VMware SD-WAN: Deploy and Manage

Lab Manual

VMware® Education Services
VMware, Inc.
www.vmware.com/education

VMware SD-WAN: Deploy and Manage

Lab Manual

VMware SD-WAN™

Part Number EDU-EN-SDWANDM4-LAB (01-APR-2022)

Typographical Conventions

The following typographical conventions are used in this course.

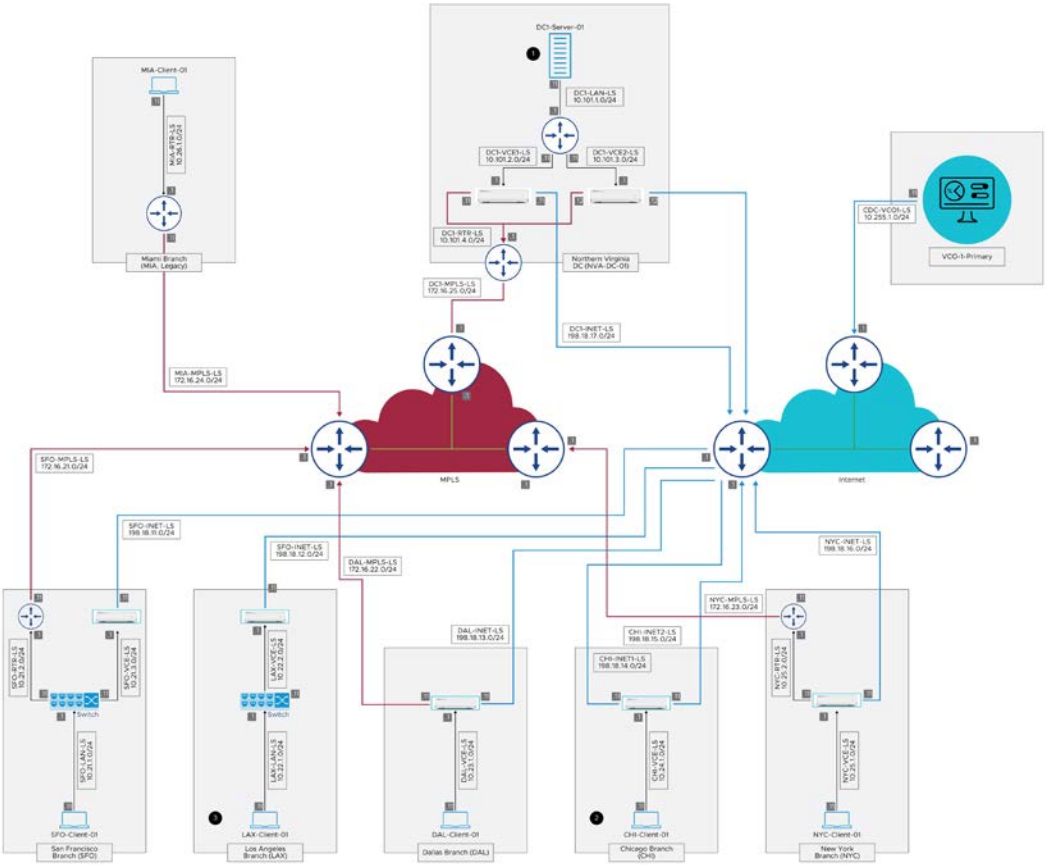
Conventions	Usage and Examples
`Monospace`	Identifies command names, command options, parameters, code fragments, error messages, filenames, folder names, directory names, and path names: • Run the `esxtop` command. • … found in the `/var/log/messages` file.
`Monospace Bold`	Identifies user inputs: • Enter **`ipconfig /release`**.
Boldface	Identifies user interface controls: • Click the **Configuration** tab.
Italic	Identifies book titles: • *vSphere Virtual Machine Administration*
< >	Indicates placeholder variables: • <ESXi_host_name> • … the `Settings/<Your_Name>.txt` file

Contents

Lab 1 Understanding the Lab Environment

Reviewing the Lab Topology

This section helps you understand the lab topology before you begin. A thorough understanding of the lab design allows you to understand the objectives of each lab.



For most of the VMware SD-WAN configuration, you must log in to VMware SD-WAN Orchestrator. The VMware SD-WAN Orchestrator VM name is VCO-1-Primary.

Data Center Site

You configure the data center site as a hub. You check VPN connectivity between various remote sites and the data center.

VMware SD-WAN Edge at the Chicago Site

You deploy a new VMware SD-WAN Edge instance called CHI-VCE-01. It is a virtual edge in the form of a VM that is already installed and configured. You activate the edge using zero-touch provisioning and provide access to the local client machines at the Chicago site.

NOTE

The purpose of this lab is to provide an overview of the lab topology. This lab does not have any tasks.

Lab 2 Exploring VMware SD-WAN Orchestrator

Objective and Tasks

Configure new accounts in VMware SD-WAN Orchestrator:

1. Access VMware SD-WAN Orchestrator
2. Create and Configure a Read-Only Account
3. Create and Configure a Read-Write Account
4. Create and Configure a Customer Support Account
5. Validate the Newly Created Accounts

Task 1: Access VMware SD-WAN Orchestrator

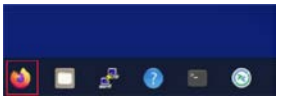
You access VMware SD-WAN Orchestrator to create new user accounts.

IMPORTANT

Use this login procedure as needed for the remainder of the lab exercises.

---

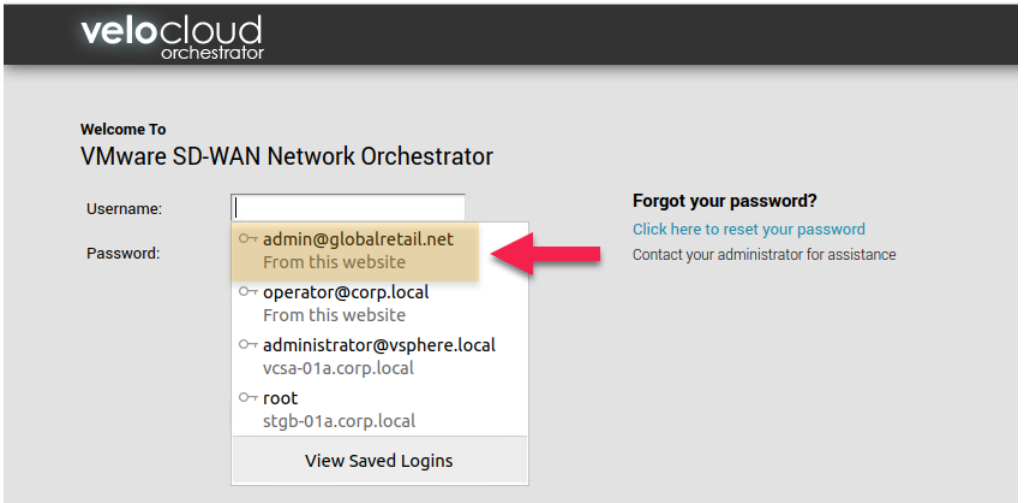
1. From the taskbar, open Firefox.



The VMware SD-WAN Orchestrator login portal appears.

2. Select **admin@globalretail.net** in the **Username** box.

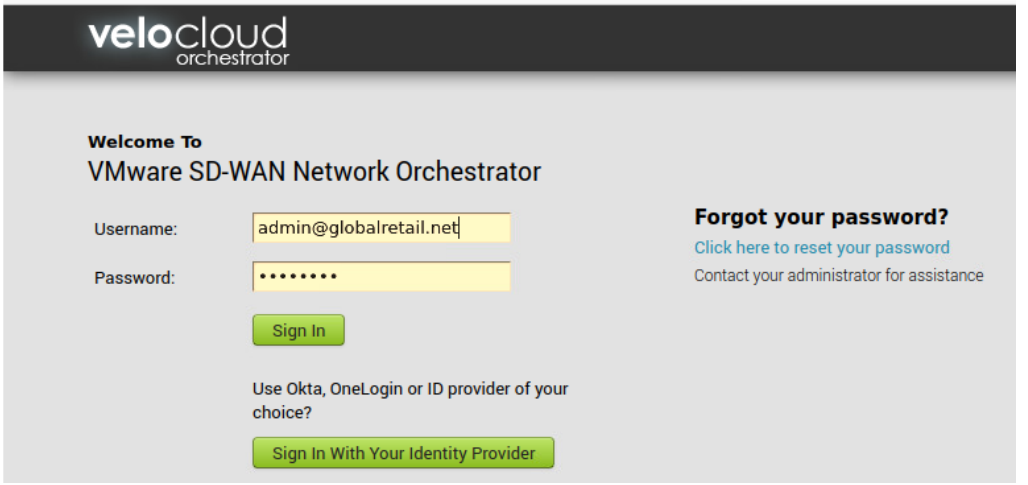
The password populates automatically.



3. Click **Sign In** to launch the orchestrator.

NOTE

Enter **`VMware1!`** in the **Password** text box if it does not populate automatically.



Task 2: Create and Configure a Read-Only Account

You create a read-only orchestrator account to provide access to a user who has no configuration or troubleshooting privileges.

1. Select **Administration** > **Administrators** in the navigation pane on the left.
2. On the Administrators page, select **New Admin.**

   The New Admin dialog box appears.
3. Enter **`admin-ro@globalretail.net`** in the **Username** text box.
4. Enter **`admin-ro`** in the **First Name** text box.
5. Enter **`VMware1!`** in the **Password** and **Confirm** text boxes.

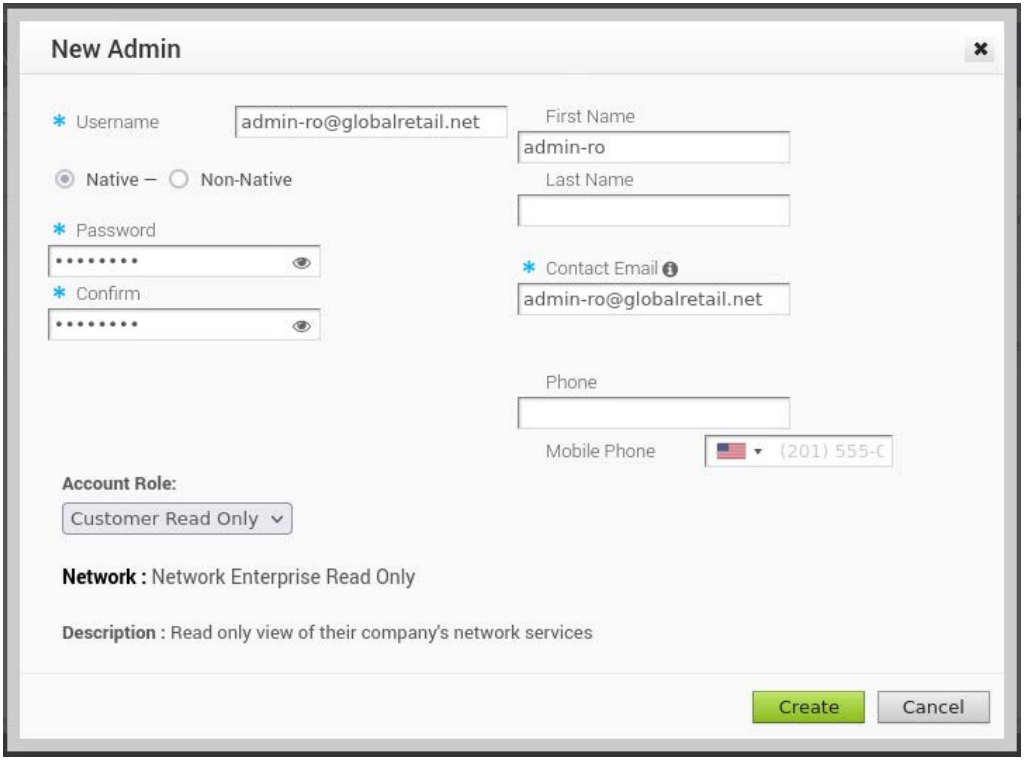
NOTE

The password is case-sensitive.

6. In the **Account Role** drop-down menu, select **Customer Read Only**.

   With this role, the user has a read-only view of the company's network services.

7. Click **Create**.



8. Click **Save Changes**.

Task 3: Create and Configure a Read-Write Account

You create a read-write orchestrator account to provide access to a user who has privileges to monitor and configure objects.

1. Select **Administration** > **Administrators** in the navigation pane on the left.
2. On the Administrators page, select **New Admin.**

   The New Admin dialog box appears.
3. Enter **`admin-rw@globalretail.net`** in the **Username** text box.
4. Enter **`admin-rw`** in the **First Name** text box.
5. Enter **`VMware1!`** in the **Password** and **Confirm** text boxes.
6. In the **Account Role** drop-down menu, select **Standard Admin**.

   With this role, the user can view and manage users and access the global settings across all services.
7. Click **Create**.
8. Click **Save Changes**.

Task 4: Create and Configure a Customer Support Account

You create a customer support orchestrator account to provide access to a user who can view but not manage objects.

1. Select **Administration** > **Administrators** in the navigation pane on the left.
2. On the Administrators page, select **New Admin.**

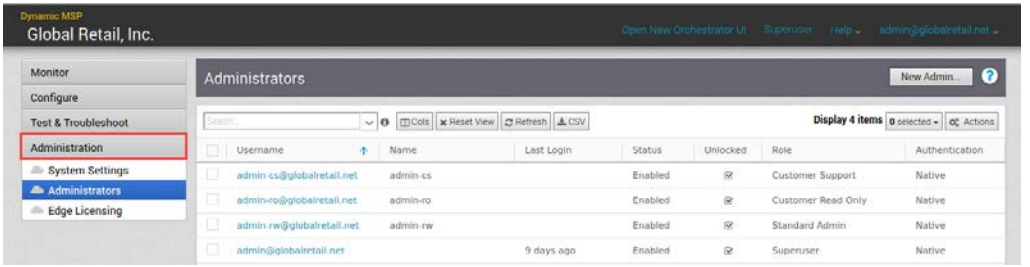
   The New Admin dialog box appears.
3. Enter **`admin-cs@globalretail.net`** in the **Username** text box.
4. Enter **`admin-cs`** in the **First Name** text box.
5. Enter **`VMware1!`** in the **Password** and **Confirm** text boxes.
6. In the **Account Role** drop-down menu, select **Customer Support**.

   With this role, the user can monitor edges and activity in the network as well as initiate diagnostic actions across the company's network.
7. Click **Create**.
8. Click **Save Changes**.

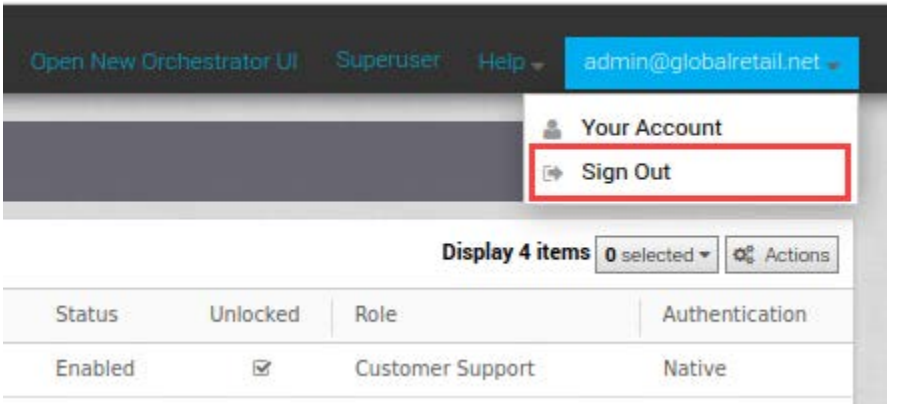
Task 5: Validate the Newly Created Accounts

You validate the newly created orchestrator accounts to ensure that they have been configured correctly.

1. Select **Administration** > **Administrators** in the navigation pane on the left.
2. Verify that the settings are correct for each of the new accounts.



3. Log out of the orchestrator, and then log in as one of the newly created roles to validate its credentials.



4. Repeat this step for each of the new accounts.
5. Log out of the orchestrator.

Lab 3 Zero-Touch Provisioning

Objective and Tasks

Configure the VMware SD-WAN Edge appliance:

1. Provision a New Branch
2. Activate a New Branch
3. Configure the LAN Interface of an Edge Appliance
4. Verify Network Connectivity

Task 1: Provision a New Branch

You provision a new branch with VMware SD-WAN Orchestrator.

1. Log in to VMware SD-WAN Orchestrator.

   Disregard this step if you are already logged in.

2. Select **Configure** > **Edges** in the navigation pane on the left.

3. On the Edges page, select **New Edge**.

   The Provision New Edge configuration page appears.

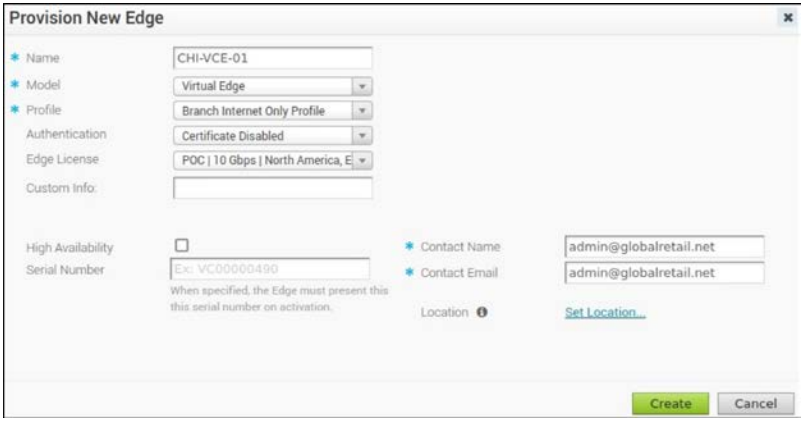
4. Enter **`CHI-VCE-01`** in the **Name** text box.

