Introduction to Versa Director

The Versa Networks lab environment consists of a fixed, pre-configured topology that will allow you to explore, configure, and manage Versa Networks CPEs by using Versa Director, the central management and orchestration platform for a Versa Secure SD-WAN solution. After completing this lab, you will be able to:

- Identify the functions of the main Versa Director tabs
- Navigate through the Versa Director environment to accomplish some basic tasks

In this lab, you will be assigned a single CPE device (Branch device) for configuration and monitoring.

The lab environment is accessed through Amazon Workspaces. You should have received an email to allow you to register your Amazon Workspaces account and set your password.

NOTE: It is common for the Amazon Workspaces email to be sent to the spam/junk folder. If you have not received the registration email, check those folders.

The remote desktop connection opens a remote workstation, where you will use various tools to navigate and configure the lab environment. The main tool you will use in this lab is Versa Director. Versa Director can be accessed by opening the Google Chrome browser on the Remote Desktop. There is a bookmark to the Versa Director device in the Google Chrome bookmark bar.

This lab environment is a shared environment. There may be up to 24 students in the environment. Each student has their own remote desktop, but the Versa Director is shared. Because of the shared environment, you may see configuration templates, device groups, workflows, and devices that other students have created, or that have been pre-provisioned within Versa Director. It is important that you only modify the configuration components that are assigned to you by your instructor.

During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not be the same, etc.) Do not be alarmed if your results vary slightly from the results shown in the lab guide. The important thing is that the lab functions in the desired manner.

Look for these hints to help you in the labs

This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

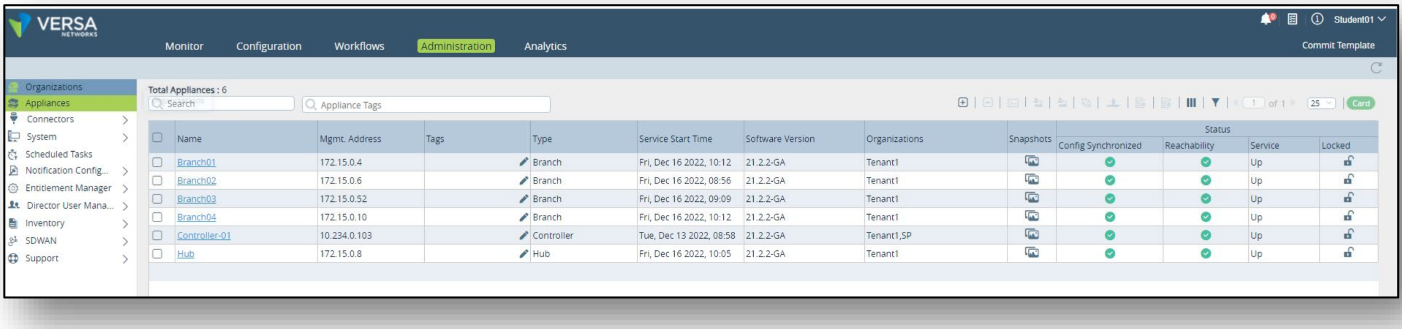
The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

Now that we’ve discussed what is expected, let’s get started!

Exercise 1: Identify the main components of Versa Director

Please refer to the Lab Access Guide for instructions on how to connect to the remote lab environment.

In the remote landing station, open the Google Chrome browser and log into Versa Director. You should be placed into the *Administration > Appliances* dashboard of Versa Director. There are 5 tabs at the top of the Versa Director user interface. Each of the tabs represents a set of dashboards to perform certain tasks, such as monitoring devices, managing configuration components on Versa Director, and creating and managing different components. The currently selected tab is highlighted automatically:



Total Appliances : 6

☐	Name	Mgmt. Address	Tags	Type	Service Start Time	Software Version	Organizations	Snapshots	Status			
									Config Synchronized	Reachability	Service	Locked
☐	Branch01	172.15.0.4		Branch	Fri, Dec 16 2022, 10:12	21.2.2-GA	Tenant1		✓	✓	Up	
☐	Branch02	172.15.0.6		Branch	Fri, Dec 16 2022, 08:56	21.2.2-GA	Tenant1		✓	✓	Up	
☐	Branch03	172.15.0.52		Branch	Fri, Dec 16 2022, 09:09	21.2.2-GA	Tenant1		✓	✓	Up	
☐	Branch04	172.15.0.10		Branch	Fri, Dec 16 2022, 10:12	21.2.2-GA	Tenant1		✓	✓	Up	
☐	Controller-01	10.234.0.103		Controller	Tue, Dec 13 2022, 08:58	21.2.2-GA	Tenant1,SP		✓	✓	Up	
☐	Hub	172.15.0.8		Hub	Fri, Dec 16 2022, 10:05	21.2.2-GA	Tenant1		✓	✓	Up	

Many times there are multiple ways to navigate between windows and dashboards.

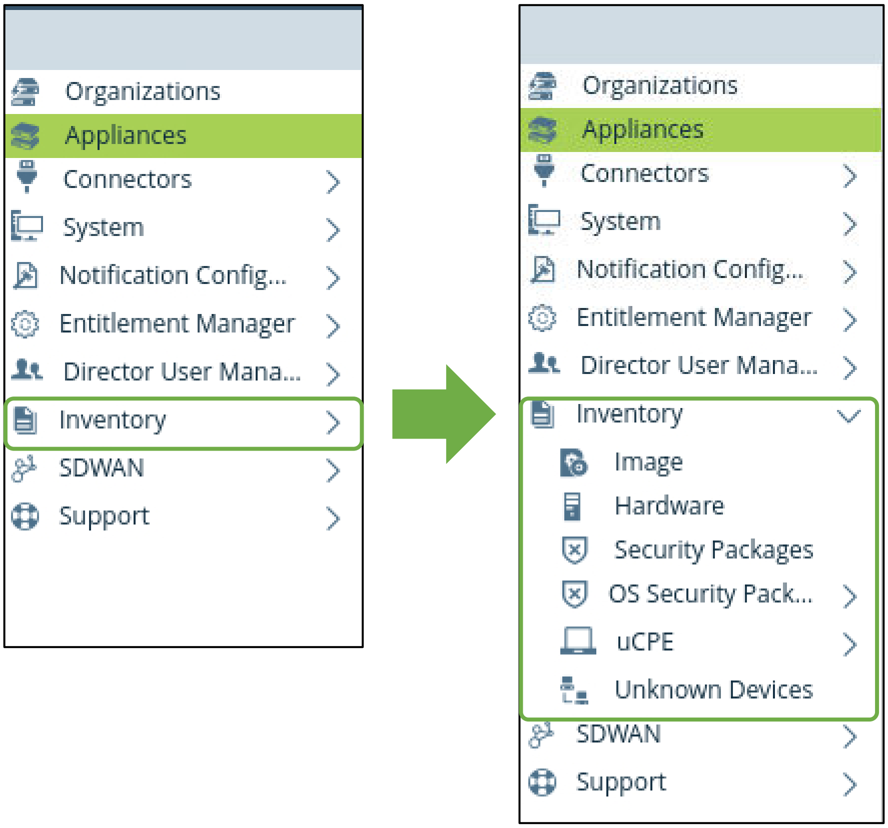
The Appliances table of the Administration dashboard lists all of the deployed appliances in the SD-WAN environment. You can click on a device in the list to navigate directly to that device's configuration and monitoring dashboard. You can also navigate to the individual device configuration and management dashboard by clicking the Monitor tab.

The main tabs are:

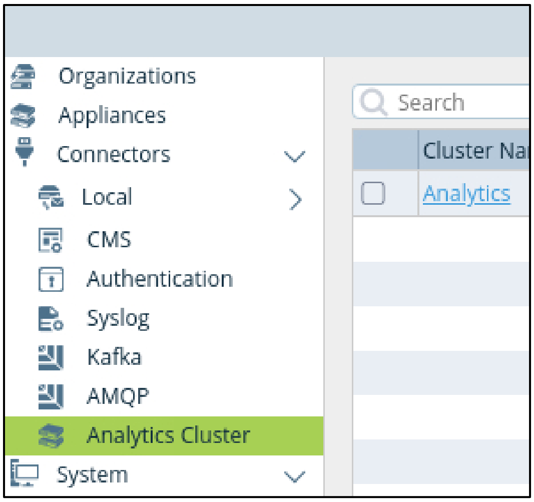
- **Monitor**: Provides access to device specific statistics, status, and configurations
- Configuration: Provides access to configuration components stored on Versa Director, including Device Groups, Bind Data, and Device and Service Templates
- **Workflows**: Provides access to create new workflows and to view and update existing workflows
- **Administration**: Provides access to SD-WAN environment configuration, including device inventory, deployment information, overlay configuration, external connectors, organization definition and configuration, user management, and licensing. It also provides access to the software management features, such as downloaded OS packages, Security Packages (Spacks), etc.
- **Analytics**: Opens the Versa Analytics GUI within Versa Director

Because you’re already here, let’s explore the *Administration* tab.

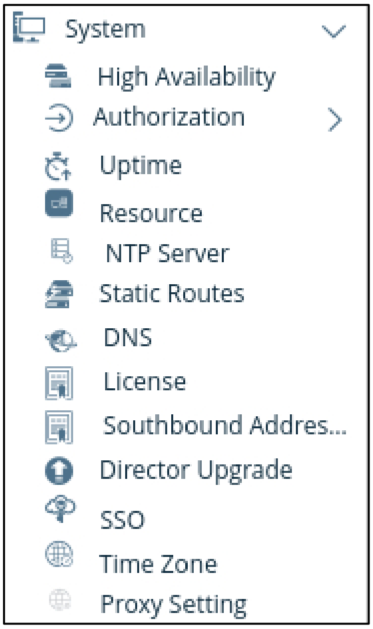
The menu on the left displays the main categories of administration information. Wherever you see a **>** symbol, this means that the category can be expanded:



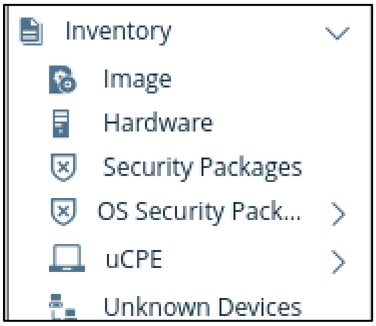
Expand the *Connectors* menu. The Connectors menu lists the different types of connections that are available to other systems, such as Analytics clusters, authentication servers, syslog servers, and so forth. If you click on the Analytics Cluster menu item, you’ll see a table that lists all of the Analytics connectors on the system (which is currently one). The Analytics connector provides the information needed for Versa Director to communicate with the Versa Analytics node or cluster.



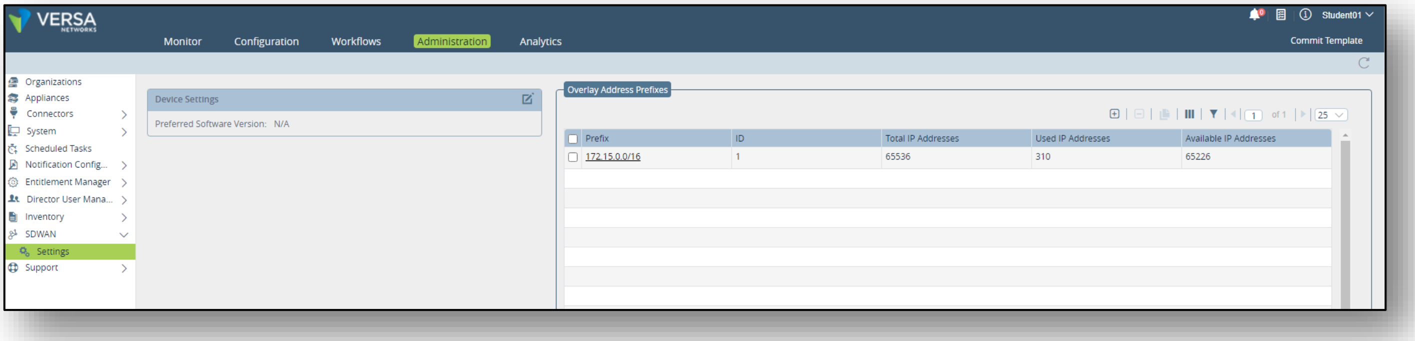
Next expand the *System* menu. The System menu is where Versa Director system information is configured, including Versa Director High Availability, NTP servers, the Versa Director license, DNS settings, Time Zone settings, and so forth. It's important to remember that the Versa Director is a computer system that may need to perform functions for the local processes, including DNS lookups and local routing. These settings are NOT for the SD-WAN systems. These settings are for the local Versa Director system.



Expand the *Inventory* menu. Here you will see dashboards to manage the software images stored on Versa Director, the current device inventory, which includes devices that have been created in the Versa Director database (Hardware), Security Package management, OS Security package management, and uCPE images. The Unknown Devices dashboard lists appliances that have been onboarded but that have a serial number that does not match a device serial number in the Hardware table.



The *SDWAN Settings* dashboard is where the SD-WAN overlay address scheme is defined.



Preferred Software Version: N/A

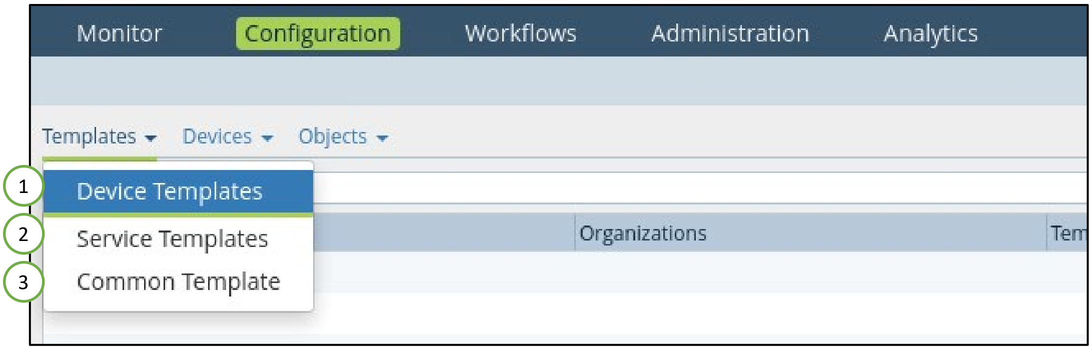
☐	Prefix	ID	Total IP Addresses	Used IP Addresses	Available IP Addresses
☐	172.15.0.0/16	1	65536	310	65226

Exercise 3: Explore Versa Director

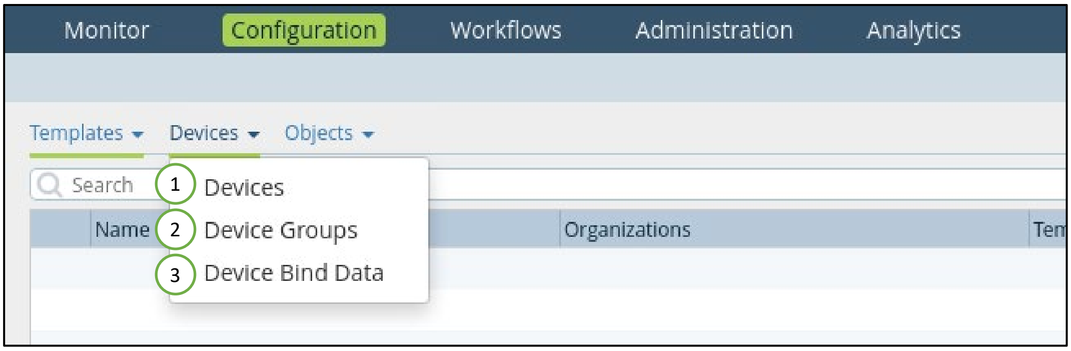
In this lab exercise, you will explore various dashboards of the Versa Director platform and answer questions related to the areas that you explore.

Task: Navigate to the *Configuration* tab. Use the GUI to find where configuration templates are stored.

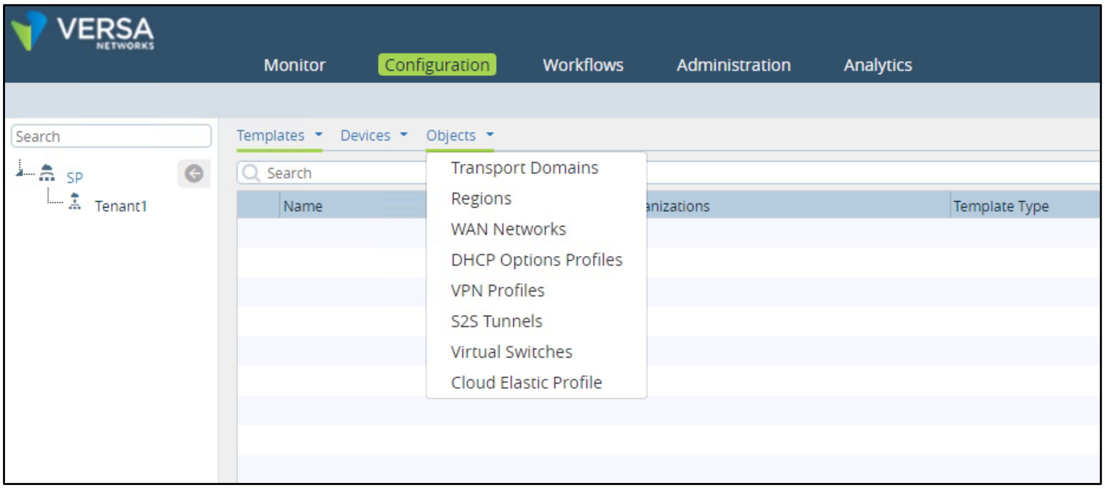
If you are assigned Branch 110, the template created for your device probably has a name related to Branch 110



Task: Use the GUI to show where the device related configuration is stored.

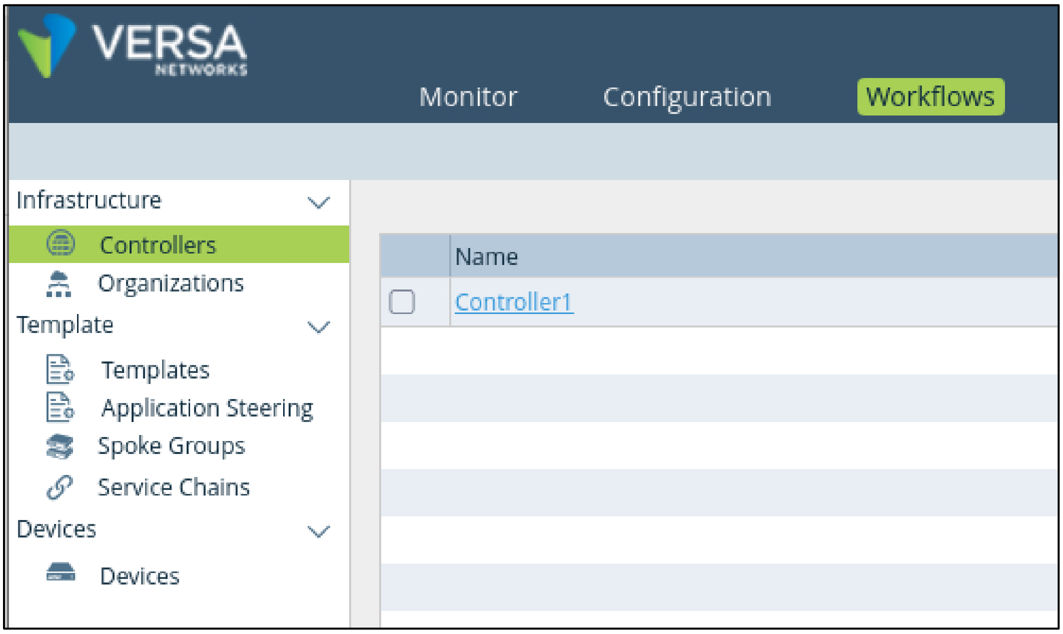


Task: Use the GUI view the different configuration objects related to the network and SD-WAN environment.

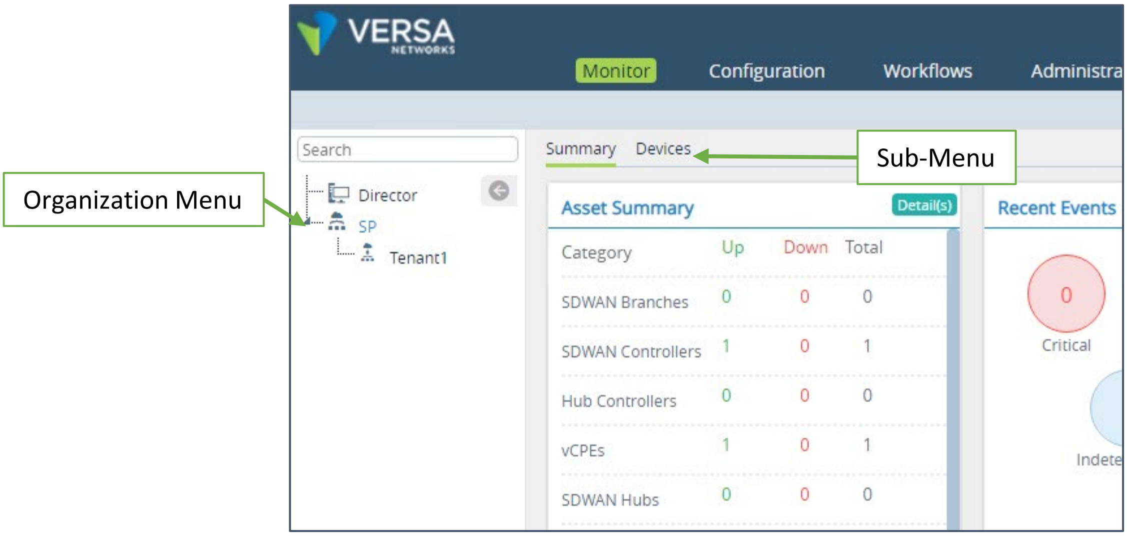


Task: A workflow is a step-by-step process to perform a task. In Versa Director, a workflow is a step-by-step process to create something, similar to a configuration wizard. The process or settings used are saved so that the process can be repeated, or so that settings in the original process can be changed and re-used to update or modify the object that the workflow created.

Navigate to the *Workflows* tab. In the *Workflows* tab, examine the different types of workflows that can be used to create configuration components.



Task: Open the *Monitor* tab. In the *Monitor* tab there is a left-side menu and a sub-menu at the top of the table displayed on the page.



Asset Summary

Category	Up	Down	Total
SDWAN Branches	0	0	0
SDWAN Controllers	1	0	1
Hub Controllers	0	0	0
vCPEs	1	0	1
SDWAN Hubs	0	0	0

With the *SP* organization selected, click on the *Devices* tab to display devices that are managed by the SP organization.

Click on the *Tenant1* organization. With the *Tenant1* organization selected, click on the *Devices* tab to display devices that are managed by the Tenant1 organization.

Question: What differences do you see between the SP organization view and the Tenant1 organization view within the corresponding Devices tables?

____

____

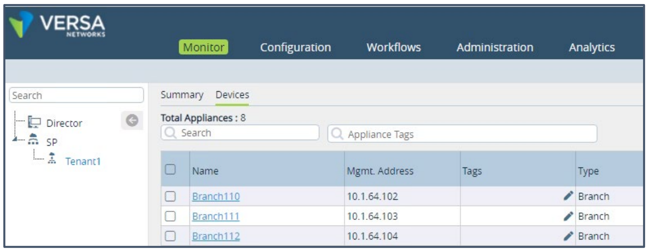
____

Task: Click on your branch device in the Tenant1 Devices table.

Question: How did the main menu bar change when you opened your branch device?

____

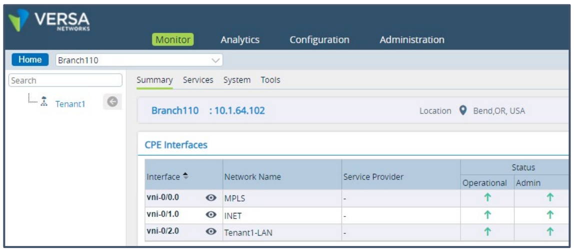
____



Total Appliances : 8

☐	Name	Mgmt. Address	Tags	Type
☐	Branch110	10.1.64.102		Branch
☐	Branch111	10.1.64.103		Branch
☐	Branch112	10.1.64.104		Branch

Before



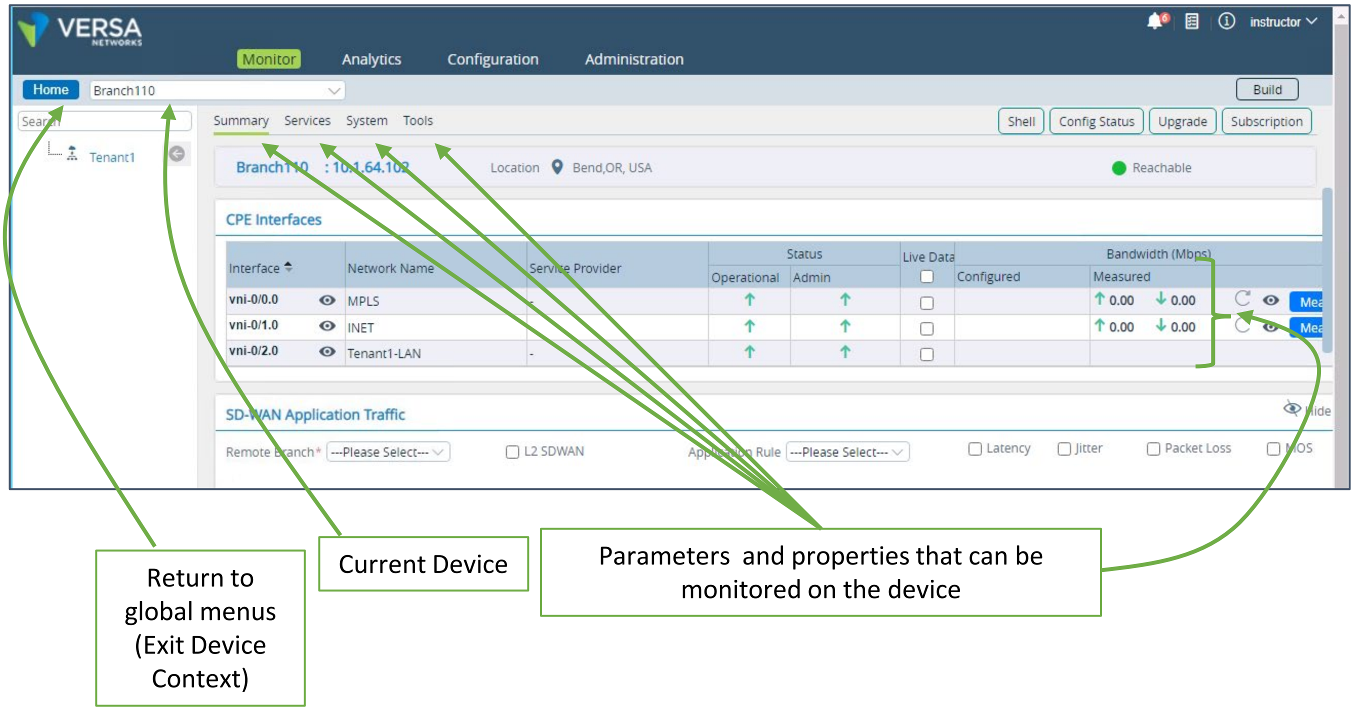
Branch110 : 10.1.64.102 Location Bend,OR, USA

CPE Interfaces

Interface	Network Name	Service Provider	Status	
			Operational	Admin
vni-0/0.0	MPLS	-	↑	↑
vni-0/1.0	INET	-	↑	↑
vni-0/2.0	Tenant1-LAN	-	↑	↑

After

Key Differences: Device Context Mode (also called Appliance Context Mode)



Interface		Network Name	Service Provider	Status		Live Data	Bandwidth (Mbps)	
				Operational	Admin	□	Configured	Measured
vni-0/0.0	👁	MPLS	-	↑	↑	□		↑ 0.00 ↓ 0.00
vni-0/1.0	👁	INET		↑	↑	□		↑ 0.00 ↓ 0.00
vni-0/2.0	👁	Tenant1-LAN	-	↑	↑	□		

Return to global menus (Exit Device Context)

Current Device

Parameters and properties that can be monitored on the device

Task: Explore the *Services* options in Device/Appliance Context mode.

Open the *Services* tab for your device. There are 2 main categories of services that can be viewed: Services and Networking. Take a few minutes to explore the type of information available in some of the Services and Networking dashboards.

What type of information is available in the Services section?

____

____

____

What type of information is available in the Networking section?

____

____

____

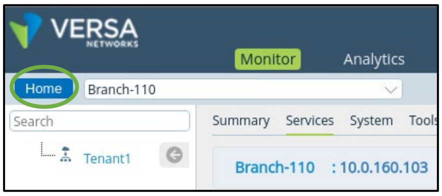
Is the information listed above for an organization, or for a specific device?

____

Task: Click the *Home* button next to your device name. What happens to the display and top menu bar?

____

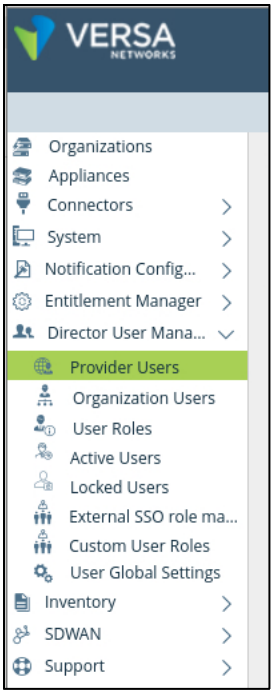
____



Clicking the *Home* button takes you back to the main Versa Director system and dashboards, and exits the device/appliance context mode.

Task: Explore the *Director User Management* menus.

Navigate to the global *Administration* tab in Versa Director (make sure you are no longer in the Device/Appliance Context mode). In the *Administration* tab, locate the *Director User Management* menu on the left side and expand the menu. Select the *Provider Users* from the menu.



Question: What uses are visible in the table?

____

____

Question: What role is assigned to your username?

____

____

Click your username to open the *Edit Provider User* dialog.

Question: What is the Landing Page configured for your user?

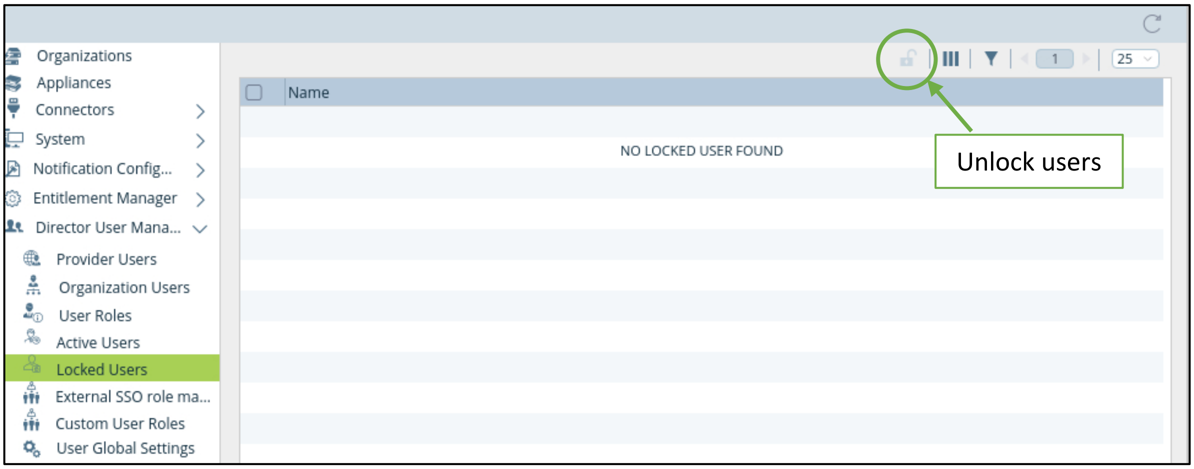
____

____

Do you remember what dashboard you were presented with when you first logged on?

Click *Cancel* to close the dialog – do not change any settings.

Click on the Locked Users menu item. This is where user accounts that have been locked out of the system due to repeated wrong passwords are listed. To unlock a user, you select the user from the list and click the unlock button in the top right. Currently there shouldn't be any locked users on the list.



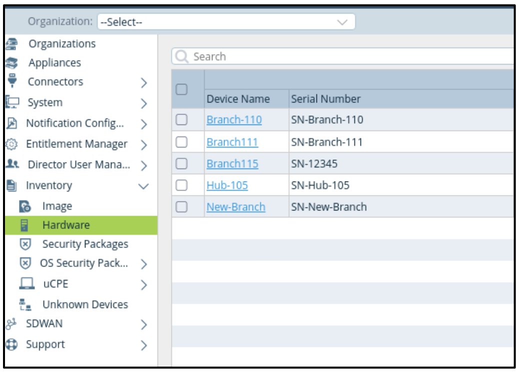
□	Name

NO LOCKED USER FOUND

Unlock users

Task: Explore the *Inventory* menu.

Expand the *Inventory* menu, then select *Image* from the list. This is where VOS software images are stored when they are downloaded to Versa Director.



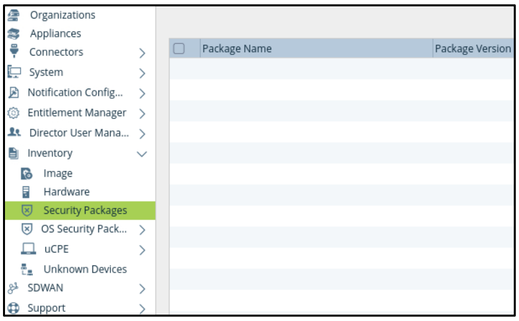
Organization: --Select--

□	Device Name	Serial Number
□	Branch-110	SN-Branch-110
□	Branch111	SN-Branch-111
□	Branch115	SN-12345
□	Hub-105	SN-Hub-105
□	New-Branch	SN-New-Branch

Note that there is no connectivity status on the Hardware table, but the Appliance table has a connectivity status.

Select the *Hardware* menu. This is where devices that have been created in Versa Director are stored. It's important to remember that when you create a device in Versa Director, it is stored as an object in the Versa Director database. The Hardware table lists devices that have been created in Versa Director. The Appliances menu table lists devices that have been deployed and are active in the network. When a device in the Hardware table is onboarded or deployed in the network, a corresponding Appliance is created in the Appliance table – but only AFTER the device is successfully onboarded and is live.

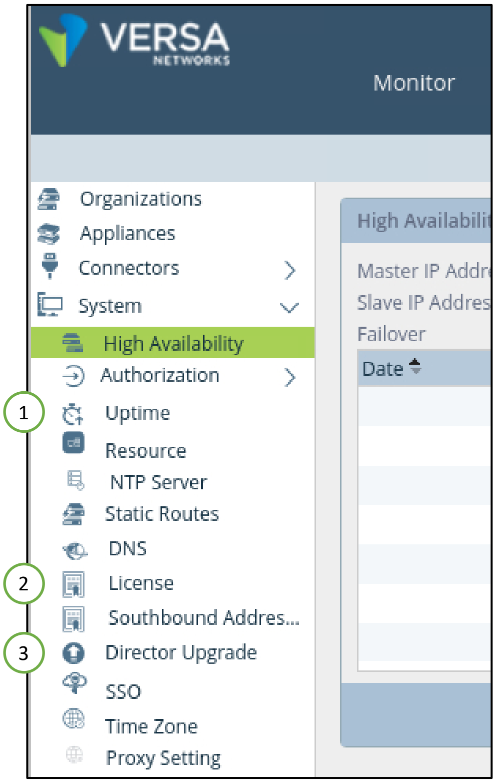
Select the *Security Packages* menu. This is where Security Package downloads are stored and listed in Versa Director. These can be used to update security package information on devices in the network.



□	Package Name	Package Version

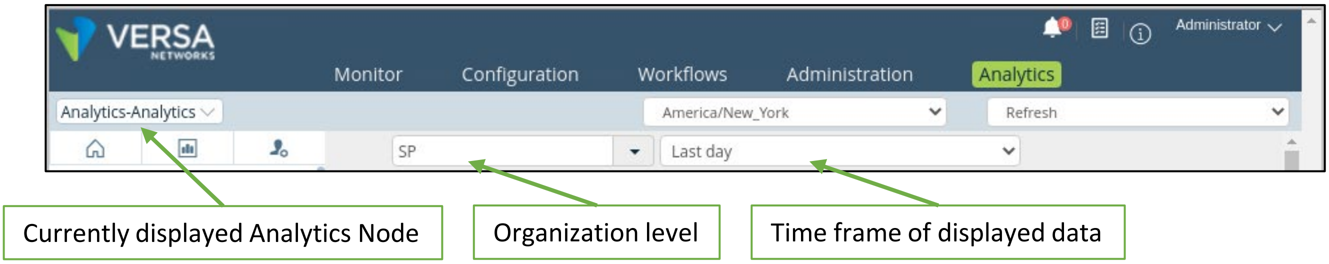
Task: Explore the *System* menus.

Expand the System menu. In the System menu. Explore each of the highlighted areas to see what information can be found there.



Task: Explore the Analytics dashboard.

The Analytics tab opens the Versa Analytics dashboard. Currently there is a single Versa Analytics node deployed in the network. However, when multiple Versa Analytics nodes are configured and linked to Versa Director, you can select which Versa Analytics node is displayed by choosing the node from the dashboard menu.



Task: Explore the Versa Analytics Dashboards

The left menu is divided into 2 main sections: Dashboards and Logs. The Dashboards display historical statistic information gathered from devices in the SD-WAN. The Logs section displays the logs that are sent from processes that run on the end devices.

What are the main dashboards available to view statistics?

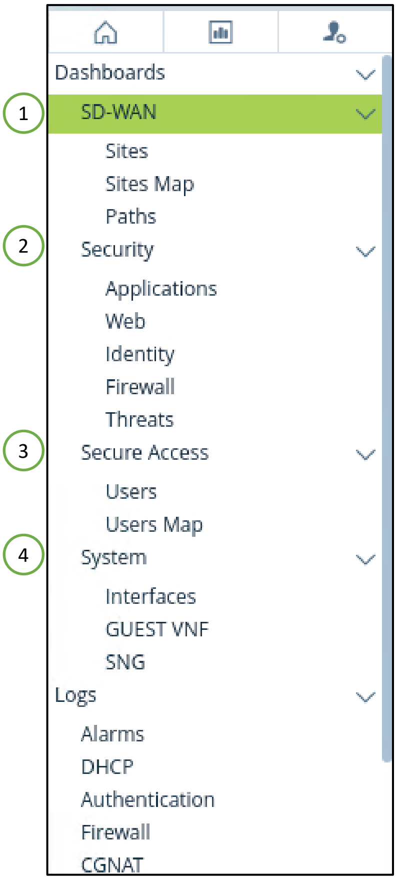
____

____

____

____

In Versa Analytics, you can select the main Dashboard title to display summary information related to that dashboard topic. You can also select the sub-menus for more specific information.

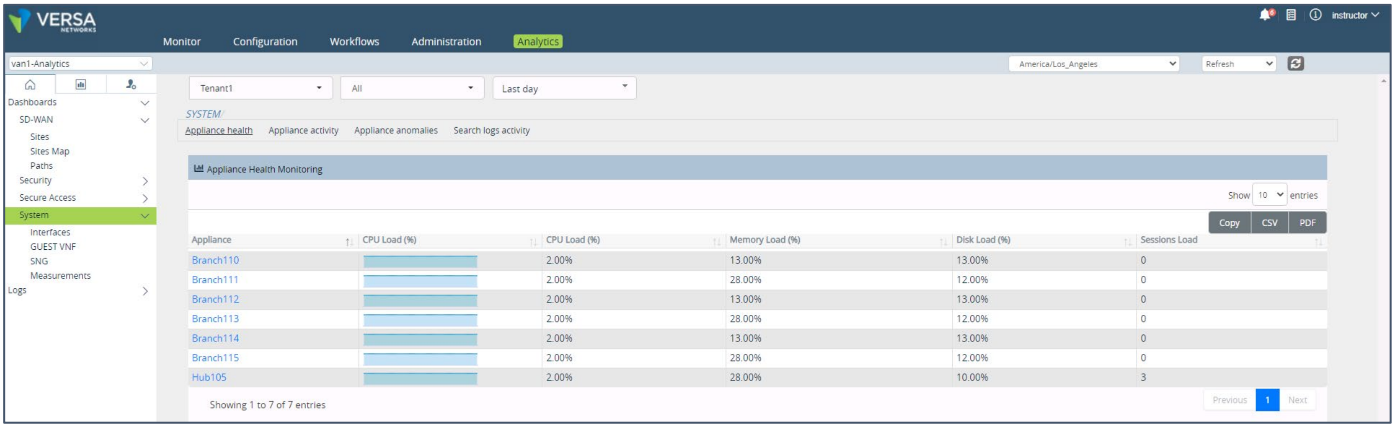


Each dashboard has sub-components that display graphs and charts related to the SD-WAN. Take a few minutes to explore the dashboards and sub-tabs within each dashboard entry. Please note that because this is a lab environment there may be many charts and graphs that don't contain any information because there isn't any production traffic running on the network.

Select the System dashboard. What information is shown on the main System dashboard?

____

____



Appliance Health Monitoring

Appliance	CPU Load (%)	CPU Load (%)	Memory Load (%)	Disk Load (%)	Sessions Load
Branch110		2.00%	13.00%	13.00%	0
Branch111		2.00%	28.00%	12.00%	0
Branch112		2.00%	13.00%	13.00%	0
Branch113		2.00%	28.00%	12.00%	0
Branch114		2.00%	13.00%	13.00%	0
Branch115		2.00%	28.00%	12.00%	0
Hub105		2.00%	28.00%	10.00%	3

Showing 1 to 7 of 7 entries

STOP **STOP!** Notify your instructor that you have completed this lab.

Versa Workflows and Templates

The Versa Networks lab environment consists of a fixed, pre-configured topology that will allow you to explore, configure, and manage Versa Networks CPEs by using Versa Director, the central management and orchestration platform for a Versa Secure SD-WAN solution. After completing this lab, you will be able to:

- Create configuration templates using template workflows;
- Create device groups;
- Associate a device to a configuration template by assigning it to a device group; and
- Verify the services enabled in a configuration template.

In this lab, you will be assigned a single CPE device (Branch device) for configuration and monitoring.

The lab environment is accessed through Amazon Workspaces. You should have received an email to allow you to register your Amazon Workspaces account and set your password.

NOTE: It is common for the Amazon Workspaces email to be sent to the spam/junk folder. If you have not received the registration email, check those folders.

The remote desktop connection opens a remote workstation, where you will use various tools to navigate and configure the lab environment. The main tool you will use in this lab is Versa Director. Versa Director can be accessed by opening the Google Chrome browser on the Remote Desktop. There is a bookmark to the Versa Director device in the Google Chrome bookmark bar.

This lab environment is a shared environment. There may be up to 24 students in the environment. Each student has their own remote desktop, but the Versa Director is shared. Because of the shared environment, you may see configuration templates, device groups, workflows, and devices that other students have created, or that have been pre-provisioned within Versa Director. It is important that you only modify the configuration components that are assigned to you by your instructor.

During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not be the same, etc.) Do not be alarmed if your results vary slightly from the results shown in the lab guide. The important thing is that the lab functions in the desired manner.

Look for these hints to help you in the labs

This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

Now that we've discussed what is expected, let's get started!

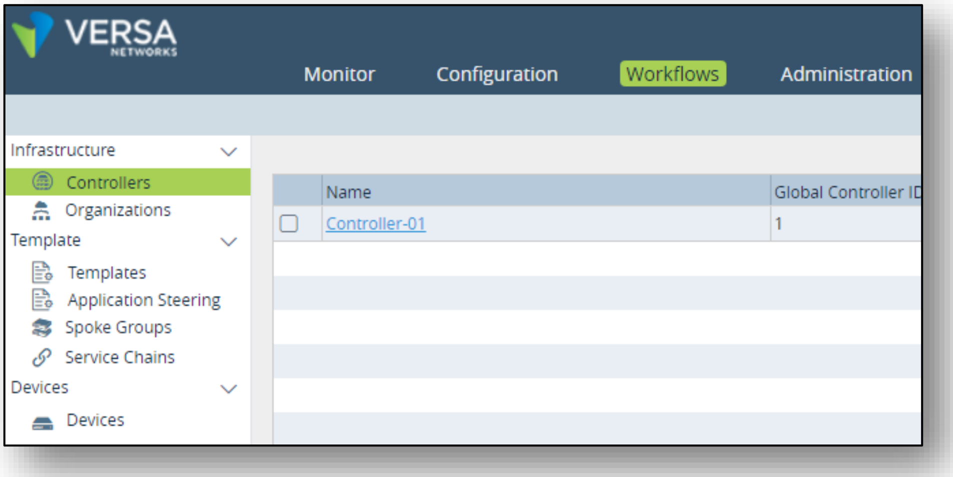
Exercise 1: Examine the Workflow Environment

In the following lab exercises, you will:

- Identify the types of workflows available in Versa Director
- Examine the structure of a Controller workflow
- Examine the structure of an Organization workflow

Please refer to the Lab Access Guide for instructions on how to connect to the remote lab environment.

In the remote landing station, open the Google Chrome browser and log into Versa Director. In Versa Director, open the Workflows dashboard. On the left-side menu there are 3 main categories of workflows. Expand all 3 categories so that the sub-components are visible. Examine sub-components in the diagram below.



