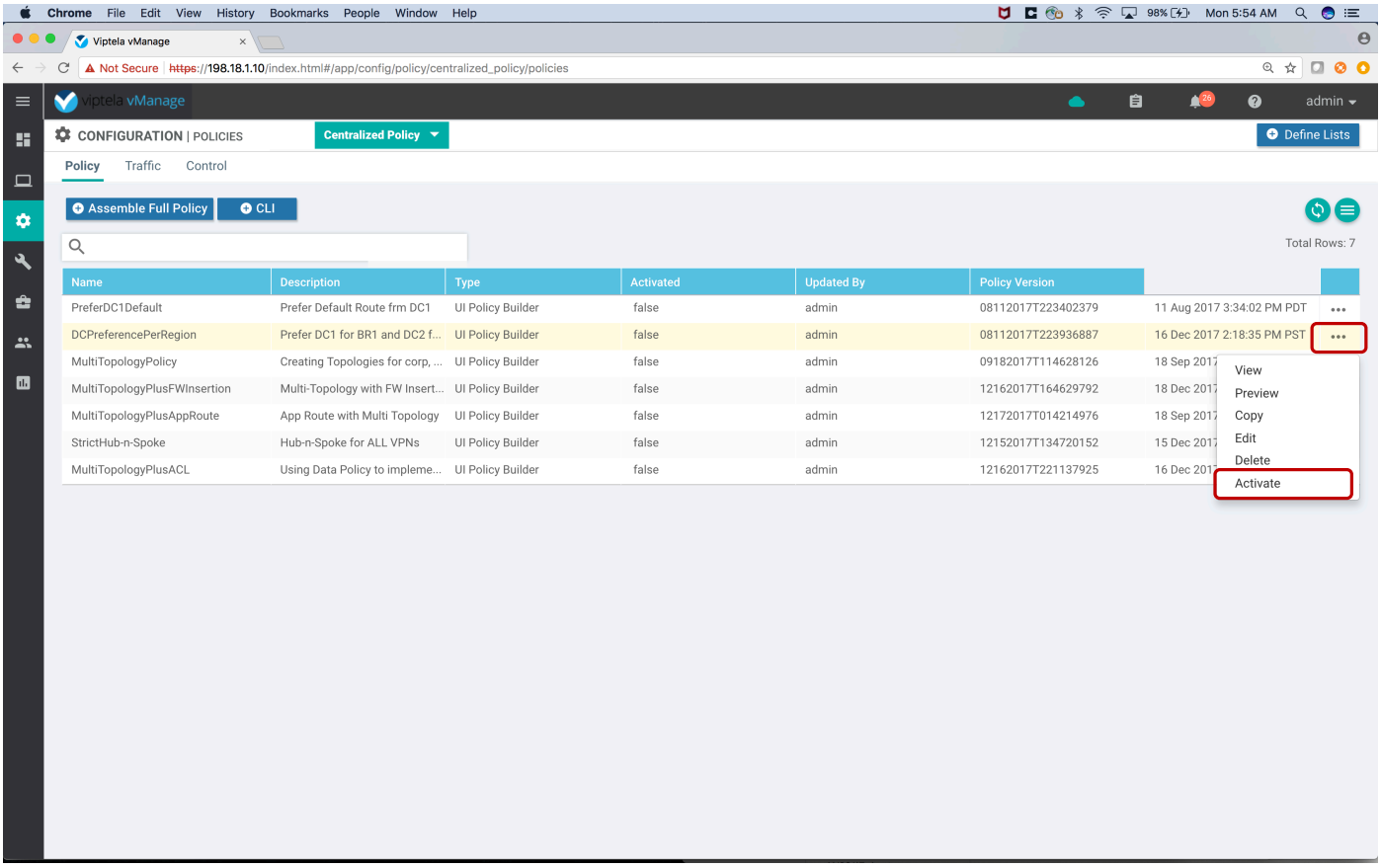


The next screen will show default route being load-shared across the two DCs.

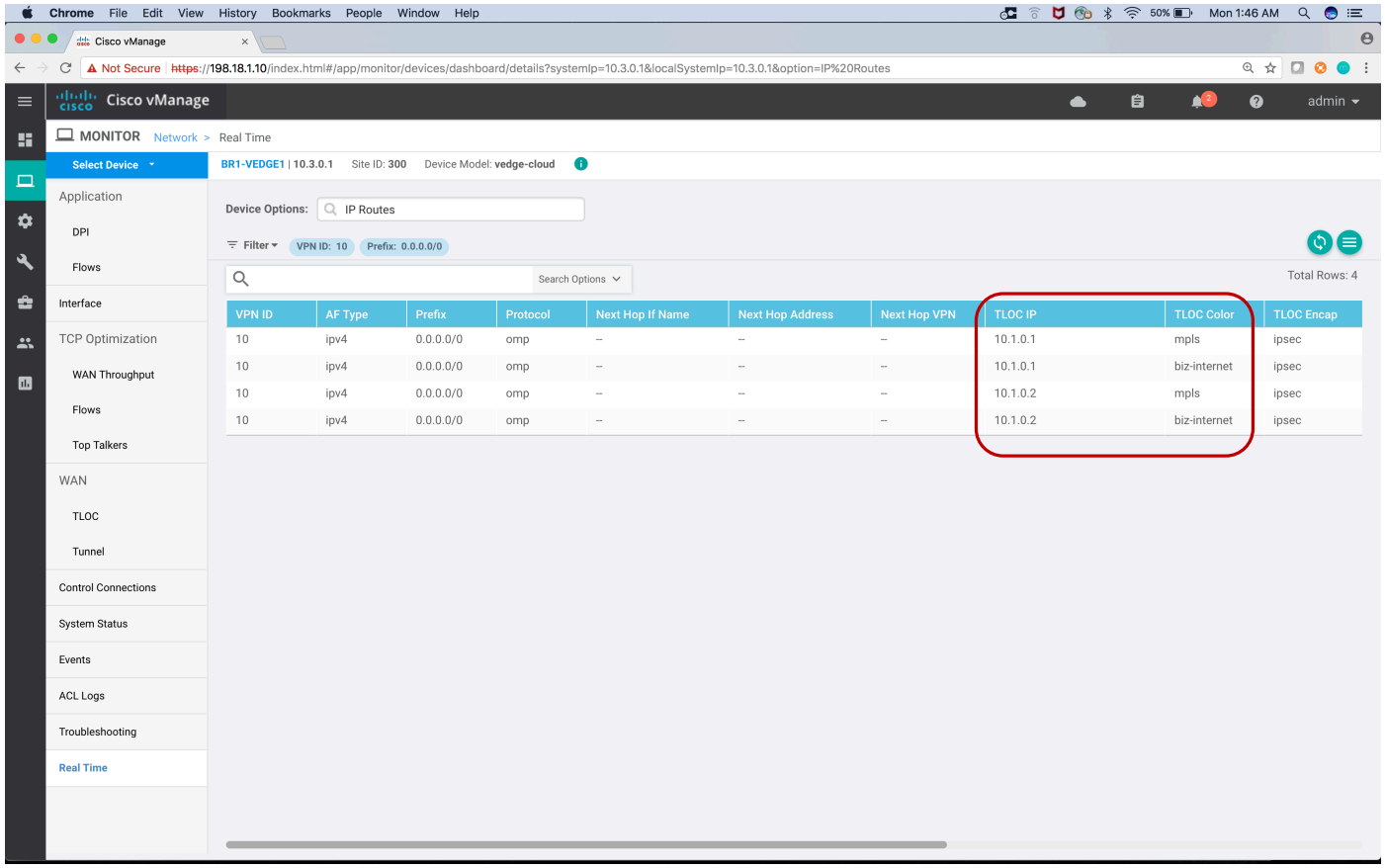


Go to BR2-VEDGE1 device dashboard and it will show the same for the default.

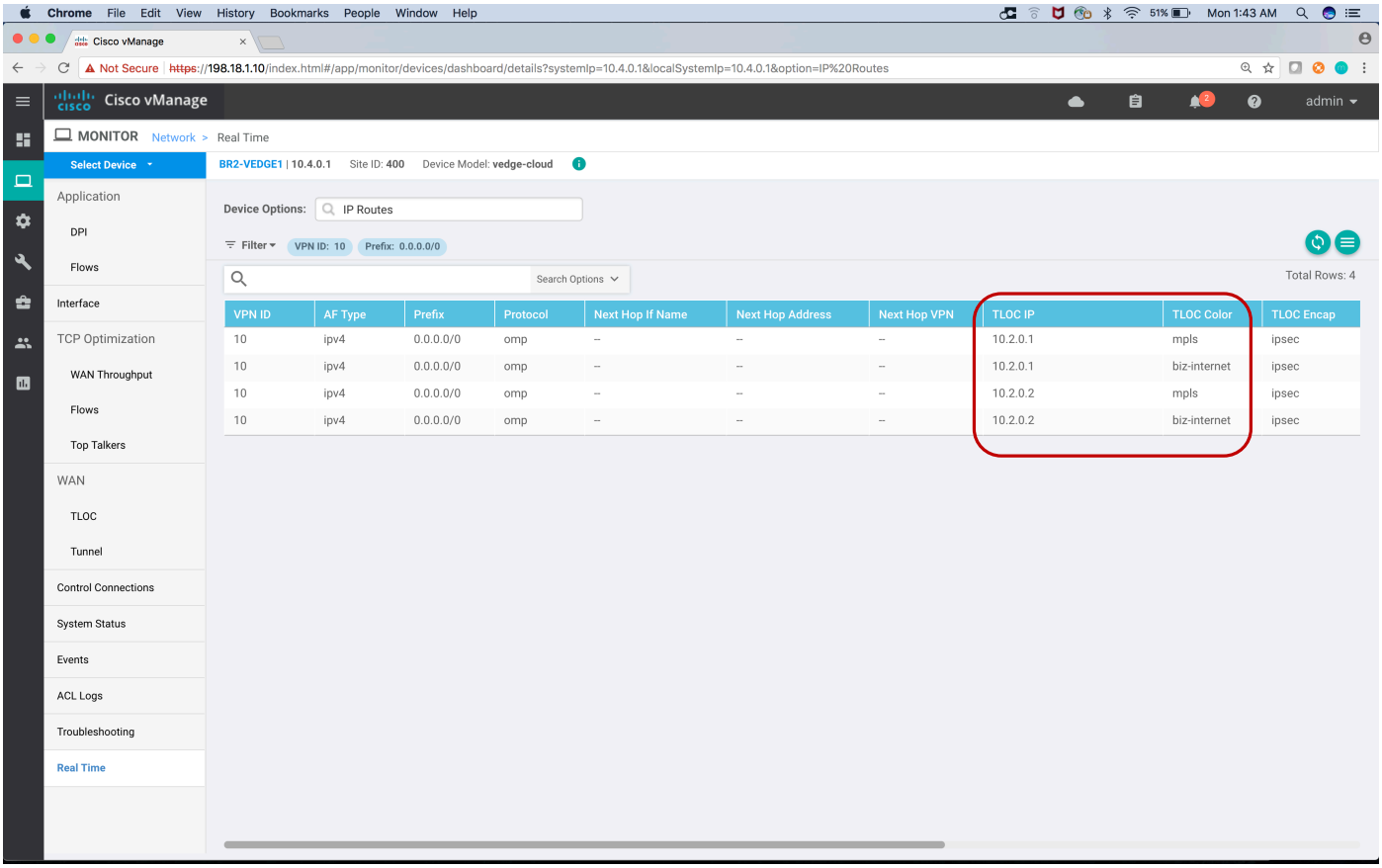
Activate the policy named “DCPreferencePerRegion”.



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



Deactivate the policy.

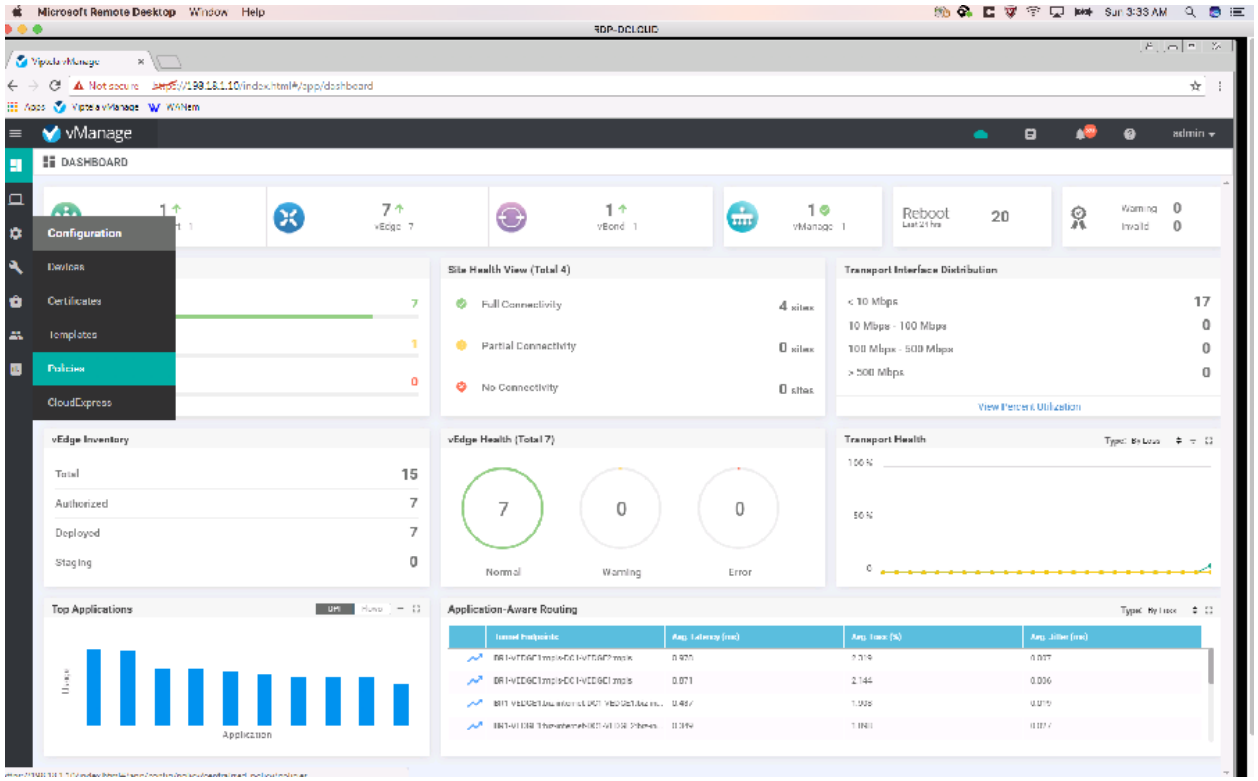
Lab 04 - Service (FW) Insertion

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.

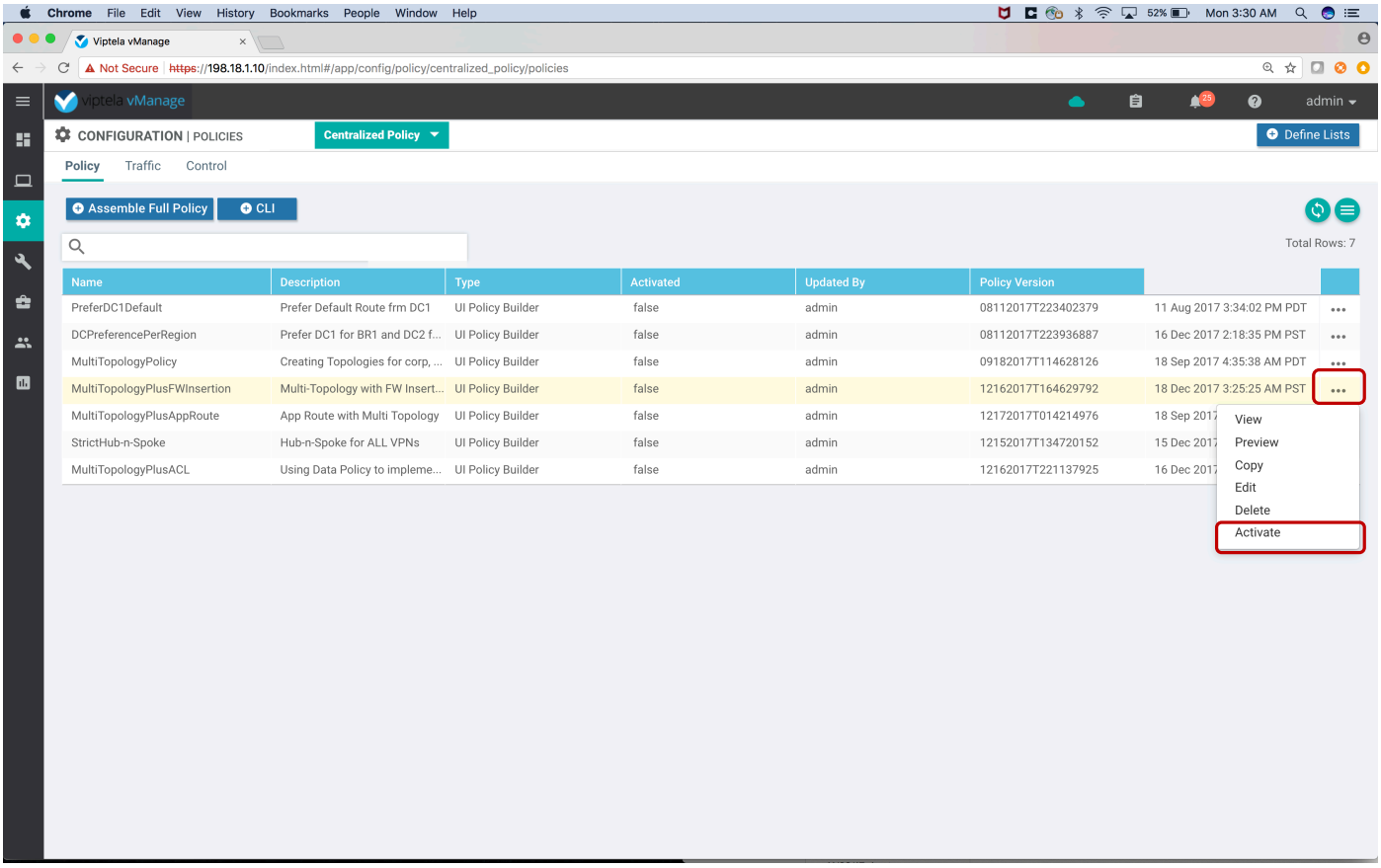
Using Cisco SD-WAN, services can be deployed anywhere in the network and based on policies redirect flows/site-traffic through those services.

Steps

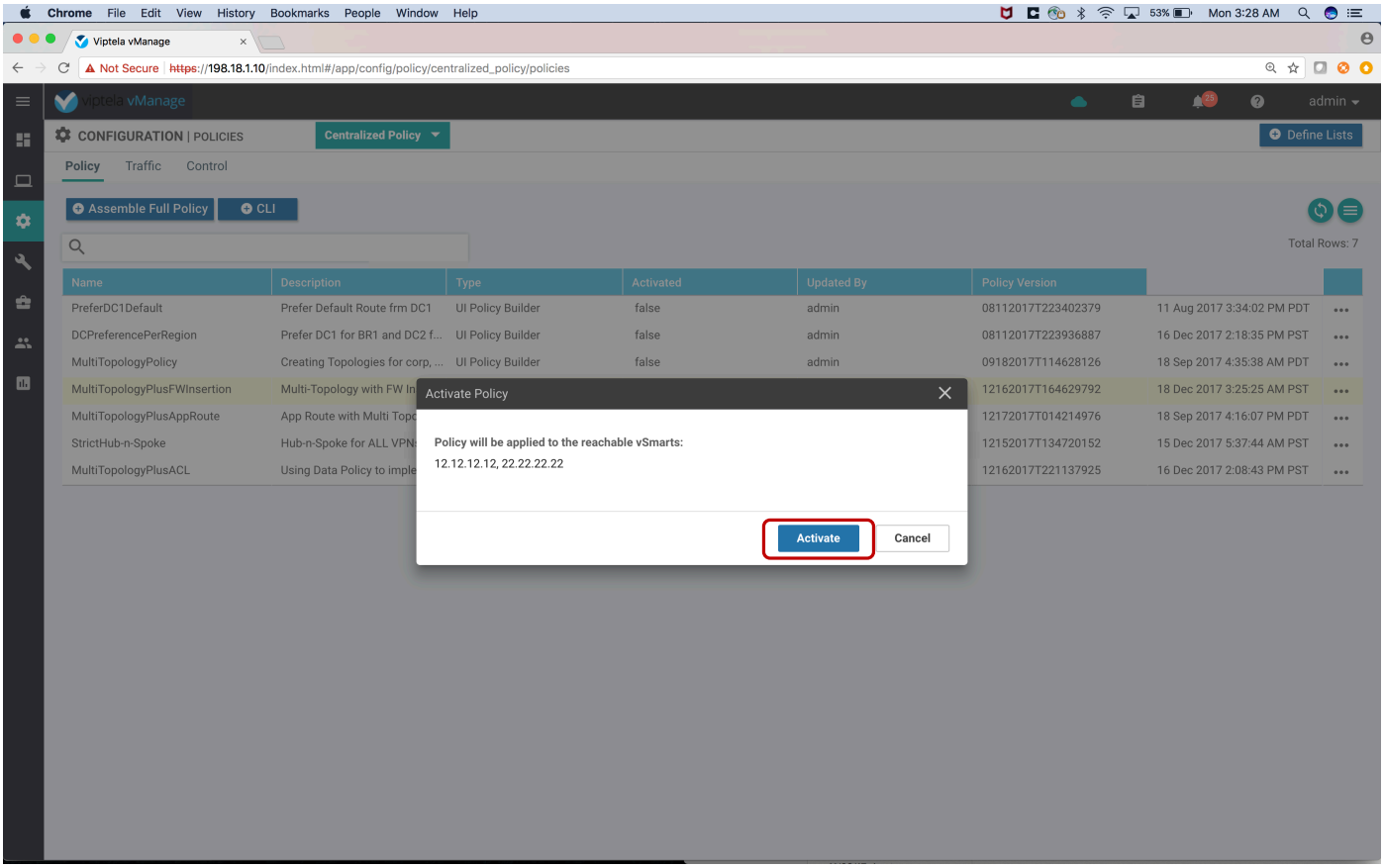
Go to vManage dashboard and go to Configuration and select Policies.



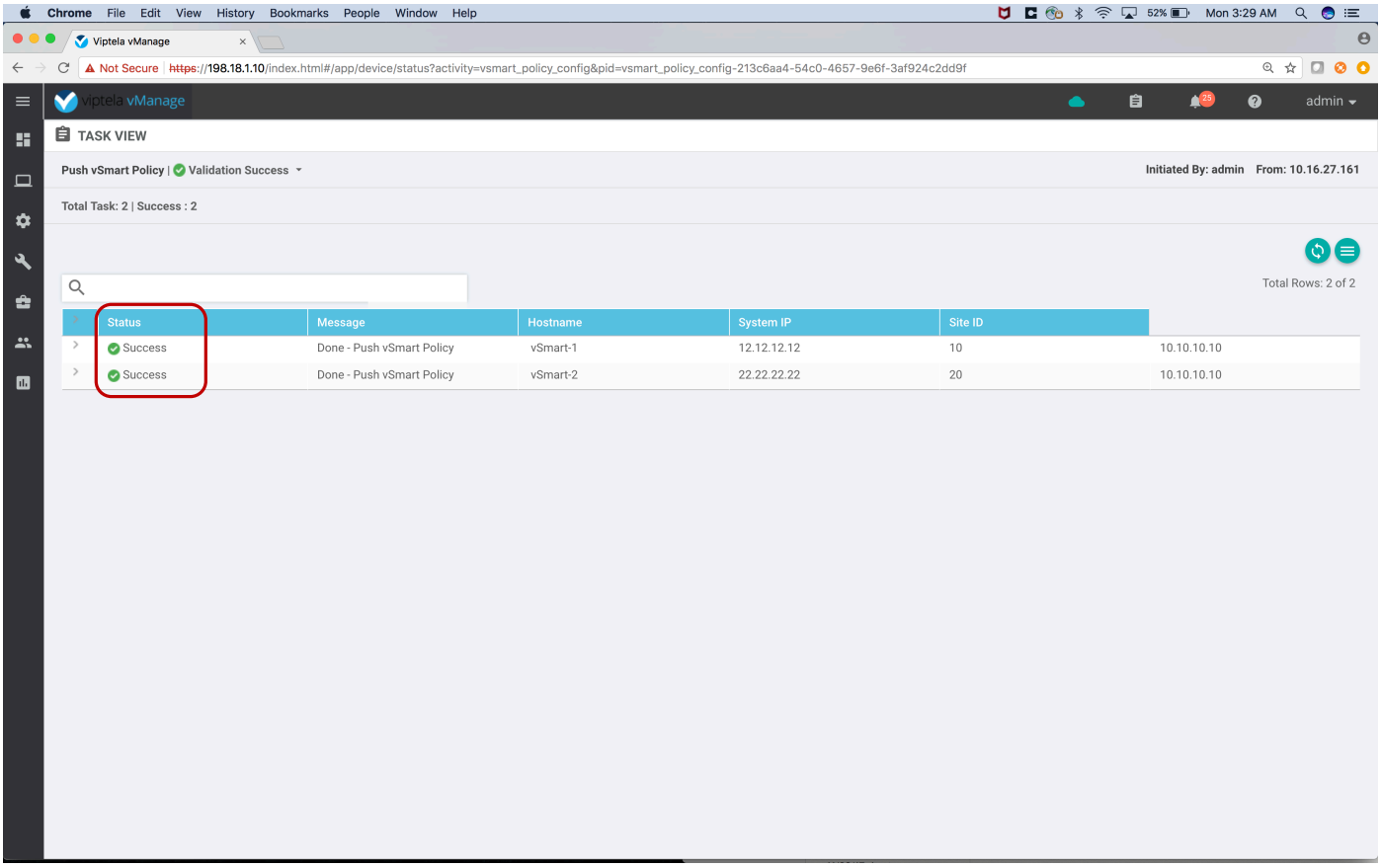
Activate the policy named “MultiTopologyPlusFWInsertion”.



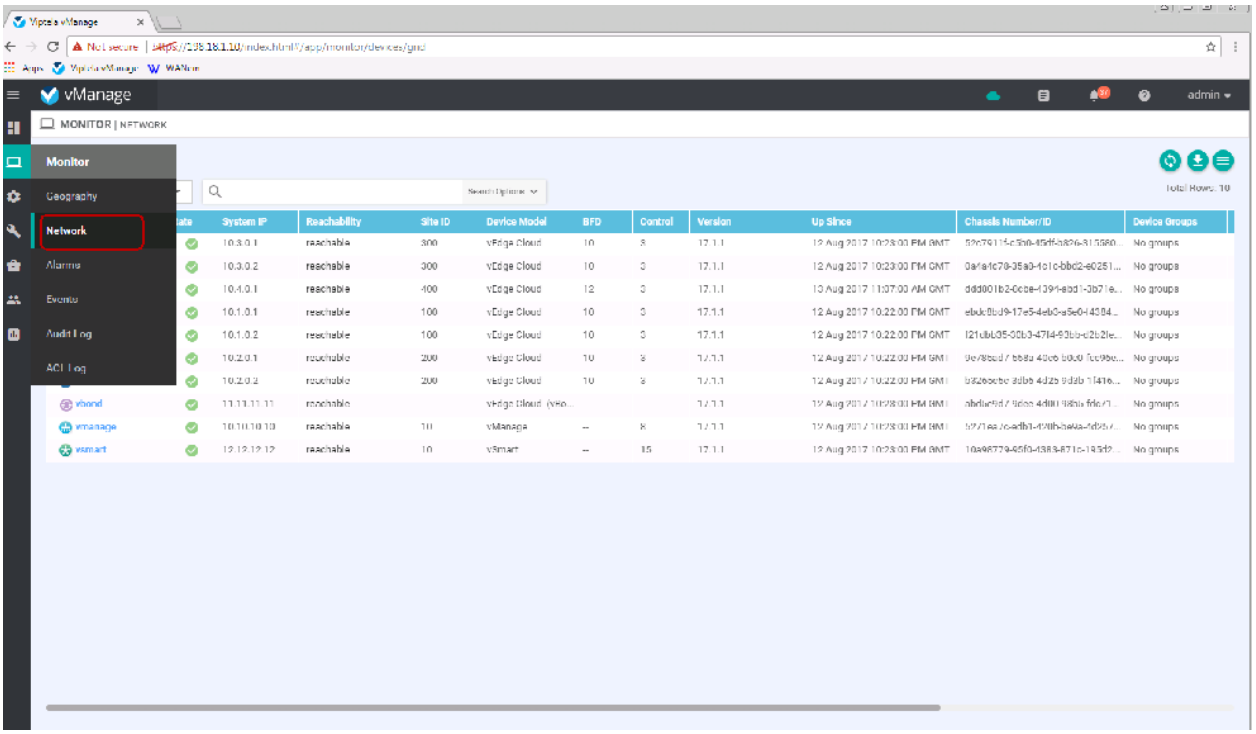
Click on “Activate” button.



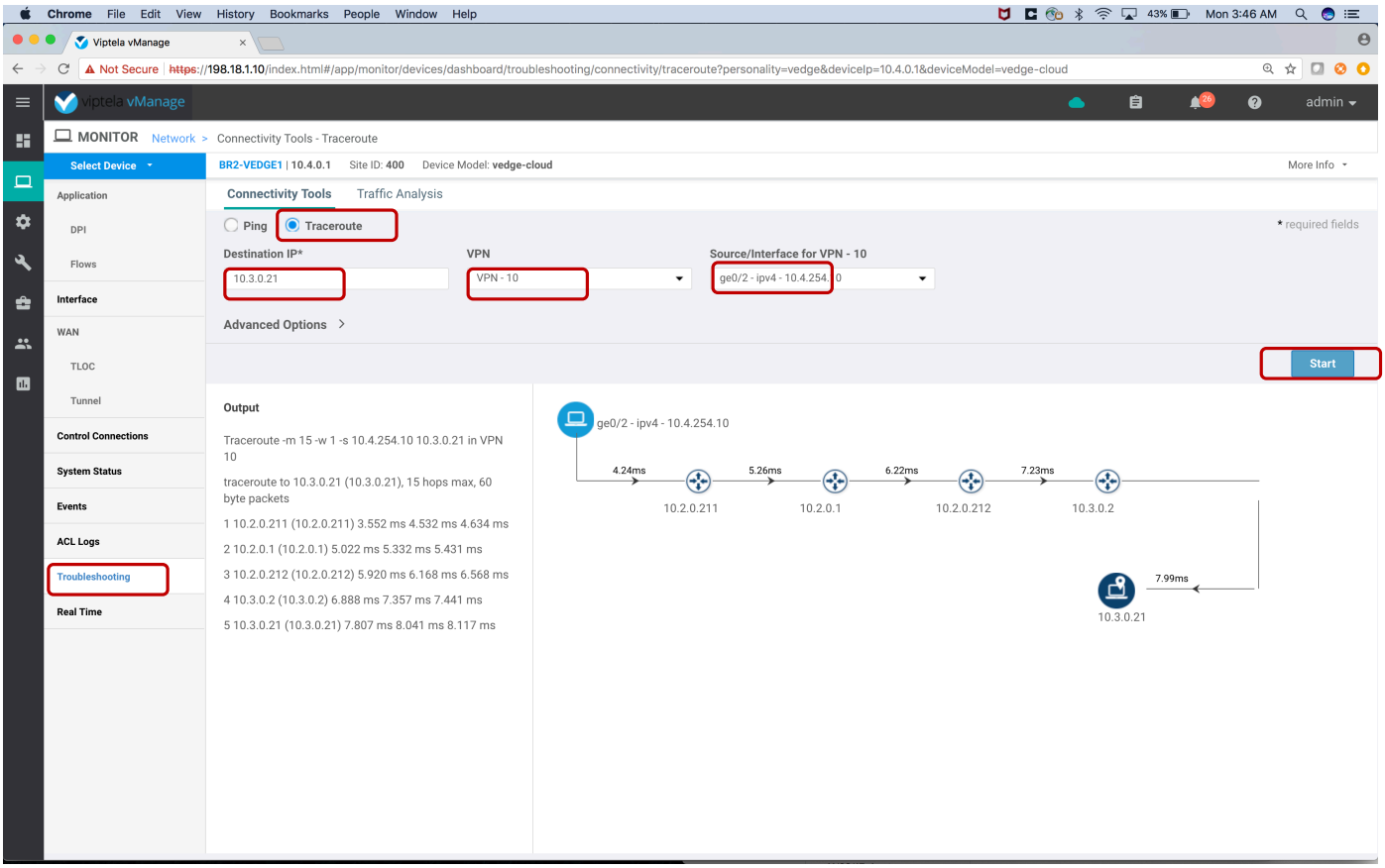
Wait till the policy is successfully pushed to the vSmarts.



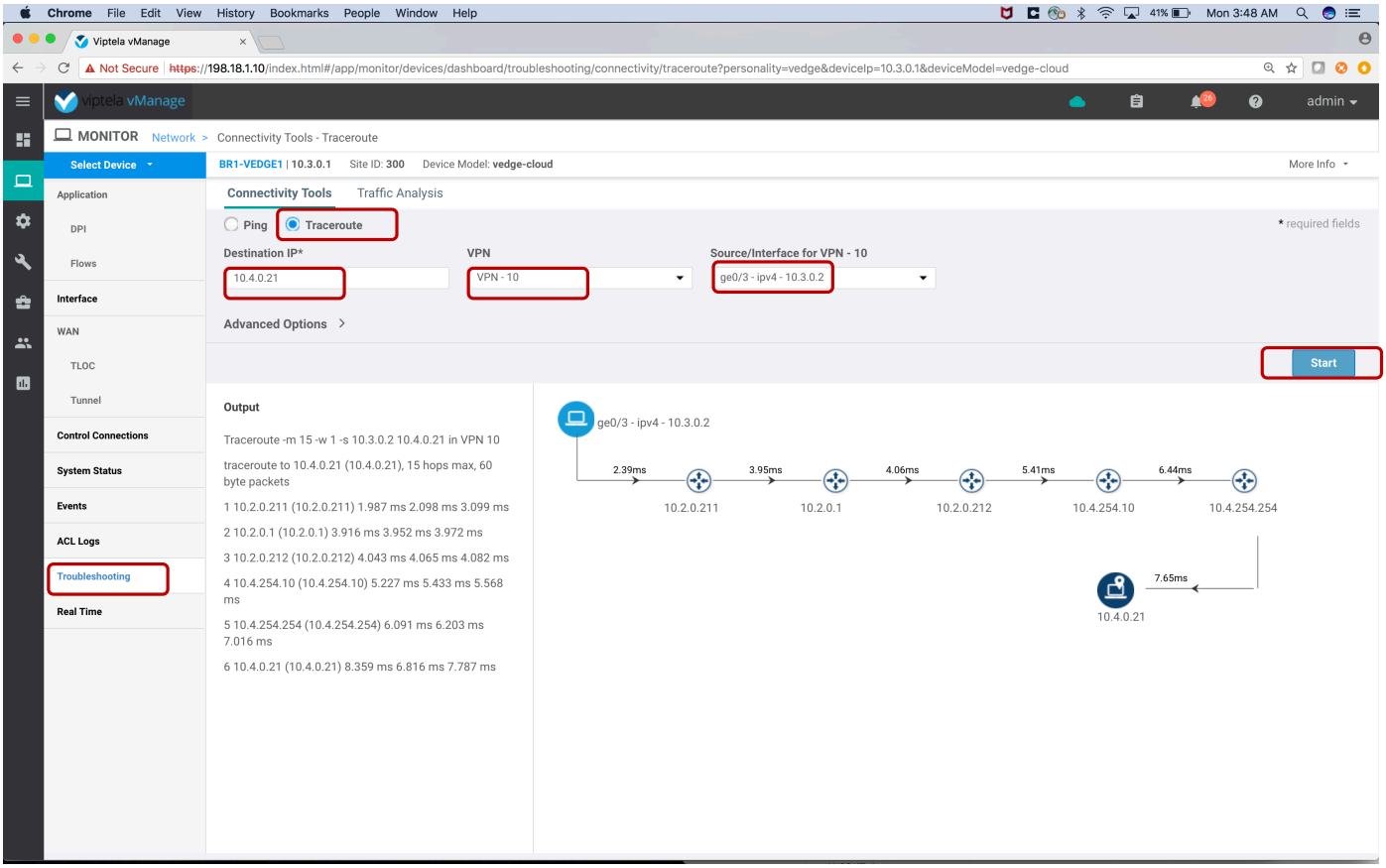
Go to Device Dashboard for BR2-VEDGE1. Go to Monitor then select Network. Click on BR2-VEDGE1.



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.



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



Deactivate the policy named “MultiTopologyPlusFWInsertion”.

Lab 06 - Application Aware Routing

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

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

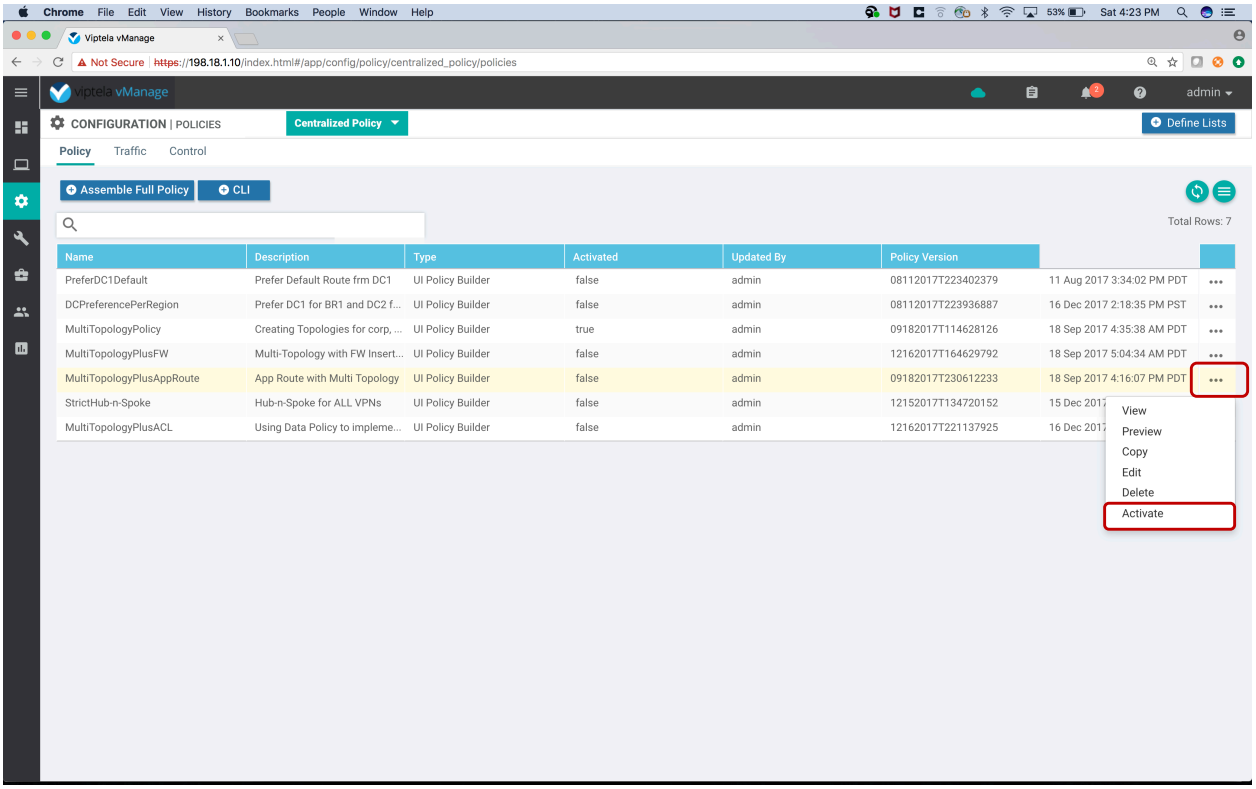
In this demonstration, some of the applications have SLAs defined and are pinned to the MPLS (interface ge0/0 on BR2-VEDGE1). Some applications are pinned to the internet transport (interface ge0/1 on BR2-VEDGE1).

