Versa Class of Service

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 structure of the Class of Service configuration hierarchy
- Configure Class of Service services

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

The lab environment is accessed through a remote desktop connection. 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 5 other 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.

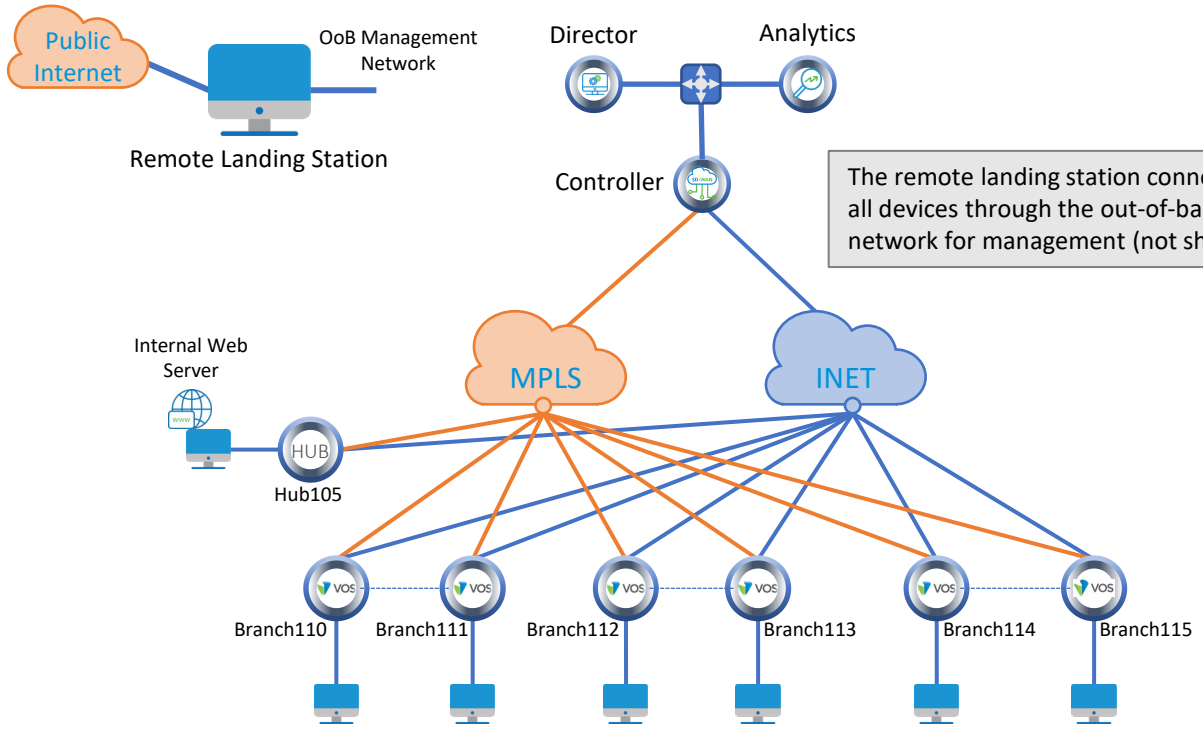
Look for these hints to help you in the labs

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. At the end of the lab guide you can find additional help on to how to complete the tasks, so if you have trouble with a task, please refer to the help section. If you still cannot accomplish the task, ask your instructor for assistance. In addition, you will see **hints** placed throughout the lab guide to help you along.

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 Topology



Each branch device connects to the MPLS transport and to the INET Transport

- MPLS: vni-0/0
- INET: vni-0/1

Each branch connects to a local LAN

- vni-0/2

Each branch pair has a cross-connect (used in HA labs only)

- vni-0/3

Remember this! You will use it a lot!

Versa Director Login: **`labuserXYZ`** (e.g. **`labuser110`**, **`labuser111`**, etc.)
Versa Director Password: **`Versa@123`**

Branch OoB Login: **`admin`**
Branch OoB Password: **`versa123`**

Testing Host Login: **`labuserXYZ`** (e.g. **`labuser110`**, **`labuser111`**, etc.)
Testing Host Password: **`versa123`**