□	Name	Global Controller ID
□	Controller-01	1

Each of these categories of objects or components is related to a type of object within Versa Director:

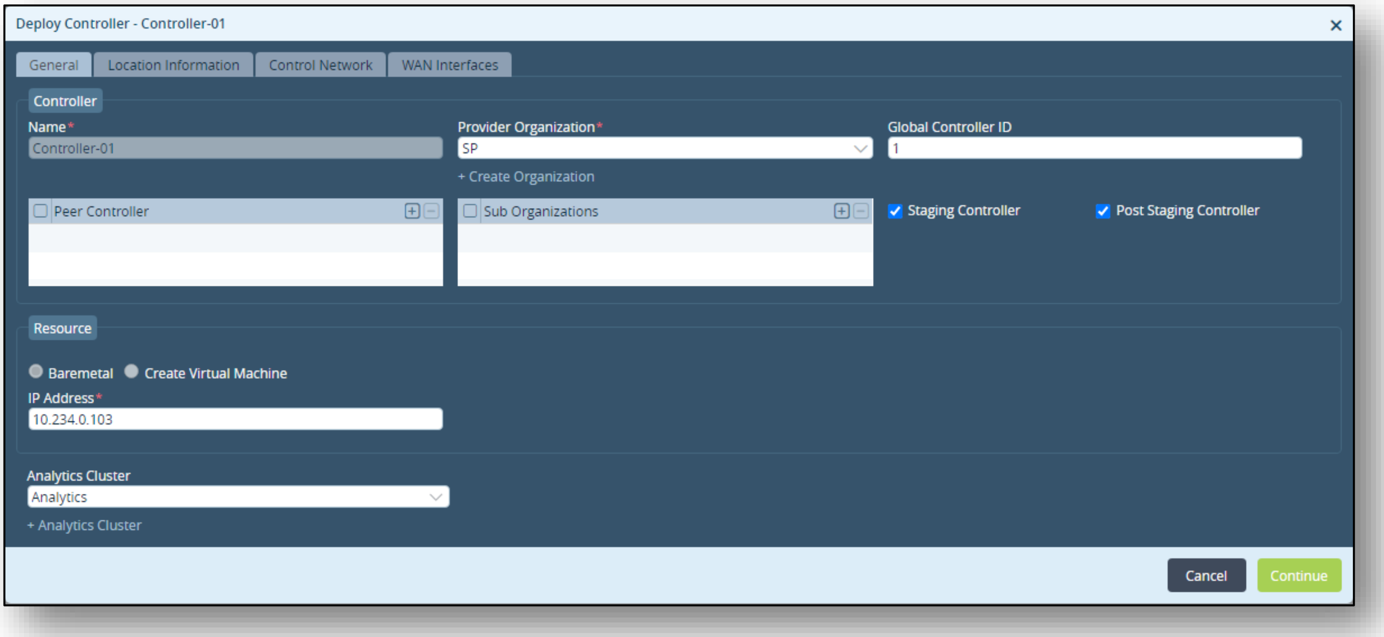
- Infrastructure Workflows are used to help create controllers and organizations.
- Template Workflows are used to create different template-based components.
- Device Workflows are used to create branch device (CPE) components.

There are already a few workflows saved in Versa Director that were used to create components in the lab environment. These include:

- A Controller workflow
- A Template workflow for each of the preconfigured templates
- A Spoke Group workflow for each of the preconfigured spoke group types that are used in the hub-and-spoke labs
- A Device workflow for each of the preconfigured devices in the lab environment.

Again, it is important to remember that these are saved processes, not the templates, controllers, or devices that the processes create. We will examine this concept as you complete the lab.

In the Infrastructure menu, click on Controllers. All of the controller workflows are listed in the table. Click on Controller1 (which is the only saved workflow) to open the workflow.



Deploy Controller - Controller-01

Name* Controller-01

Provider Organization* SP

Global Controller ID 1

□ Peer Controller

□ Sub Organizations

☑ Staging Controller ☑ Post Staging Controller

○ Baremetal ○ Create Virtual Machine

IP Address* 10.234.0.103

Analytics Cluster Analytics

Note that the dialog title is “Deploy Controller – Controller-01”. This is because the end result of completing the workflow is the creation and deployment of a controller.

Question: What organization owns and manages this controller? ____________________________________

Question: What is the IP Address of the controller? ____

Question: To what analytics cluster will this controller forward log and statistics information?

____

Question: What are the 2 roles that this controller will perform in the SD-WAN?

____

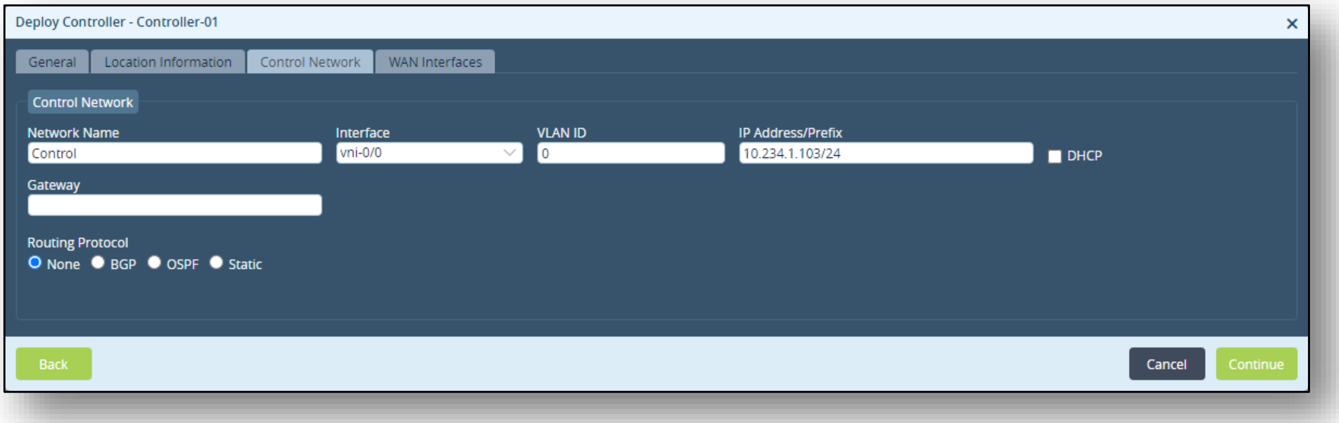
This controller is managed by the SP organization. We’ll see later in the lab that sub-organizations that fall under the SP organization can use this controller. When multiple sub-organizations use a parent controller, the controller acts as a multi-tenant controller and maintains separate control plane functionality for each tenant.

The IP address listed is the out-of-band management interface that is used for initial communication between the Versa Director and the Versa Controller. It is only used for the creation and onboarding process. Once the controller is provisioned, a separate interface associates with the Control Network is used for further communication between the head-end components.

This controller will be configured as a Staging controller and as a Post Staging controller. The Staging Controller function allows devices to be onboarded through this controller. The Post Staging Controller function allows this controller to act as a BGP route reflector, and SD-WAN CPEs will be able to establish BGP sessions with the controller for control plane information.

Continue to the Location Information tab. The Location Information tab can be used to indicate where the controller is physically located.

Continue to the Control Network tab.



Control Network

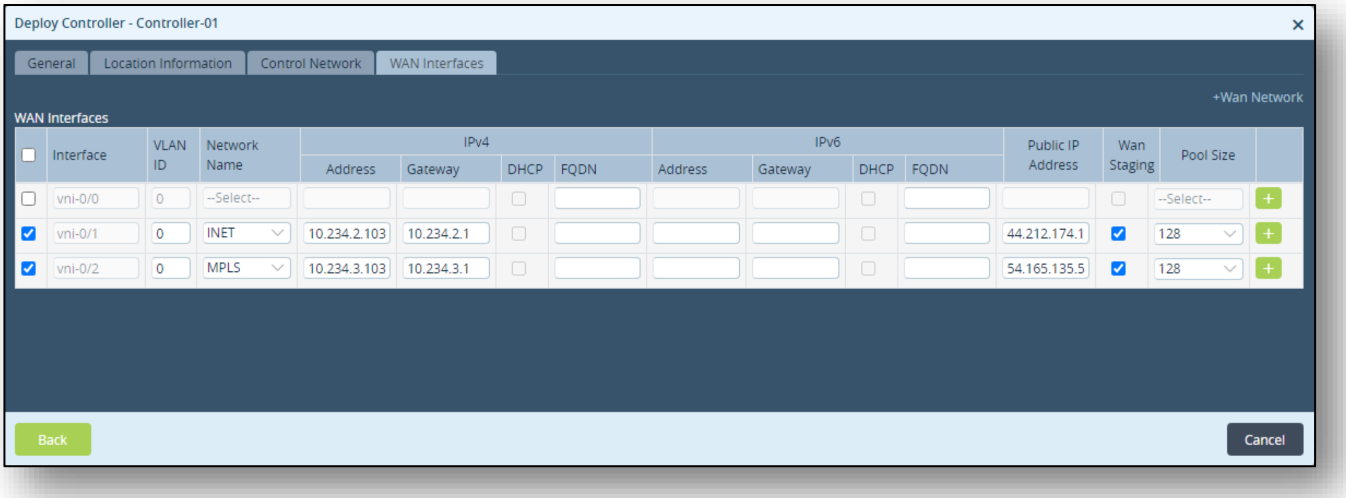
Network Name	Interface	VLAN ID	IP Address/Prefix	
Control	vni-0/0	0	10.234.1.103/24	□ DHCP

Gateway:

Routing Protocol: ● None ○ BGP ○ OSPF ○ Static

The Control Network tab is where you define the North-Bound interface that is normally used to communicate with Versa Director and Versa Analytics. If the Versa Controller or Versa Analytics nodes are not on the same broadcast domain as the north-bound interface, routing can be configured on the north-bound interface to enable reachability.

Continue to the WAN Interfaces tab.



WAN Interfaces

☐	Interface	VLAN ID	Network Name	IPv4				IPv6				Public IP Address	Wan Staging	Pool Size	
				Address	Gateway	DHCP	FQDN	Address	Gateway	DHCP	FQDN				
☐	vni-0/0	0	--Select--			☐				☐			☐	--Select--	+
☑	vni-0/1	0	INET	10.234.2.103	10.234.2.1	☐				☐		44.212.174.1	☑	128	+
☑	vni-0/2	0	MPLS	10.234.3.103	10.234.3.1	☐				☐		54.165.135.5	☑	128	+

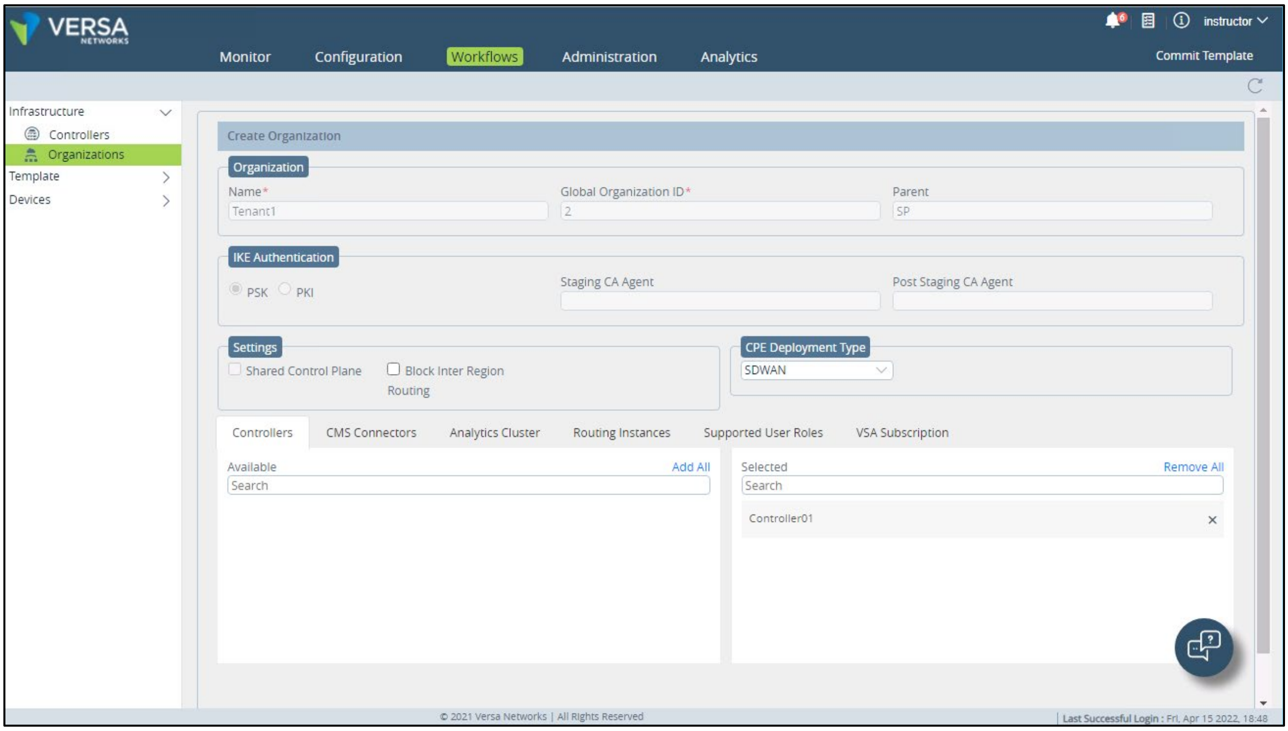
The WAN interfaces are the south-bound interfaces that connect to the SD-WAN environment. It is over these interfaces that CPEs will communicate with the controller. Note that because this controller has been deployed in a cloud environment, the internal WAN IP addresses and the public WAN IP addresses of the cloud environment are configured.

If you were creating a new controller, a Deploy button would be present in this dialog box, which would begin the process of building the controller, including all of the Virtual Routers, VRF tables, routing protocols, encryption profiles, and all other configuration components required to build a fully functional controller. Because the controller is created before most other SD-WAN components, and other SD-WAN components rely on configuration parameters of the controller when they are created, a provisioned controller cannot be modified using the workflow as changes to the controller would impact all other devices connected to the controller.

Click *Cancel* to exit the workflow dialog.

In the Infrastructure menu, select *Organizations*. The primary organization (SP in this example) is created during the initial Versa Director configuration process. Subsequent organizations (sub-organizations) are created using the Organizations workflow.

Open the Tenant1 organization workflow.



Create Organization

Organization
Name*: Tenant1
Global Organization ID*: 2
Parent: SP

IKE Authentication
● PSK ○ PKI
Staging CA Agent:
Post Staging CA Agent:

Settings
□ Shared Control Plane
□ Block Inter Region Routing

CPE Deployment Type: SDWAN

Available
Search

Selected
Search
Controller01 ×

The Organization workflow allows you to define a sub-organization and its associated parameters. Note that the controller Controller1 is listed in the Controllers tab. This configuration allows the Tenant1 sub-organization to use the Controller1. If another sub-organization under the SP domain is created, it could also be allowed to use the Controller1 controller. Other tenant-specific configuration parameters can be configured as well, including tenant-specific Analytics connectors, the default routing instances that will be created for devices within the sub-organization, and the supported user roles available to users within the sub-organization, which allows the parent organization to manage and control what type of access users within the sub-organization are allowed to be assigned.

IMPORTANT! Do not change any of the organization parameters!

Take a few minutes to explore the configuration parameters included in the organization workflow, then click Cancel to exit out of the workflow.

Exercise 2: Examine Template Workflows

It's common for the Controllers and Organizations workflows to be used only once or twice in an entire deployment, as those components are normally defined and deployed in the initial stages of the SD-WAN deployment. The workflows that are used frequently are the Template and Devices workflows.

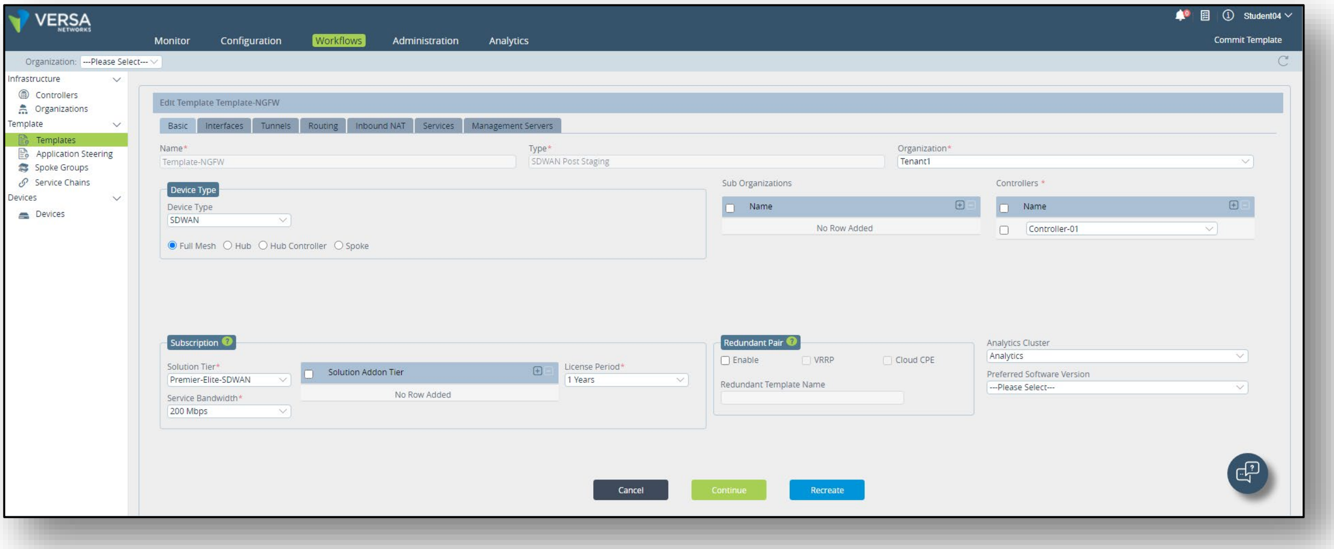
In the following exercises you will:

- Examine the structure of a Device Template workflow

In the Template workflow menu, select Templates. This opens the Device Template workflow table. Device Template workflows are used to build the base configuration template that a group of devices will inherit when a device is created in a later step. There are multiple workflows saved that were created during the initial lab setup. Device Templates that are created using the Device Template workflow are placed in the *Configuration > Templates > Device Templates* table in Versa Director, and are stored in the local Versa Director database.

Click on the *Template-NGFW* workflow to open the workflow.

The template that is created by a workflow inherits the name of the workflow. Continue to the next page in the lab guide to answer some questions and fill in some details related to this example workflow.



Organization: ---Please Select---

Edit Template Template-NGFW

Name*: Template-NGFW

Type*: SDWAN Post Staging

Organization*: Tenant1

Device Type

Device Type: SDWAN

● Full Mesh ○ Hub ○ Hub Controller ○ Spoke

Sub Organizations

□	Name
	No Row Added

Controllers *

□	Name
□	Controller-01

Subscription

Solution Tier*: Premier-Elite-SDWAN

Service Bandwidth*: 200 Mbps

□	Solution Addon Tier
	No Row Added

License Period*: 1 Years

Redundant Pair

□ Enable □ VRRP □ Cloud CPE

Redundant Template Name:

Analytics Cluster: Analytics

Preferred Software Version: ---Please Select---

Fill in the following information based on the workflow in your lab, or the image above:

What organization will have access to this workflow and the template that this workflow creates? ____

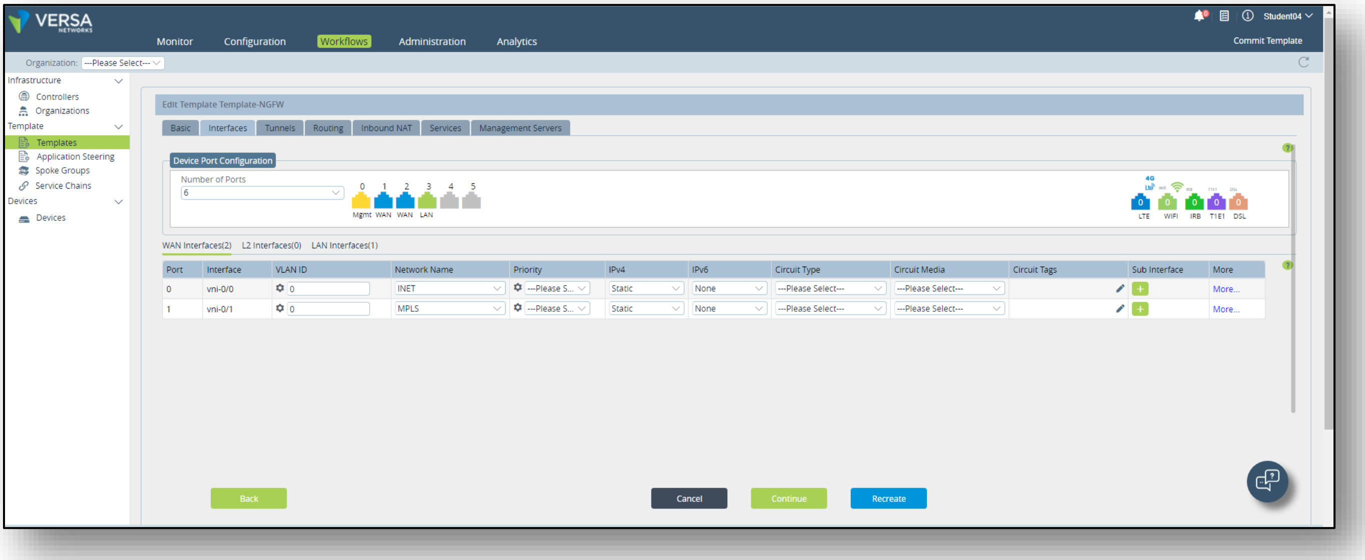
To what controller(s) will devices that use this template connect? ____________________

What subscription information will be inherited by devices that use the template created by this workflow? ____

This is the inherited subscription profile, which can be over-ridden by a more specific subscription profile on a device if desired.

Open the Interfaces tab of the workflow.

The Interfaces tab allows you to define the common interface layout of the devices that will share the template configuration created by the workflow. Note that the device *Port Configuration* diagram is a logical diagram and does not represent the actual physical device – it is only used for port mapping purposes and basic port parameters.



Organization: ---Please Select---

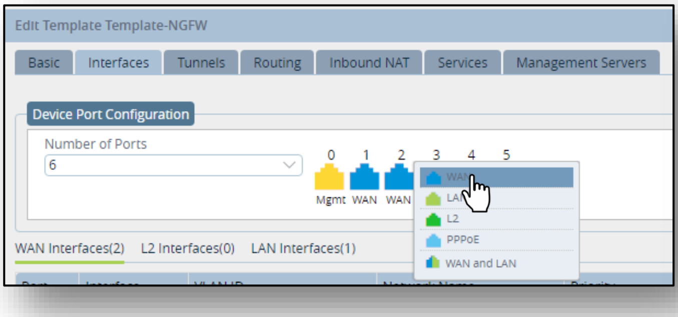
Edit Template Template-NGFW

Number of Ports: 6

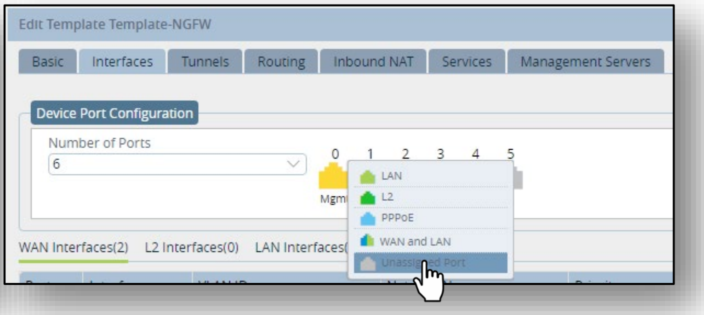
Port	Interface	VLAN ID	Network Name	Priority	IPv4	IPv6	Circuit Type	Circuit Media	Circuit Tags	Sub Interface	More
0	vni-0/0	0	INET	---Please S...	Static	None	---Please Select---	---Please Select---		+	More...
1	vni-0/1	0	MPLS	---Please S...	Static	None	---Please Select---	---Please Select---		+	More...

The LAN interfaces are the customer site facing interfaces at the local site. The *Network Name* is a user-defined name, the *Organization* determines which sub-organization owns the port, the *Zones* allows the user to define a specific security zone associated with the interface, and the Routing Instance is auto-populated based on the routing instance name configured for the organization. The method that devices will acquire address is specified in the template. However, the actual addressing is configured during the device creation process, as addressing is device specific.

To assign a port to a role, click on the port and select the role from the popup window. You can also change the assignment of a port by clicking on a port that already has an assignment.



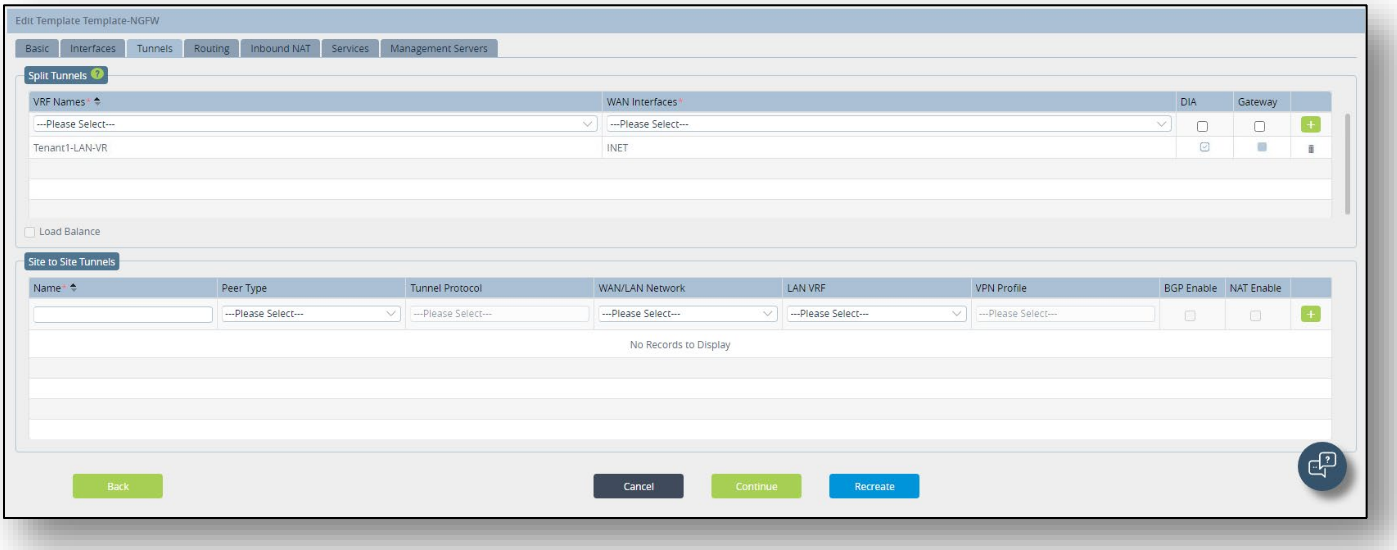
Number of Ports: 6



Number of Ports: 6

Open the Tunnels tab of the workflow.

The Tunnels tab allows you to specify direct internet access or SD-WAN gateway functions on devices that use the template created by the workflow. You can also configure site-to-site tunnels for non-SD-WAN tunnels between devices.



Split Tunnels

VRF Names*	WAN Interfaces*	DIA	Gateway	
---Please Select---	---Please Select---	□	□	+
Tenant1-LAN-VR	INET	☑	■	🗑

□ Load Balance

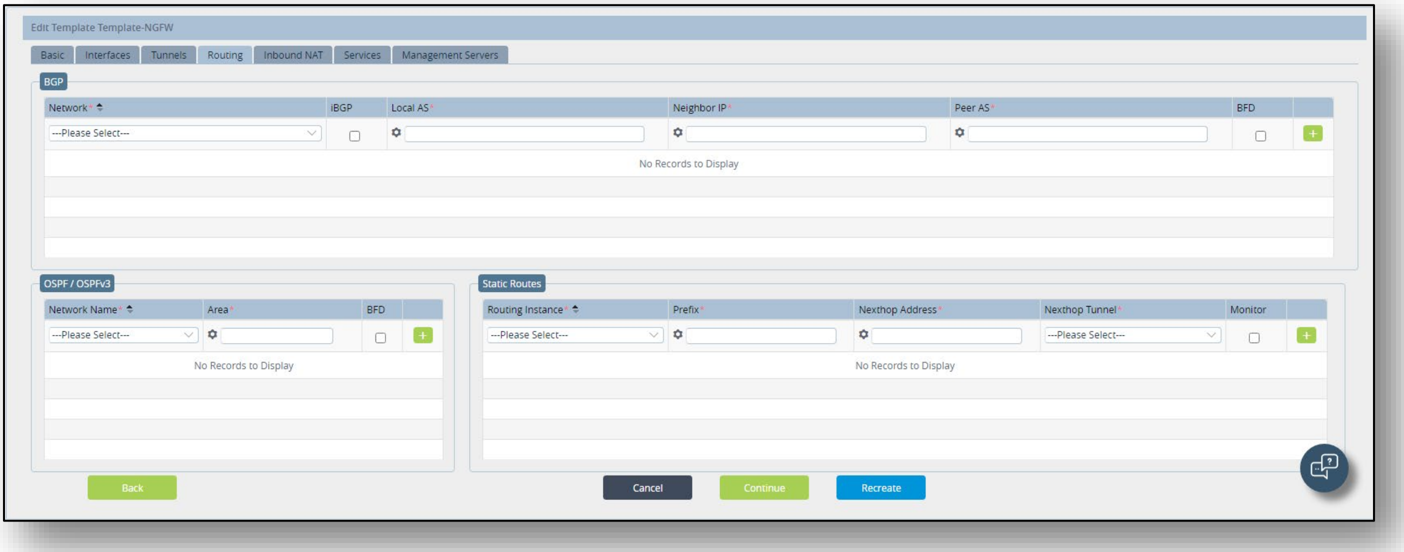
Site to Site Tunnels

Name*	Peer Type	Tunnel Protocol	WAN/LAN Network	LAN VRF	VPN Profile	BGP Enable	NAT Enable	
	---Please Select---	---Please Select---	---Please Select---	---Please Select---	---Please Select---	□	□	+

No Records to Display

Open the Routing tab of the workflow.

The Routing template allows you to define base routing protocol parameters if desired. When routing protocol information is configured in the workflow, the workflow process automatically creates the route redistribution policies required to advertise the local routing information – and routes learned through the workflow-created routing processes – to remote sites in the SD-WAN.



Edit Template Template-NGFW

Basic | Interfaces | Tunnels | Routing | Inbound NAT | Services | Management Servers

BGP

Network*	iBGP	Local AS*	Neighbor IP*	Peer AS*	BFD
---Please Select---	□				□

No Records to Display

OSPF / OSPFv3

Network Name*	Area*	BFD
---Please Select---		□

No Records to Display

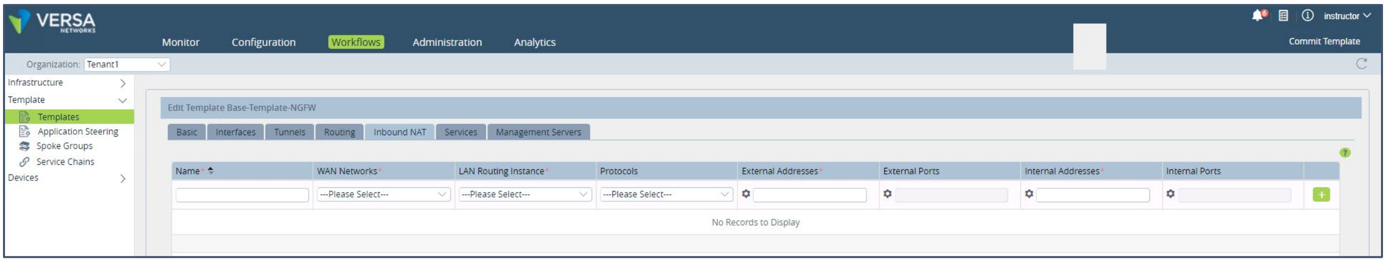
Static Routes

Routing Instance*	Prefix*	Nexthop Address*	Nexthop Tunnel*	Monitor
---Please Select---			---Please Select---	□

No Records to Display

Open the Inbound NAT tab.

The Inbound NAT tab allows you to create static destination-NAT to allow outside resources to reach internal NATed devices.



Organization: Tenant1

Edit Template Base-Template-NGFW

Basic | Interfaces | Tunnels | Routing | Inbound NAT | Services | Management Servers

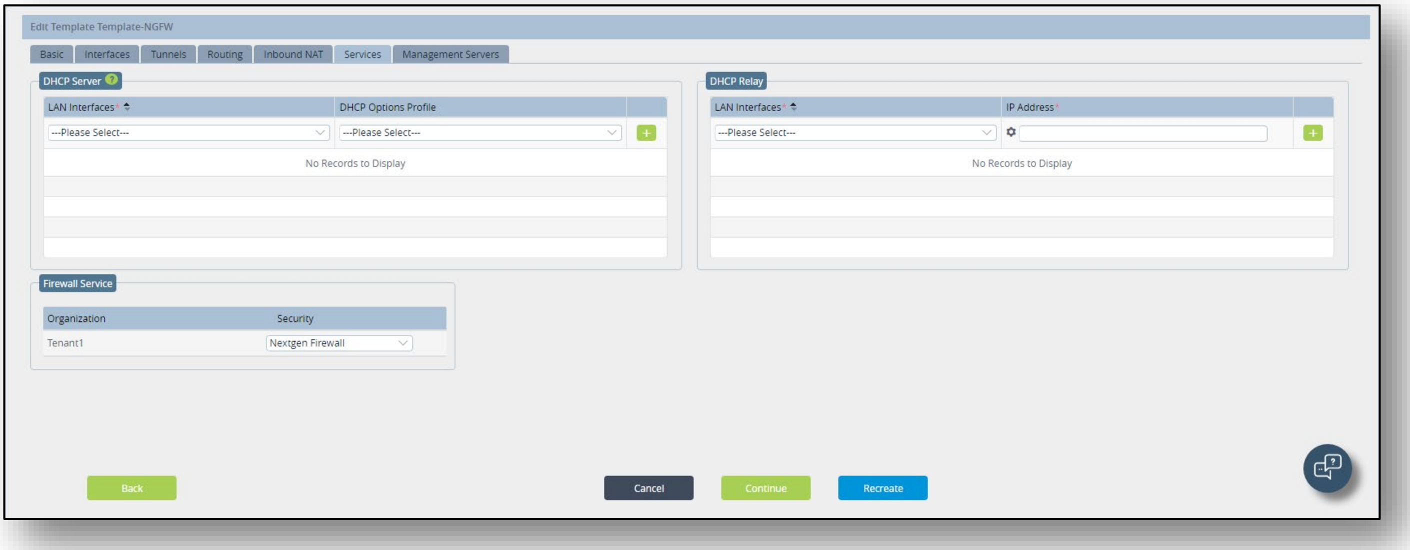
Name*	WAN Networks*	LAN Routing Instance*	Protocols	External Addresses*	External Ports	Internal Addresses*	Internal Ports
	---Please Select---	---Please Select---	---Please Select---				

No Records to Display

Open the Services tab.

Enabling the services in the template workflow allows you to configure the services in the resulting template.

The Services tab allows you to define what services will be active on the device. The services themselves are not created in the Workflow. The services are activated in the workflow, which instructs the workflow to create the configuration hierarchy necessary to add the services later by defining the services within the template that will be created. If you do not enable the services in the workflow, the corresponding configuration hierarchy will not be created in the template.



Edit Template Template-NGFW

Basic | Interfaces | Tunnels | Routing | Inbound NAT | Services | Management Servers

DHCP Server

LAN Interfaces	DHCP Options Profile
---Please Select---	---Please Select---
No Records to Display	

DHCP Relay

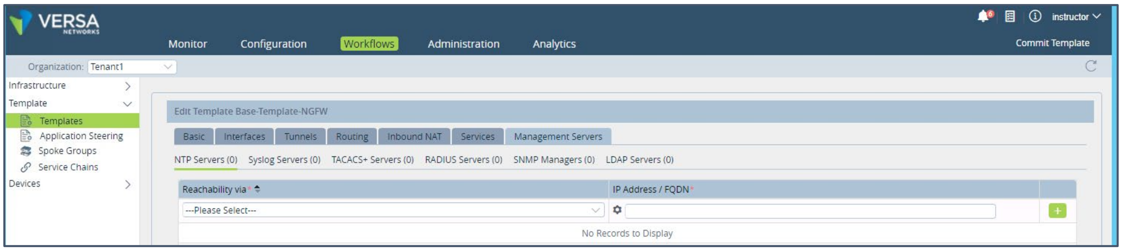
LAN Interfaces	IP Address
---Please Select---	
No Records to Display	

Firewall Service

Organization	Security
Tenant1	Nextgen Firewall

Open the Management Servers tab.

The Management Servers tab allows you to define parameters such as NTP servers, Syslog Servers, and other management server connectivity that will be common among all devices that use the resulting template.



Organization: Tenant1

Edit Template Base-Template-NGFW

Basic | Interfaces | Tunnels | Routing | Inbound NAT | Services | Management Servers

NTP Servers (0) | Syslog Servers (0) | TACACS+ Servers (0) | RADIUS Servers (0) | SNMP Managers (0) | LDAP Servers (0)

Reachability via	IP Address / FQDN
---Please Select---	
No Records to Display	

Important! Do not change this workflow!

This workflow is used to reset the Base-Template device template throughout the lab! You will have the opportunity to create your own template workflow next!

Click ***Cancel*** to close the workflow dialog, then select *Yes* from the popup.

Exercise 4: Examine Device Workflows

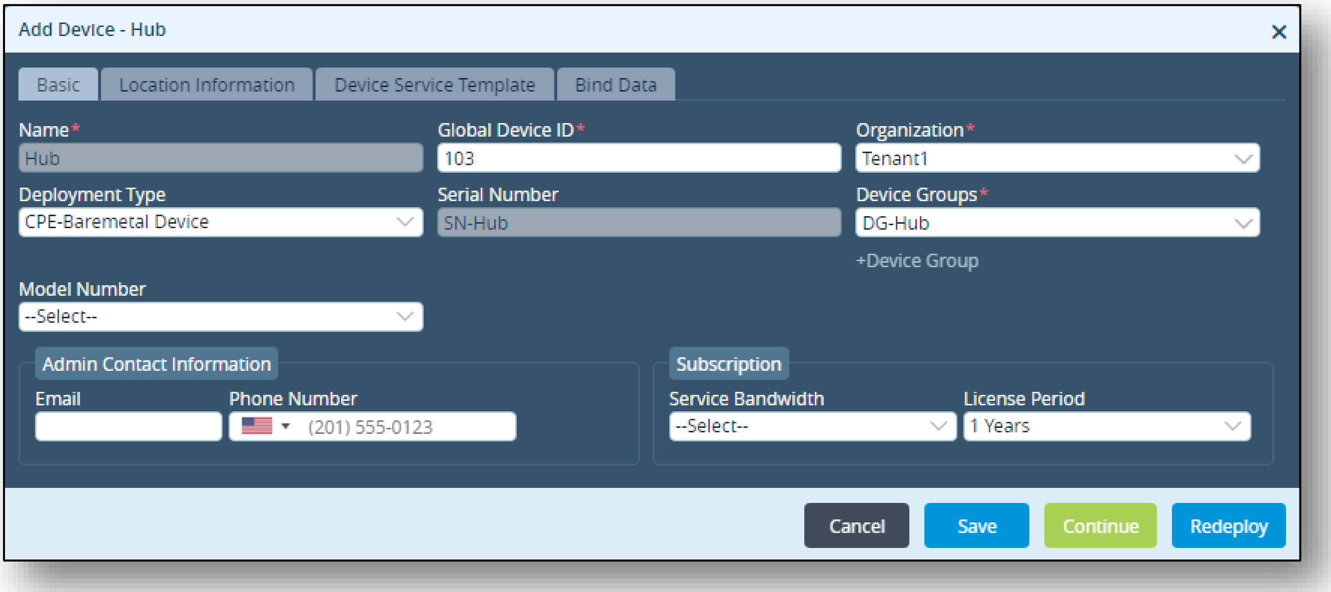
After completing this lab exercise, you will be able to:

- Identify the components of a Device workflow

Next you will explore the Devices device template. The Device workflow is used to create the individual devices in the network. Devices created by the Device workflows are added to the *Administration > Inventory > Hardware* table in Versa Director.

Select *Devices* from the Devices workflow section. You will see several device workflows in the table. These device workflows were used to create the devices in the pre-configured lab environment. In this part of the lab you will examine the properties of one of the pre-configured device workflows.

Select the *Hub* device workflow in the table. This will open the workflow that was used to create the Hub device.



Add Device - Hub

Name*: Hub
Global Device ID*: 103
Organization*: Tenant1
Deployment Type: CPE-Baremetal Device
Serial Number: SN-Hub
Device Groups*: DG-Hub
+Device Group
Model Number: --Select--

Admin Contact Information
Email:
Phone Number: (201) 555-0123

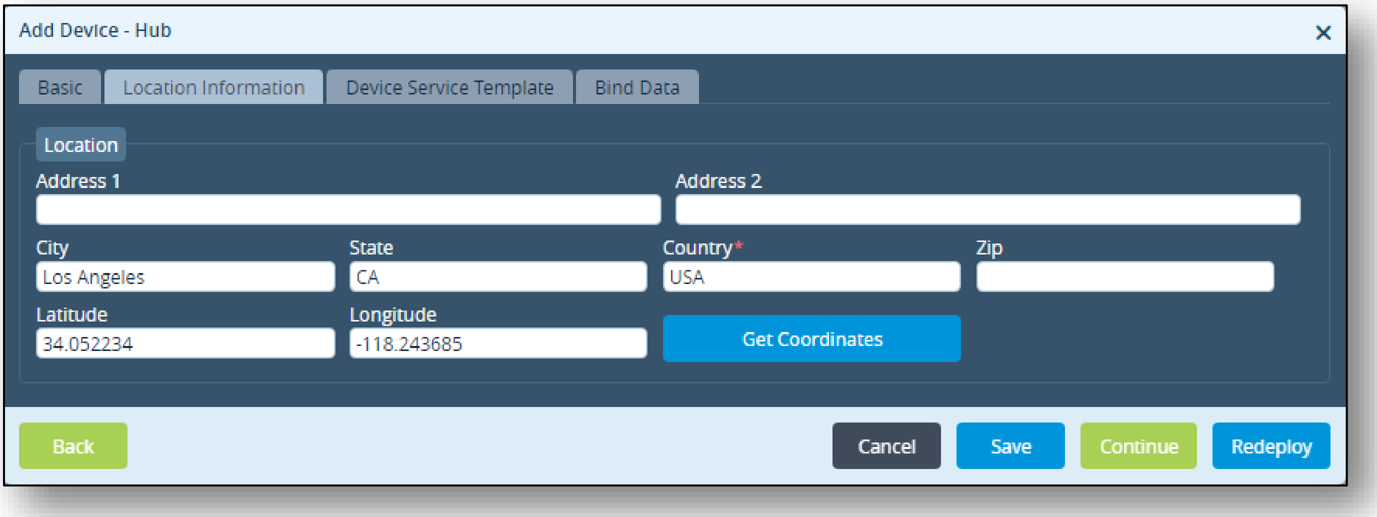
Subscription
Service Bandwidth: --Select--
License Period: 1 Years

The Basic tab of the device workflows is used for the base parameters. The device that is created in the *Hardware Inventory* will inherit the name of the device workflow.

In most situations, the *Global Device ID* chosen by Versa Director is used to avoid overlapping device IDs within other organizations, as the Global Device ID must be unique on Versa Director. The Serial Number is the software or hardware serial number of the device. The Subscription properties can be left at the default values, in which case the subscription values in the template to which the device is linked will be used. If you wish to assign different subscription values to the individual device, you may do so here.

The *Device Groups* parameter is used to link the device to a template. If a device group needed to link the device to a template does not exist, the *+Device Group* shortcut will open the Device Group creation dialog, where you can create the desired device group without leaving the Device workflow.

Open the Location Information tab.

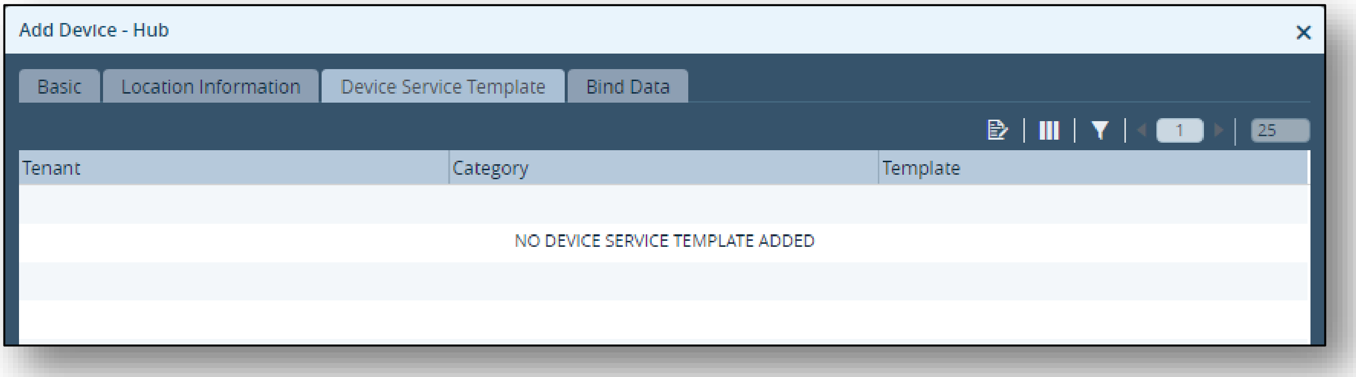


Address 1		Address 2	
City	State	Country*	Zip
Los Angeles	CA	USA	
Latitude	Longitude		
34.052234	-118.243685		

You must enter a Country value. Other values are optional, but the more specific you are, the better.

The Location Information tab allows you to enter device location information. The final location is based on Latitude and Longitude values that are calculated from the address information. The more detailed the address information, the more accurate the latitude and longitude values will be. This information is used to display the device on maps in the Monitor and Analytics dashboards.