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

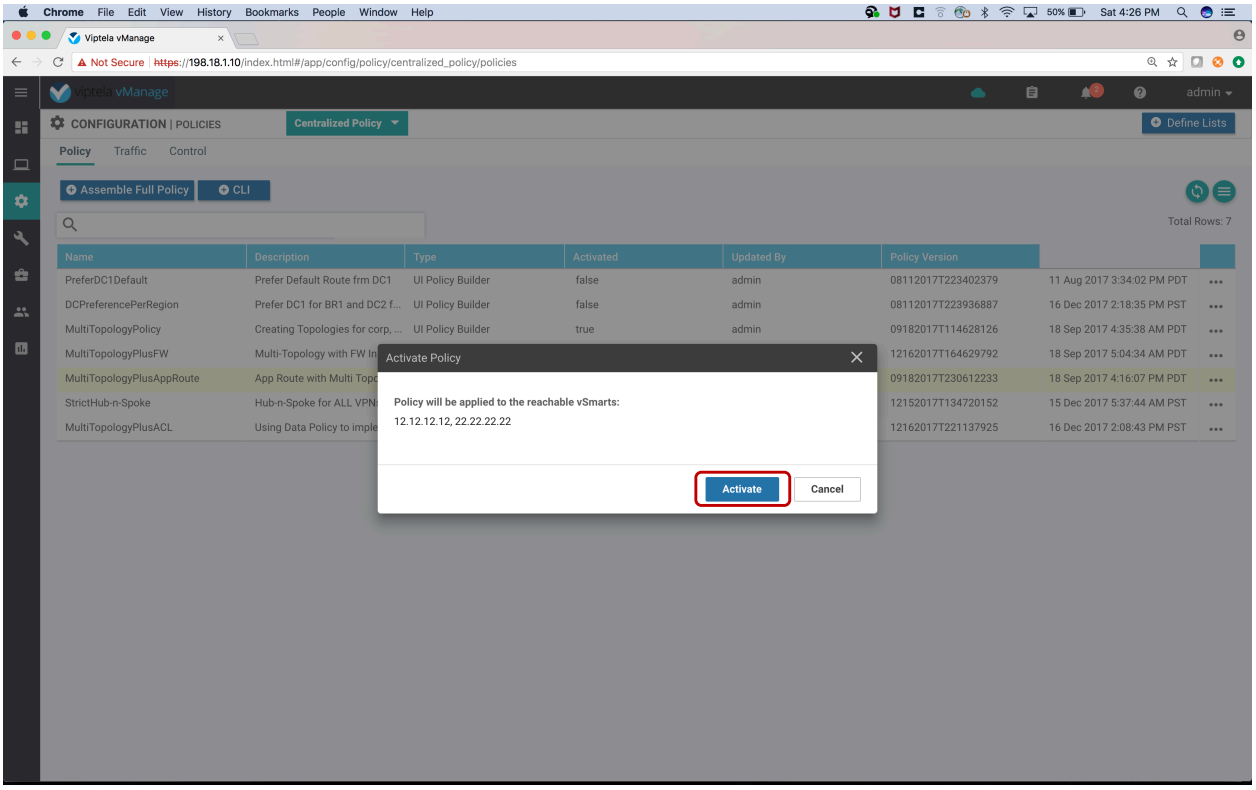
You would observe traffic received switch from mpls interface to internet interface after the latency impairment on MPLS transport.

Steps

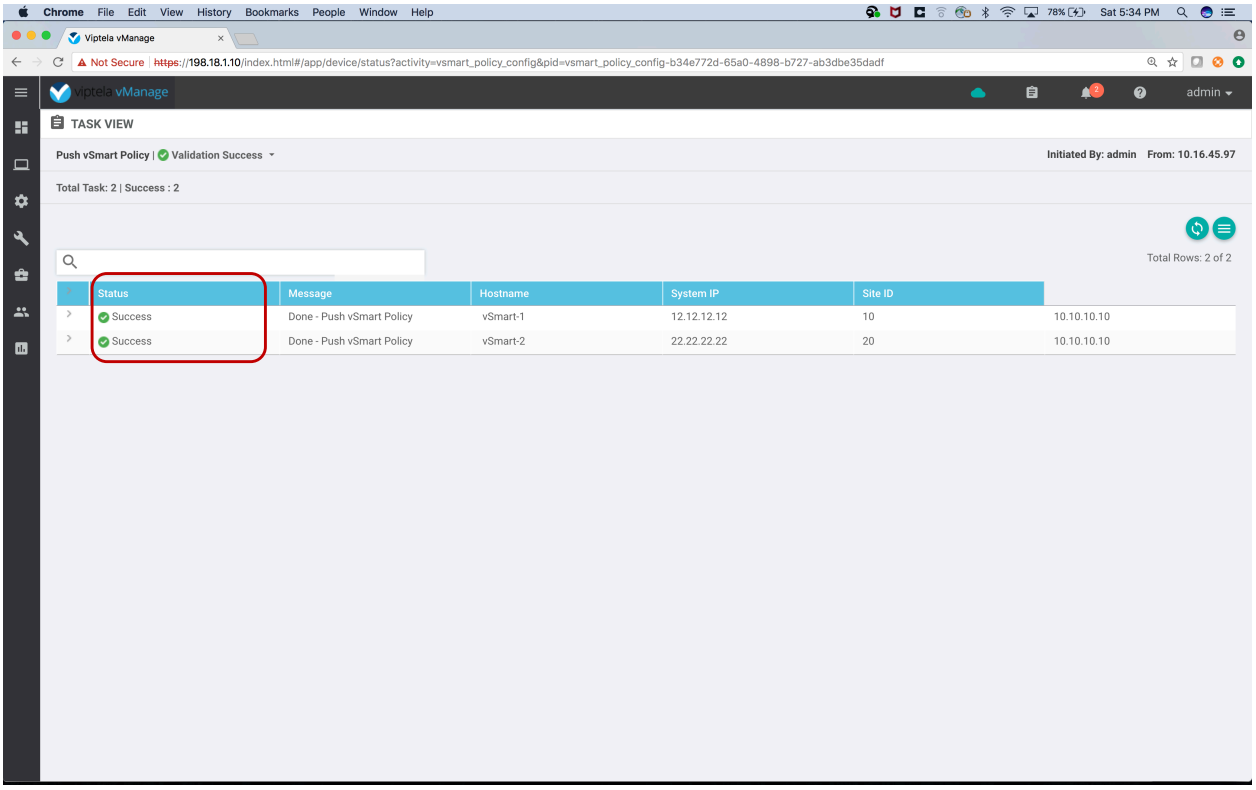
Go to the Policy configuration page, and activate the Application Aware Routing policy named “MultiTopologyPlusAppRoute”.



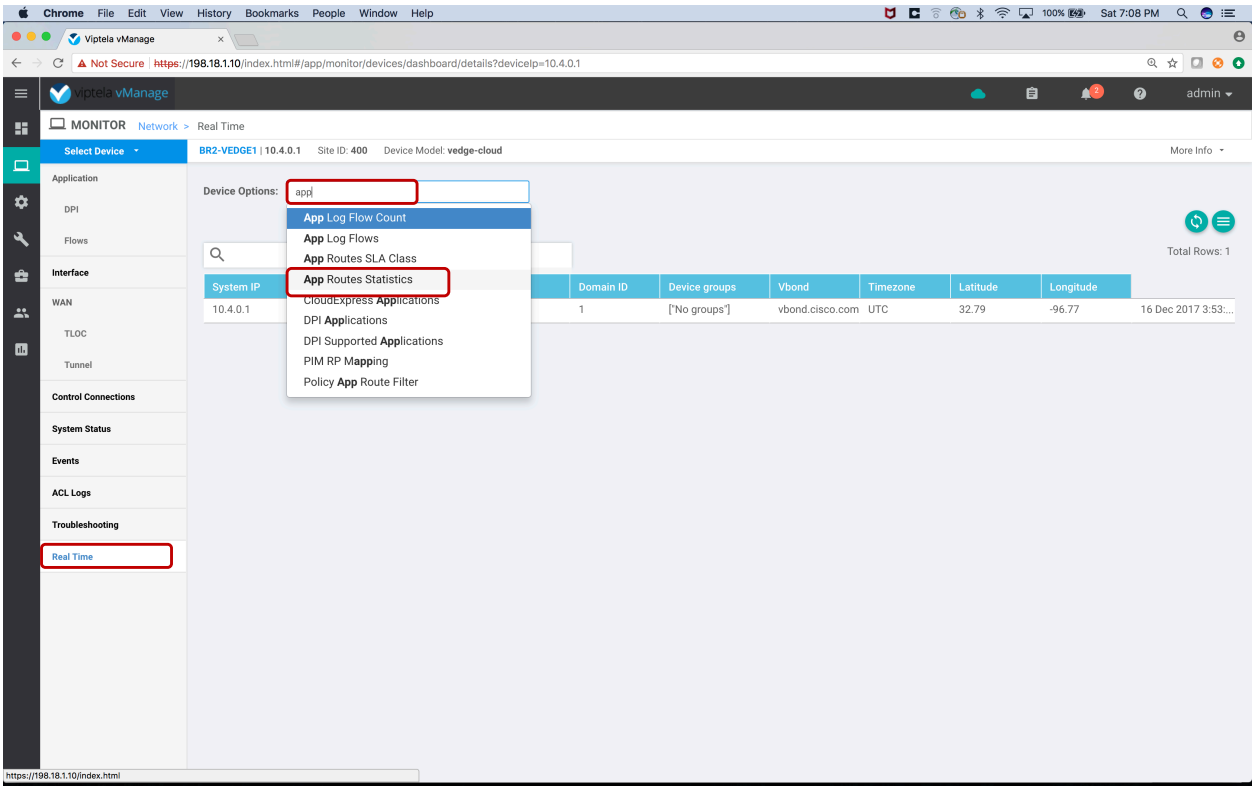
Click on the “Activate” button.



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

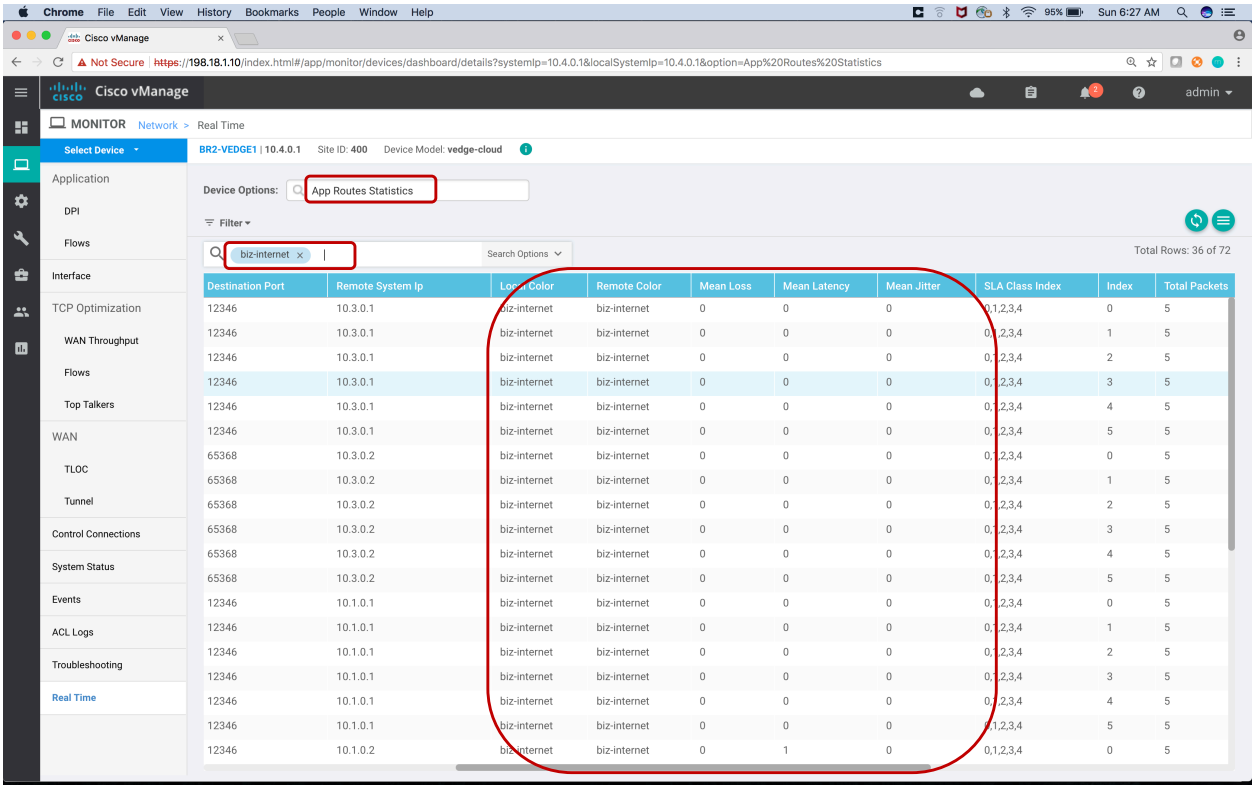


To see the current performance measurement on both the transports, go to device dashboard for BR2-VEDGE1. Click on “Real Time” tab. Search for “App Routes Statistics” and select it.

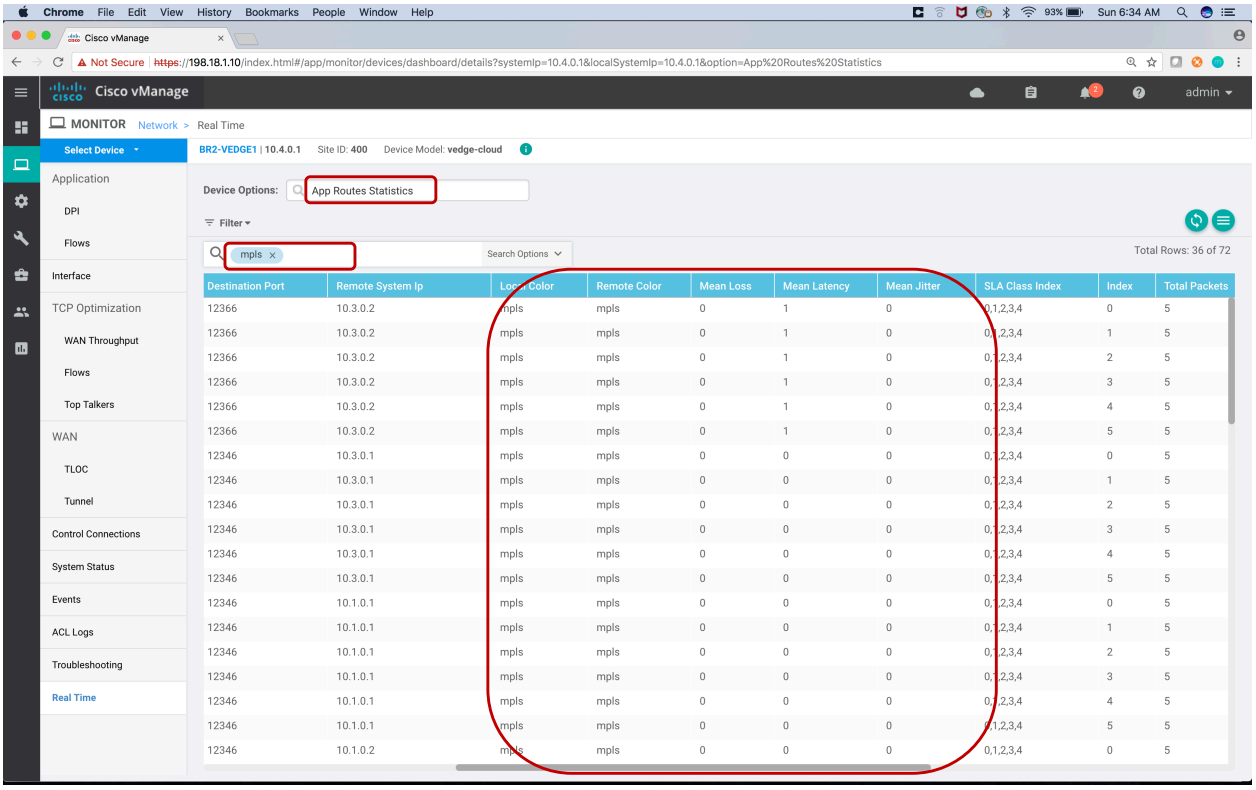


Scroll to the right and you will see the columns showing latency, loss and jitter for each of the tunnels on MPLS and Internet. The values (at or close to zero) are much lower than the SLA definitions defined for the app-route policies.

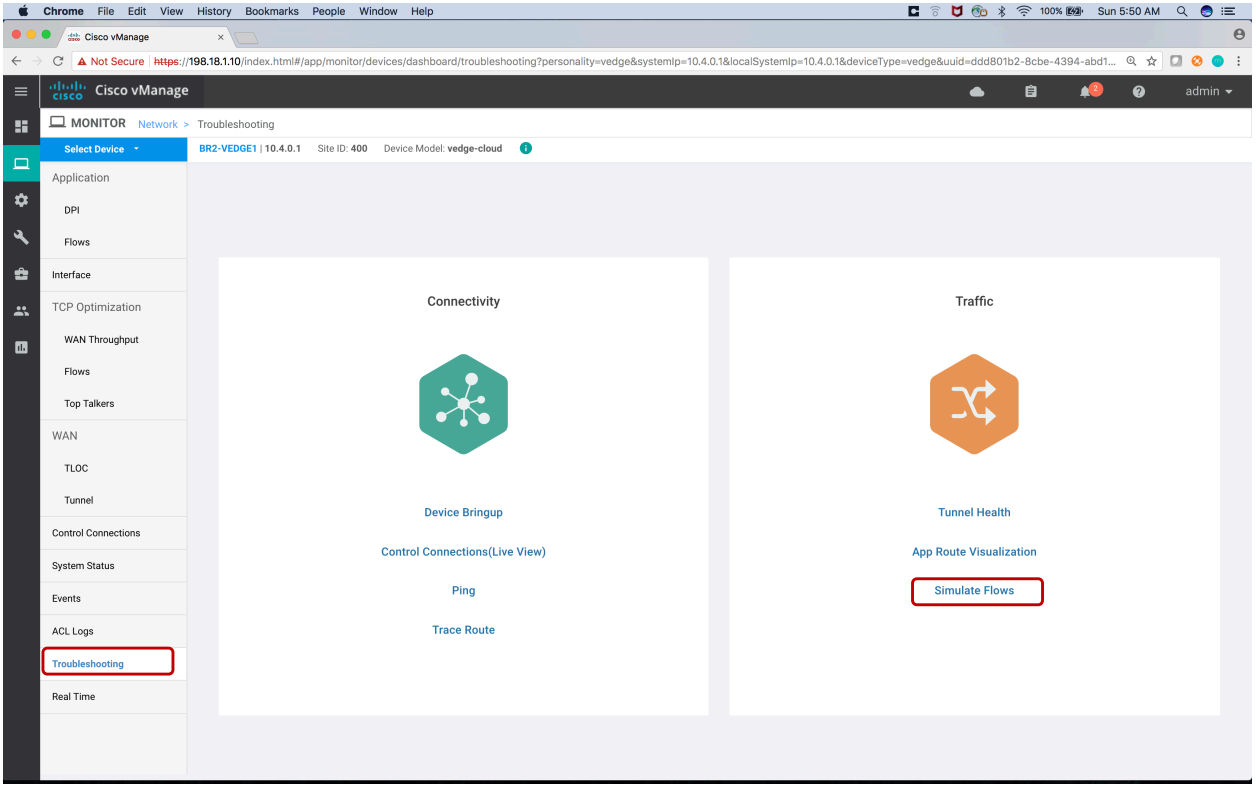
To view the tunnels statistics on internet transport, type in “biz-internet” in the search column and hit return.



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

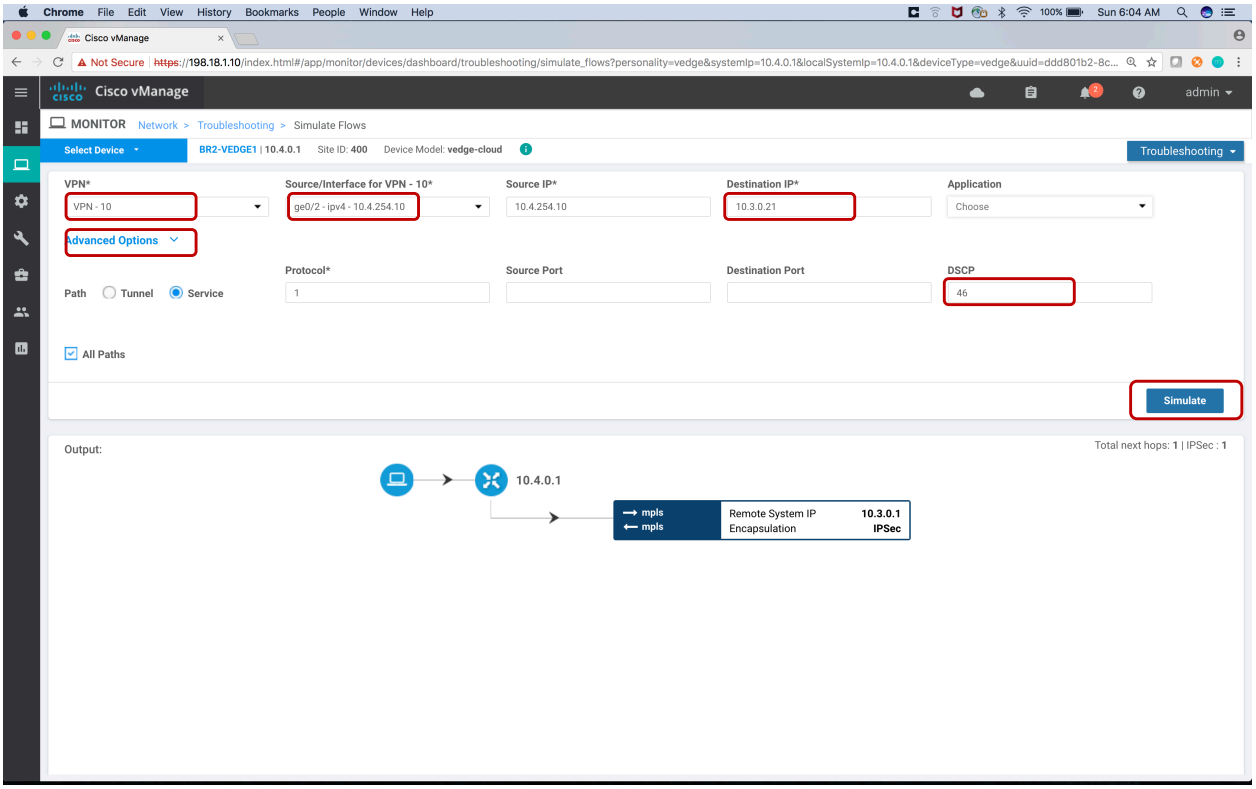


Click on the “Troubleshooting” tab and then click on “Simulate Flows”. This will provide simulation on what IPSec tunnels will used for the defined flow based on policies and transport performance measurements.



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

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

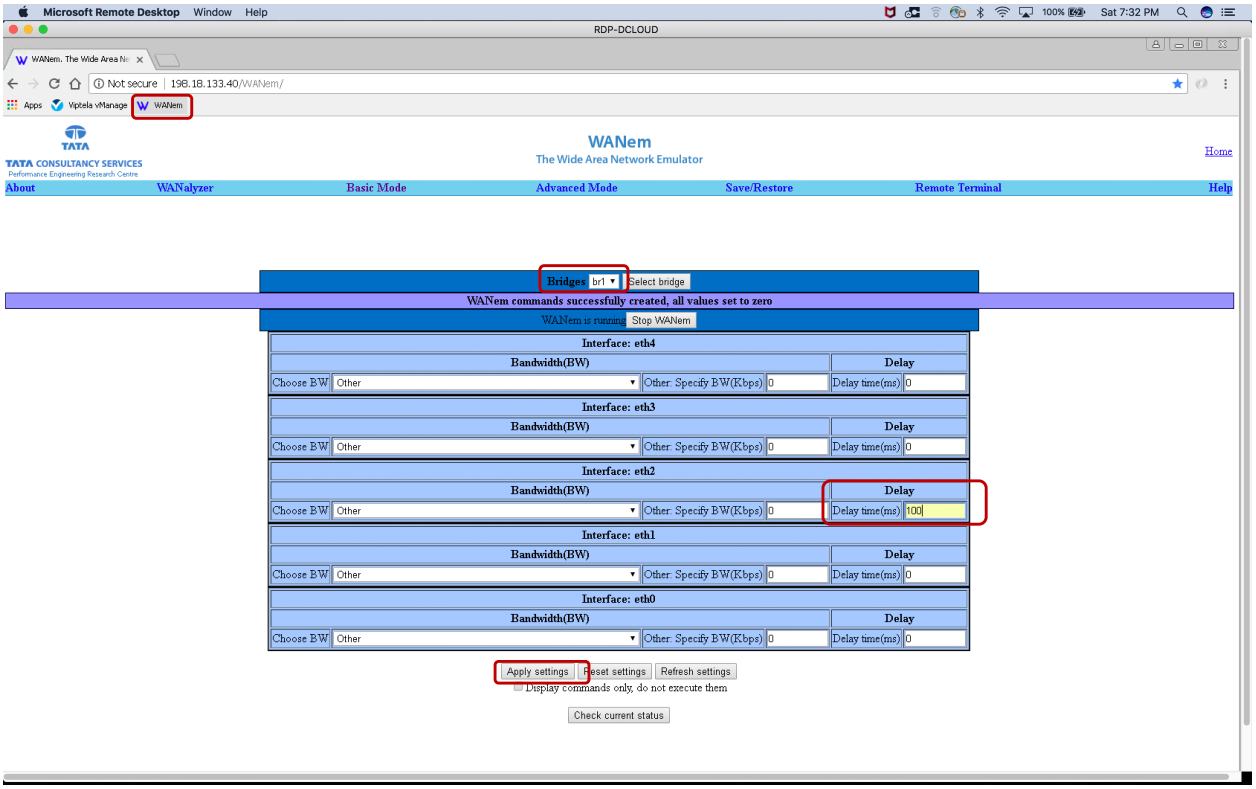


Go to the Chrome browser and click on the “WANem” (Wan Emulator) bookmark.

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

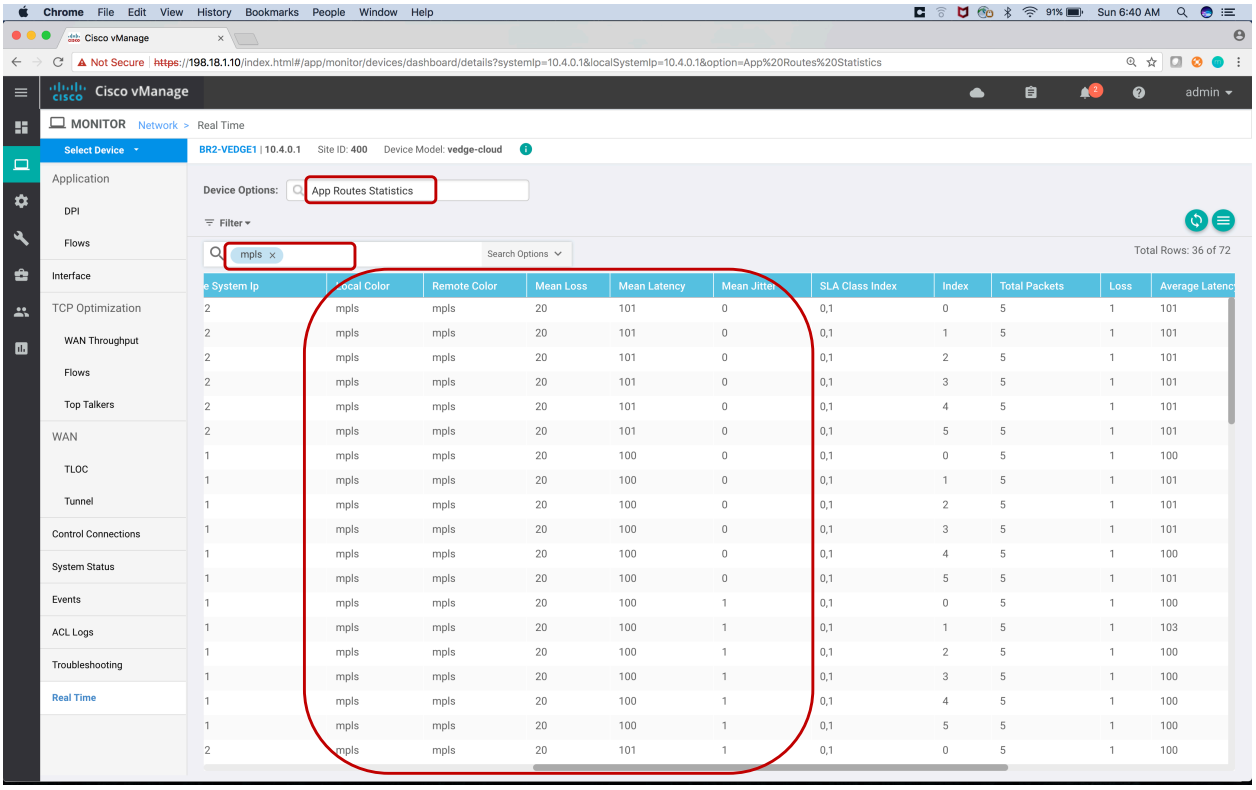
Put in a value of 100 msec for delay for “interface 2” which will introduce latency of 100msec on BR2-VEDGE1 on MPLS.

Then click on “Apply Settings” button.



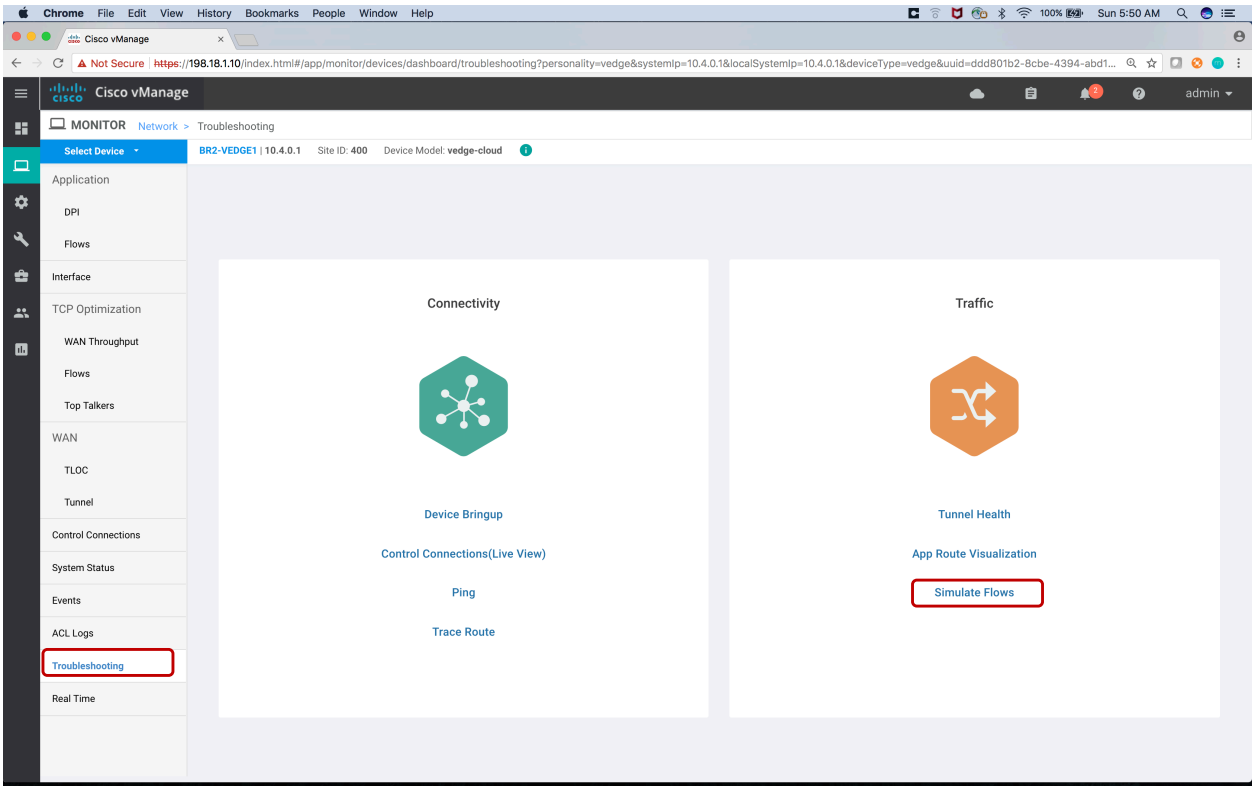
Go back to the vManage's device dashboard and look for App Route Statistics under "Real Time".

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



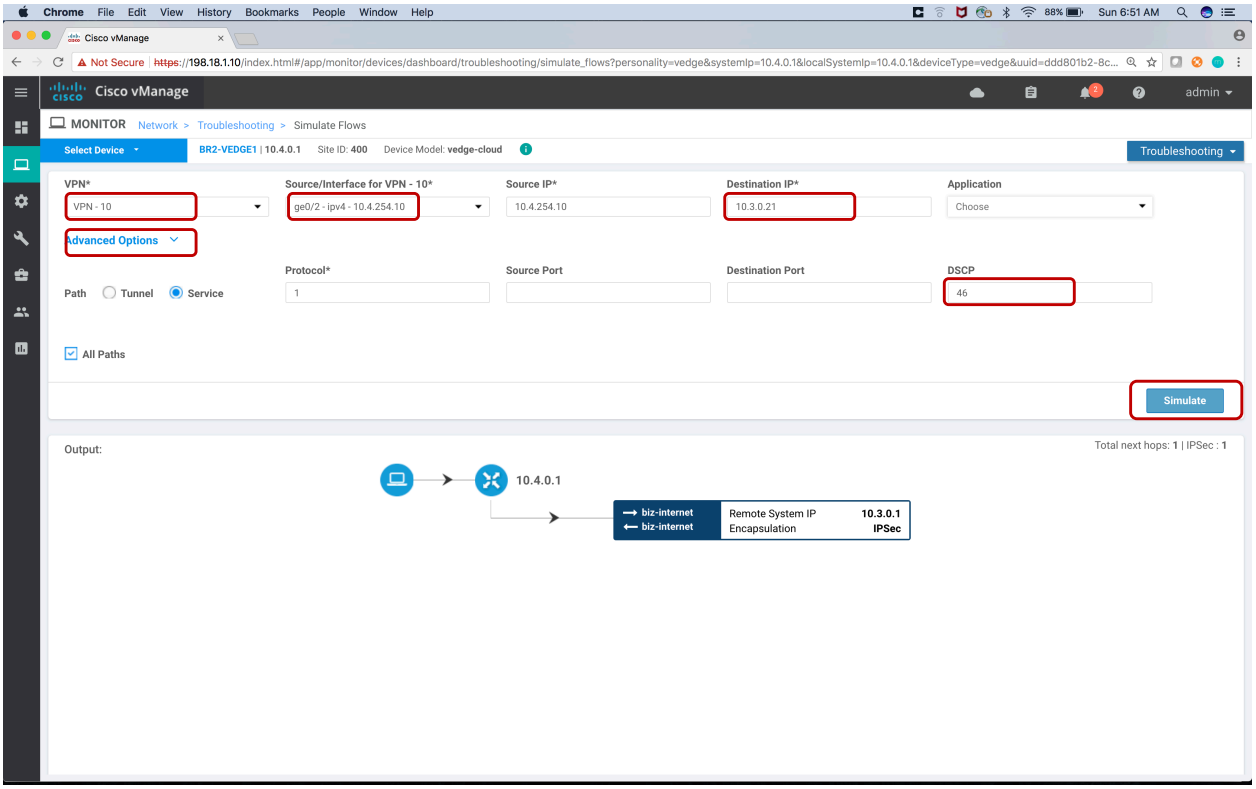
The policy has an SLA definition of up to 5% packet loss and 50 msec latency for voice / video applications (DSCP 46) with preferred path of MPLS.

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



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

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



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.

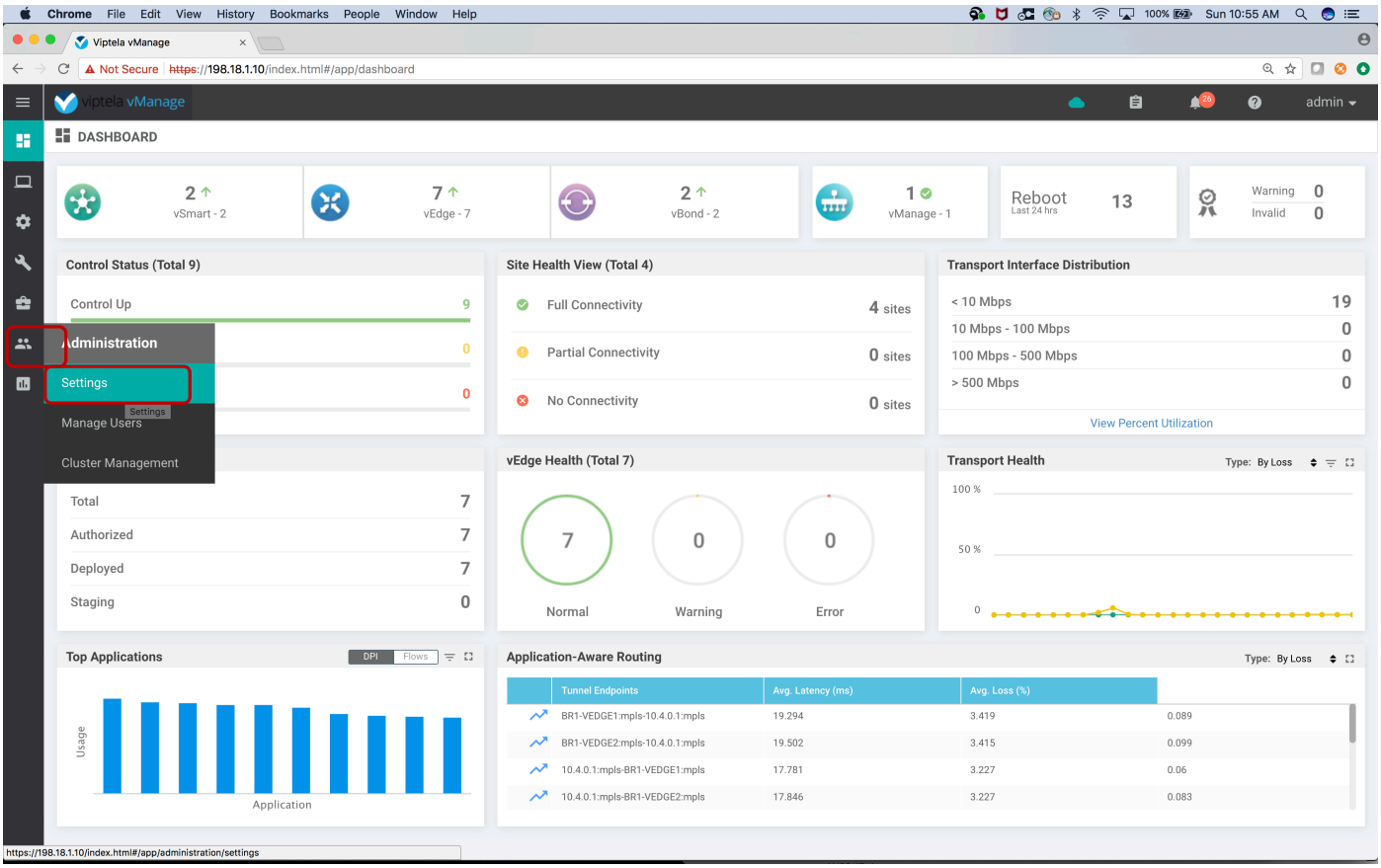
Cisco SD-WAN provides a method to run application probes for each one of these applications and compute the Viptela Quality of Experience (vQoE) score for each one of the paths (DIA or regional Hub/DC internet exits). vEdge routers then based on vQoE scores to pick the best optimal path for a given SaaS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

Steps

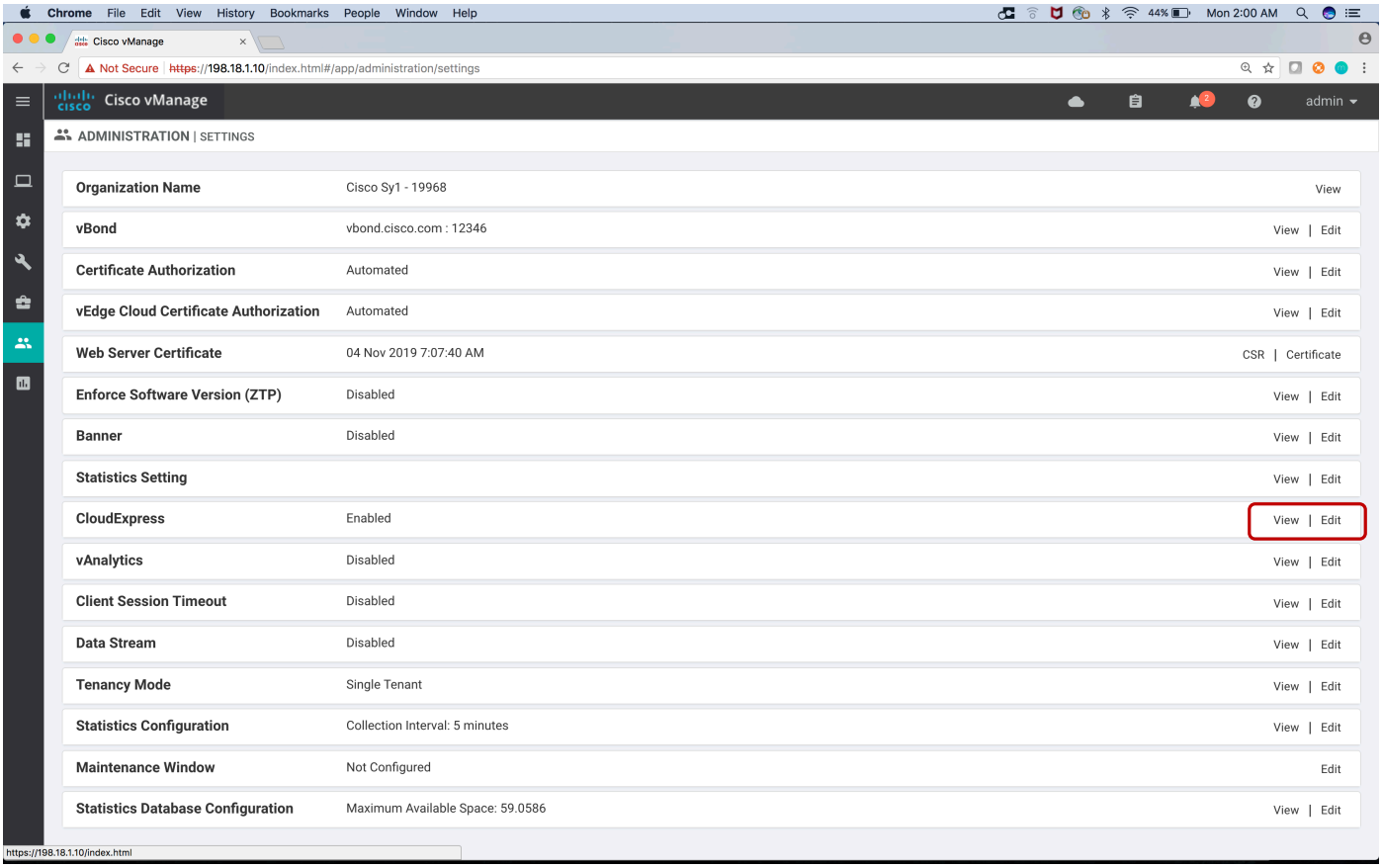
CloudExpress is off by default in Cisco SD-WAN. All aspects, including configurations and visibility, are provided from vManage.