5. In the **Model** drop-down menu, select **Virtual Edge**.

6. In the **Profile** drop-down menu, select **Branch Internet Only Profile**.

7. In the **Authentication** drop-down menu, select **Certificate Disabled**.

8. In the **Edge License** drop-down menu, select **POC | 10 Gbps | North America**.

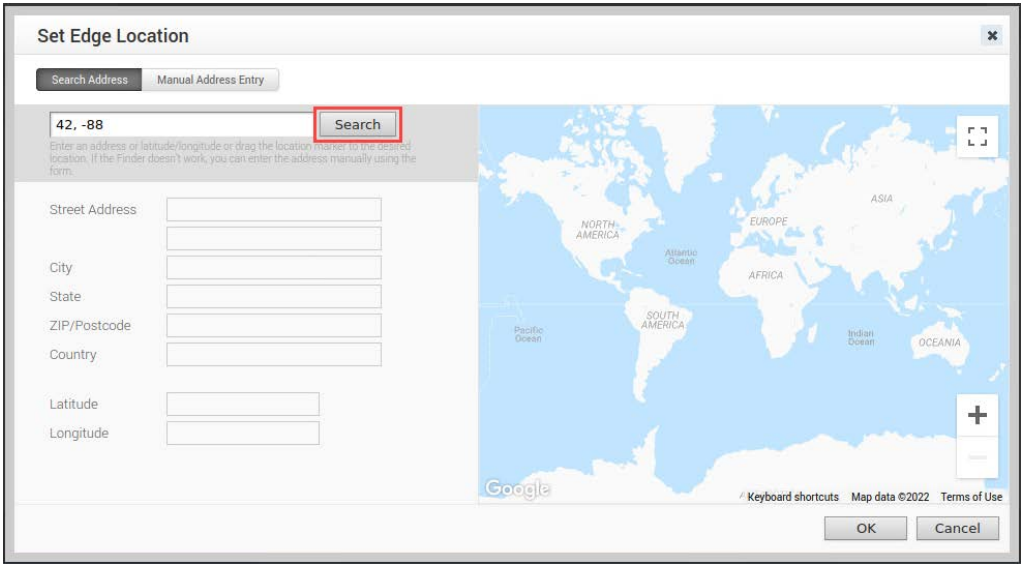


9. Next to Location, click **Set Location**.

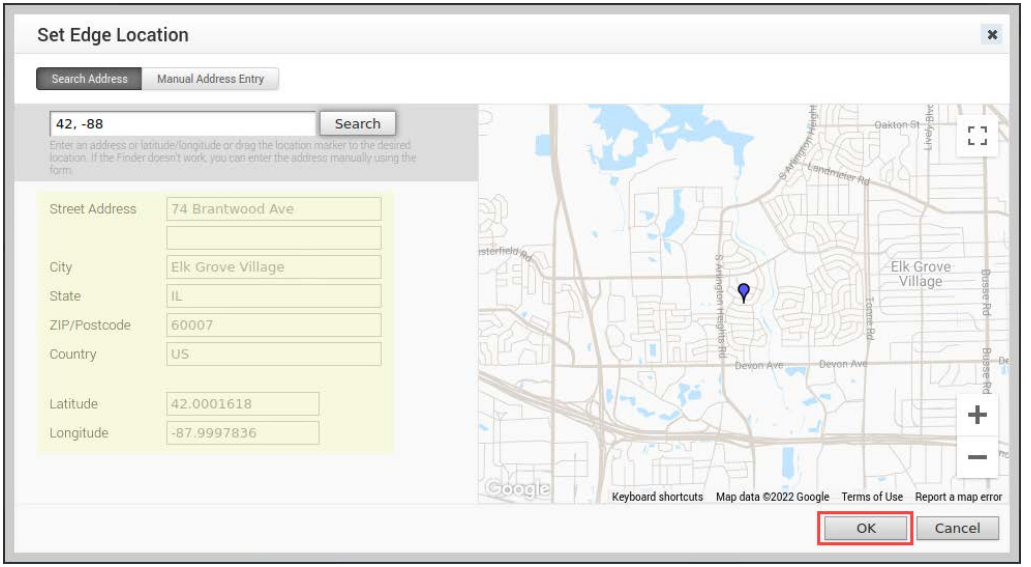
   The Set Edge Location page appears.

10. Enter **`42, -88`** in the **Search** box.

11. Click **Search**.



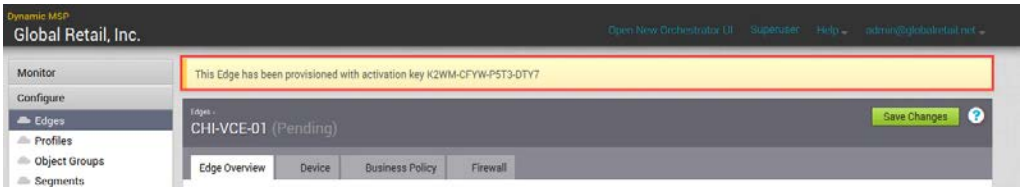
The edge location fields are populated automatically.



12. Click **OK**.

13. Scroll down and click **Create**.

    The `This Edge has been provisioned` message appears.



NOTE

It is not necessary to click **Save Changes**.

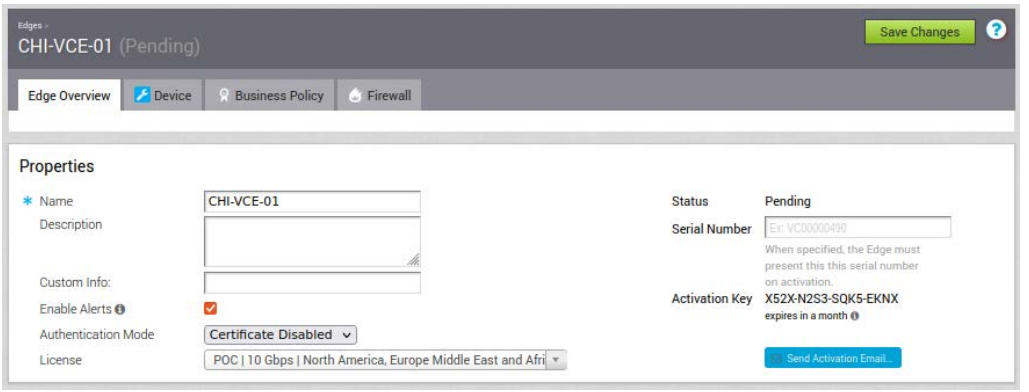
Task 2: Activate a New Branch

You initiate a download of the edge configuration to activate the new hardware appliance.

NOTE

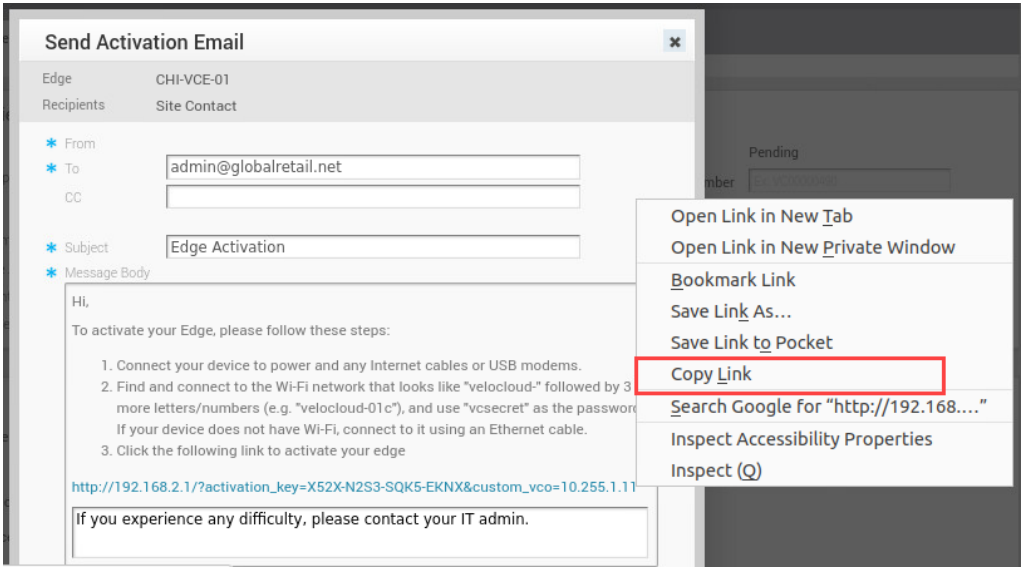
Because you do not have access to an email system in the lab environment, this lab simulates the email activation process.

1. Under Properties, click **Send Activation Email**.



   The Send Activation Email window appears.

2. Right-click the activation URL and select **Copy Link**.



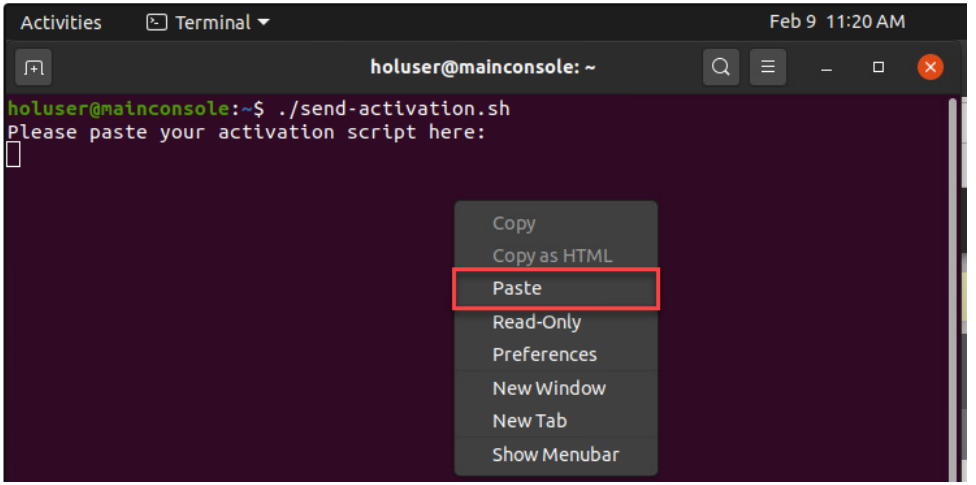
3. Close the Send Activation Email window.

4. Send the activation URL to the CHI-CLIENT-01 desktop.

   a. From the taskbar, open a Terminal window.

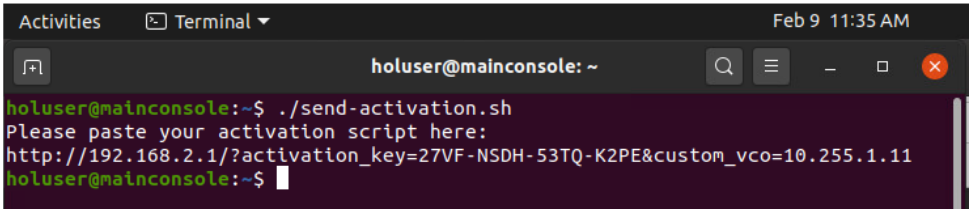
   b. Run the `./send-activation.sh` script.

   c. Right-click in the Terminal window and select **Paste** to enter the URL from the activation email.

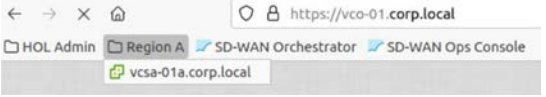


   d. Press Enter.

   The command prompt reappears when the action is complete.

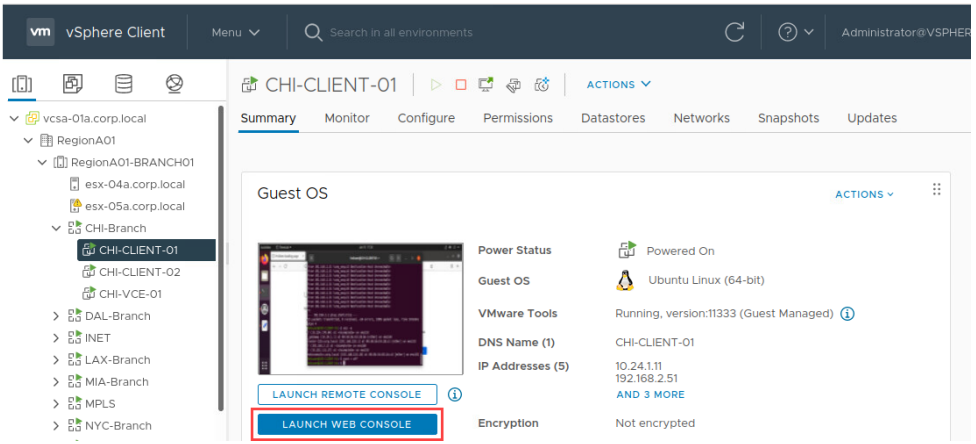


5. Connect to your vCenter Server system.
   a. From the taskbar, open the Firefox browser.
      Disregard this step if the browser is already open.
   b. Click the **Region A** bookmark folder and select the **vcsa-01a.corp.local** bookmark.



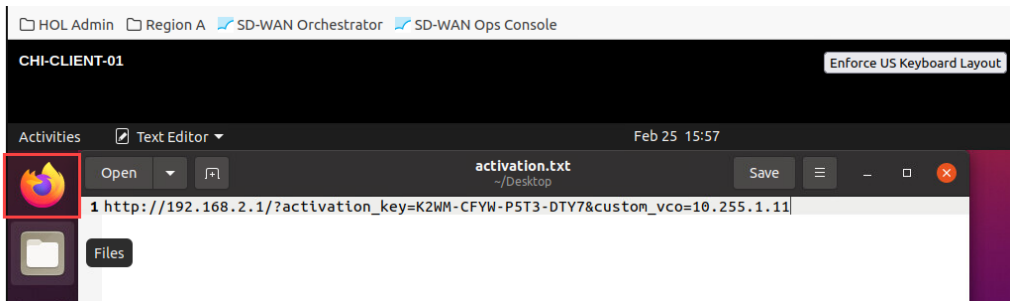
   c. Log in to vCenter Server.
      - User name: administrator@vsphere.local
      - Password: VMware1!

6. From the vCenter Server system, access the Chicago client desktop.
   a. Select **RegionA01 Data Center** > **RegionA01-BRANCH01** > **CHI-Branch vApp** > **CHI-CLIENT-01**.
   b. Click **LAUNCH WEB CONSOLE**.



7. From the CHI-CLIENT-01 desktop, double-click the **activation.txt** file icon and copy the edge activation_key URL.

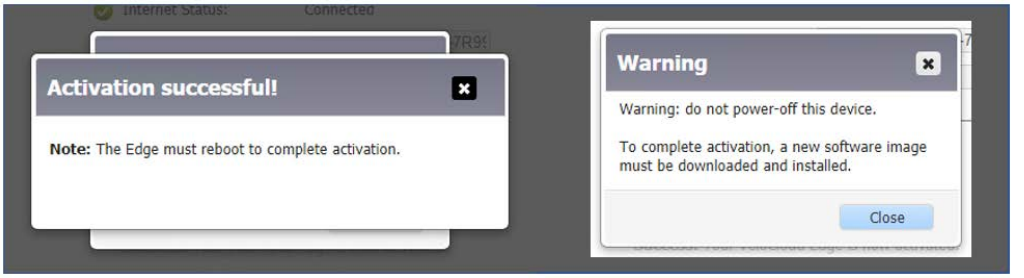
8. From the CHI-CLIENT-01 desktop, open the Firefox browser.



9. In the browser address bar, paste the activation URL that you copied from the text file and press Enter.

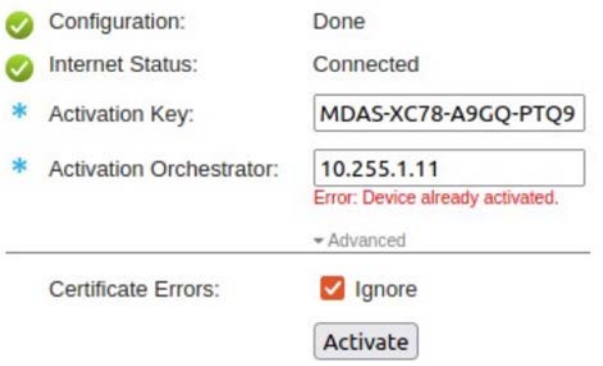
   The URL takes you to the Edge Activation page.

10. Click **Advanced**.
11. Next to Certificate Errors, select the **Ignore** check box.
12. Click **Activate** to initiate the software update.
13. Dismiss the `Activation successful!` message and close the `Warning` message.



IMPORTANT

You might encounter an `Error: Device already activated.` error instead of seeing the `Activation successful!` message. You can ignore this error and continue with next step.

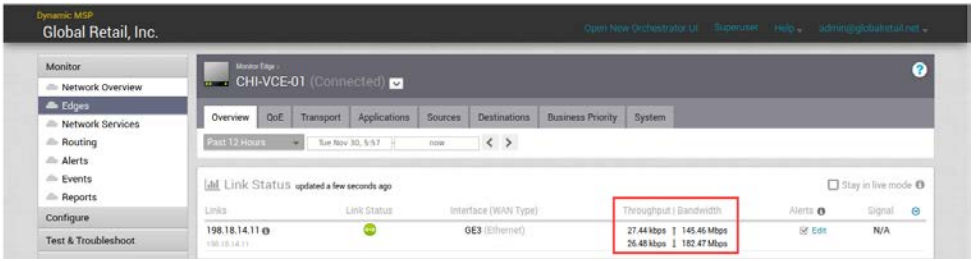


14. Return to VMware SD-WAN Orchestrator to verify that the edge is successfully activated.
    a. Select **Monitor** > **Edges** and confirm that the Chicago edge status is Active.

       Activation might take up to 5 minutes. Refresh the browser window to see the latest status.

    b. On the Edges page, select **CHI-VCE-01** to view more details.

       If Throughput | Bandwidth statistics are updating under Link Status, then the commissioning was successful.