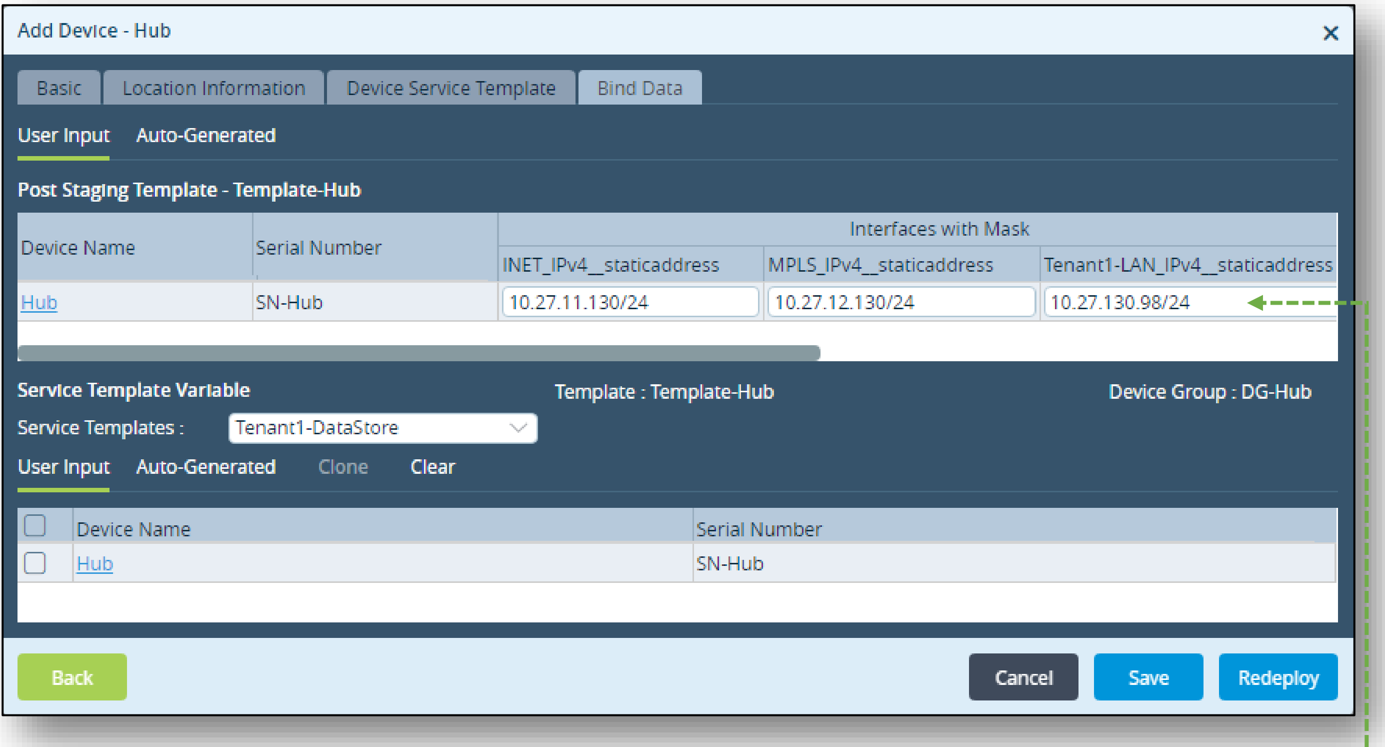
Open the Device Service Template tab of the Device workflow.



Tenant	Category	Template
NO DEVICE SERVICE TEMPLATE ADDED		

The Device Service Template tab allows you to assign service templates to the device directly. In many instances, the service templates are assigned through the device group. Services templates are configuration components that are specific to a service, such as Class of Service, Security, or SD-WAN Policy (application steering). Allowing the administrator to assign a service template directly to a device allows more flexibility for service assignment.

Open the Bind Data tab of the Device workflow.



Add Device - Hub

Basic | Location Information | Device Service Template | Bind Data

User Input | Auto-Generated

Post Staging Template - Template-Hub

Device Name	Serial Number	Interfaces with Mask		
		INET_IPv4__staticaddress	MPLS_IPv4__staticaddress	Tenant1-LAN_IPv4__staticaddress
Hub	SN-Hub	10.27.11.130/24	10.27.12.130/24	10.27.130.98/24

Service Template Variable

Template : Template-Hub

Device Group : DG-Hub

Service Templates : Tenant1-DataStore

User Input | Auto-Generated | Clone | Clear

□	Device Name	Serial Number
□	Hub	SN-Hub

The Bind Data tab is where you enter device-specific information. When the Bind Data tab is opened, the template associated with the Device Group (in the Basic tab) is scanned for any variables or values that the user needs to enter. If the Bind Data tab is empty when you open it, this is usually because the Device Group configured in the Basic tab is not properly configured, and does not have a corresponding device template configured. When there is a problem with the device group template assignment, the Bind Data tab tries to look for template information, but can't find a related template.

There are 2 ways to enter user-defined information in the Bind Data fields. The first is to enter them directly in the fields listed in the Device Name field. The scroll bar at the bottom of the Post Staging Template window allows you to scroll for additional values.

Another common method of entering the bind data is to click on the device name in the table. This will open a new dialog window that displays all of the required fields.

Click the Hub device name in the table to examine the pre-configured bind data for the device.

IMPORTANT: Do NOT change the bind data information for the Hub105 device!

Click ***Cancel*** to close the bind data dialog when you are finished examining the data, then click ***Cancel*** again to close the Device Workflow dialog.

Exercise 5: Practice

In the next lab exercises you will perform the following tasks:

- Create a Template workflow that is named after your branch-id (e.g. Template-Branch01, Template-Branch02, etc.)
- Create a new device group that links to your newly created template
- Re-assign your existing device to the new device group
- Commit the template in order to re-configure the existing device in the network (using the new template configuration)

Because this course does not cover deployment of devices, you will not deploy the new device that you create. However, you will examine the objects created in Versa Director, and you will re-assign your existing device to the new device group that references the template that you create. You will then commit the template so that you are familiar with the process of creating a template using Workflows and applying the template to a device.

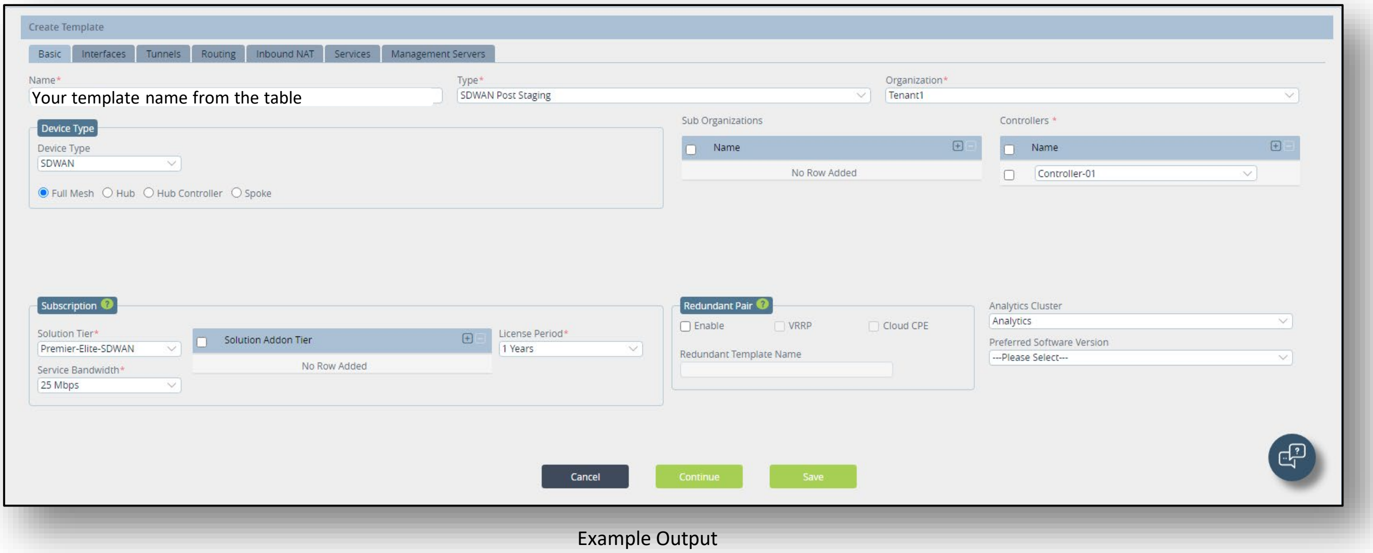
Create a new Device Template

In this exercise you will create a new Device Template using a Template workflow. Use a template workflow to create the template with the following parameters:

Basic Tab:

Workflow Name:	Template-[branch name]
Type:	SDWAN Post Staging
Organization:	Tenant1
Device Type:	SDWAN Full Mesh
Controllers:	Controller-01
Analytics Cluster:	Analytics
Solution Tier:	Premier-Elite-SDWAN
Bandwidth:	25 Mbps

Example: Template-Branch01



Name*: Your template name from the table
Type*: SDWAN Post Staging
Organization*: Tenant1

Device Type
Device Type: SDWAN
● Full Mesh ○ Hub ○ Hub Controller ○ Spoke

Sub Organizations
□	Name
	No Row Added

Controllers *
□	Name
□	Controller-01

Subscription
Solution Tier*: Premier-Elite-SDWAN
Service Bandwidth*: 25 Mbps

□	Solution Addon Tier
	No Row Added

License Period*: 1 Years

Redundant Pair
□ Enable □ VRRP □ Cloud CPE
Redundant Template Name:

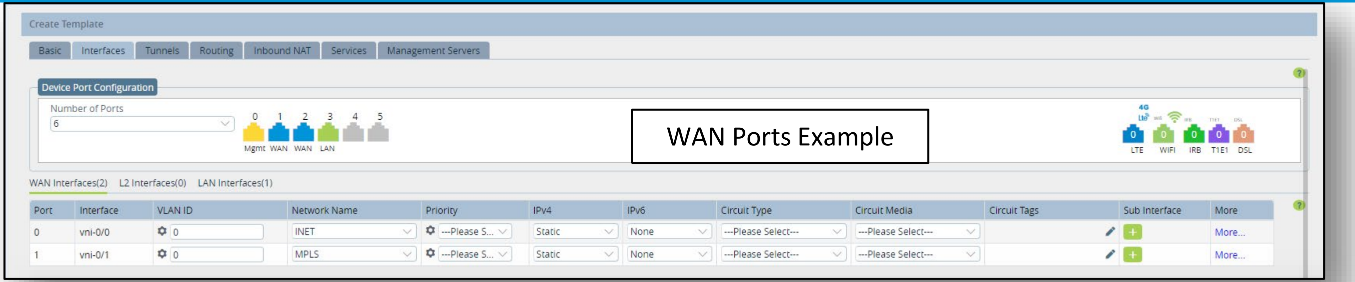
Analytics Cluster: Analytics
Preferred Software Version: ---Please Select---

Example Output

Interfaces Tab

Assign the following interface parameters in the Interfaces tab:

Port 1 (WAN Interface 0, vni-0/0)	Port Type: WAN Network Name: INET IPv4 Address: Static
Port 2 (WAN Interface 1, vni-0/1)	Port Type: WAN Network Name: MPLS IPv4 Address: Static
Port 3 (LAN Interface 2, vni-0/2)	Network Name: Tenant1-LAN Organization: Tenant1 Zones: Leave default Routing Instance: (Auto-populate) IPv4 Address: Static



Create Template

Basic | Interfaces | Tunnels | Routing | Inbound NAT | Services | Management Servers

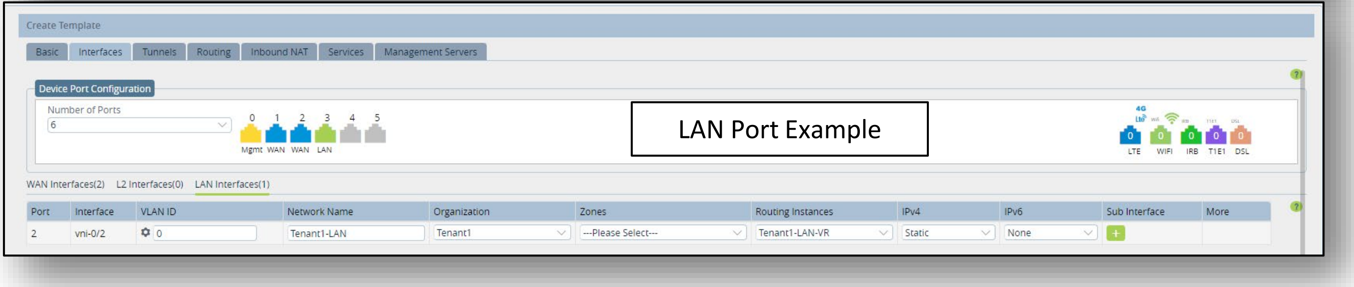
Device Port Configuration

Number of Ports: 6

WAN Ports Example

WAN Interfaces(2) L2 Interfaces(0) LAN Interfaces(1)

Port	Interface	VLAN ID	Network Name	Priority	IPv4	IPv6	Circuit Type	Circuit Media	Circuit Tags	Sub Interface	More
0	vni-0/0	0	INET	---Please S...	Static	None	---Please Select---	---Please Select---		+	More...
1	vni-0/1	0	MPLS	---Please S...	Static	None	---Please Select---	---Please Select---		+	More...



Create Template

Basic | Interfaces | Tunnels | Routing | Inbound NAT | Services | Management Servers

Device Port Configuration

Number of Ports: 6

LAN Port Example

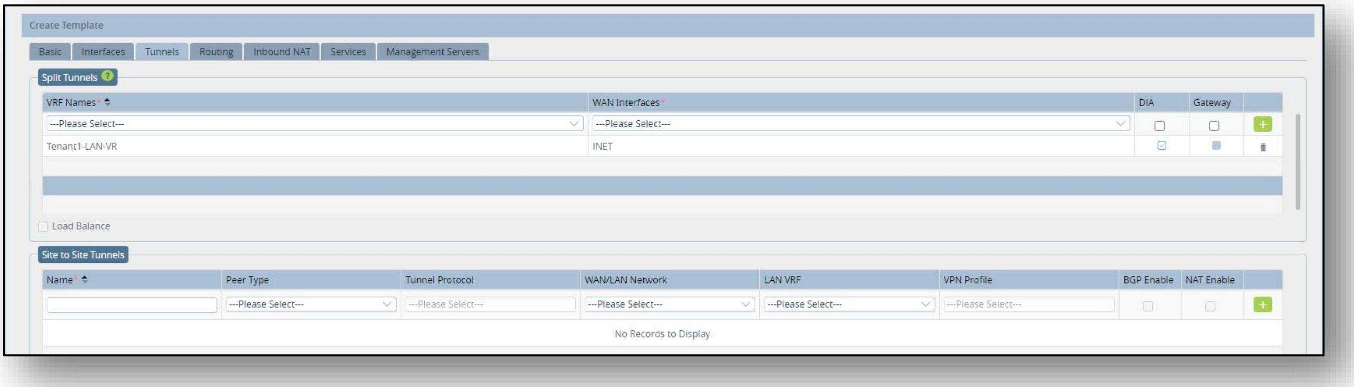
WAN Interfaces(2) L2 Interfaces(0) LAN Interfaces(1)

Port	Interface	VLAN ID	Network Name	Organization	Zones	Routing Instances	IPv4	IPv6	Sub Interface	More
2	vni-0/2	0	Tenant1-LAN	Tenant1	---Please Select---	Tenant1-LAN-VR	Static	None	+	

Tunnels Tab

Configure Split Tunnels. In the Split Tunnels, link the VRF Tenant1-LAN-VR with the WAN interface INET. Make the Split Tunnels a DIA type, which allows traffic sourced from the Tenant1-LAN-VR and destined to a non-SD-WAN destination to use the INET routing instance to forward traffic (Direct Internet Access).

Be sure to click the + button to add the DIA configuration .



Create Template

Basic | Interfaces | Tunnels | Routing | Inbound NAT | Services | Management Servers

Split Tunnels

VRF Names*	WAN Interfaces*	DIA	Gateway	
---Please Select---	---Please Select---	□	□	+
Tenant1-LAN-VR	INET	☑	■	

□ Load Balance

Site to Site Tunnels

Name*	Peer Type	Tunnel Protocol	WAN/LAN Network	LAN VRF	VPN Profile	BGP Enable	NAT Enable	
	---Please Select---	---Please Select---	---Please Select---	---Please Select---	---Please Select---	□	□	+

No Records to Display

Routing Tab

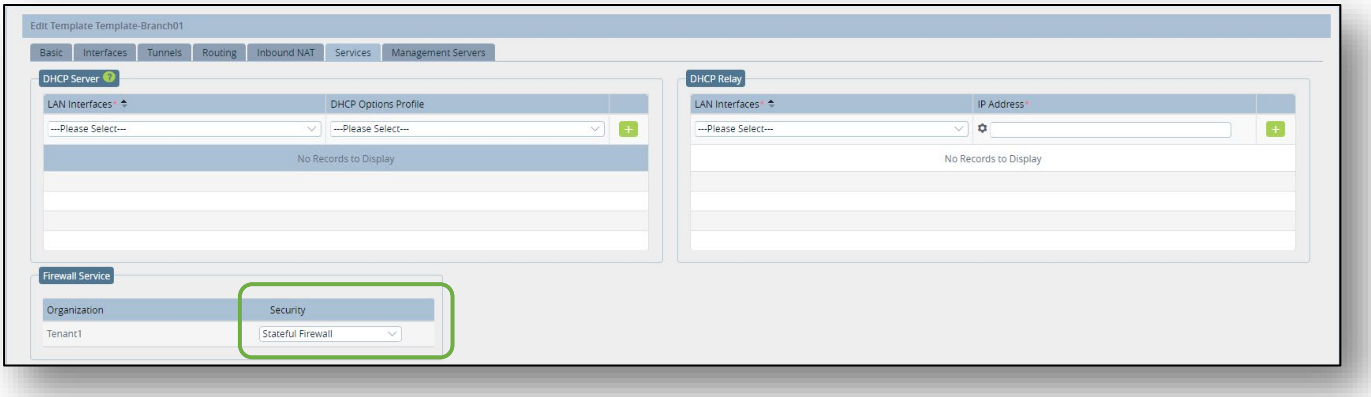
Do not configure any Routing parameters.

Inbound NAT Tab

Do not configure any Inbound NAT properties.

Services Tab

Enable the SFW services under the Services tab.



DHCP Server

LAN Interfaces*	DHCP Options Profile
---Please Select---	---Please Select---

No Records to Display

DHCP Relay

LAN Interfaces*	IP Address*
---Please Select---	

No Records to Display

Firewall Service

Organization	Security
Tenant1	Stateful Firewall

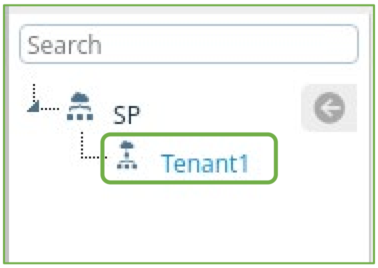
Management Servers Tab

Do not configure any Management Servers properties.

Click the Create button to create the workflow and the corresponding device template.

Question: Is your template workflow listed in the workflow table? ___________________________________

Question: Is the object listed in the table a workflow or a template? _________________________________



Navigate to the *Configuration > Templates > Device Templates hierarchy*. Make sure that the *Tenant1* organization is selected from the organization menu on the left.

Question: Is there a template listed in the table that matches the workflow name you used? _________________________________

Click on the template that you created with your workflow to open the template and use the values in the lab to fill in the information below.

Interface Name:	Address associated with the interface
vni-0/0	
vni-0/1	
vni-0/2	

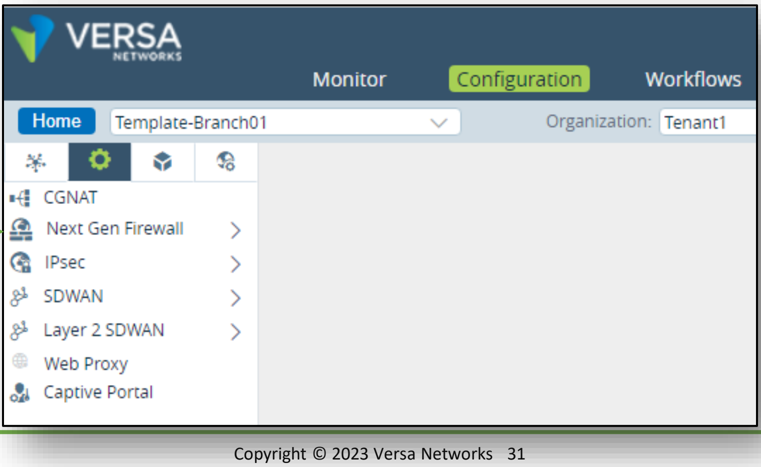
Question: Why do you think that there are variable names in the interface IP Address field of the interfaces instead of actual IP addresses?

____

Network Name	Interface associated with the network
MPLS	
INET	
LAN-Network	

Virtual Routers	Networks associated with the Virtual Router
MPLS-Transport-VR	
INET-Transport-VR	
Tenant1-Control-VR	
Tenatn1-LAN-VR	

Open the Services tab of the template and identify the type of security services that are enabled:



Template-Branch01

Organization: Tenant1

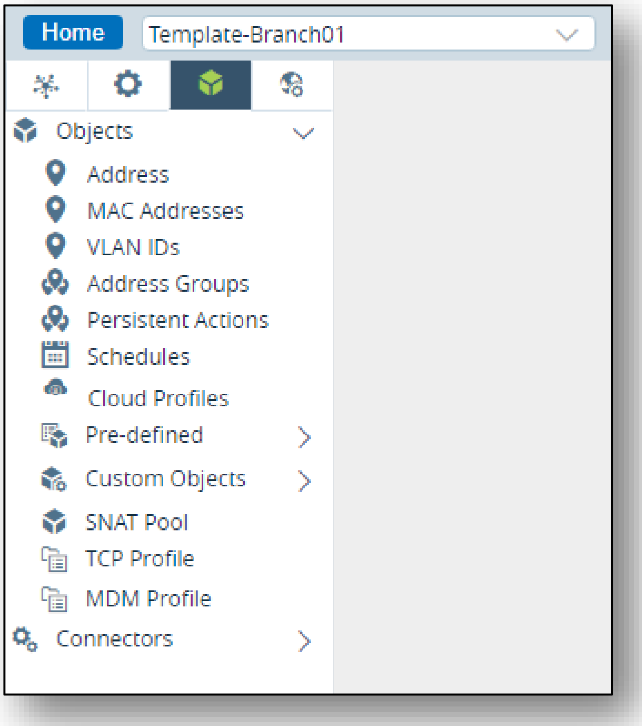
NextGen Firewall services have been enabled in this configuration template

Using the information in the Services tab of the template, fill in the following information:

Location	Values
Stateful Firewall > Security > Policies	What 2 policies are automatically created? ____ ____
Stateful Firewall > IPsec	What 2 VPN profiles are automatically created? ____ ____
SDWAN > Controllers	What controller is listed? ____

Open the *Objects & Connectors* tab of the template.

Expand the *Objects* menu and examine the types of configuration objects:



In the next lab parts you will:

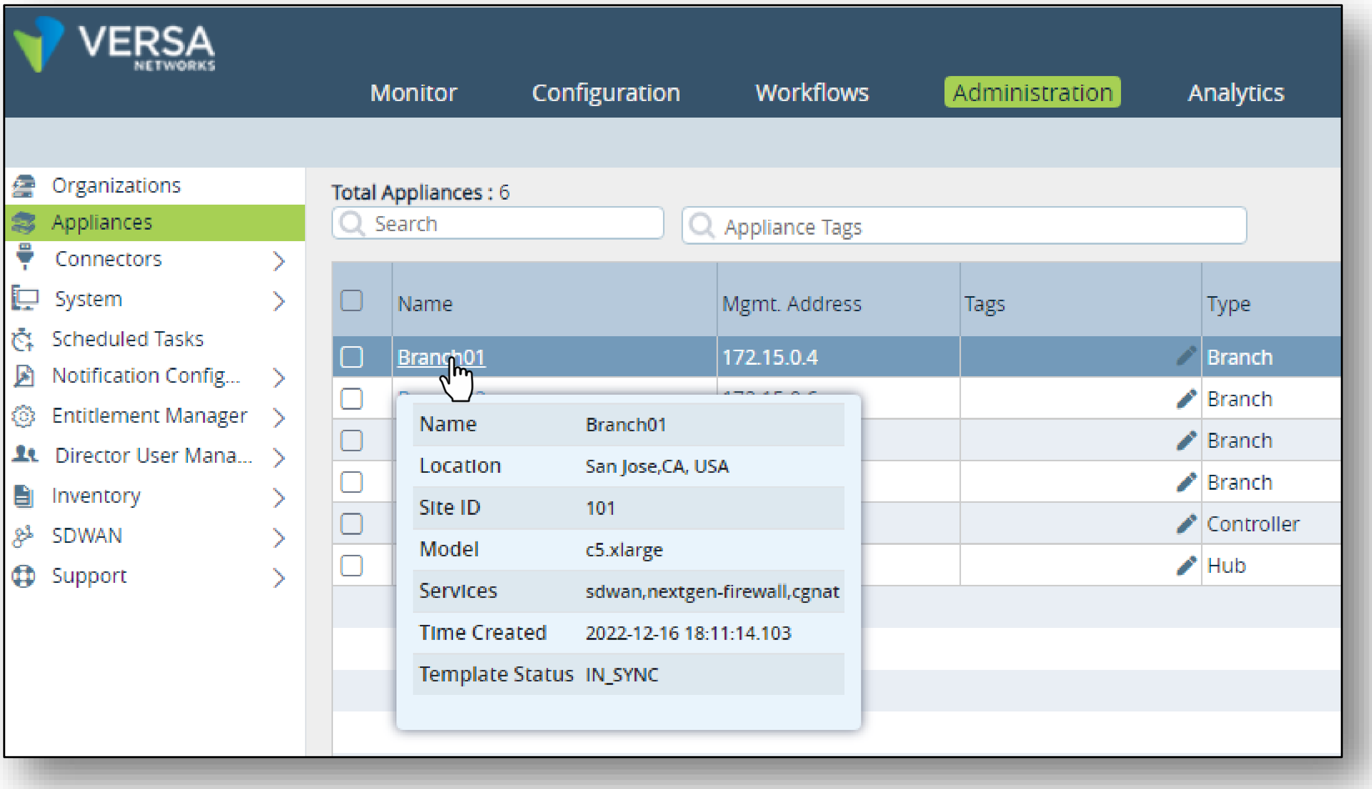
- Compare the newly created Device Template to the running configuration on your device

Steps:

- Open your device in Appliance Context mode (by using the Monitor tab, the Configuration > Devices table, or through the Administration > Appliances table.)
- Identify the security features configured on your device and compare them with the security features configured in the device template you just created.

Step by Step Guide

Navigate to the *Administration > Appliances* dashboard. Locate your device in the Appliances table. Click on your device to open the Appliance Context mode of your device.

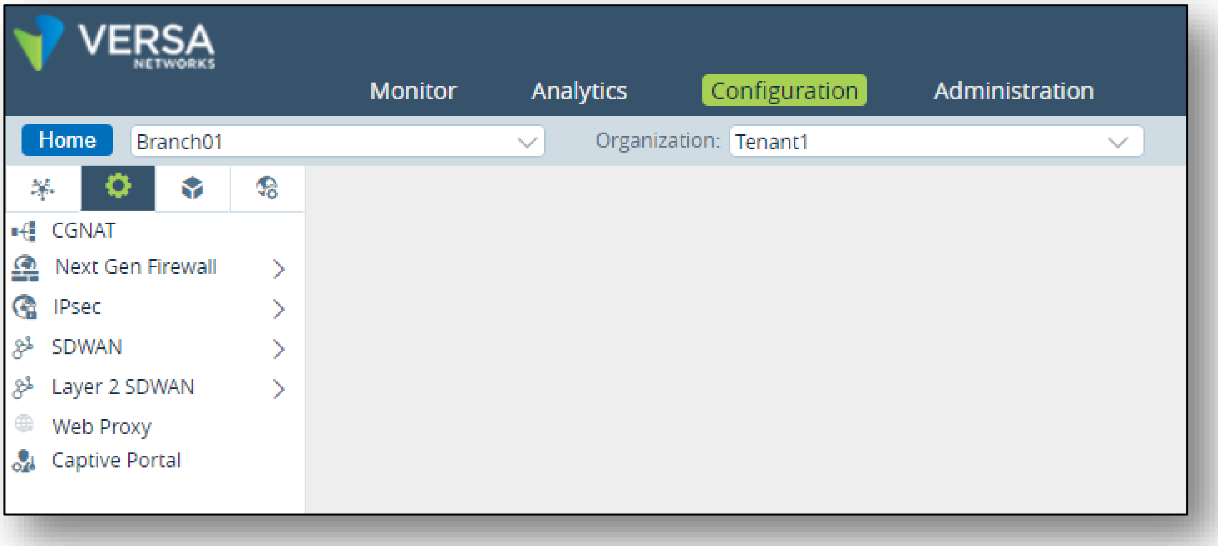


Total Appliances : 6

□	Name	Mgmt. Address	Tags	Type
□	Branch01	172.15.0.4		Branch
□				Branch
□				Branch
□				Branch
□				Controller
□				Hub

Name	Branch01
Location	San Jose,CA, USA
Site ID	101
Model	c5.xlarge
Services	sdwan,nextgen-firewall,cgnat
Time Created	2022-12-16 18:11:14.103
Template Status	IN_SYNC

From Appliance Context mode, navigate to the *Configuration* > *Services* dashboard and identify which type of security service is currently active in the device:



Question: What type of security service is currently available on the device? ____

Question: Are these services the same services that are available under the template that you created? ____

Click the Home button to exit device configuration mode.

In the next lab parts you will:

- Create a device group named DG-[branch-ID] (e.g. DG-Branch01, DG-Branch02, etc.);
- Assign the template you created to the device group;
- Re-assign your branch device to the new device group; and
- Commit the template you created in order to re-configure your branch device.

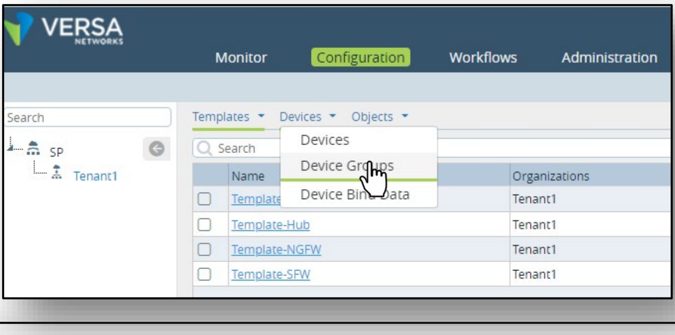
Steps:

- Create a new device group with the name DG-[Branch name] (e.g. DG-Branch01, DG-Branch02, etc.).
- Assign the template that you created to the device group.
- Reassign your device to the new device group (either through the Devices > Device Group dashboard or through the Device Workflow for your device)
- Commit the changes
- Verify that the services changed on your device from Next Gen Firewall to Stateful Firewall services.

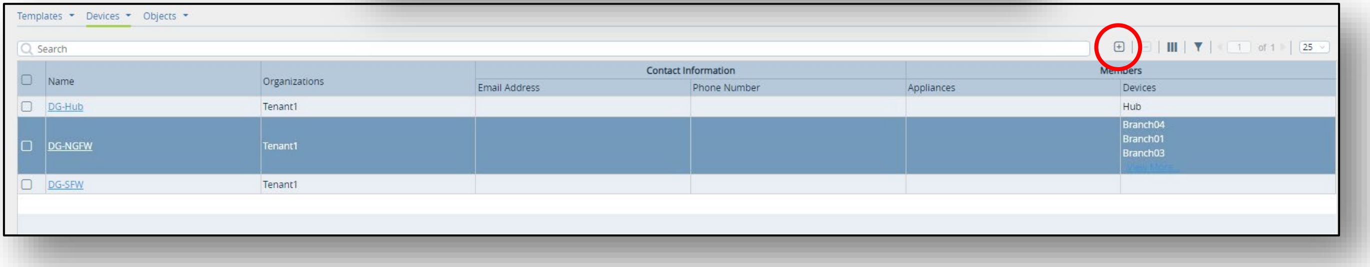
Step by Step Guide

From the main Versa Director dashboard, navigate to *Configuration > Devices > Device Groups*.

In the Device Groups dashboard, click the + button to create a new device group.



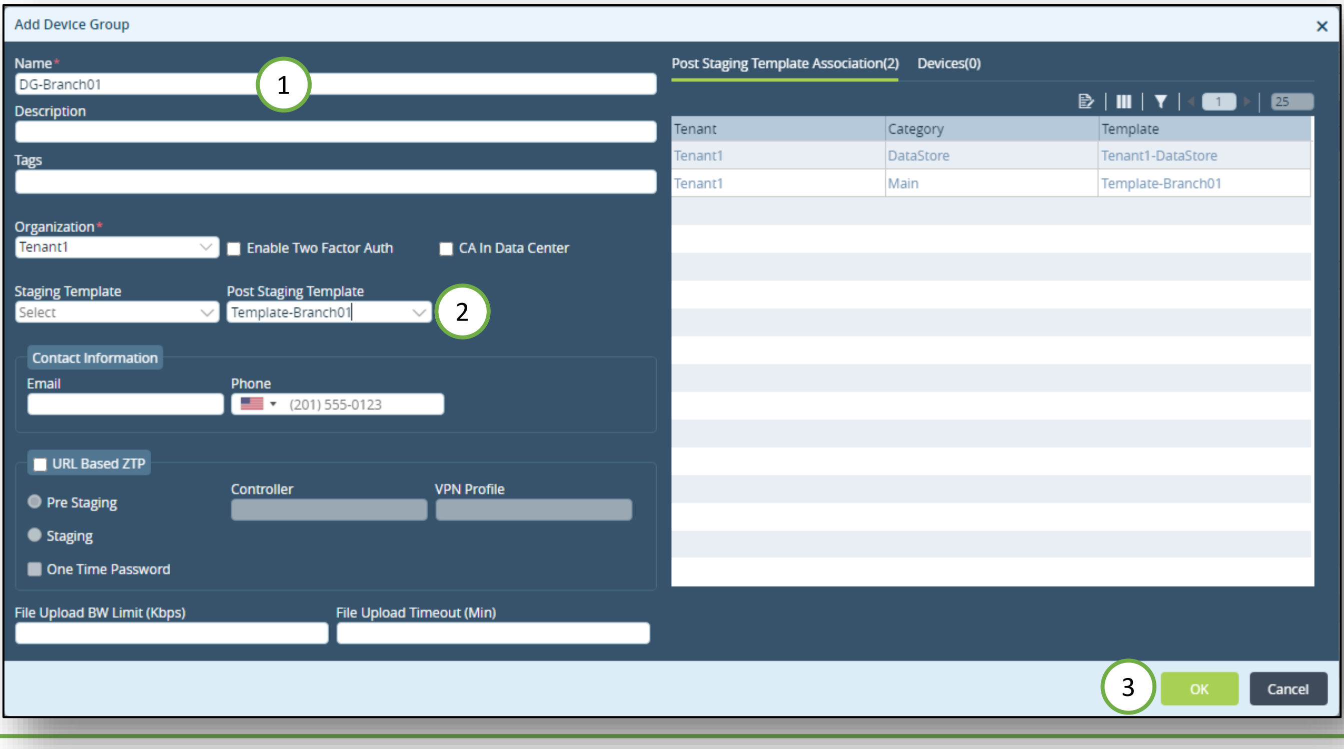
Name	Organizations
Template	Tenant1
Template-Hub	Tenant1
Template-NGFW	Tenant1
Template-SFW	Tenant1



		Contact Information		Members	
Name	Organizations	Email Address	Phone Number	Appliances	Devices
DG-Hub	Tenant1				Hub
DG-NGFW	Tenant1				Branch04 Branch01 Branch03 View More...
DG-SFW	Tenant1				

Name the device group DG-[Branch-id] (e.g. DG-Branch01, DG-Branch02, etc.)

Assign the template you created earlier to the Post Staging Template field, then click OK to create the device group.



Name* DG-Branch01

Description

Tags

Organization* Tenant1

□ Enable Two Factor Auth

□ CA In Data Center

Staging Template Select

Post Staging Template Template-Branch01

Contact Information

Email

Phone (201) 555-0123

□ URL Based ZTP

○ Pre Staging

○ Staging

□ One Time Password

Controller

VPN Profile

File Upload BW Limit (Kbps)

File Upload Timeout (Min)

Tenant	Category	Template
Tenant1	DataStore	Tenant1-DataStore
Tenant1	Main	Template-Branch01

Question: Does your new device group appear in the Device Group table?_____________________________

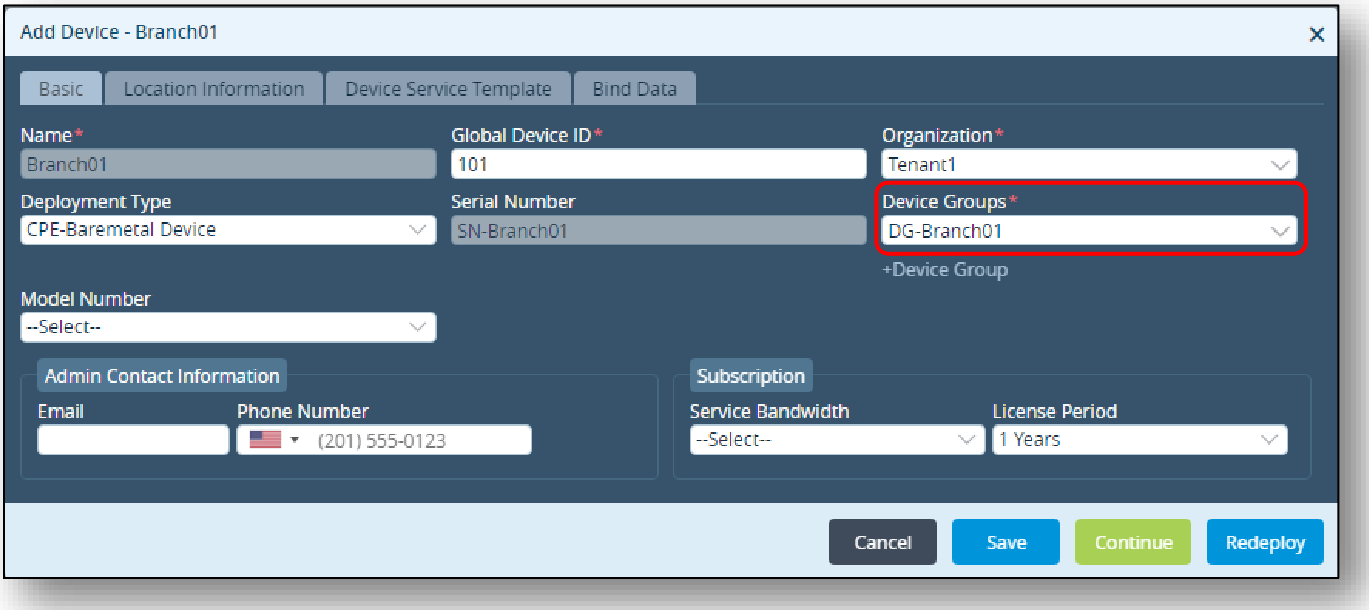
Question: Does your branch device appear in your device group Members list? _________________________

Assign Device to a New Device Group

In the next steps, you will use the Device workflow to assign your branch device to the new device group.

Navigate to the *Workflows > Devices > Devices* dashboard and locate your device in the Device Workflow list. Click your device to open the workflow.

Locate your new device group in the Device Groups drop-down menu, and assign your new device group to the device.



Add Device - Branch01

Name*: Branch01
Global Device ID*: 101
Organization*: Tenant1
Deployment Type: CPE-Baremetal Device
Serial Number: SN-Branch01
Device Groups*: DG-Branch01
Model Number: --Select--

Admin Contact Information
Email:
Phone Number: (201) 555-0123

Subscription
Service Bandwidth: --Select--
License Period: 1 Years

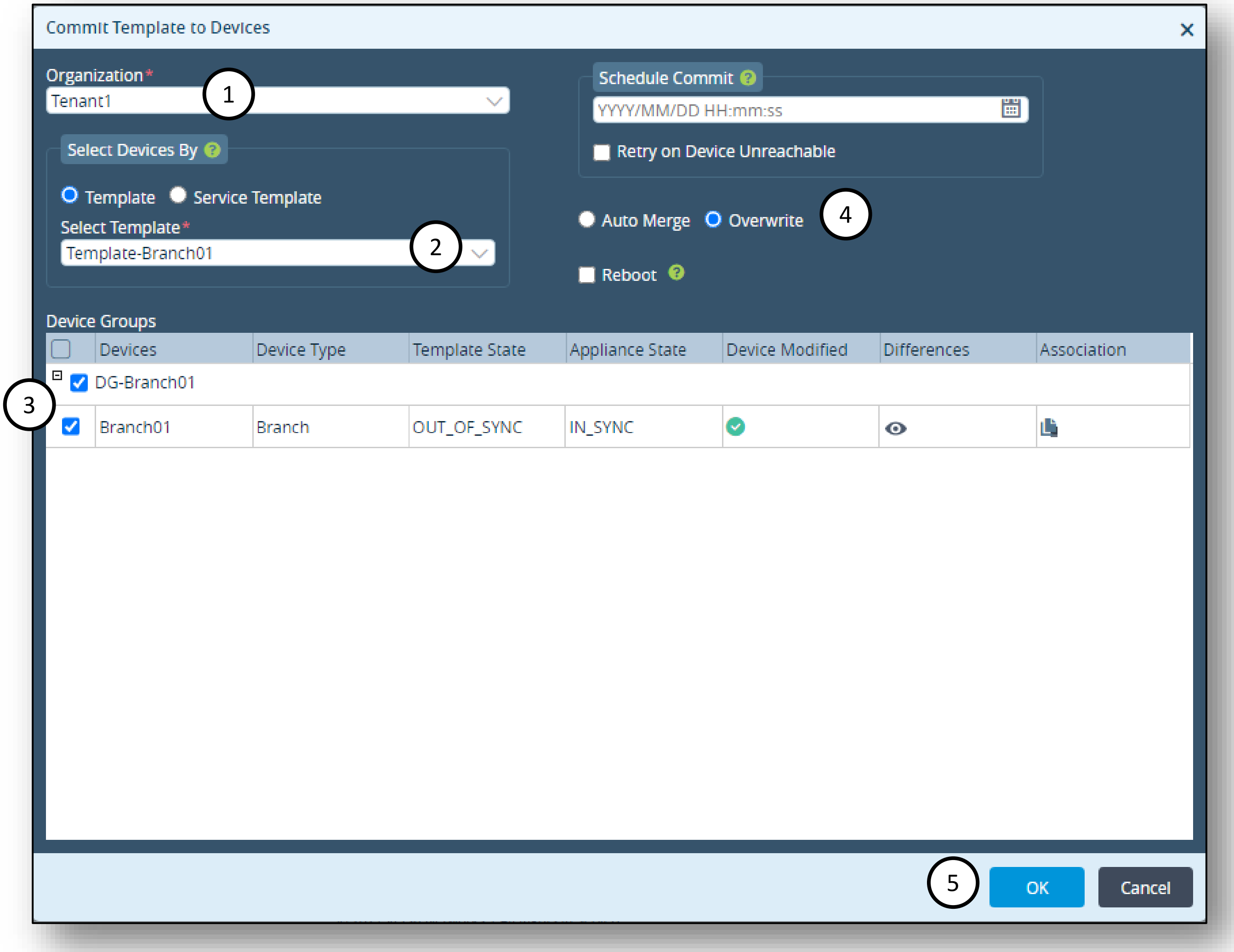
Click the Redeploy button to apply the changes to the Device workflow.

You have successfully update the device information in Versa Director. The next step is to apply the changes made in Versa Director to your appliance by committing the template.

Click the *Commit Template* link in the top-right corner of Versa Director.

In the Commit dialog:

1. Select the Tenant1 organization
2. Select your newly created template from the Select Template drop-down
3. Locate your device in the Device Groups table and select the box next to your device
4. Ensure that the Overwrite option is selected
5. Click the OK button to apply the changes to the device.



Commit Template to Devices

Organization*: Tenant1

Select Devices By: ● Template ○ Service Template

Select Template*: Template-Branch01

Schedule Commit: YYYY/MM/DD HH:mm:ss

□ Retry on Device Unreachable

○ Auto Merge ● Overwrite

□ Reboot

Device Groups

□	Devices	Device Type	Template State	Appliance State	Device Modified	Differences	Association
☑	DG-Branch01						
☑	Branch01	Branch	OUT_OF_SYNC	IN_SYNC	✓		

Verify the Changes on the Device and Revert back to NGFW Services

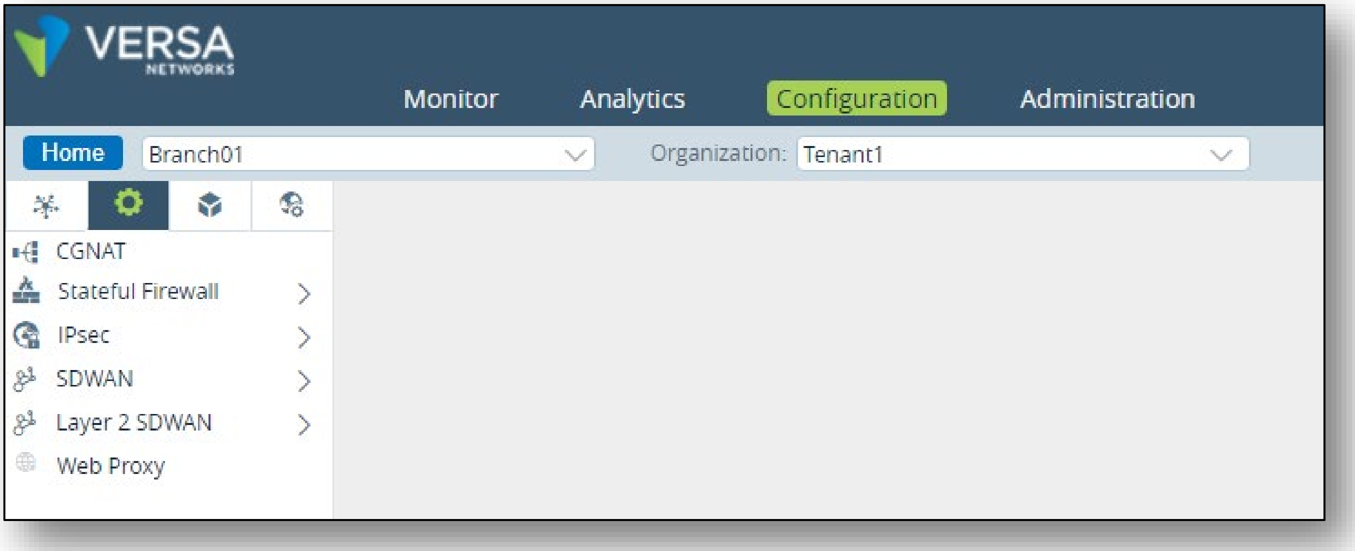
In the next lab steps you will:

- Verify that the changes have been applied to your device (security services changed from Next Gen Firewall to Stateful Firewall)
- Change your template services from SFW to NGFW services using the Template Workflow
- Re-deploy your template with the new services definition
- Apply the template changes to your device
- Verify that the security services changed from SFW to Next Gen Firewall services.

In the Versa Director dashboard, navigate to *Administration* > *Appliances* and locate your device in the appliances table.

Click your appliance in the Appliance table to open the Appliance Context mode of your device.

In the Appliance Context mode of your device, navigate to the *Configuration* > *Services* dashboard and fill in the diagram below:



Question: What type of security services are configurable on the device?