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.

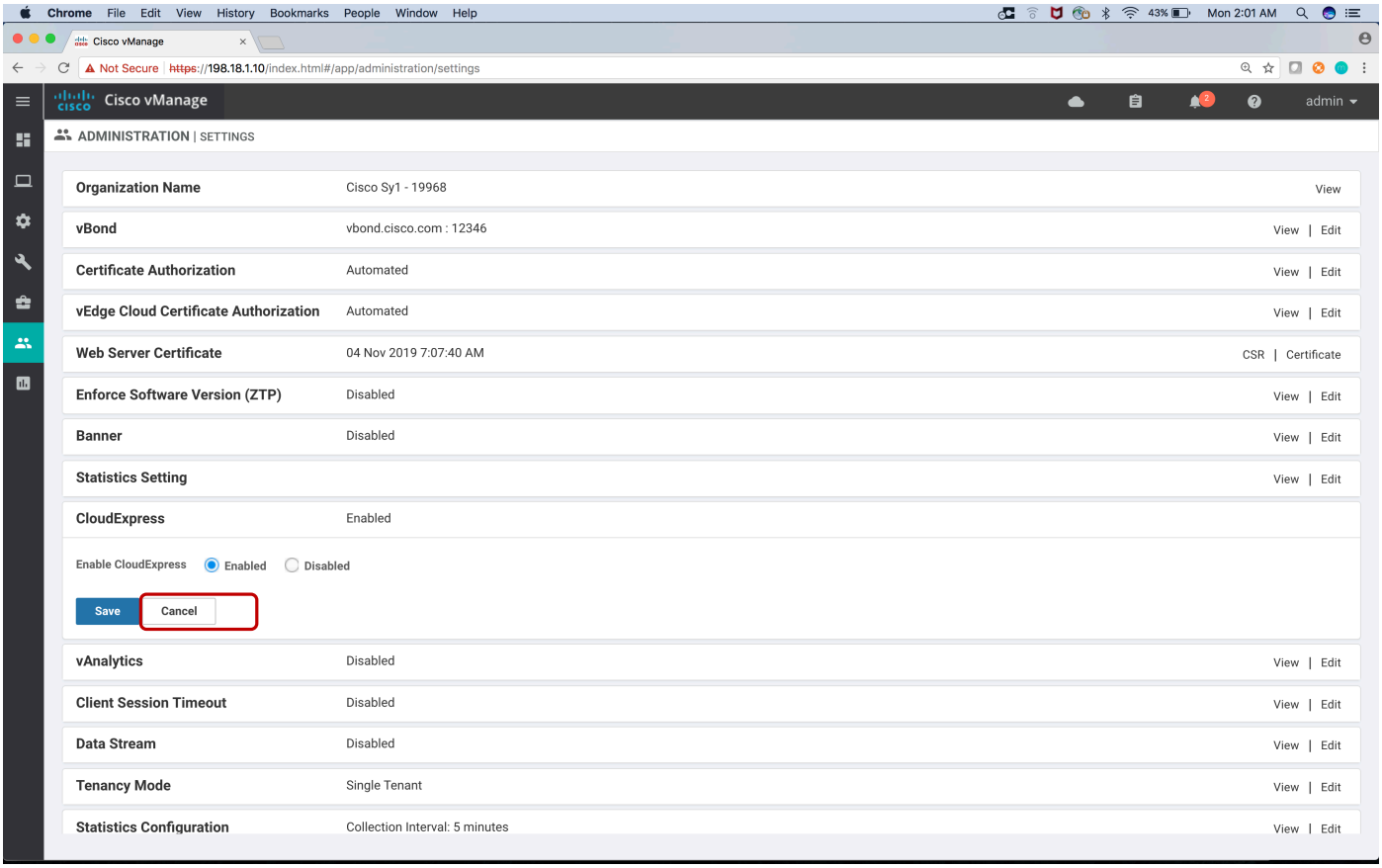
From vManage Dashboard go to “Administration” -> “Settings”



Click on “Edit” for CloudExpress.

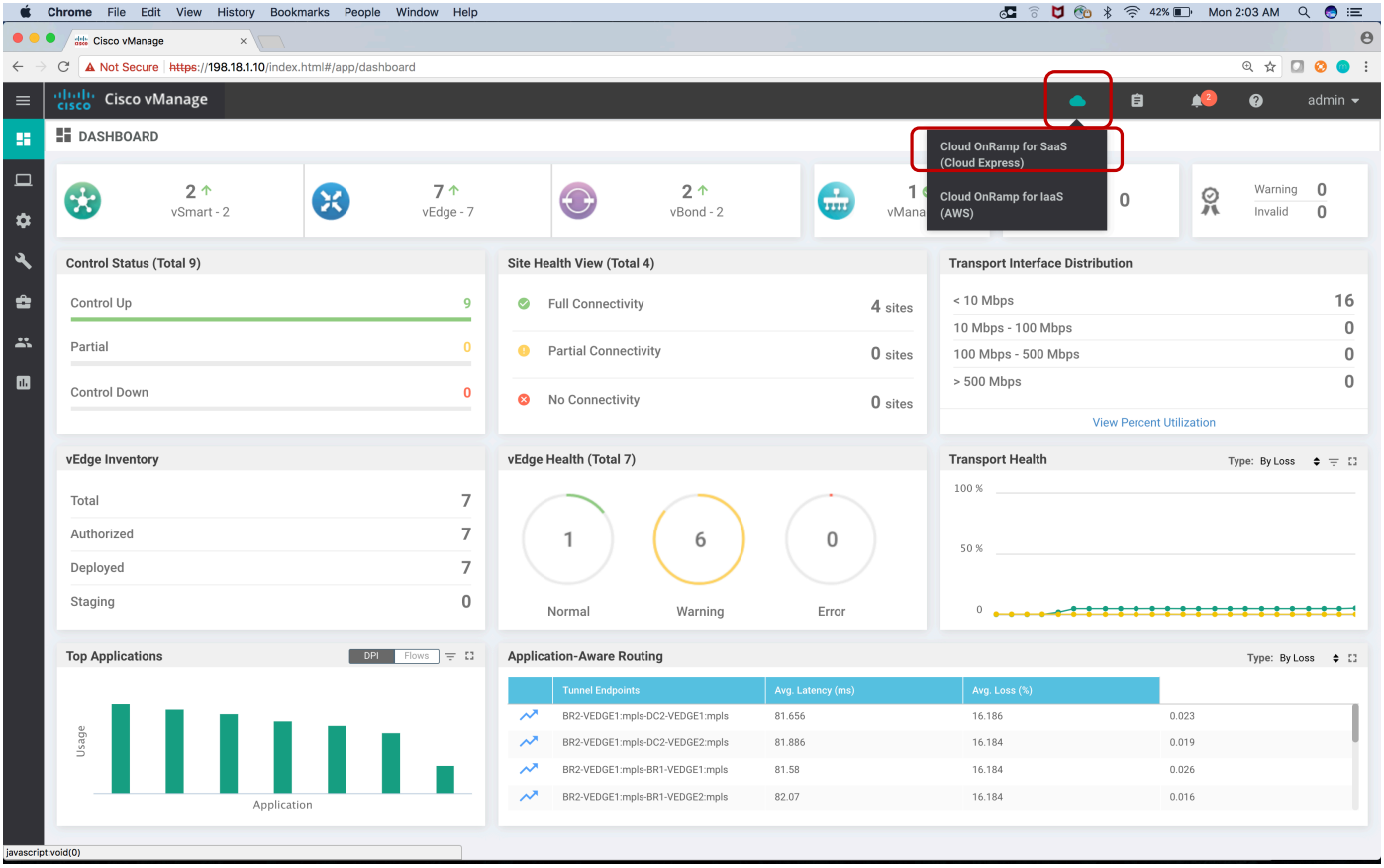


Here you would “Enable” the service and save it. Press “Cancel” to exit out.



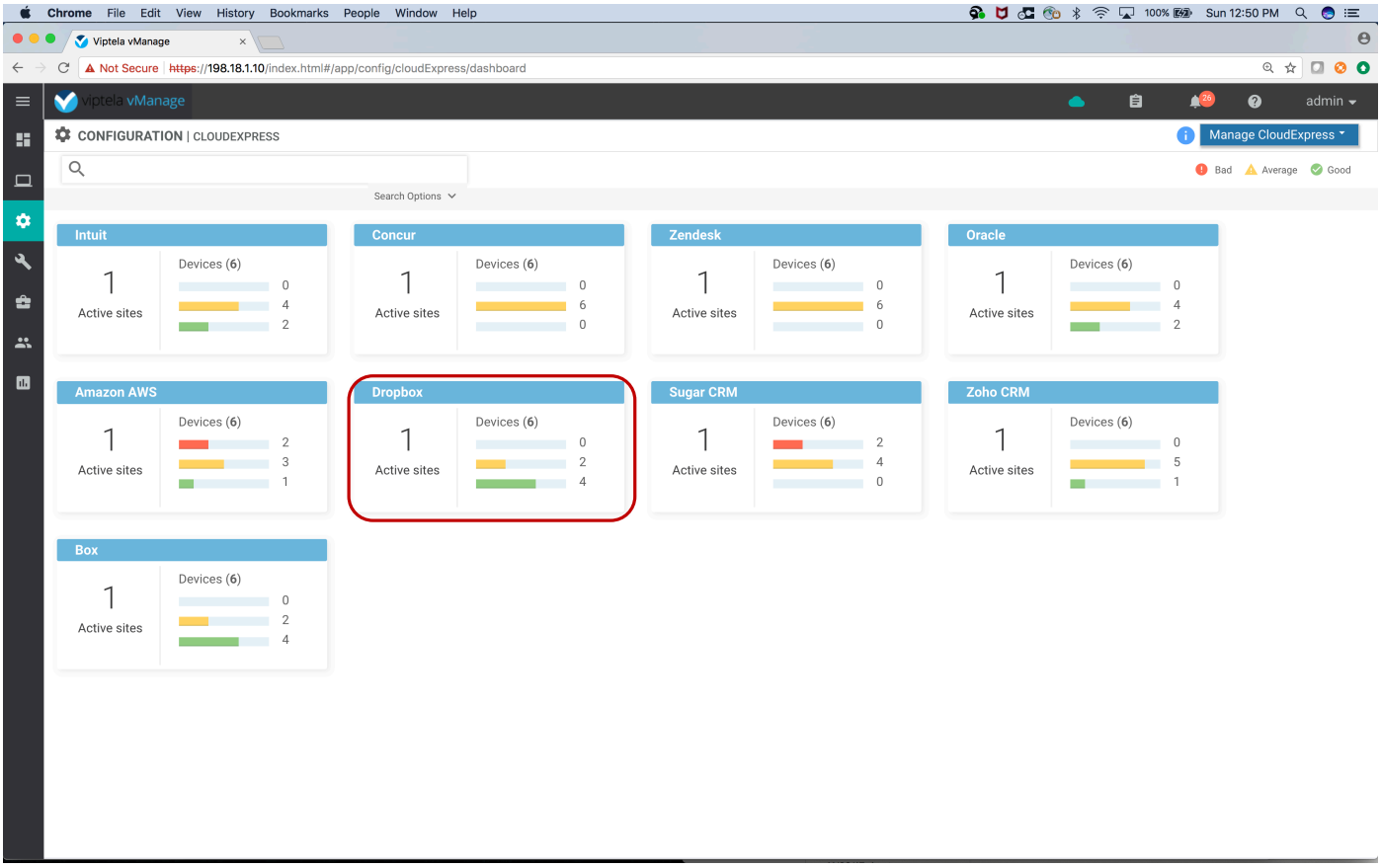
Go to CloudExpress Dashboard by clicking on the Cloud OnRamp icon ( ) and select “Cloud OnRamp for SaaS (Cloud Express)”.

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



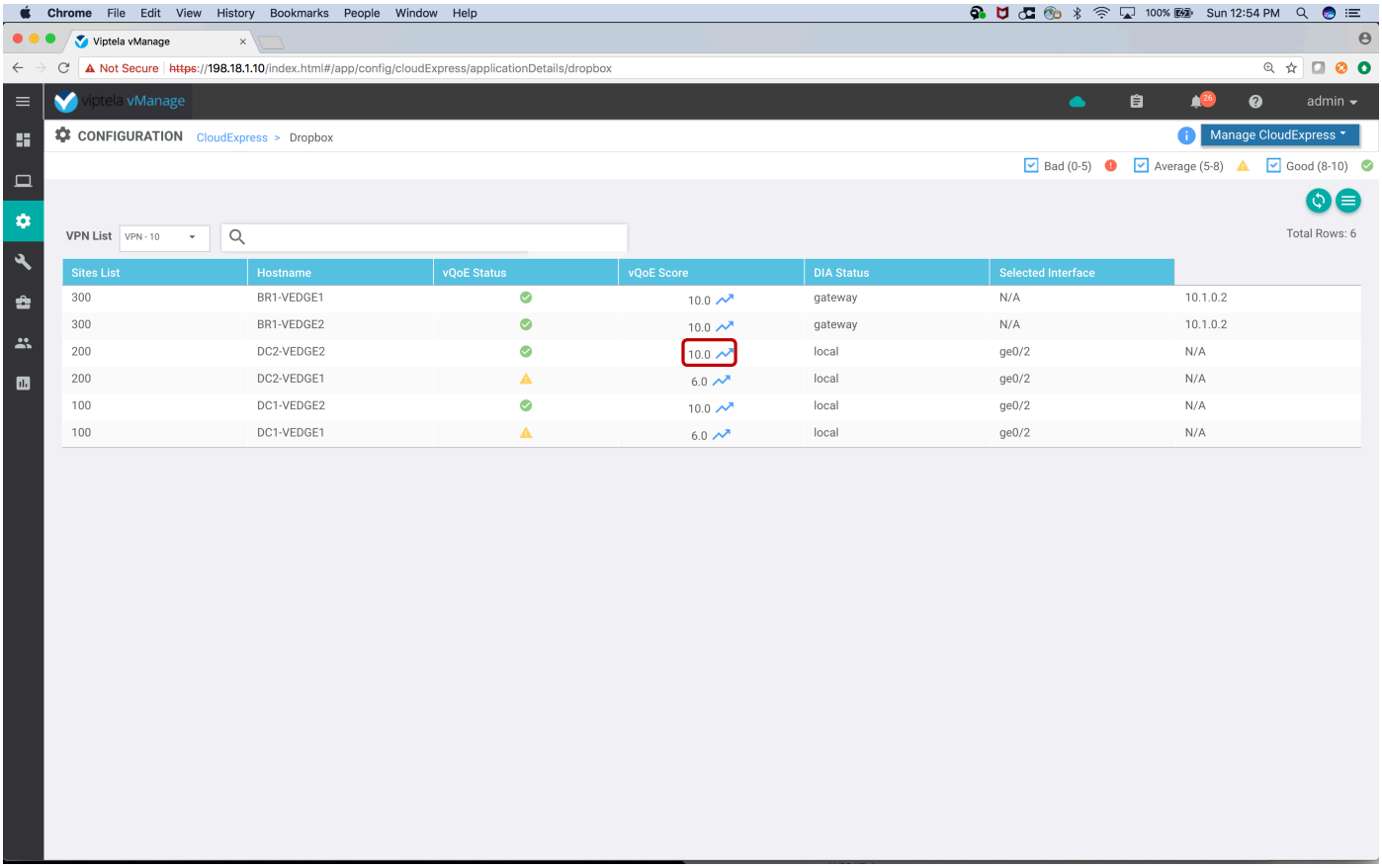
CloudExpress dashboard will show you all the applications that are enabled for CloudExpress, number of sites and number of devices.

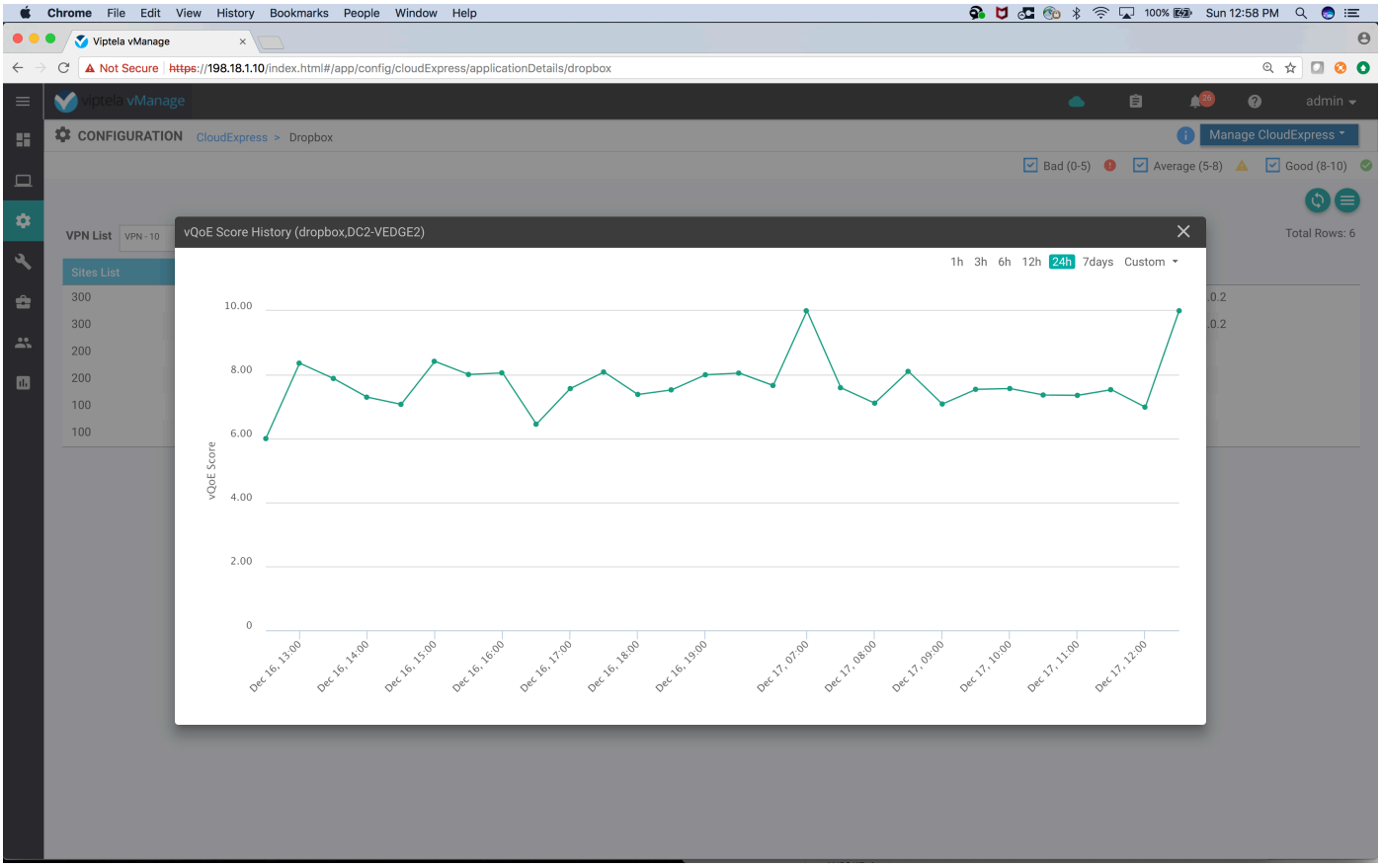
Click on one of the application's tab to view details for that application.



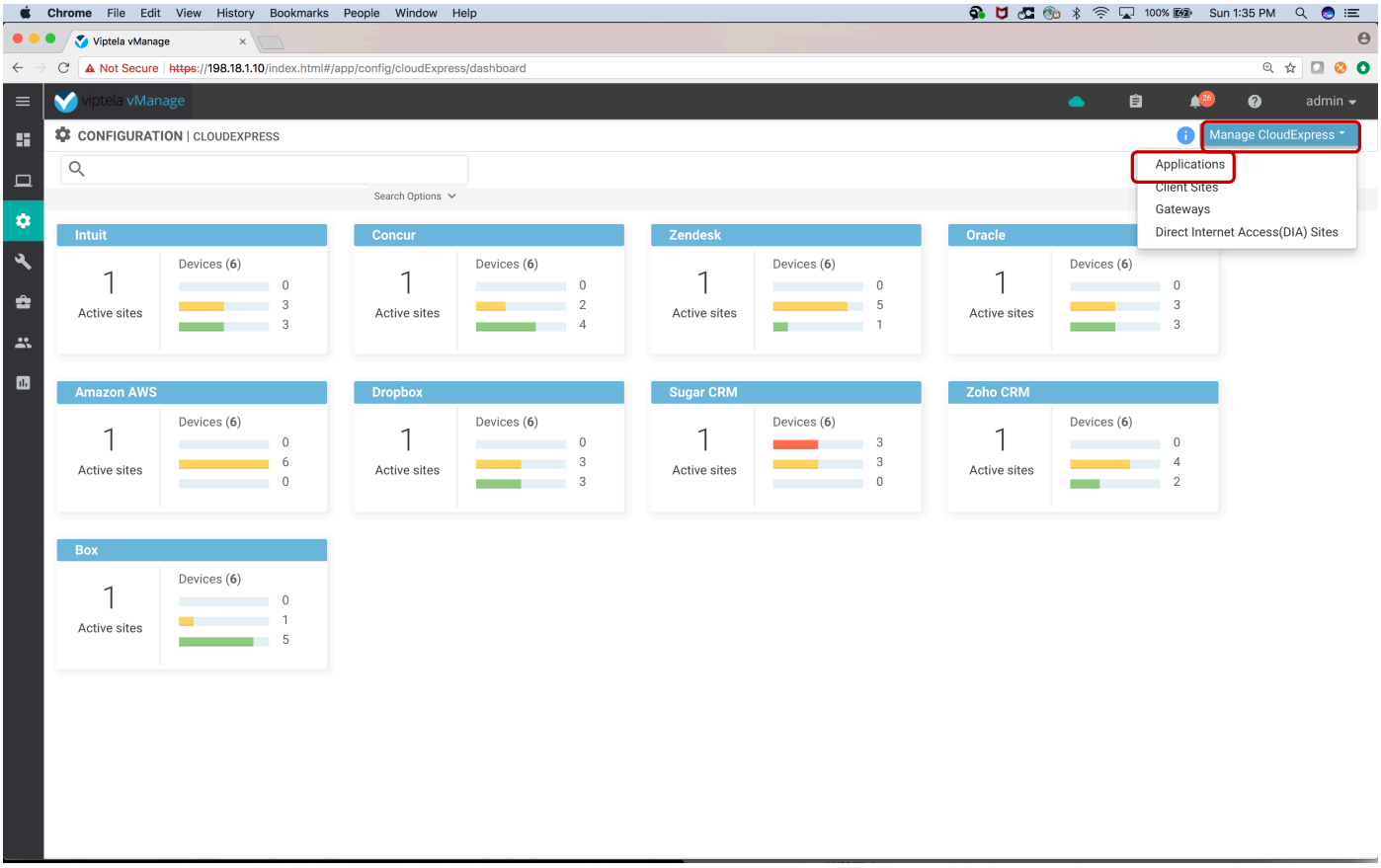
The application dashboard shows the list of devices and the reported Viptela Quality of Experience (vQoE) score for the application.

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

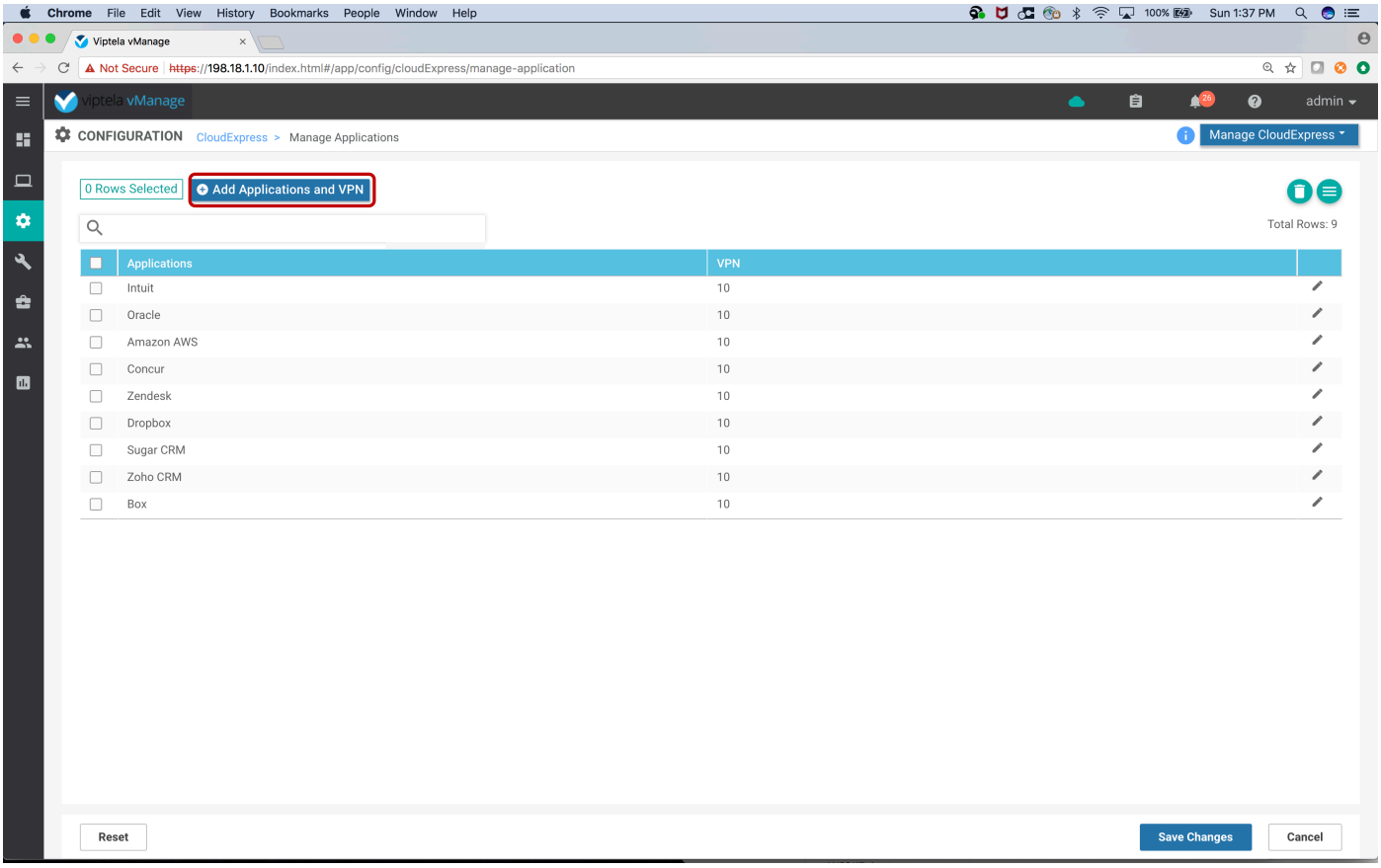




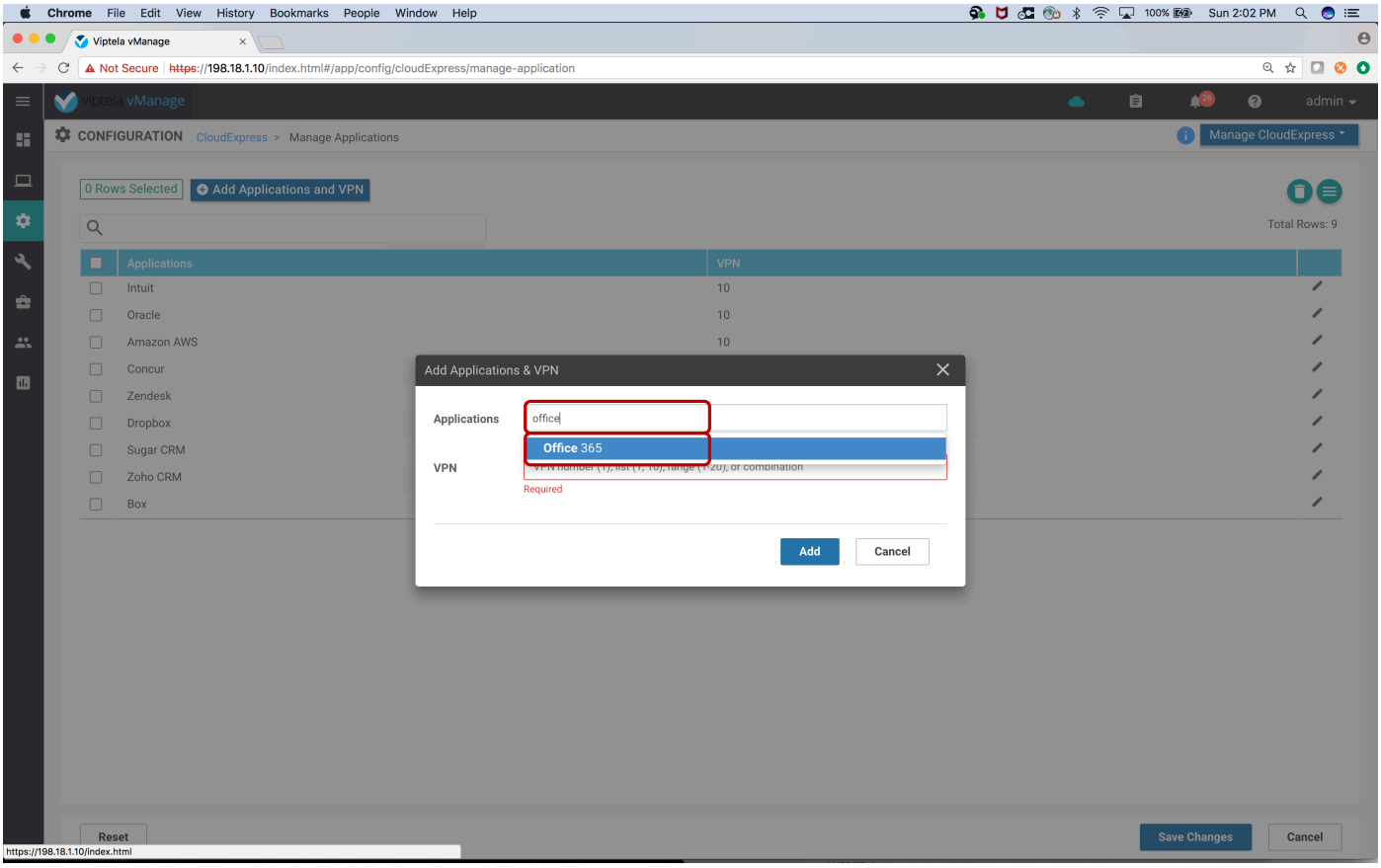
To add in a new application to the list go to CloudExpress dashboard. Click on the “Manage CloudExpress” pull down and select “Applications”.



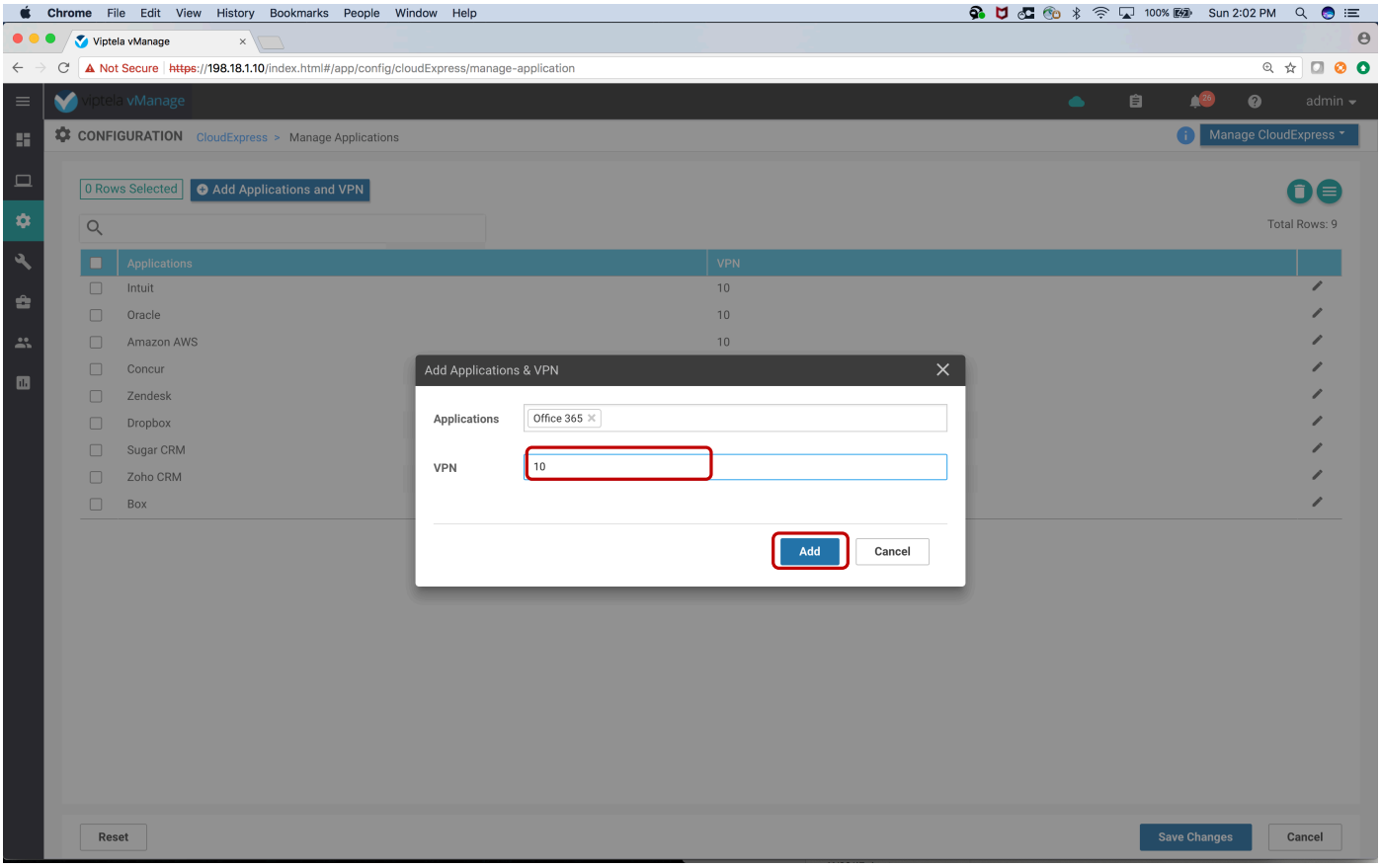
On the next page click on the “Add Applications and VPNs” button.



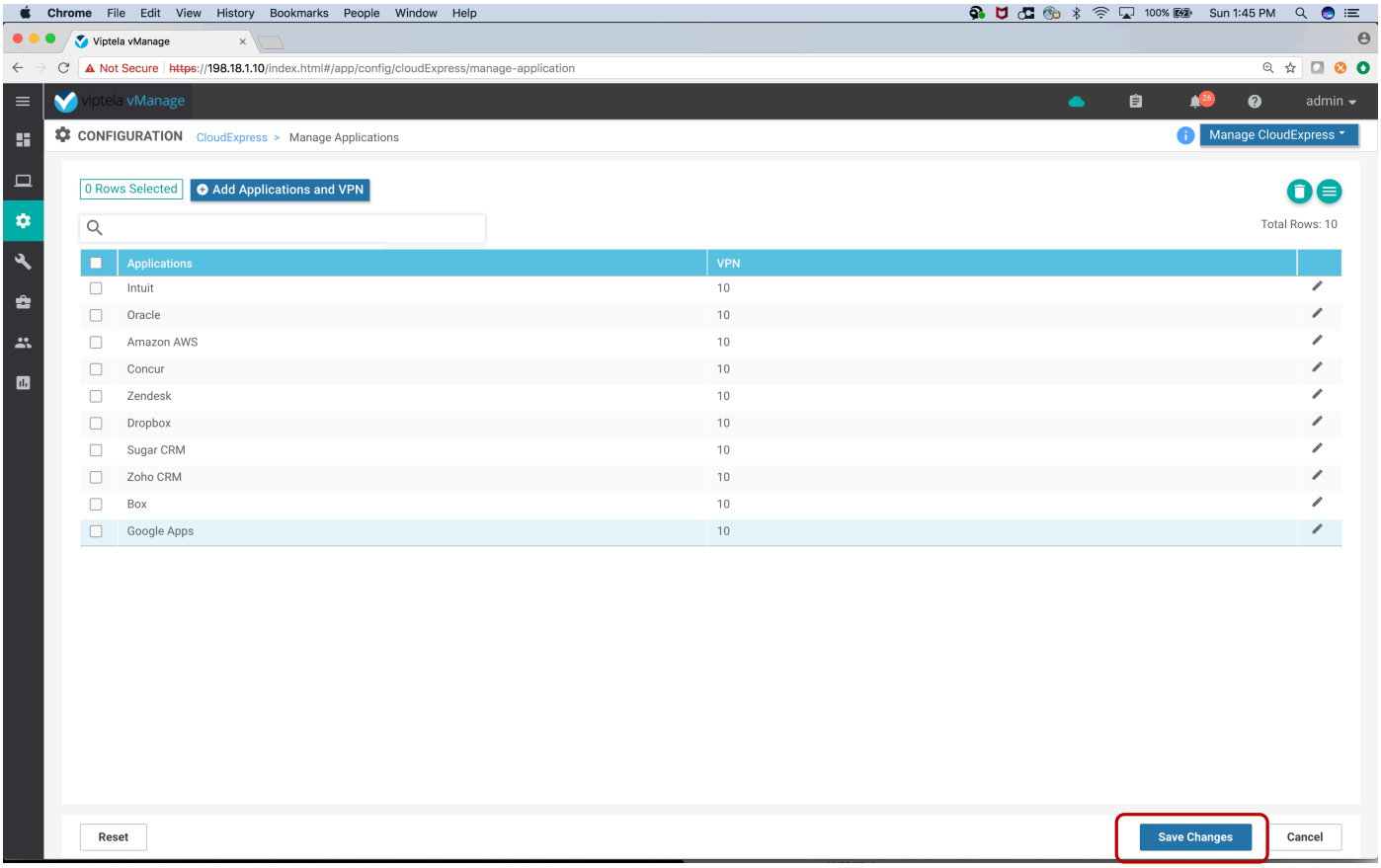
Type in “office” in the applications box and select “Office 365” in the drop down.