Task 3: Configure the LAN Interface of an Edge Appliance

You configure the LAN interface of an edge appliance.

1. Select **Configure** > **Edges** in the navigation pane on the left.
2. On the Edges page, select **CHI-VCE-01**.
3. Click the **Device** tab.
4. Scroll down to Configure VLAN.
5. Under the Action column, click **Edit**.

6. Enter **`10.24.1.1`** in the **Edge LAN IP Address** text box.
7. Enter **24** in **CIDR Prefix** text box.
8. Click the **Network** box to autofill the IP address.
9. Scroll down and click **Update VLAN**.
10. Scroll to the top of the page and click **Save Changes**.

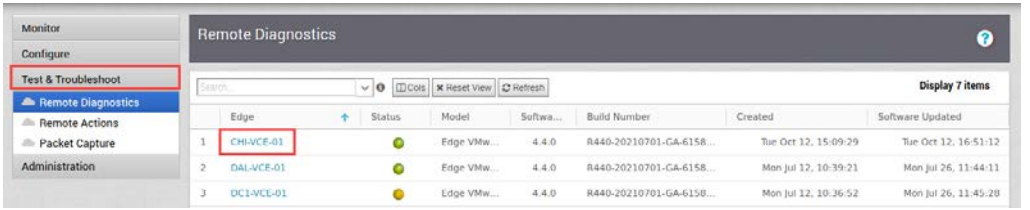
11. Click **Confirm**.

Task 4: Verify Network Connectivity

You verify remote network connectivity with the orchestrator troubleshooting tools.

1. Select **Test & Troubleshoot** > **Remote Diagnostics** in the navigation pane on the left.
2. On the Remote Diagnostics page, select **CHI-VCE-01**.

   The edge might take several minutes to enter live mode.



3. Scroll down to the Ping Test tool.
4. Ping the Chicago client IP address from 10.24.1.1 VLAN-1.
   a. From the **Segment** drop-down menu, select **Global Segment**.
   b. Enter **`10.24.1.11`** in the **Destination** text box.
   c. Select **10.24.1.1 VLAN-1** from the **Ping From** drop-down menu.
   d. Click **Run**.

Lab 4 Configuring Segmentation

Objective and Tasks

Configure segments and firewall rules:

1. Configure a Cardholder Data Environment Segment
2. Configure a Guest Segment
3. Configure a CDE Segment Firewall Rule
4. Test the CDE Segment Firewall Rule
5. Test the Guest Segment with No Firewall Rule
6. Reconnect the Edge to the Corporate VLAN

Task 1: Configure a Cardholder Data Environment Segment

You configure a segment named CDE Segment and assign it to a branch profile.

The Cardholder Data Environment (CDE) segment allows secure card payment traffic.

1. Log in to VMware SD-WAN Orchestrator.

   Disregard this step if you are already logged in.

2. Select **Configure** > **Segments** in the navigation pane on the left.

3. On the Segments page, click the plus sign (+) icon.

4. Enter **`CDE Segment`** in the **Segment Name** text box.

5. Enter **`Chicago CDE`** in the **Description** text box.

6. From the **Type** drop-down menu, select **CDE**.

7. Click **Save Changes**.

8. Select **Configure** > **Profiles** in the navigation pane on the left.

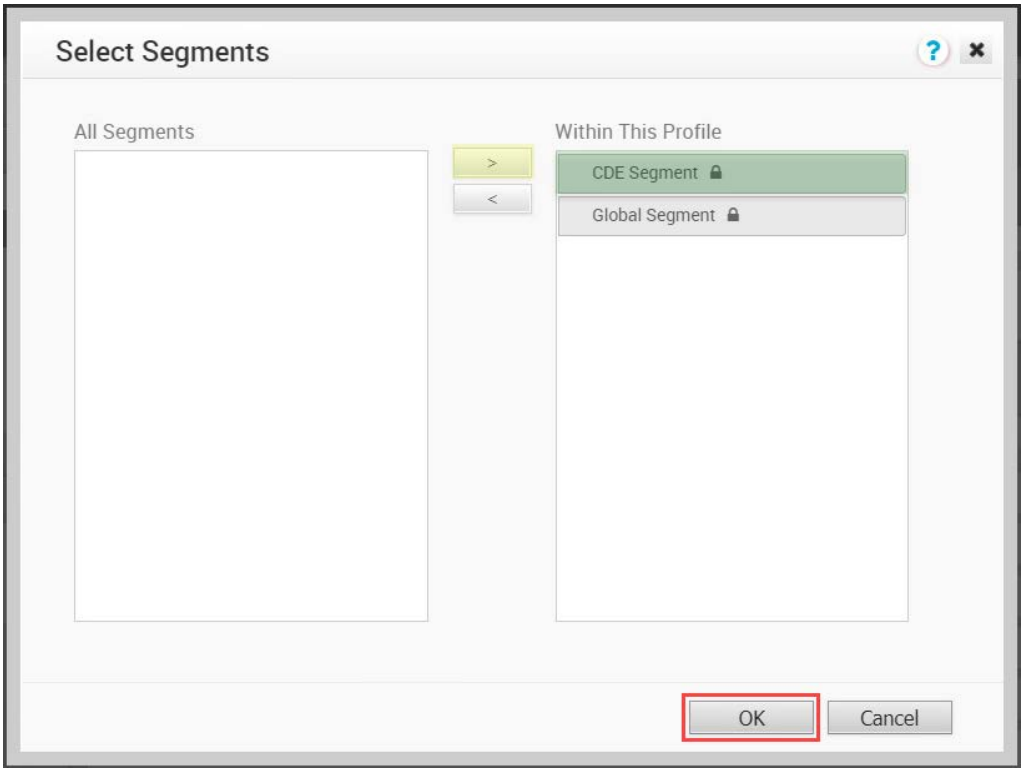
9. On the Profiles page, select **Branch Internet Only Profile**.

10. Click the **Device** tab.

11. Next to Select Profile Segments, click **Change**.

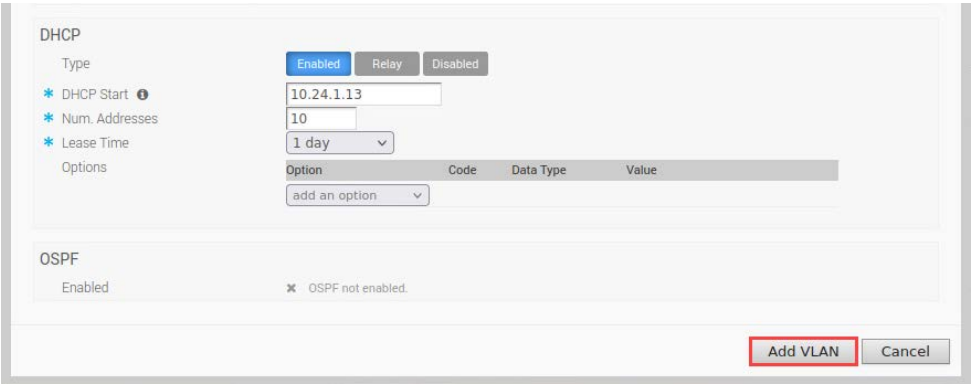
The Select Segments dialog box appears.

12. Under All Segments, select **CDE Segment**.
13. Click the right arrow to transfer CDE Segment to the Within This Profile column.
14. Click **OK**.



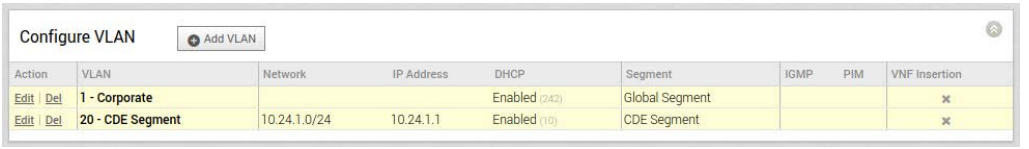
15. Configure the VLAN settings for CDE Segment.
    a. Scroll down to Configure VLAN.
    b. Click **Add VLAN**.
    c. From the **Segment** drop-down menu, select **CDE Segment**.
    d. Enter **20** in the **VLAN Id** text box.
    e. Select the **Assign Overlapping Subnets** check box and click **OK** when the warning appears.

    f. Enter **10.24.1.1** in the **Edge LAN IP Address** text box.
    g. Enter **24** in the **CIDR Prefix** text box.
    h. Under DHCP, enter **10** in the **Num. Addresses** text box.
    i. Scroll down and click **Add VLAN**.



    j. Scroll up and click **Save Changes**.

16. Inspect the Configure VLAN section and verify that 20 - CDE Segment appears in the VLAN column.



Task 2: Configure a Guest Segment

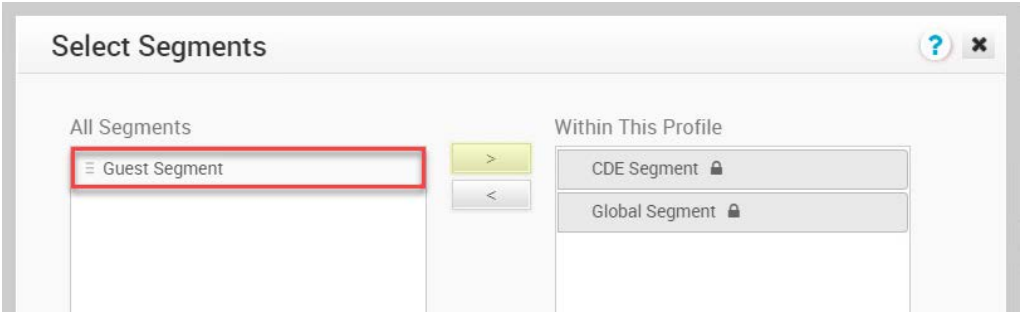
You configure a guest segment to allow non-employee guests to access the network.

1. Select **Configure** > **Segments** in the navigation pane on the left.
2. On the Segments page, click the plus sign (+) icon.

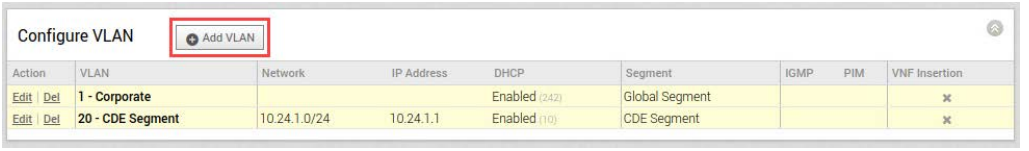
3. Enter **`Guest Segment`** in the **Segment Name** text entry box.
4. Enter **`Chicago Guest`** in the **Description** text box.
5. Click **Save Changes**.

6. Select **Configure** > **Profiles** in the navigation pane on the left.
7. On the Profiles page, select **Branch Internet Only Profile**.
8. Click the **Device** tab.
9. Next to Select Profile Segments, click **Change**.

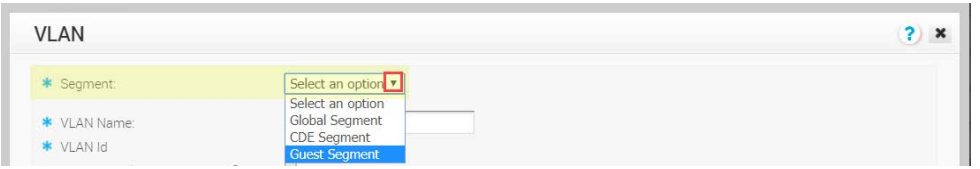
10. Under All Segments, select **Guest Segment**.



11. Click the right arrow to transfer Guest Segment to the Within This Profile column.
12. Click **OK**.
13. Scroll down to Configure VLAN and click **Add VLAN**.

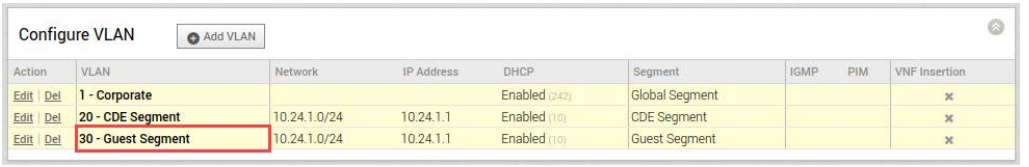


14. Configure the VLAN settings for Guest Segment.
    a. From the **Segment** drop-down menu, select **Guest Segment**.



    b. Enter **30** in the **VLAN Id** entry field.
    c. Select the **Assign Overlapping Subnets** check box and click **OK**.
    d. Enter **10.24.1.1** in the **Edge LAN IP Address** text box.
    e. Enter **24** in the **CIDR Prefix** text box.
    f. Scroll down to DHCP and enter **10** in the **Num. Addresses** text box.
    g. Click **Add VLAN**.

15. Scroll down to Configure VLAN and verify that 30 - Guest Segment appears in the VLAN column.

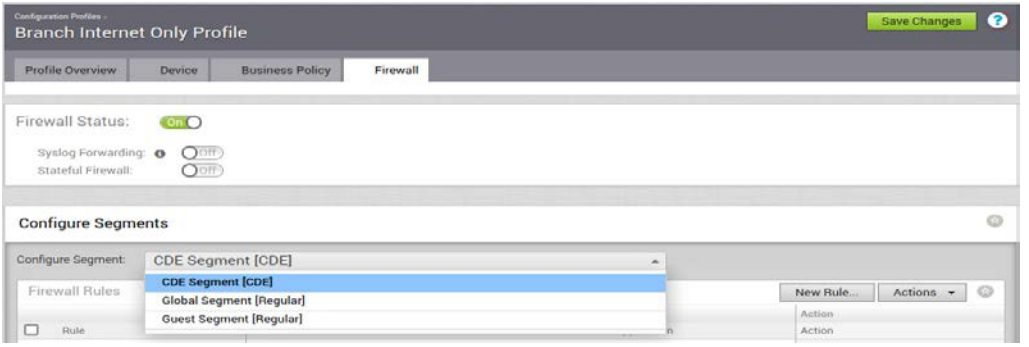


16. Scroll up and click **Save Changes**.

Task 3: Configure a CDE Segment Firewall Rule

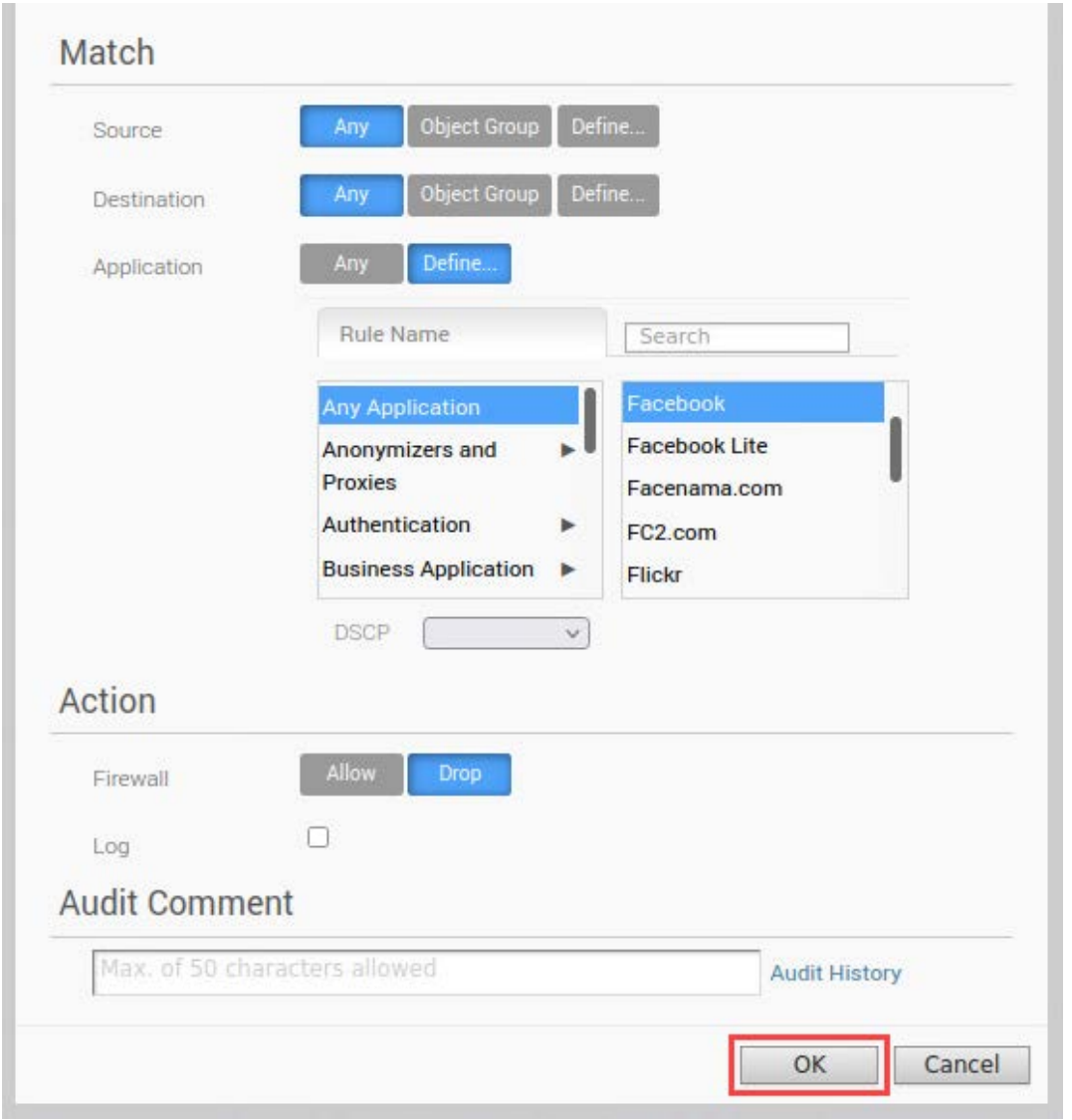
You configure a firewall rule for the CDE segment.