____

Question: Were the changes you made applied to the device? ______________________

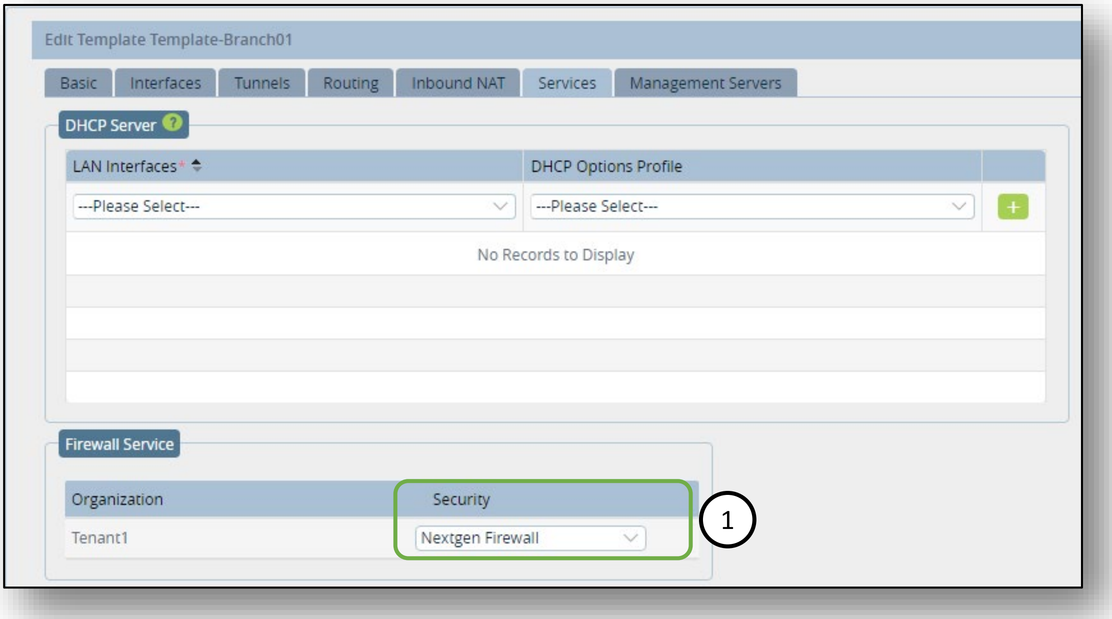
Next you will change the services available on your device back to Next Gen Firewall services by changing your template using the Template workflow.

Click the Home button next to your device name to exit Appliance Context mode. This returns you to the main Versa Director user interface.

In the main Versa Director user interface, navigate to *Workflows* > *Template* > *Templates* to display the saved Device Template workflows.

Locate your Template workflow in the table and click the workflow to open it for modification.

In your Template workflow, navigate to the Services tab.



Edit Template Template-Branch01

DHCP Server

LAN Interfaces*	DHCP Options Profile
---Please Select---	---Please Select---

No Records to Display

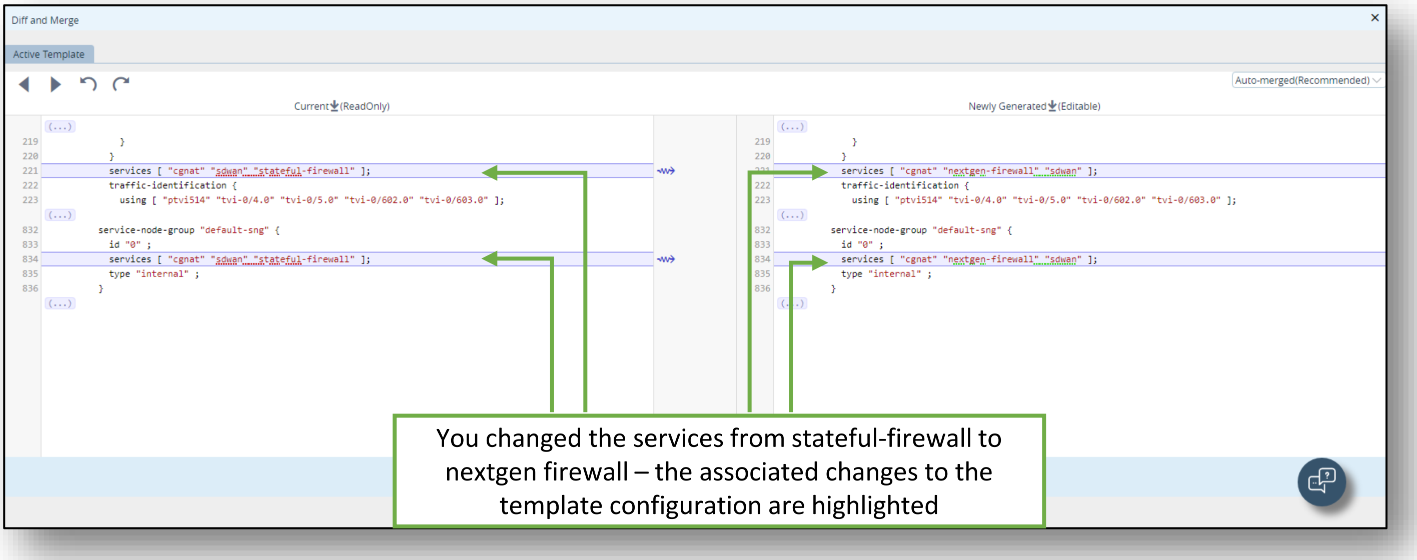
Firewall Service

Organization	Security
Tenant1	Nextgen Firewall

In the Services tab:

1. Change the services to Nextgen Firewall
2. Click Recreate

When an existing template is changed by updating the Template workflow, Versa Director will prompt you to confirm/validate the changes by doing a Difference (diff and merge) validation. The changes to the template will be displayed, and the administrator is required to verify and deploy the changes:



Diff and Merge

Current (ReadOnly)

```
(...)
            }
          }
          services [ "cgnat" "sdwan" "stateful-firewall" ];
          traffic-identification {
            using [ "ptvi514" "tvi-0/4.0" "tvi-0/5.0" "tvi-0/602.0" "tvi-0/603.0" ];
(...)
        service-node-group "default-sng" {
          id "0" ;
          services [ "cgnat" "sdwan" "stateful-firewall" ];
          type "internal" ;
        }
(...)
```

Newly Generated (Editable)

```
(...)
            }
          }
          services [ "cgnat" "nextgen-firewall" "sdwan" ];
          traffic-identification {
            using [ "ptvi514" "tvi-0/4.0" "tvi-0/5.0" "tvi-0/602.0" "tvi-0/603.0" ];
(...)
        service-node-group "default-sng" {
          id "0" ;
          services [ "cgnat" "nextgen-firewall" "sdwan" ];
          type "internal" ;
        }
(...)
```

You changed the services from stateful-firewall to nextgen firewall – the associated changes to the template configuration are highlighted

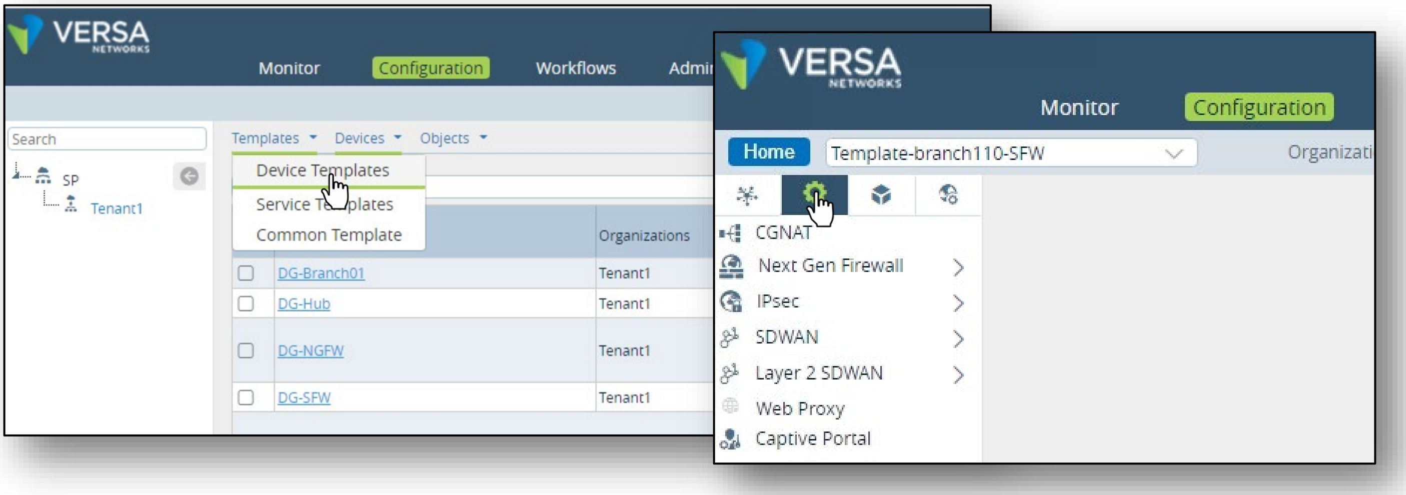
Click Deploy to apply the workflow changes to the template, and to re-write the template data.

Verify the Template Changes, and Apply the Update to your Device

Navigate to *Configuration* > *Templates* > *Device Templates*. Ensure that the *Tenant1* organization is selected in the left-side menu.

Locate and open the device template that you just updated through the Device Template workflow.

In the *Services* tab of the template configuration, verify that the Next Gen Firewall services are present in the template.

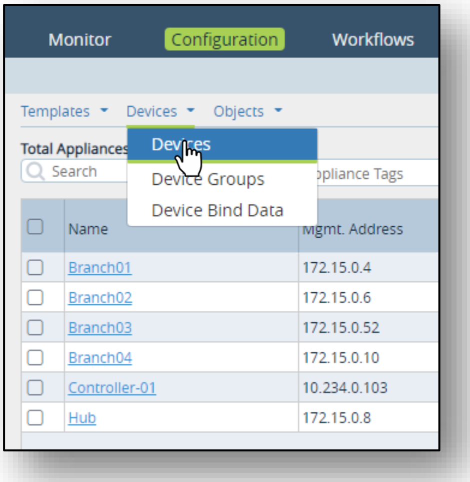


	Organizations
DG-Branch01	Tenant1
DG-Hub	Tenant1
DG-NGFW	Tenant1
DG-SFW	Tenant1

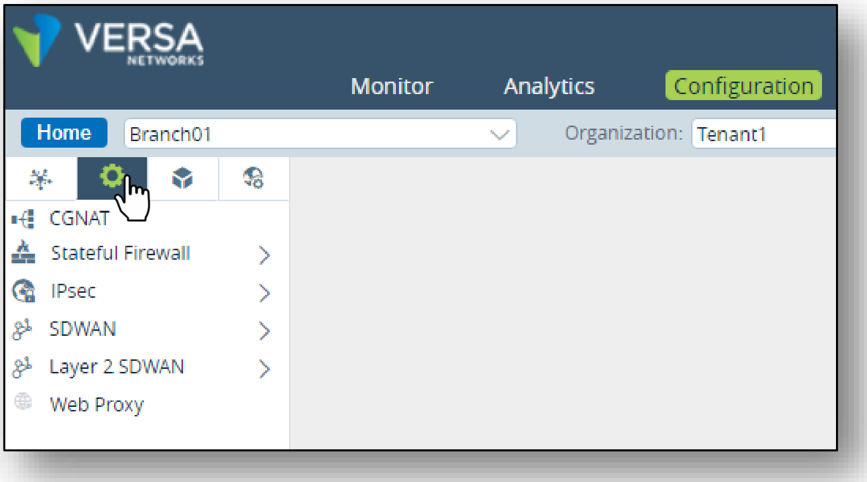
Navigate to the *Monitor* > *Devices* dashboard. Ensure that the Tenant1 organization is selected in the left-side menu.

Locate your device in the Devices table, and open your device. This places you in Appliance Context mode for your device (in the same way that clicking your device in the *Administration* > *Appliances* table places you in Appliance Context mode).

From Appliance Context mode, navigate to the *Configuration* > *Services* dashboard.



Name	Mgmt. Address
Branch01	172.15.0.4
Branch02	172.15.0.6
Branch03	172.15.0.52
Branch04	172.15.0.10
Controller-01	10.234.0.103
Hub	172.15.0.8



Question: What security services are available on the appliance?

____

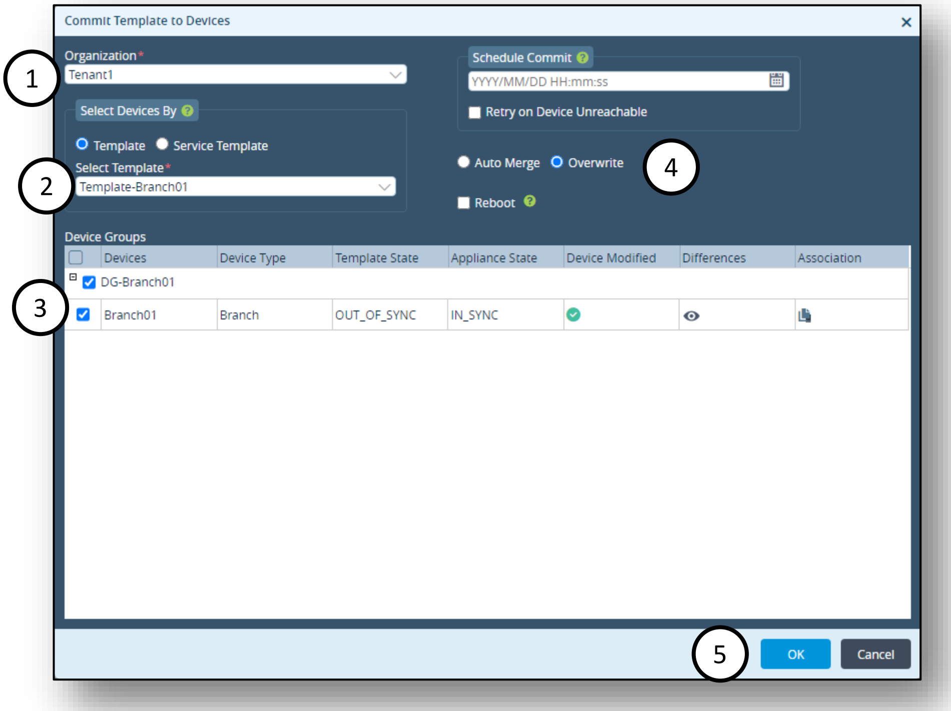
The Stateful Firewall services are still present on the device. Although you modified the template and verified the changes, the template changes haven't been committed to the devices that the template is assigned to.

Click the ***Home*** button next to your appliance name to exit Appliance Context mode.

From the main Versa Director user interface, click ***Commit Template***.

From the Commit dialog:

1. Select the Tenant1 organization
2. Select your template from the Select Template drop-down menu
3. Select your device from the device list
4. Ensure that Overwrite is selected
5. Click OK to commit the changes to the device.



Commit Template to Devices

Organization* Tenant1

Schedule Commit YYYY/MM/DD HH:mm:ss

□ Retry on Device Unreachable

Select Devices By

● Template ○ Service Template

Select Template* Template-Branch01

○ Auto Merge ● Overwrite

□ Reboot

Device Groups

□	Devices	Device Type	Template State	Appliance State	Device Modified	Differences	Association
☑	DG-Branch01						
☑	Branch01	Branch	OUT_OF_SYNC	IN_SYNC	✓	👁	📄

Verify the Changes on the End Device

Now that you have committed the template changes to your device, you will verify the changes one more time.

From the Versa Director user interface, navigate to *Administration > Appliances* and locate you device in the appliance list. Click your appliance to open the Appliance Context dashboard.

In the Appliance Context dashboard, navigate to *Configuration > Services*.

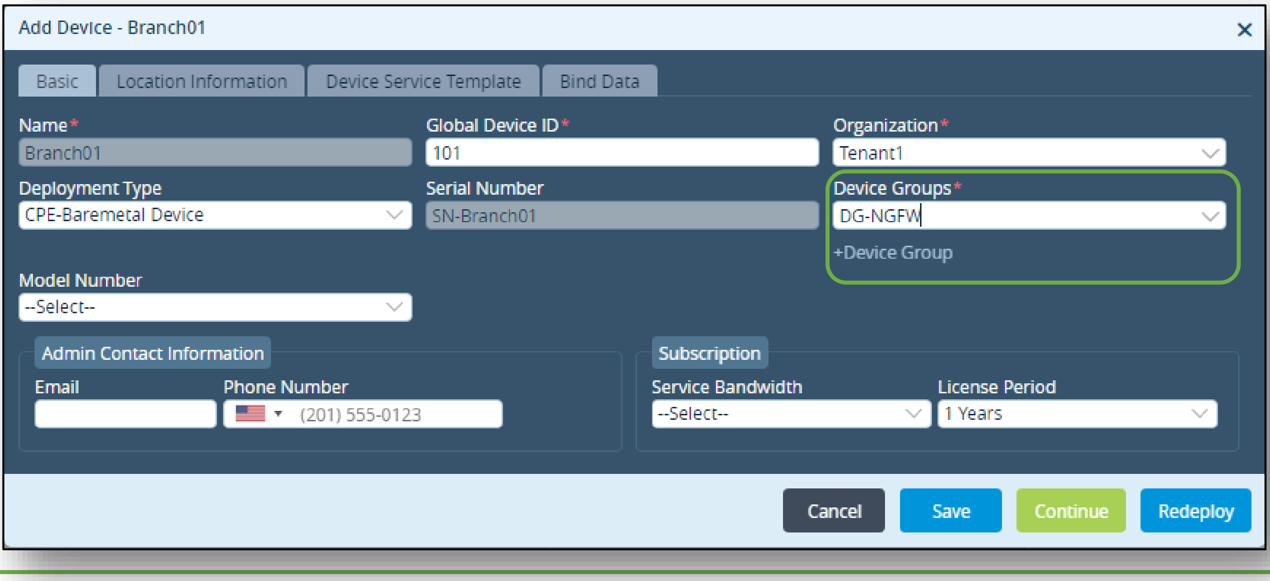
Question: Did the available services change from Stateful Firewall to Next Gen Firewall? _____

Exercise 6: Reset the Lab Environment

In this lab part you will:

- Re-assign your device to the Base-Template-NGFW template by re-assigning the Device Group in your Device workflow
- Commit the changes to reset your device configuration to the base configuration
- Delete your user-created Device Template Workflow (which will delete the template associated with the workflow)
- Delete the user-created Device Group that you created during this lab.

1. Navigate to the *Workflows > Devices > Device* hierarchy to display the saved device workflows.
2. Locate **your device** workflow in the Device Workflow table and click the workflow to open it.
3. In the Device workflow, set the Device Group to DG-NGFW.
4. Click Redeploy to update your device workflow and save the changes.



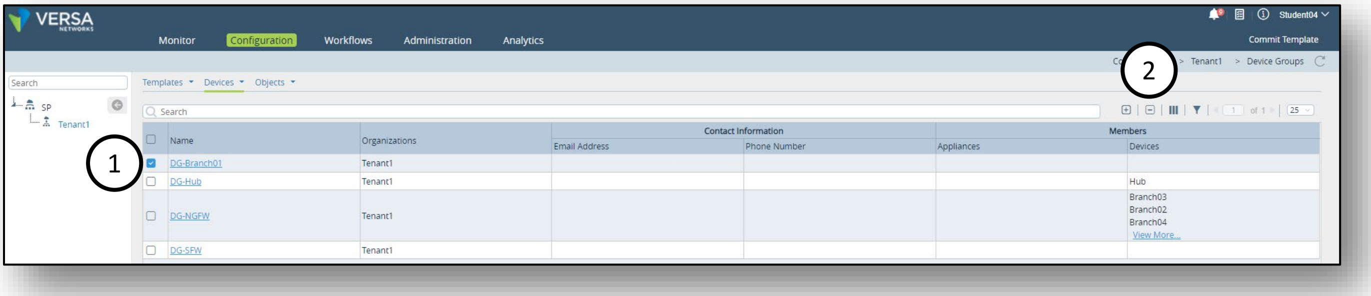
Add Device - Branch01

Name*: Branch01
Global Device ID*: 101
Organization*: Tenant1
Deployment Type: CPE-Baremetal Device
Serial Number: SN-Branch01
Device Groups*: DG-NGFW
Model Number: --Select--
Email:
Phone Number: (201) 555-0123
Service Bandwidth: --Select--
License Period: 1 Years

Navigate to the *Configuration > Devices > Device Groups* dashboard.

In the *Device Groups* table:

1. Check the box next to your user-defined device group
2. Click the ⊟ button to remove your user-defined device group.
3. Confirm the device group deletion

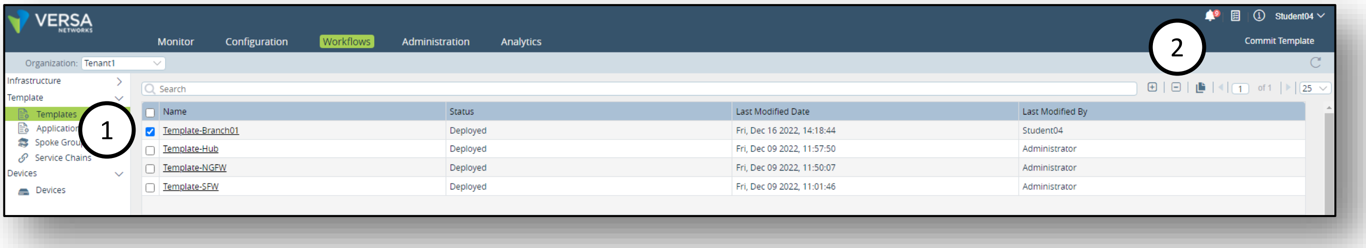


□	Name	Organizations	Contact Information		Members	
			Email Address	Phone Number	Appliances	Devices
☑	DG-Branch01	Tenant1				
□	DG-Hub	Tenant1				Hub
□	DG-NGFW	Tenant1				Branch03 Branch02 Branch04 View More...
□	DG-SFW	Tenant1				

Navigate to the *Workflows > Template > Templates* dashboard.

In the *Templates* workflow table:

1. Check the box next to your user-defined template workflow.
2. Click the ⊟ button to remove your user-defined template workflow
3. Confirm the workflow deletion



□	Name	Status	Last Modified Date	Last Modified By
☑	Template-Branch01	Deployed	Fri, Dec 16 2022, 14:18:44	Student04
□	Template-Hub	Deployed	Fri, Dec 09 2022, 11:57:50	Administrator
□	Template-NGFW	Deployed	Fri, Dec 09 2022, 11:50:07	Administrator
□	Template-SFW	Deployed	Fri, Dec 09 2022, 11:01:46	Administrator

To finalize the configuration change, click ***Commit Template*** in the top right, select the Tenant1 organization, and the Template-NGFW template from the Commit Template to Devices dialog. Locate your device in the device groups table, select your device, and click OK to commit the changes to your device.

STOP **STOP!** Notify your instructor that you have completed this lab.

Versa SD-WAN Topologies

The Versa Networks lab environment consists of a fixed, pre-configured topology that will allow you to explore, configure, and manage Versa Networks CPEs by using Versa Director, the central management and orchestration platform for a Versa Secure SD-WAN solution. After completing this lab, you will be able to:

- Analyze the configuration components of full mesh and hub-and-spoke topologies
- Configure and analyze the following topologies:
  - Full Mesh
  - Spoke-to-Hub-Only
  - Spoke-to-Spoke-via-Hub
  - Spoke-to-Spoke-Direct

In this lab, you will be assigned a single CPE device (Branch device) for configuration and monitoring.

The lab environment is accessed through Amazon Workspaces. You should have received an email to allow you to register your Amazon Workspaces account and set your password.

NOTE: It is common for the Amazon Workspaces email to be sent to the spam/junk folder. If you have not received the registration email, check those folders.

The remote desktop connection opens a remote workstation, where you will use various tools to navigate and configure the lab environment. The main tool you will use in this lab is Versa Director. Versa Director can be accessed by opening the Google Chrome browser on the Remote Desktop. There is a bookmark to the Versa Director device in the Google Chrome bookmark bar.

This lab environment is a shared environment. There may be up to 24 students in the environment. Each student has their own remote desktop, but the Versa Director is shared. Because of the shared environment, you may see configuration templates, device groups, workflows, and devices that other students have created, or that have been pre-provisioned within Versa Director. It is important that you only modify the configuration components that are assigned to you by your instructor.

Look for these hints to help you in the labs

During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not be the same, etc.) Do not be alarmed if your results vary slightly from the results shown in the lab guide. The important thing is that the lab functions in the desired manner.

This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

Now that we’ve discussed what is expected, let’s get started!

Lab Exercise Overview

In this lab you will perform various tasks. You will begin by examining some pre-configured objects within Versa Director that will be used to build hub and spoke topologies. A flow of the lab exercises is:

Examine the Spoke Groups that are pre-configured in the Spoke Groups workflow table

Analyze the LAN routes learned on your device, and the BGP next-hops of the routes.

Create a new device template, named after your username and device ID, that is configured as a spoke device configuration (you will use a Device Template Workflow to create the new template)
The template will be configured with the S2H-Only spoke group

Create a new device group named after your username and device ID that references the new template you created

Create a new device group named after your username and device ID that references the new template you created

Re-assign your device to the new device group using the Device Workflow and redeploy the device workflow

Commit the template to reconfigure your device

Analyze the LAN routes learned on your device, and the BGP next-hops of the routes.

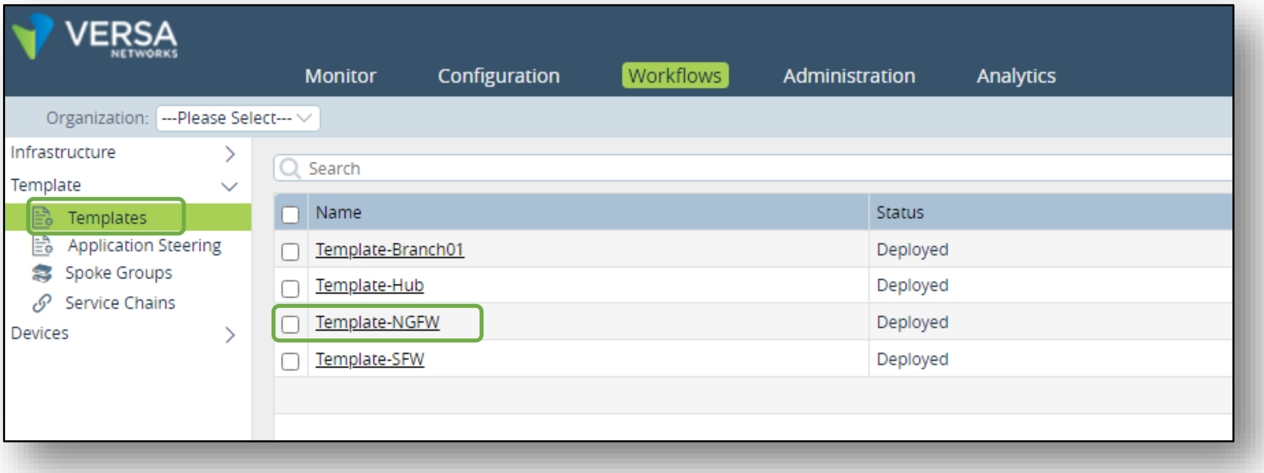
Analyze the LAN routes learned on your device, and the BGP next-hops of the routes.

Modify the spoke group in your template workflow to S2SviaH, re-deploy the workflow to recreate the template, then you will commit the template to your device

Analyze the LAN routes learned on your device, and the BGP next-hops (remote gateway) of the routes.

Exercise 1: Examine Full Mesh Configuration and Reachability

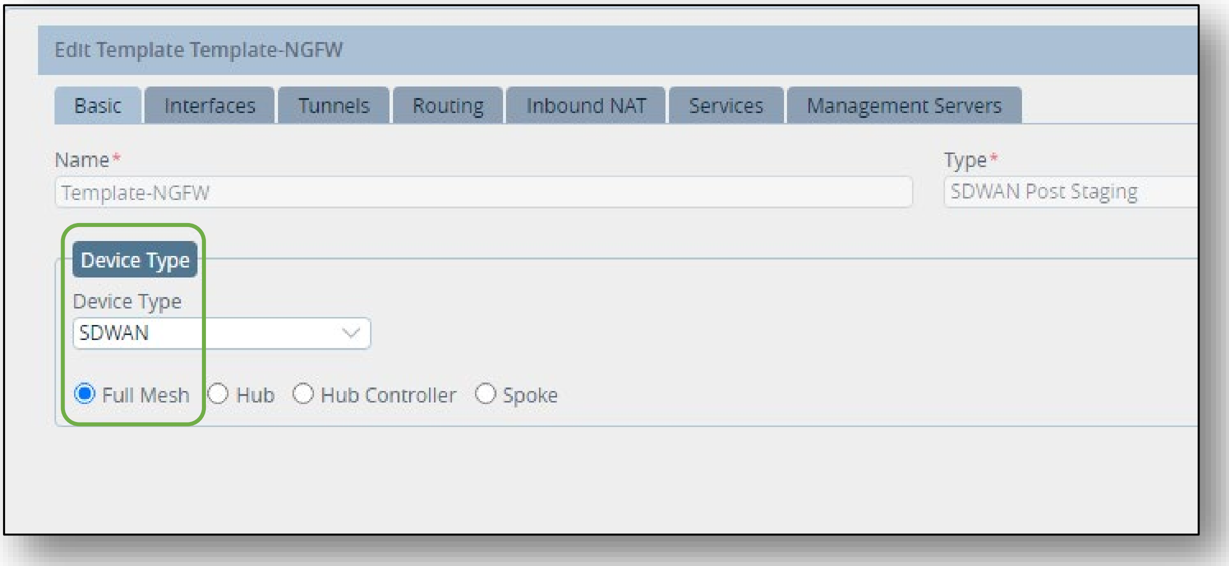
Open the Workflows tab in Versa Director and navigate to the *Template > Templates* dashboard. Locate the Template-NGFW template workflow and click on the workflow to open it for viewing.



Organization: ---Please Select---

	Name	Status
□	Template-Branch01	Deployed
□	Template-Hub	Deployed
□	Template-NGFW	Deployed
□	Template-SFW	Deployed

The Template-NGFW workflow creates a device template that is configured for Full Mesh topology.



Name* Template-NGFW

Type* SDWAN Post Staging

Device Type SDWAN

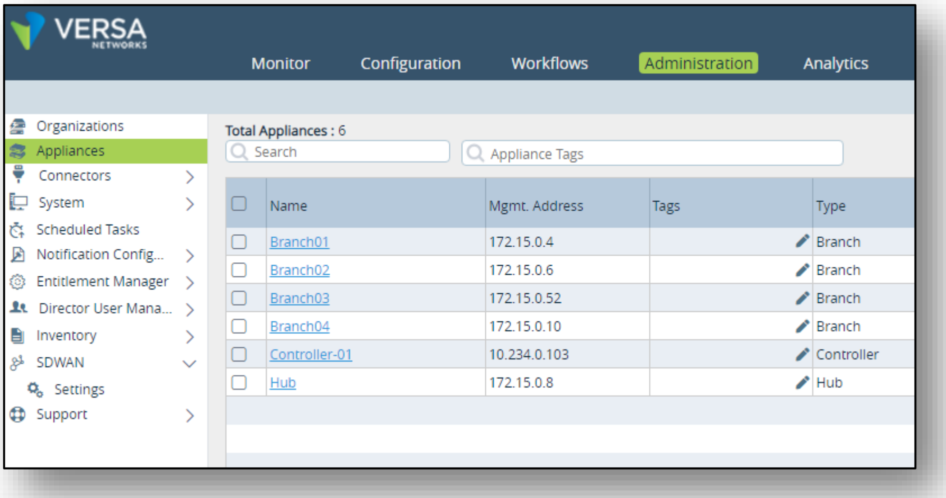
● Full Mesh ○ Hub ○ Hub Controller ○ Spoke

The Full Mesh setting creates default BGP policies policies that send all routes to the Versa Controllers, and that allow all routes received from the Versa Controllers. This creates a forwarding plane that has visibility of and that can forward to all remote CPE devices.

Click *Cancel* to close the Template Workflow. DO NOT MAKE ANY CHANGES!

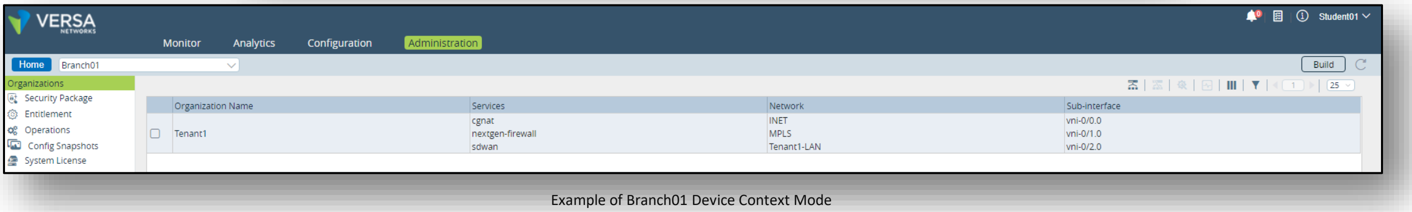
Next you'll analyze the full mesh reachability by using Versa Director and the Monitor tab (Appliance Context mode).

From Versa Director, navigate to *Administration > Appliances* and locate your device in the Appliances table. Click on your appliance to open the Appliance Context mode of your device.



Total Appliances : 6

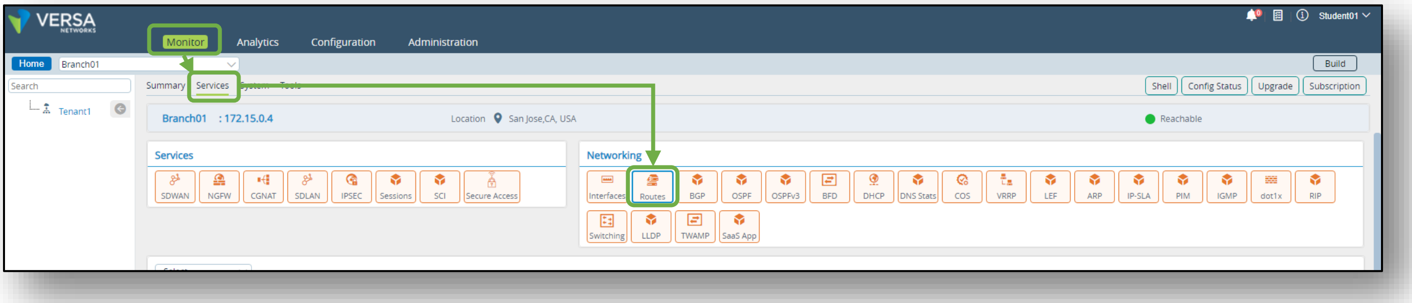
☐	Name	Mgmt. Address	Tags	Type
☐	Branch01	172.15.0.4		Branch
☐	Branch02	172.15.0.6		Branch
☐	Branch03	172.15.0.52		Branch
☐	Branch04	172.15.0.10		Branch
☐	Controller-01	10.234.0.103		Controller
☐	Hub	172.15.0.8		Hub



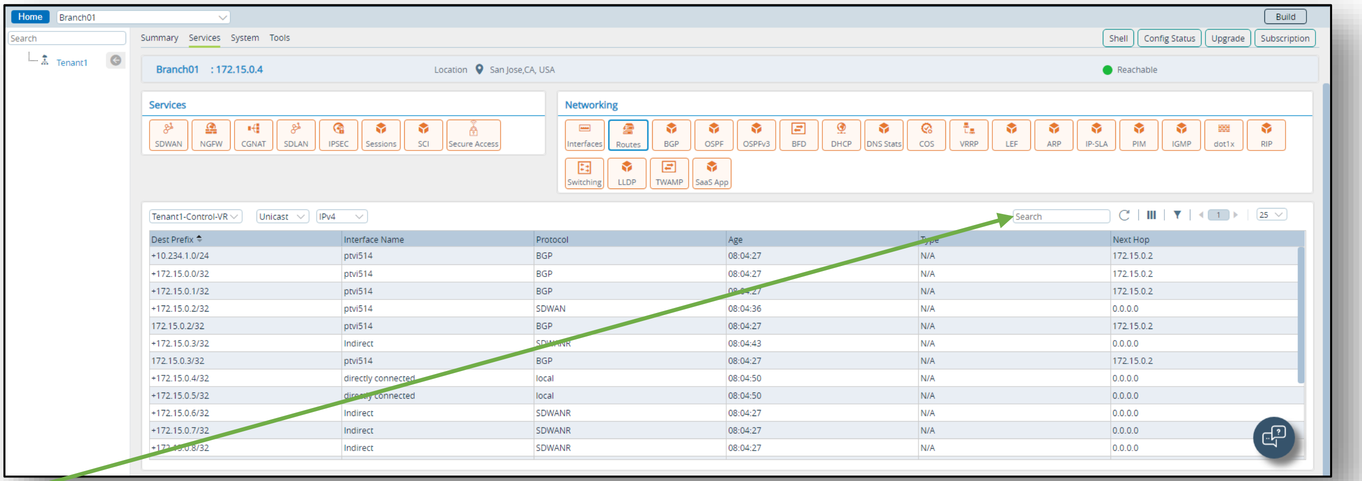
☐	Organization Name	Services	Network	Sub-interface
☐	Tenant1	cgnat nextgen-firewall sdwan	INET MPLS Tenant1-LAN	vni-0/0.0 vni-0/1.0 vni-0/2.0

Example of Branch01 Device Context Mode

From device context mode of your device, click on *Monitor* to open the device monitoring dashboard. Locate and select the *Services* tab to open the services monitoring dashboard. You will be examining the *Route* service to identify what routes and remote nodes are present and visible to your device.



Branch01 : 172.15.0.4 Location San Jose,CA, USA ● Reachable



Branch01 : 172.15.0.4 Location San Jose,CA, USA Reachable

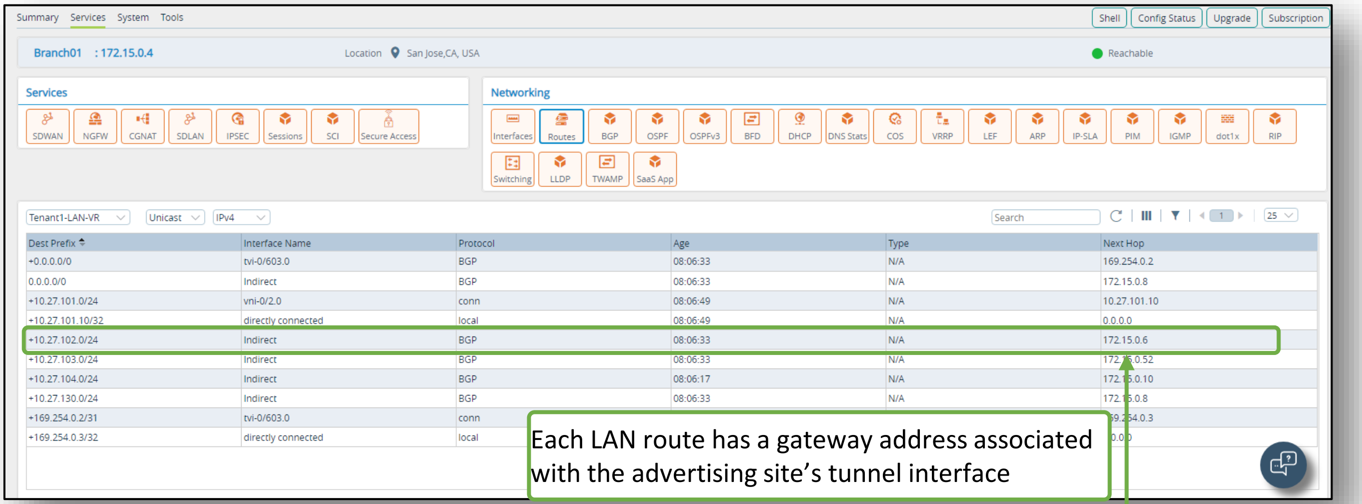
Tenant1-Control-VR Unicast IPv4

Dest Prefix	Interface Name	Protocol	Age	Type	Next Hop
+10.234.1.0/24	ptvi514	BGP	08:04:27	N/A	172.15.0.2
+172.15.0.0/32	ptvi514	BGP	08:04:27	N/A	172.15.0.2
+172.15.0.1/32	ptvi514	BGP	08:04:27	N/A	172.15.0.2
+172.15.0.2/32	ptvi514	SDWAN	08:04:36	N/A	0.0.0.0
172.15.0.2/32	ptvi514	BGP	08:04:27	N/A	172.15.0.2
+172.15.0.3/32	Indirect	SDWANR	08:04:43	N/A	0.0.0.0
172.15.0.3/32	ptvi514	BGP	08:04:27	N/A	172.15.0.2
+172.15.0.4/32	directly connected	local	08:04:50	N/A	0.0.0.0
+172.15.0.5/32	directly connected	local	08:04:50	N/A	0.0.0.0
+172.15.0.6/32	Indirect	SDWANR	08:04:27	N/A	0.0.0.0
+172.15.0.7/32	Indirect	SDWANR	08:04:27	N/A	0.0.0.0
+172.15.0.8/32	Indirect	SDWANR	08:04:27	N/A	0.0.0.0

You can filter the routes listed by entering filter text in the Search box

Locate the SDWAN routes in the route table. SDWAN routes are routes routes that are advertised and received as Versa-Private routes (node advertisements). Note that each remote device advertises 2 SDWAN routes. The first is the endpoint used for clear-channel reachability, and the second is the endpoint used for encrypted-channel reachability. The encrypted endpoint is the default endpoint in the routing table.

You can change which virtual router's routing table is displayed by selecting the virtual router from the drop-down menu.

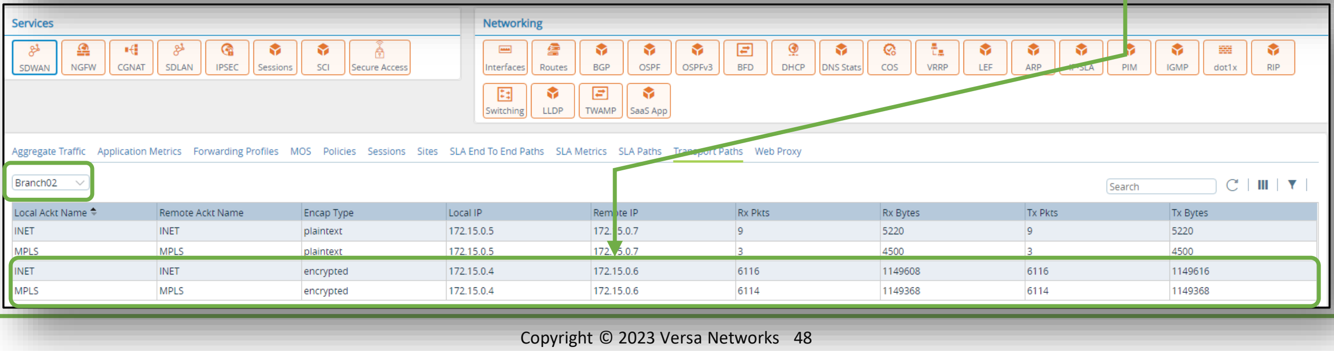


Branch01 : 172.15.0.4 Location San Jose,CA, USA Reachable

Tenant1-LAN-VR Unicast IPv4

Dest Prefix	Interface Name	Protocol	Age	Type	Next Hop
+0.0.0.0/0	tvi-0/603.0	BGP	08:06:33	N/A	169.254.0.2
0.0.0.0/0	Indirect	BGP	08:06:33	N/A	172.15.0.8
+10.27.101.0/24	vni-0/2.0	conn	08:06:49	N/A	10.27.101.10
+10.27.101.10/32	directly connected	local	08:06:49	N/A	0.0.0.0
+10.27.102.0/24	Indirect	BGP	08:06:33	N/A	172.15.0.6
+10.27.103.0/24	Indirect	BGP	08:06:33	N/A	172.15.0.52
+10.27.104.0/24	Indirect	BGP	08:06:17	N/A	172.15.0.10
+10.27.130.0/24	Indirect	BGP	08:06:33	N/A	172.15.0.8
+169.254.0.2/31	tvi-0/603.0	conn			169.254.0.3
+169.254.0.3/32	directly connected	local			0.0.0.0

Each LAN route has a gateway address associated with the advertising site's tunnel interface



Branch02

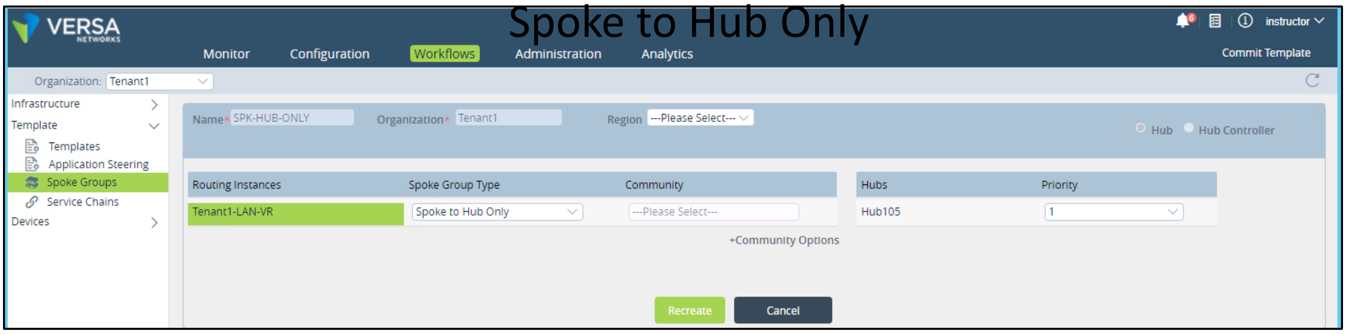
Local Ackt Name	Remote Ackt Name	Encap Type	Local IP	Remote IP	Rx Pkts	Rx Bytes	Tx Pkts	Tx Bytes
INET	INET	plaintext	172.15.0.5	172.15.0.7	9	5220	9	5220
MPLS	MPLS	plaintext	172.15.0.5	172.15.0.7	3	4500	3	4500
INET	INET	encrypted	172.15.0.4	172.15.0.6	6116	1149608	6116	1149616
MPLS	MPLS	encrypted	172.15.0.4	172.15.0.6	6114	1149368	6114	1149368

Exercise 2: Examine Spoke Groups

In the next part of the lab exercise, you will examine the pre-configured spoke groups using Versa Director. The spoke groups are created and can be viewed through the *Workflows > Template > Spoke Groups* dashboard.