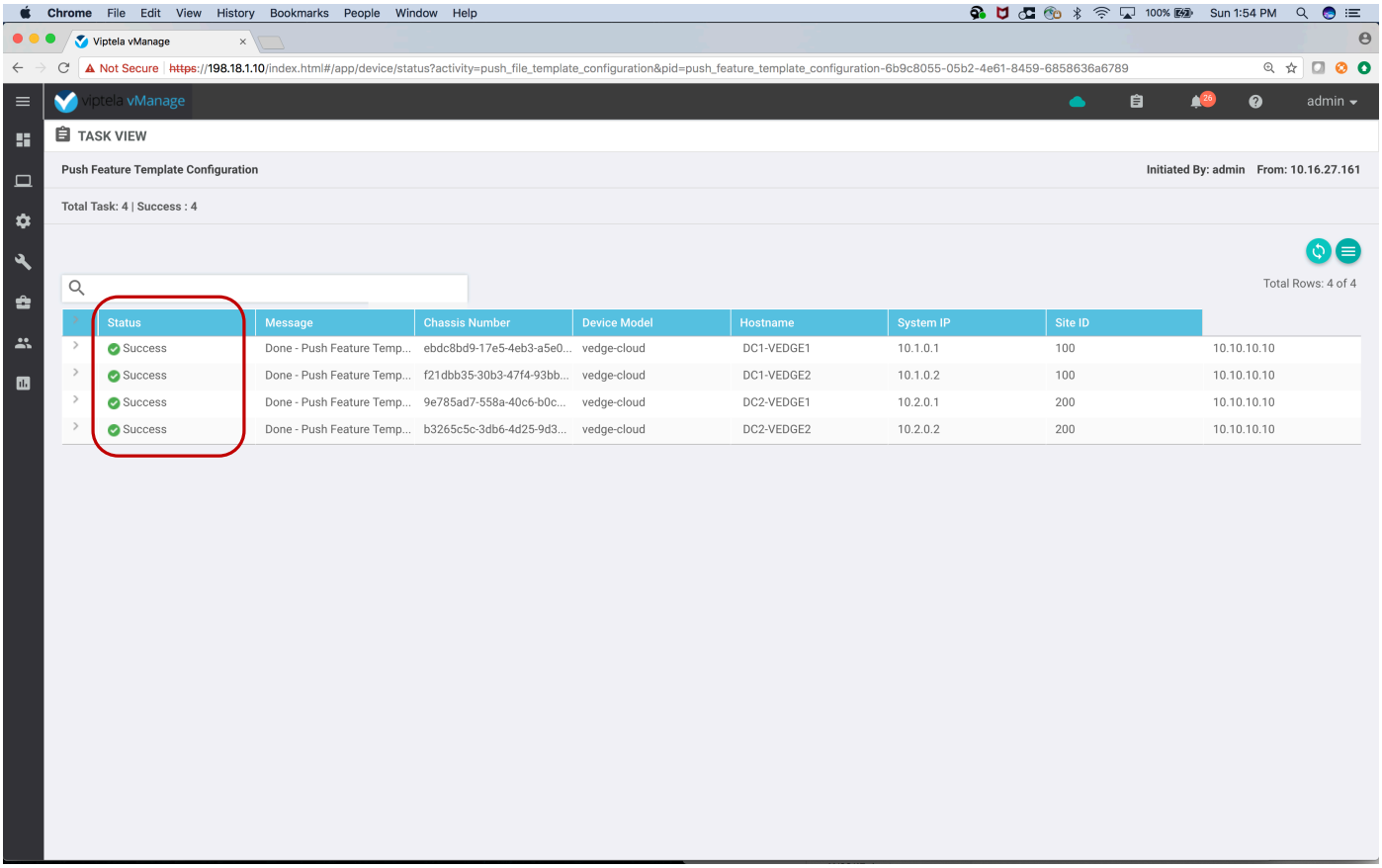
Enter Corporate VPN number (10) and click “Add” button.



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

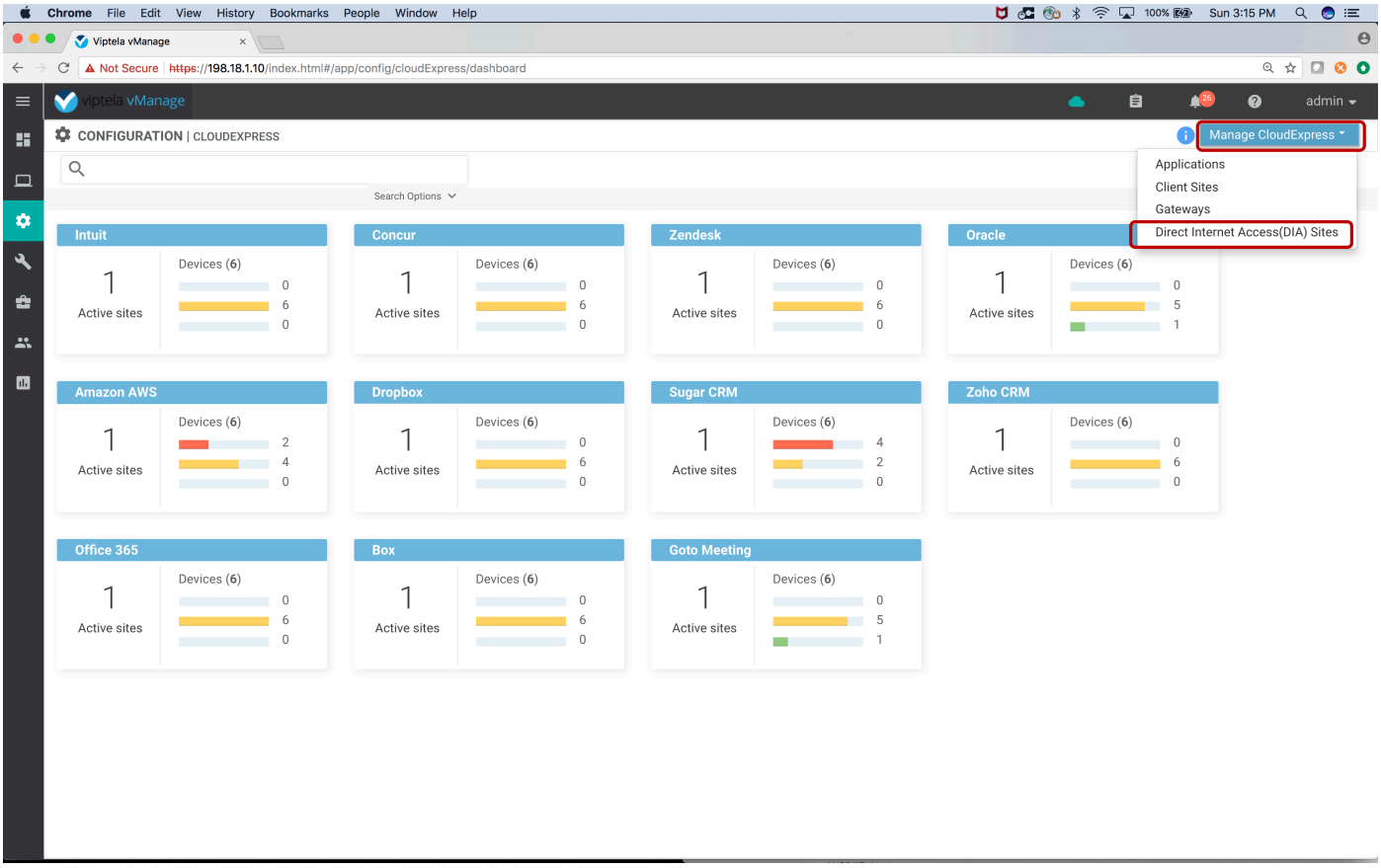


Wait till the new application (goggle apps) configuration of the devices is successful.

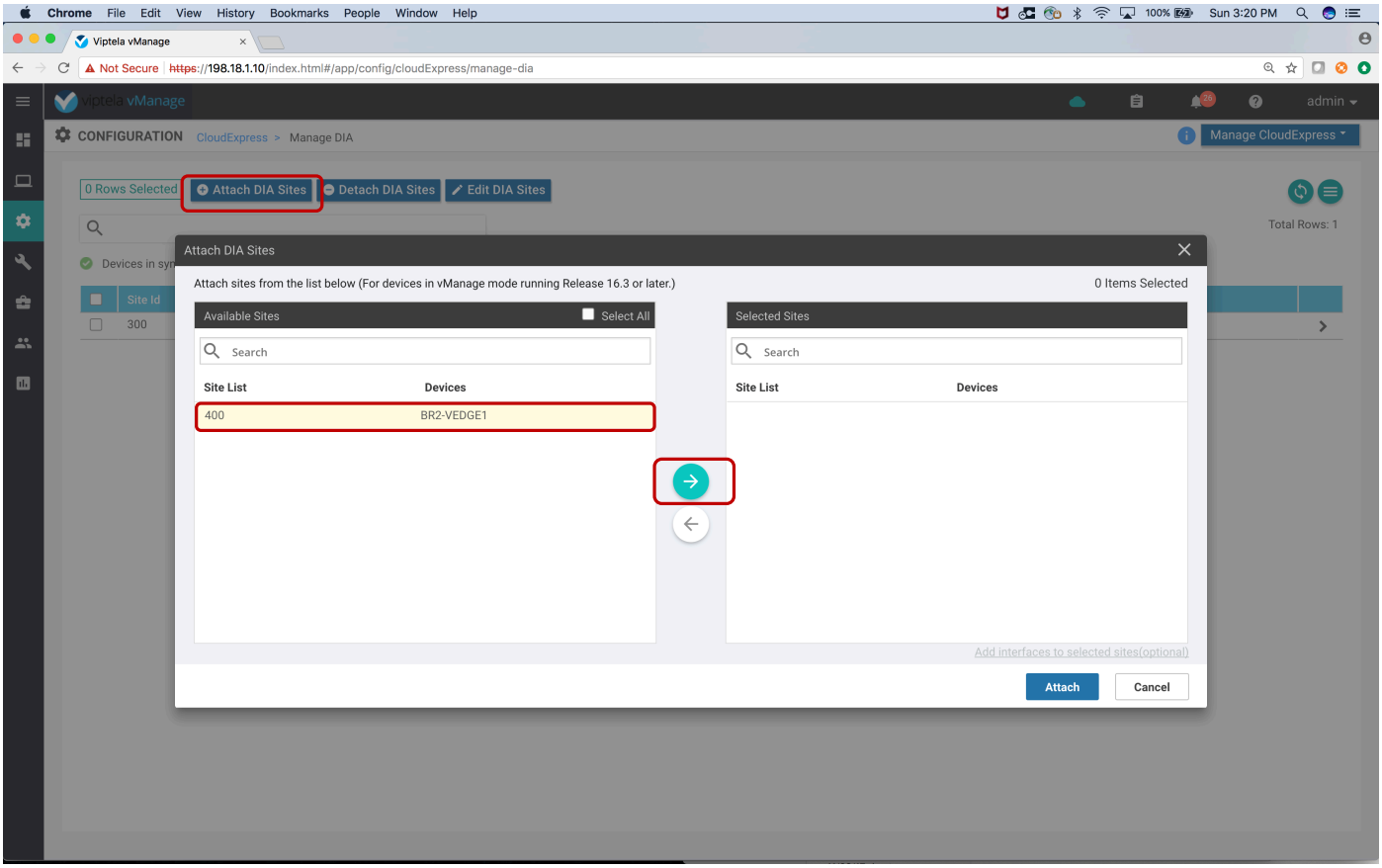


In order to configure the BR2-VEDGE1 as the CloudExpress DIA sites, go to CloudExpress dashboard.

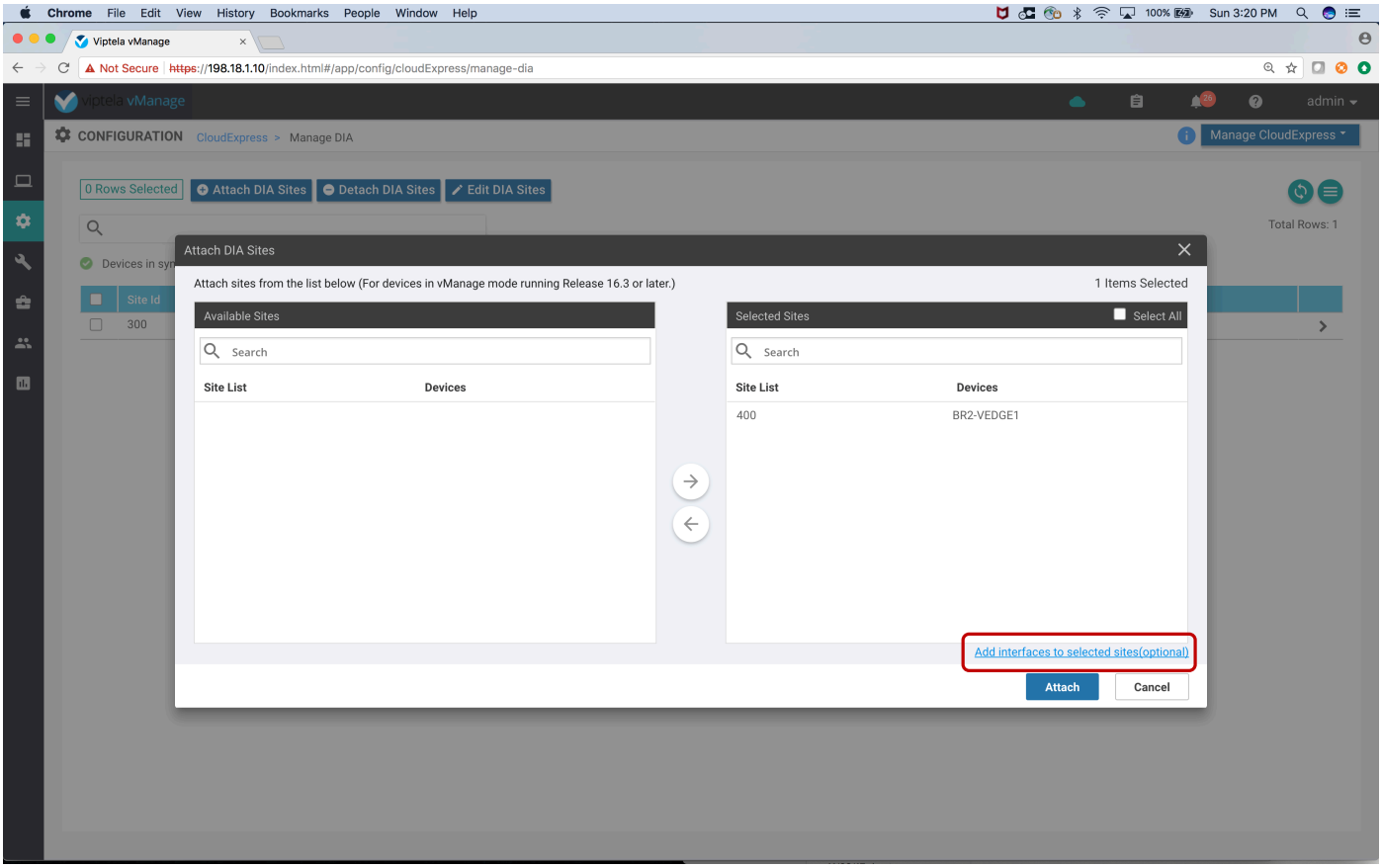
Click on “Manage CloudExpress” button and select “Diresct Internet Access (DIA) Sites”.



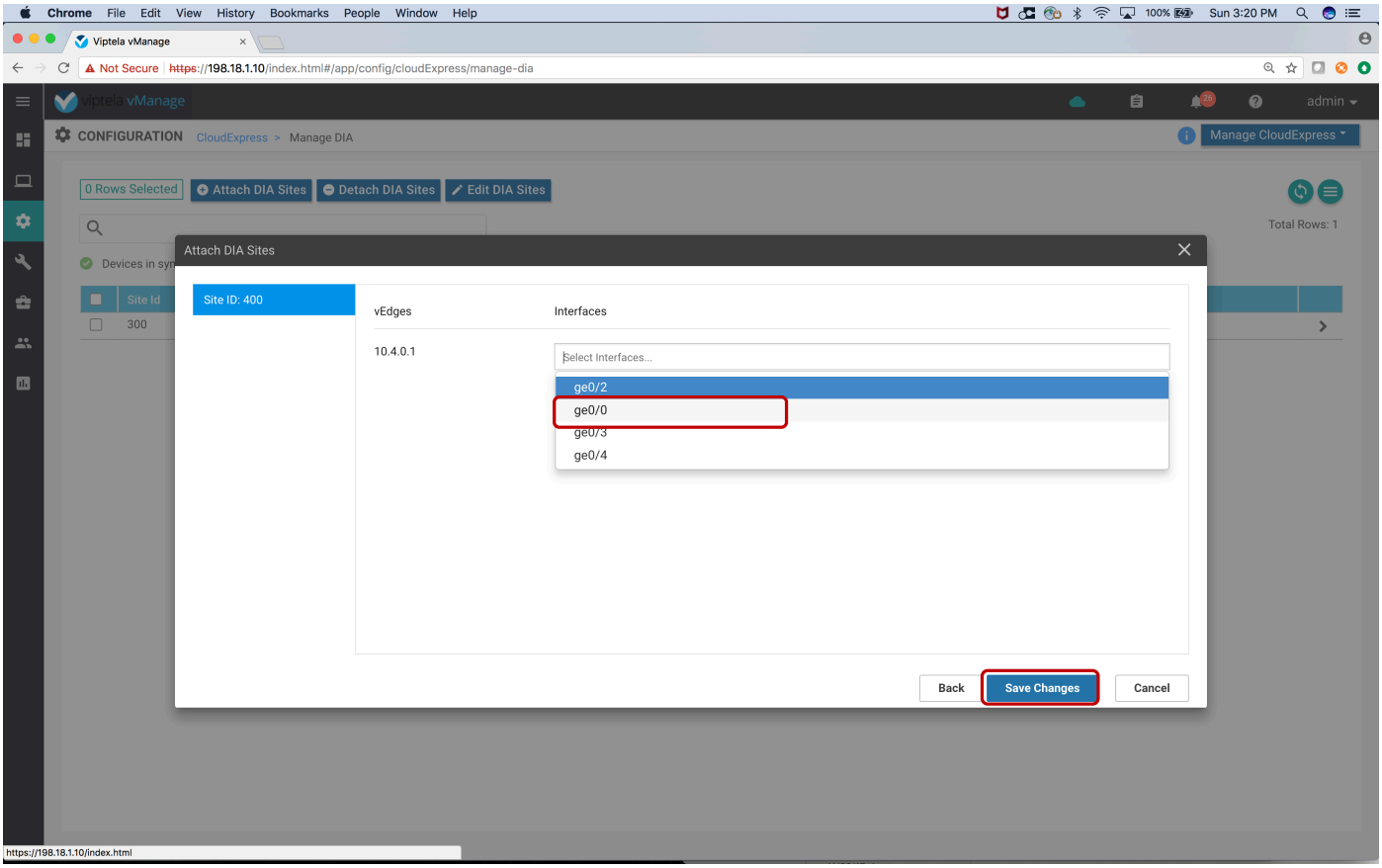
Click on the “Attach DIA Sites” button. On the next pop-up, select BR2-VEDGE1 and Click the right arrow key to move the device in right hand column.



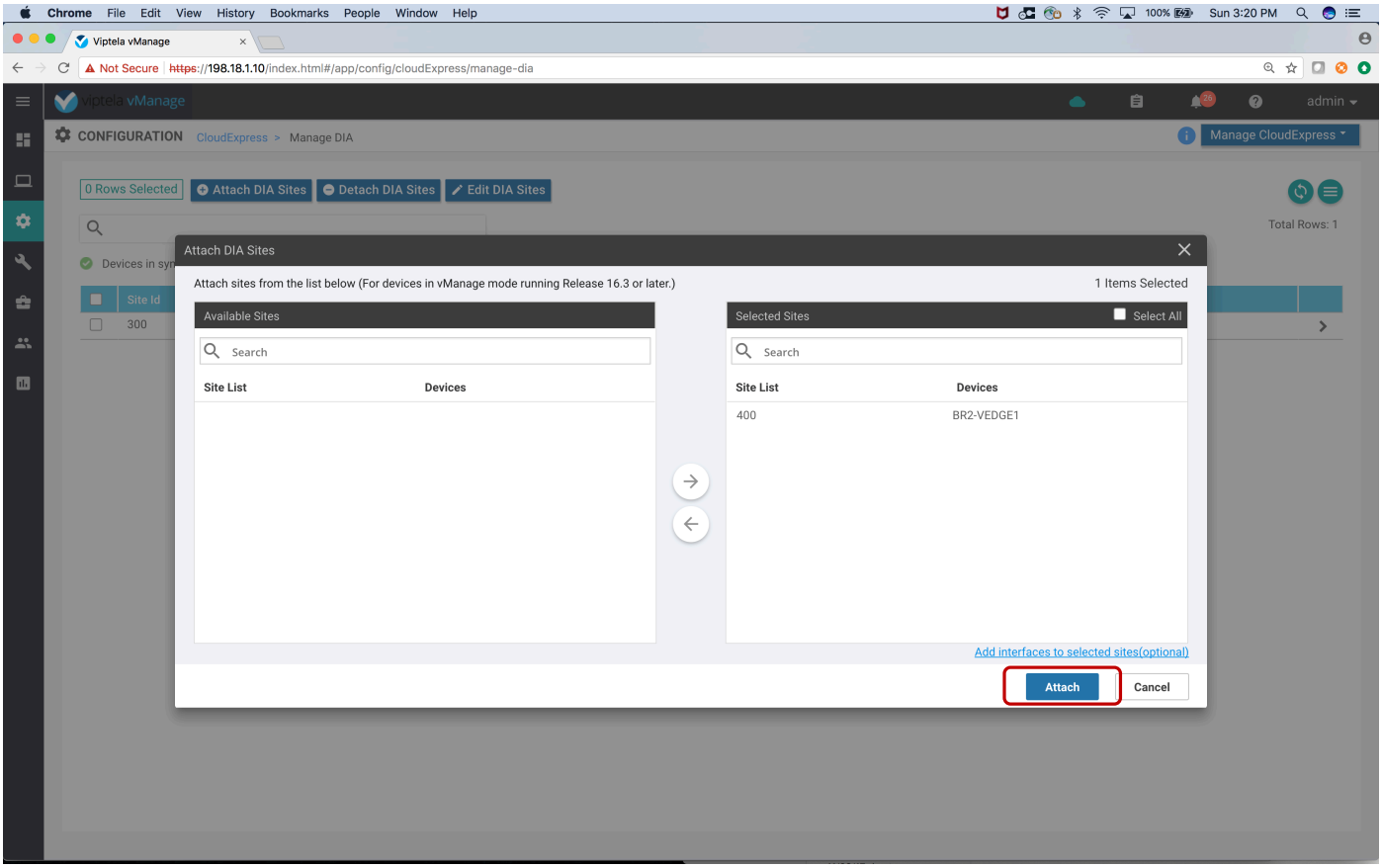
Click on the link “Add interfaces to selected Sites”.



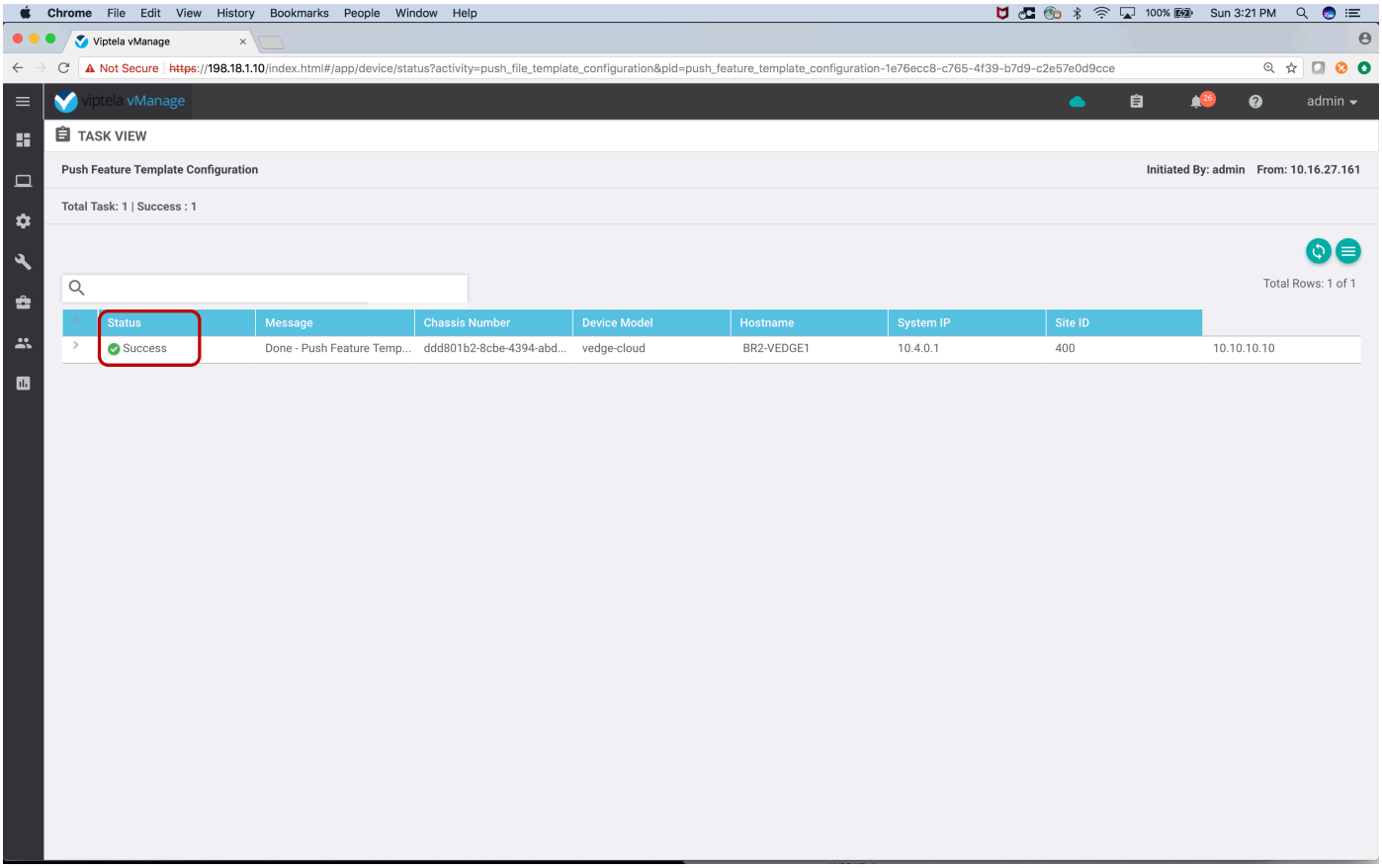
Click in the box “Select Interfaces”, select ge0/0 (internet) interface on BR2-VEDGE1. Then click on “Save Changes” button.



Click on the “Attach” button.



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



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

Lab 08 - Multi-Topology/Different Topologies Per VPN

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

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

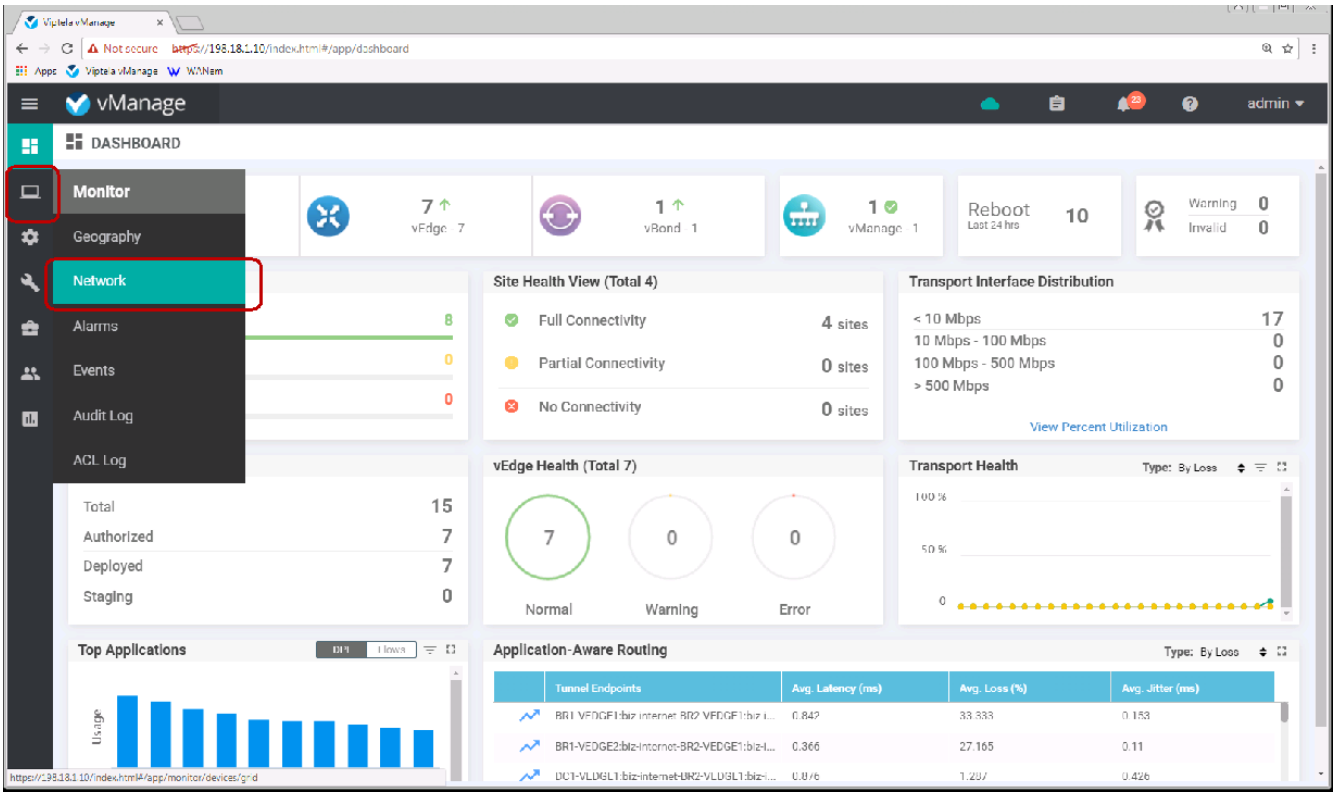
Corporate VPN 10 – Full Mesh

PCI/IOT VPN 20 – Hub-n-Spoke

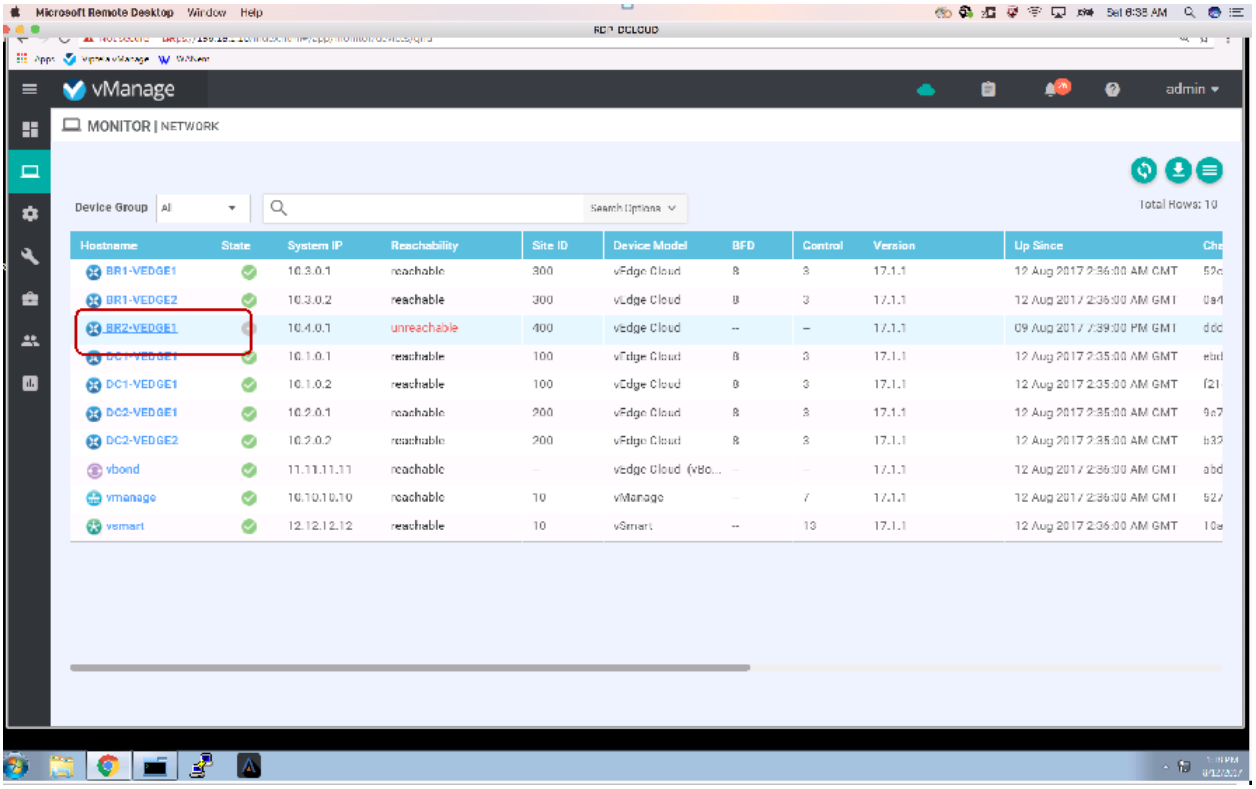
GuestWiFI VPN 40 – DIA ONLY in Branches

Steps

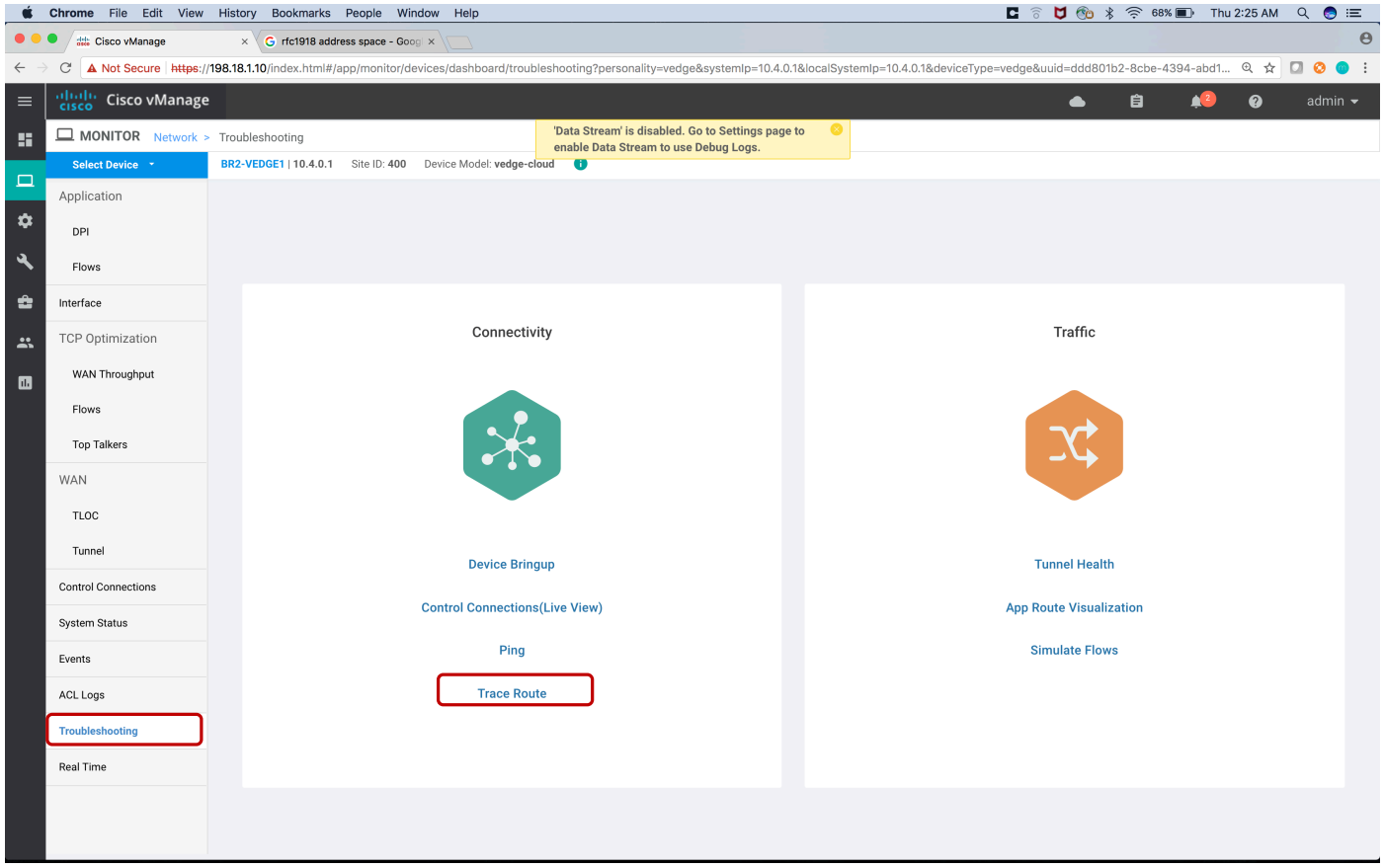
Go to vManage dashboard. Click on the Monitor icon and click on Network from the drop down.



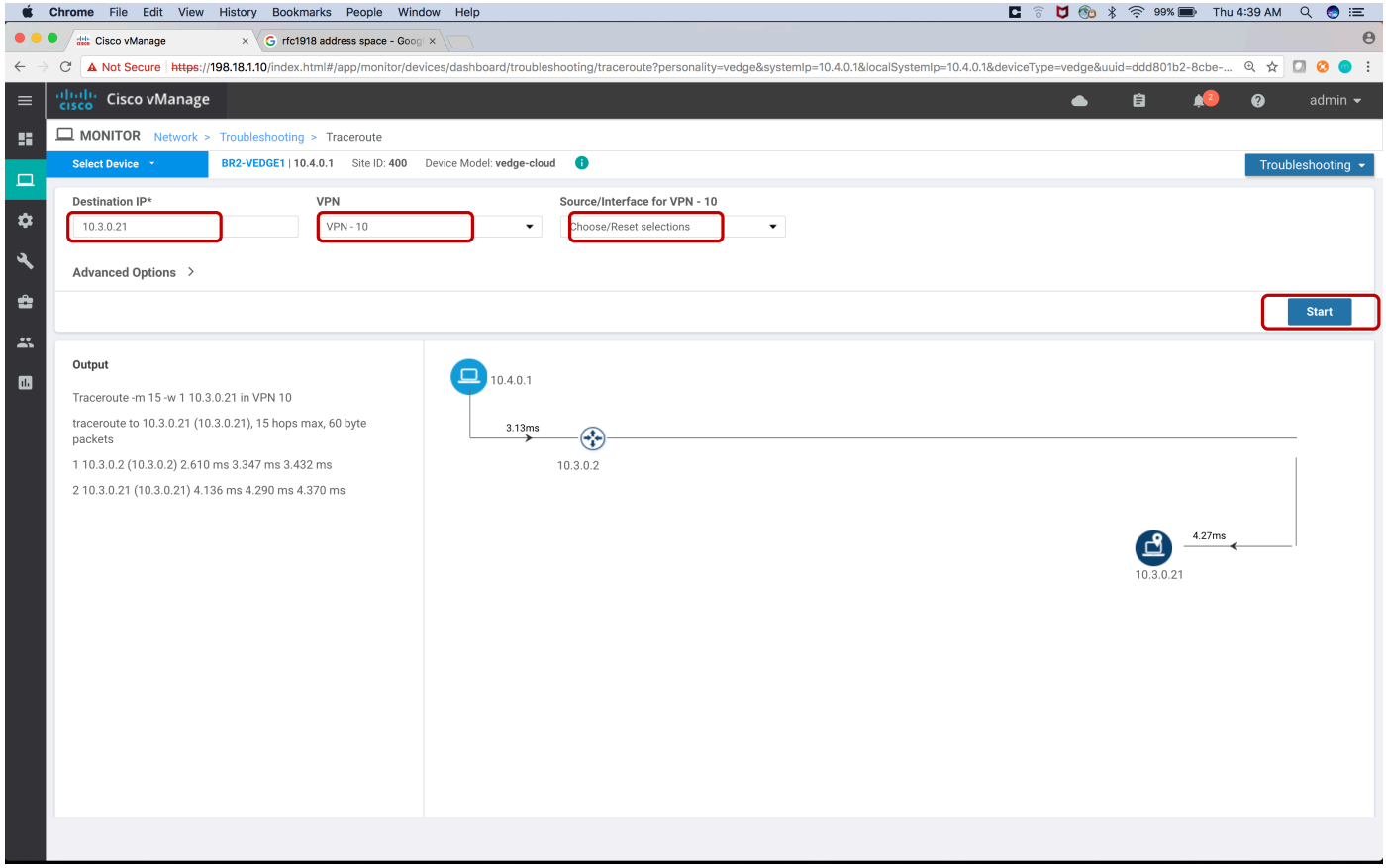
Find BR2-VEDGE1 and click on the name.