1. Select **Configure** > **Profiles** in the navigation pane on the left.
2. On the Profiles page, select **Branch Internet Only Profile.**
3. Click the **Firewall** tab.
4. From the **Configure Segment** drop-down menu, select **CDE Segment [CDE]**.

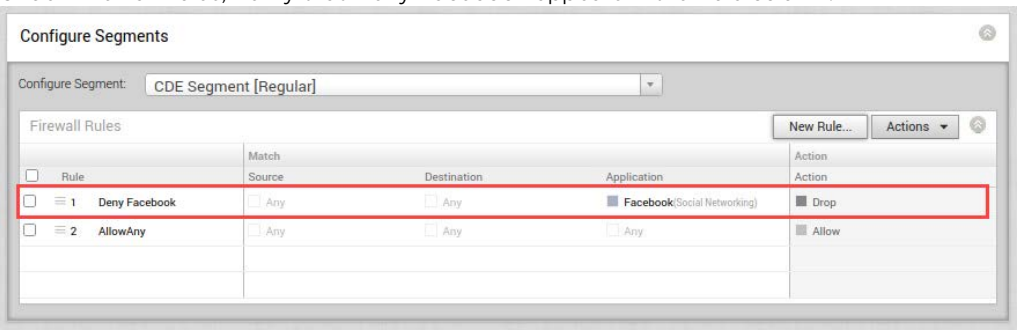


5. Under Firewall Rules, click **New Rule**.

6. Configure the Configure Rule dialog box.
   a. Enter **Deny Facebook** in the **Rule Name** text box.
   b. Next to Application, click **Define**.
   c. In the Rule Name Search box, type **Facebook** and press Enter.
   d. Next to Firewall, click **Drop**.
   e. Scroll down and click **OK**.



7. Scroll down to Configure Segments.
8. Under Firewall Rules, verify that Deny Facebook appears in the Rule column.



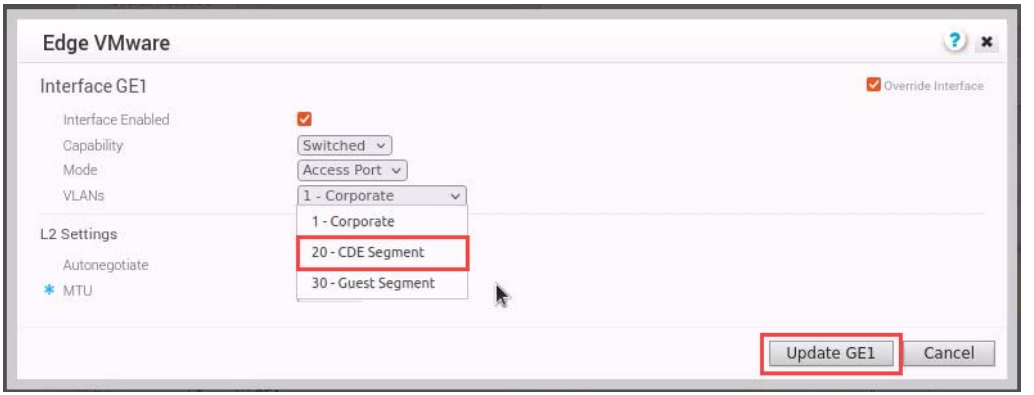
9. Click **Save Changes**.

Task 4: Test the CDE Segment Firewall Rule

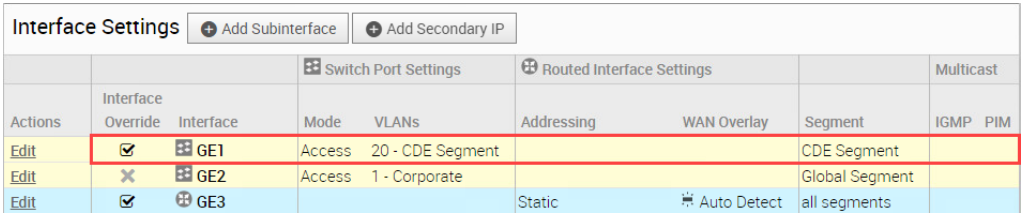
You configure the Chicago edge to use the CDE segment and then verify that you cannot access Facebook.

1. Select **Configure** > **Edges** in the navigation pane on the left.
2. On the Edges page, select **CHI-VCE-01**.
3. Click the **Device** tab.
4. Scroll down to the GE1 interface under Interface Settings.
5. Under Actions, click **Edit**.

   The Edge VMware dialog box appears.
6. Select the **Override Interface** check box.
7. From the **VLANs** drop-down menu, select **20 - CDE Segment**.
8. Click **Update GE1**.



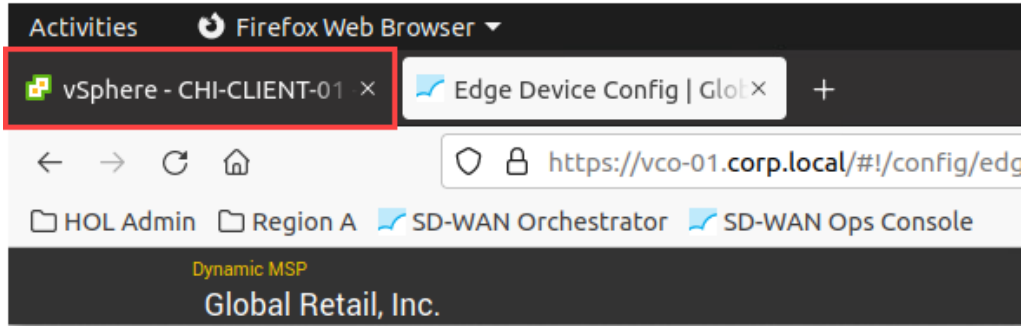
9. Under Interface Settings, verify that 20 - CDE Segment appears in the VLANs column next to the GE1 interface.



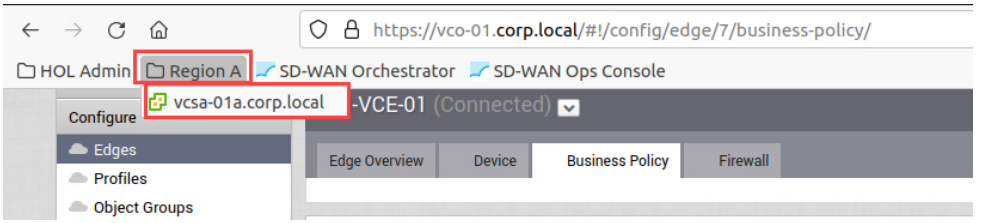
10. Scroll up and click **Save Changes**.

11. In the Confirm Changes dialog box, click **Confirm**.

12. From the top Firefox taskbar, click the **vSphere - CHI-CLIENT-01** tab.



13. If the **vSphere - CHI-CLIENT-01** tab is closed, access the Chicago client desktop from the vCenter Server system.
    a. Click the **Region A** bookmark folder and select the **vcsa-01a.corp.local** bookmark.



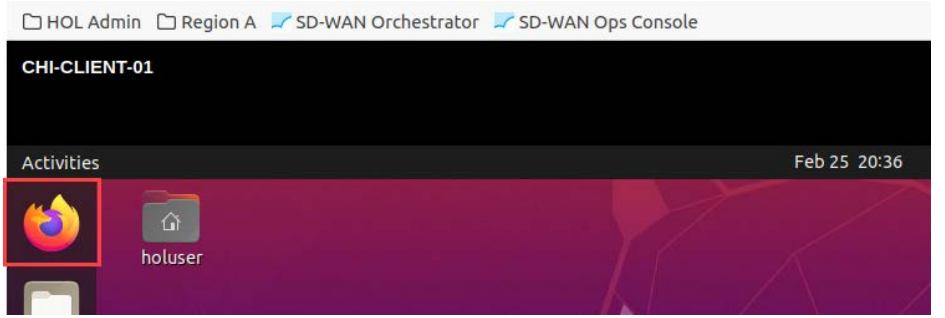
    b. Log in to vCenter Server.
       - User name: administrator@vsphere.local
       - Password: VMware1!

    c. Select **RegionA01 Data Center** > **RegionA01-BRANCH01** > **CHI-Branch vApp** > **CHI-CLIENT-01**.

14. Click **LAUNCH WEB CONSOLE**.
15. From the taskbar of the Chicago client desktop, open a Terminal window.
16. Run the `netstat -rn` command.
17. Verify that 10.24.1.1 appears in the Gateway column.

```
holuser@CHI-CLIENT-01:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.24.1.1       0.0.0.0         UG        0 0          0 ens160
10.24.1.0       0.0.0.0         255.255.255.0   U         0 0          0 ens160
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 ens160
192.168.2.0     0.0.0.0         255.255.255.0   U         0 0          0 ens160
192.168.110.10  192.168.120.1   255.255.255.255 UGH       0 0          0 ens192
192.168.120.0   0.0.0.0         255.255.255.0   U         0 0          0 ens192
```

18. Minimize the Terminal window.
19. Open Firefox.



20. In the Firebox browser, enter **`facebook.com`** in the address bar.
    Access to the Facebook web page is denied as per the CDE segment firewall rule.

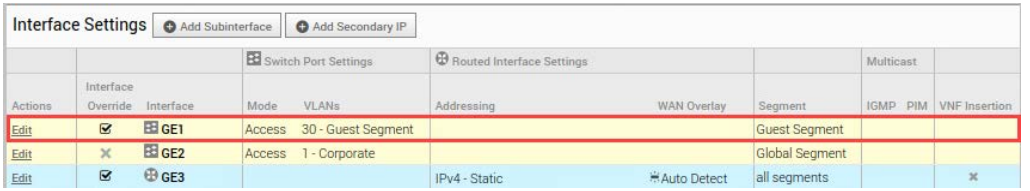
Task 5: Test the Guest Segment with No Firewall Rule

You configure the Chicago edge to utilize the guest segment and then verify that you can access Facebook.

1. Select **Configure** > **Edges** in the navigation pane on the left.
2. On the Edges page, select **CHI-VCE-01**.
3. Click the **Device** tab.
4. Scroll down to the GE1 interface under Interface Settings.
5. Under Actions, click **Edit**.

   The Edge VMware dialog box appears.
6. Select the **Override Interface** check box.
7. From the **VLANs** drop-down menu, select **30 - Guest Segment**.
8. Click **Update GE1**.

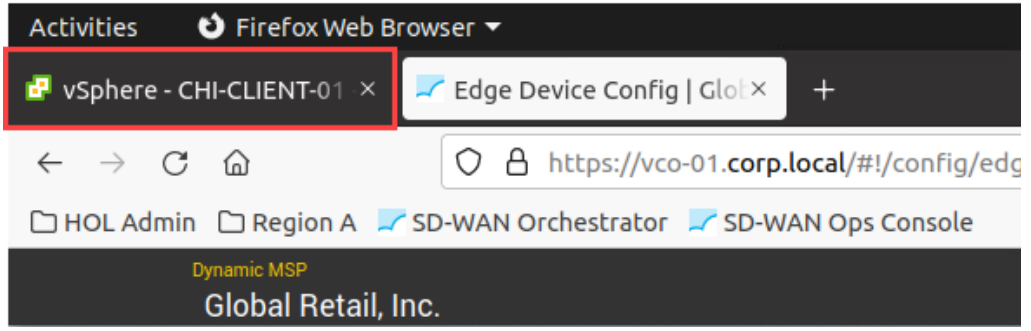
9. Under Interface Settings, verify that 30 - Guest Segment appears in the VLANs column next to the GE1 interface.



10. Scroll up and click **Save Changes**.

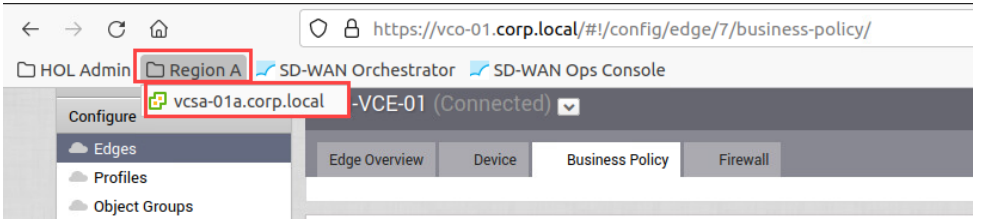
11. In the Confirm Changes dialog box, click **Confirm**.

12. From the top Firefox taskbar, click the **vSphere - CHI-CLIENT-01** tab.



13. If the **vSphere - CHI-CLIENT-01** tab is closed, access the Chicago client desktop from the vCenter Server system.

    a. Click the **Region A** bookmark folder and select the **vcsa-01a.corp.local** bookmark.



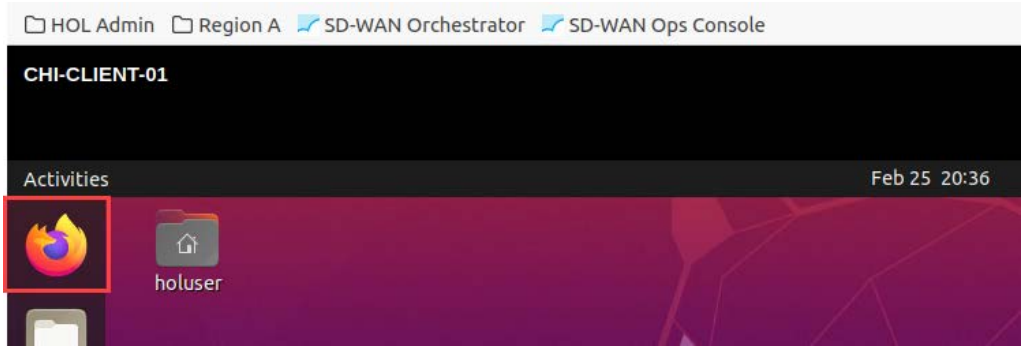
    b. Log in to vCenter Server.

    - User name: administrator@vsphere.local
    - Password: VMware1!

    c. Select **RegionA01 Data Center** > **RegionA01-BRANCH01** > **CHI-Branch vApp** > **CHI-CLIENT-01**.

14. Click **LAUNCH WEB CONSOLE**.

15. Open Firefox.



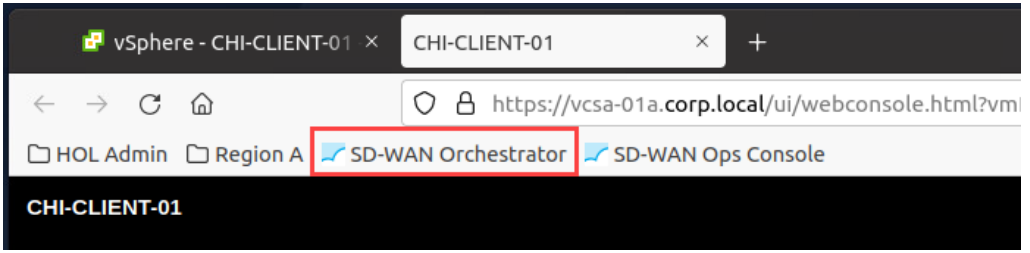
16. In the Firebox browser, enter **`facebook.com`** in the address bar.

    Access to the Facebook web page is allowed as per the guest segment firewall rule.

Task 6: Reconnect the Edge to the Corporate VLAN

You reconfigure the Chicago edge to use the corporate VLAN.

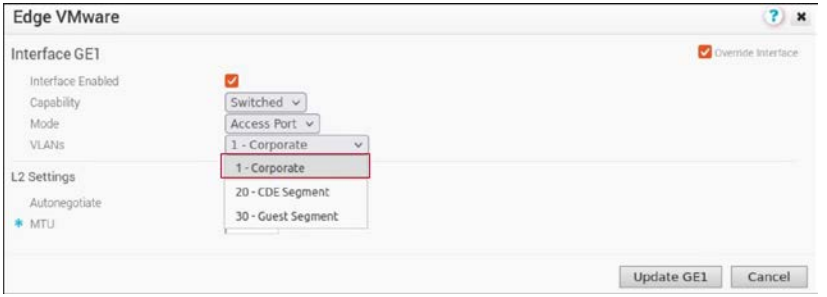
1. From the Firefox bookmark bar, click **SD-WAN Orchestrator**.



2. Select **Configure** > **Edges** in the navigation pane on the left.
3. On the Edges page, select **CHI-VCE-01**.
4. Click the **Device** tab.
5. Scroll down to the GE1 interface under Interface Settings.
6. Under Actions, click **Edit**.

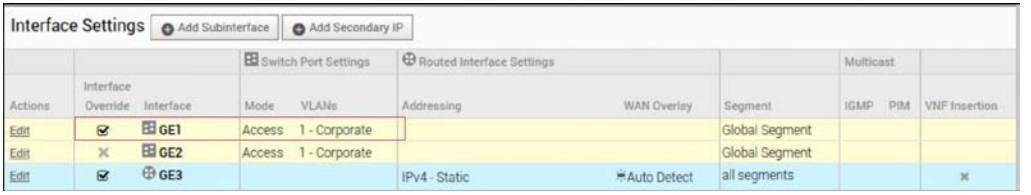
   The Edge VMware dialog box appears.
7. Select the **Override Interface** check box.

8. From the **VLANs** drop-down menu, select **1 - Corporate**.



9. Click **Update GE1**.

10. Under Interface Settings, verify that 1 - Corporate appears in the VLANs column next to the GE1 interface.



11. Scroll up and click **Save Changes**.

12. In the Confirm Changes dialog box, click **Confirm**.

The `Changes saved successfully` message appears.

Lab 5 Configuring Profiles

Objective and Tasks

Create a new profile and apply restrictions to the profile:

1. Create a New Configuration Profile
2. Apply a Profile Restriction
3. Create a New Edge
4. Change the Profile Assigned to the Edge

Task 1: Create a New Configuration Profile

You create a new VMware SD-WAN profile. You do not assign it to any edge device.

1. Log in to VMware SD-WAN Orchestrator.

   Disregard this step if you are already logged in.