Interface Addresses

CPE	vni-0/0	vni-0/1	vni-0/2
Branch110	192.168.19.110/24	192.168.20.110/24	172.16.110.1/24
Branch111	192.168.19.111/24	192.168.20.111/24	172.16.111.1/24
Branch112	192.168.19.112/24	192.168.20.112/24	172.16.112.1/24
Branch113	192.168.19.113/24	192.168.20.113/24	172.16.113.1/24
Branch114	192.168.19.114/24	192.168.20.114/24	172.16.114.1/24
Branch115	192.168.19.115/24	192.168.20.115/24	172.16.115.1/24
MPLS Gateway	192.168.19.3		
INET Gateway		192.168.20.3	

Controller Addresses

MPLS	MPLS Gateway	INET	INET Gateway
192.168.17.3/24	192.168.17.1	192.168.18.3/24	192.168.18.1

Exercise 1: Connect to the remote lab environment

The first lab exercise is to become familiar with how to connect to the remote lab environment. Your instructor should have reviewed the following information with you prior to starting:

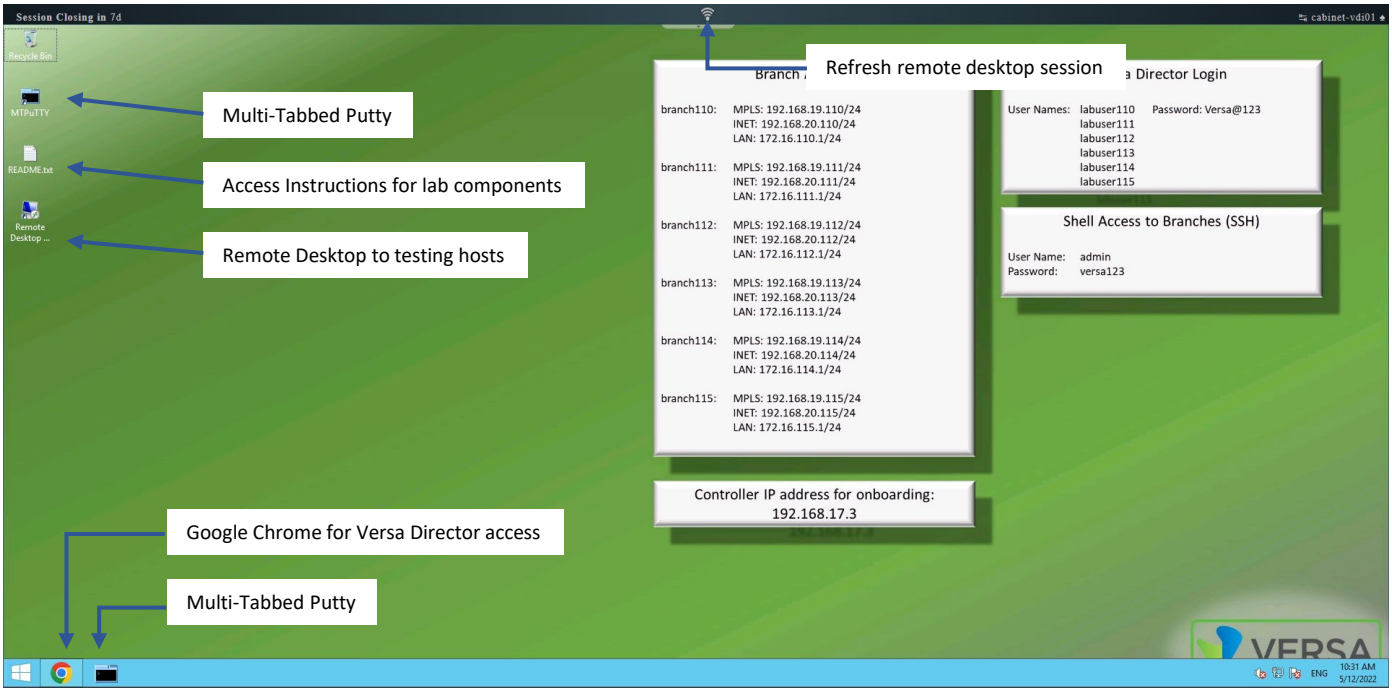
- Branch/Node/CPE Assignment
- Remote Lab Access

If you have not yet been assigned a branch device, please contact the instructor as this is a shared environment, and each student will configure and monitor a specific branch node.

Question: What node is assigned to you in the lab topology? _____

Follow the instructions provided by your instructor to connect to the remote lab environment.