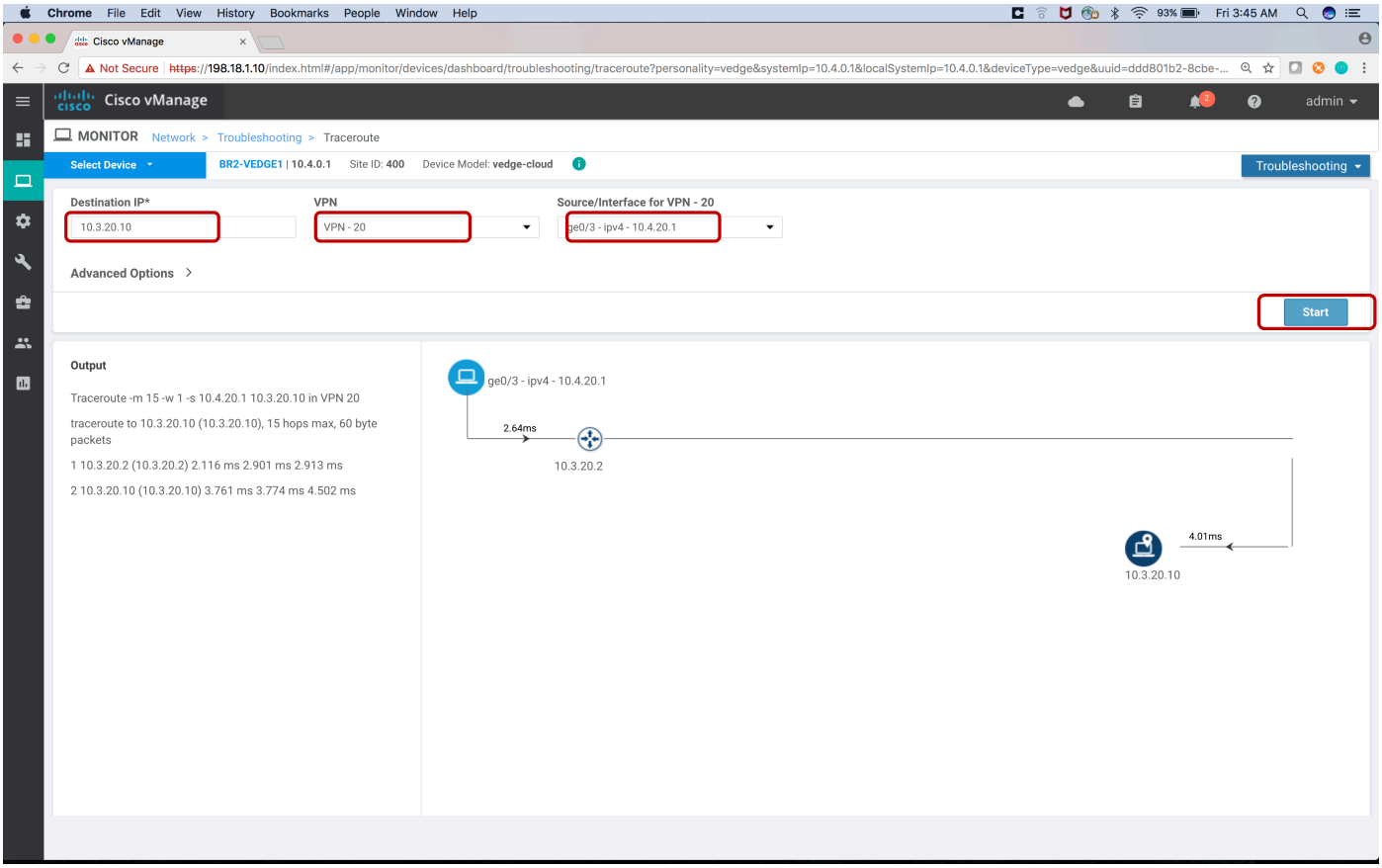
Select Troubleshooting from the left column and then select “Traceroute” option.



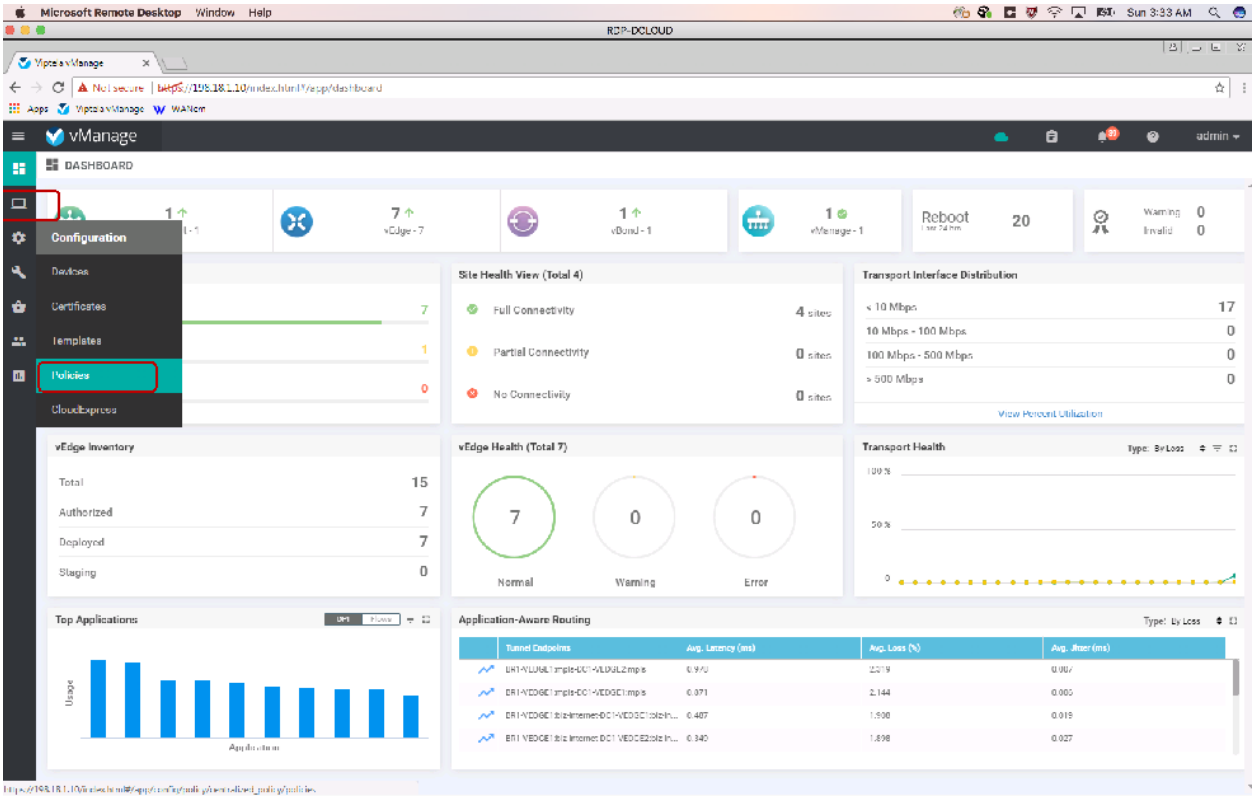
Put in 10.3.0.21 as the destination IP. Select VPN 10 from drop down menu. And click on “Start” button. It shows direct path between Branch1 and Branch2 for VPN 10.



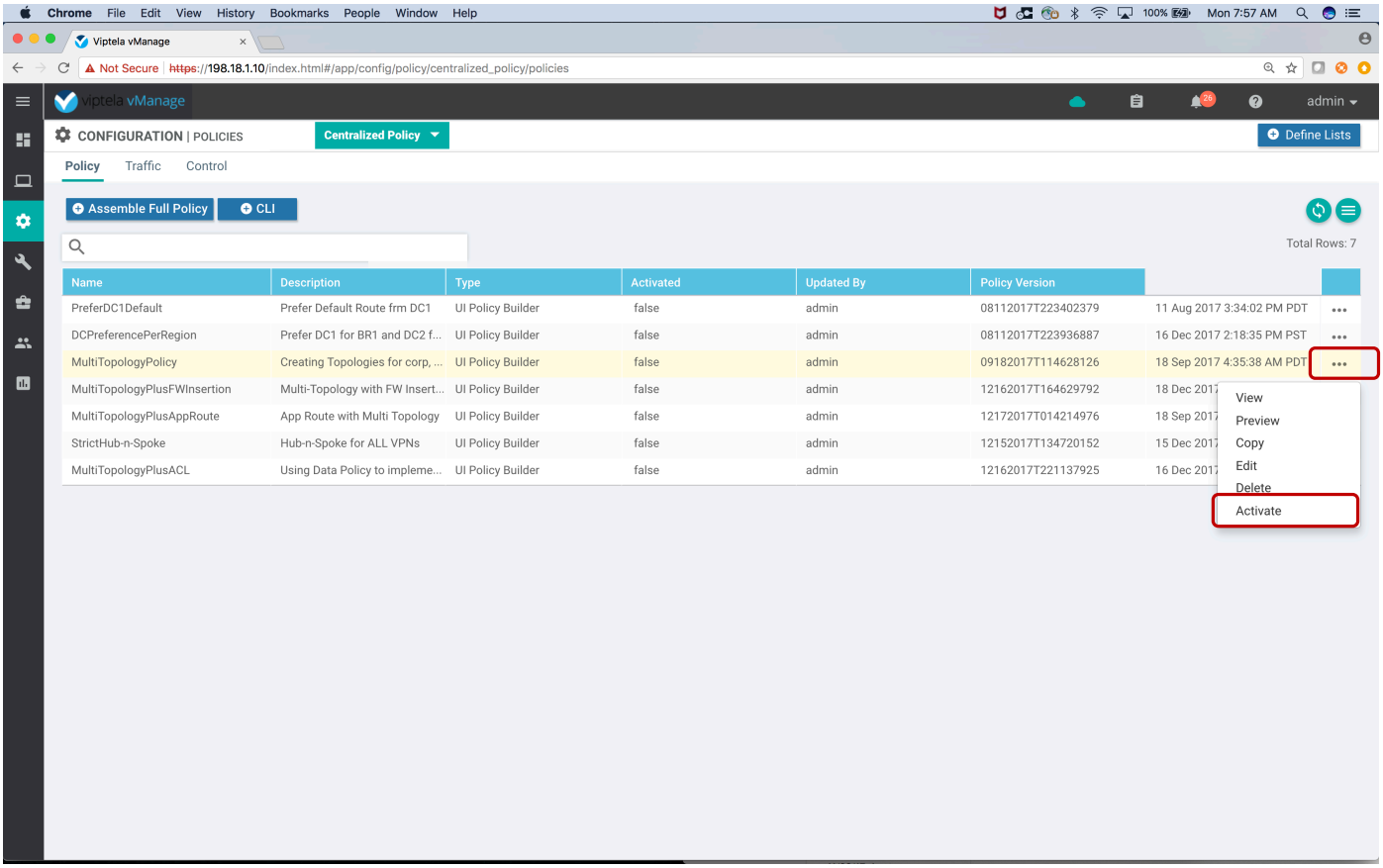
Do the same for VPN 20. This time the destination IP would be 10.3.20.10 and VPN would be 20. It shows direct connectivity between Branch1 and Branch2 for VPN 20.



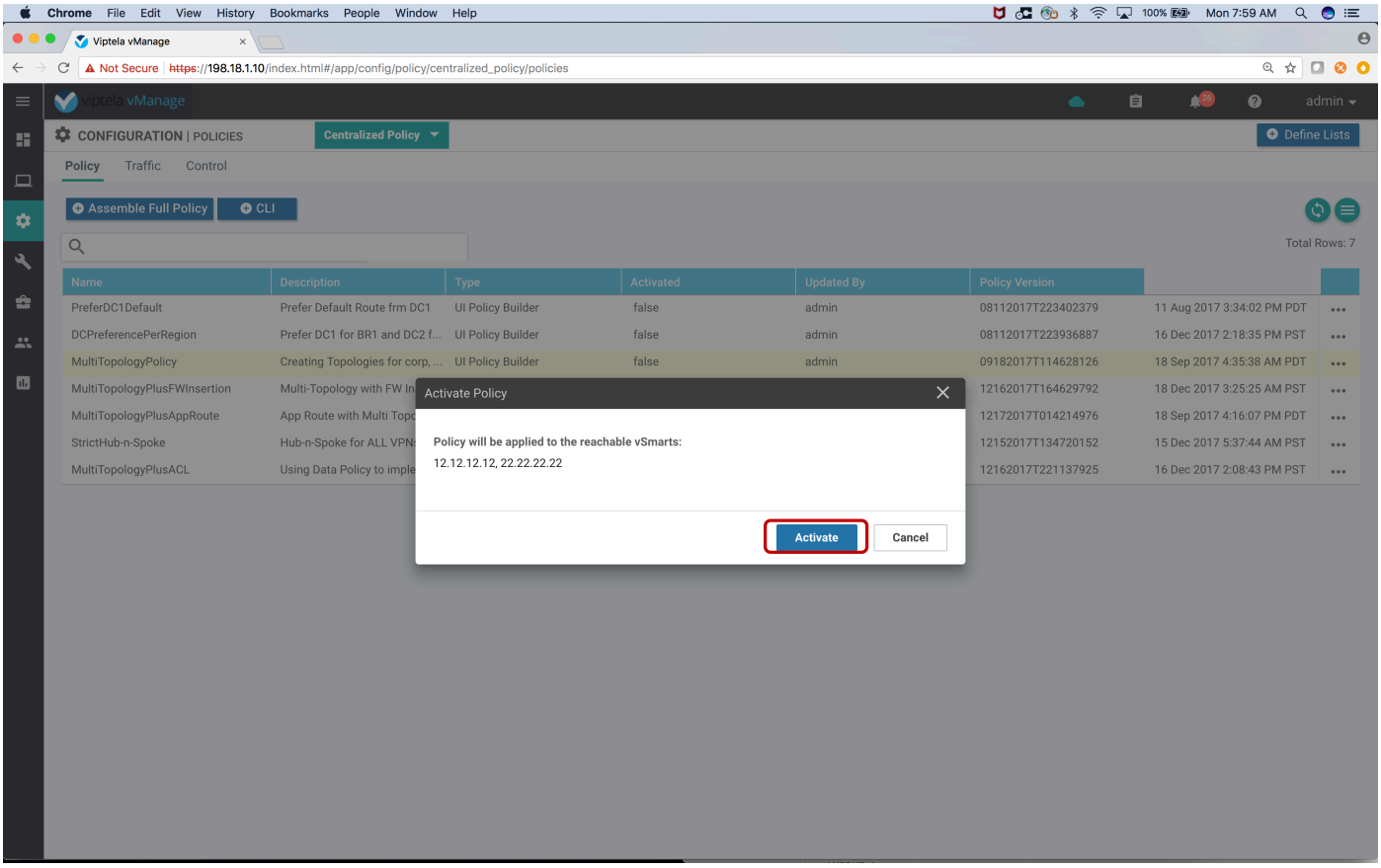
Go to vManage dashboard and go to Configuration and select Policies.



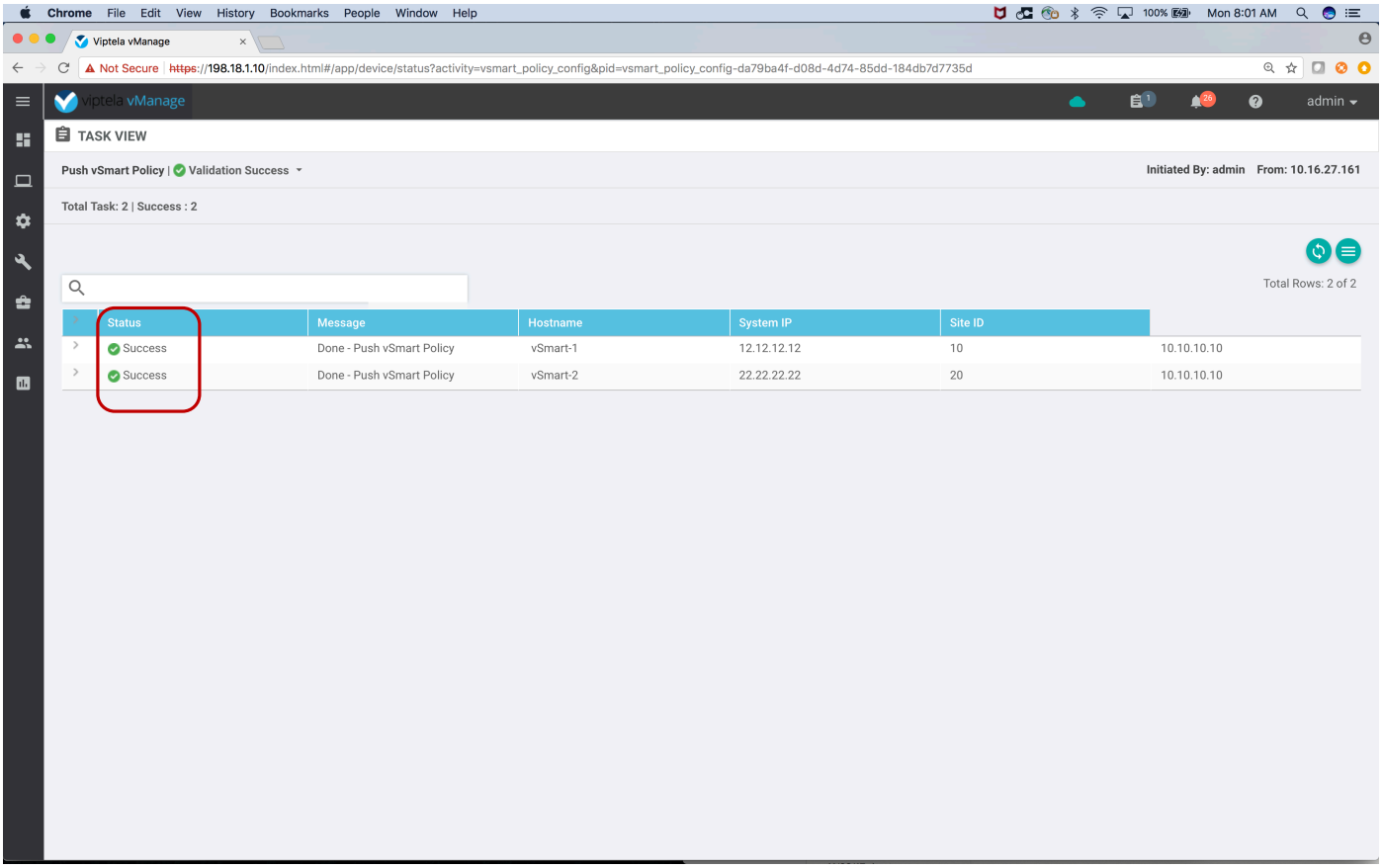
Click in the right most column of the policy named “MultiTopologyPolicy”. From pull down click on “Activate”.



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

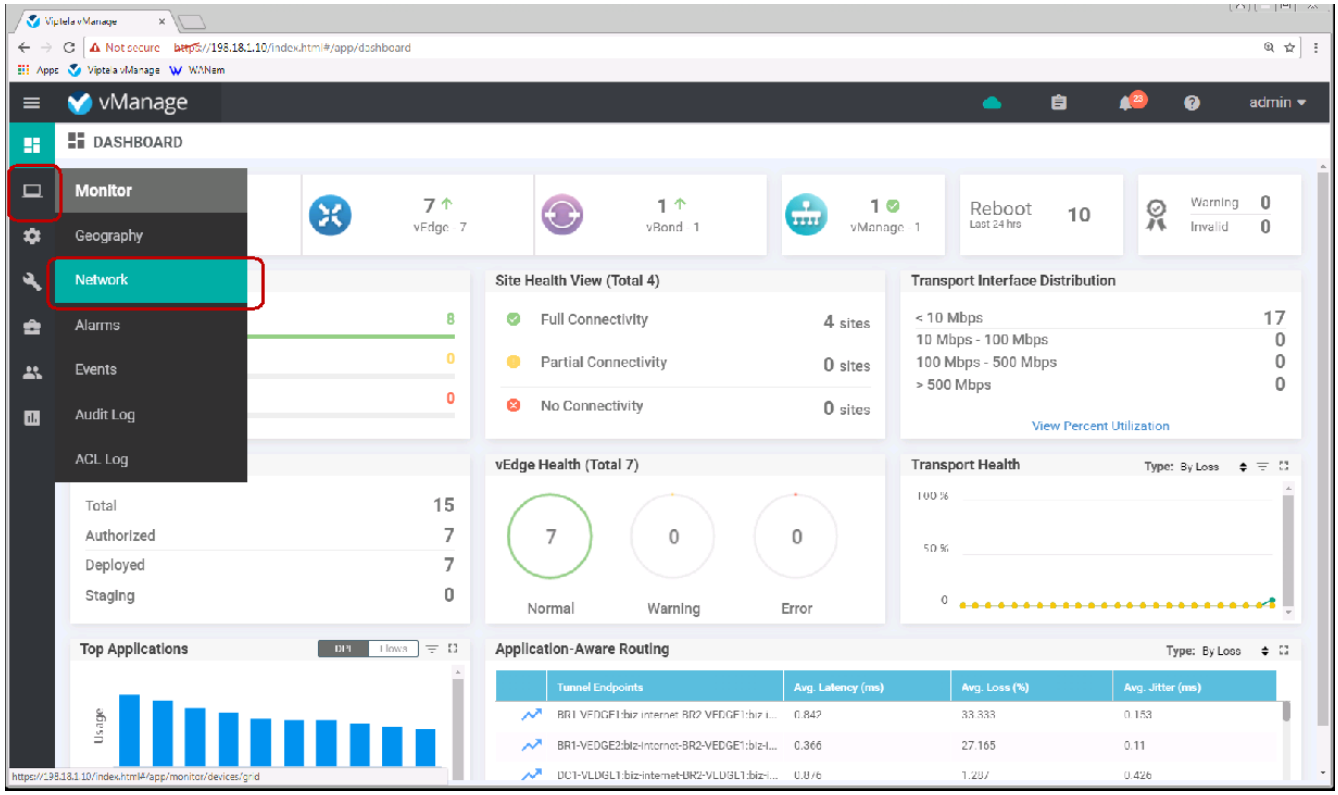


Wait until the policy has been successfully been pushed to the vSmarts. Activation Status would change to “Success”.

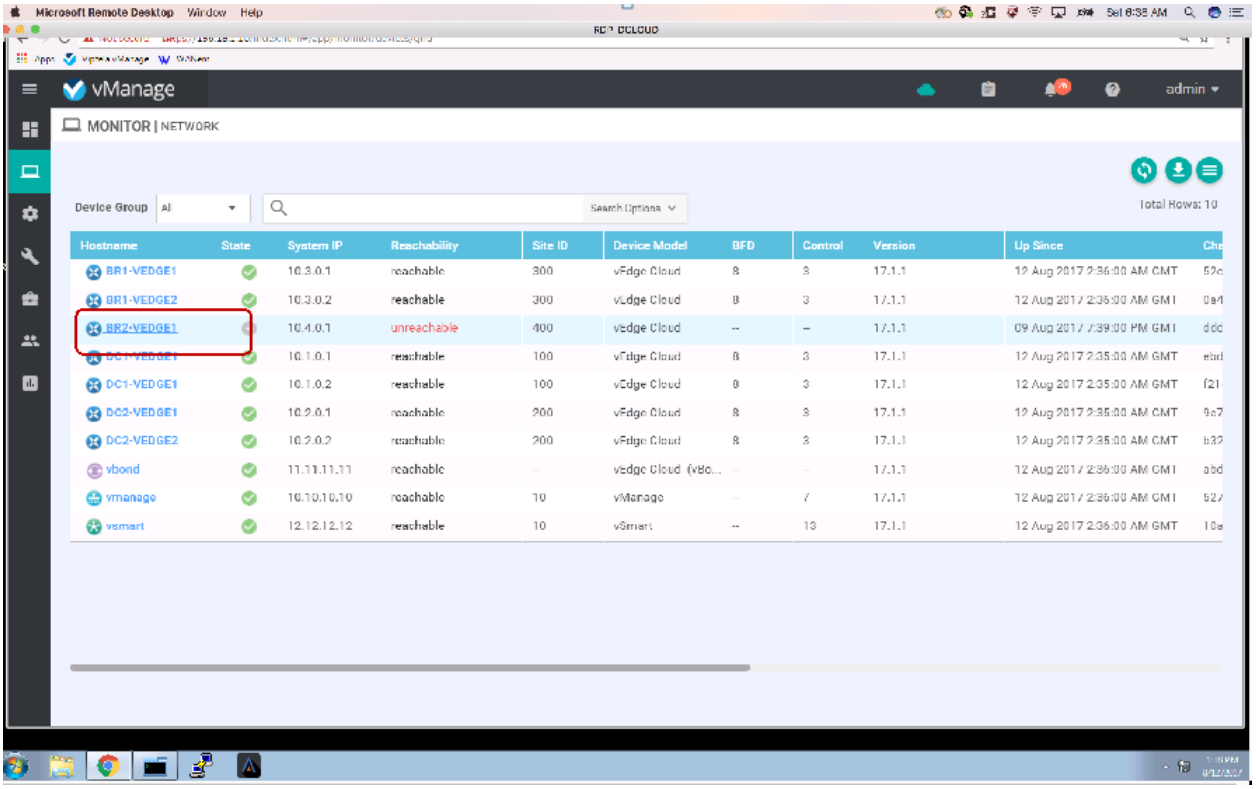


To validate full mesh for VPN 10 and Hub-n-Spoke for VPN 20, go to the dashboard for BR2-VEDGE1.

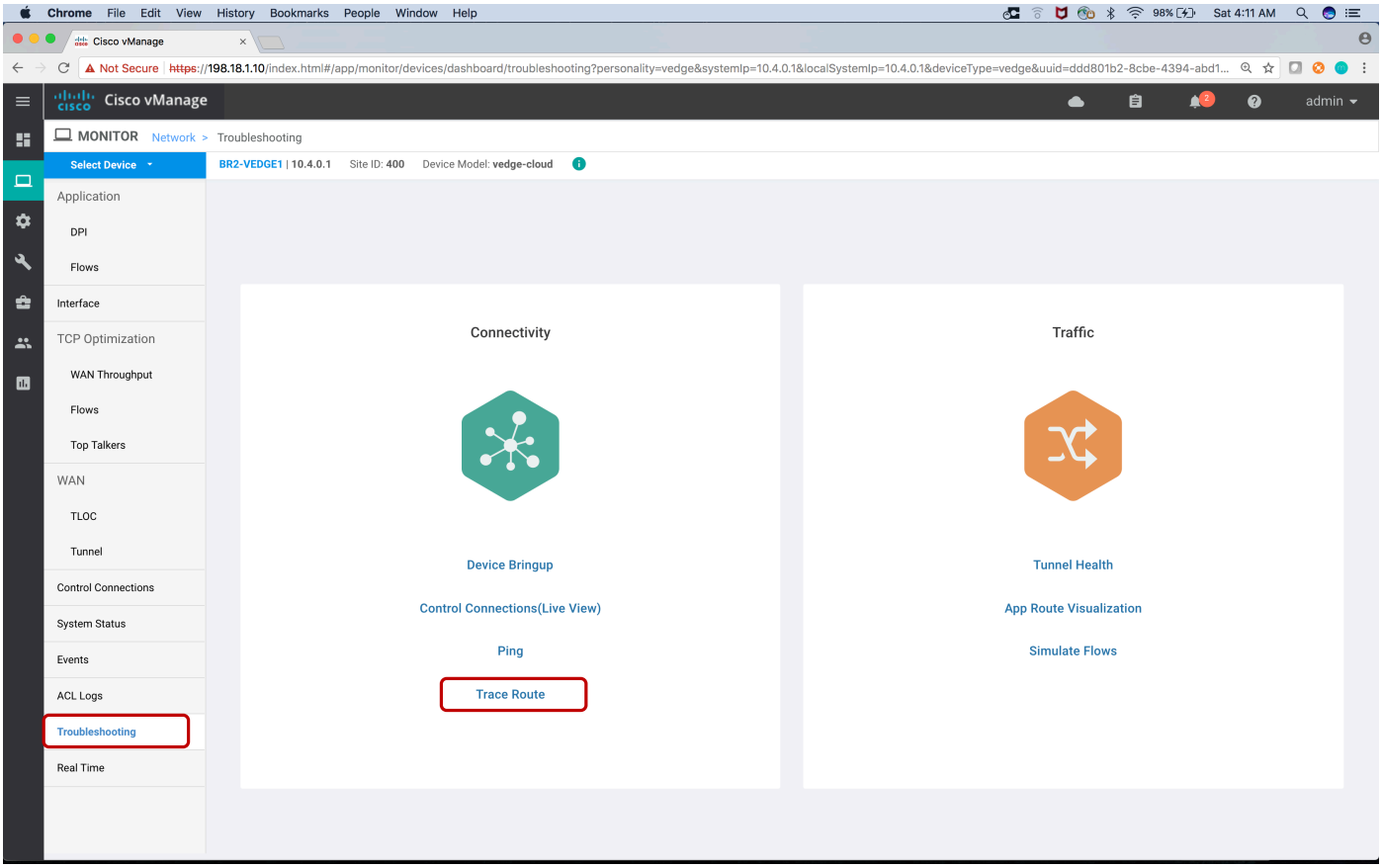
Go to vManage dashboard. Click on the Monitor icon and click on Network from the drop down.



Find BR2-VEDGE1 and click on the name.



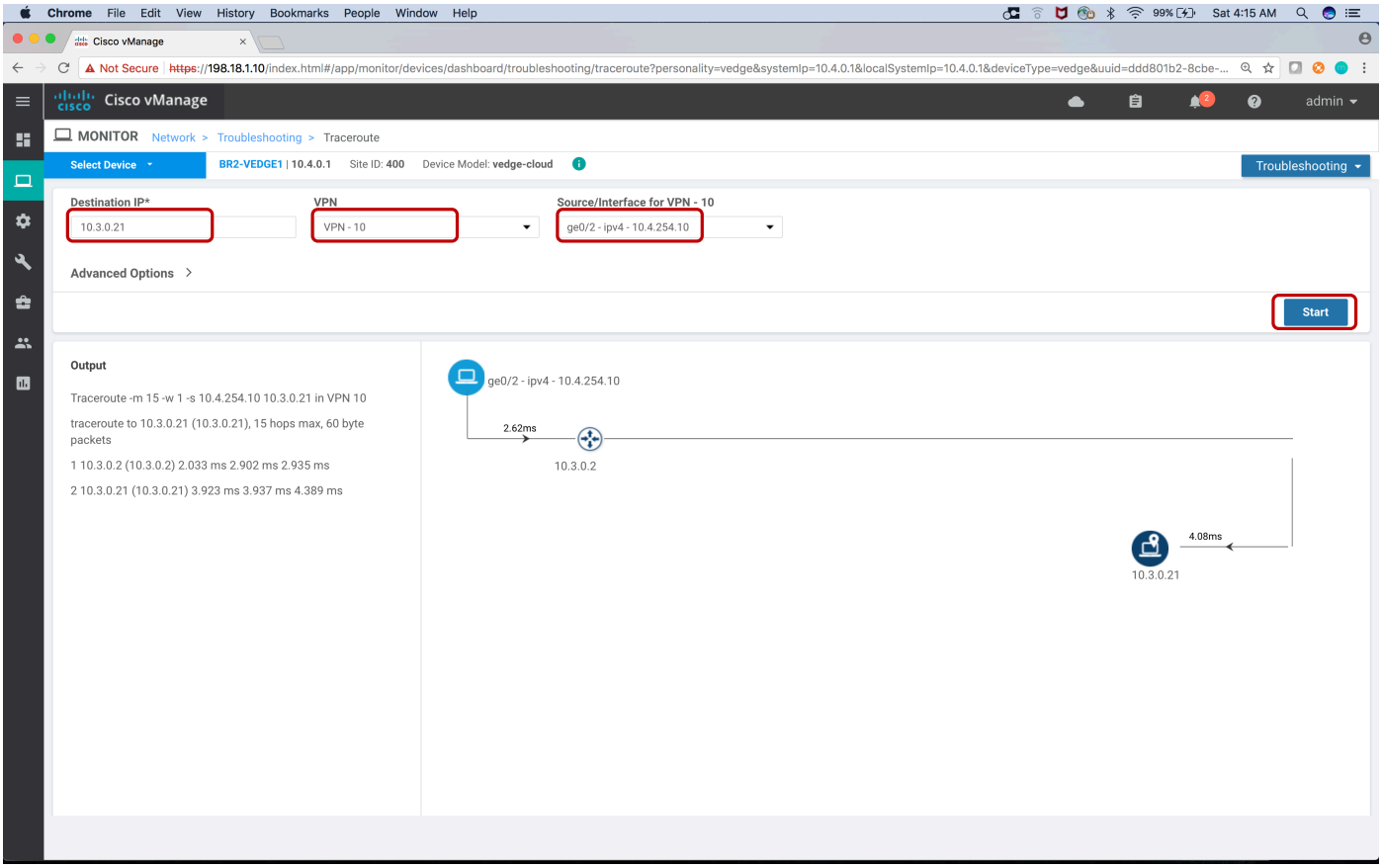
Select Troubleshooting from the left column. Then select “Traceroute”.



Put in 10.3.0.21 as the destination IP.

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

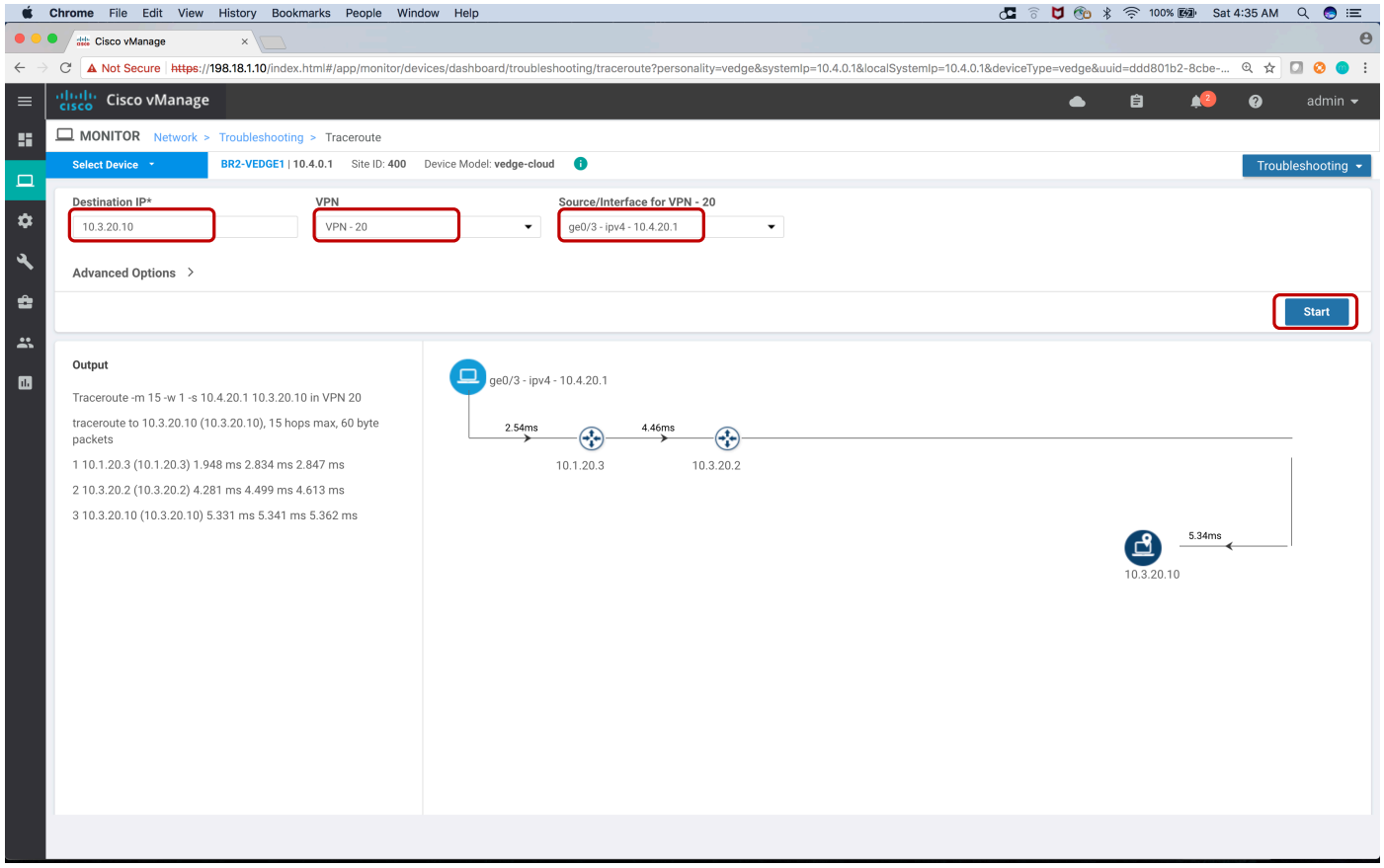
It shows direct path between Branch1 and Branch2 for VPN 10.



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.



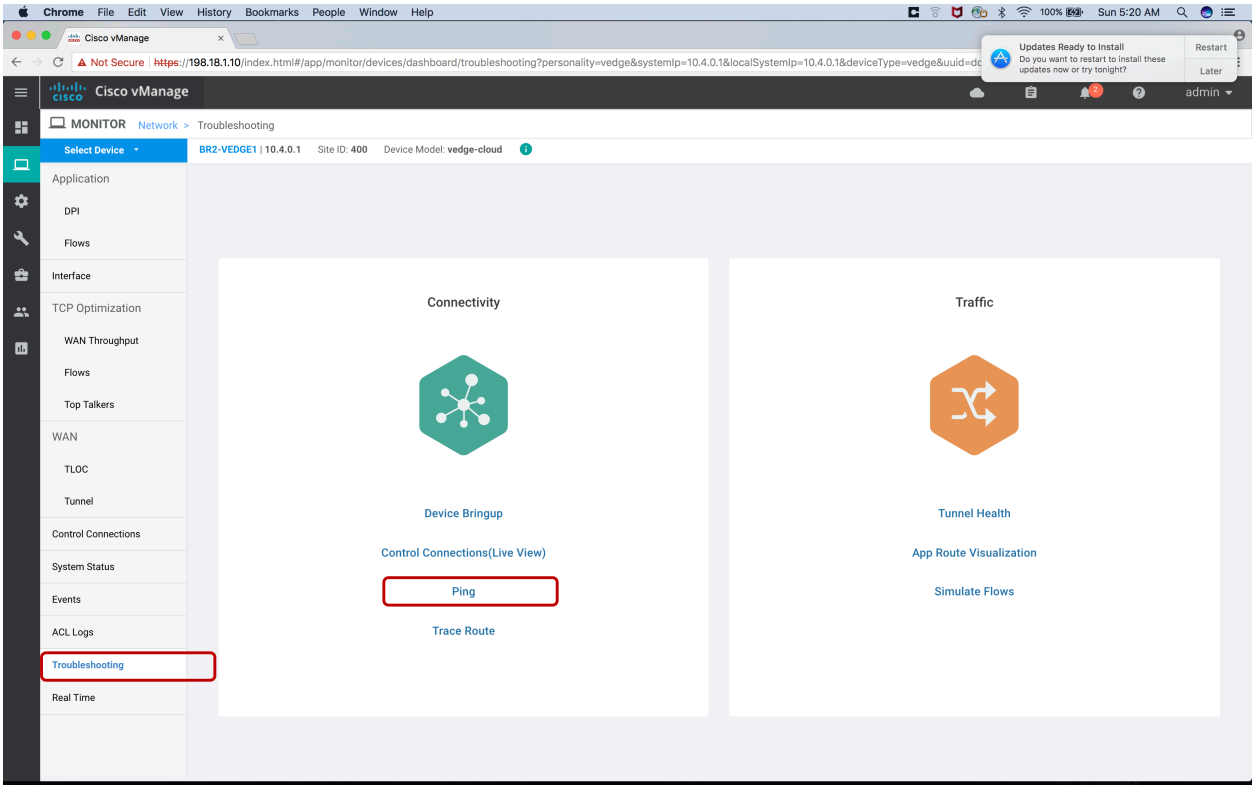
Lab 09 - Application Firewalling using Centralized Policies

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.