2. Select **Configure** > **Profiles** in the navigation pane on the left.
3. On the Profiles page, click **New Profile**.
4. Enter **`New Segment Profile`** in the **Name** text box.

5. Click **Create**.

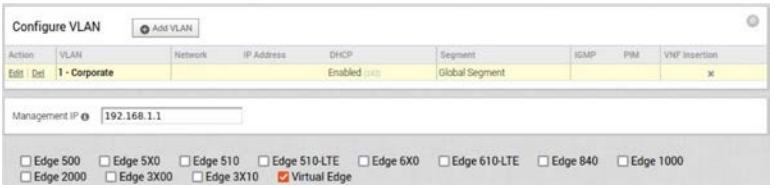
Task 2: Apply a Profile Restriction

You create a profile called Branch Virtual Profile and apply a restriction to it.

1. Create a new profile.
   a. Select **Configure** > **Profiles** in the navigation pane on the left.
   b. On the Profiles page, click **New Profile**.
   c. Enter **`Branch Virtual Profile`** in the **Name** text box.
   d. (Optional) Enter a description of the profile in the **Description** text box.
   e. Click **Create**.

      The configuration page for Branch Virtual Profile appears. Under Profile Overview, the enabled edge appliances are shown next to Enabled Models.

2. Click the **Device** tab.
3. Scroll down to Configure VLAN.
4. Deselect the check boxes of all edge appliance models except **Virtual Edge**.



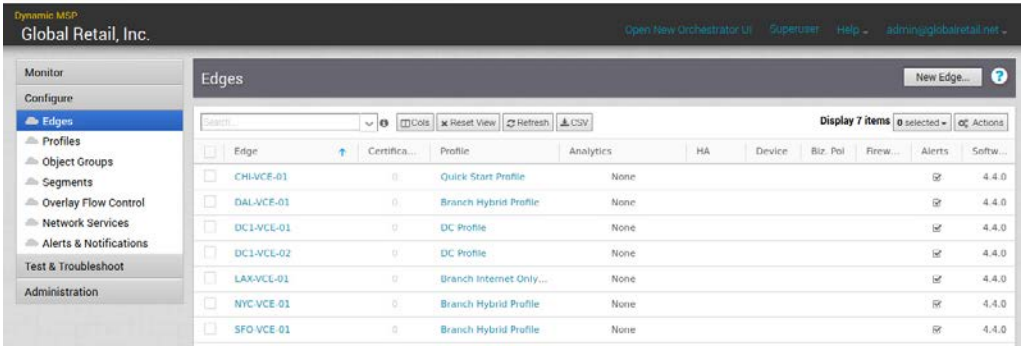
5. Scroll up and click **Save Changes**.

   Branch Virtual Profile is now restricted to Virtual Edge only.

Task 3: Create a New Edge

You provision a new edge. You assign it the profile that you created in an earlier task to verify the profile restriction.

1. Select **Configure** > **Edges** in the navigation pane on the left.

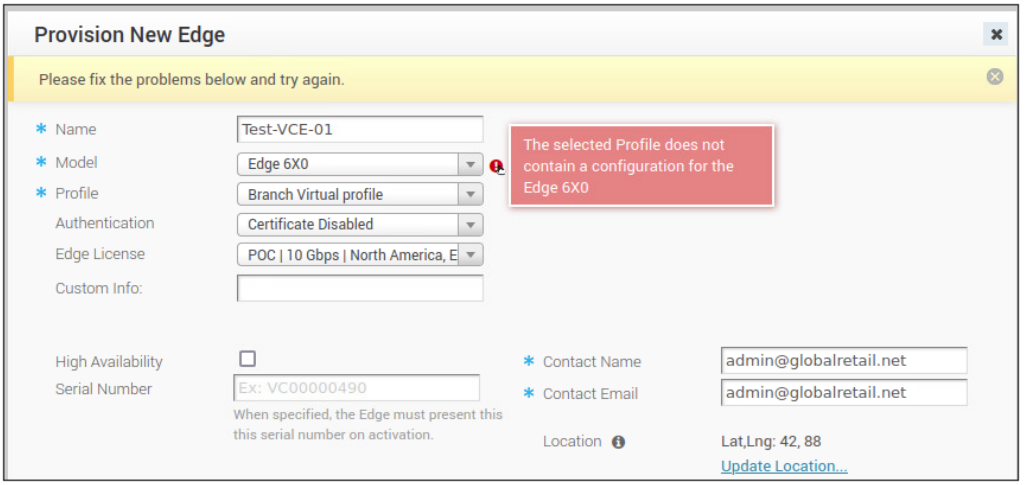


2. On the Edges page, click **New Edge**.

   The Provision New Edge dialog box appears.
3. Enter **`Test-VCE-01`** in the **Name** text box.
4. From the **Model** drop-down menu, select **Edge 6X0**.
5. From the **Profile** drop-down menu, select **Branch Virtual Profile**.
6. From the **Edge License** drop-down menu, select **POC | 10 Gbps | North America**.

7. Click **Create**.

   The error message `The selected Profile does not contain a configuration for the Edge 6X0` appears.



NOTE

This is the expected result. The error is valid because the profile was configured in an earlier task to be restricted to Virtual Edge only.

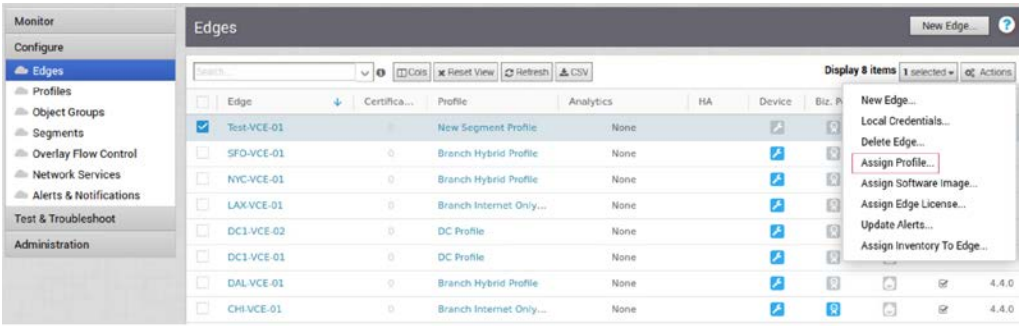
8. From the **Profile** drop-down menu, select **New Segment Profile** and click **Create**.

   The new edge provisioning is successful because New Segment Profile has no restrictions.

Task 4: Change the Profile Assigned to the Edge

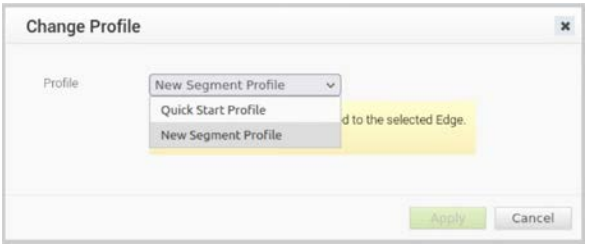
You change the profile assigned to the Test-VCE-01 edge to Branch Internet Only Profile.

1. Select **Configure** > **Edges** in the navigation pane on the left.
2. On the Edges page, select the **Test-VCE-01** check box.
3. From the **Actions** drop-down menu, select **Assign Profile**.



The Change Profile dialog box appears.

4. From the **Profile** drop-down menu, select **Quick Start Profile**.



5. Click **Apply**.

Lab 6 Configuring and Verifying Overlay Tunnels

Objective and Tasks

Understand the configuration of user-defined and auto-defined overlay tunnels:

1. Configure an Auto-Detected Overlay
2. Verify the Auto-Detected Overlay
3. Verify the User-Defined Overlay

Task 1: Configure an Auto-Detected Overlay

You configure the CHI-VCE-01 public WAN link on the GE4 interface to trigger an auto-detected overlay.

1. Log in to VMware SD-WAN Orchestrator.

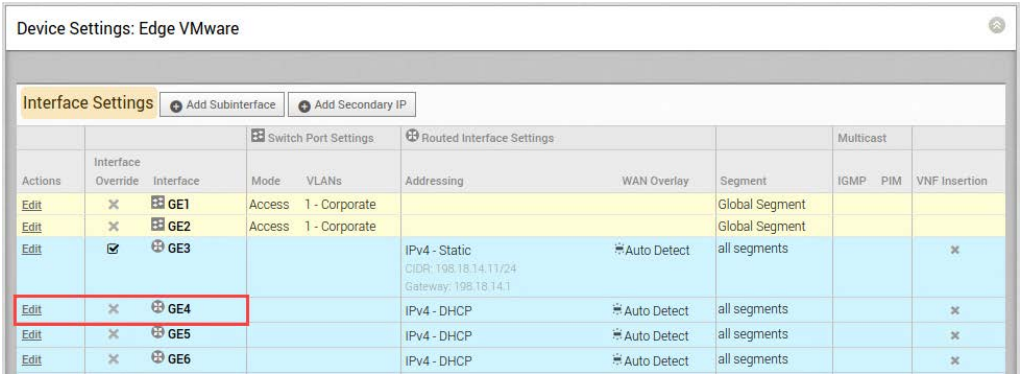
   Disregard this step if you are already logged in.

2. Select **Configure** > **Edges** in the navigation pane on the left.

3. On the Edges page, select **CHI-VCE-01** and click the **Device** tab.

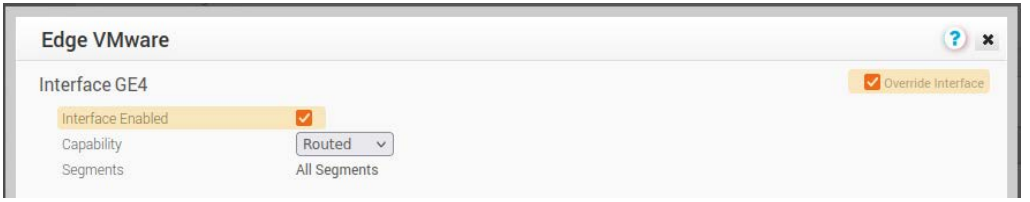
4. Scroll down to Interface Settings.

5. Next to the GE4 interface, click **Edit**.



6. Select the **Override Interface** check box.

7. Verify that the **Interface Enabled** check box is selected.

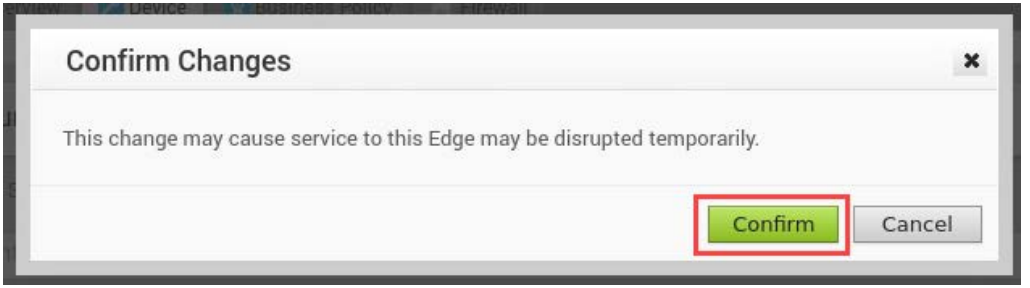


8. Configure the GE4 interface.
    a. From the **Addressing Type** drop-down menu, select **Static**.
    b. Enter **198.18.15.11** in the **IP Address** text box.
    c. Enter **24** in the **CIDR prefix** text box.
    d. Enter **198.18.15.1** in the **Gateway** text box.

9. Scroll down and click **Update GE4**.

10. Scroll up and click **Save Changes**.

11. Click **Confirm**.



NOTE

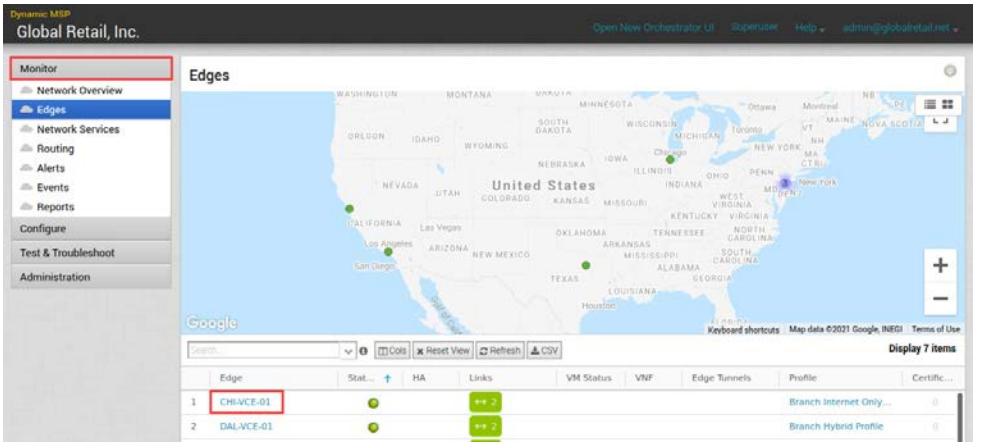
A warning appears if you fail to save changes.

12. Verify that two WAN links were created.

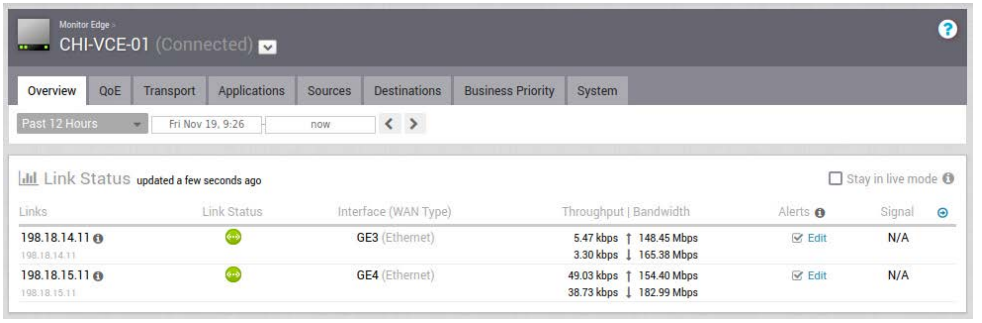
    Verification can take up to 5 minutes.

    a. From the VMware SD-WAN Orchestrator dashboard, select **Monitor** > **Edges**.

    b. On the Edges page, select **CHI-VCE-01**.



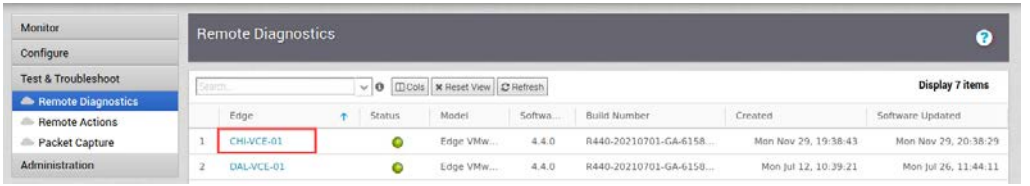
    c. Verify that two public Internet links are active.



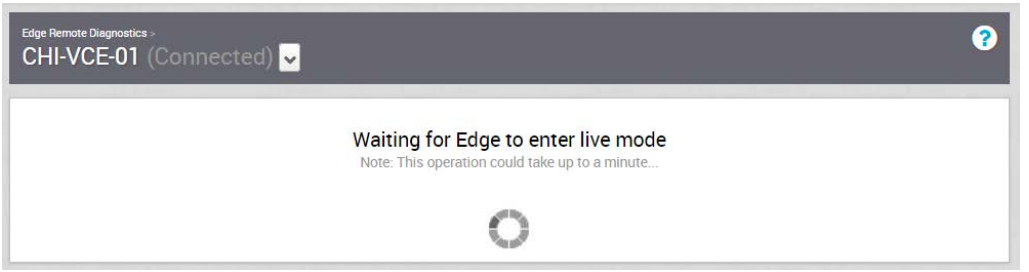
Task 2: Verify the Auto-Detected Overlay

You verify that the WAN link automatically built an overlay tunnel to the primary and secondary gateways.

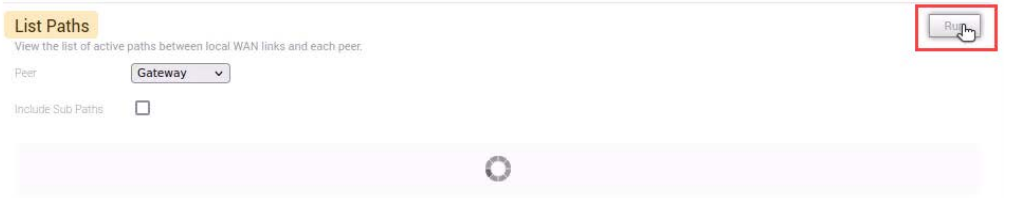
1. Select **Test & Troubleshoot** > **Remote Diagnostics** in the navigation pane on the left.
2. On the Remote Diagnostics page, select **CHI-VCE-01**.



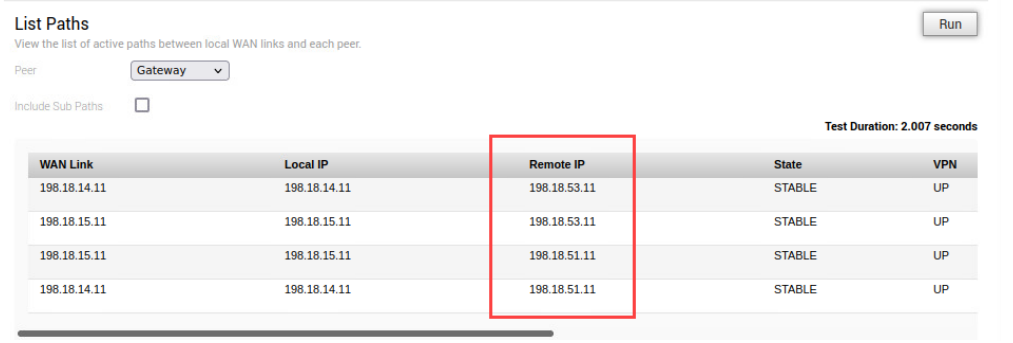
Allow 10 to 20 seconds for the Edge Remote Diagnostics window to appear.