Once you have started your remote desktop session, you will be presented with the remote desktop:



On the remote desktop, open the Google Chrome browser window. The Google Chrome browser window contains a bookmark to the Versa Director. Log into the Versa Director with the username associated with your assigned branch device:

CPE	Username	Password
Branch110	labuser110	Versa@123
Branch111	labuser111	Versa@123
Branch112	labuser112	Versa@123
Branch113	labuser113	Versa@123
Branch114	labuser114	Versa@123
Branch115	labuser115	Versa@123

Versa Application Steering and SLA

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 components required to enable traffic steering using SD-WAN Policy
- Identify the components used to measure and monitor transport path statistics
- Configure SD-WAN Profiles to define how application traffic should be treated
- Configure SD-WAN Policy to assign traffic flows to SD-WAN Profiles

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

The lab environment is accessed through a remote desktop connection. 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 5 other 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.

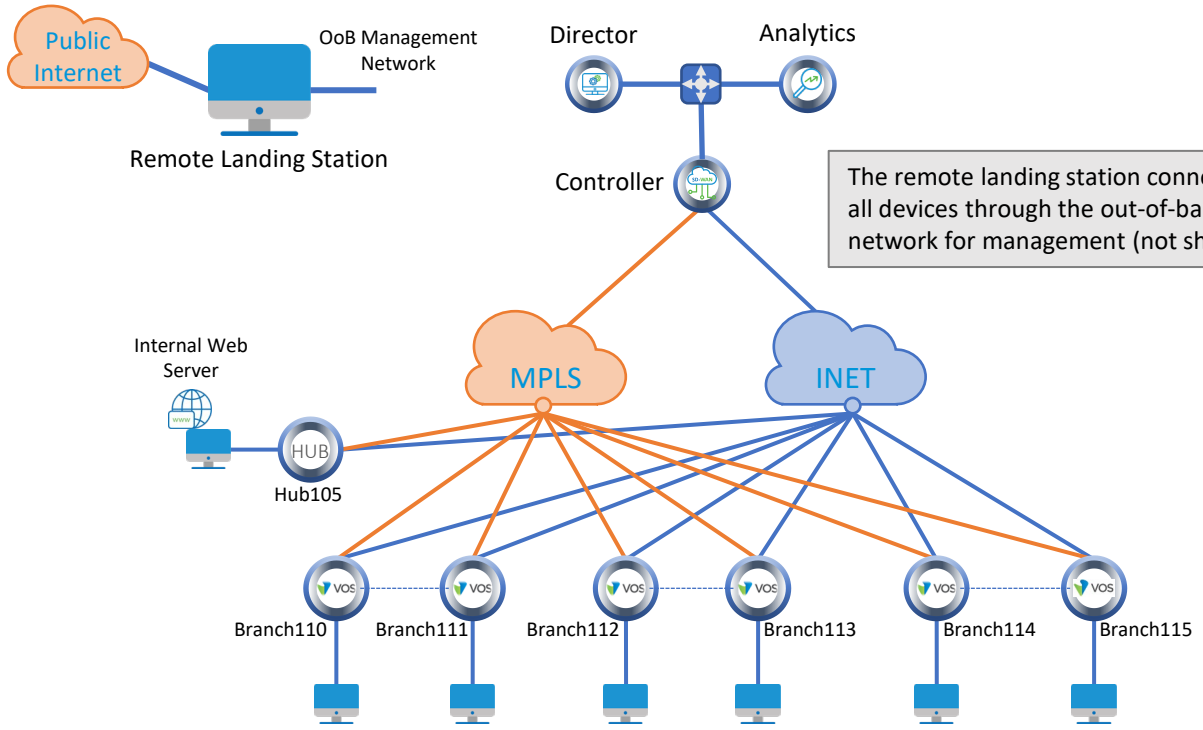
During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not 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.

This lab guide will step you through a set of exercises, and you will be asked to perform some basic tasks that will allow you to become more familiar with the the lab goals. If you cannot accomplish the task, ask your instructor for assistance.

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 Topology



Each branch device connects to the MPLS transport and to the INET Transport

- MPLS: vni-0/0
- INET: vni-0/1

Each branch connects to a local LAN

- vni-0/2

Each branch pair has a cross-connect (used in HA labs only)

- vni-0/3

Remember this! You will use it a lot!