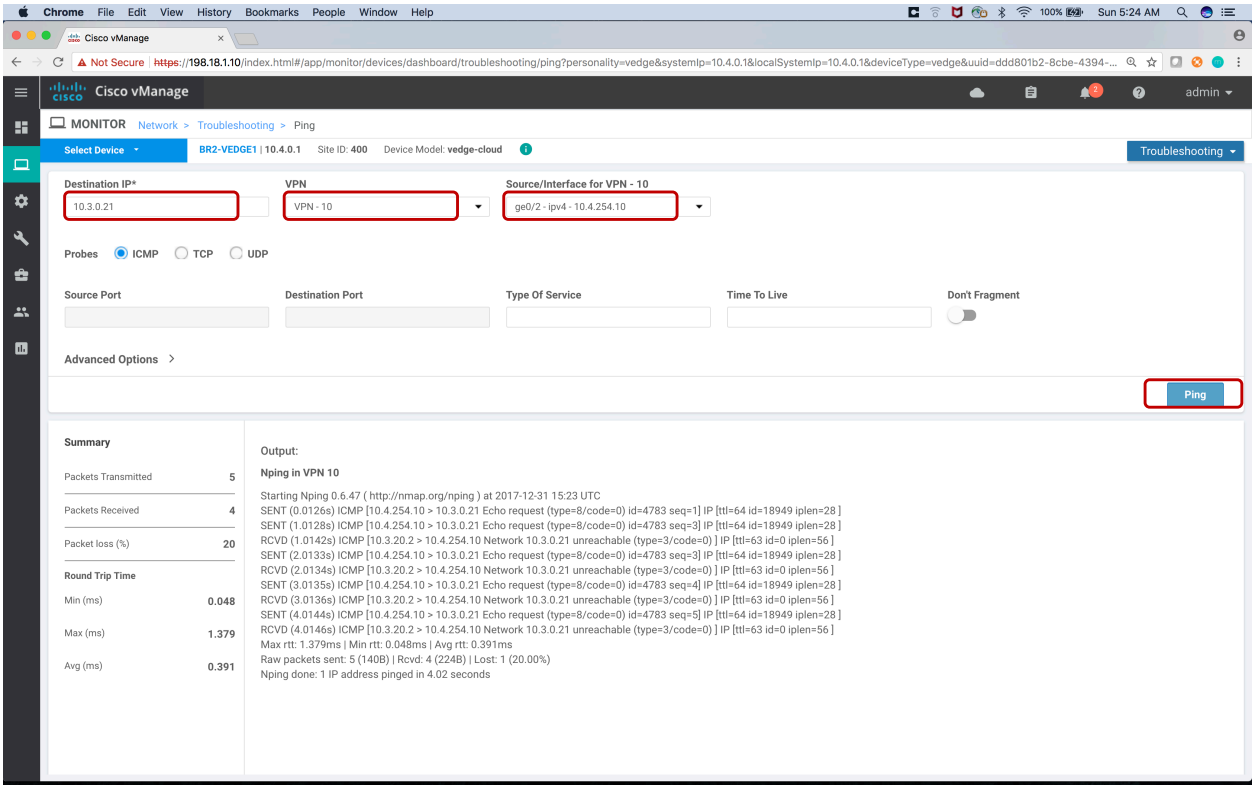
This policy will be implemented as a centralized data policy where based on source and destination prefix match, traffic between BR1 and BR2 is dropped. More granular matches can be done to limit certain applications and allow other applications to flow between the Branches.

Steps

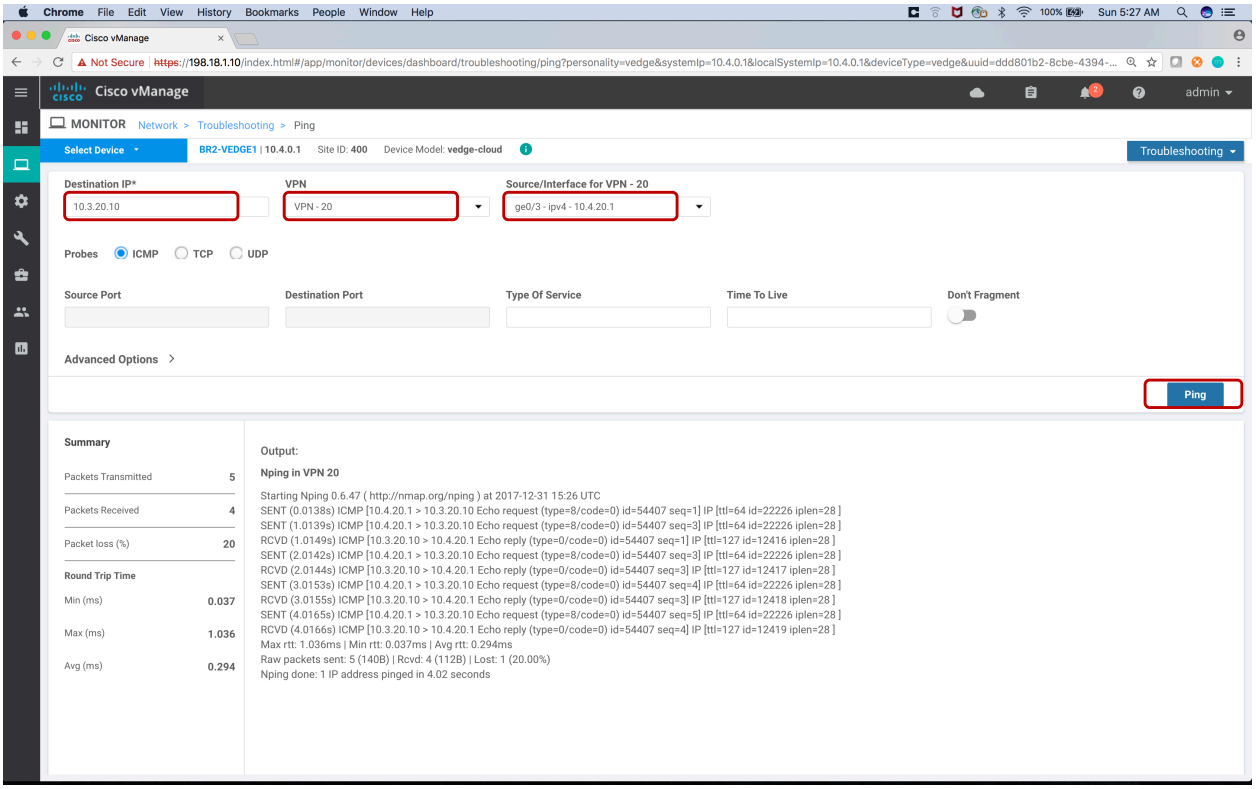
Go to the device dashboard for BR2-VEDGE1 and click "Troubleshooting" tab. Then select "Ping".



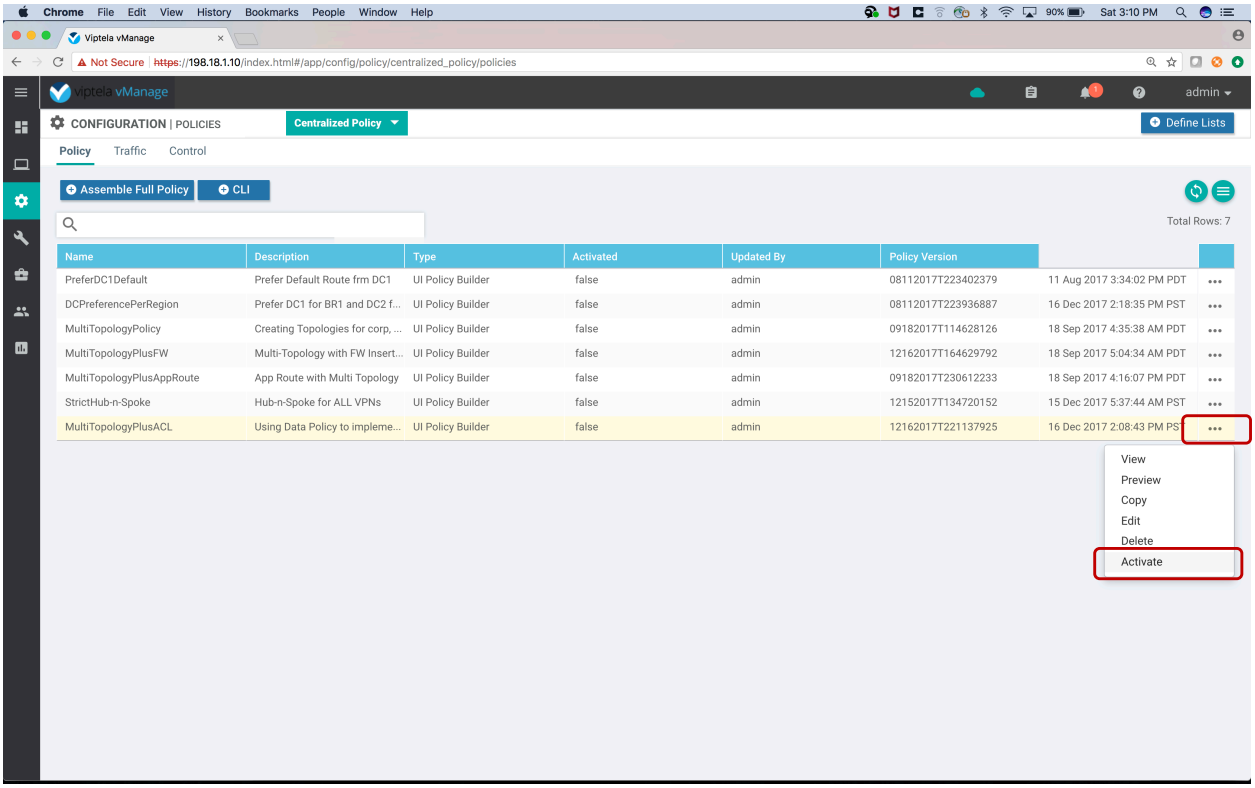
Validate connectivity from BR2-VEDGE1 to the test host in Branch3 in VPN 10 (10.3.0.21).



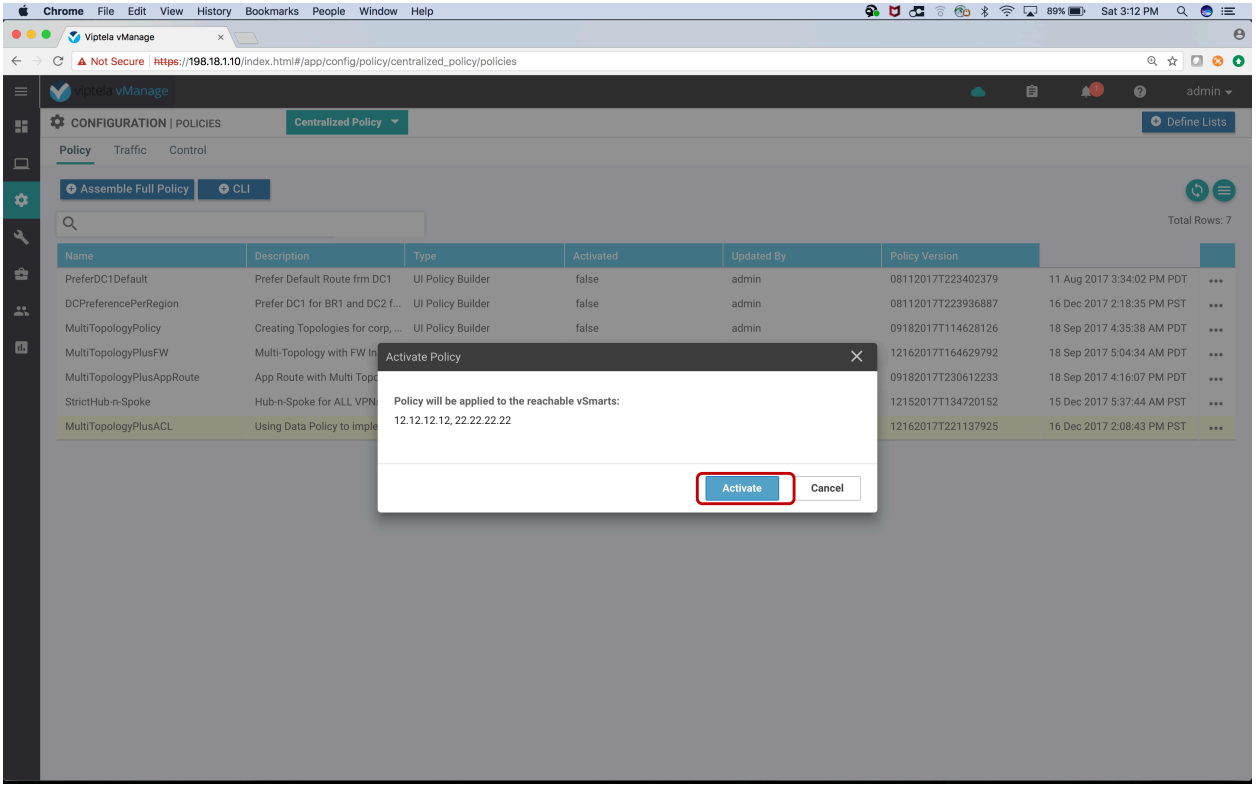
Validate connectivity from BR2-VEDGE1 to the test host in Branch3 in VPN 20 (10.3.20.10).



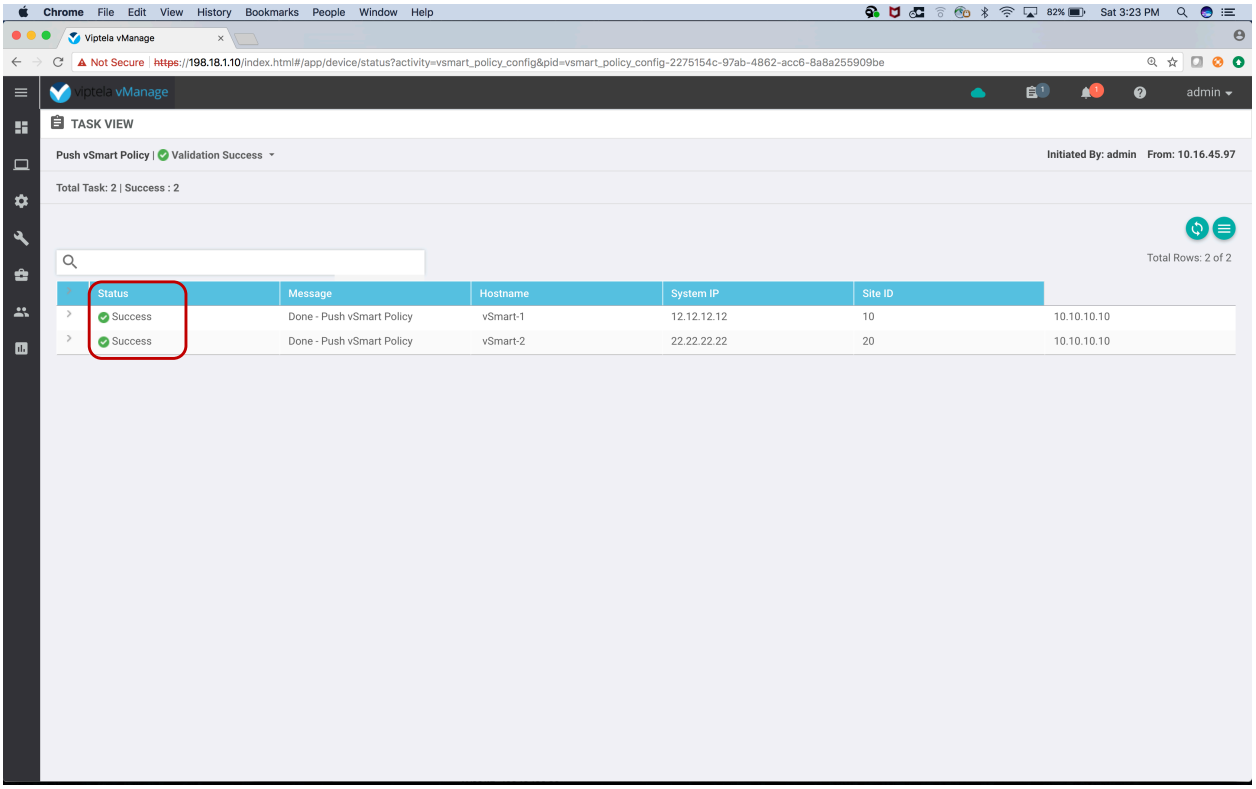
Activate the policy named “MultiTopologyPlusACL”.



Click the “Activate” button.

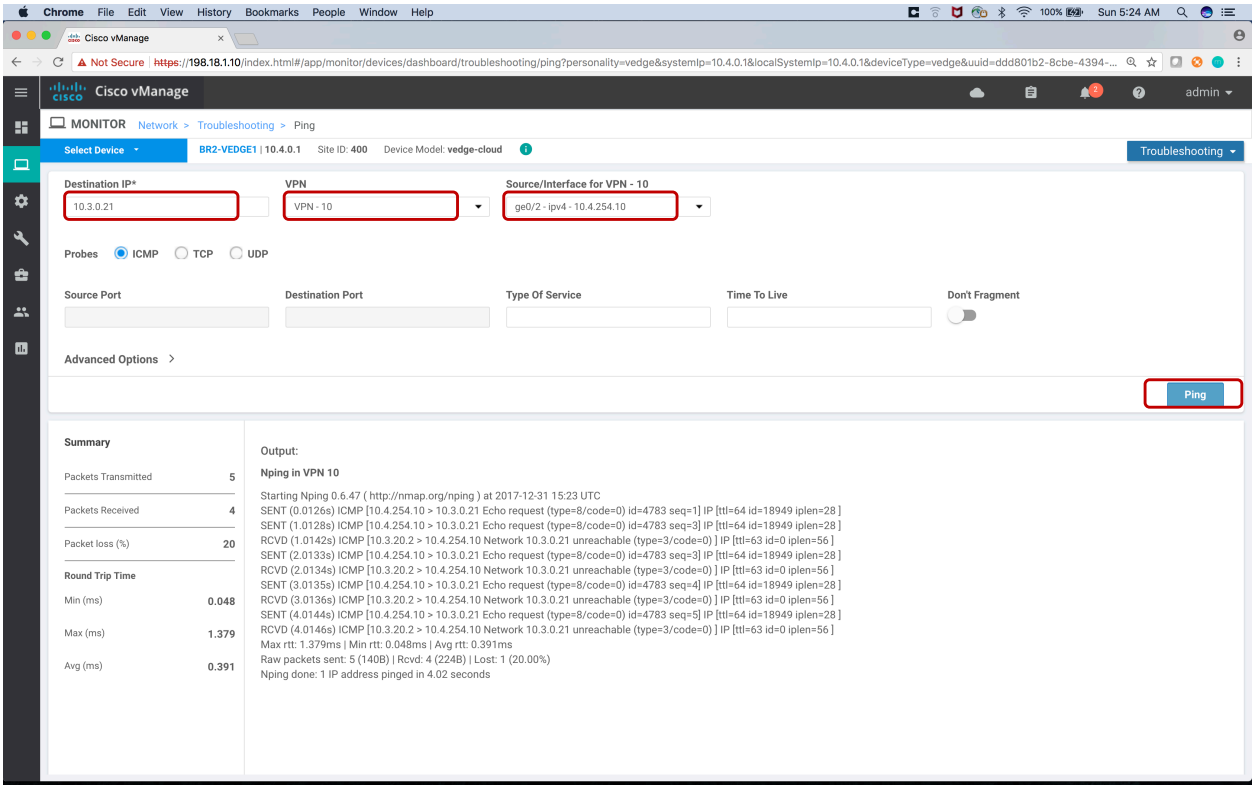


Wait till the policy is pushed successfully pushed to both the vSmarts.



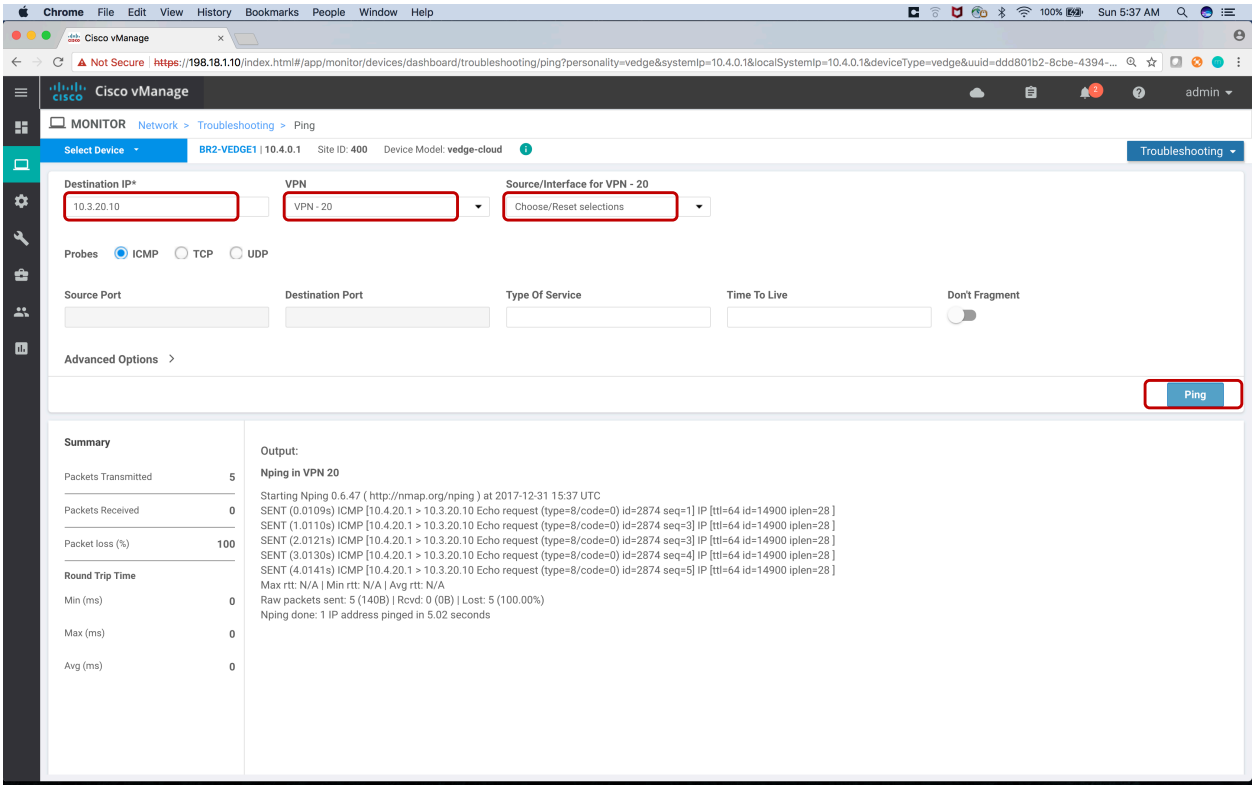
Go to device dashboard for BR2-VEDGE1 and Click on “Troubleshooting” tab.

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



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.



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

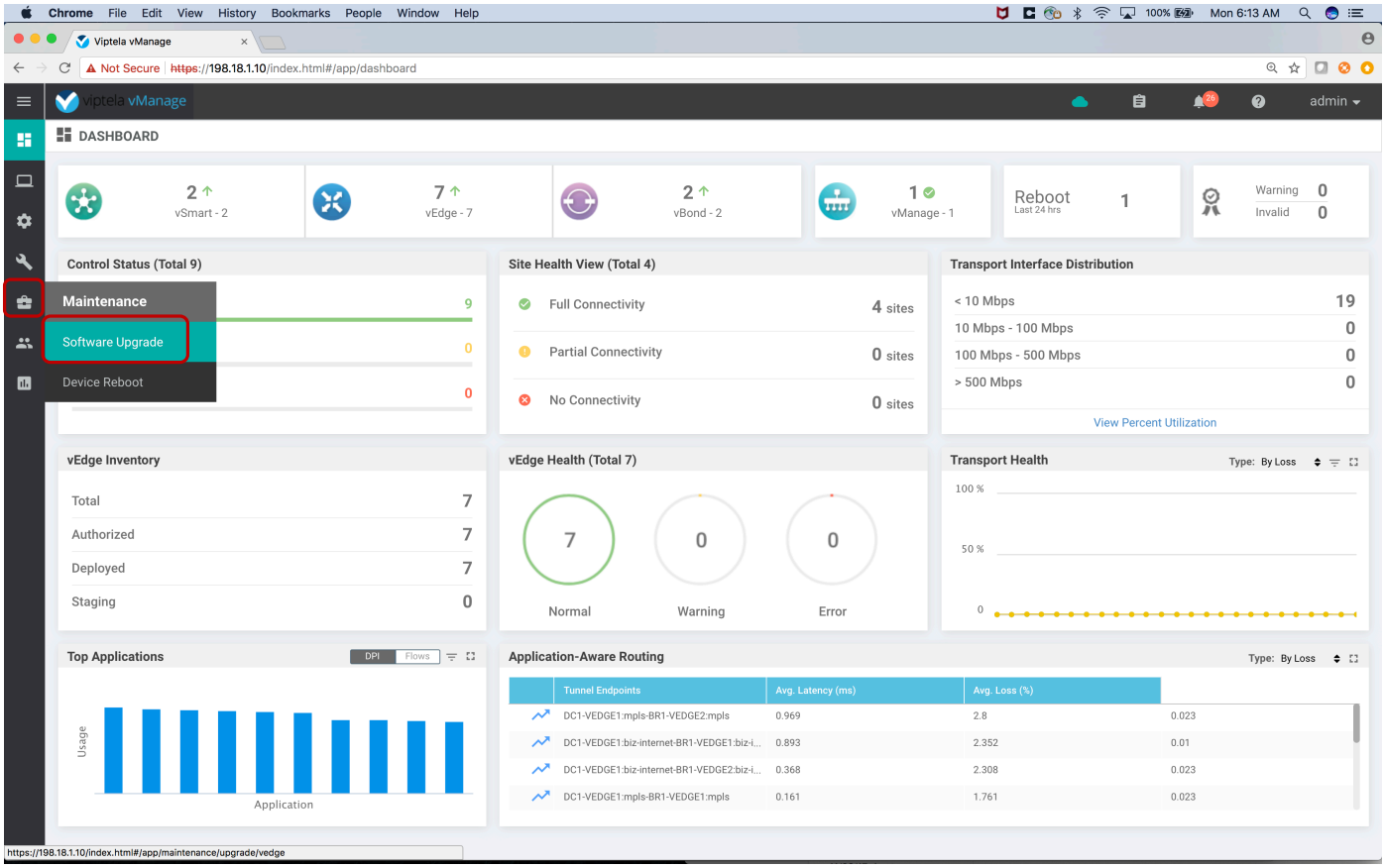
1- Upgrade the vManage

2- Then upgrade the vBonds/vSmarts

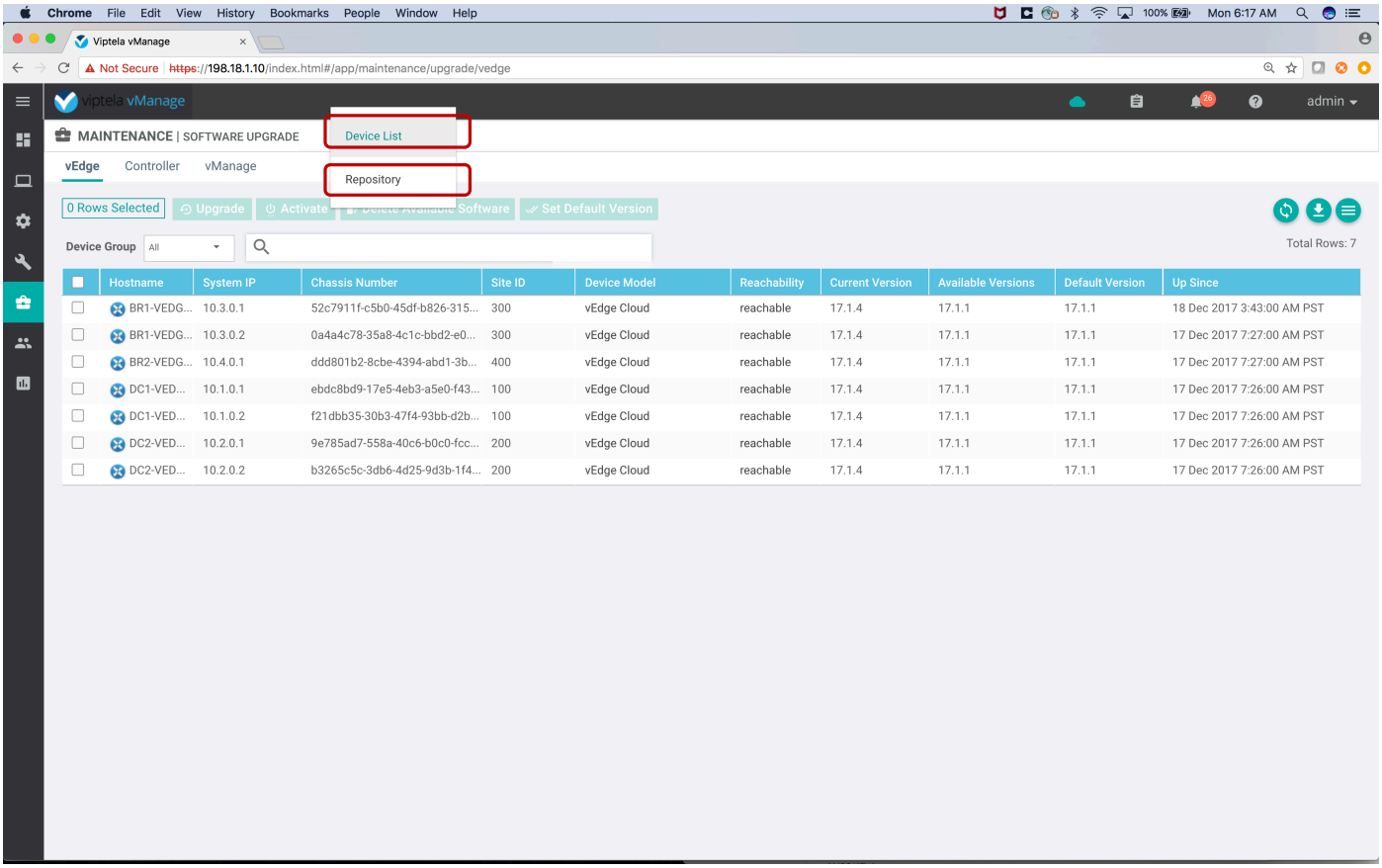
3- Then upgrade the vEdges

Steps

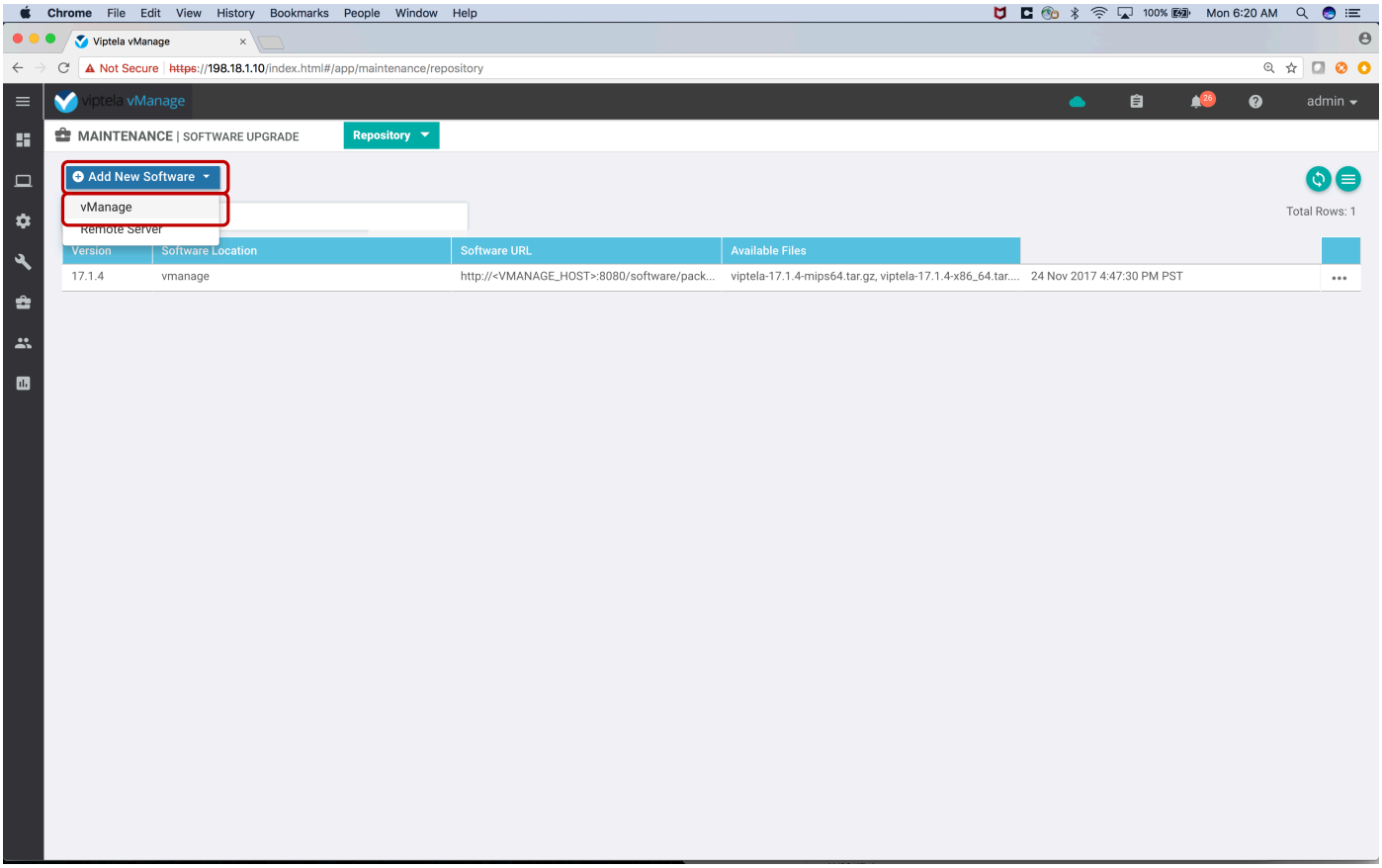
Go to vManage Dashboard.
Click on “Maintenance” icon and select “Software Upgrade” from the pull-down.



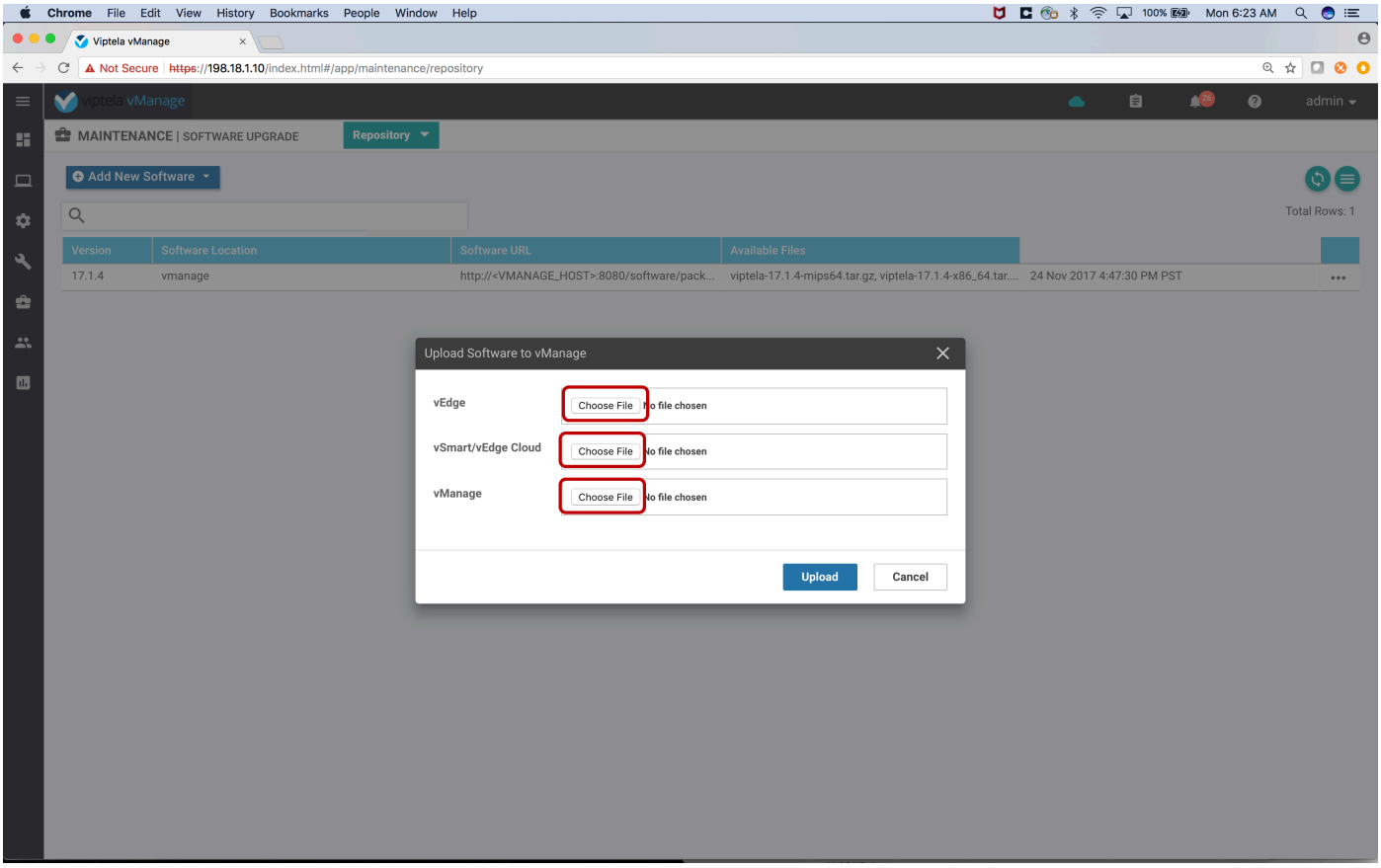
Click on “Device List” and then select “Repository”.



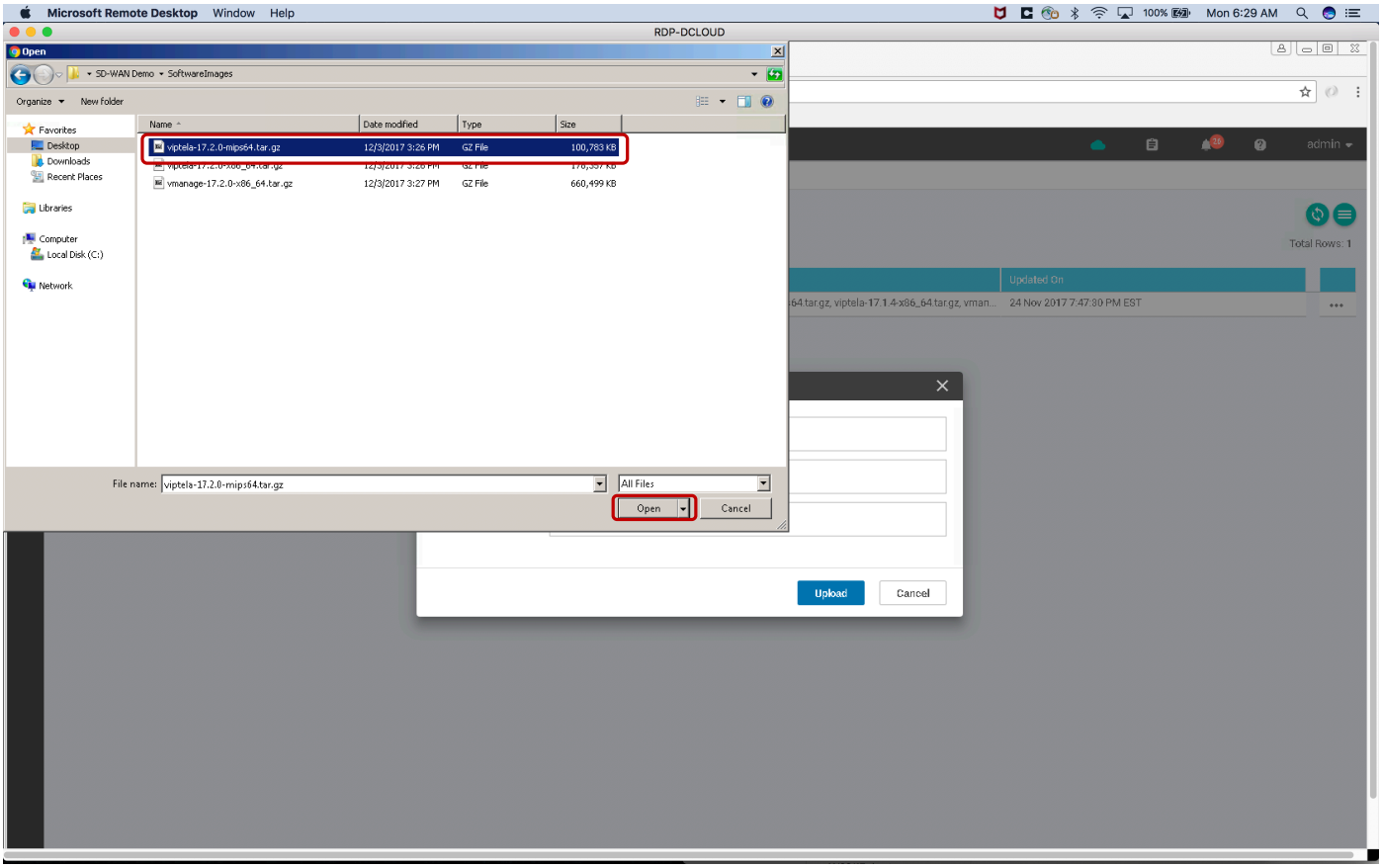
Click on “Add New Software” and then select “vManage”.
This is to upload software to vManage rather than rely on an external server.