3. Scroll down to List Paths and click **Run**.



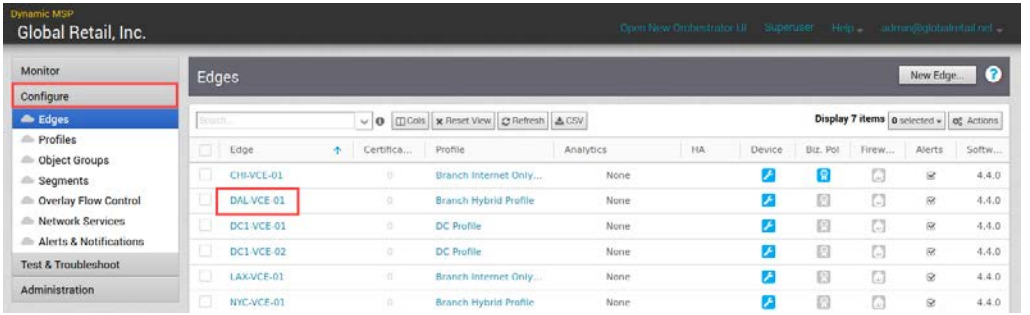
The resultant paths should now show VPN tunnels between each local IP address and the remote IP address of each VMware SD-WAN Gateway instance.



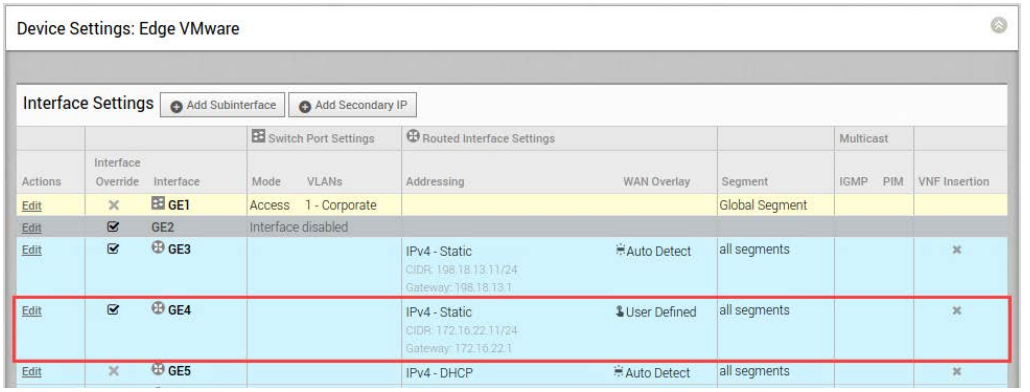
Task 3: Verify the User-Defined Overlay

You verify the user-defined private WAN overlay without altering its configuration.

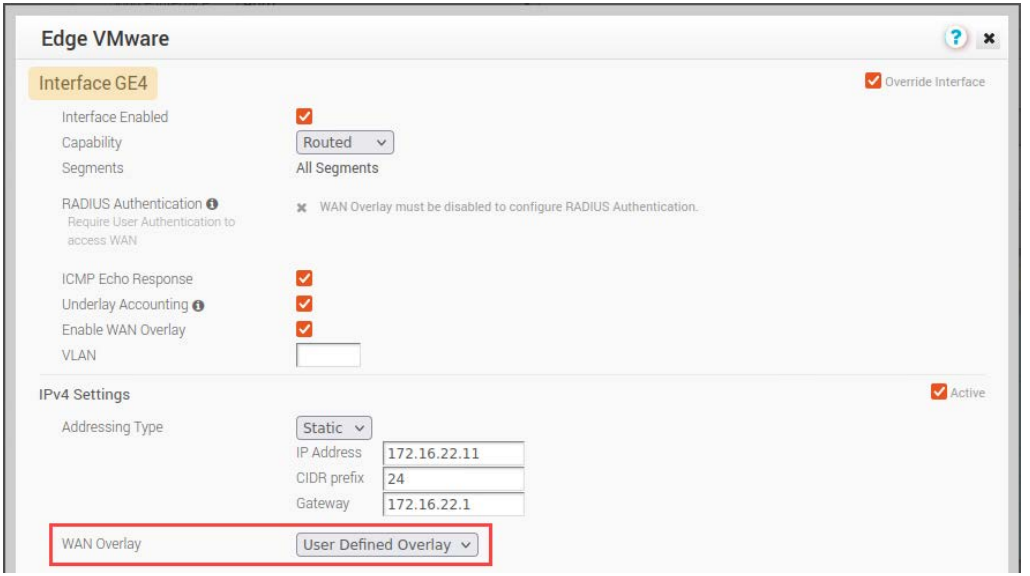
1. Select **Configure** > **Edges** in the navigation pane on the left.
2. On the Edges page, select **DAL-VCE-01**.



3. Click the **Device** tab.
4. Scroll down to the GE4 interface under Interface Settings.
5. Under Actions, click **Edit**.



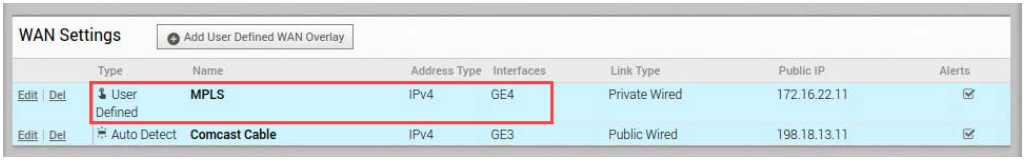
6. Verify that User Defined Overlay appears in the **WAN Overlay** drop-down menu.



7. Click the X in the upper-right corner to close the Edge VMware dialog box.

   No configuration changes were made.

8. Under WAN Settings, verify that User Defined appears in the Type column for the GE4 interface.



Lab 7 Configuring Overlays for Cloud VPN

Objective and Tasks

Configure overlays and VPNs to establish secure data paths between the branch sites and the data center:

1. Explore the OFC Table and Enable Cloud VPN for Internet-Only Profiles
2. Enable Cloud VPN for Branch Hybrid Profile
3. Change the Device Role from Edge to Hub
4. Enable Hub-Spoke Topology for Branch Hybrid Profile
5. Enable Branch to Branch VPN with Gateways
6. Verify the Path for Branch to Branch VPN
7. Enable Branch to Branch VPN with Hubs

Task 1: Explore the OFC Table and Enable Cloud VPN for Internet-Only Profiles

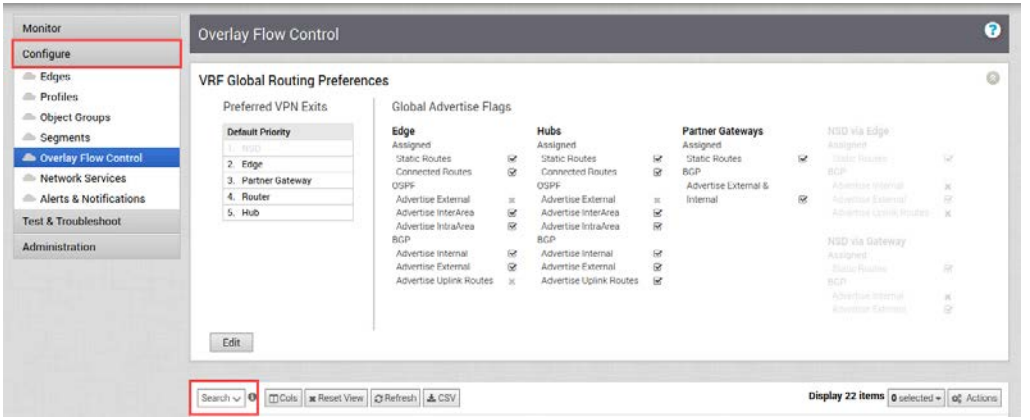
You explore the Overlay Flow Control (OFC) table to see a global view of all routes. You examine the OFC table before and after enabling the Cloud VPN option.

1. Log in to VMware SD-WAN Orchestrator.

   Disregard this step if you are already logged in.

2. Select **Configure** > **Overlay Flow Control** in the navigation pane on the left.

3. On the Overlay Flow Control page, click **Search**.

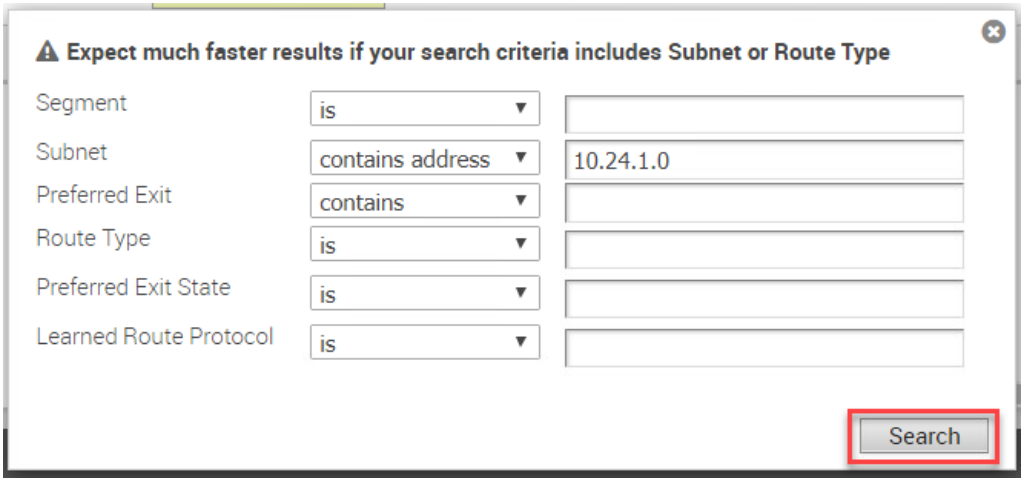


4. From the **Subnet** drop-down menu, select **contains address**.

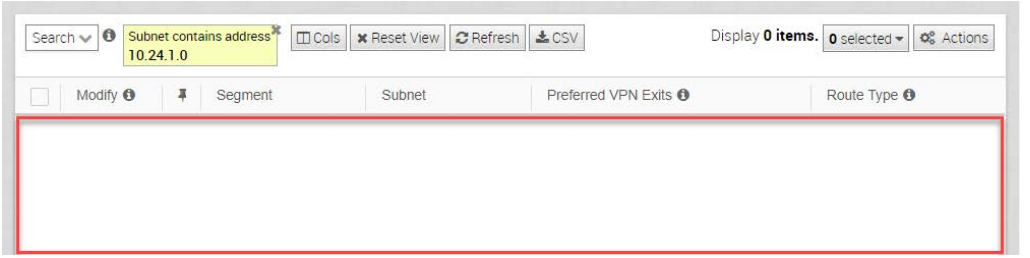
5. Enter **`10.24.1.0`** in the **Subnet** text box.

   This IP address is for the Chicago branch.

6. Click **Search** to initiate the routing table search.

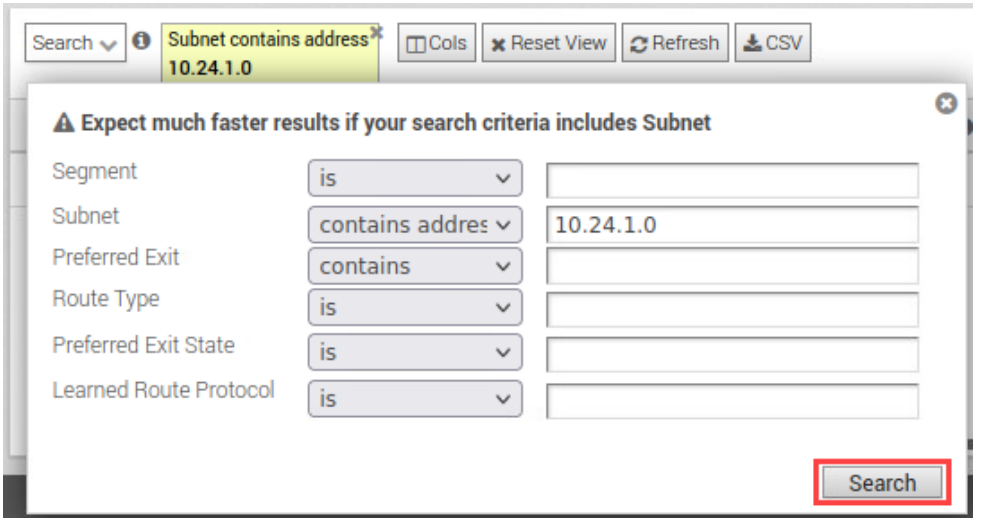


No results are found. This result is expected because Cloud VPN is disabled in the profile.

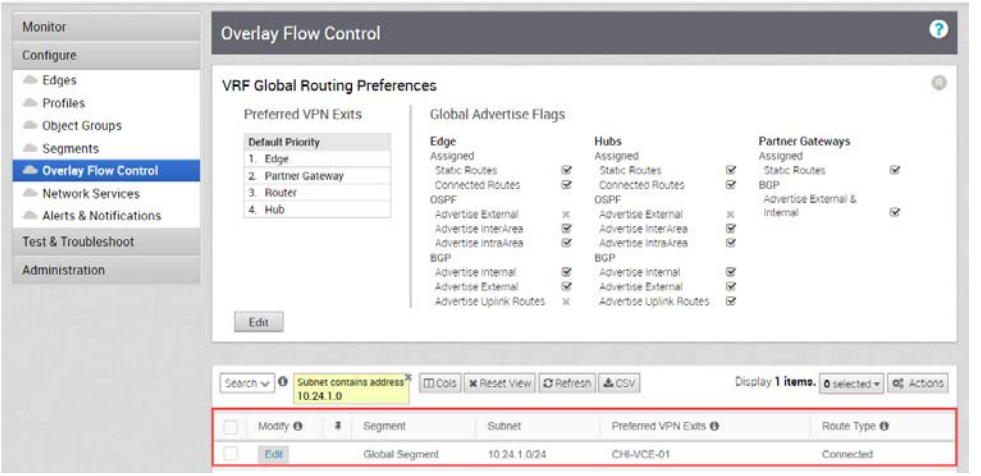


7. Enable Cloud VPN for Branch Internet Only Profile.
   a. Select **Configure** > **Profiles** in the navigation pane on the left.
   b. On the Configuration Profiles page, select **Branch Internet Only Profile**.
   c. Click the **Device** tab.
   d. Under Configure Segments, turn on the **Cloud VPN** toggle.
   e. Click **Save Changes**.
   f. Click the browser back button twice to return to the Configuration Profiles page.

8. Identify the subnet route in the OFC table.
   a. Select **Configure** > **Overlay Flow Control** in the navigation pane on the left.
   b. Click **Search.**
   c. From the **Subnet** drop-down menu, select **contains address**.
   d. Enter **`10.24.1.0`** in the **Subnet** text box.
   e. Click **Search**.



The 10.24.1.0/24 route appears in the OFC table because Cloud VPN is enabled.



Task 2: Enable Cloud VPN for Branch Hybrid Profile

You enable Cloud VPN functionality for Branch Hybrid Profile.

1. Select **Configure** > **Profiles** in the navigation pane on the left.
2. On the Configuration Profiles page, select **Branch Hybrid Profile**.
3. Click the **Device** tab.
4. Under Configure Segments, turn on the **Cloud VPN** toggle.
5. Click **Save Changes**.
6. (Optional) Verify that Cloud VPN is enabled for DC Profile.
    a. Select **Configure** > **Profiles** in the navigation pane on the left.
    b. On the Configuration Profiles page, select **DC Profile**.
    c. Click the **Device** tab.
    d. Under Configure Segments, verify that the **Cloud VPN** toggle is on.

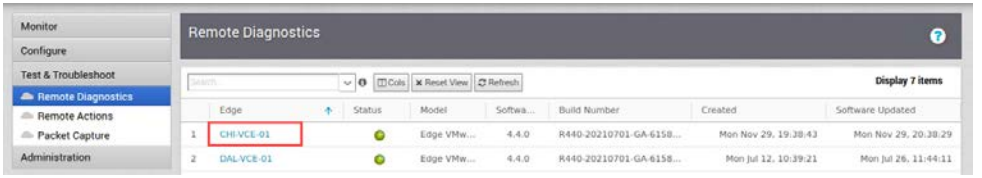
Task 3: Change the Device Role from Edge to Hub

You change the role of device DC1-VCE-01 from edge to hub. Before enabling the hub role, you run the `List Path` command to verify that it only displays a gateway peer. After enabling the hub role, the `List Path` command displays both a gateway and a hub device as peers.

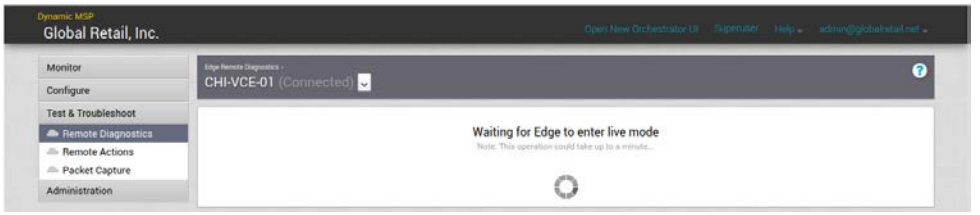
1. Verify the peer status before changing the device configuration.

   a. Select **Test & Troubleshoot** > **Remote Diagnostics** in the navigation pane on the left.

   b. On the Remote Diagnostics page, select **CHI-VCE-01**.



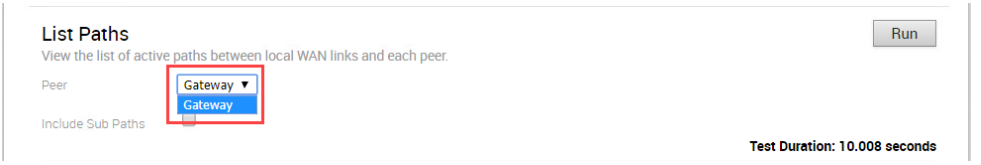
   Allow 10 to 20 seconds for the Edge Remote Diagnostics window to appear.