There are 4 pre-configured spoke groups:

- SPK-SPK-HUB: Configured as a spoke-to-spoke-via-hub spoke group, with hub 105 as the hub device.
- SK-HUB-ONLY: Configured as a spoke-to-hub-only spoke group, with hub 105 as the hub device.
- SPKTOSPK-DIRECT-MESHGRP-101: Configured as a Spoke to Spoke Direct spoke group, with BGP community 101 added to the group.
- SPKTOSPK-DIRECT-MESHGRP-102: Configured as a Spoke to Spoke Direct spoke group, with BGP community 102 added to the group.



Spoke to Hub Only

Organization: Tenant1

Name* SPK-HUB-ONLY Organization* Tenant1 Region ---Please Select---

○ Hub ○ Hub Controller

Routing Instances	Spoke Group Type	Community	Hubs	Priority
Tenant1-LAN-VR	Spoke to Hub Only	---Please Select---	Hub105	1

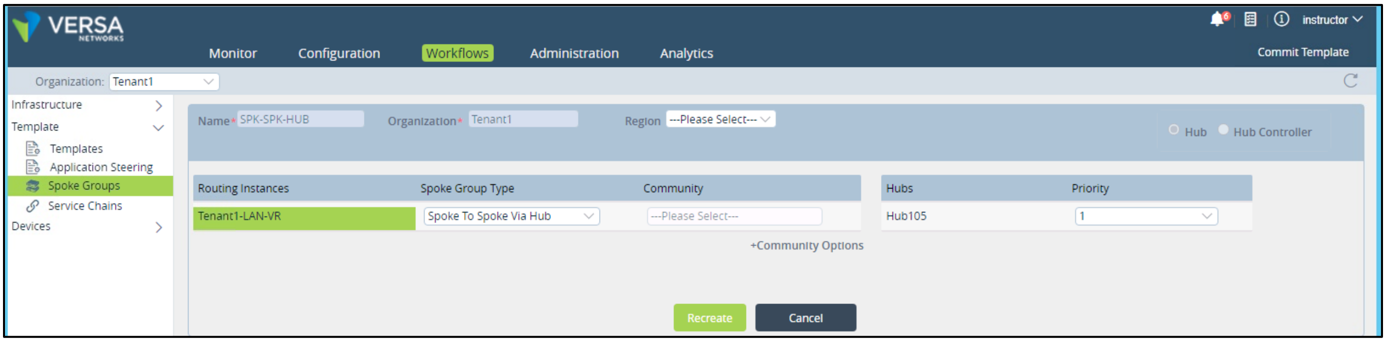
Click on the **SPK-HUB-ONLY** spoke group to view its configuration.

The spoke group has the following parameters:

- **Routing Instances**: This identifies the customer LAN-facing routes that will be advertised to the hub within this spoke group.
- **Spoke Group Type**: This determines the reachability (topology) of the hub-and-spoke deployment. Routing policy will be configured on devices that belong to this spoke group to determines which routes are accepted from the controller, what community values are added to BGP route redistribution policies, etc.
- **Community**: Used for Spoke-to-Spoke Direct only (adds an extra region/group specific BGP community).
- **Hubs**: Allows you to list the hubs from which received routes will be accepted (uses BGP routing policy to accept/reject routes received from hubs).
- **Priority**: The priority of the routes received from the hubs (uses BGP policy/Local Preference to adjust the priority of routes received from hubs). Multiple hubs can be configured, each with a different priority.

Click Cancel to close the dialog without making any changes.

Spoke to Spoke via Hub



Organization: Tenant1

Name* SPK-SPK-HUB Organization* Tenant1 Region ---Please Select---

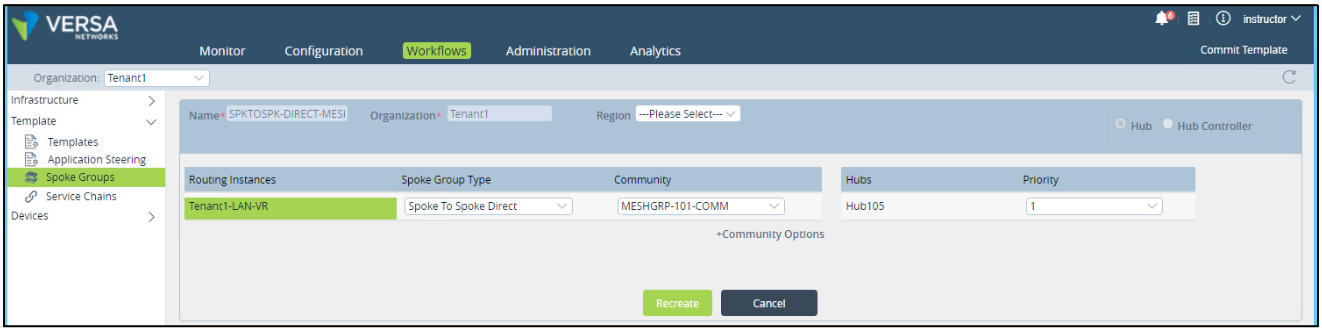
Routing Instances	Spoke Group Type	Community	Hubs	Priority
Tenant1-LAN-VR	Spoke To Spoke Via Hub	---Please Select---	Hub105	1

Click on the **SPK-SPK-HUB** spoke group to view its configuration.

The spoke group has the following same parameter set as the Spoke to Hub Only topology. However, when a spoke group is designated as Spoke To Spoke Via Hub type, the BGP policies created by Versa Director for the CPE devices add different community values to routes advertised by the CPE devices. These new community values allow the hub to re-process and re-advertise the routes to other devices (with the hub set as the BGP next-hop). These policies are managed and coordinated by Versa Director automatically, and the administrator does not have to manage them directly.

Click Cancel to close the dialog without making any changes.

Spoke to Spoke Direct



Organization: Tenant1

Name* SPKTOSPK-DIRECT-MESI Organization* Tenant1 Region ---Please Select---

Routing Instances	Spoke Group Type	Community	Hubs	Priority
Tenant1-LAN-VR	Spoke To Spoke Direct	MESHGRP-101-COMM	Hub105	1

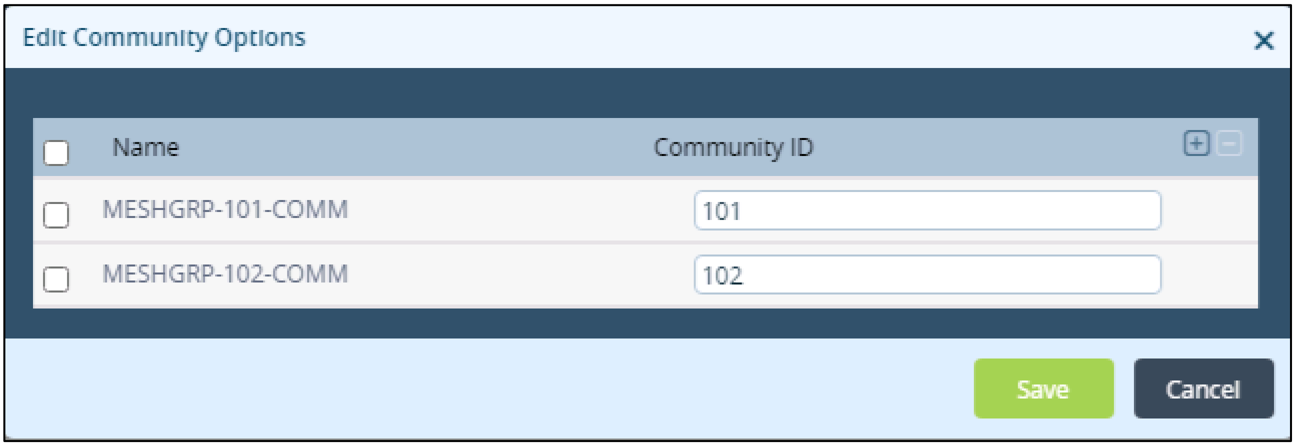
Click on the **SPKTOSPK-DIRECT-MESHGRP-101** spoke group to view its configuration.

The spoke group has the same parameters as the other spoke group types, but adds an additional BGP community parameter to define the mesh group to which the devices will belong. All devices assigned to the same mesh group will be able to form point-to-point tunnels between devices. Devices that do not have the same BGP community assigned will behave as Spoke to Spoke Via Hub, and will be required to forward traffic through the hub to reach the remote networks.

Click the Community drop-down to view the options.

These options are named communities that the administrator configures.

Click the *+Community Options* link to view the BGP community dialog.



Edit Community Options

□	Name	Community ID
□	MESHGRP-101-COMM	101
□	MESHGRP-102-COMM	102

BGP Communities consist of 2 parts. The Versa Director user interface allows the administrator to configure the 2nd part of the community value (the Community ID value show above). This allows Versa Director to ensure that different organizations cannot assign the same complete community value to a mesh group, and maintains multi-tenant routing consistency. In the example, if another organization in a multi-tenant environment assigns the same mesh group community value of 101, the complete community value will still be unique in the control plane, as the first part of the BGP community will be organization specific.

Click Cancel to close the Community Options dialog without making any changes.

Click Cancel again to close the Spoke Group dialog.

Exercise 4: Add Device to a Spoke Group

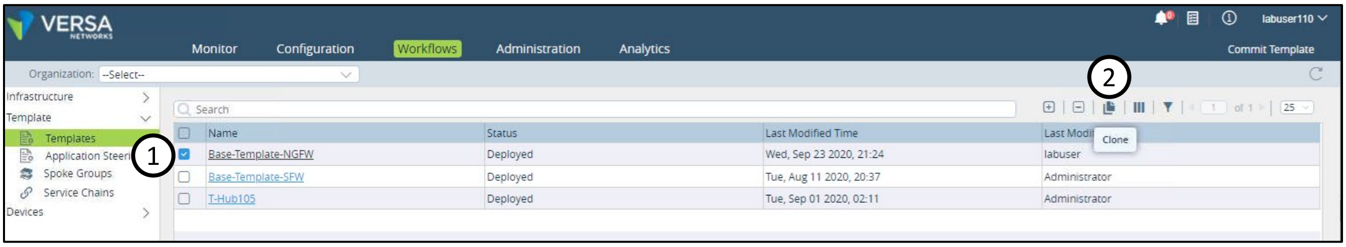
In the next part of the lab exercise, you will create a Device Template Workflow that will be used to configure devices to be part of a Spoke-to-Hub-Only topology. The tasks that will be complete in this lab exercise are:

- Create a new template using a Template Workflow.
- The template workflow should be configured as a Spoke topology, with the SPK-HUB-ONLY spoke group.
- The template workflow can be created by cloning the Base-Template-NGFW Template Workflow, giving it a new name, and changing the topology type.
- Create a new device group that references the new template.
- Assigning your device to the new device group. You can use your device workflow to perform this re-assignment.
- Commit the template to the device.

The following steps will walk you through these processes.

Create a new device template with a device template workflow.

1. Navigate to the *Workflows > Template > Templates* dashboard. From the Templates workflow table, check the box next to the Base-Template-NGFW workflow. This will enable the *Clone* button on the task bar.
2. Click the *Clone* button to create a clone (copy) of the workflow.



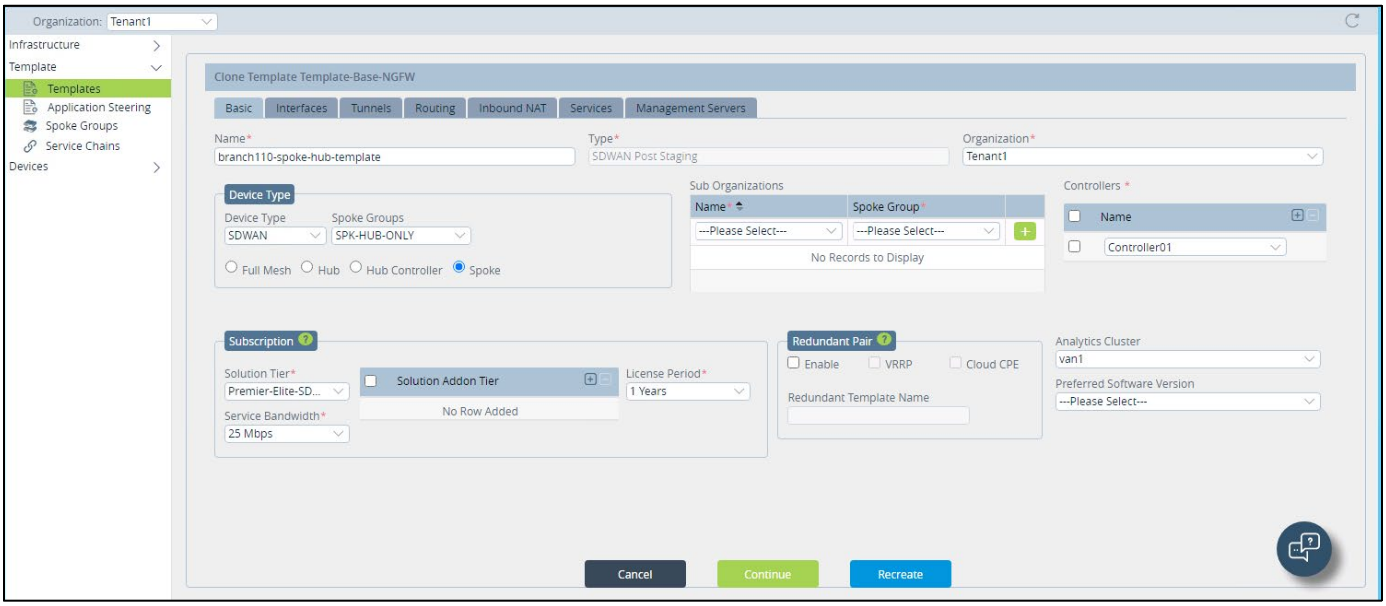
☐	Name	Status	Last Modified Time	Last Modi
☑	Base-Template-NGFW	Deployed	Wed, Sep 23 2020, 21:24	labuser
☐	Base-Template-SFW	Deployed	Tue, Aug 11 2020, 20:37	Administrator
☐	T-Hub105	Deployed	Tue, Sep 01 2020, 02:11	Administrator

In the Clone Template dialog, rename the workflow to a name that is unique to your user-id/branch-id and the topology type. e.g. *branch110-spoke-hub-template*

Change the Device Type to *Spoke* and select *SPK-HUB-ONLY* as the Spoke Group.

All other parameters of the workflow should remain the same.

Click Recreate button to save the workflow and to create a new template based on the workflow parameters.



Clone Template Template-Base-NGFW

Name*: branch110-spoke-hub-template

Type*: SDWAN Post Staging

Organization*: Tenant1

Device Type

Device Type: SDWAN

Spoke Groups: SPK-HUB-ONLY

○ Full Mesh ○ Hub ○ Hub Controller ● Spoke

Sub Organizations

Name*	Spoke Group*
---Please Select---	---Please Select---
No Records to Display	

Controllers*

□	Name
□	Controller01

Subscription

Solution Tier*: Premier-Elite-SD...

Service Bandwidth*: 25 Mbps

□	Solution Addon Tier
No Row Added	

License Period*: 1 Years

Redundant Pair

□ Enable □ VRRP □ Cloud CPE

Redundant Template Name:

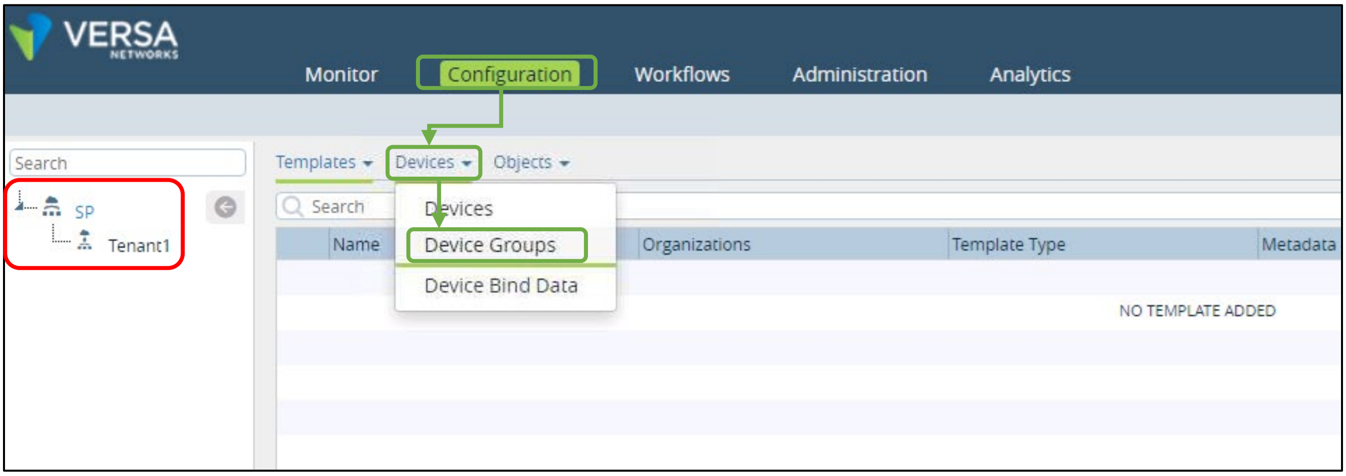
Analytics Cluster: van1

Preferred Software Version: ---Please Select---

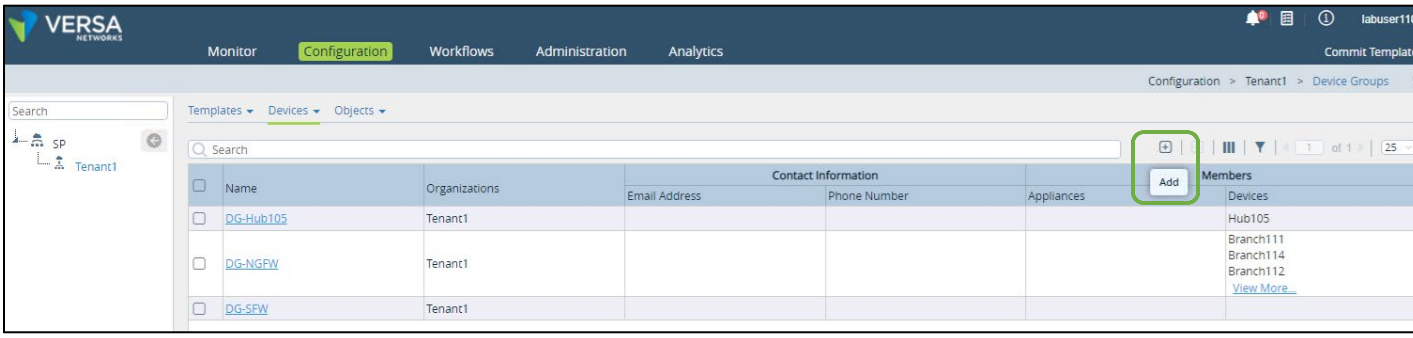
Example Workflow Clone

Create a new device group that is associated with the new template.

1. Navigate to the *Configuration > Devices > Device Groups* dashboard. Ensure that the *Tenant1* organization is selected on the left-side menu.
2. From the Device Groups dashboard, click the + button to create a new device group.
3. Give the device group a unique name based on your node or user ID, and associate the device group with the device template you created in the previous exercise.

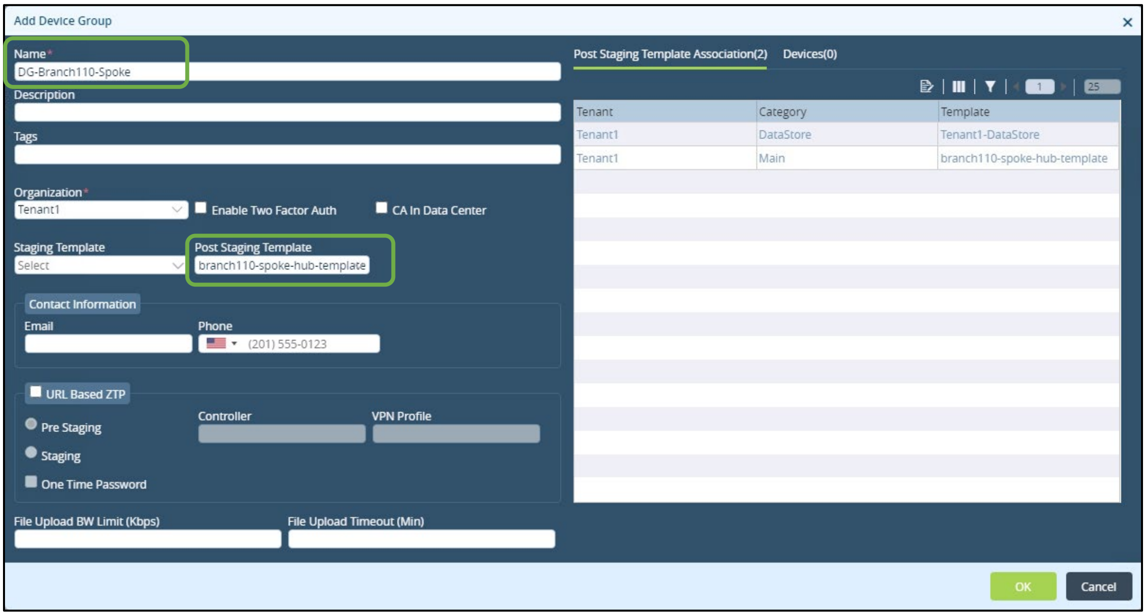


Step 1



			Contact Information			Members
☐	Name	Organizations	Email Address	Phone Number	Appliances	Devices
☐	DG-Hub105	Tenant1				Hub105
☐	DG-NGFW	Tenant1				Branch111 Branch114 Branch112 View More...
☐	DG-SFW	Tenant1				

Step 2



Name* DG-Branch110-Spoke

Description

Tags

Organization* Tenant1 ☐ Enable Two Factor Auth ☐ CA In Data Center

Staging Template Select

Post Staging Template branch110-spoke-hub-template

Contact Information

Email

Phone (201) 555-0123

☐ URL Based ZTP

○ Pre Staging

○ Staging

☐ One Time Password

Controller

VPN Profile

File Upload BW Limit (Kbps)

File Upload Timeout (Min)

Tenant	Category	Template
Tenant1	DataStore	Tenant1-DataStore
Tenant1	Main	branch110-spoke-hub-template

Step 3

Question: Where do you find the complete list of templates that are associated with the device group, and that will be used as sources for the final device configurations?

____

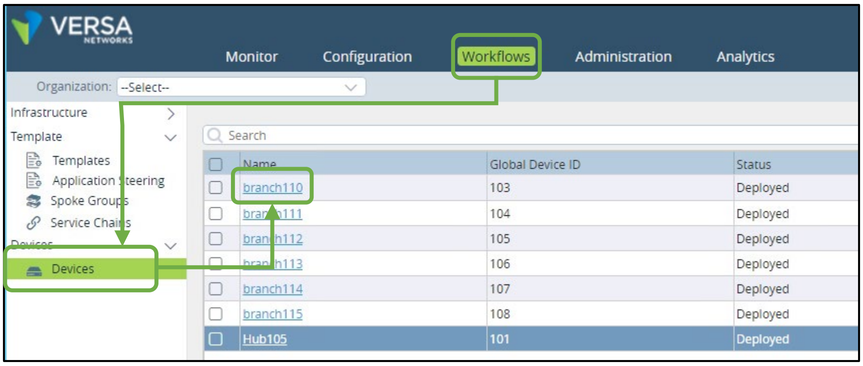
____

Answer: The Post Staging Template Association table shows all of the templates that will be used to build the final device configurations. This includes the Common Template (DataStore) and any service templates that will be applied to the configuration.

Change the device group to which your device belongs

In the next steps you will re-assign your device to the device group you created in the previous steps, which will assign a new configuration to your device.

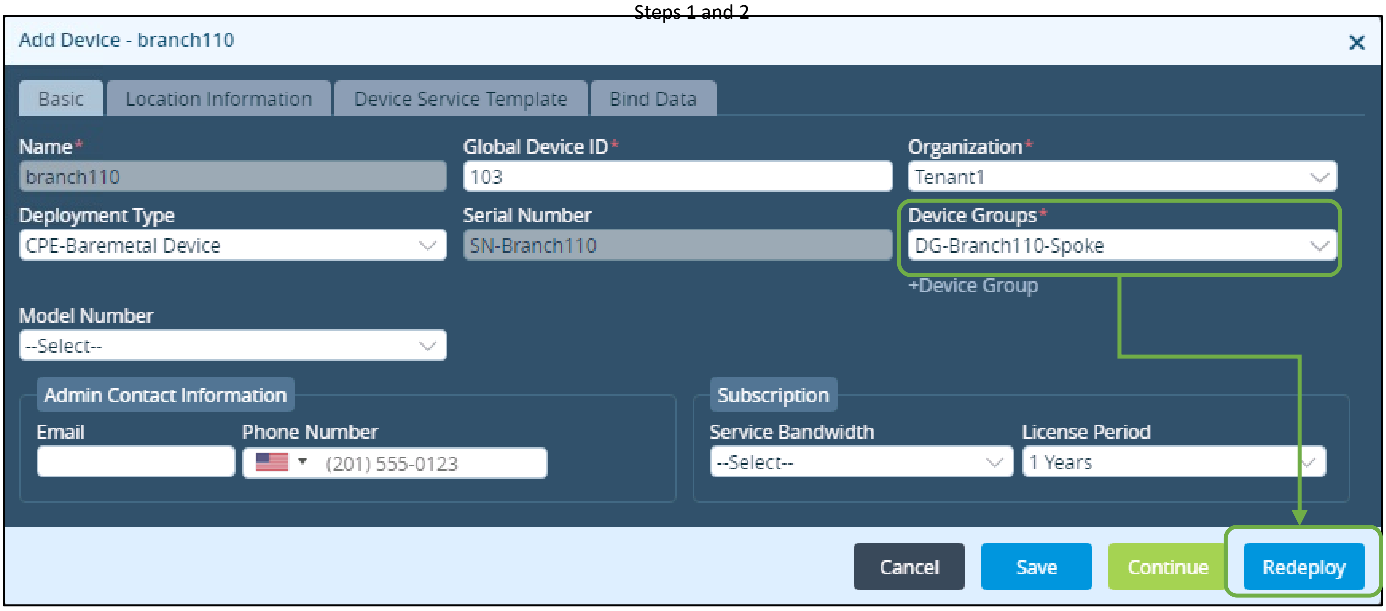
1. Navigate to the *Workflows > Devices > Devices* dashboard and locate the workflow that is associated with your device in the table (this is the workflow that was used to create your device in the pre-staging environment).
2. Click your device workflow to open the workflow for modification.
3. In the *Basic* tab of your device workflow, assign the new device group you created in the previous steps to the device.
4. Click the *Redeploy* button to recreate your device in Versa Director. This will re-configure the device parameters within Versa Director, but the changes still need to be pushed to the end device with the Commit Template function.



Organization: --Select--

Name	Global Device ID	Status
branch110	103	Deployed
branch111	104	Deployed
branch112	105	Deployed
branch113	106	Deployed
branch114	107	Deployed
branch115	108	Deployed
Hub105	101	Deployed

Steps 1 and 2



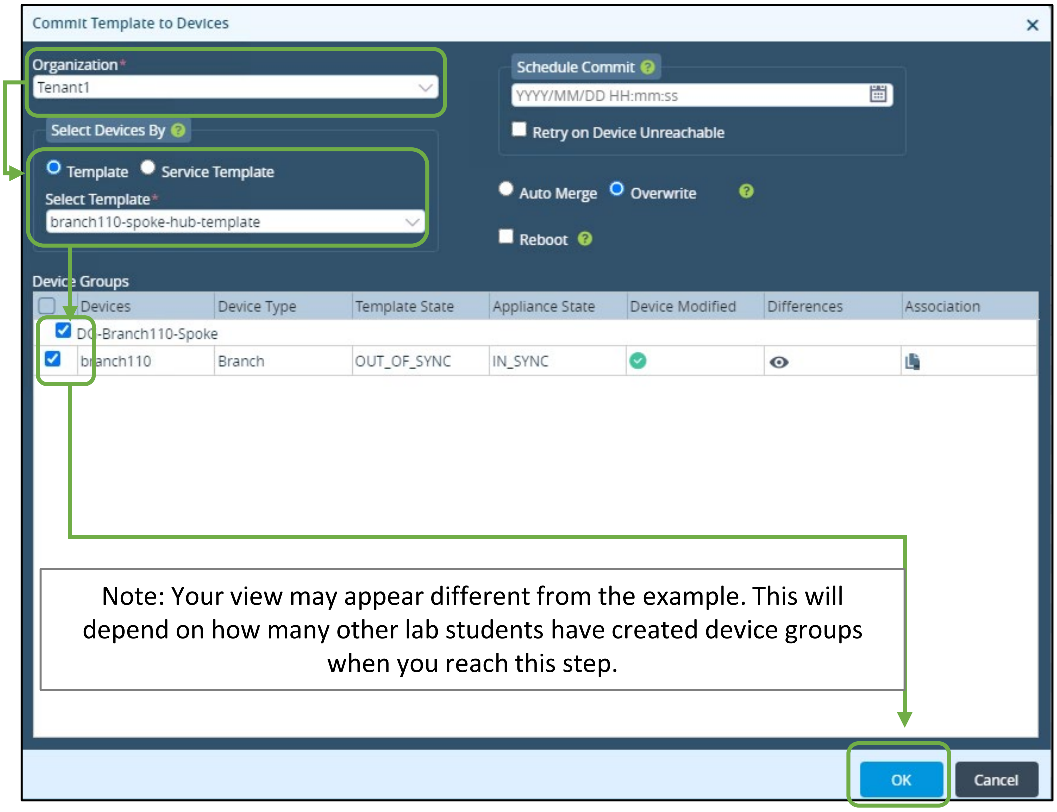
Name* branch110
Global Device ID* 103
Organization* Tenant1
Deployment Type CPE-Baremetal Device
Serial Number SN-Branch110
Device Groups* DG-Branch110-Spoke
Model Number --Select--
Email
Phone Number (201) 555-0123
Service Bandwidth --Select--
License Period 1 Years

Steps 3 and 4

Commit the Template to Your Device

In the next steps you will commit the changes to your device. You do this by applying the device group settings to the appliances through the Commit Template process.

1. Click the *Commit Template* button in the top-right corner of Versa Director.
2. In the Commit dialog, select Tenant1 from the organization dropdown menu.
3. Select your template from the Select Template dropdown menu.
4. Locate your Device Group in the Device Groups table, and mark the box next to your device.
5. Click *OK* to commit the template.



Commit Template to Devices

Organization*: Tenant1

Select Devices By: ● Template ○ Service Template

Select Template*: branch110-spoke-hub-template

Schedule Commit: YYYY/MM/DD HH:mm:ss

□ Retry on Device Unreachable

○ Auto Merge ● Overwrite

□ Reboot

Device Groups

□	Devices	Device Type	Template State	Appliance State	Device Modified	Differences	Association
☑	DG-Branch110-Spoke						
☑	branch110	Branch	OUT_OF_SYNC	IN_SYNC	✓		

Note: Your view may appear different from the example. This will depend on how many other lab students have created device groups when you reach this step.

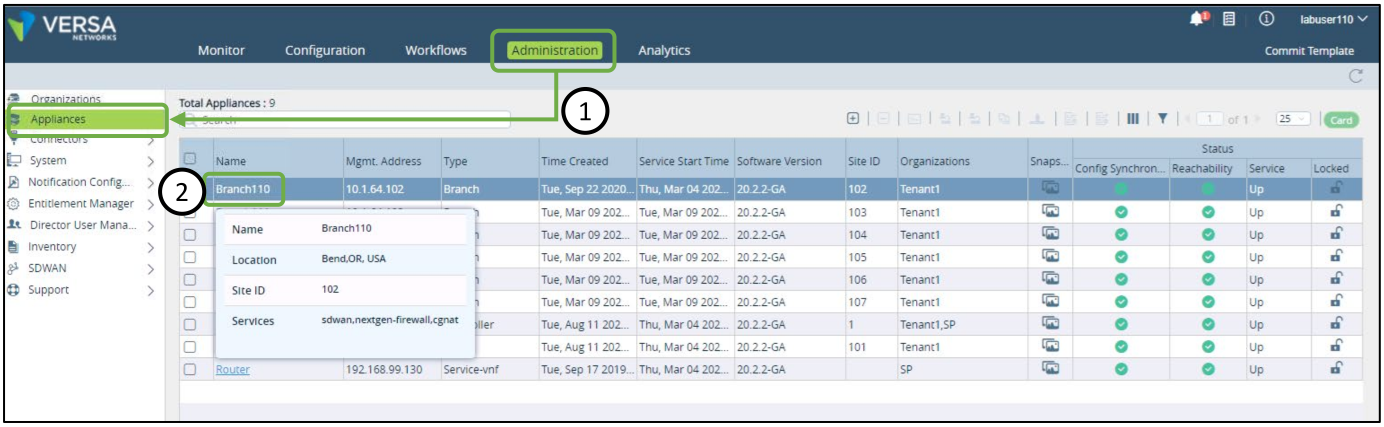
Steps 2 through 5

Verify the Changes to Your Device

The output of the following steps will depend on where the other lab participants are in the process. If you are the first person to reach this point in the lab, it will appear that the changes have not been applied – this is because the hub-and-spoke routes are filtered based on the routing policies configured on other devices.

Node routes will begin with a 10.x prefix (the control plane address space) and end with a value of 101 or higher (IP addresses reserved for CPE devices)

1. Navigate to *Administration > Appliances* and locate your appliance in the table.
2. Click your appliance name to open the Appliance Context mode of your appliance.
3. In Appliance Context mode, navigate to the *Services* tab, then click the *Routes* button.
4. In the Routes table, ensure that the Tenant1-Control-VR route table is selected.
5. Analyze the nodes that are visible to the appliance.

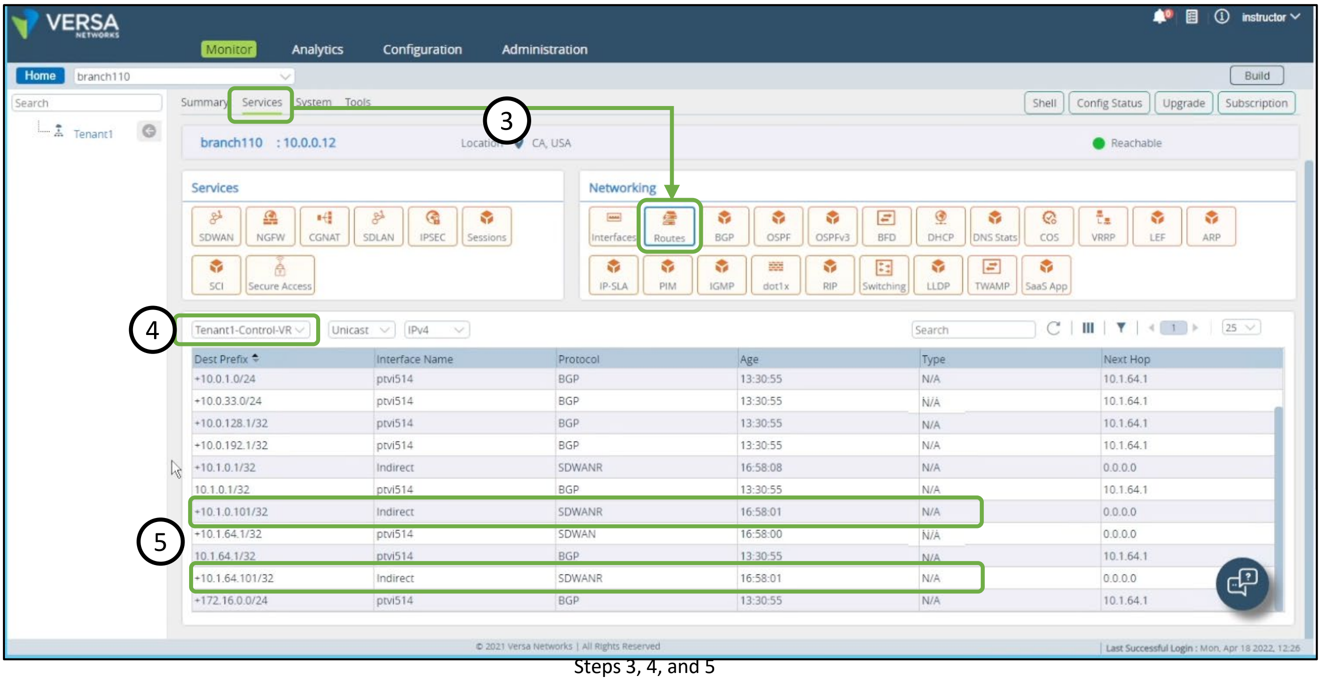


Total Appliances : 9

Name	Mgmt. Address	Type	Time Created	Service Start Time	Software Version	Site ID	Organizations	Snaps...	Status: Config Synchron...	Status: Reachability	Status: Service	Status: Locked
Branch110	10.1.64.102	Branch	Tue, Sep 22 2020...	Thu, Mar 04 202...	20.2.2-GA	102	Tenant1		●	●	Up	
			Tue, Mar 09 202...	Tue, Mar 09 202...	20.2.2-GA	103	Tenant1		✓	✓	Up	
			Tue, Mar 09 202...	Tue, Mar 09 202...	20.2.2-GA	104	Tenant1		✓	✓	Up	
			Tue, Mar 09 202...	Tue, Mar 09 202...	20.2.2-GA	105	Tenant1		✓	✓	Up	
			Tue, Mar 09 202...	Tue, Mar 09 202...	20.2.2-GA	106	Tenant1		✓	✓	Up	
			Tue, Mar 09 202...	Tue, Mar 09 202...	20.2.2-GA	107	Tenant1		✓	✓	Up	
			Tue, Aug 11 202...	Thu, Mar 04 202...	20.2.2-GA	1	Tenant1,SP		✓	✓	Up	
			Tue, Aug 11 202...	Thu, Mar 04 202...	20.2.2-GA	101	Tenant1		✓	✓	Up	
Router	192.168.99.130	Service-vnf	Tue, Sep 17 2019...	Thu, Mar 04 202...	20.2.2-GA		SP		✓	✓	Up	

Name	Branch110
Location	Bend,OR, USA
Site ID	102
Services	sdwan,nextgen-firewall,cgnat

Steps 1 and 2



branch110 : 10.0.0.12 Location CA, USA

Tenant1-Control-VR | Unicast | IPv4

Dest Prefix	Interface Name	Protocol	Age	Type	Next Hop
+10.0.1.0/24	ptvi514	BGP	13:30:55	N/A	10.1.64.1
+10.0.33.0/24	ptvi514	BGP	13:30:55	N/A	10.1.64.1
+10.0.128.1/32	ptvi514	BGP	13:30:55	N/A	10.1.64.1
+10.0.192.1/32	ptvi514	BGP	13:30:55	N/A	10.1.64.1
+10.1.0.1/32	Indirect	SDWANR	16:58:08	N/A	0.0.0.0
10.1.0.1/32	ptvi514	BGP	13:30:55	N/A	10.1.64.1
+10.1.0.101/32	Indirect	SDWANR	16:58:01	N/A	0.0.0.0
+10.1.64.1/32	ptvi514	SDWAN	16:58:00	N/A	0.0.0.0
10.1.64.1/32	ptvi514	BGP	13:30:55	N/A	10.1.64.1
+10.1.64.101/32	Indirect	SDWANR	16:58:01	N/A	0.0.0.0
+172.16.0.0/24	ptvi514	BGP	13:30:55	N/A	10.1.64.1

© 2021 Versa Networks | All Rights Reserved

Last Successful Login : Mon, Apr 18 2022, 12:26

Steps 3, 4, and 5

Control-VR Route Table Analysis

The nodes visible to your appliance in the Control-VR routing table will depend on the progress other lab users have made in their configuration. As other lab members reconfigure their devices to the hub-and-spoke topology, the node advertisements they send to the controller will be marked with BGP communities that identify the routes as spoke-sourced routes, and your appliance will begin to filter them out and remove them from the known-nodes list in the routing table.

WAIT

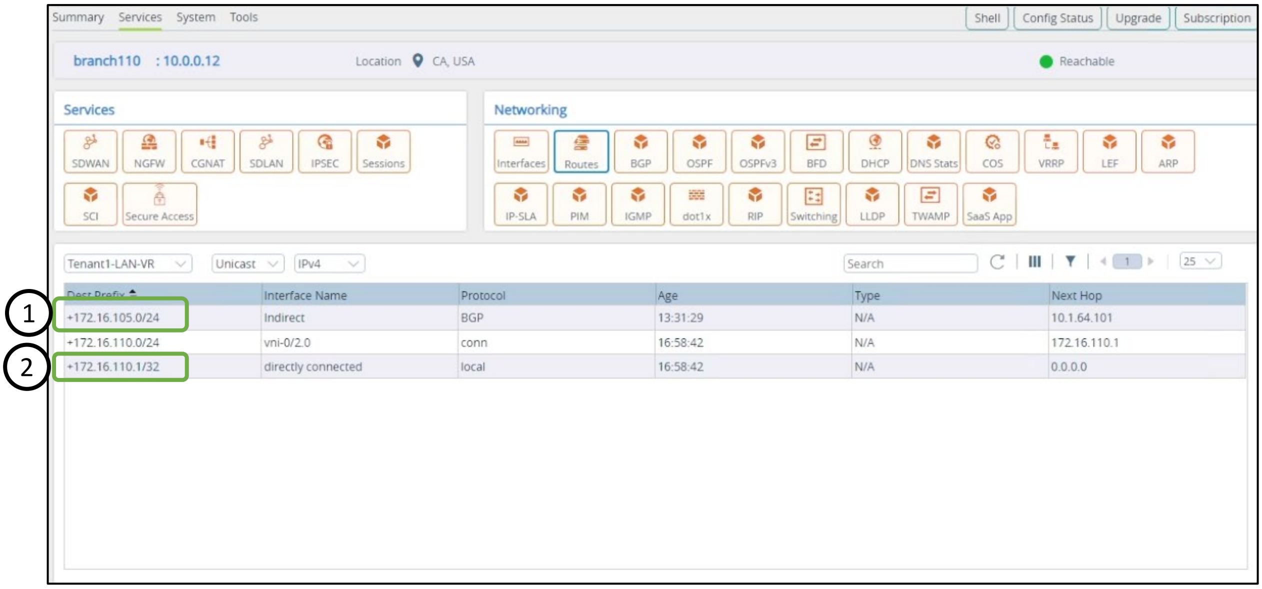
It may take some time for other nodes to be re-configured. You can refresh the route table by selecting a different route table in the route table dropdown menu, or by clicking the browser Refresh button. Wait until remote nodes begin to disappear from the Control-VR routing table before proceeding, or ask your instructor for instructions on how to continue.

Tenant1-LAN-VR Route Table Analysis

The Tenant LAN VR is where remote routes are stored. Each remote route is associated with a remote site that is found in the Control-VR routing table. You will see the following relationships between the routes in the Tenant1-LAN-VR route table and the Control-VR route table:

- Each remote LAN in the tenant LAN VR will have a BGP next-hop (gateway address) of a remote site that is located in the Control VR (SDWAN route).

1. Select the *Tenant1-LAN-VR* route table from the routing table dropdown menu.
2. Locate the Hub LAN in the routing table (172.16.105.0/24)
3. As other lab members finish completing their configurations, note that the remote LANs associated with their devices are no longer listed in the routing table (you will have to refresh the browser window, or you can change the routing table in the dropdown, then change it back to re-query the device routing table). Once all other nodes have been converted to Hub-and-Spoke, the Tenant1-LAN-VR routing table should be similar to the example below.



Tenant1-LAN-VR Unicast IPv4

Dest Prefix	Interface Name	Protocol	Age	Type	Next Hop
+172.16.105.0/24	Indirect	BGP	13:31:29	N/A	10.1.64.101
+172.16.110.0/24	vni-0/2.0	conn	16:58:42	N/A	172.16.110.1
+172.16.110.1/32	directly connected	local	16:58:42	N/A	0.0.0.0

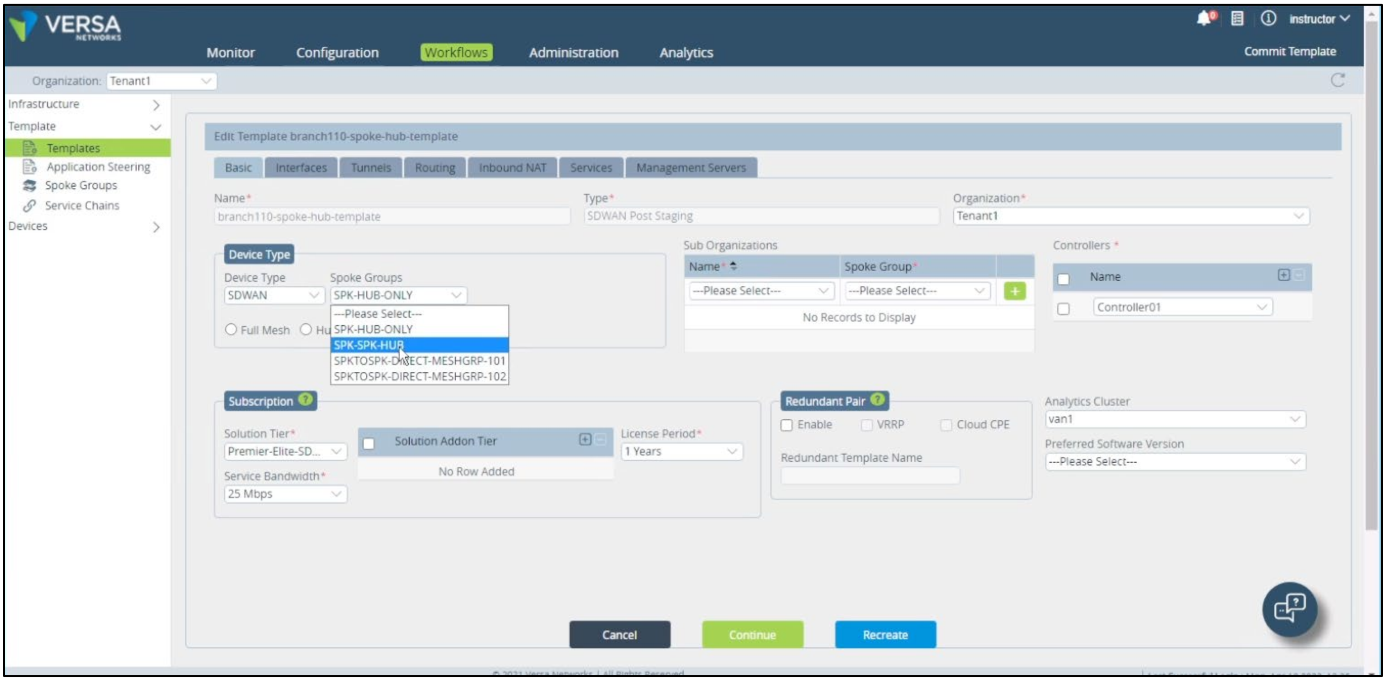
WAIT

Before proceeding with the lab, verify with your instructor that other students have progressed to a point where your upcoming changes will be effective. If you proceed prior to the following steps before other students have completed their lab steps to this point, your output may not match the following examples.