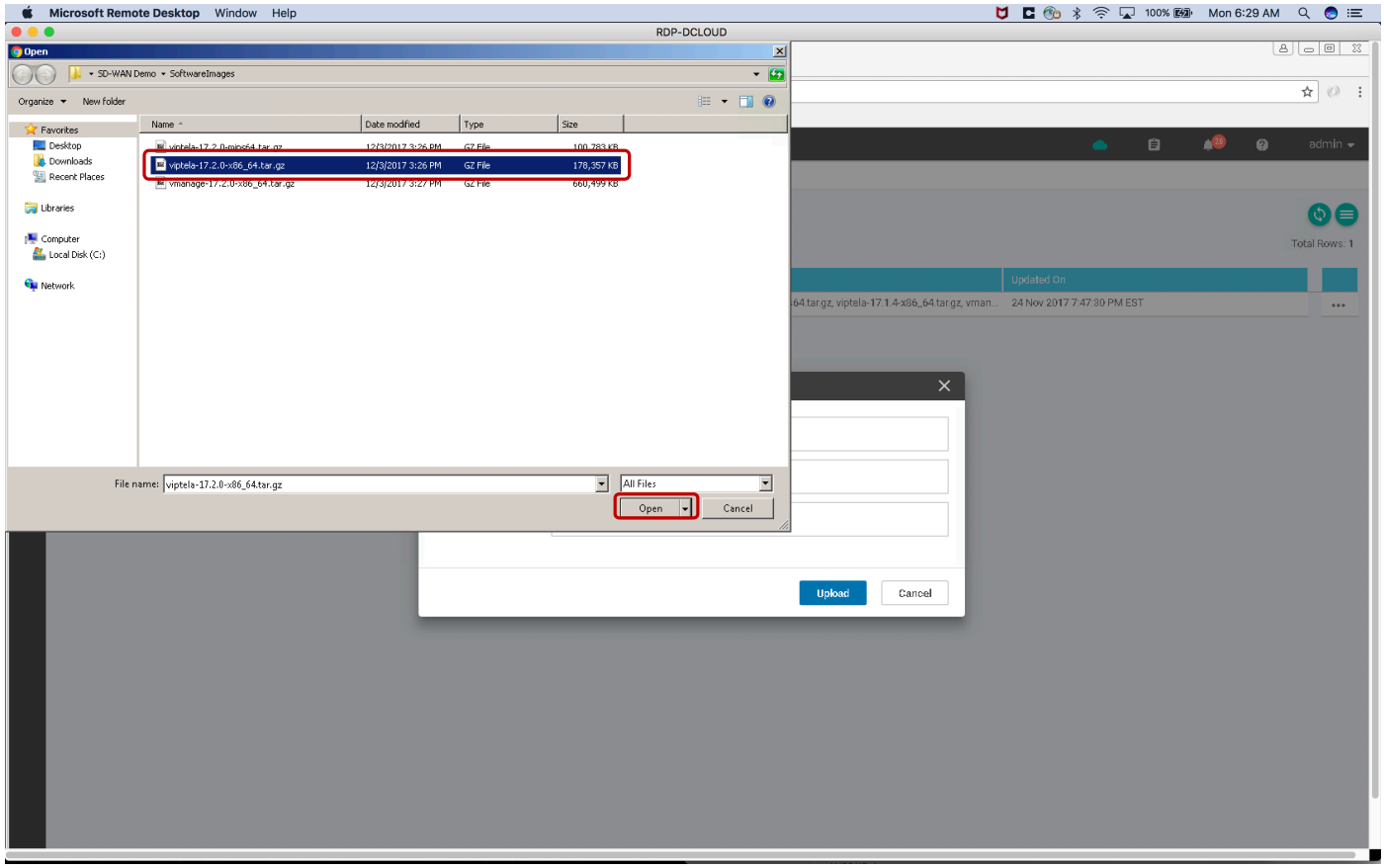
Click on choose file for vEdges, vSmart/vBond/vEdge Cloud and vManage.



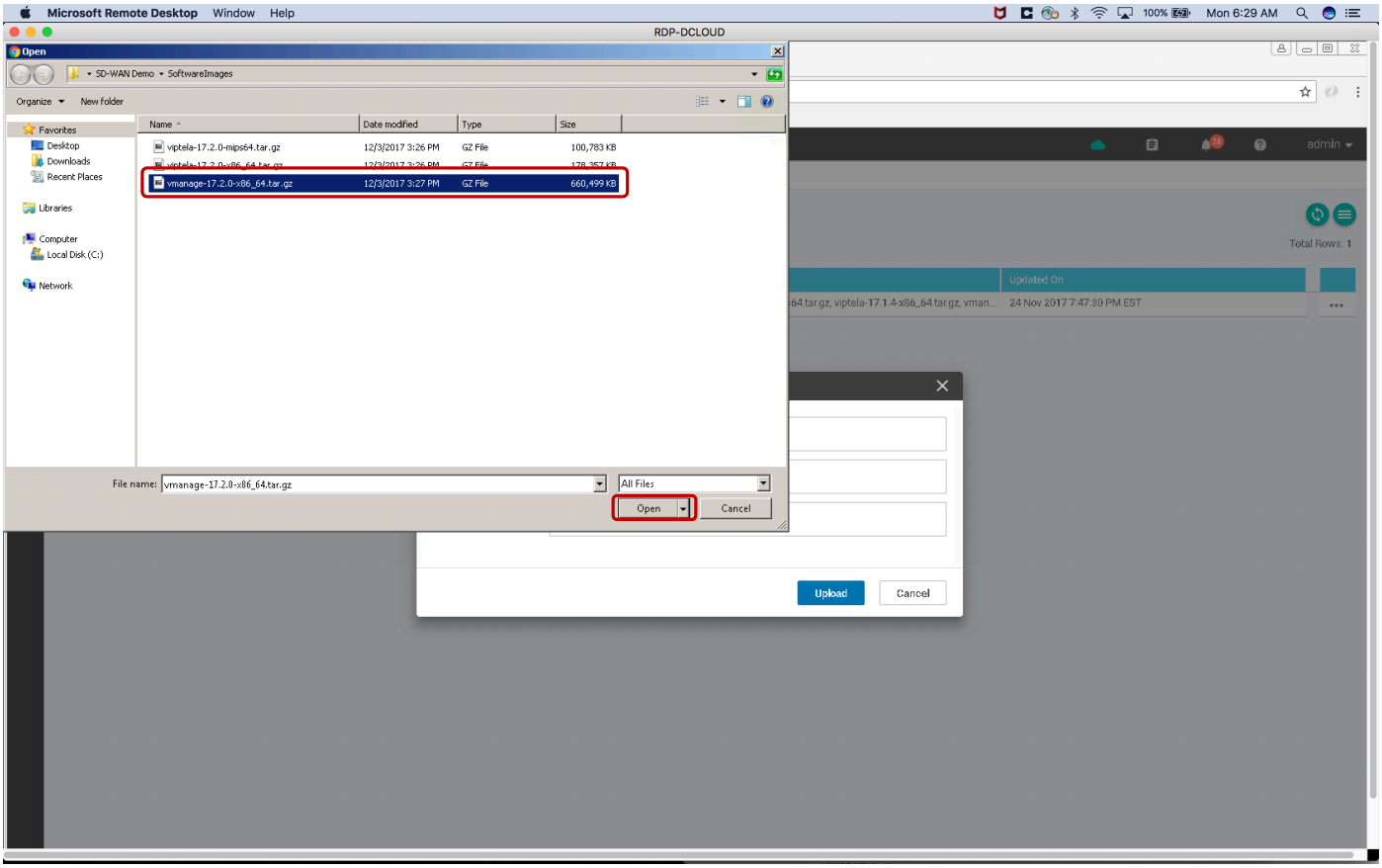
The software images are in the folder \Desktop\SD-WAN Demo\SoftwareImages.
Select the following files for each and click on “Open” tab.
For vEdge (select the mips file):



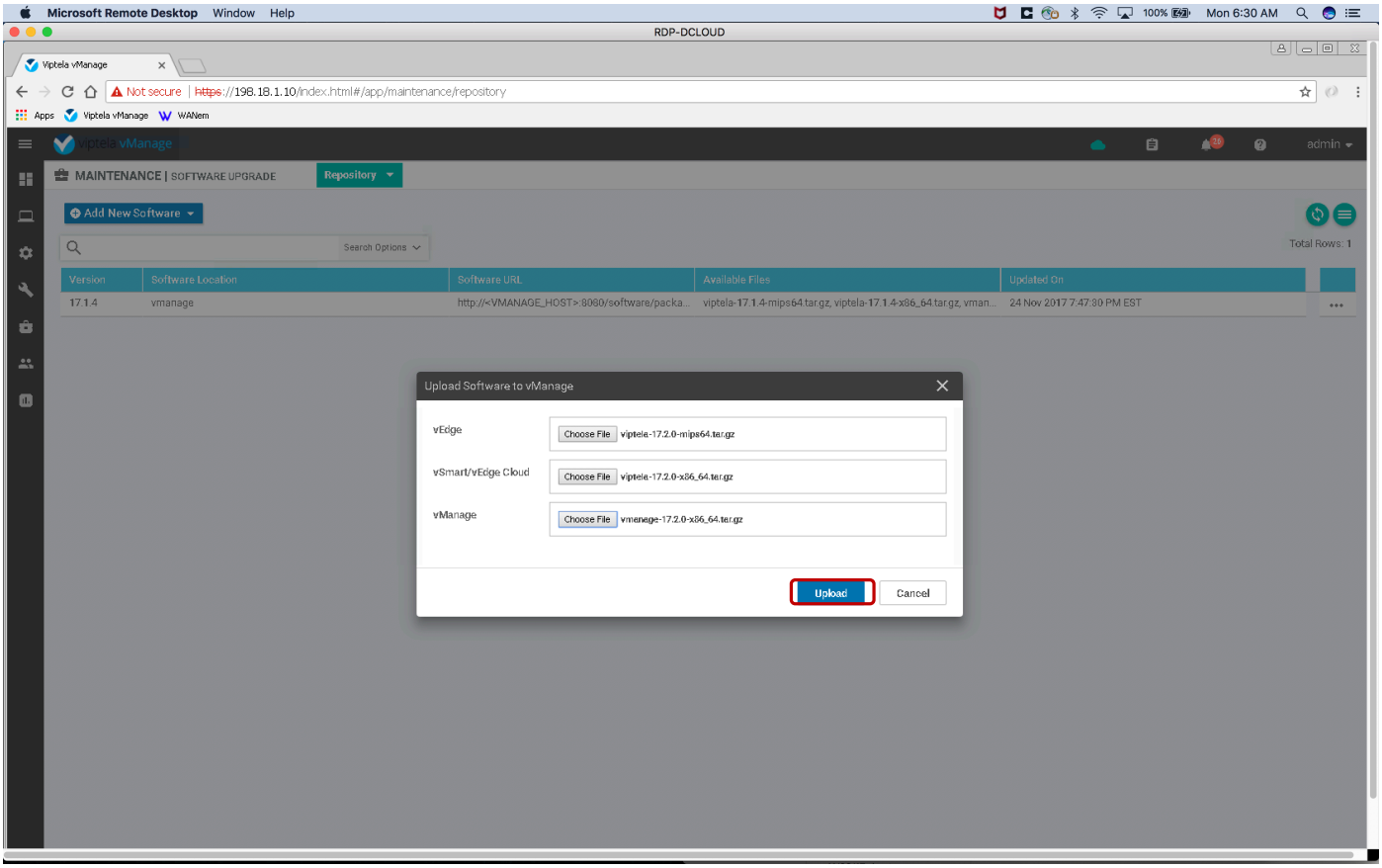
For vSmart/vEdge Cloud (Select the x86 file):



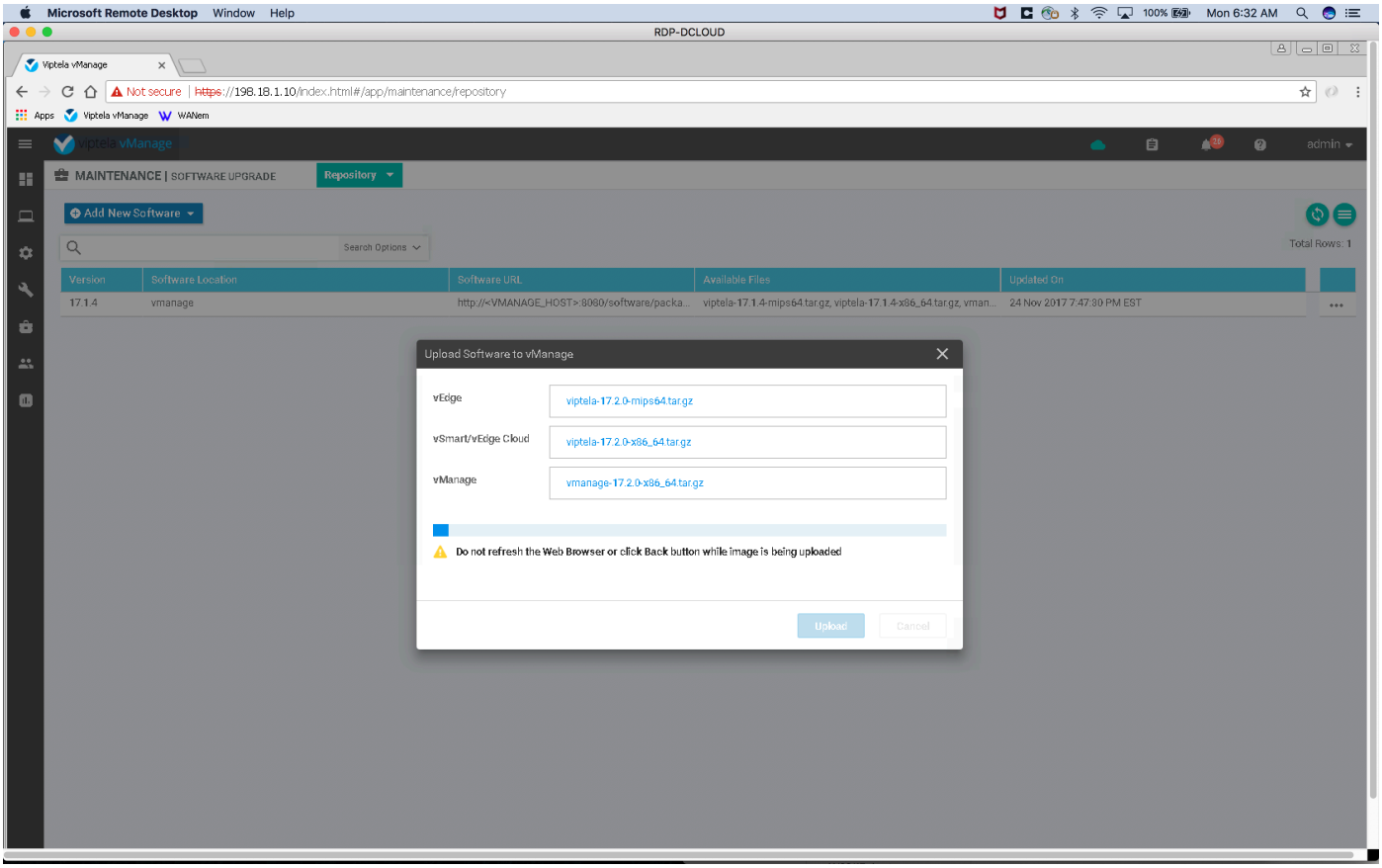
For vManage (select vmanage file):



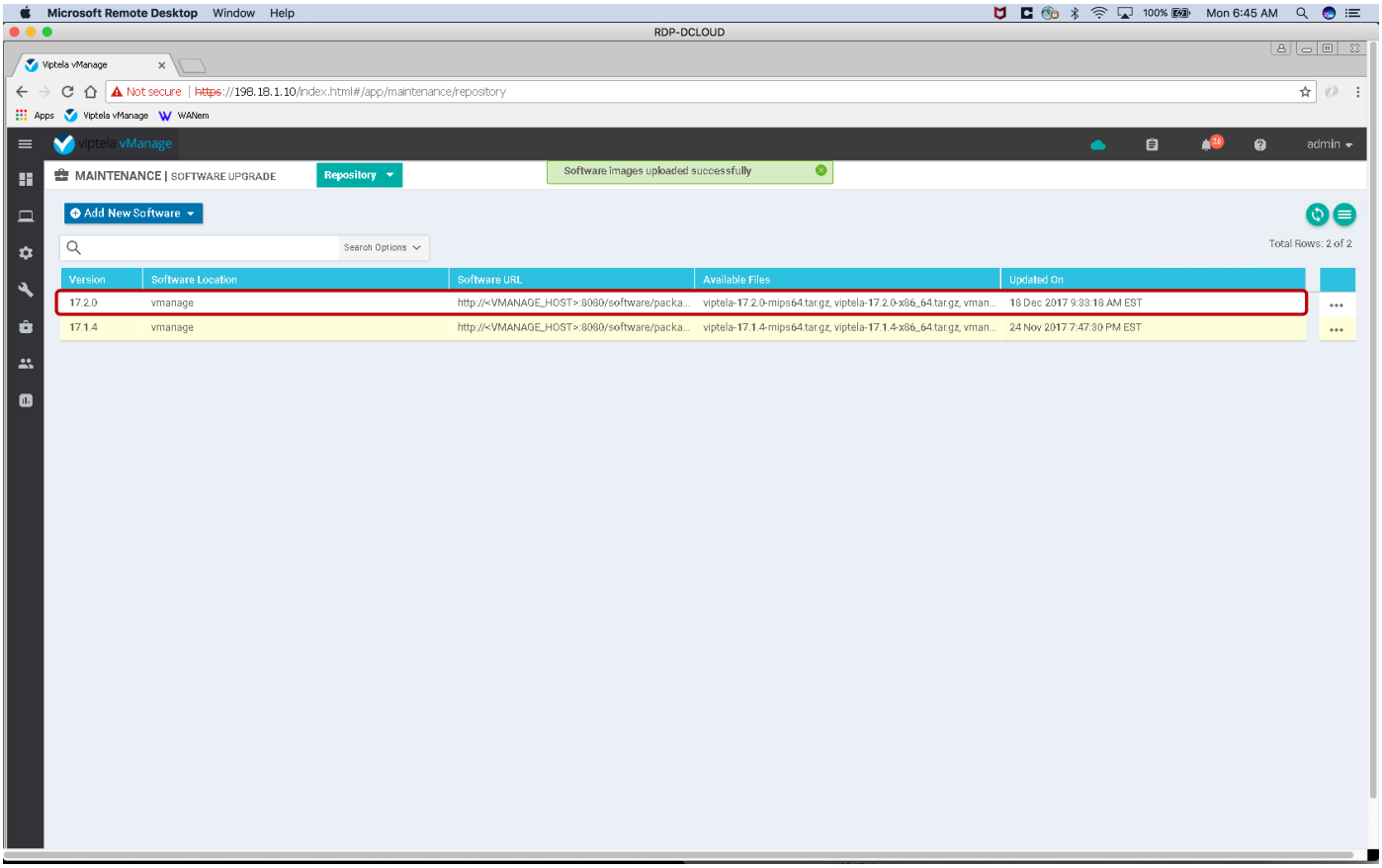
On the next screen, click on Update.



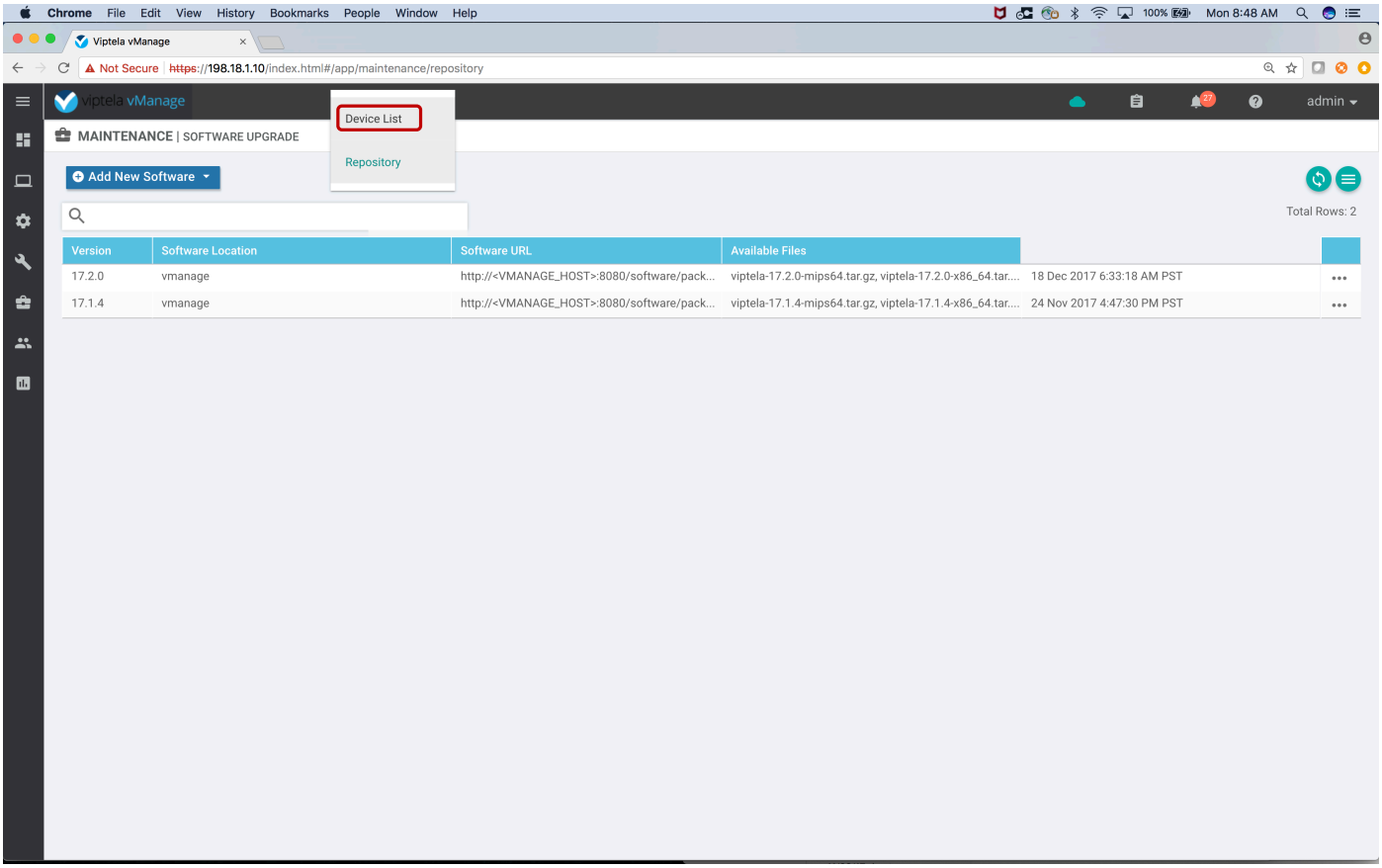
The upload will start and will take some time. Do not refresh the browser or try to go back.



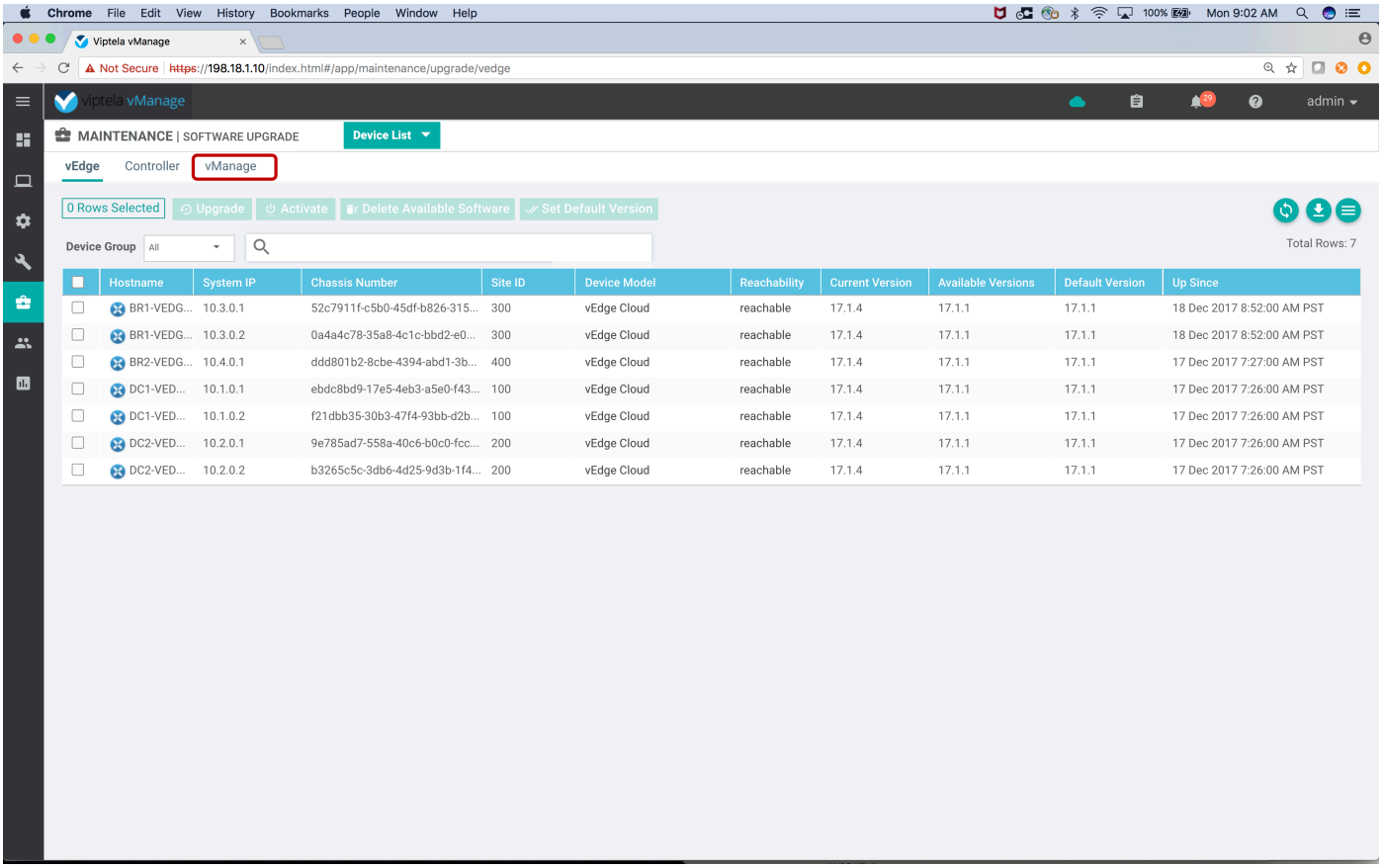
Once the upload completes, the 17.2.0 image will show up in the repository.



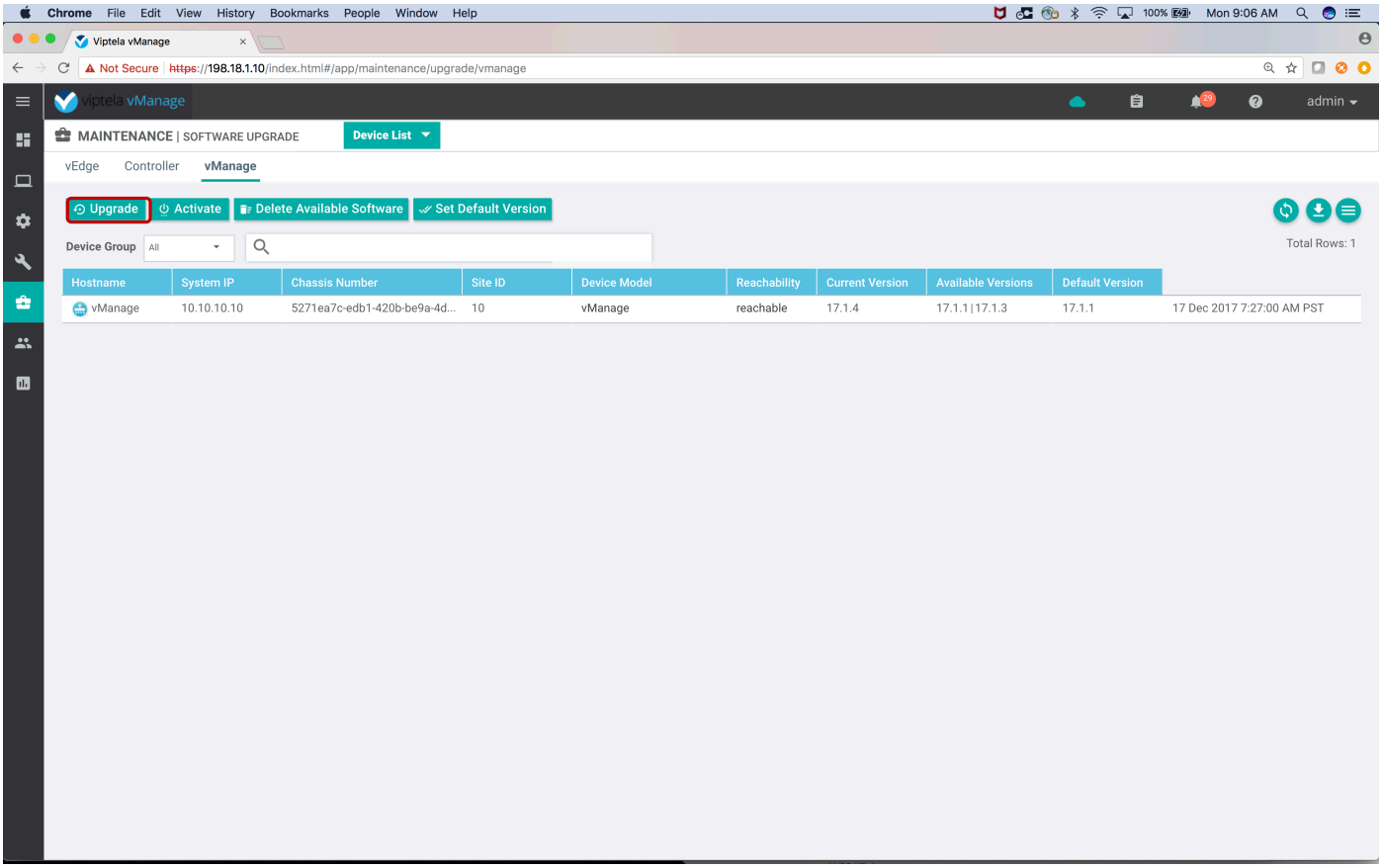
Click on “Device List” or go through “Maintenance” -> “Software Upgrade”.



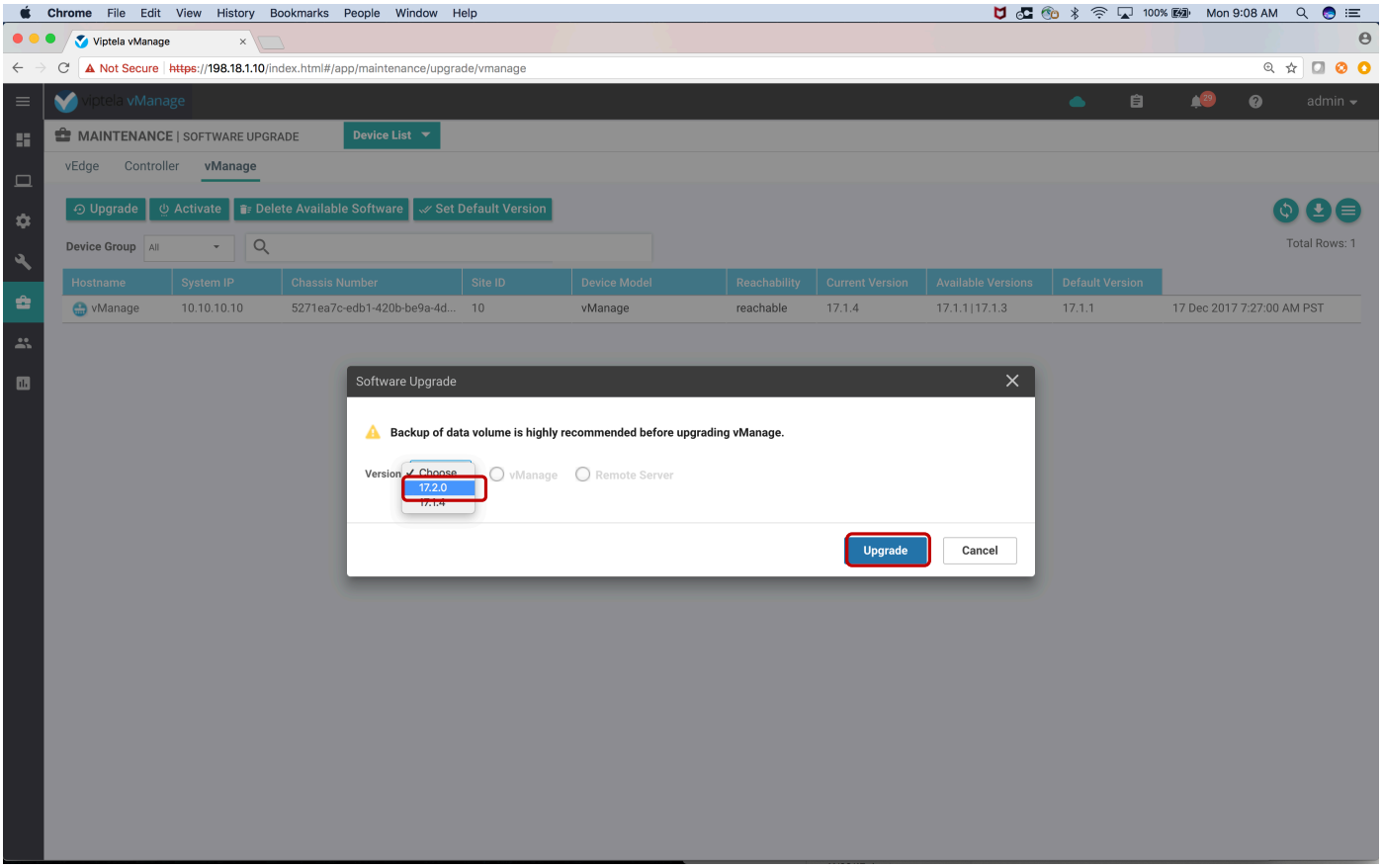
First, upgrade vManage.
Click on vManage tab.



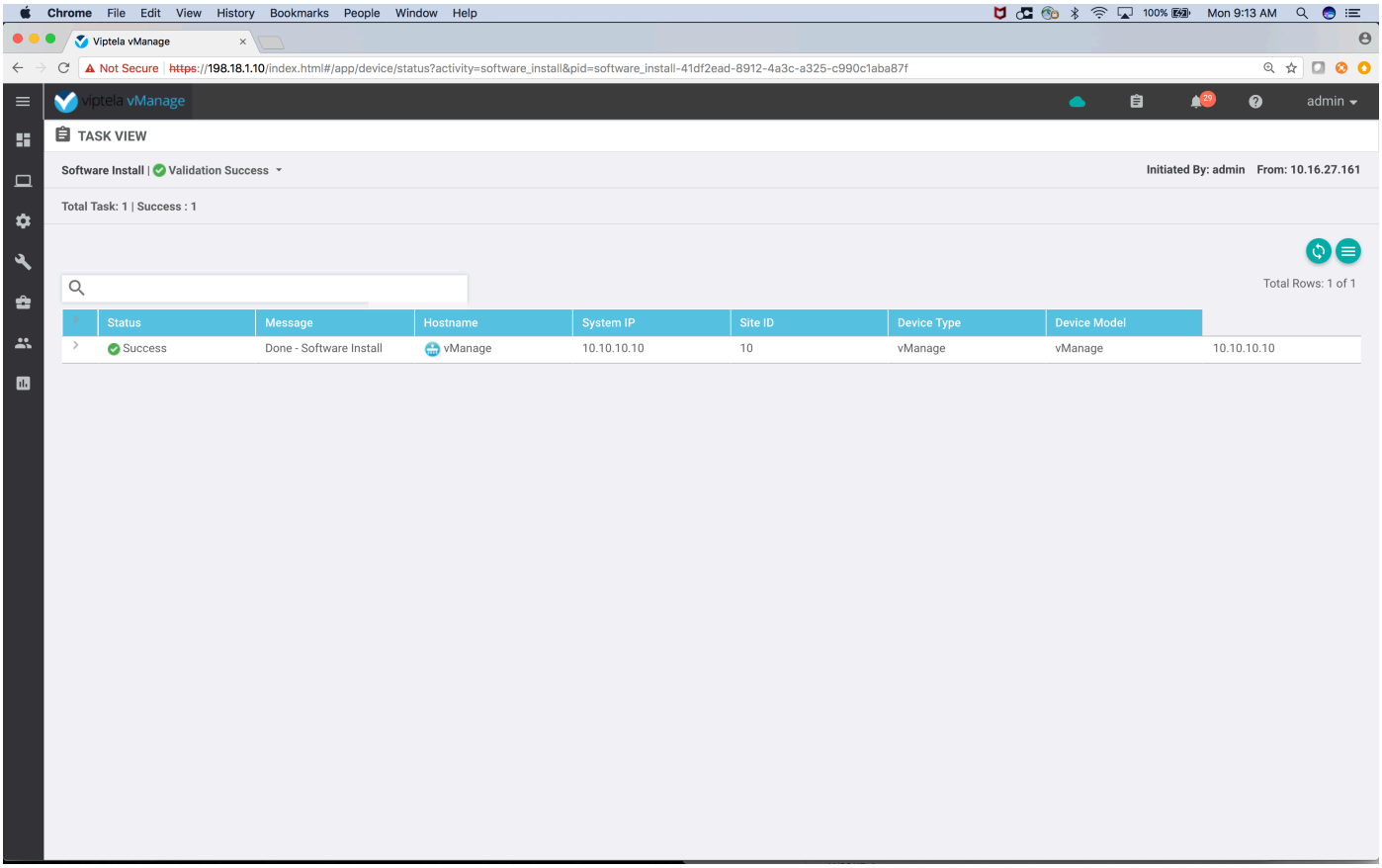
Click on the “Upgrade” button.