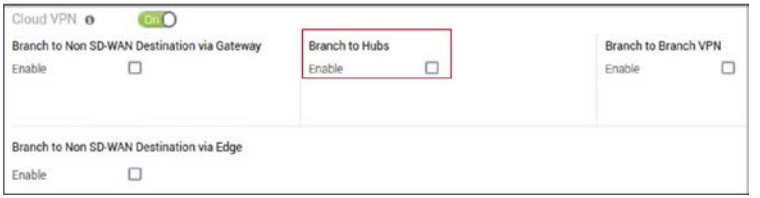
   c. Scroll down to List Paths.

      The commands are in alphabetical order.

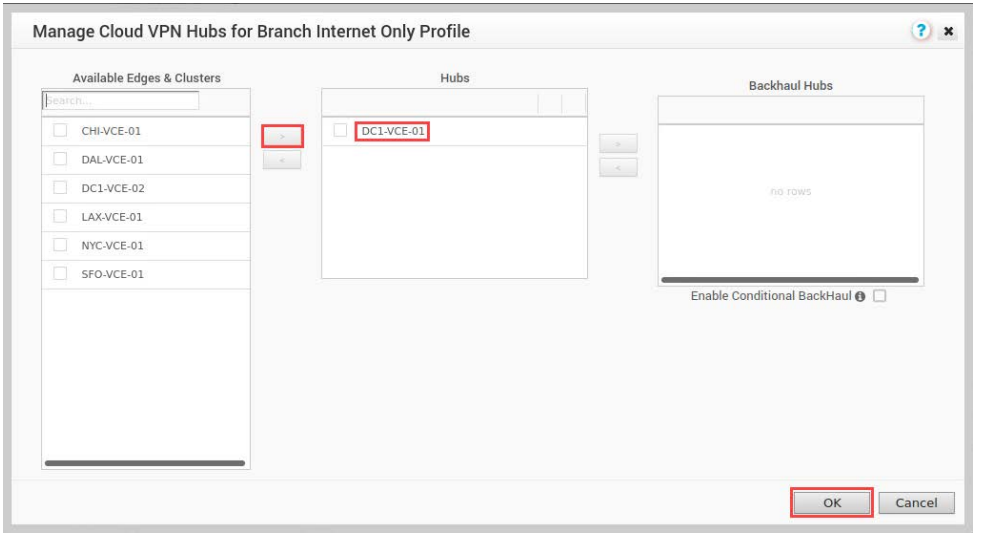
   d. Click the **Peer** drop-down menu and verify that Gateway is the only choice.



2. Change the role of device DC1-VCE-01.
   a. Select **Configure** > **Profiles** in the navigation pane on the left.
   b. On the Configuration Profiles page, select **Branch Internet Only Profile**.
   c. Click the **Device** tab and scroll down to Cloud VPN.
   d. Under Branch to Hubs, select the **Enable** check box.



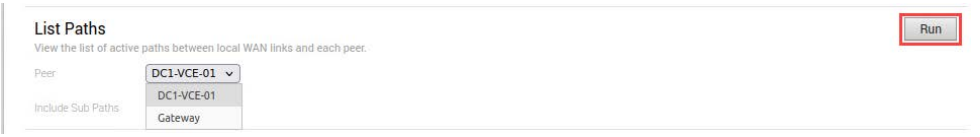
   e. Click **Select Hubs**.
   f. Select the **DC1-VCE-01** check box.
   g. Click the right arrow to add DC1-VCE-01 to the Hubs column.
   h. Click OK.



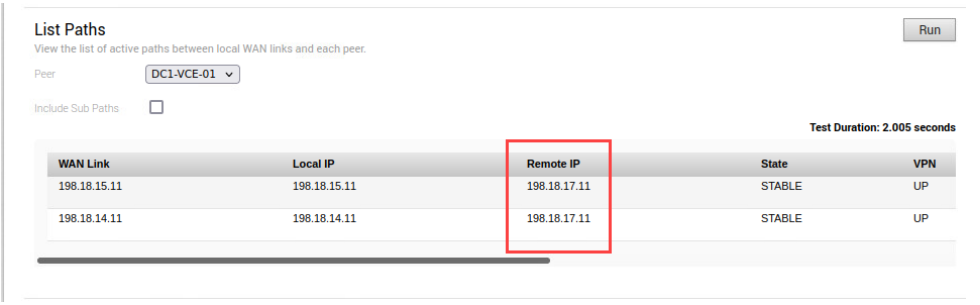
   i. Scroll up and click **Save Changes**.

3. Run the `List Paths` command.
   a. Select **Test & Troubleshoot** > **Remote Diagnostics** in the navigation pane on the left.
   b. On the Remote Diagnostics page, select **CHI-VCE-01**.
   c. Scroll down to List Paths.

      List Paths now displays the newly added hub in the **Peer** drop-down menu.
   d. From the **Peer** drop-down menu, select **DC1-VCE-01** and click **Run**.



Now that a hub-spoke Cloud VPN is enabled for Branch Internet Only Profile, the CHI and LAX branch sites have overlay tunnels to the hub site.

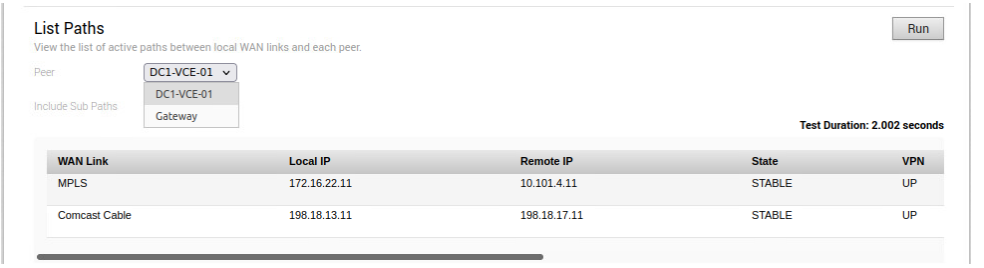


Task 4: Enable Hub-Spoke Topology for Branch Hybrid Profile

You enable a hub-spoke topology for Branch Hybrid Profile. DC1-VCE-01 acts as the hub, and the Chicago and Los Angeles edges act as the spokes.

1. Select **Configure** > **Profiles** in the navigation pane on the left.
2. On the Configuration Profiles page, select **Branch Hybrid Profile**.
3. Click the **Device** tab.
4. Scroll down and verify that the **Cloud VPN** toggle is turned on.
5. Under Branch to Hubs, select the **Enable** check box.
6. Click **Select Hubs**.
7. Select the **DC1-VCE-01** check box.
8. Click the right arrow to add DC1-VCE-01 to the Hubs column.
9. Click **OK**.
10. Click **Save Changes**.
11. Verify the path status of the device.
    a. Select **Test & Troubleshoot** > **Remote Diagnostics** in the navigation pane on the left.
    b. On the Remote Diagnostics page, select **DAL-VCE-01**.
    c. Scroll down to List Paths and select **DC1-VCE-01** from the **Peer** drop-down menu.
    d. Click **Run**.

    Two paths are now present.

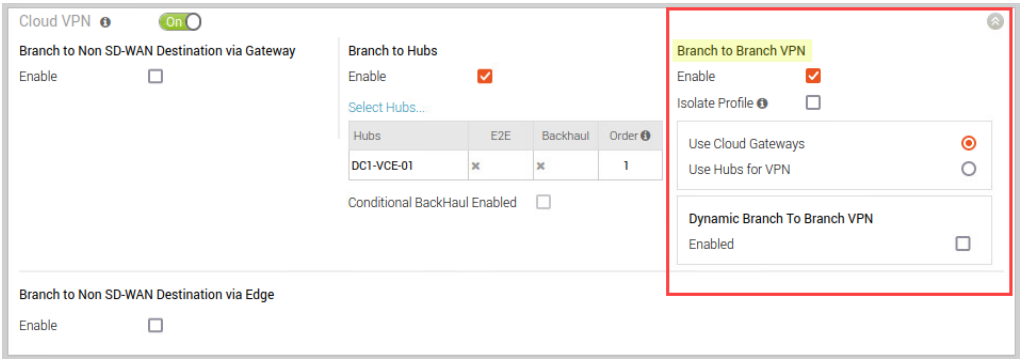


Task 5: Enable Branch to Branch VPN with Gateways

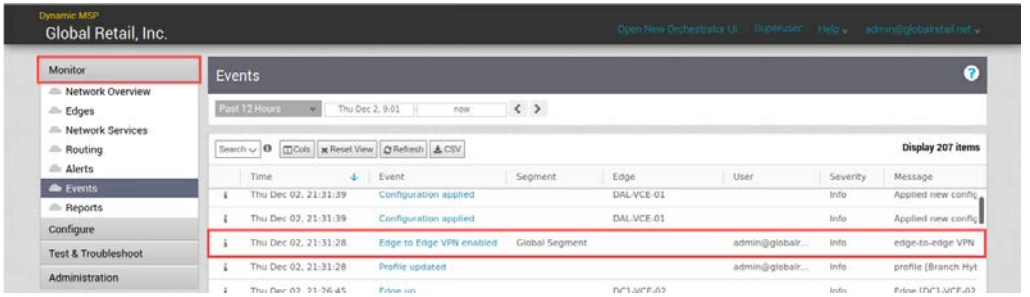
You change the configuration of Branch Hybrid Profile and Branch Internet Only Profile, using gateways to establish Cloud VPN tunnels for branch-to-branch communications.

The gateway distributes routes to all edge devices. The routes learned from other edges are called overlay routes.

1. Select **Configure** > **Profiles** in the navigation pane on the left.
2. On the Configuration Profiles page, select **Branch Hybrid Profile**.
3. Click the **Device** tab and scroll down to Cloud VPN.
4. Under Branch to Branch VPN, select the **Enable** check box.
5. Under Dynamic Branch to Branch VPN, deselect the **Enabled** check box.



6. Click **Save Changes**.
7. Select **Monitor** > **Events** to verify the configuration change.



8. Repeat the configuration steps for Branch Internet Only Profile.

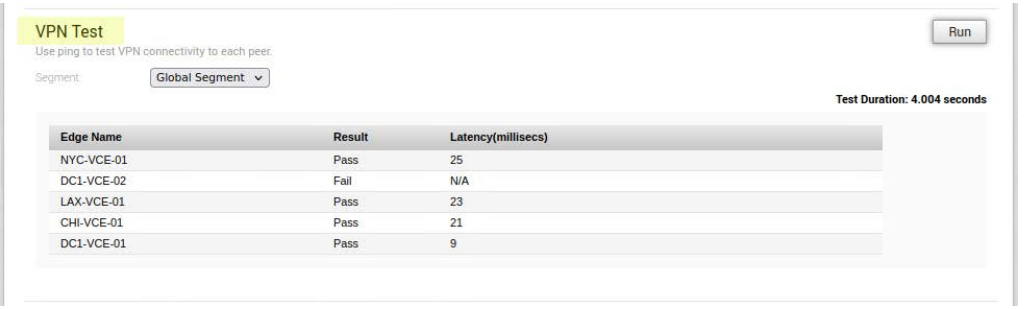
Task 6: Verify the Path for Branch to Branch VPN

You verify the Branch to Branch with Gateways configuration changes.

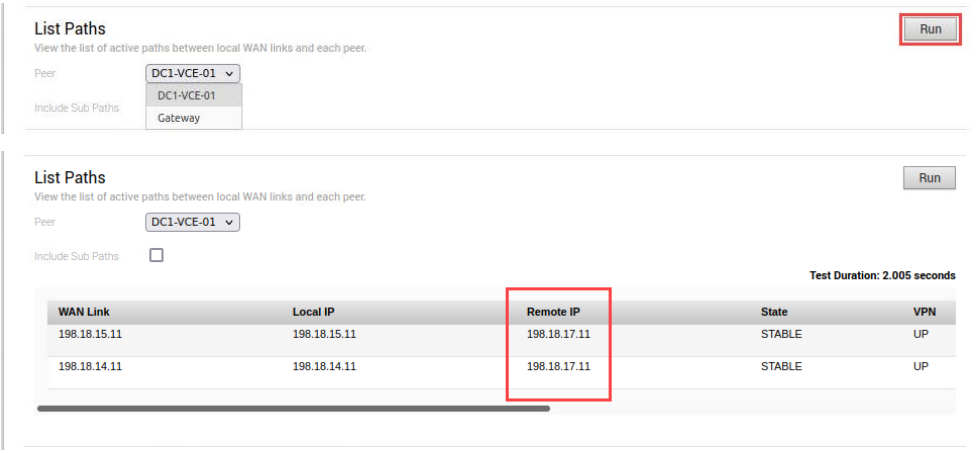
1. Select **Test & Troubleshoot** > **Remote Diagnostics** in the navigation pane on the left.
2. On the Remote Diagnostics page, select one of the edge devices.

   Any site can be tested.
3. Scroll down to VPN Test and click **Run**.

   Verify that VPN connectivity is established between the selected edge and the other sites.



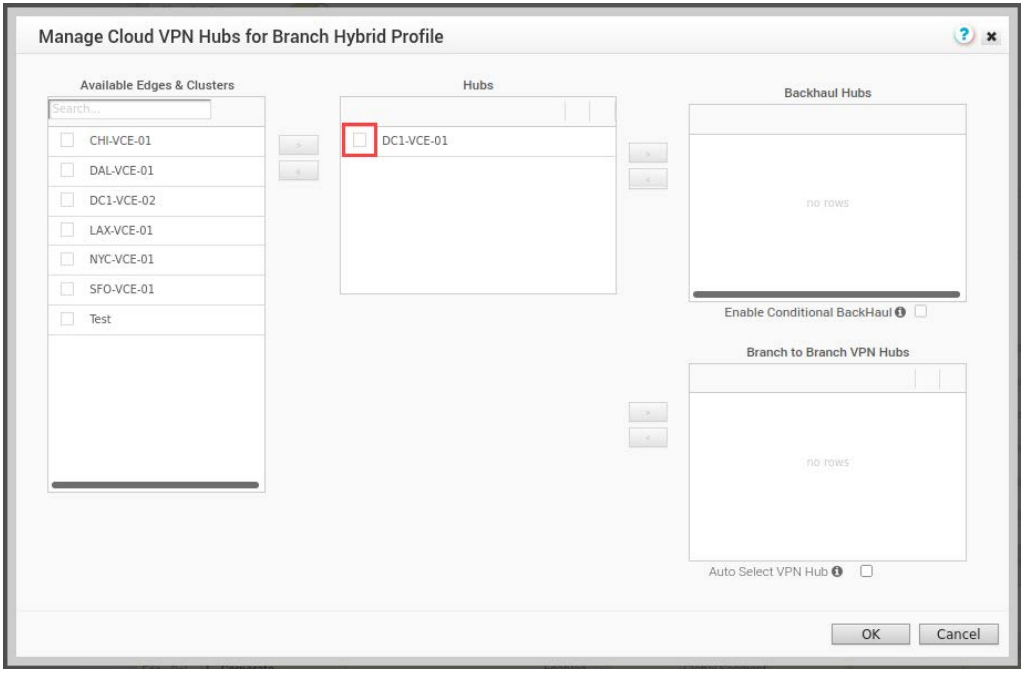
4. (Optional) Run the `List Paths` command.
   a. Select **Test & Troubleshoot** > **Remote Diagnostics** in the navigation pane on the left.
   b. On the Remote Diagnostics page, select the edge device being verified.
   c. Scroll down to List Paths.
   d. From the **Peer** drop-down menu, select the edge device being verified and click **Run**.



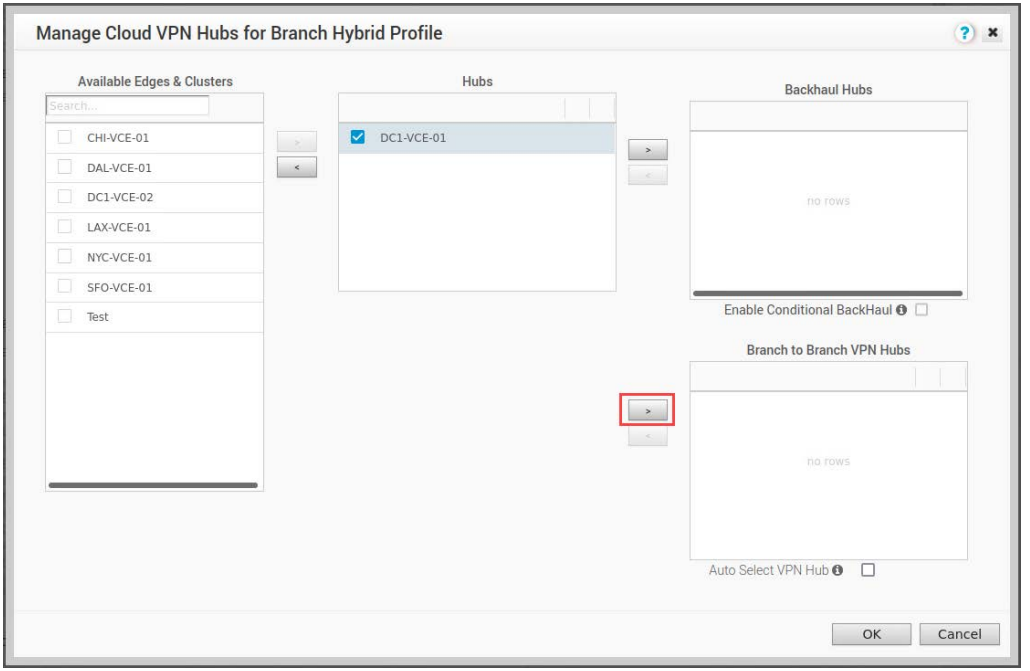
Task 7: Enable Branch to Branch VPN with Hubs

You enable Branch to Branch VPN with hubs. This topology might be beneficial for proofs of concept and trials.