Change the Hub-and-Spoke Topology Type in the Device Template

In the next steps you will change the spoke group configured in your device template workflow. This will reconfigure the corresponding template with different BGP policies which will change how routes are advertised and accepted in the SD-WAN.

1. Navigate to the *Workflows > Template > Templates* in Versa Director.
2. Locate your Template workflow in the workflow table.
3. Click your Template workflow to open the workflow.
4. Change the Spoke Group in the workflow to the **SPK-SPK-HUB** spoke group.
5. Click *Recreate* to update the workflow and recreate the device template.
6. When prompted with the Diff and Merge page, examine the changes that will be applied to the configuration by modifying the workflow (and the template).
7. Click *Deploy* to apply the changes to the template in Versa Director.



Organization: Tenant1

Edit Template branch110-spoke-hub-template

Name*: branch110-spoke-hub-template

Type*: SDWAN Post Staging

Organization*: Tenant1

Device Type

Device Type: SDWAN

Spoke Groups: SPK-HUB-ONLY

○ Full Mesh ○ Hu

---Please Select---
SPK-HUB-ONLY
SPK-SPK-HUB
SPKTOSPK-DIRECT-MESHGRP-101
SPKTOSPK-DIRECT-MESHGRP-102

Sub Organizations

Name*	Spoke Group*
---Please Select---	---Please Select---

No Records to Display

Controllers *

□	Name
□	Controller01

Subscription

Solution Tier*: Premier-Elite-SD...

Service Bandwidth*: 25 Mbps

□ Solution Addon Tier

No Row Added

License Period*: 1 Years

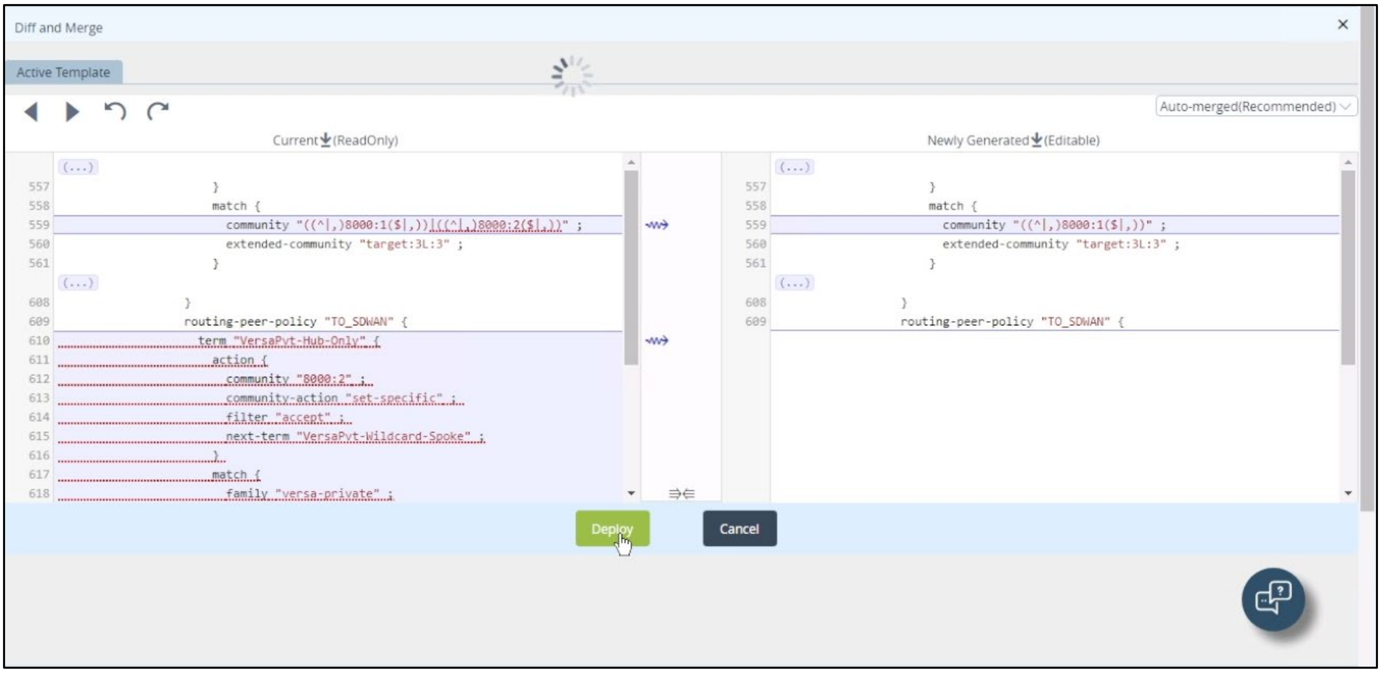
Redundant Pair

□ Enable □ VRRP □ Cloud CPE

Redundant Template Name

Analytics Cluster: van1

Preferred Software Version: ---Please Select---



Current (ReadOnly)

```
(...)
                    }
                    match {
                      community "((^|,)8000:1($|,))|((^|,)8000:2($|,))" ;
                      extended-community "target:3L:3" ;
                    }
(...)
                }
                routing-peer-policy "TO_SDWAN" {
                  term "VersaPvt-Hub-Only" {
                    action {
                      community "8000:2" ;
                      community-action "set-specific" ;
                      filter "accept" ;
                      next-term "VersaPvt-Wildcard-Spoke" ;
                    }
                    match {
                      family "versa-private" ;
```

Newly Generated (Editable)

```
(...)
                    }
                    match {
                      community "((^|,)8000:1($|,))" ;
                      extended-community "target:3L:3" ;
                    }
(...)
                }
                routing-peer-policy "TO_SDWAN" {
```

Question: What configuration parameters change when you set the device to Spoke-to-Spoke-via-Hub?

____

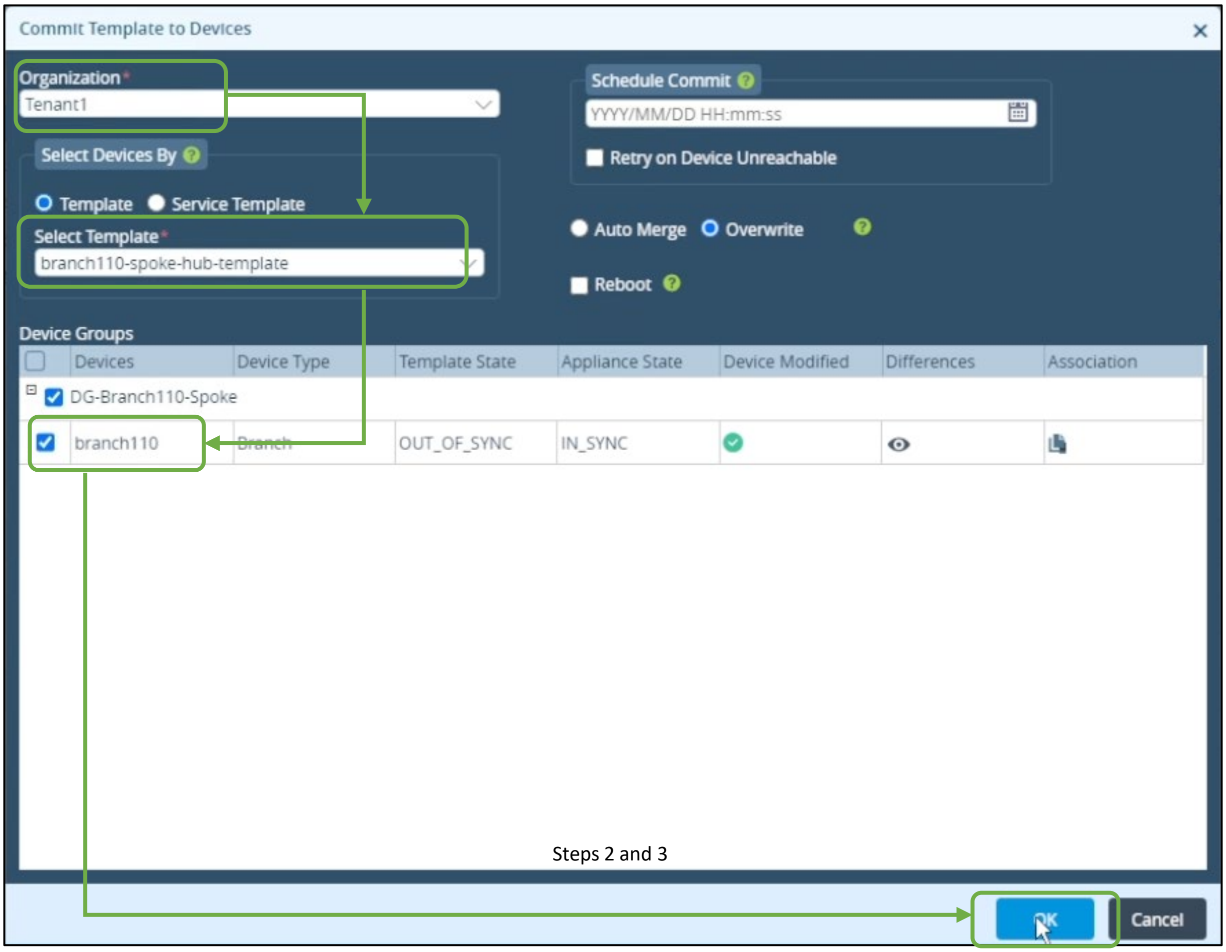
____

Answer: Redistribution and routing policy is changed to add different community values to routes that are sent, and a different set of routes are allowed into the device based on community values attached to received routes. The community values attached to advertised routes also allows the hub to process the routes differently in order to re-advertise the routes back to sites.

Apply the Device Template Configuration Changes to Your Device

Now that you have modified the configuration template associated with your device in Versa Director, you need to apply the changes to the appliance.

1. Click Commit Template in the top-right corner of Versa Director
2. In the Commit dialog, select the following:
    - Organization: Tenant1
    - Template: Your device template
    - Device Group: locate your device in the list and select it
3. Click OK to apply the configuration to your appliance.



Commit Template to Devices

Organization* Tenant1

Select Devices By

◉ Template ○ Service Template

Select Template* branch110-spoke-hub-template

Schedule Commit YYYY/MM/DD HH:mm:ss

□ Retry on Device Unreachable

○ Auto Merge ◉ Overwrite

□ Reboot

Device Groups

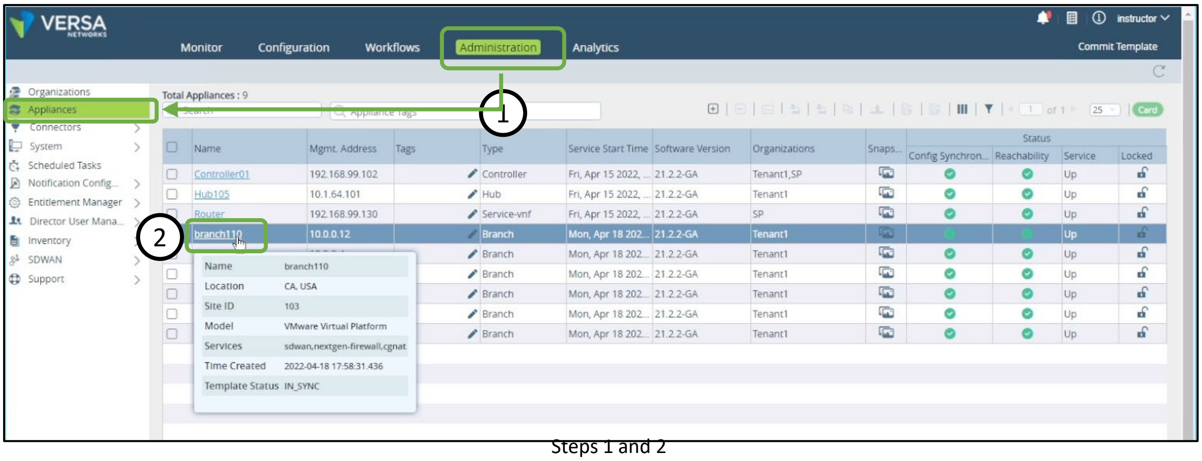
□	Devices	Device Type	Template State	Appliance State	Device Modified	Differences	Association
☑	DG-Branch110-Spoke						
☑	branch110	Branch	OUT_OF_SYNC	IN_SYNC	✓	👁	

Steps 2 and 3

Analyze the Routes in Your Appliance Control-VR

Now that you have applied the changes to your device, you will analyze how the topology change (spoke group type) affects the reachability information for your device.

1. Navigate to the *Administration > Appliances* dashboard and locate your appliance in the appliance table.
2. Click your appliance name to open the Appliance Context mode of your appliance.
3. In the Appliance Context mode of your appliance, navigate to the *Services > Routes* dashboard (ensure that the Tenant1 organization is selected on the left-side menu).
4. Ensure that the Tenant1-Control-VR routing table is selected in the routing table dropdown menu.

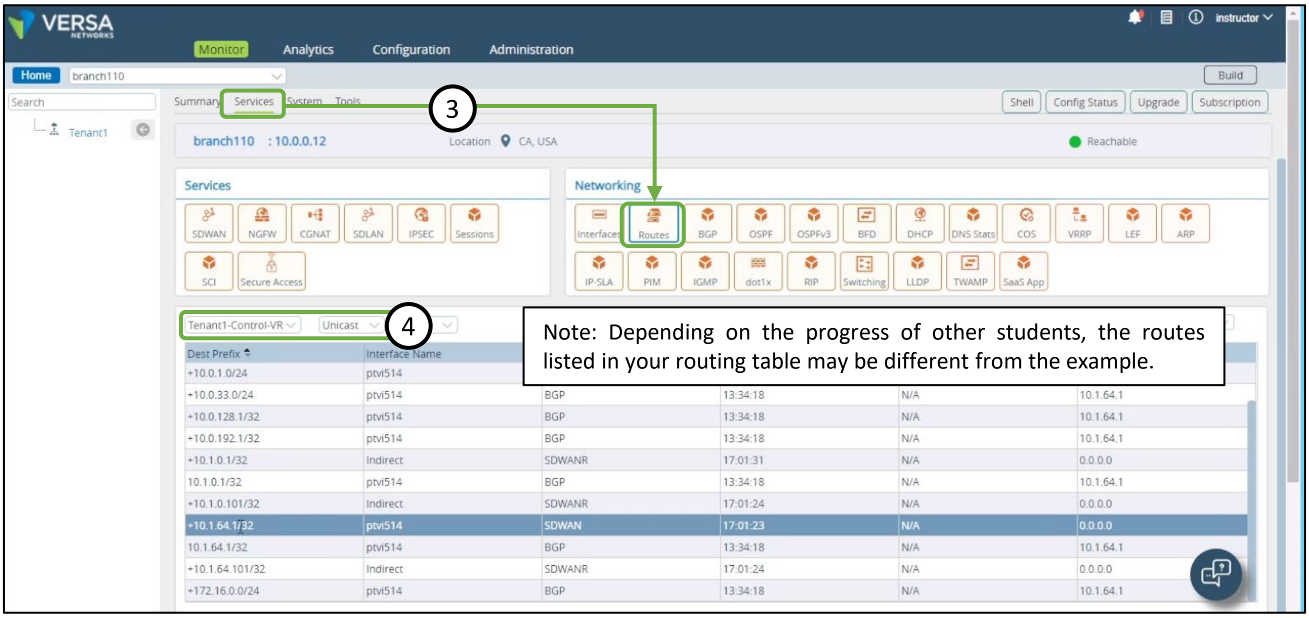


Total Appliances : 9

☐	Name	Mgmt. Address	Tags	Type	Service Start Time	Software Version	Organizations	Snaps...	Status Config Synchron...	Reachability	Service	Locked
☐	Controller01	192.168.99.102		Controller	Fri, Apr 15 2022, ...	21.2.2-GA	Tenant1,SP		✓	✓	Up	
☐	Hub105	10.1.64.101		Hub	Fri, Apr 15 2022, ...	21.2.2-GA	Tenant1		✓	✓	Up	
☐	Router	192.168.99.130		Service-vnf	Fri, Apr 15 2022, ...	21.2.2-GA	SP		✓	✓	Up	
☐	branch110	10.0.0.12		Branch	Mon, Apr 18 202...	21.2.2-GA	Tenant1		●	●	Up	
				Branch	Mon, Apr 18 202...	21.2.2-GA	Tenant1		✓	✓	Up	
☐				Branch	Mon, Apr 18 202...	21.2.2-GA	Tenant1		✓	✓	Up	
☐				Branch	Mon, Apr 18 202...	21.2.2-GA	Tenant1		✓	✓	Up	
☐				Branch	Mon, Apr 18 202...	21.2.2-GA	Tenant1		✓	✓	Up	
☐				Branch	Mon, Apr 18 202...	21.2.2-GA	Tenant1		✓	✓	Up	

Name	branch110
Location	CA, USA
Site ID	103
Model	VMware Virtual Platform
Services	sdwan,nextgen-firewall,cgnat
Time Created	2022-04-18 17:58:31.436
Template Status	IN_SYNC

Steps 1 and 2



branch110 : 10.0.0.12 Location CA, USA ● Reachable

Note: Depending on the progress of other students, the routes listed in your routing table may be different from the example.

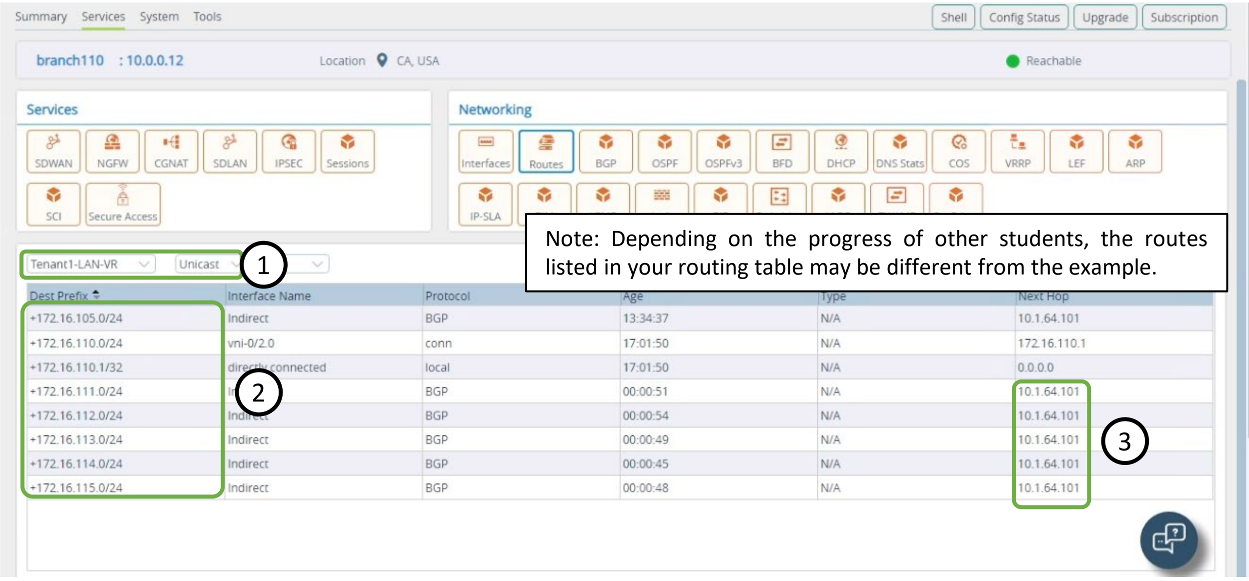
Dest Prefix	Interface Name				
+10.0.1.0/24	ptvi514				
+10.0.33.0/24	ptvi514	BGP	13:34:18	N/A	10.1.64.1
+10.0.128.1/32	ptvi514	BGP	13:34:18	N/A	10.1.64.1
+10.0.192.1/32	ptvi514	BGP	13:34:18	N/A	10.1.64.1
+10.1.0.1/32	Indirect	SDWANR	17:01:31	N/A	0.0.0.0
10.1.0.1/32	ptvi514	BGP	13:34:18	N/A	10.1.64.1
+10.1.0.101/32	Indirect	SDWANR	17:01:24	N/A	0.0.0.0
+10.1.64.1/32	ptvi514	SDWAN	17:01:23	N/A	0.0.0.0
10.1.64.1/32	ptvi514	BGP	13:34:18	N/A	10.1.64.1
+10.1.64.101/32	Indirect	SDWANR	17:01:24	N/A	0.0.0.0
+172.16.0.0/24	ptvi514	BGP	13:34:18	N/A	10.1.64.1

Steps 3 and 4

Analyze the Routes in Your Appliance Tenant1-LAN-VR Routing Table

Next you will analyze the remote LAN routes in your Tenant1-LAN-VR routing table. Pay special attention to the Next-Hop (remote gateway) associated with each remote LAN prefix.

1. Select the Tenant1-LAN-VR routing table from the routing table dropdown list.
2. In the Tenant1-LAN-VR routing table, identify the remote LANs that are visible to your appliance.
3. Note the Next Hop associated with each remote LAN.



Note: Depending on the progress of other students, the routes listed in your routing table may be different from the example.

Dest Prefix	Interface Name	Protocol	Age	Type	Next Hop
+172.16.105.0/24	Indirect	BGP	13:34:37	N/A	10.1.64.101
+172.16.110.0/24	vni-0/2.0	conn	17:01:50	N/A	172.16.110.1
+172.16.110.1/32	directly connected	local	17:01:50	N/A	0.0.0.0
+172.16.111.0/24	Indirect	BGP	00:00:51	N/A	10.1.64.101
+172.16.112.0/24	Indirect	BGP	00:00:54	N/A	10.1.64.101
+172.16.113.0/24	Indirect	BGP	00:00:49	N/A	10.1.64.101
+172.16.114.0/24	Indirect	BGP	00:00:45	N/A	10.1.64.101
+172.16.115.0/24	Indirect	BGP	00:00:48	N/A	10.1.64.101

Question: Why is the next-hop for all of the remote LANs the same?

____

____

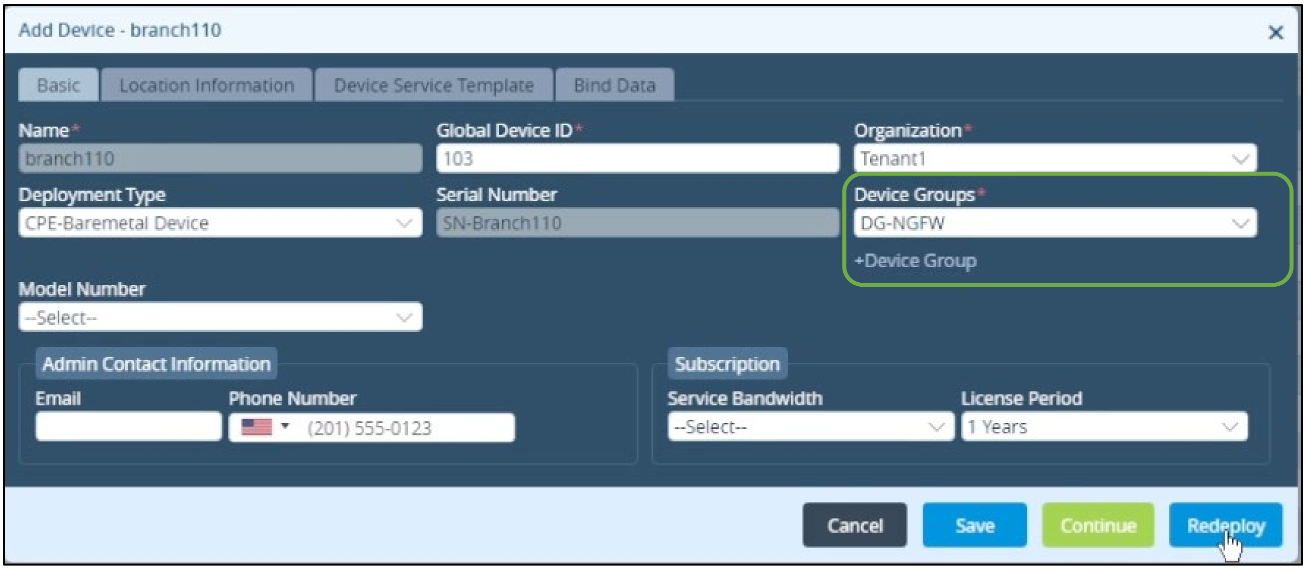
Answer: The hub site accepted all of the routes it received in the BGP advertisements sent by the spokes (sites). It then reprocessed the routes based on the new community values associated with the routes and re-advertised the LAN prefixes. This process of "recycling" the routes causes the hub device to be the originator of the LAN subnets, and it is therefore the gateway to reach the LAN destinations.

Exercise 5: Reset the Lab Environment

In this lab part you will:

- Re-assign your device to the Base-Template-NGFW template by re-assigning the Device Group in your Device workflow
- Commit the changes to reset your device configuration to the base configuration
- Delete your user-created Device Template Workflow (which will delete the template associated with the workflow)
- Delete the user-created Device Group that you created during this lab.

1. Navigate to the *Workflows* > *Devices* > *Device* hierarchy to display the saved Device workflows.
2. Locate **your device** workflow in the Device Workflow table and click the workflow to open it.
3. In the Device workflow, set the Device Group to DG-NGFW.
4. Click *Redeploy* to update your device workflow and save the changes.



Add Device - branch110 ✕

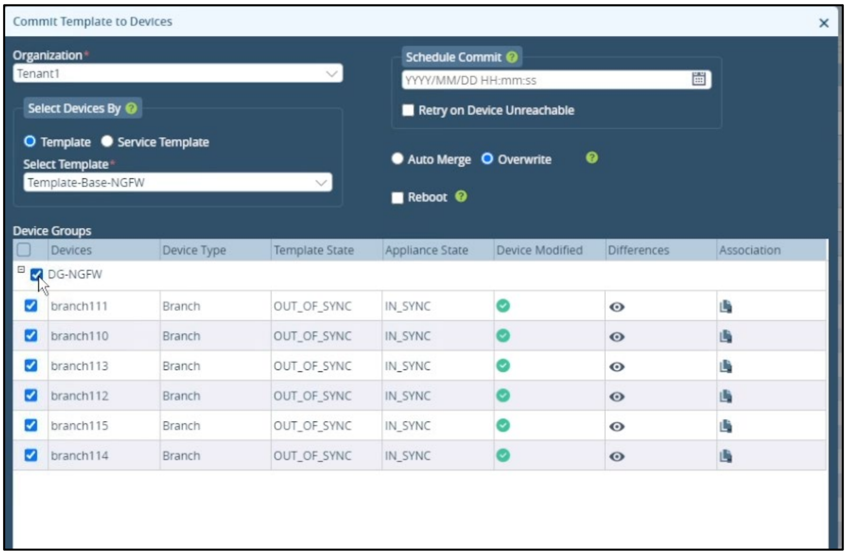
Name*: branch110
Global Device ID*: 103
Organization*: Tenant1
Deployment Type: CPE-Baremetal Device
Serial Number: SN-Branch110
Device Groups*: DG-NGFW
+Device Group
Model Number: --Select--

Admin Contact Information
Email:
Phone Number: (201) 555-0123

Subscription
Service Bandwidth: --Select--
License Period: 1 Years

Commit the template to update your device.

Note: The example shows a commit template on all devices in the base device group. Please only check YOUR device from the list so that other students in the lab can perform the same task with their corresponding device.



Commit Template to Devices ✕

Organization*: Tenant1

Schedule Commit: YYYY/MM/DD HH:mm:ss
□ Retry on Device Unreachable

Select Devices By
● Template ○ Service Template
Select Template*: Template-Base-NGFW

○ Auto Merge ● Overwrite
□ Reboot

Device Groups

□	Devices	Device Type	Template State	Appliance State	Device Modified	Differences	Association
☑	DG-NGFW						
☑	branch111	Branch	OUT_OF_SYNC	IN_SYNC	✓	👁	📄
☑	branch110	Branch	OUT_OF_SYNC	IN_SYNC	✓	👁	📄
☑	branch113	Branch	OUT_OF_SYNC	IN_SYNC	✓	👁	📄
☑	branch112	Branch	OUT_OF_SYNC	IN_SYNC	✓	👁	📄
☑	branch115	Branch	OUT_OF_SYNC	IN_SYNC	✓	👁	📄
☑	branch114	Branch	OUT_OF_SYNC	IN_SYNC	✓	👁	📄

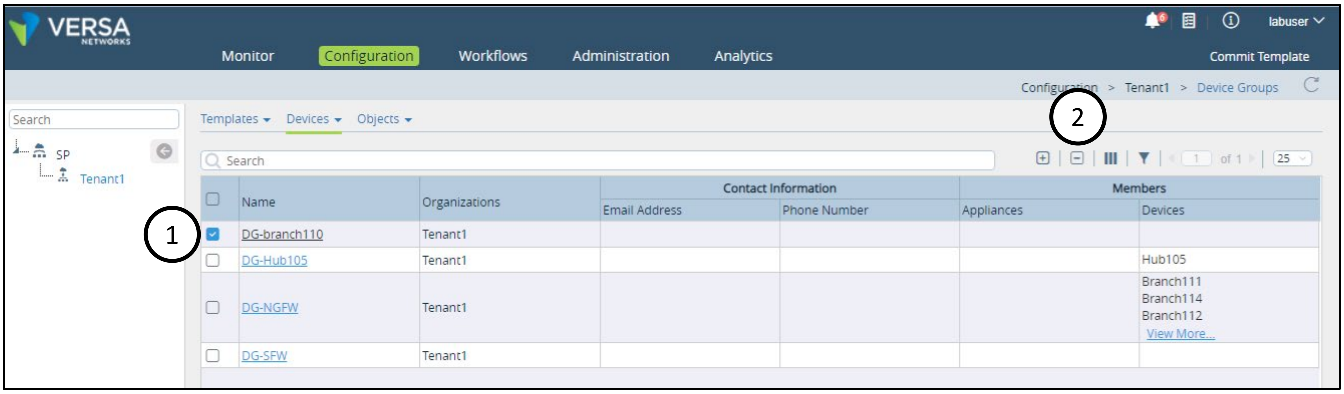
Note: Ask your instructor if you should delete the device group and template workflows, as you may be able to use the same device group and template for future lab exercises.

Navigate to the *Configuration* > *Devices* > *Device Groups* dashboard.

In the *Device Groups* table:

1. Check the box next to your user-defined device group.
2. Click the button to remove your user-defined device group.
3. Confirm the device group deletion.

⊟

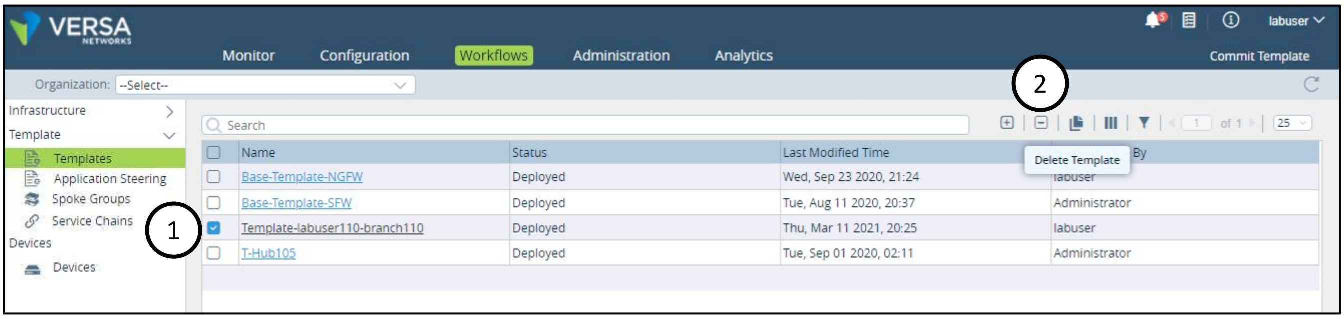


☐	Name	Organizations	Contact Information		Members	
			Email Address	Phone Number	Appliances	Devices
☑	DG-branch110	Tenant1				
☐	DG-Hub105	Tenant1				Hub105
☐	DG-NGFW	Tenant1				Branch111 Branch114 Branch112 View More...
☐	DG-SFW	Tenant1				

Navigate to the *Workflows* > *Template* > *Templates* dashboard.

In the *Templates* workflow table:

1. Check the box next to your user-defined template.
2. Click the ⊟ button to remove your user-defined template.
3. Confirm the wokflow deletion.



☐	Name	Status	Last Modified Time	By
☐	Base-Template-NGFW	Deployed	Wed, Sep 23 2020, 21:24	labuser
☐	Base-Template-SFW	Deployed	Tue, Aug 11 2020, 20:37	Administrator
☑	Template-labuser110-branch110	Deployed	Thu, Mar 11 2021, 20:25	labuser
☐	T-Hub105	Deployed	Tue, Sep 01 2020, 02:11	Administrator

STOP

STOP! Notify your instructor that you have completed this lab.

Versa Configuration Management

The Versa Networks lab environment consists of a fixed, pre-configured topology that will allow you to explore, configure, and manage Versa Networks CPEs by using Versa Director, the central management and orchestration platform for a Versa Secure SD-WAN solution. After completing this lab, you will be able to:

- Identify when a device configuration is in sync or out of sync with Versa Director
- Import and Export device configurations

In this lab, you will be assigned a single CPE device (Branch device) for configuration and monitoring.

The lab environment is accessed through Amazon Workspaces. You should have received an email to allow you to register your Amazon Workspaces account and set your password.

NOTE: It is common for the Amazon Workspaces email to be sent to the spam/junk folder. If you have not received the registration email, check those folders.

The remote desktop connection opens a remote workstation, where you will use various tools to navigate and configure the lab environment. The main tool you will use in this lab is Versa Director. Versa Director can be accessed by opening the Google Chrome browser on the Remote Desktop. There is a bookmark to the Versa Director device in the Google Chrome bookmark bar.

This lab environment is a shared environment. There may be up to 24 students in the environment. Each student has their own remote desktop, but the Versa Director is shared. Because of the shared environment, you may see configuration templates, device groups, workflows, and devices that other students have created, or that have been pre-provisioned within Versa Director. It is important that you only modify the configuration components that are assigned to you by your instructor.

During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not be the same, etc.) Do not be alarmed if your results vary slightly from the results shown in the lab guide. The important thing is that the lab functions in the desired manner.

Look for these hints to help you in the labs

This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

Now that we've discussed what is expected, let's get started!

Lab Exercise Overview

In this lab you will perform various tasks. You will begin by verifying that your device configuration is synchronized with the configuration on Versa Director. A flow of the lab exercises is:

Examine the device Sync State and verify that the configuration is in synch

Create a backup (export) of the device configuration

Modify a parameter in the device configuration using Appliance Context Mode

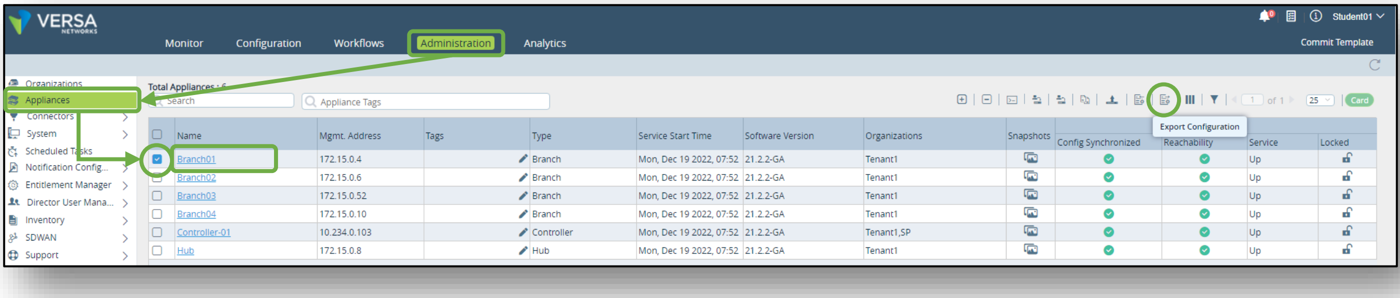
Examine the Sync State and verify that the configuration is out of sync

Import the device configuration to resolve the out-of-sync state

Exercise 1: Create A Backup of the Device Configuration (Export)

Please refer to the Lab Access Guide for instructions on how to connect to the remote lab environment.

In the remote landing station, open the Google Chrome browser and log into Versa Director. In Versa Director, open the *Administration > Appliances* dashboard in Versa Director. Locate your appliance in the Appliances table and check the box next to the appliance, then click the ***Export Configuration*** button to export the configuration to a text file. The file will be saved in the remote desktop Downloads folder.



☐	Name	Mgmt. Address	Tags	Type	Service Start Time	Software Version	Organizations	Snapshots	Config Synchronized	Reachability	Service	Locked
☑	Branch01	172.15.0.4		Branch	Mon, Dec 19 2022, 07:52	21.2.2-GA	Tenant1		✓	✓	Up	🔓
☐	Branch02	172.15.0.6		Branch	Mon, Dec 19 2022, 07:52	21.2.2-GA	Tenant1		✓	✓	Up	🔓
☐	Branch03	172.15.0.52		Branch	Mon, Dec 19 2022, 07:52	21.2.2-GA	Tenant1		✓	✓	Up	🔓
☐	Branch04	172.15.0.10		Branch	Mon, Dec 19 2022, 07:52	21.2.2-GA	Tenant1		✓	✓	Up	🔓
☐	Controller-01	10.234.0.103		Controller	Mon, Dec 19 2022, 07:52	21.2.2-GA	Tenant1,SP		✓	✓	Up	🔓
☐	Hub	172.15.0.8		Hub	Mon, Dec 19 2022, 07:52	21.2.2-GA	Tenant1		✓	✓	Up	🔓

Exercise 2: Manually modify your device configuration (in Appliance Context mode)

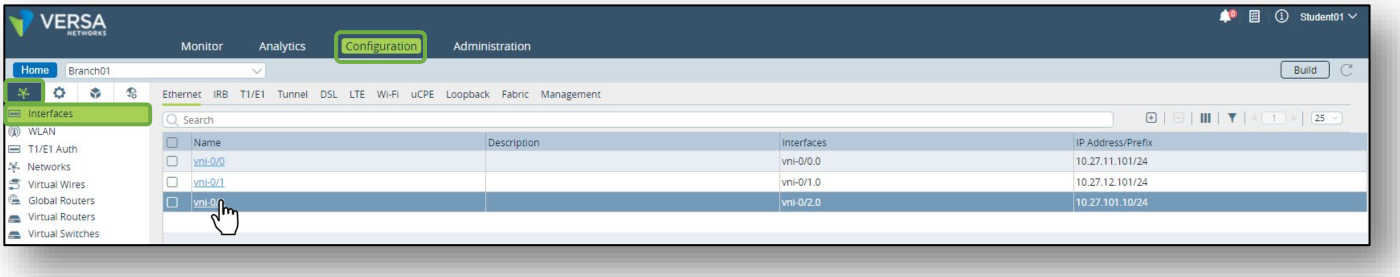
In this part you will change the LAN IP address of your device to a different address. This simulates a wrong or changed configuration on a port that will not impact your CPE to Director connectivity.

IMPORTANT

You are changing the IP address of a port on your device. Be sure you DO NOT CHANGE the WAN port addresses, as this will impact your ability to communicate with Versa Director.

In the *Administration > Appliances* dashboard, click on your device name to open the Appliance Context mode. This will allow you to directly modify the configuration of the device.

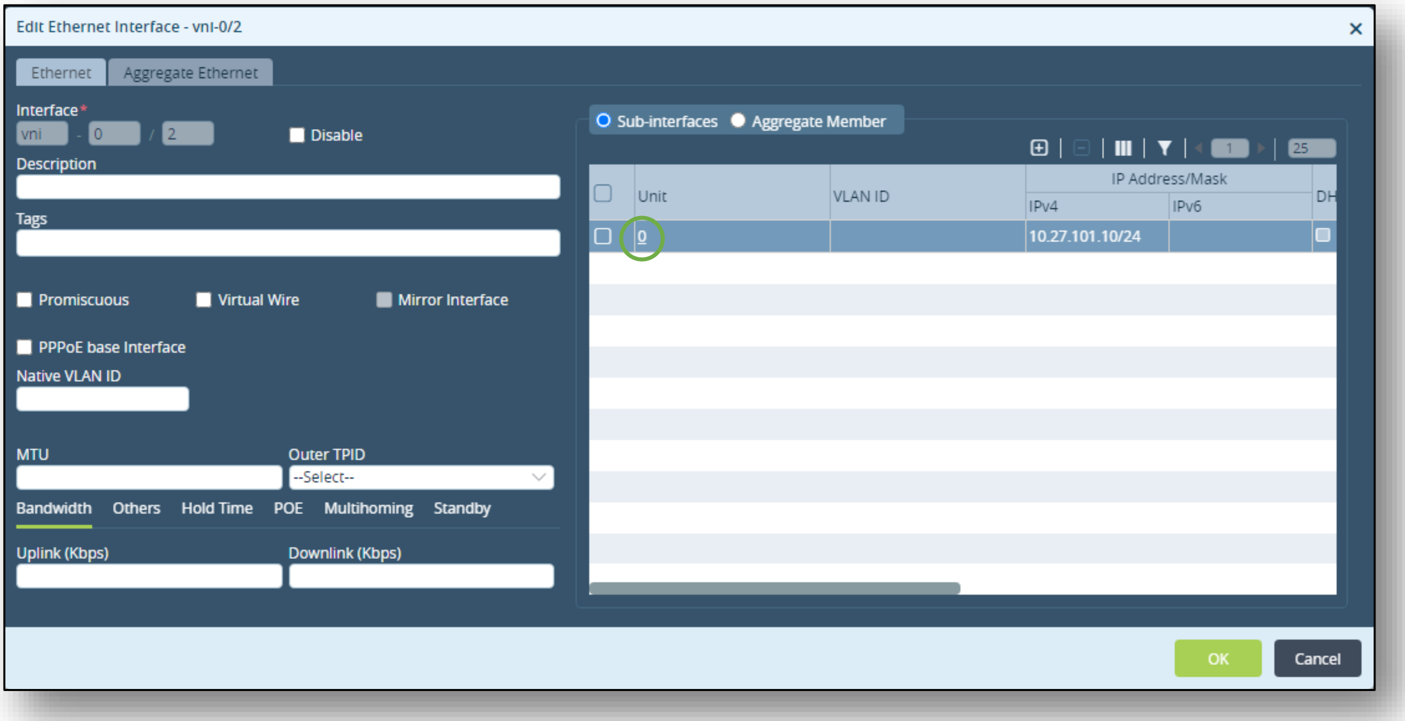
In the Appliance Context mode, click the *Configuration* tab to view the device configuration.



Name	Description	Interfaces	IP Address/Prefix
vni-0/0		vni-0/0.0	10.27.11.101/24
vni-0/1		vni-0/1.0	10.27.12.101/24
vni-0/2		vni-0/2.0	10.27.101.10/24

Select the Interfaces item in the left-side Configuration menu to display the interface configuration.

Locate the vni-0/2 interface. The vni-0/2 interface is the logical port that is mapped to the local LAN. Click the vni-0/2 interface to open the interface configuration.


Edit Ethernet Interface - vni-0/2

Interface* vni - 0 / 2

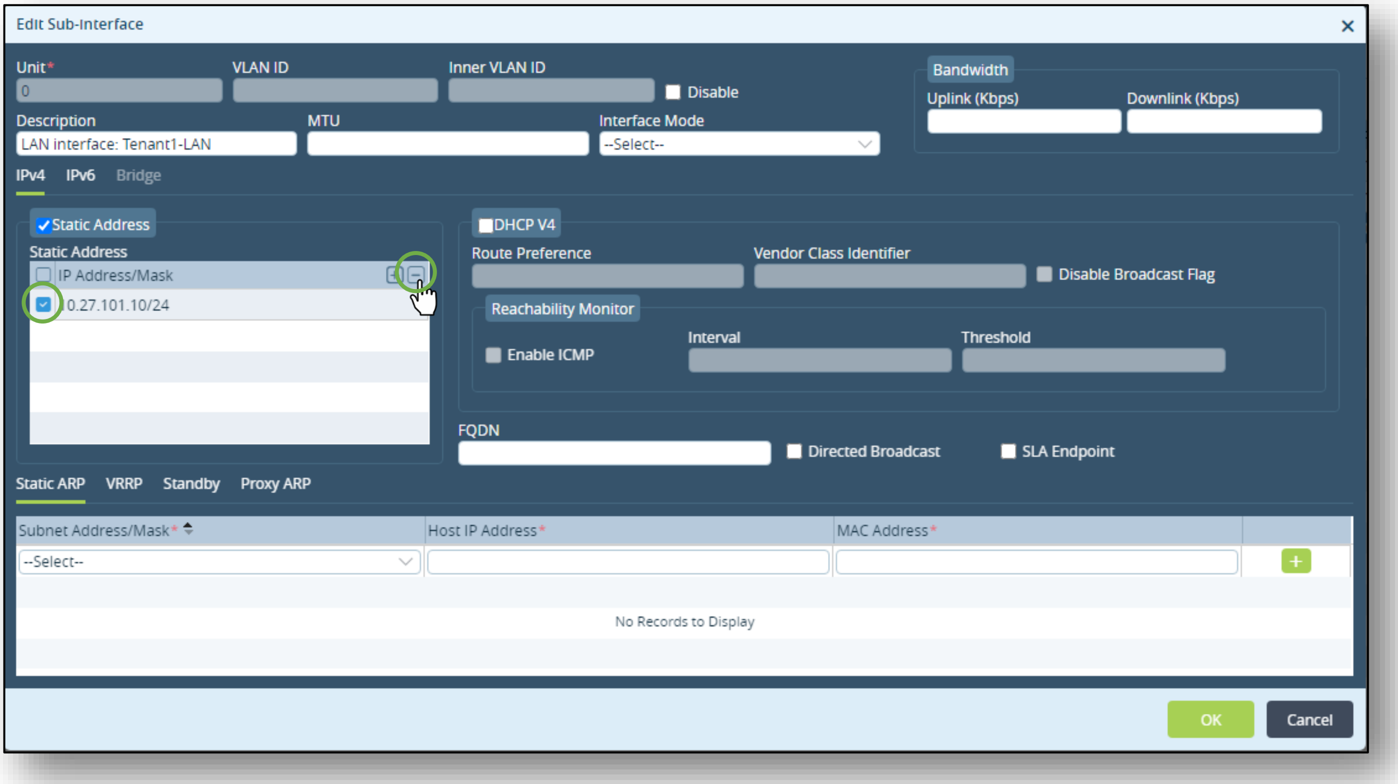
Outer TPID: --Select--

● Sub-interfaces

Unit	VLAN ID	IP Address/Mask		DH
		IPv4	IPv6	
0		10.27.101.10/24		

In the vni-0/2 interface configuration window, locate the Unit 0 (sub-interface 0) in the table. Note the IP address assigned to the interface.