Versa Director Login: **labuserXYZ** (e.g. **labuser110**, **labuser111**, etc.)
Versa Director Password: **Versa@123**

Branch OoB Login: **admin**
Branch OoB Password: **versa123**

Testing Host Login: **labuserXYZ** (e.g. **labuser110**, **labuser111**, etc.)
Testing Host Password: **versa123**

Interface Addresses

CPE	vni-0/0	vni-0/1	vni-0/2
Branch110	192.168.19.110/24	192.168.20.110/24	172.16.110.1/24
Branch111	192.168.19.111/24	192.168.20.111/24	172.16.111.1/24
Branch112	192.168.19.112/24	192.168.20.112/24	172.16.112.1/24
Branch113	192.168.19.113/24	192.168.20.113/24	172.16.113.1/24
Branch114	192.168.19.114/24	192.168.20.114/24	172.16.114.1/24
Branch115	192.168.19.115/24	192.168.20.115/24	172.16.115.1/24
MPLS Gateway	192.168.19.3		
INET Gateway		192.168.20.3	

Controller Addresses

MPLS	MPLS Gateway	INET	INET Gateway
192.168.17.3/24	192.168.17.1	192.168.18.3/24	192.168.18.1

Exercise 2: Create SLA Profiles to Track Link Statistics

In the following lab exercises, you will:

- Configure a set of SLA profiles that can be used to monitor the performance of links between sites

> **Note**: Configuration modifications in this lab will be performed in Appliance Context mode (directly on your device) and will not be performed through device templates.

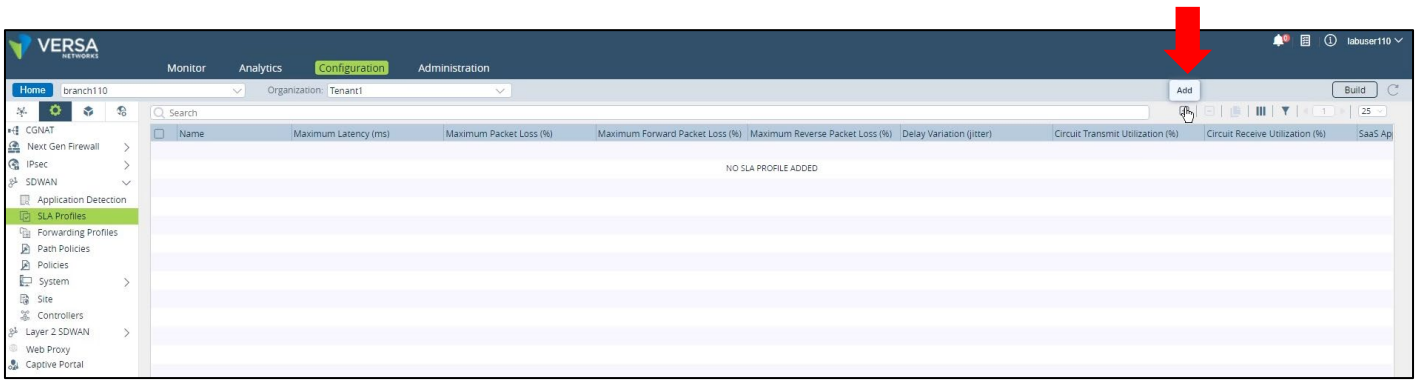
> **Note:** The images in this lab are for demonstration purposes only. Your lab experience may differ from the images provided in the lab guide.

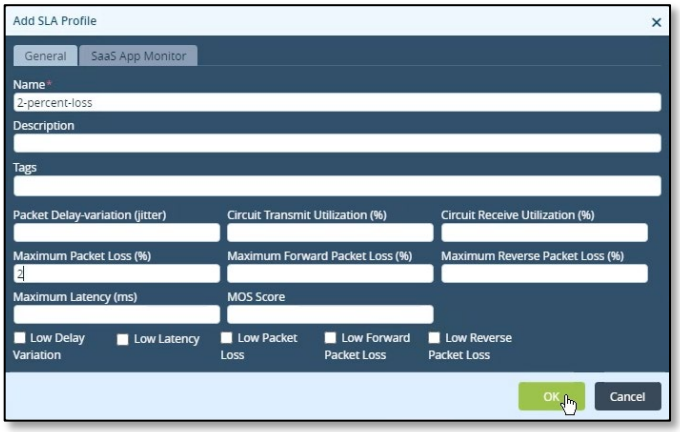
The SLA Monitoring process is constantly running on Versa Operating System. Each device sends probes to other devices on all available transport networks (paths) to determine the path performance, and the statistics that are gathered are automatically sent to Versa Analytics.