1. Select **Configure** > **Profiles** in the navigation pane on the left.
2. On the Configuration Profiles page, select **Branch Hybrid Profile**.
3. Click the **Device** tab and scroll down to Cloud VPN.
4. Under Branch to Branch VPN, click **Use Hubs for VPN** and then click **Select Hubs**.
5. Select the **DC1-VCE-01** check box.



6. Click the right arrow to add DC1-VCE-01 to the Branch to Branch VPN Hubs column.



7. Click **OK**.
8. Scroll up and click **Save Changes**.

Lab 8 Dynamic Multipath Optimization

Objective and Tasks

Configure business policies that enable deep application recognition and link steering:

1. Ping the Data Center Server from the Chicago Client
2. Run iPerf on Port 5001
3. List the Active Flows
4. Configure a Preferred Option Business Policy
5. Run iPerf on Port 8080
6. Verify That Traffic Follows the Preferred Route

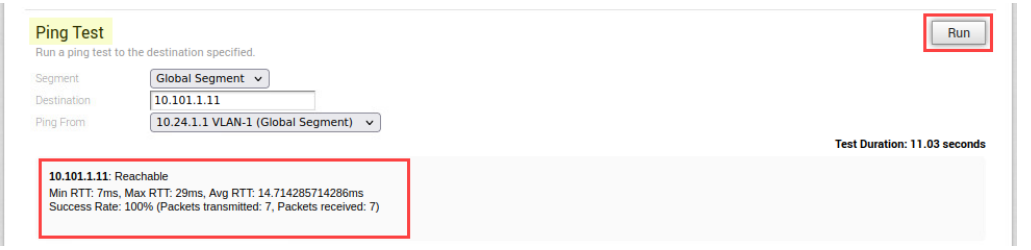
Task 1: Ping the Data Center Server from the Chicago Client

You verify that 10.101.1.11 is reachable from 10.24.1.1 VLAN-1.

1. Log in to VMware SD-WAN Orchestrator.

   Disregard this step if you are already logged in.

2. Select **Test & Troubleshoot** > **Remote Diagnostics** in the navigation pane on the left.
3. From the Remote Diagnostics page, select **CHI-VCE-01**.
4. Scroll down to Ping Test.
5. Enter **`10.101.1.11`** in the **Destination** text box.
6. From the **Ping From** drop-down menu, select **10.24.1.1 VLAN-1 (Global Segment)**.
7. Click **Run**.

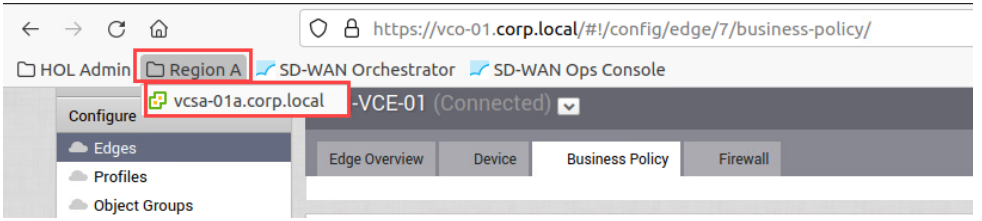


8. Verify that 10.101.1.11 is reachable.

Task 2: Run iPerf on Port 5001

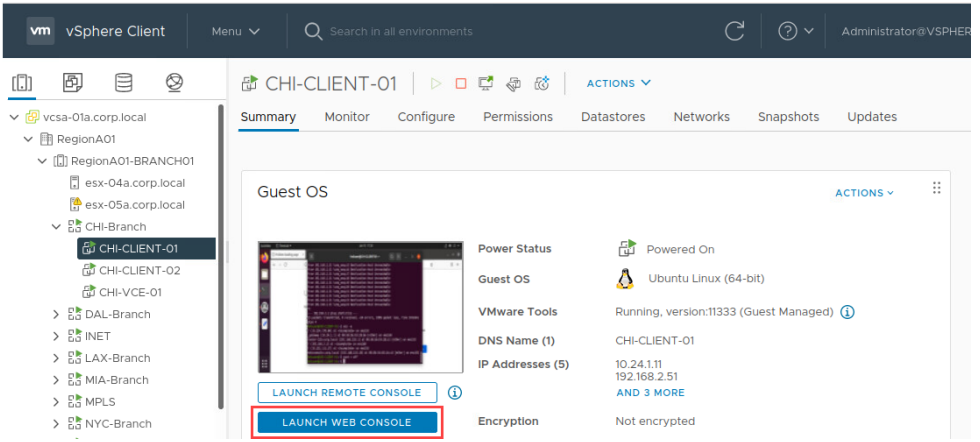
You connect to the vCenter Server system and run iPerf on the Chicago client and the data center server, using 5001 as the port.

1. Connect to your vCenter Server system.
   a. From the taskbar, open the Firefox browser.
   b. Click the **Region A** bookmark folder and select the **vcsa-01a.corp.local** bookmark.

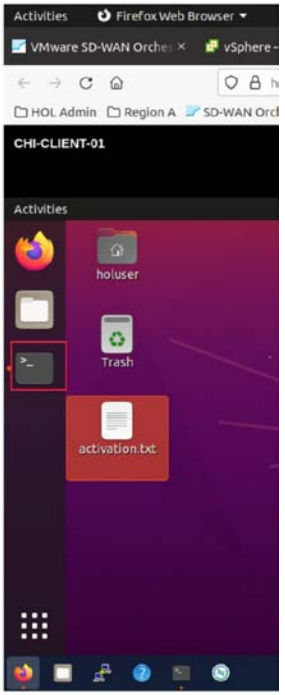


   c. Log in to vCenter Server.
      - User name: administrator@vsphere.local
      - Password: VMware1!

2. From the vCenter Server system, access the Chicago client desktop.
   a. Select **RegionA01 Data Center** > **RegionA01-BRANCH01** > **CHI-Branch vApp** > **CHI-CLIENT-01**.
   b. Click **LAUNCH WEB CONSOLE**.



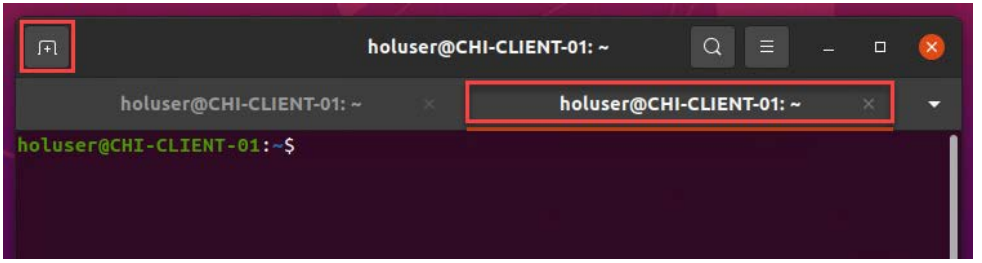
3. Log in to the DC1 server using SSH.
    a. From the taskbar in the CHI-CLIENT-01 desktop, open a Terminal window.



    b. Run the `ssh root@dc1-server-01.corp.local` command.
    c. At the prompt, enter **`yes`** to accept the ECDSA key fingerprint and continue connecting to the server.
    d. At the prompt, enter **`VMware1!`** as the password.
4. Run iPerf.
    a. In the Terminal window, run the `cd /root` command.
    b. Run the `./start-server.sh` script.

5. Run iPerf from the CHI-CLIENT-01 desktop.

   a. In the Terminal window, click the plus sign (+) icon in the top-left corner to open a new tab.



   b. Run the `iperf -c 10.101.1.11 -p 5001 -t 5000` command.

      In this test command, -c is the client, -p is the port (TCP), and -t is the timer.

      The iPerf command does not need to run completely before you continue to the next task.

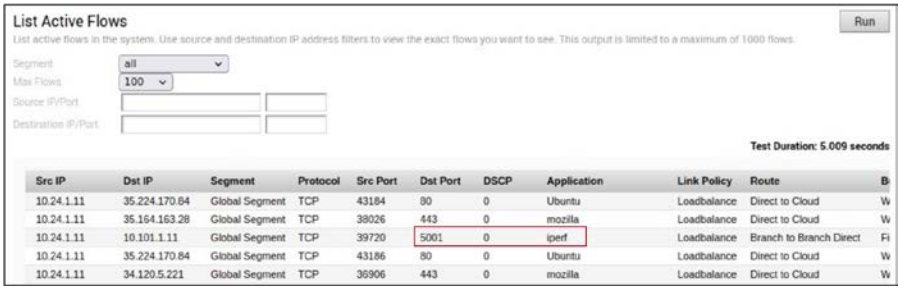
   c. If iPerf does not respond, run the `iperf3 -s -p 5001` command from the DC1 tab.

      A failure to respond might be the result of a reachability issue between the Chicago client and the DC server. Alternatively, the DC1 iPerf service is not running on port 5001.

Task 3: List the Active Flows

You verify the active flows from CHI-VCE-01 to ensure that the traffic of an application flows smoothly between the sites.

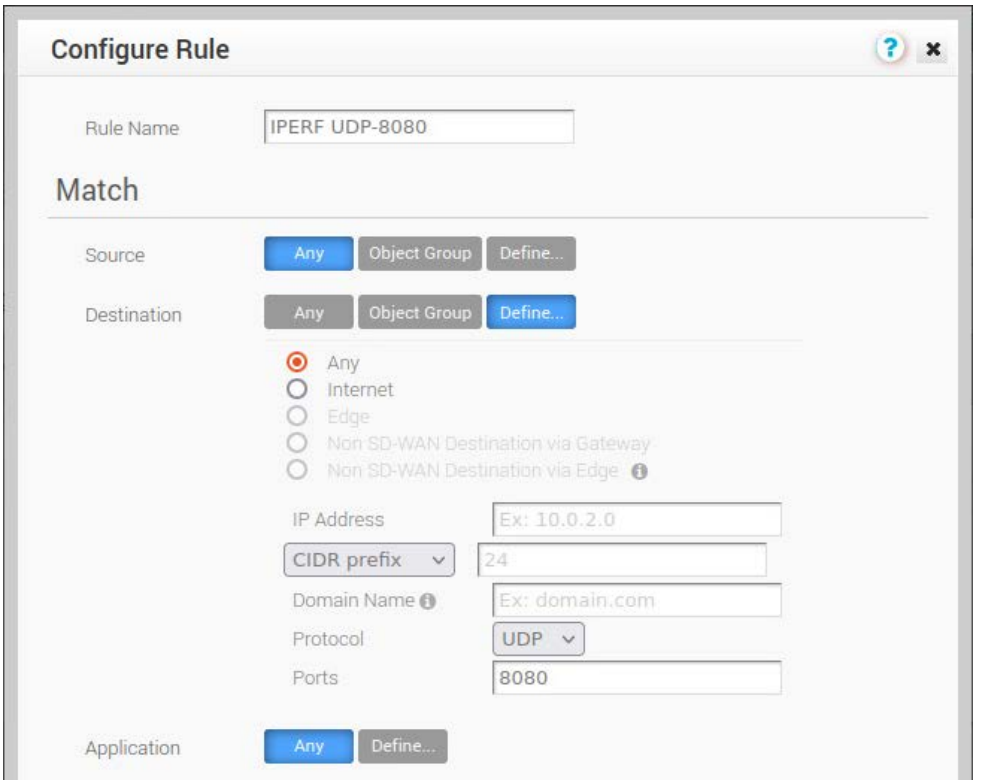
1. Select **Test & Troubleshoot** > **Remote Diagnostics** in the navigation pane on the left.
2. From the Remote Diagnostics page, select **CHI-VCE-01**.
3. Scroll down to List Active Flows and click **Run**.
4. Verify that deep application recognition recognizes the TCP port 5001 as iPerf.



Task 4: Configure a Preferred Option Business Policy

You configure a business policy to influence link steering. You verify that traffic follows the preferred route.

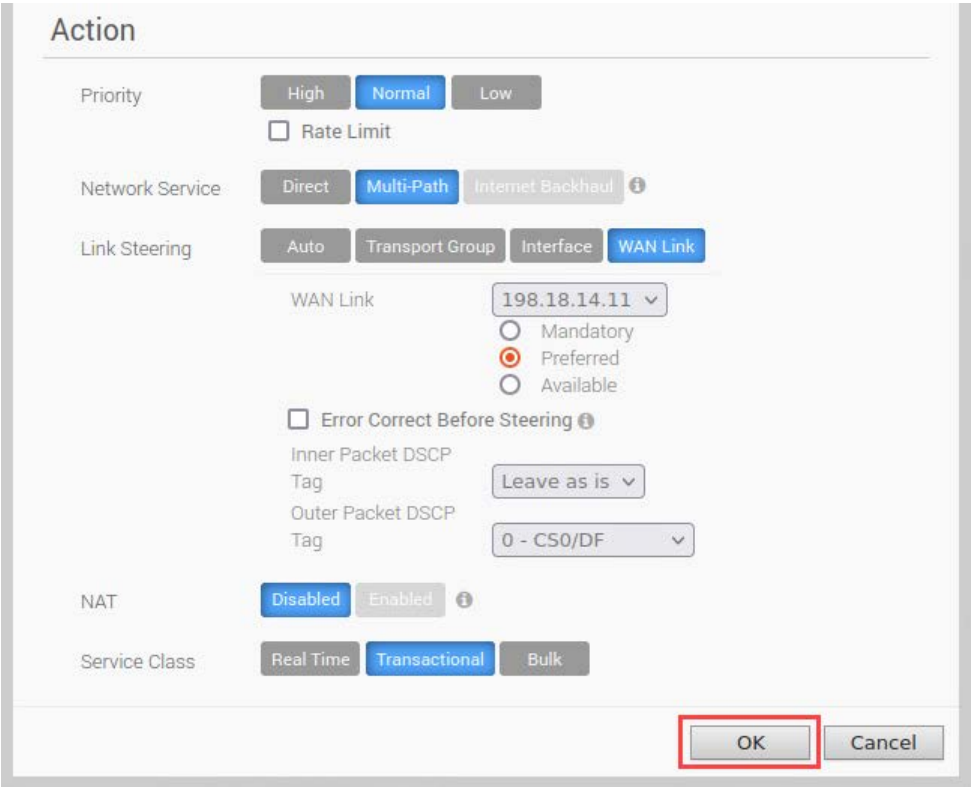
1. Click **Configure** > **Edges** in the navigation pane on the left.
2. On the Edges page, select **CHI-VCE-01**.
3. Click the **Business Policy** tab.
4. Click **New Rule**.
5. Configure the business rule.
   a. Enter **`IPERF UDP-8080`** in the **Rule Name** text box.
   b. Next to Source, select **Any**.
   c. Next to Destination, select **Define** and click **Any**.
   d. From the **Protocol** drop-down menu, select **UDP**.
   e. Enter **`8080`** in the **Ports** text box.



   f. Next to Link Steering, click **WAN Link**.
   g. Select **198.18.14.11** from the **WAN Link** drop-down menu.

h. Under WAN Link, click **Preferred**.

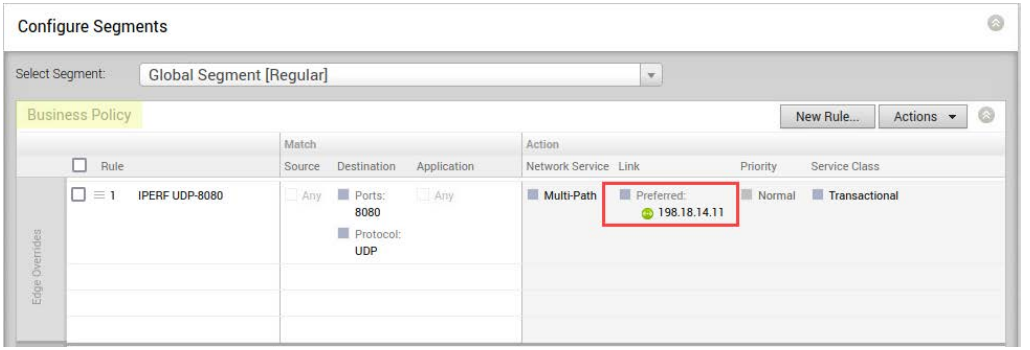
i. Click **OK**.



j. Click **Save Changes**.

6. Review the new rule.

   Traffic now follows the preferred 198.18.14.11 route.



Task 5: Run iPerf on Port 8080

You connect to the vCenter Server system and run iPerf on the Chicago client and data center server, using 8080 as the port.

1. Connect to your vCenter Server system.
   a. From the taskbar, open the Firefox browser.
   b. Click the **Region A** bookmark folder and select the **vcsa-01a.corp.local** bookmark.
   c. Log in to vCenter Server.
      - User name: administrator@vsphere.local
      - Password: VMware1!
2. From the vCenter Server system, access the Chicago client desktop.
   a. Select **RegionA01 Data Center** > **RegionA01-BRANCH01** > **CHI-Branch vApp** > **CHI-CLIENT-01**.
   b. Click **LAUNCH WEB CONSOLE**.
3. Initiate traffic from the Chicago branch to the DC1 server on UDP port 8080.
   a. From the CHI-CLIENT-01 desktop, open a Terminal window.
   b. Run the `iperf -c 10.101.1.11 -p 8080 -t 5000 -u` command to start an iPerf test for the DC1 server.

      You ran iPerf on the DC1 server machine in an earlier lab task.

Task 6: Verify That Traffic Follows the Preferred Route

You start live monitoring to verify that traffic follows the route configured in the business policy.

1. Select **Monitor** > **Edges** in the navigation pane on the left.
2. On the Edges page, select **CHI-VCE-01**.
3. Click the **Transport** tab.
4. Click **Start Live Monitoring**.
5. Select the **Show TCP/UDP Details** check box.
6. Review the graph to verify that UDP traffic on port 8080 uses the preferred 198.18.14.11 link.