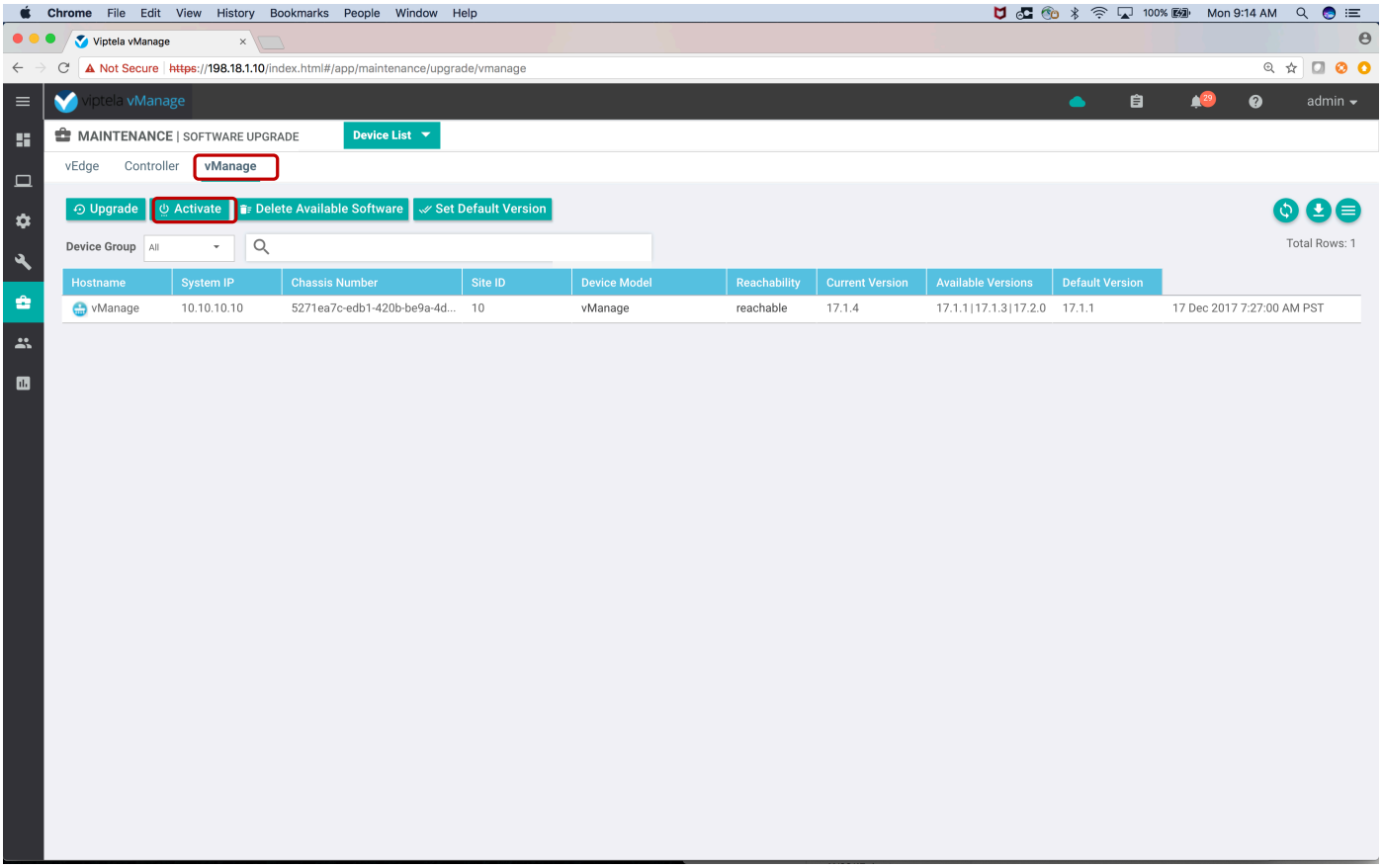
In the pop-up, click on version field and select 17.2.0. Then click on “Upgrade” button.



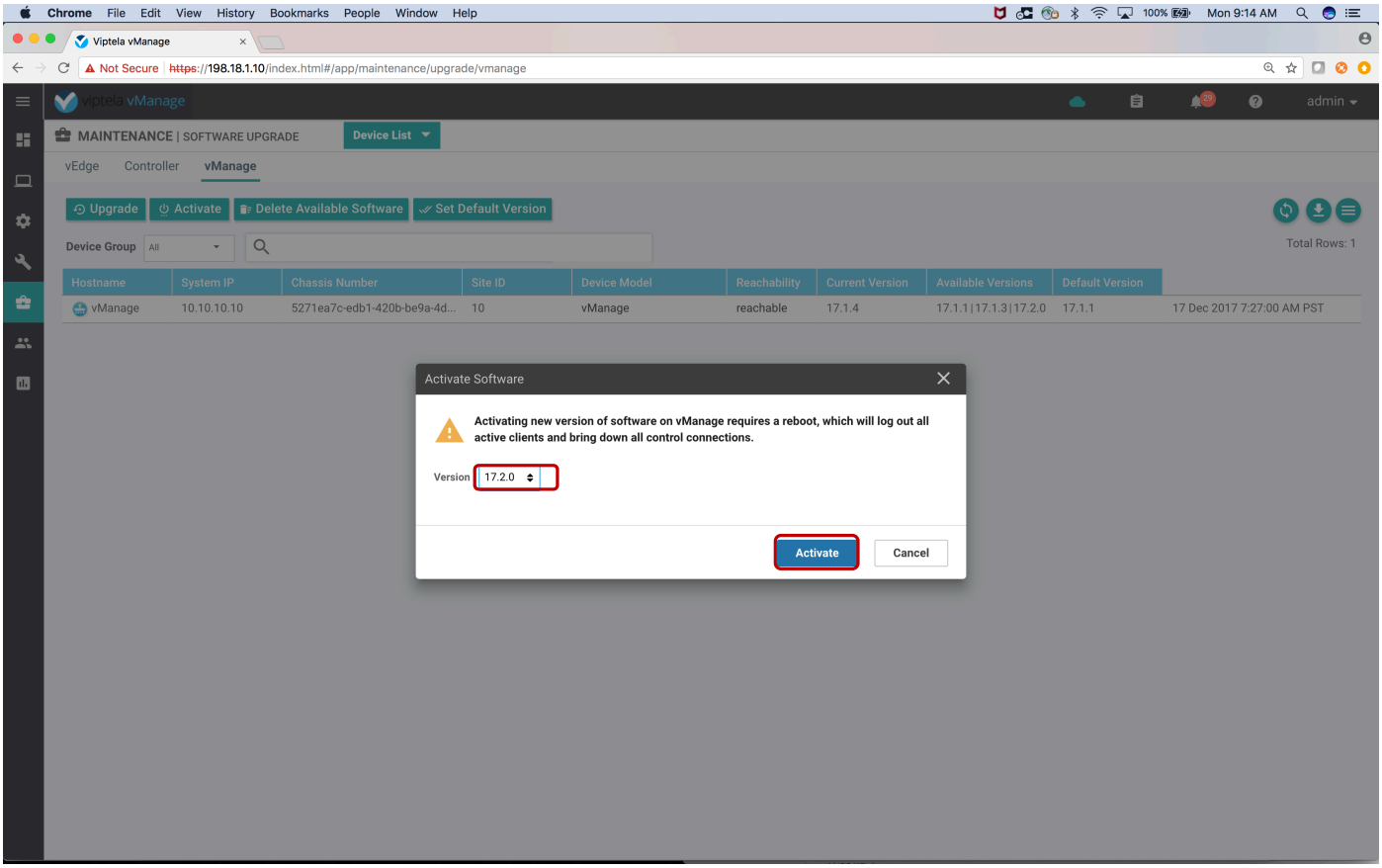
The vManage will install the new version. Wait till it is finished uploading the image.



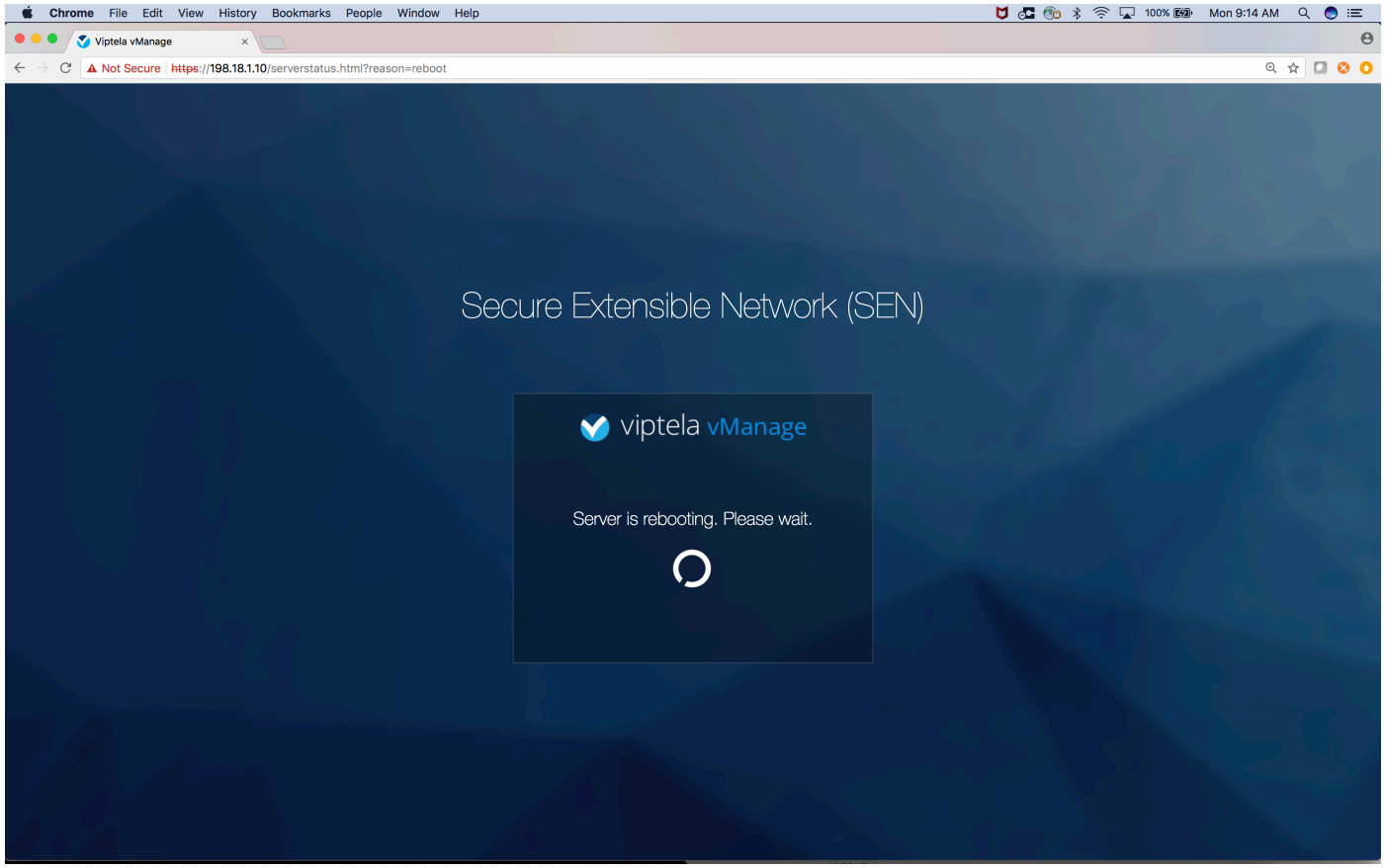
Go to software upgrade page and click on “vManage” tab. Then click on “Activate” button.



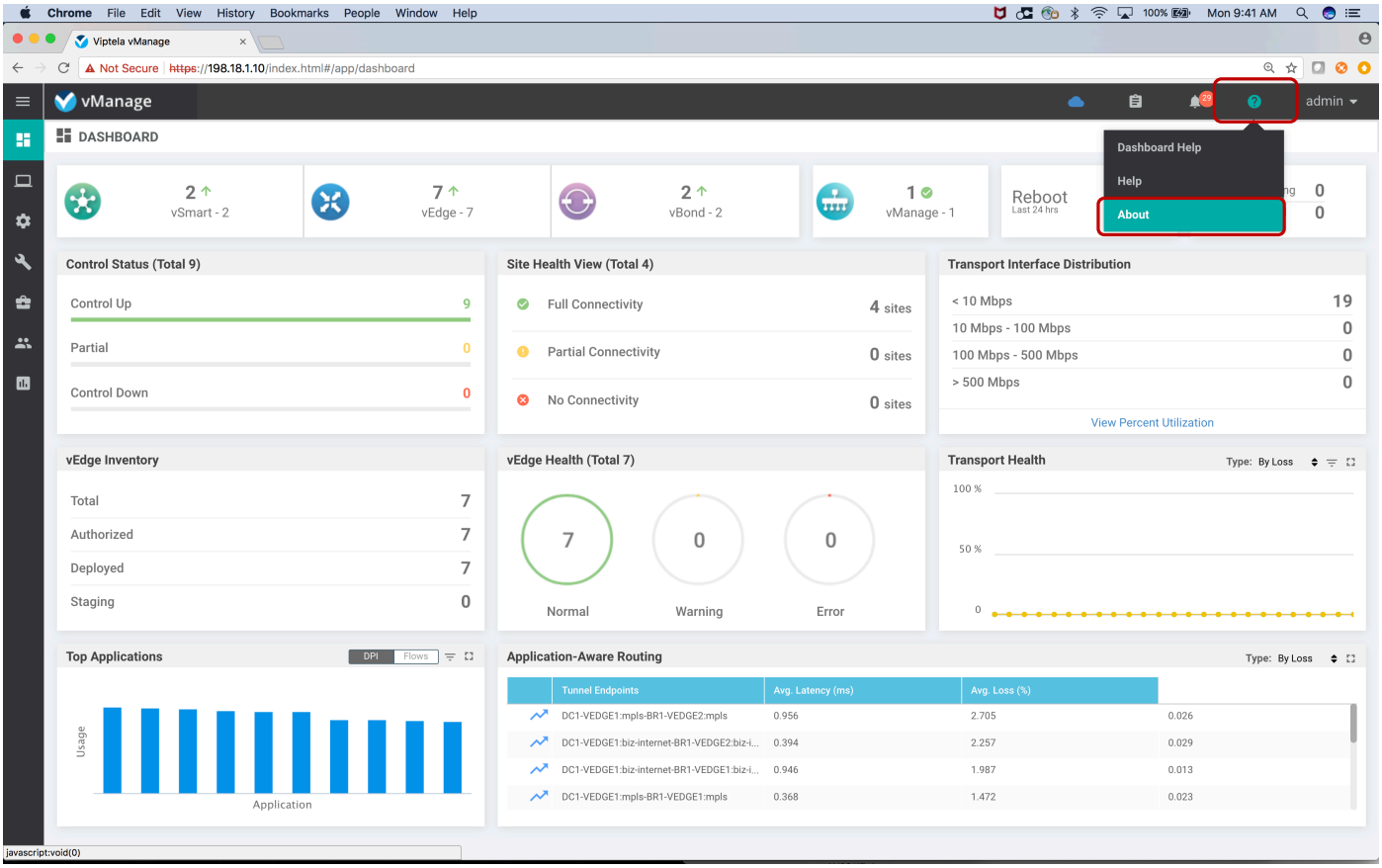
Click on the version field and select 17.2.0. Click on “Activate”.



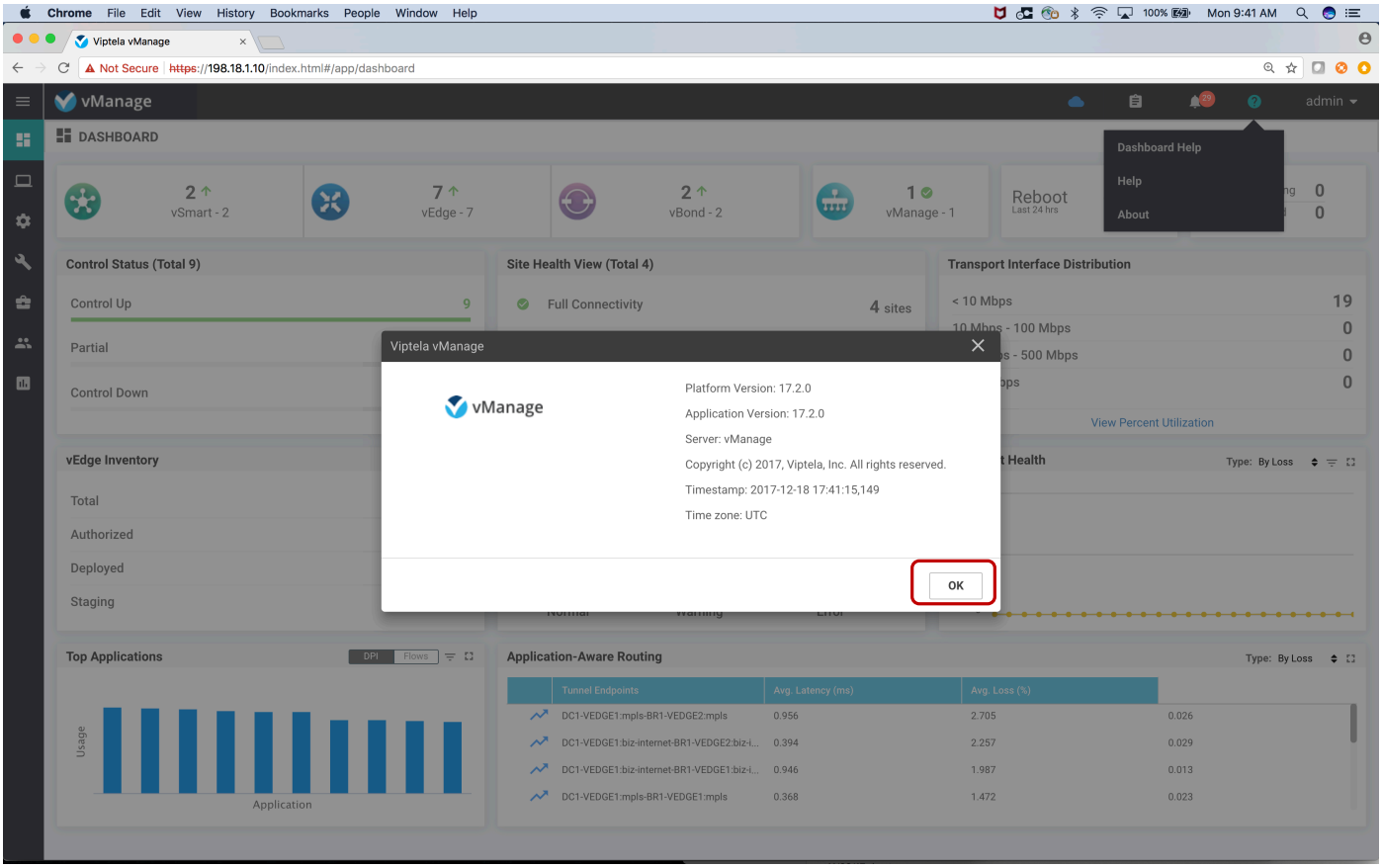
The vManage will reboot and you will lose the session to vManage.



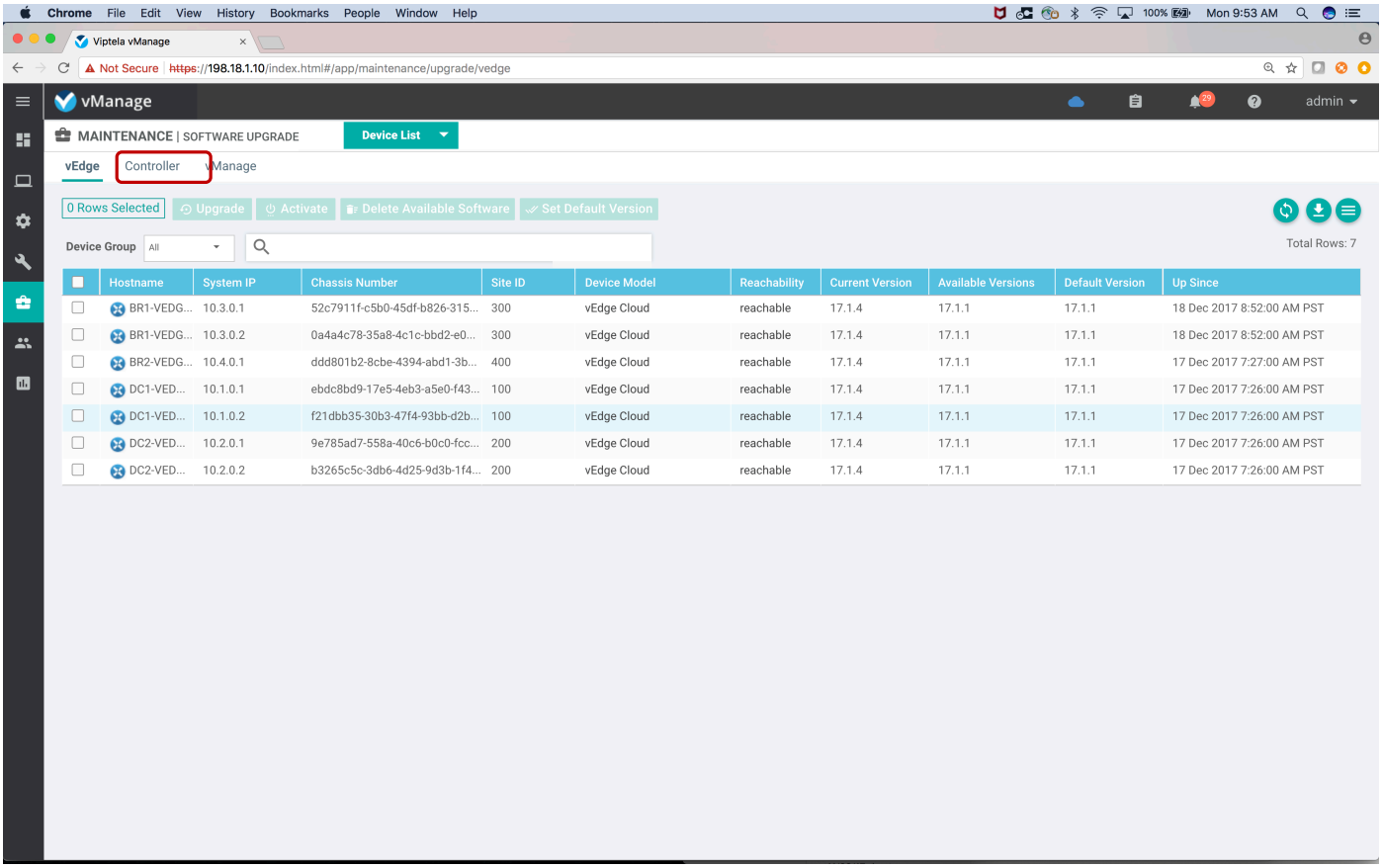
It will take few minutes to reboot. Once the vManage is back on-line, log back in again to vManage portal. To validate the current version on vManage, click on the icon with ? and then click on “About” in the pull down menu.



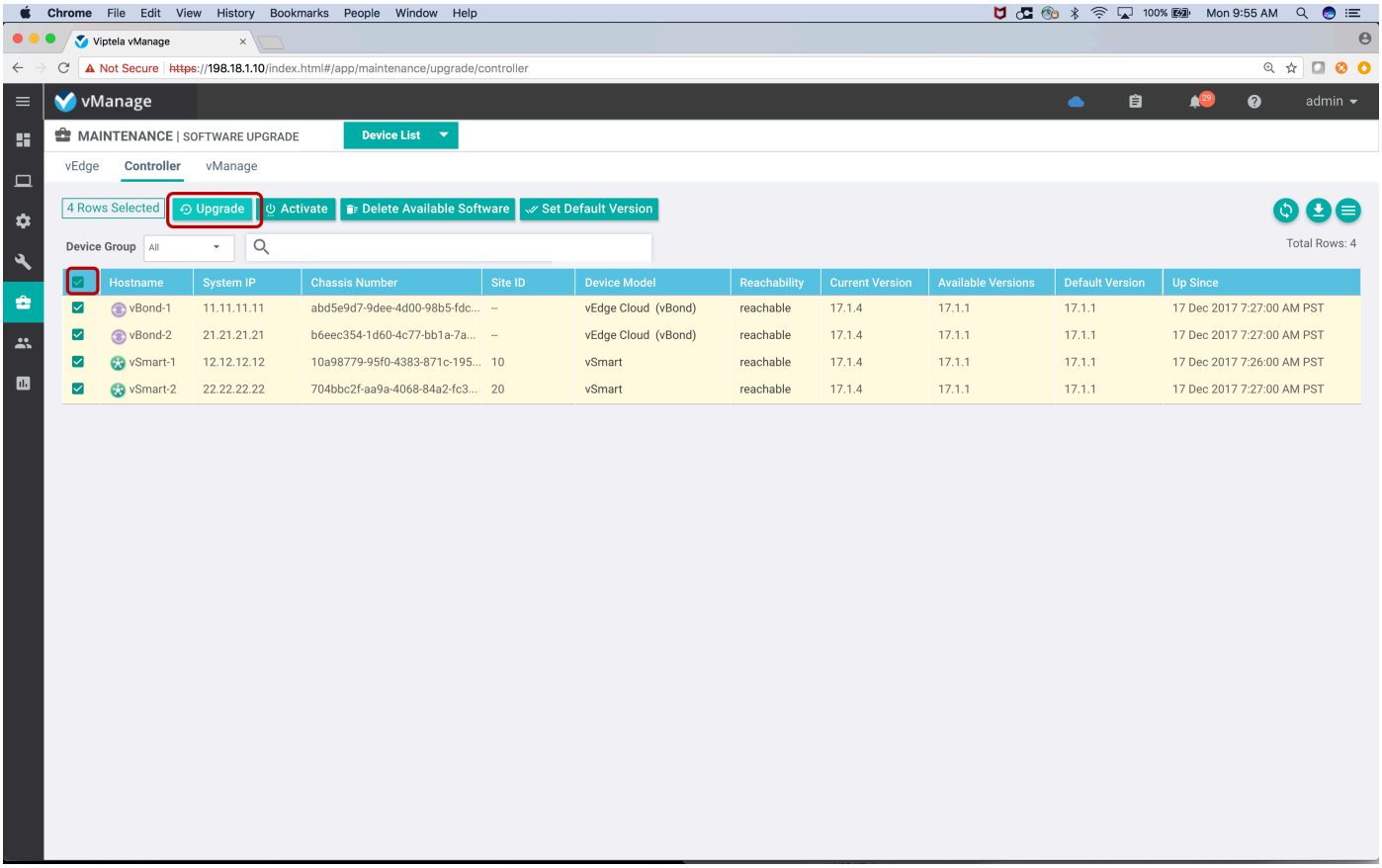
The pop-up should show the current version of vManage as 17.2.0. Click on “OK” button to close the pop-up.



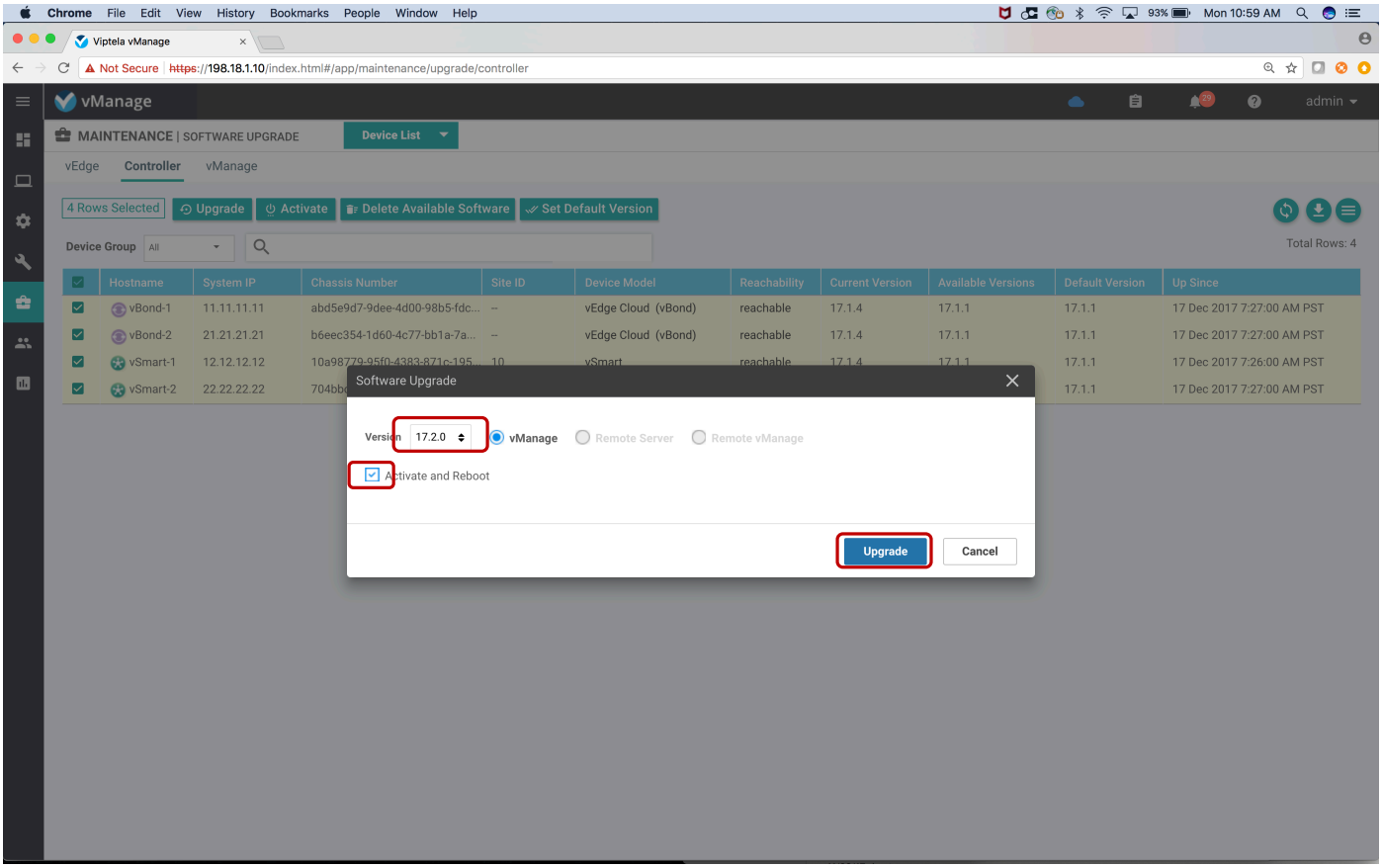
Go to Software Upgrade page and Click on “Controllers” to upgrade vBonds and vSmarts.



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”.

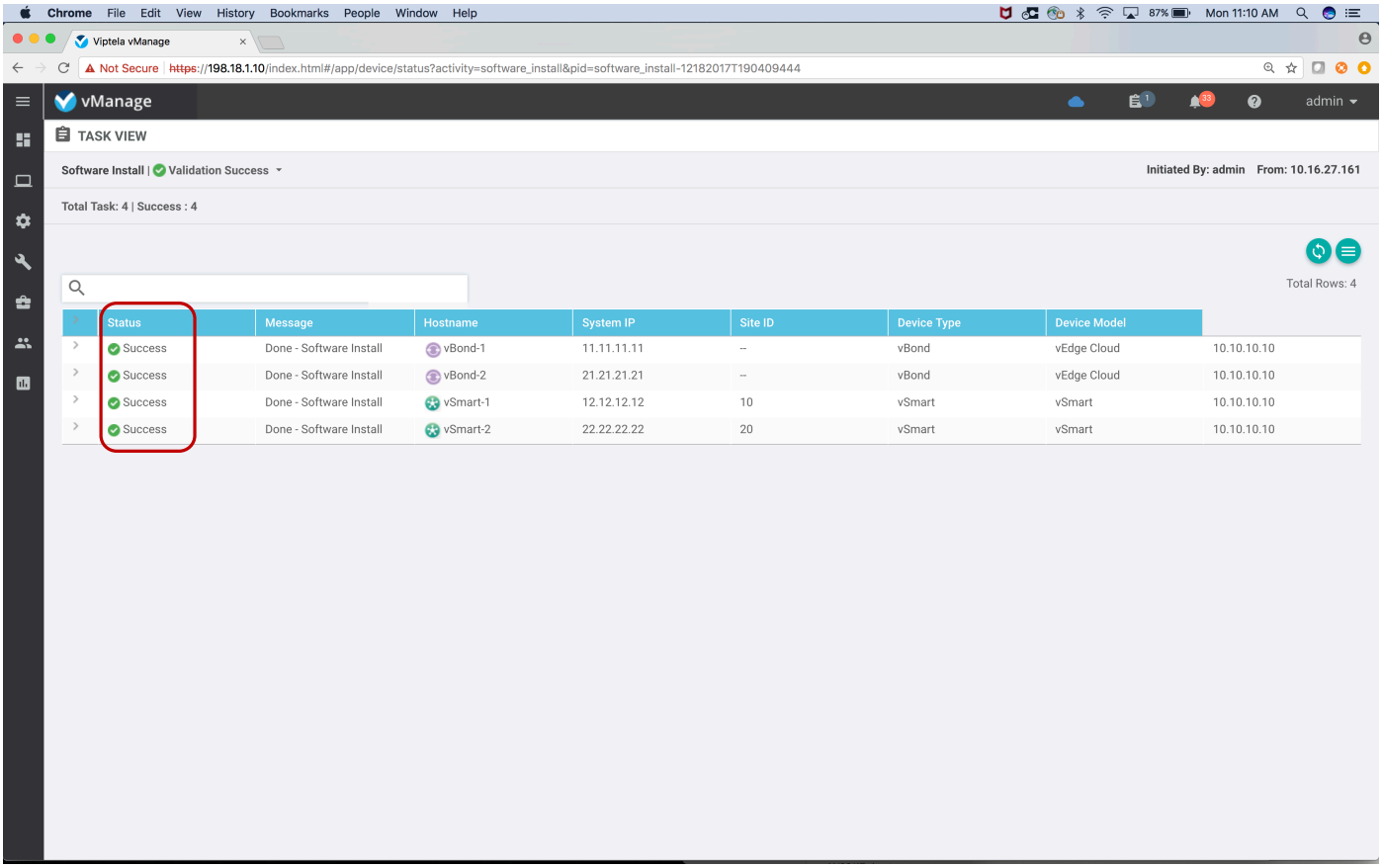


Select 17.2.0 from the version field. Check mark the “Activate and Reboot” option. Then click on “Upgrade” button.

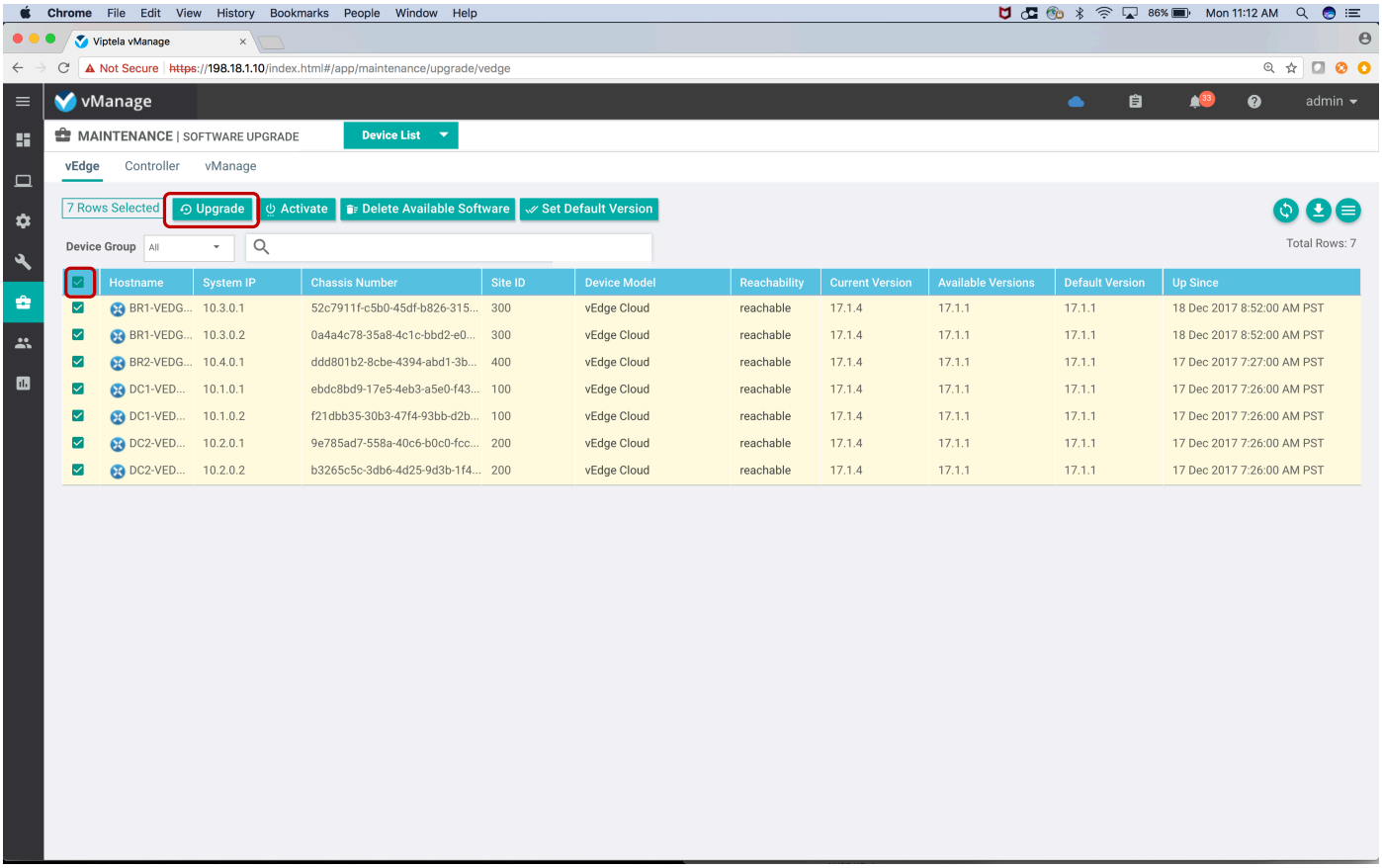


vManage will download the code and will activate the new version by rebooting the devices. This may take some time.

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

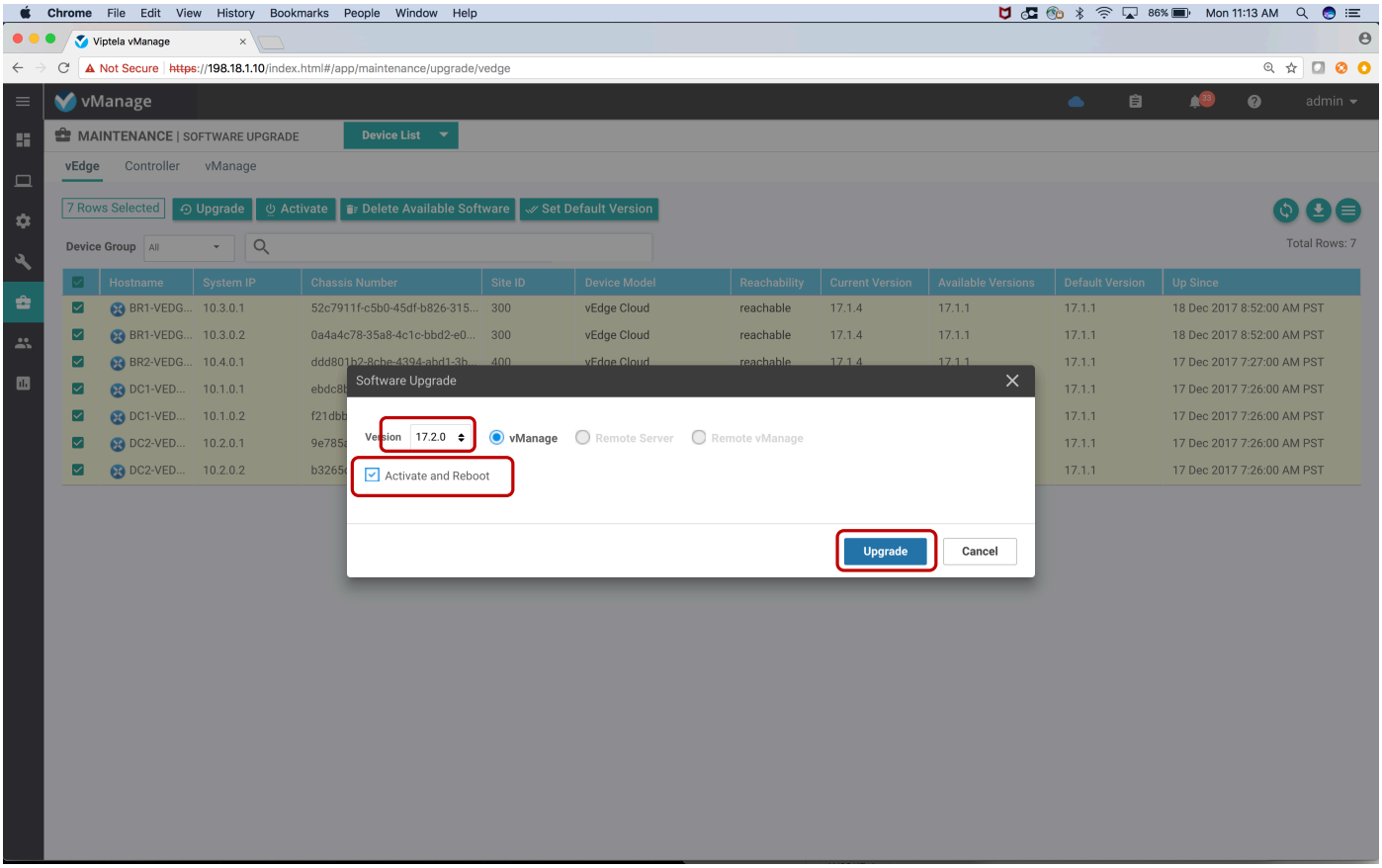


Now the vEdges are left for upgrade. Go to the Software Upgrade page and select ALL the vEdges. Individual or a sub-group of vEdges can be upgraded at a given time. Click on “Upgrade” button.



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]



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.**