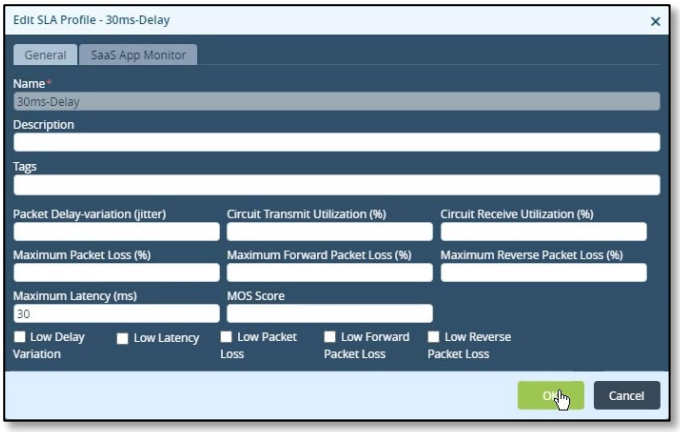
You can configure your device to use the statistics that are gathered to determine whether a transport path is suitable for different types of applications, based on administrative rules. To configure your device to track SLA statistics you configure SLA profiles.

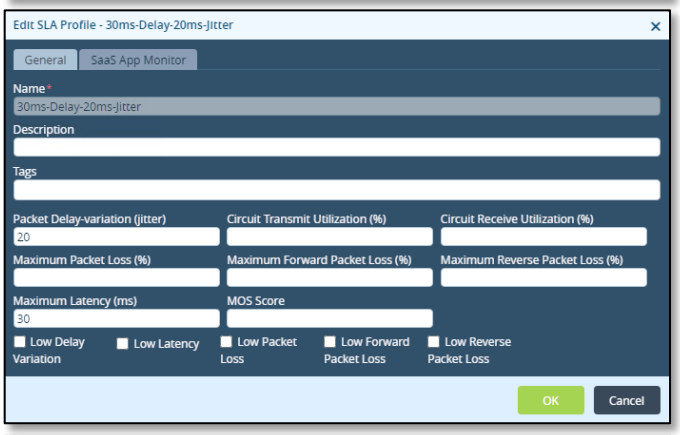
SLA profiles are configured under the Configuration > Services > SLA Profiles hierarchy.

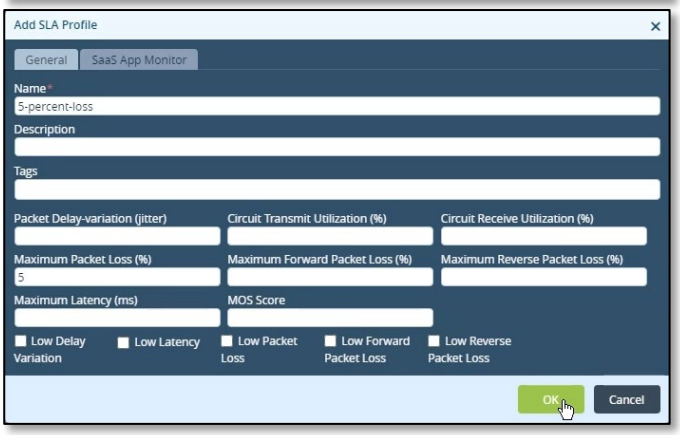
Navigate to the Configuration > Services > SLA Profiles hierarchy. Click the Add button to create SLA profiles.