Click the Unit 0 to modify the sub-interface.



Edit Sub-Interface

Unit* 0

Description: LAN interface: Tenant1-LAN

Interface Mode: --Select--

☑ Static Address

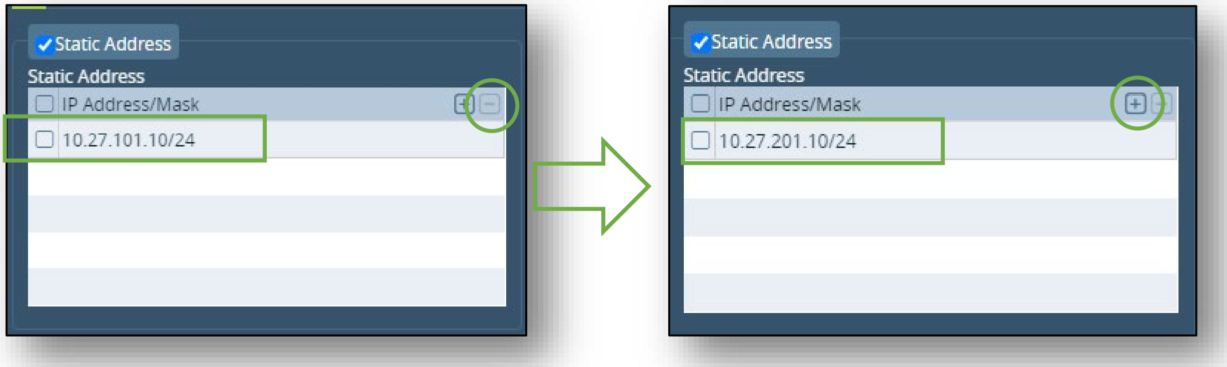
☐ IP Address/Mask
☑ 0.27.101.10/24

☐ DHCP V4

Subnet Address/Mask*	Host IP Address*	MAC Address*
--Select--		

No Records to Display

In the Edit Sub-Interface window, locate the Static IPv4 Address box. The interfaces in VOS can have multiple IP addresses assigned to the same interface. Remove the existing sub-interface IP address and add a new address that is incorrect. You can choose any IPv4 address in the 10.27.xxx.yyy/24 range that is different from the one that is originally configured on your device, then click OK.



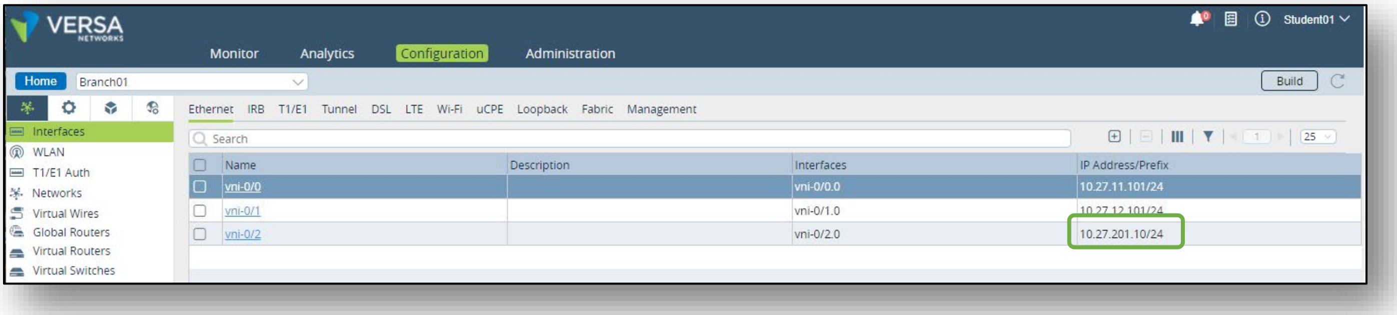
☑ Static Address

☐ IP Address/Mask
☐ 10.27.101.10/24

☑ Static Address

☐ IP Address/Mask
☐ 10.27.201.10/24

Because you are in Appliance Context mode, the changes will take place immediately. Continue to click the OK buttons until you have returned to the main Interfaces dashboard. Verify that your change was applied in the Interfaces table.



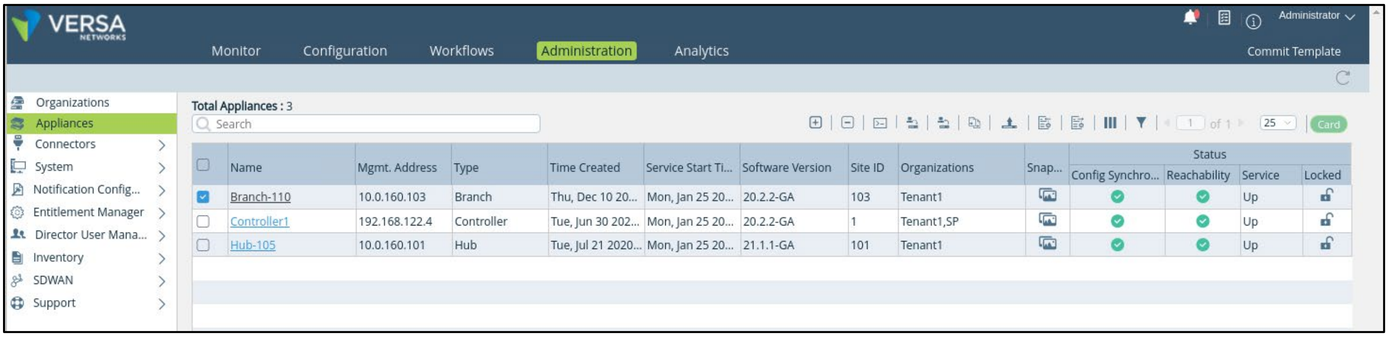
□	Name	Description	Interfaces	IP Address/Prefix
□	vni-0/0		vni-0/0.0	10.27.11.101/24
□	vni-0/1		vni-0/1.0	10.27.12.101/24
□	vni-0/2		vni-0/2.0	10.27.201.10/24

Exercise 3: Reload the saved configuration file to fix the address change

In this part you will reload the saved configuration to your device to reset the change you just made. This is done through the main *Administration > Appliances* dashboard.

Click the *Home* button in the top-left corner to exit Appliance Context mode, then navigate to *Administration > Appliances*.

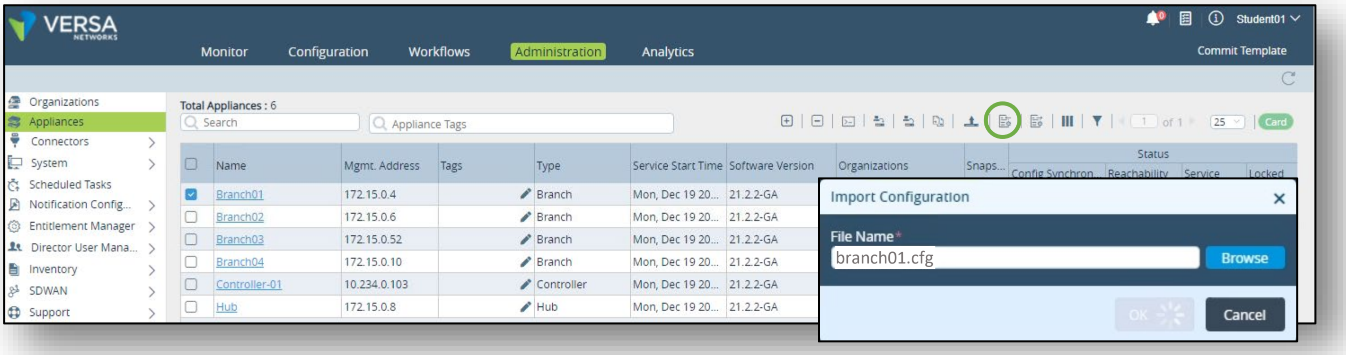
In the *Administration > Appliances* dashboard, locate your device in the table and check the box next to your device.



Total Appliances : 3

□	Name	Mgmt. Address	Type	Time Created	Service Start Ti...	Software Version	Site ID	Organizations	Snap...	Status			
										Config Synchro...	Reachability	Service	Locked
☑	Branch-110	10.0.160.103	Branch	Thu, Dec 10 20...	Mon, Jan 25 20...	20.2.2-GA	103	Tenant1		✓	✓	Up	
□	Controller1	192.168.122.4	Controller	Tue, Jun 30 202...	Mon, Jan 25 20...	20.2.2-GA	1	Tenant1,SP		✓	✓	Up	
□	Hub-105	10.0.160.101	Hub	Tue, Jul 21 2020...	Mon, Jan 25 20...	21.1.1-GA	101	Tenant1		✓	✓	Up	

After you have marked the box next to your device, click on the Import Configuration button and browse to the Downloads folder. Locate the configuration file that was saved by the export process (device-name.cfg file). Click OK and you should see a message that indicates that the configuration file was imported.



Total Appliances : 6

	Name	Mgmt. Address	Tags	Type	Service Start Time	Software Version
☑	Branch01	172.15.0.4		Branch	Mon, Dec 19 20...	21.2.2-GA
□	Branch02	172.15.0.6		Branch	Mon, Dec 19 20...	21.2.2-GA
□	Branch03	172.15.0.52		Branch	Mon, Dec 19 20...	21.2.2-GA
□	Branch04	172.15.0.10		Branch	Mon, Dec 19 20...	21.2.2-GA
□	Controller-01	10.234.0.103		Controller	Mon, Dec 19 20...	21.2.2-GA
□	Hub	172.15.0.8		Hub	Mon, Dec 19 20...	21.2.2-GA

Organizations | Snaps... | Status: Config Synchron... | Reachability | Service | Locked

Import Configuration

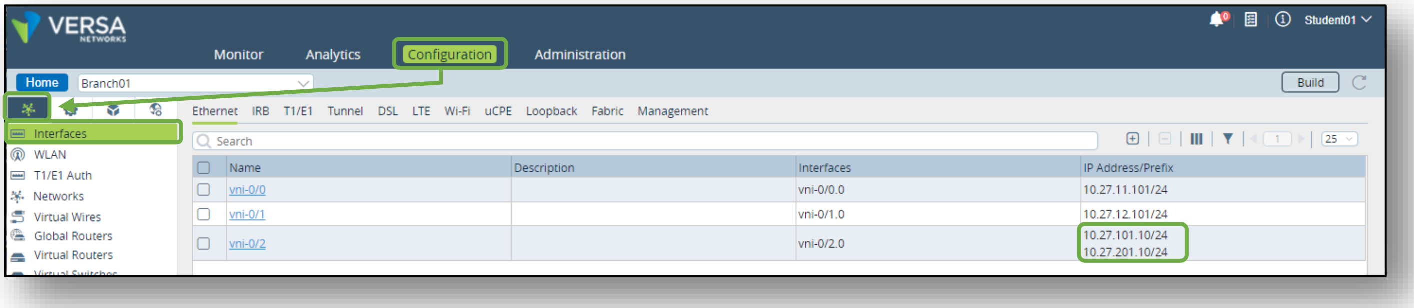
File Name*: branch01.cfg

Browse | OK | Cancel

After you have marked the box next to your device, click on the Import Configuration button and browse to the Downloads folder. Locate the configuration file that was saved by the export process (device-name.cfg file). Click OK and you should see a message that indicates that the configuration file was imported.

Next you will verify that the configuration was imported.

Click your device in the Appliances table to open the Appliance Context mode for your device. In Appliance Context mode, navigate to *Configuration* > *Networking* > *Interfaces*



	Name	Description	Interfaces	IP Address/Prefix
□	vni-0/0		vni-0/0.0	10.27.11.101/24
□	vni-0/1		vni-0/1.0	10.27.12.101/24
□	vni-0/2		vni-0/2.0	10.27.101.10/24 10.27.201.10/24

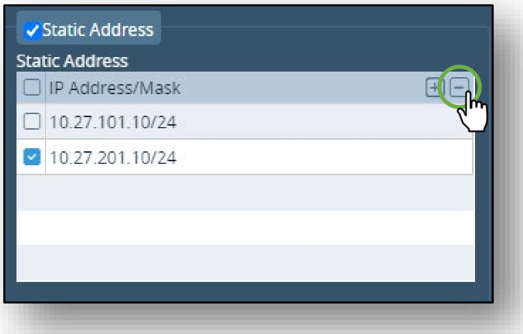
Note that 2 IP addresses are present: the misconfigured interface address and the imported (correct) interface address. This is because the configuration import process acts as a “merge” operation. If conflicting values are present in the configuration, the imported value over-writes the old value. If multiple values are supported in part of a configuration, then imported value is added to the configuration.

Remove the incorrect IP address from the interface.

Open the vni-0/2 interface, then edit the sub-interface that contains the IP addresses.

Select the incorrect address and click the – button to delete the interface.

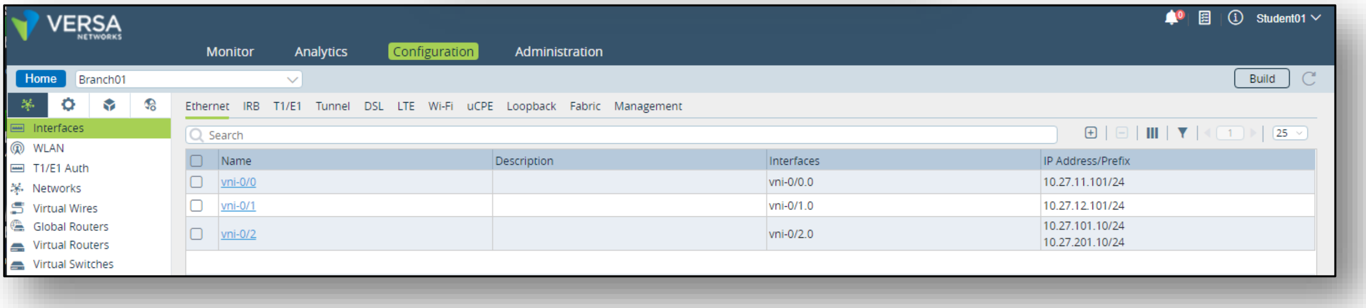
Click OK until you reach the Interfaces configuration dashboard. Verify that the incorrect interface has been removed.



☑ Static Address

Static Address

□	IP Address/Mask
□	10.27.101.10/24
☑	10.27.201.10/24



□	Name	Description	Interfaces	IP Address/Prefix
□	vni-0/0		vni-0/0.0	10.27.11.101/24
□	vni-0/1		vni-0/1.0	10.27.12.101/24
□	vni-0/2		vni-0/2.0	10.27.101.10/24 10.27.201.10/24

STOP **STOP!** Notify your instructor that you have completed this lab.

Statistics and Monitoring

The Versa Networks lab environment consists of a fixed, pre-configured topology that will allow you to explore, configure, and manage Versa Networks CPEs by using Versa Director, the central management and orchestration platform for a Versa Secure SD-WAN solution. After completing this lab, you will be able to:

- Identify how to track and monitor statistics in Versa Director
- Identify how to track and monitor statistics in Versa Analytics

In this lab, you will be assigned a single CPE device (Branch device) for configuration and monitoring.

The lab environment is accessed through Amazon Workspaces. You should have received an email to allow you to register your Amazon Workspaces account and set your password.

NOTE: It is common for the Amazon Workspaces email to be sent to the spam/junk folder. If you have not received the registration email, check those folders.

The remote desktop connection opens a remote workstation, where you will use various tools to navigate and configure the lab environment. The main tool you will use in this lab is Versa Director. Versa Director can be accessed by opening the Google Chrome browser on the Remote Desktop. There is a bookmark to the Versa Director device in the Google Chrome bookmark bar.

This lab environment is a shared environment. There may be up to 24 students in the environment. Each student has their own remote desktop, but the Versa Director is shared. Because of the shared environment, you may see configuration templates, device groups, workflows, and devices that other students have created, or that have been pre-provisioned within Versa Director. It is important that you only modify the configuration components that are assigned to you by your instructor.

During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not be the same, etc.) Do not be alarmed if your results vary slightly from the results shown in the lab guide. The important thing is that the lab functions in the desired manner.

Look for these hints to help you in the labs

This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

Now that we've discussed what is expected, let's get started!

Lab Exercise Overview

In this lab you will perform various tasks and is an open lab environment. You will not be given specific tasks or steps to take to accomplish lab tasks. Instead, you will explore Versa Director monitoring capabilities and Analytics information on your own based on the general guidelines below. You will begin by analyzing real-time statistics for your device through the Versa Director Monitor dashboard. A flow of the lab exercises is:

Open the Versa Director Monitor dashboard

Identify where the interface packet counters are located

Identify where the session flow counters are located

Identify where the security and SD-WAN traffic counters are located

Open the Versa Analytics dashboard

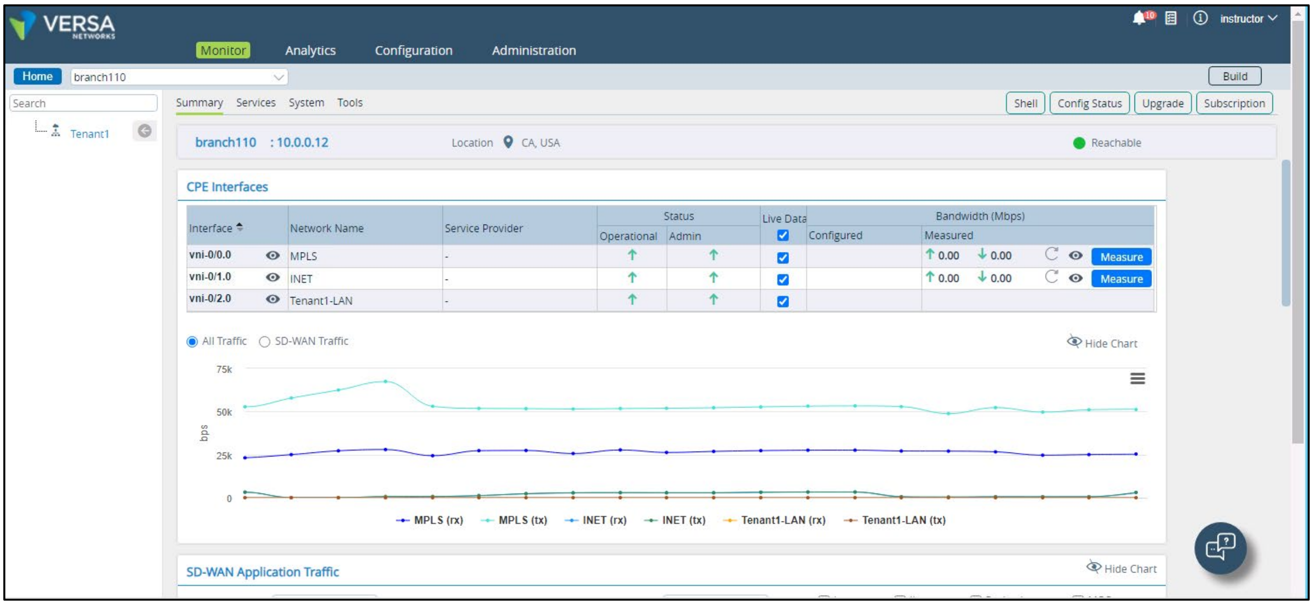
Identify where the SD-WAN statistics and SLA performance statistics are located

Identify where the historical device system information is located

Identify and explore the network logs are stored and the information stored in the log files.

Monitor Dashboard Overview

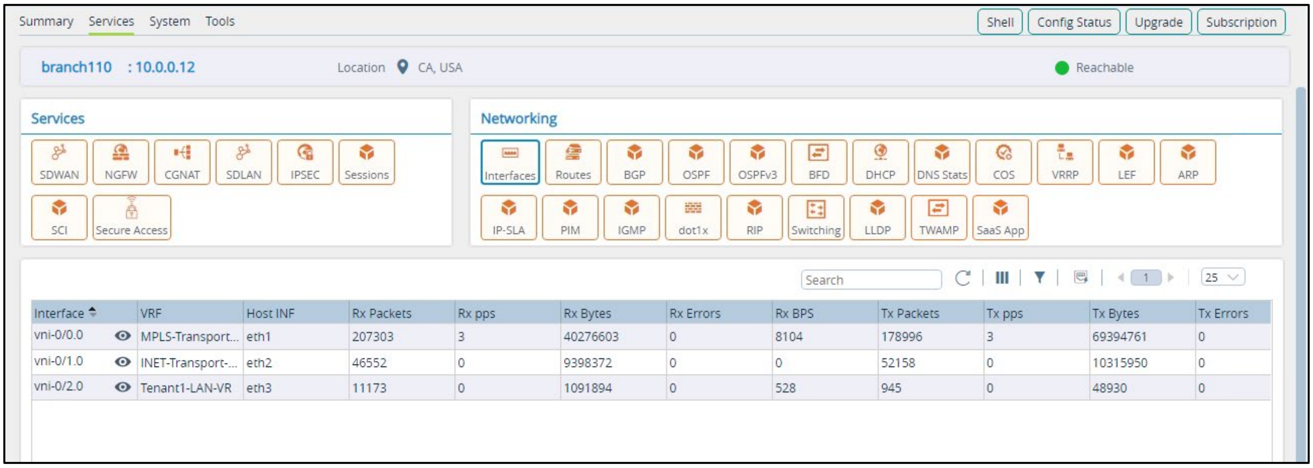
The Monitor dashboard provides real-time statistics and counter information, as well as access to the routing tables, services, and other information about the device.



branch110 : 10.0.0.12 Location CA, USA ● Reachable

CPE Interfaces

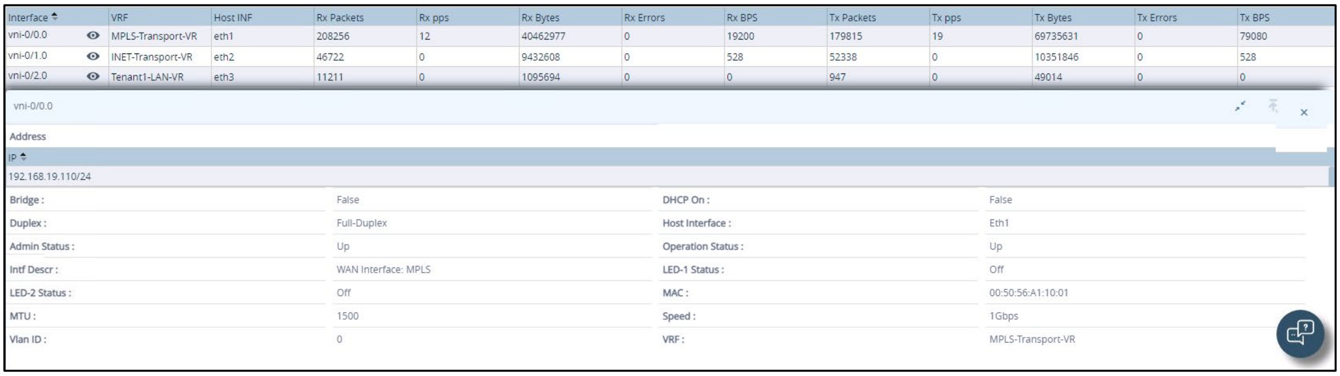
Interface	Network Name	Service Provider	Status		Live Data	Bandwidth (Mbps)		
			Operational	Admin	☑	Configured	Measured	
vni-0/0.0	MPLS	-	↑	↑	☑		↑ 0.00 ↓ 0.00	Measure
vni-0/1.0	INET	-	↑	↑	☑		↑ 0.00 ↓ 0.00	Measure
vni-0/2.0	Tenant1-LAN	-	↑	↑	☑			



branch110 : 10.0.0.12 Location CA, USA ● Reachable

Interface	VRF	Host INF	Rx Packets	Rx pps	Rx Bytes	Rx Errors	Rx BPS	Tx Packets	Tx pps	Tx Bytes	Tx Errors
vni-0/0.0	MPLS-Transport...	eth1	207303	3	40276603	0	8104	178996	3	69394761	0
vni-0/1.0	INET-Transport-...	eth2	46552	0	9398372	0	0	52158	0	10315950	0
vni-0/2.0	Tenant1-LAN-VR	eth3	11173	0	1091894	0	528	945	0	48930	0

Wherever you see an eye icon 👁, this indicates that more details can be viewed by clicking the icon.



Interface		VRF	Host INF	Rx Packets	Rx pps	Rx Bytes	Rx Errors	Rx BPS	Tx Packets	Tx pps	Tx Bytes	Tx Errors	Tx BPS
vni-0/0.0	👁	MPLS-Transport-VR	eth1	208256	12	40462977	0	19200	179815	19	69735631	0	79080
vni-0/1.0	👁	INET-Transport-VR	eth2	46722	0	9432608	0	528	52338	0	10351846	0	528
vni-0/2.0	👁	Tenant1-LAN-VR	eth3	11211	0	1095694	0	0	947	0	49014	0	0

vni-0/0.0

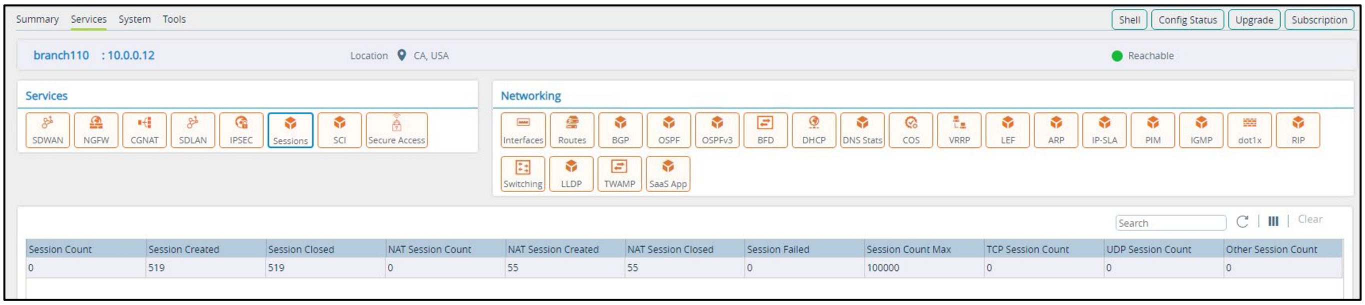
Address

IP
192.168.19.110/24

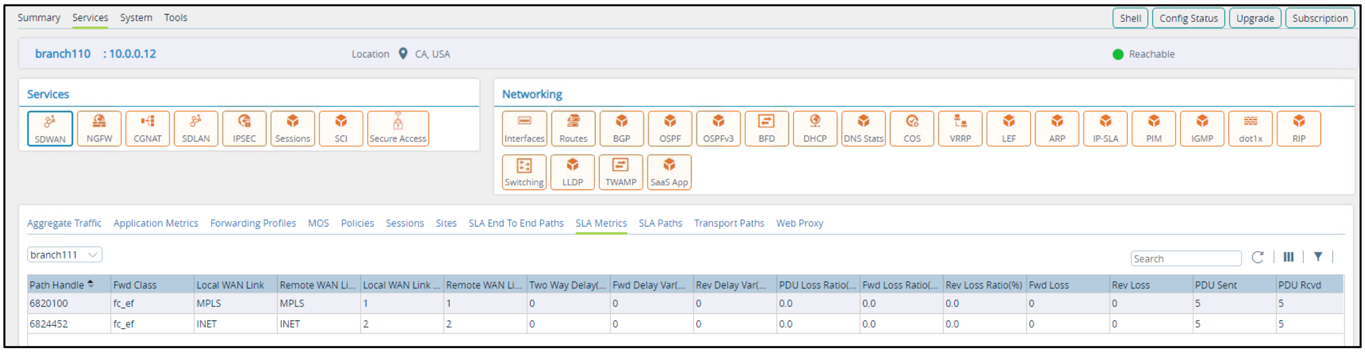
Bridge :	False	DHCP On :	False
Duplex :	Full-Duplex	Host Interface :	Eth1
Admin Status :	Up	Operation Status :	Up
Intf Descr :	WAN Interface: MPLS	LED-1 Status :	Off
LED-2 Status :	Off	MAC :	00:50:56:A1:10:01
MTU :	1500	Speed :	1Gbps
Vlan ID :	0	VRF :	MPLS-Transport-VR

Services Menu

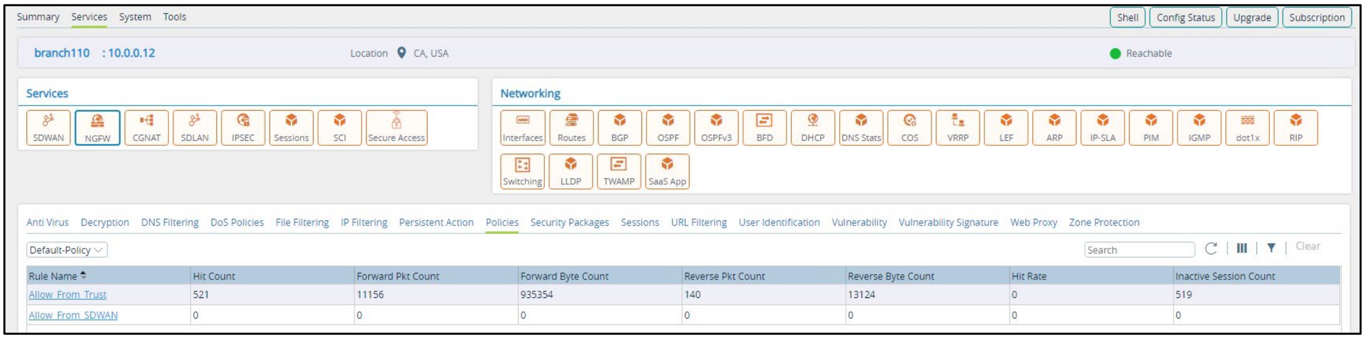
The Services tab provides access to real-time counters and status for many things such as SD-WAN statistics, session information, security counters and policy hits, interface status and parameters, routing tables, and routing protocols.



Session Count	Session Created	Session Closed	NAT Session Count	NAT Session Created	NAT Session Closed	Session Failed	Session Count Max	TCP Session Count	UDP Session Count	Other Session Count
0	519	519	0	55	55	0	100000	0	0	0



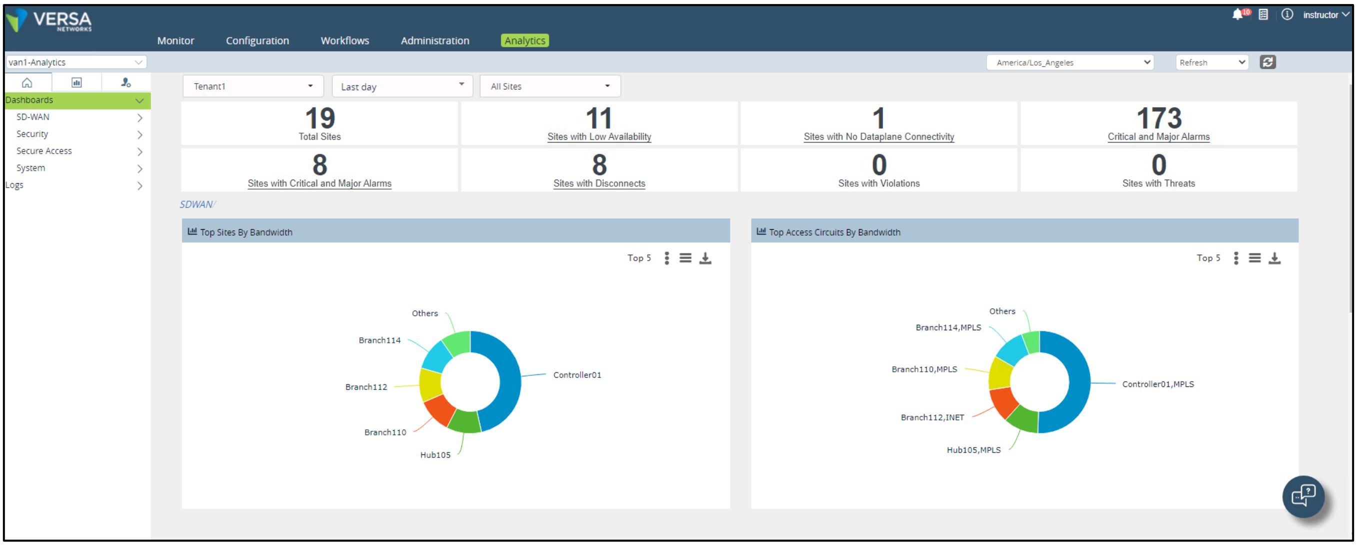
Path Handle	Fwd Class	Local WAN Link	Remote WAN Li...	Local WAN Link ...	Remote WAN Li...	Two Way Delay(...	Fwd Delay Var(...	Rev Delay Var(...	PDU Loss Ratio(...	Fwd Loss Ratio(...	Rev Loss Ratio(%)	Fwd Loss	Rev Loss	PDU Sent	PDU Rcvd
6820100	fc_ef	MPLS	MPLS	1	1	0	0	0	0.0	0.0	0.0	0	0	5	5
6824452	fc_ef	INET	INET	2	2	0	0	0	0.0	0.0	0.0	0	0	5	5

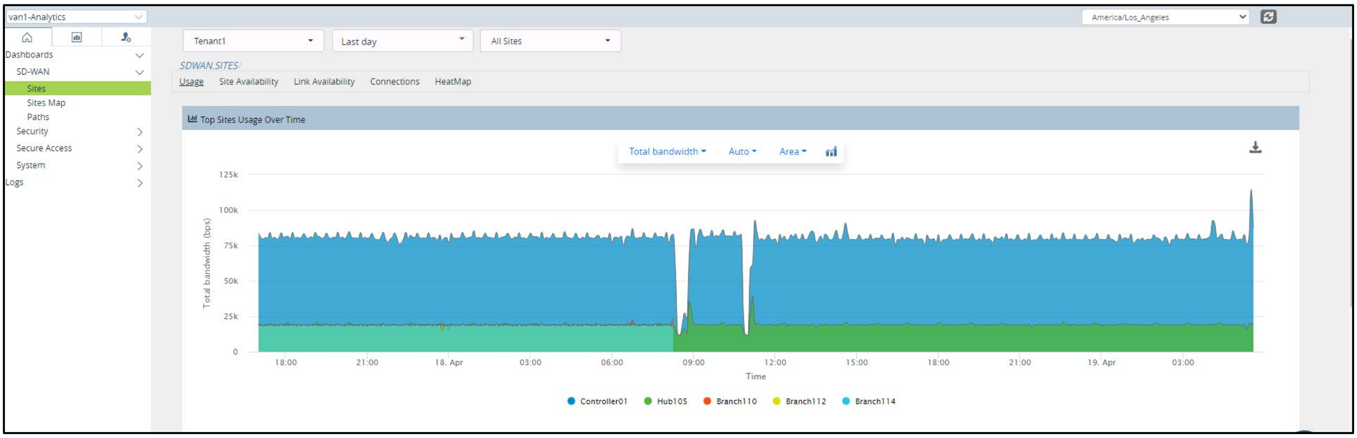


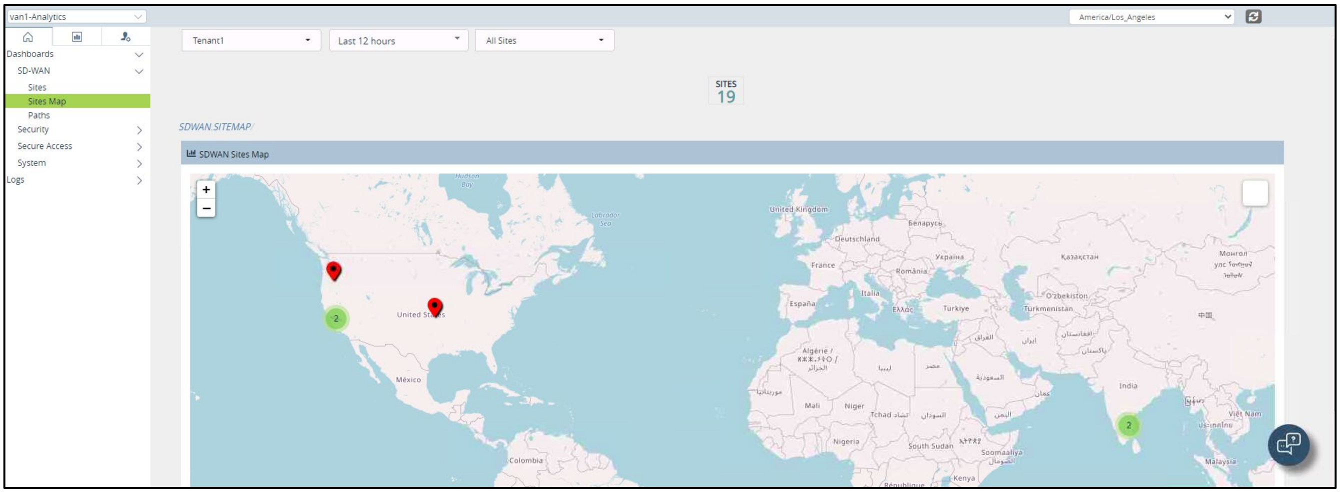
Rule Name	Hit Count	Forward Pkt Count	Forward Byte Count	Reverse Pkt Count	Reverse Byte Count	Hit Rate	Inactive Session Count
Allow_From_Trust	521	11156	935354	140	13124	0	519
Allow_From_SDWAN	0	0	0	0	0	0	0

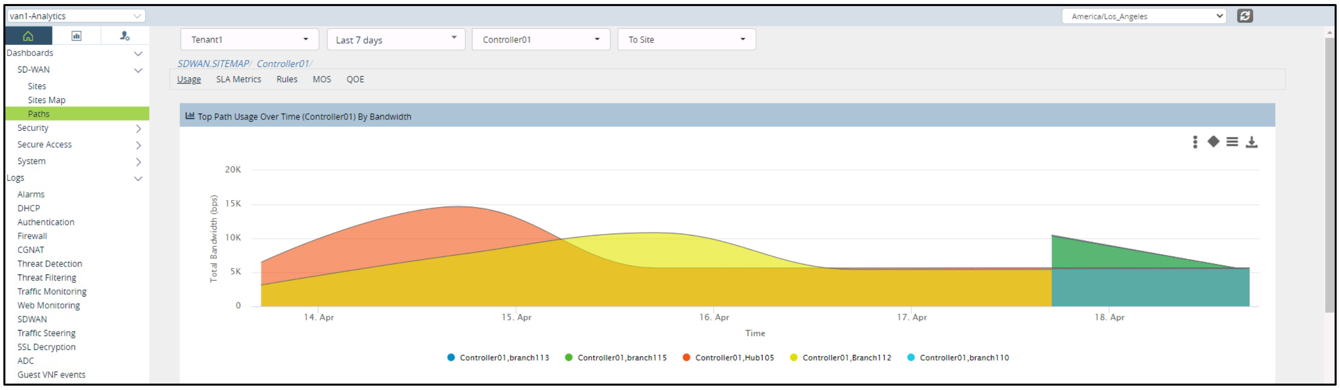
Versa Analytics

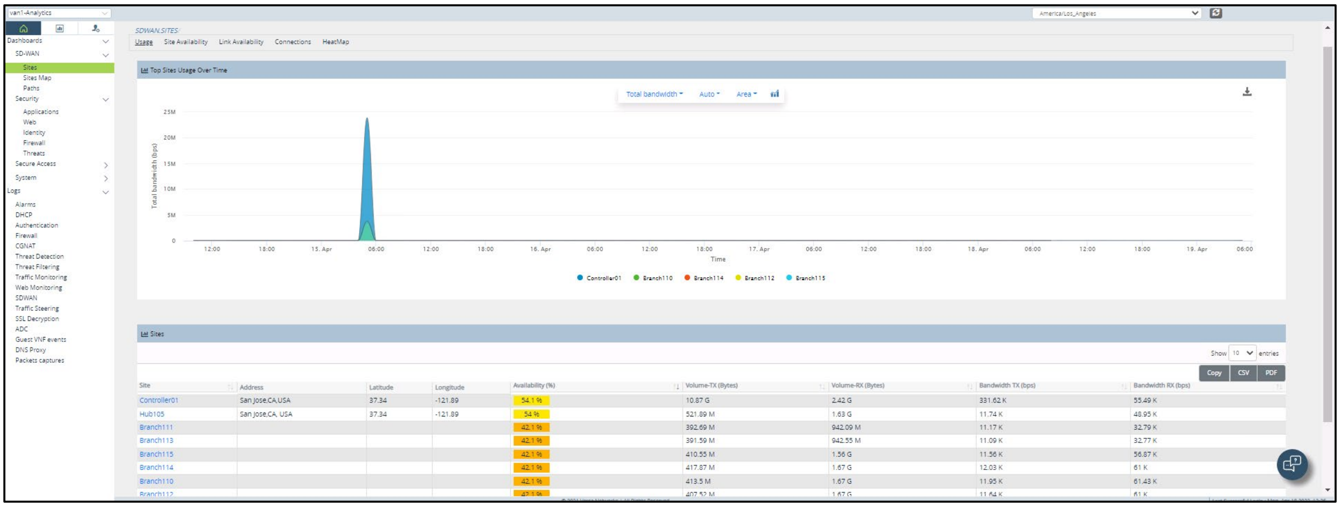
The Versa Analytics dashboard provides near-real-time and historical information about the statistics and logs that are gathered from the network. The information can be sorted and filtered based on event and statistic properties, as well as time periods. Below are examples of some of the different Analytics dashboards available.





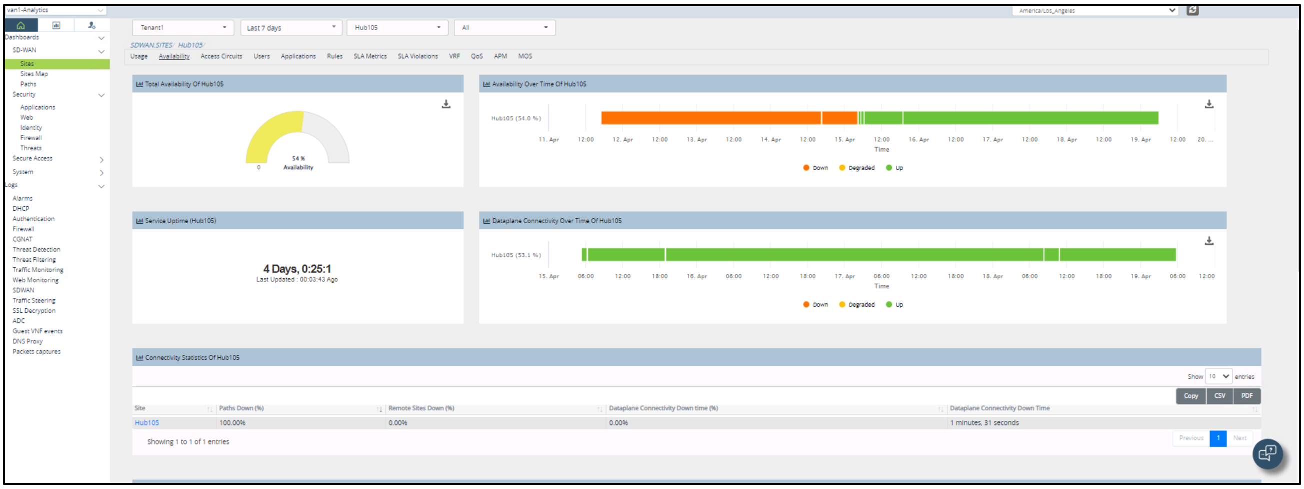






Site	Address	Latitude	Longitude	Availability (%)	Volume-TX (Bytes)	Volume-RX (Bytes)	Bandwidth TX (bps)	Bandwidth RX (bps)
Controller01	San Jose,CA,USA	37.34	-121.89	54.1 %	10.87 G	2.42 G	331.62 K	55.49 K
Hub105	San Jose,CA, USA	37.34	-121.89	54 %	521.89 M	1.63 G	11.74 K	48.95 K
Branch111				42.1 %	392.69 M	942.09 M	11.17 K	32.79 K
Branch113				42.1 %	391.59 M	942.55 M	11.09 K	32.77 K
Branch115				42.1 %	410.55 M	1.56 G	11.56 K	56.87 K
Branch114				42.1 %	417.87 M	1.67 G	12.03 K	61 K
Branch110				42.1 %	413.5 M	1.67 G	11.95 K	61.43 K
Branch112				42.1 %	407.52 M	1.67 G	11.64 K	61 K

Selecting individual sites provides site-specific details



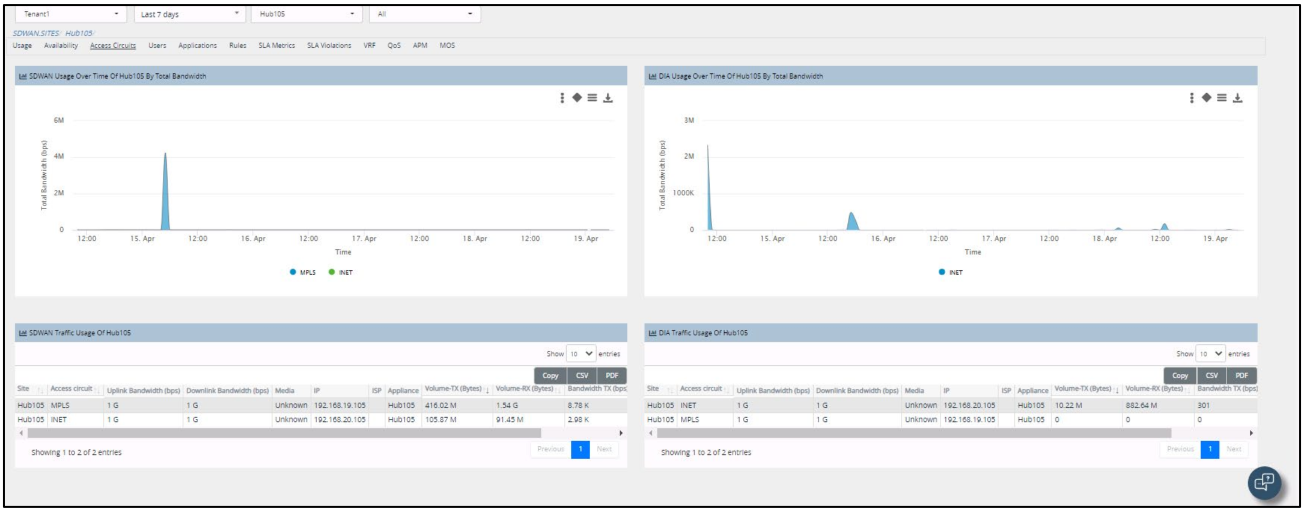
Tenant1 | Last 7 days | Hub105 | All

SDWAN.SITES/ Hub105/

4 Days, 0:25:1
Last Updated : 00:03:43 Ago

Site	Paths Down (%)	Remote Sites Down (%)	Dataplane Connectivity Down time (%)	Dataplane Connectivity Down Time
Hub105	100.00%	0.00%	0.00%	1 minutes, 31 seconds

Showing 1 to 1 of 1 entries



Tenant1 | Last 7 days | Hub105 | All

SDWAN.SITES/ Hub105/

SDWAN Traffic Usage Of Hub105

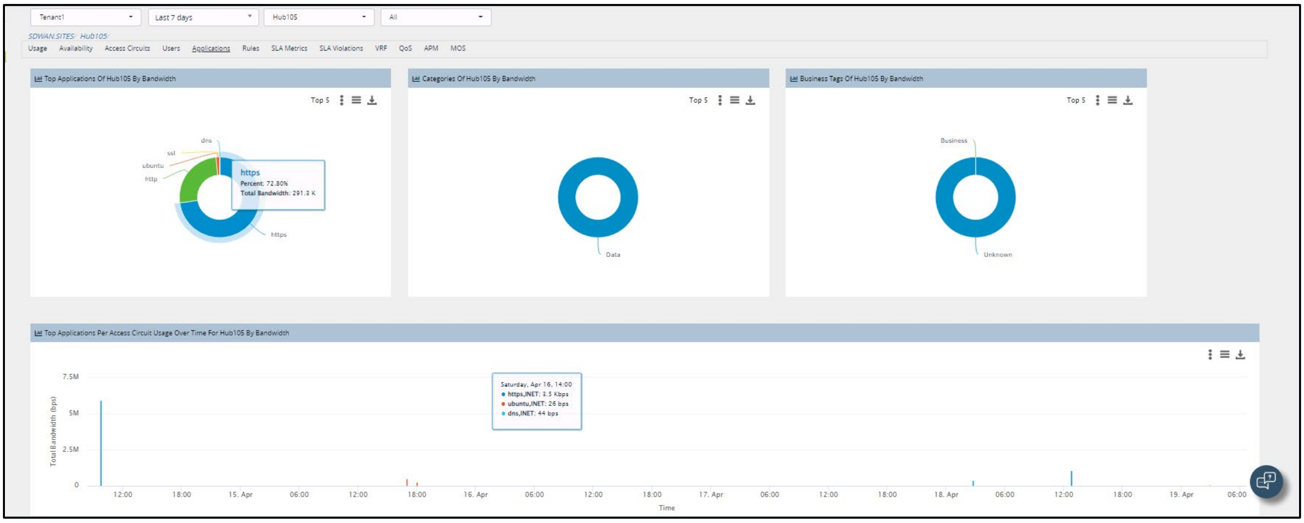
Site	Access circuit	Uplink Bandwidth (bps)	Downlink Bandwidth (bps)	Media	IP	ISP	Appliance	Volume-TX (Bytes)	Volume-RX (Bytes)	Bandwidth TX (bps
Hub105	MPLS	1 G	1 G	Unknown	192.168.19.105		Hub105	416.02 M	1.54 G	8.78 K
Hub105	INET	1 G	1 G	Unknown	192.168.20.105		Hub105	105.87 M	91.45 M	2.98 K

Showing 1 to 2 of 2 entries

DIA Traffic Usage Of Hub105

Site	Access circuit	Uplink Bandwidth (bps)	Downlink Bandwidth (bps)	Media	IP	ISP	Appliance	Volume-TX (Bytes)	Volume-RX (Bytes)	Bandwidth TX (bps
Hub105	INET	1 G	1 G	Unknown	192.168.20.105		Hub105	10.22 M	882.64 M	301
Hub105	MPLS	1 G	1 G	Unknown	192.168.19.105		Hub105	0	0	0

Showing 1 to 2 of 2 entries



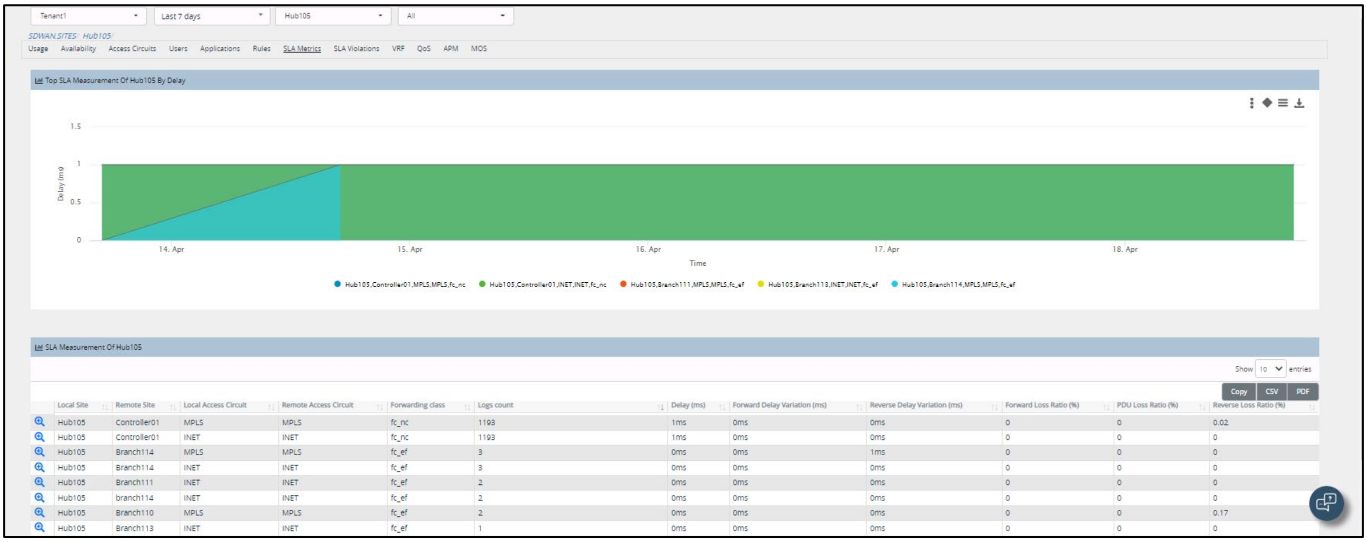
Tenant1 | Last 7 days | Hub105 | All

SDWAN.SITES/ Hub105/

https
Percent: 72.80%
Total Bandwidth: 291.3 K

Saturday, Apr 16, 14:00
● https,INET: 3.5 Kbps
● ubuntu,INET: 26 bps
● dns,INET: 44 bps

Selecting individual sites provides site-specific details

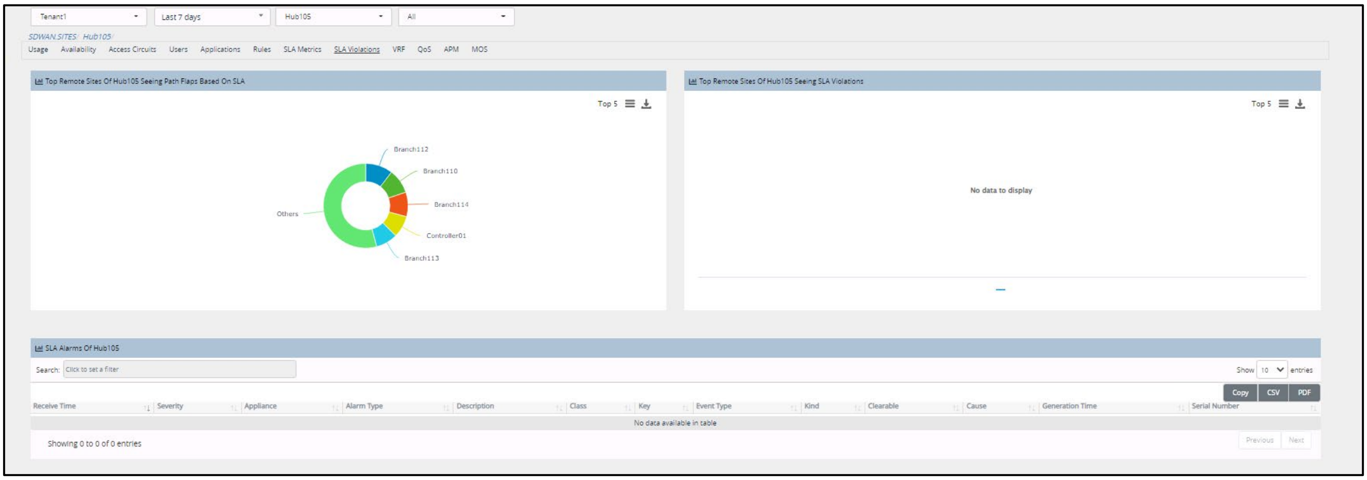

Tenant1
Last 7 days
Hub105
All
SDWAN.SITES / Hub105
Usage
Availability
Access Circuits
Users
Applications
Rules
SLA Metrics
SLA Violations
VRF
QoS
APM
MOS
Top SLA Measurement Of Hub105 By Delay
1.5
1
0.5
0
Delay (ms)
14. Apr
15. Apr
16. Apr
17. Apr
18. Apr
Time
Hub105,Controller01,MPLS,MPLS,fc_nc
Hub105,Controller01,INET,INET,fc_nc
Hub105,Branch111,MPLS,MPLS,fc_ef
Hub105,Branch113,INET,INET,fc_ef
Hub105,Branch114,MPLS,MPLS,fc_ef

SLA Measurement Of Hub105

Show 10 entries

Copy CSV PDF

Local Site	Remote Site	Local Access Circuit	Remote Access Circuit	Forwarding class	Logs count	Delay (ms)	Forward Delay Variation (ms)	Reverse Delay Variation (ms)	Forward Loss Ratio (%)	PDU Loss Ratio (%)	Reverse Loss Ratio (%)
Hub105	Controller01	MPLS	MPLS	fc_nc	1193	1ms	0ms	0ms	0	0	0.02
Hub105	Controller01	INET	INET	fc_nc	1193	1ms	0ms	0ms	0	0	0
Hub105	Branch114	MPLS	MPLS	fc_ef	3	0ms	0ms	1ms	0	0	0
Hub105	Branch114	INET	INET	fc_ef	3	0ms	0ms	0ms	0	0	0
Hub105	Branch111	INET	INET	fc_ef	2	0ms	0ms	0ms	0	0	0
Hub105	branch114	INET	INET	fc_ef	2	0ms	0ms	0ms	0	0	0
Hub105	Branch110	MPLS	MPLS	fc_ef	2	0ms	0ms	0ms	0	0	0.17
Hub105	Branch113	INET	INET	fc_ef	1	0ms	0ms	0ms	0	0	0



SLA Alarms Of Hub105

Search: Click to set a filter

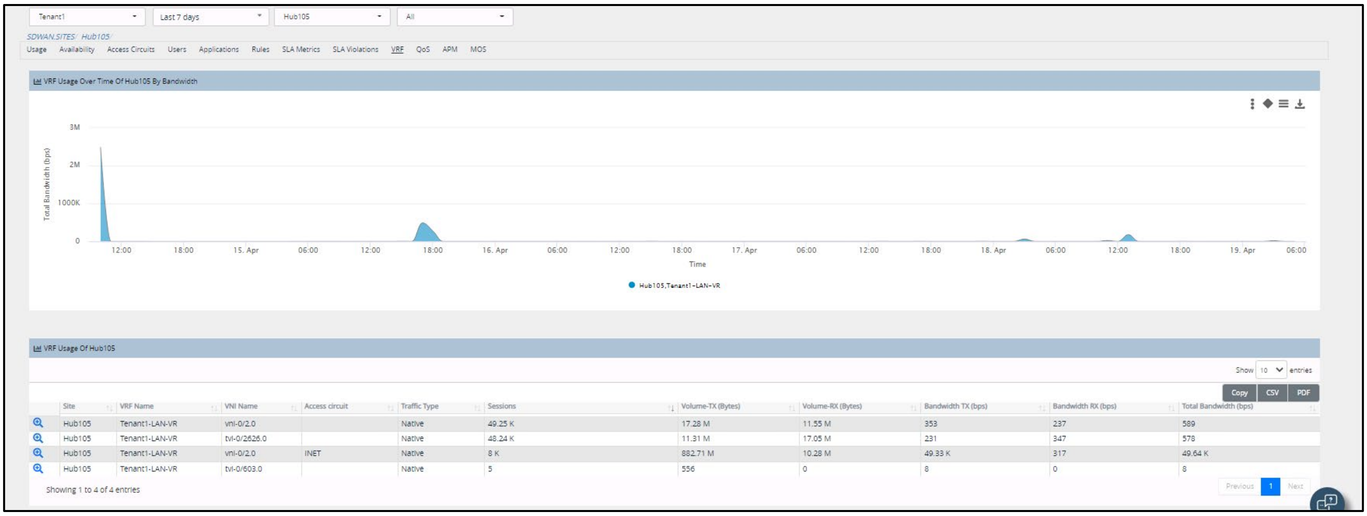
Show 10 entries

Copy CSV PDF

Receive Time	Severity	Appliance	Alarm Type	Description	Class	Key	Event Type	Kind	Clearable	Cause	Generation Time	Serial Number
No data available in table												

Showing 0 to 0 of 0 entries

Previous Next



VRF Usage Of Hub105

Show 10 entries

Copy CSV PDF

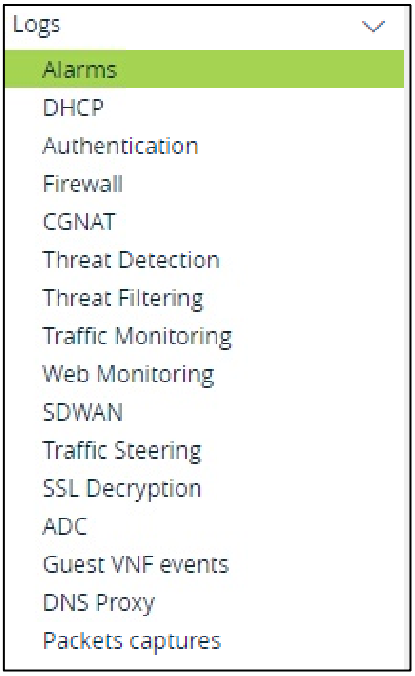
Site	VRF Name	VNI Name	Access circuit	Traffic Type	Sessions	Volume-TX (Bytes)	Volume-RX (Bytes)	Bandwidth TX (bps)	Bandwidth RX (bps)	Total Bandwidth (bps)
Hub105	Tenant1-LAN-VR	vni-0/2.0		Native	49.25 K	17.28 M	11.55 M	353	237	589
Hub105	Tenant1-LAN-VR	tvi-0/2626.0		Native	48.24 K	11.31 M	17.05 M	231	347	578
Hub105	Tenant1-LAN-VR	vni-0/2.0	INET	Native	8 K	882.71 M	10.28 M	49.33 K	317	49.64 K
Hub105	Tenant1-LAN-VR	tvi-0/603.0		Native	5	556	0	8	0	8

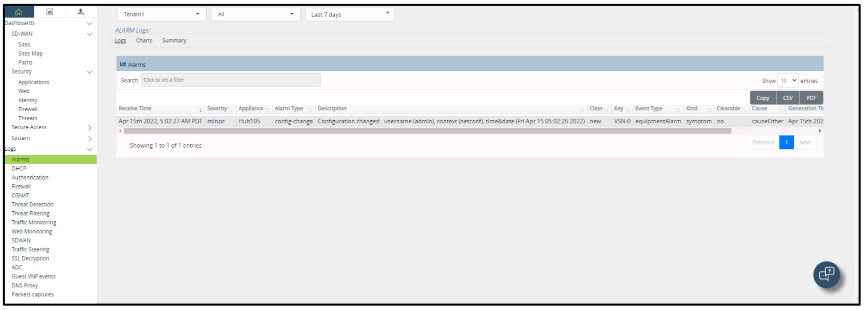
Showing 1 to 4 of 4 entries

Previous 1 Next

Logs

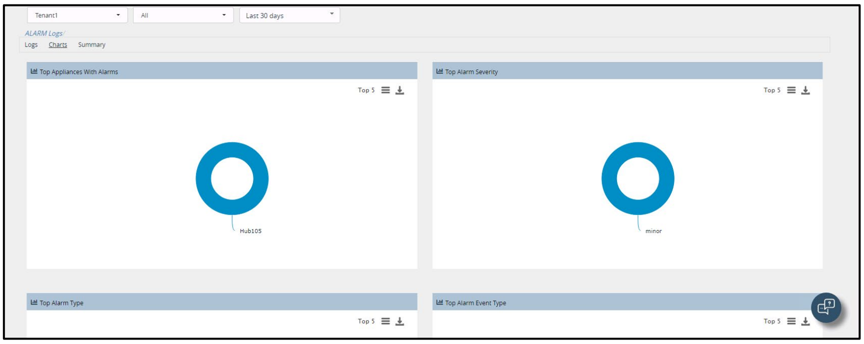
The Logs dashboard contains the log entries that are forwarded to Versa Analytics from end devices. Note: Logs are triggered events, many of which are configured in service policies. Because few services are currently configured in the lab environment, most of the log categories do not contain any data.

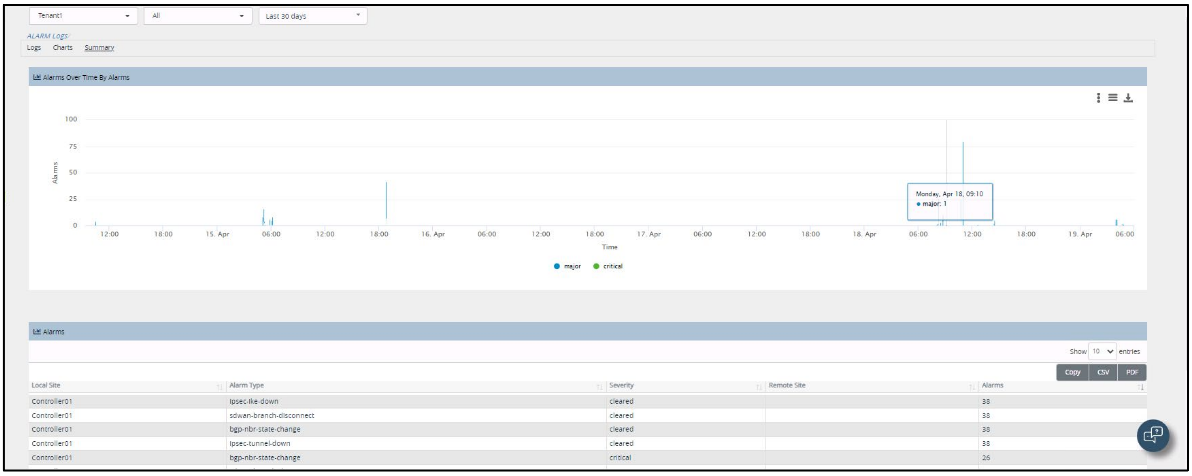




Receive Time	Severity	Appliance	Alarm Type	Description	Class	Key	Event Type	Kind	Clearable	Cause	Generation Ti
Apr 15th 2022, 5:02:27 AM PDT	minor	Hub105	config-change	Configuration changed : username (admin), context (netconf), time&date (Fri Apr 15 05:02:26 2022)	new	VSN-0	equipmentAlarm	symptom	no	causeOther	Apr 15th 202

Showing 1 to 1 of 1 entries





Local Site	Alarm Type	Severity	Remote Site	Alarms
Controller01	ipsec-ike-down	cleared		38
Controller01	sdwan-branch-disconnect	cleared		38
Controller01	bgp-nbr-state-change	cleared		38
Controller01	ipsec-tunnel-down	cleared		38
Controller01	bgp-nbr-state-change	critical		26

STOP! When you have finished exploring the Monitor and Analytics dashboards, notify your instructor that you have completed this lab.

Diagnostic Tools

The Versa Networks lab environment consists of a fixed, pre-configured topology that will allow you to explore, configure, and manage Versa Networks CPEs by using Versa Director, the central management and orchestration platform for a Versa Secure SD-WAN solution. After completing this lab, you will be able to:

- Use the built-in diagnostic tools to test reachability between devices; and
- Configure and run the speedtest function between devices.

In this lab, you will be assigned a single CPE device (Branch device) for configuration and monitoring.

The lab environment is accessed through Amazon Workspaces. You should have received an email to allow you to register your Amazon Workspaces account and set your password.

NOTE: It is common for the Amazon Workspaces email to be sent to the spam/junk folder. If you have not received the registration email, check those folders.

The remote desktop connection opens a remote workstation, where you will use various tools to navigate and configure the lab environment. The main tool you will use in this lab is Versa Director. Versa Director can be accessed by opening the Google Chrome browser on the Remote Desktop. There is a bookmark to the Versa Director device in the Google Chrome bookmark bar.

This lab environment is a shared environment. There may be up to 24 students in the environment. Each student has their own remote desktop, but the Versa Director is shared. Because of the shared environment, you may see configuration templates, device groups, workflows, and devices that other students have created, or that have been pre-provisioned within Versa Director. It is important that you only modify the configuration components that are assigned to you by your instructor.

During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not be the same, etc.) Do not be alarmed if your results vary slightly from the results shown in the lab guide. The important thing is that the lab functions in the desired manner.

Look for these hints to help you in the labs

This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

Now that we've discussed what is expected, let's get started!

Lab Exercise Overview

In this lab you will perform various tasks and is an open lab environment. You will be given minimal guidance on how to perform the tasks. In this lab you will:

Open the Versa Director Monitor dashboard

Open the Appliance Context mode of your device in order to gain access to the diagnostic tools

Initiate a PING to the WAN interface of the Hub device on the MPLS transport

Initiate a PING to the WAN interface of the Hub device on the INET transport

Initiate a PING to the LAN interface on the Hub device in the LAN routing instance

Initiate a speedtest from your node to the Hub device over the MPLS transport

Initiate a speedtest from your node to the Hub device over the LAN routing instance

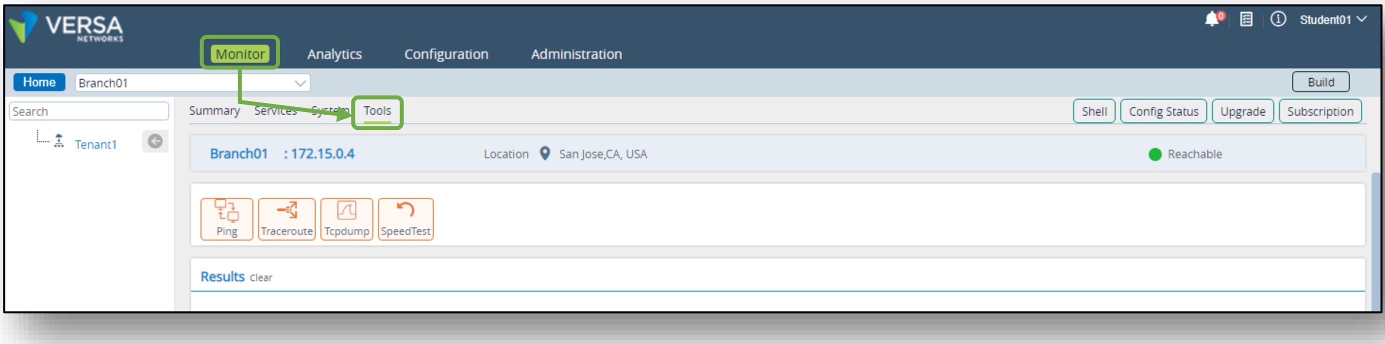
Exercise 1: Access the Diagnostic Tools

Please refer to the Lab Access Guide for instructions on how to connect to the remote lab environment.

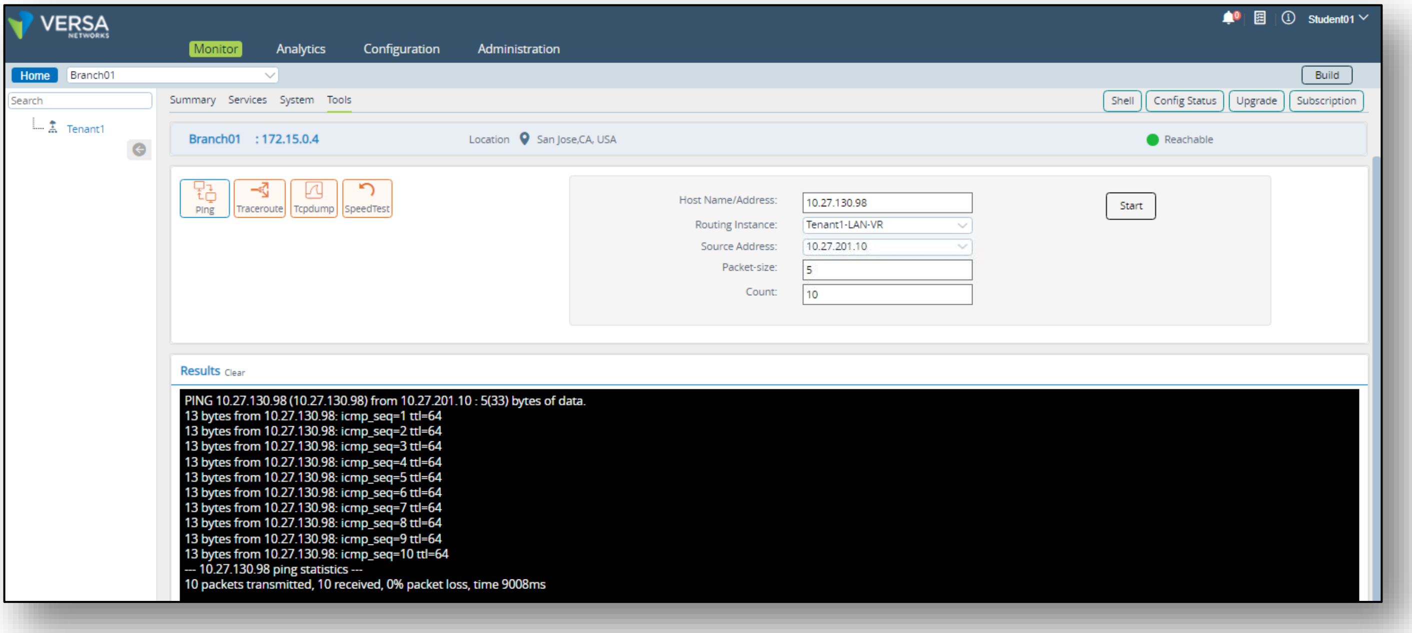
In the remote landing station, open the Google Chrome browser and log into Versa Director. In Versa Director, open the *Administration > Appliances* dashboard in Versa Director.

In this lab part you will navigate to the Appliance Context mode of your assigned node. All configuration and diagnostic tasks will be performed from the Appliance Context mode.

Navigate to the Appliance Context mode of your device. In the Appliance Context mode of your device, locate and open the Tools tab in the Monitor dashboard.



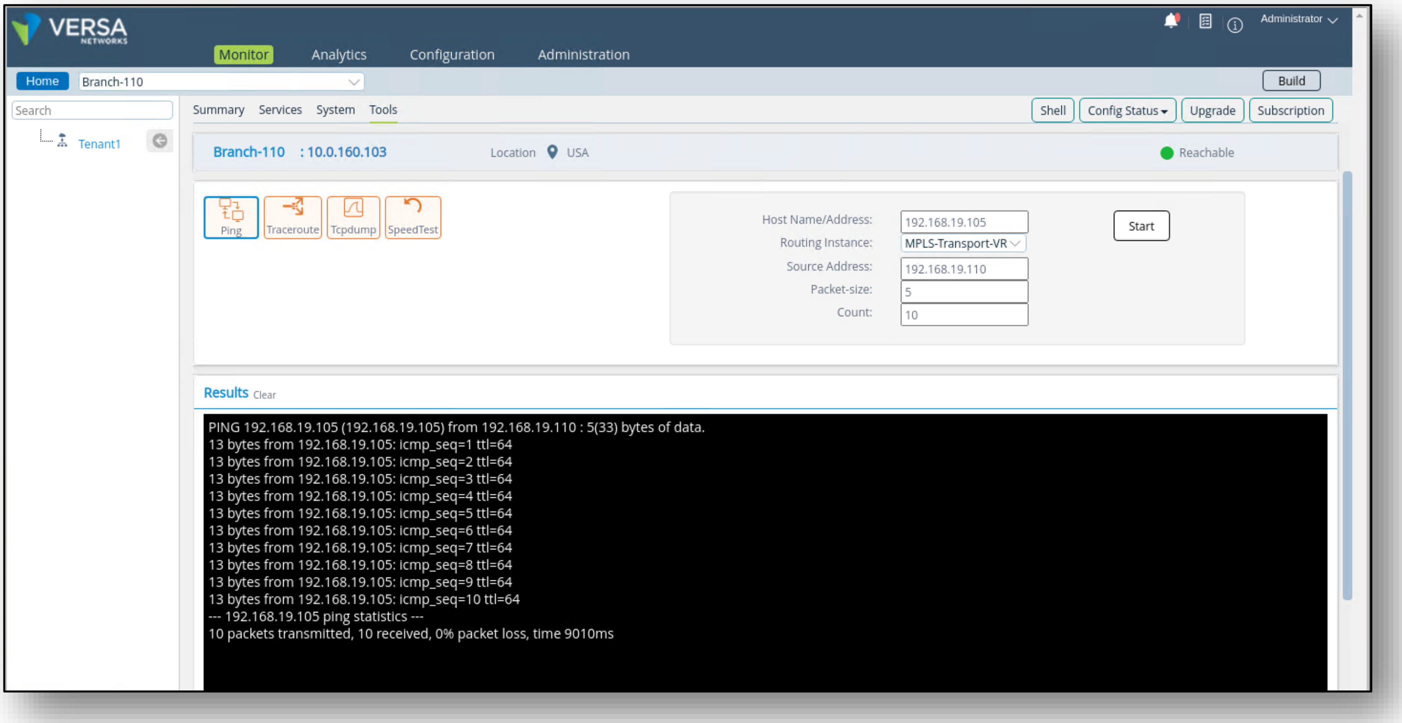
Open the Ping utility and initiate an ICMP request to the LAN port of the Hub device (10.27.130.98). Ensure that you are sourcing the ICMP request from the Tenant LAN VR and the IP address of your local LAN port.



Host Name/Address: 10.27.130.98
Routing Instance: Tenant1-LAN-VR
Source Address: 10.27.201.10
Packet-size: 5
Count: 10

```
PING 10.27.130.98 (10.27.130.98) from 10.27.201.10 : 5(33) bytes of data.
13 bytes from 10.27.130.98: icmp_seq=1 ttl=64
13 bytes from 10.27.130.98: icmp_seq=2 ttl=64
13 bytes from 10.27.130.98: icmp_seq=3 ttl=64
13 bytes from 10.27.130.98: icmp_seq=4 ttl=64
13 bytes from 10.27.130.98: icmp_seq=5 ttl=64
13 bytes from 10.27.130.98: icmp_seq=6 ttl=64
13 bytes from 10.27.130.98: icmp_seq=7 ttl=64
13 bytes from 10.27.130.98: icmp_seq=8 ttl=64
13 bytes from 10.27.130.98: icmp_seq=9 ttl=64
13 bytes from 10.27.130.98: icmp_seq=10 ttl=64
--- 10.27.130.98 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9008ms
```

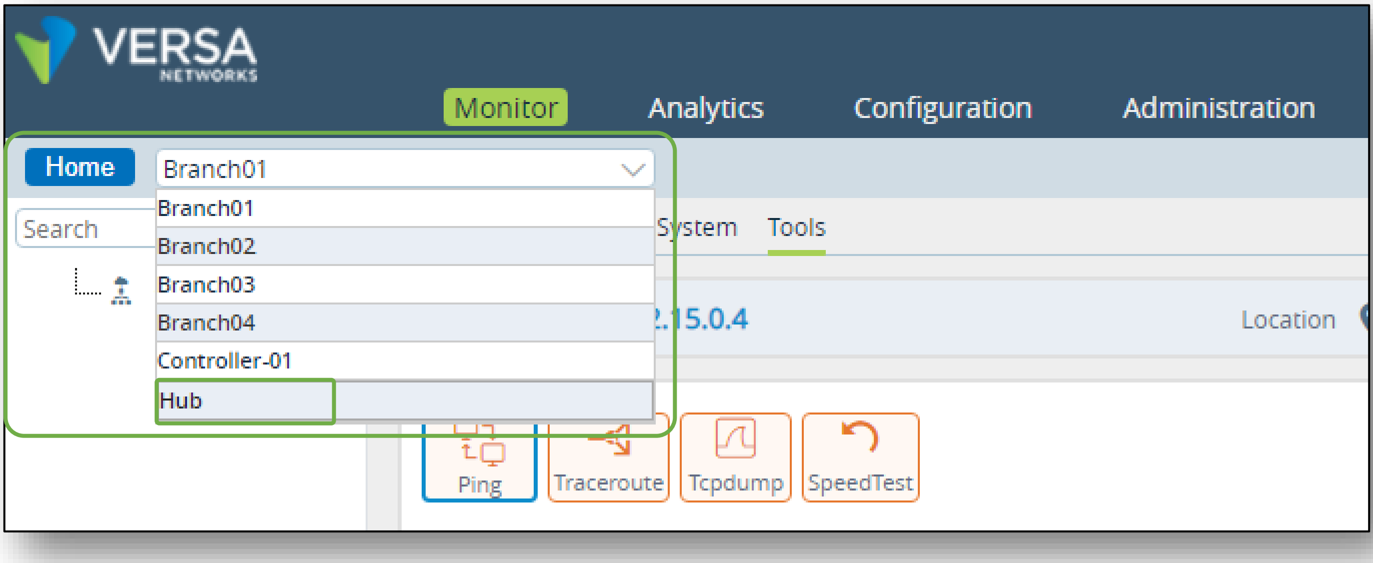
From the Ping utility, initiate an ICMP request to the MPLS WAN port of the Hub device (192.168.19.105) to verify connectivity to the WAN interface of the hub. Be sure to source your ICMP request from the WAN IP address of your device and from the MPLS transport virtual router.



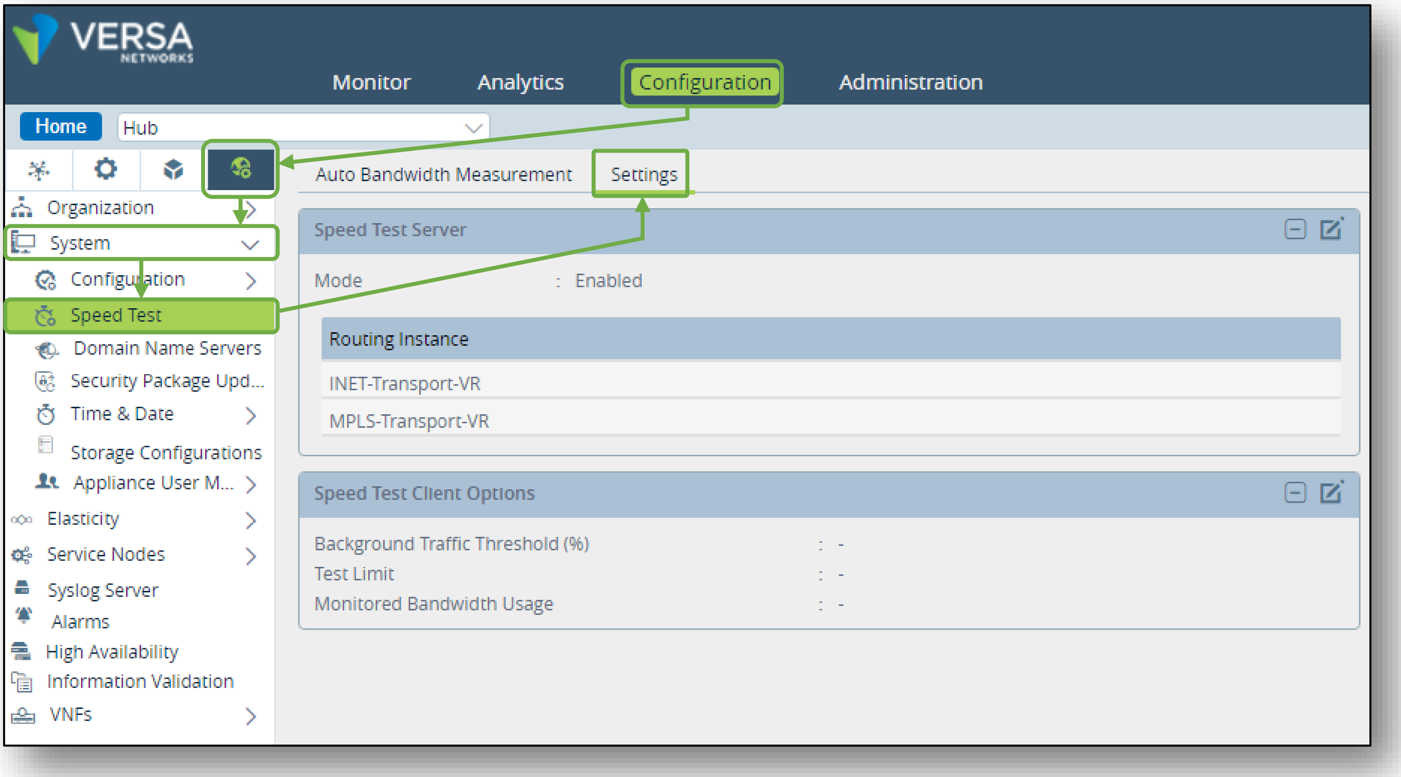
Host Name/Address: 192.168.19.105
Routing Instance: MPLS-Transport-VR
Source Address: 192.168.19.110
Packet-size: 5
Count: 10

```
PING 192.168.19.105 (192.168.19.105) from 192.168.19.110 : 5(33) bytes of data.
13 bytes from 192.168.19.105: icmp_seq=1 ttl=64
13 bytes from 192.168.19.105: icmp_seq=2 ttl=64
13 bytes from 192.168.19.105: icmp_seq=3 ttl=64
13 bytes from 192.168.19.105: icmp_seq=4 ttl=64
13 bytes from 192.168.19.105: icmp_seq=5 ttl=64
13 bytes from 192.168.19.105: icmp_seq=6 ttl=64
13 bytes from 192.168.19.105: icmp_seq=7 ttl=64
13 bytes from 192.168.19.105: icmp_seq=8 ttl=64
13 bytes from 192.168.19.105: icmp_seq=9 ttl=64
13 bytes from 192.168.19.105: icmp_seq=10 ttl=64
--- 192.168.19.105 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9010ms
```

Navigate to the Hub device configuration by selecting the Hub-105 device from the top-left dropdown menu.



From the Hub device Appliance Context, navigate to *Configuration > Others > System* and locate the Speed Test Server configuration section. Click the Settings tab to display the currently configured speedtest server settings.



Speed Test Server

Mode : Enabled

Routing Instance
INET-Transport-VR
MPLS-Transport-VR

Speed Test Client Options

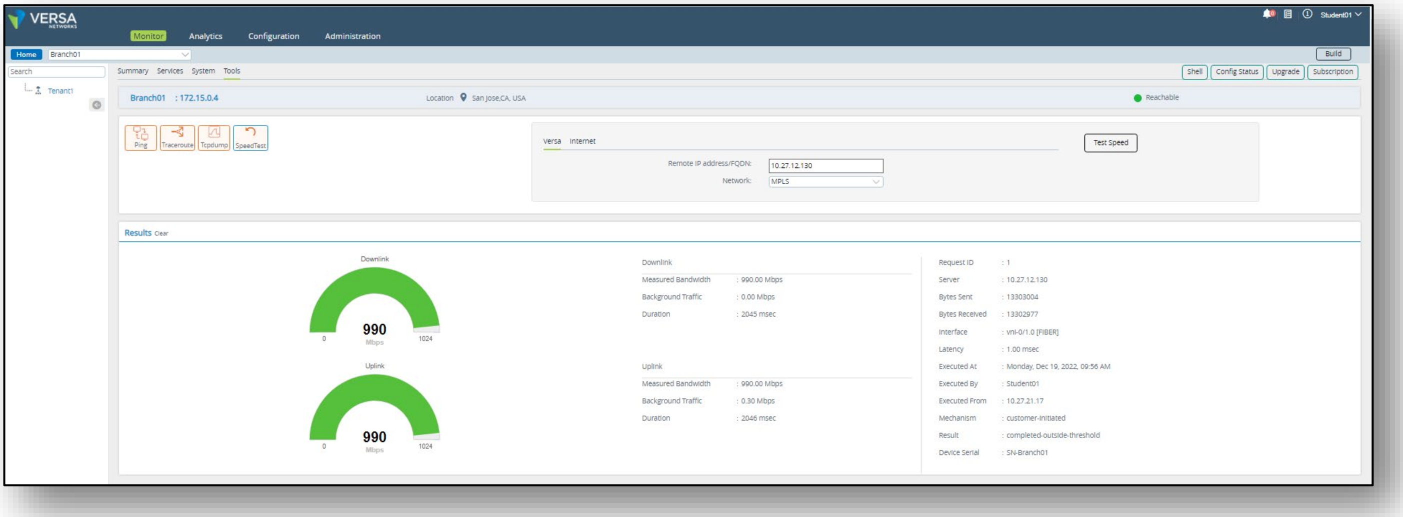
Background Traffic Threshold (%) : -
Test Limit : -
Monitored Bandwidth Usage : -

The speedtest server function can respond to and service speedtest request on the routing instances on which the server is enabled. On the hub device, the speedtest server function is enabled on the customer-facing LAN and both transport networks.

Return to the Appliance Context mode of **YOUR** device by selecting your device from the device drop-down menu.

From your Appliance Context mode, navigate to *Monitor > Tools* and select the SpeedTest tool.

In the SpeedTest dashboard, initiate a speed test between your device and the Hub device MPLS WAN port (10.27.12.130). Ensure that the correct routing instance and interface for the traffic is selected. The results will be shown after the test is complete.



Branch01 : 172.15.0.4 Location San Jose,CA, USA Reachable

Remote IP address/FQDN: 10.27.12.130

Network: MPLS

Downlink

Measured Bandwidth : 990.00 Mbps

Background Traffic : 0.00 Mbps

Duration : 2045 msec

Uplink

Measured Bandwidth : 990.00 Mbps

Background Traffic : 0.30 Mbps

Duration : 2046 msec

Request ID : 1

Server : 10.27.12.130

Bytes Sent : 13303004

Bytes Received : 13302977

Interface : vni-0/1.0 [FIBER]

Latency : 1.00 msec

Executed At : Monday, Dec 19, 2022, 09:56 AM

Executed By : Student01

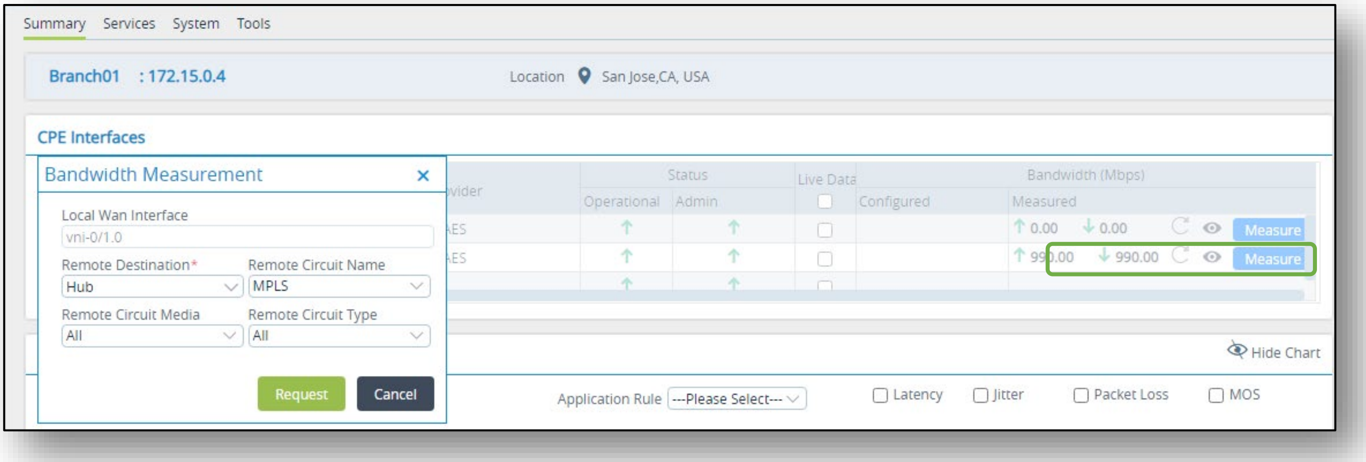
Executed From : 10.27.21.17

Mechanism : customer-initiated

Result : completed-outside-threshold

Device Serial : SN-Branch01

Another way to start a speed test is from the Summary tab of the Appliance Context. Navigate to the Summary tab and locate the INET interface in the CPE Interfaces table (vni-0/1.0). On the right side of the table, click the Measure button to initiate a speed test on that link. Fill in the dialog box that appears and click Request.



Branch01 : 172.15.0.4 Location San Jose,CA, USA

Local Wan Interface: vni-0/1.0

Remote Destination*: Hub

Remote Circuit Name: MPLS

Remote Circuit Media: All

Remote Circuit Type: All

Measured: ↑ 0.00 ↓ 0.00

Measured: ↑ 990.00 ↓ 990.00

Application Rule: ---Please Select---

STOP! Notify your instructor that you have completed this lab.