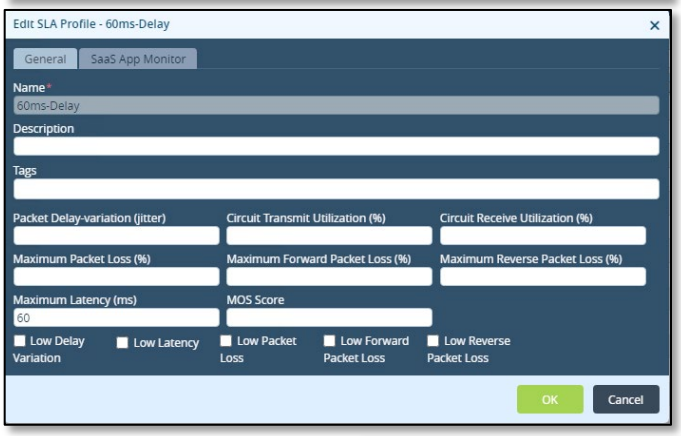


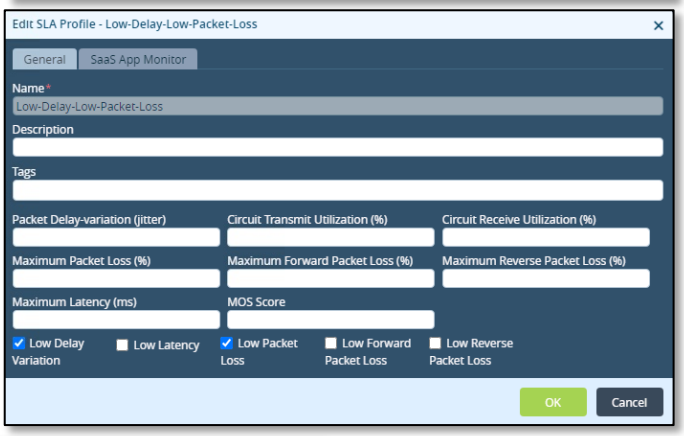


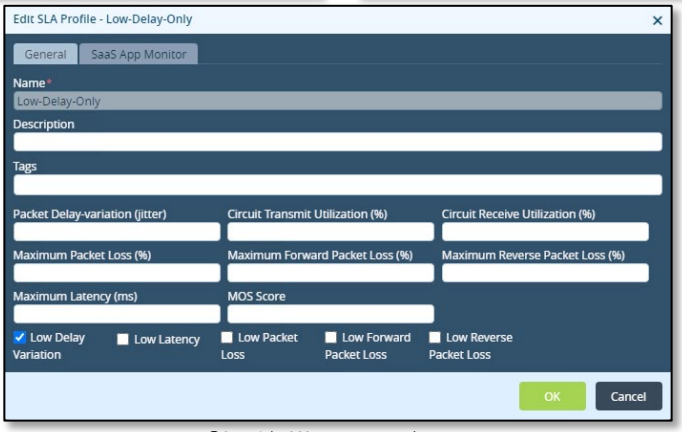




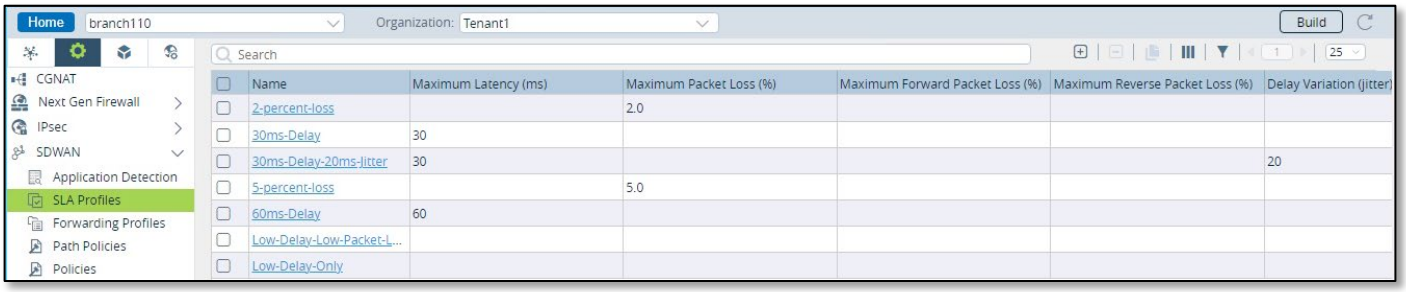






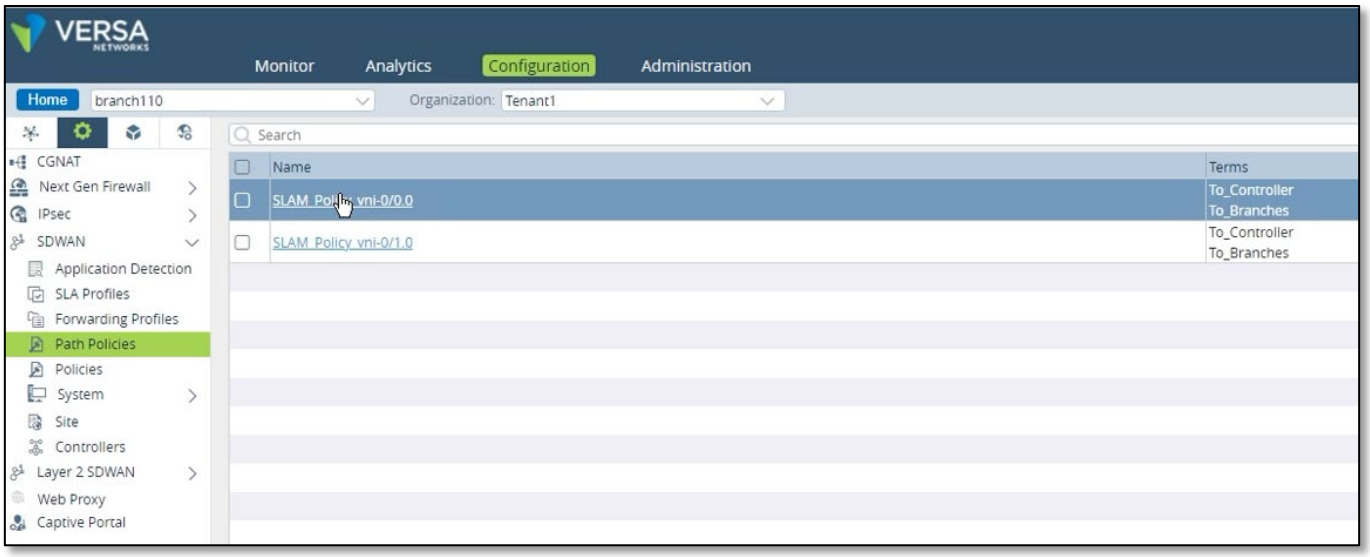


When finished, your SLA profiles should look similar to the result below.



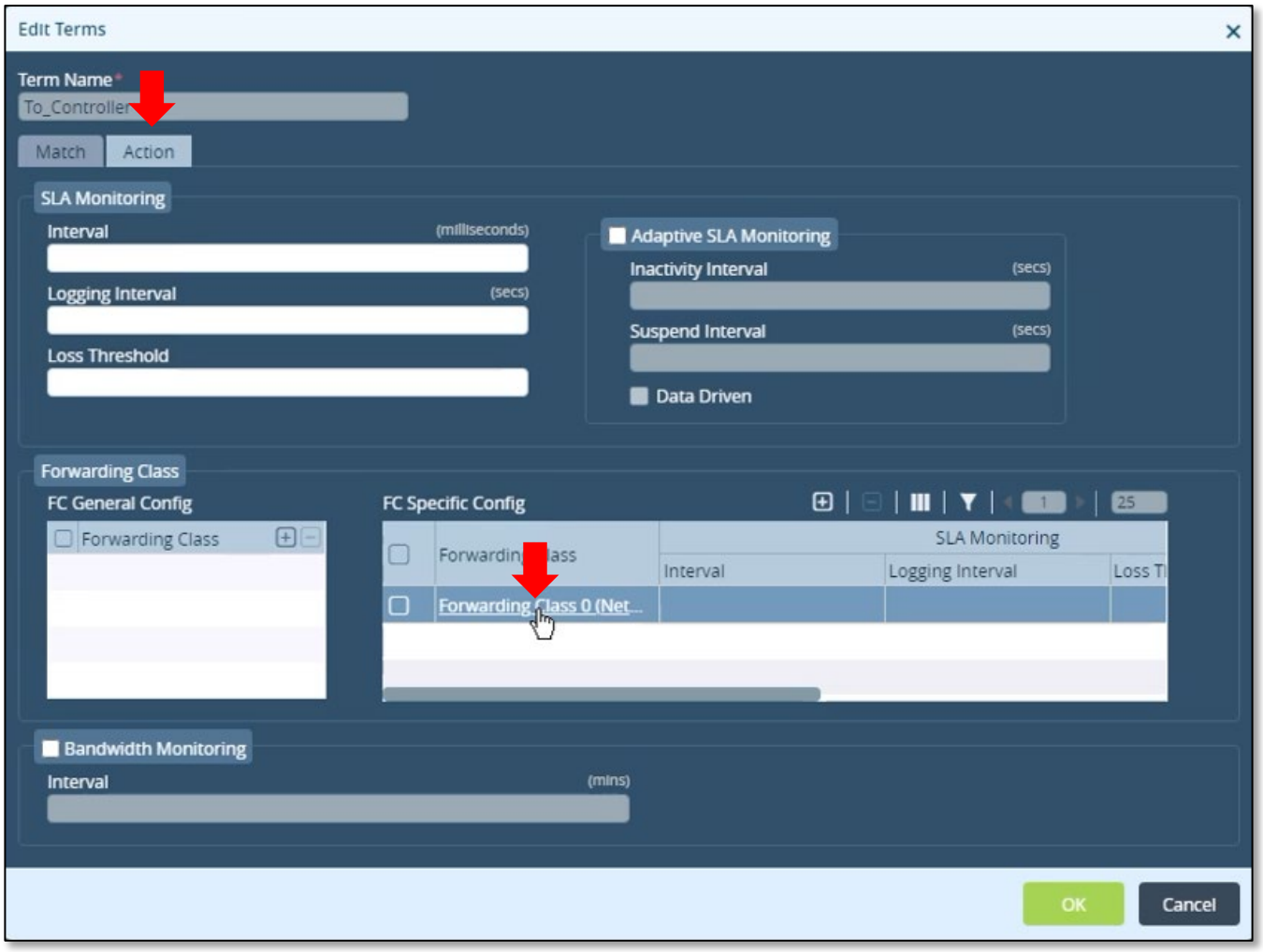
Next you will adjust the SLA probe frequency on your links. This is done with two steps. The first step is to modify the Path Policies. The path policies determine the properties of the SLA probe system. The second step is to ensure that the policies are applied to the interfaces. Because the default policies are already applied to the interfaces, you will only verify that the policies are applied.

Navigate to Configuration > Services > SD-WAN > Path Policies and locate the 2 default path policies. Click on the SLAM_Policy-vni-0/0.0 name to open the policy for editing.



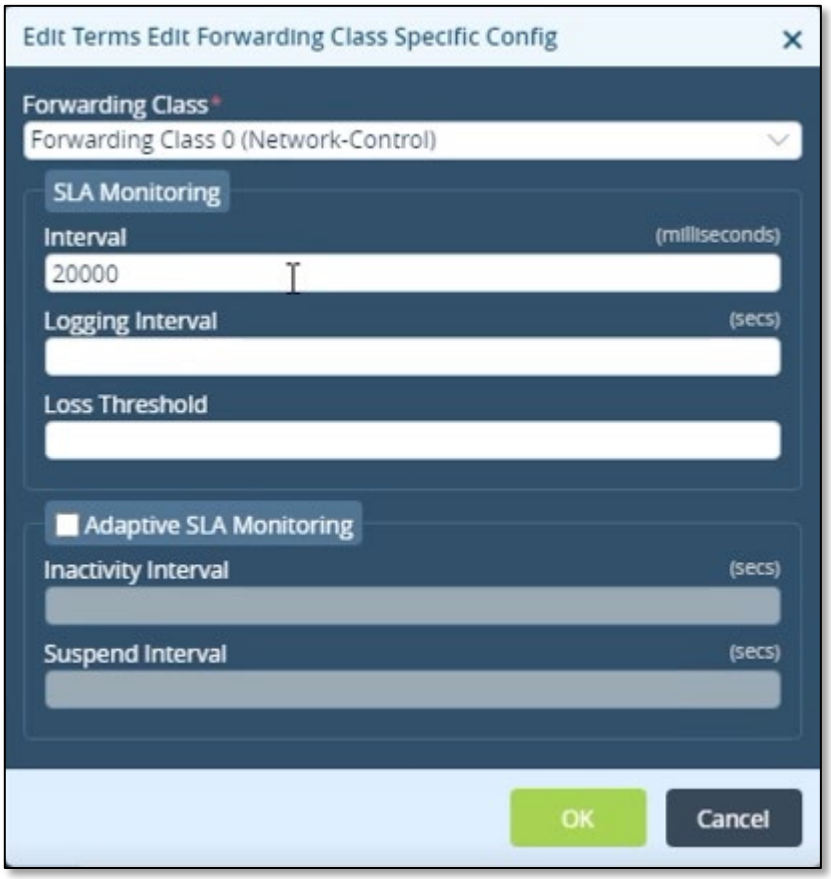
In the SLAM_Policy-vni-0/0.0, click the To_Controller term to open the term.

In the To_Controller term, select the Action tab and locate the forwarding class specific configuration. There should be a ForwardingClass 0 setting configured by default. Open the ForwardingClass 0 entry.



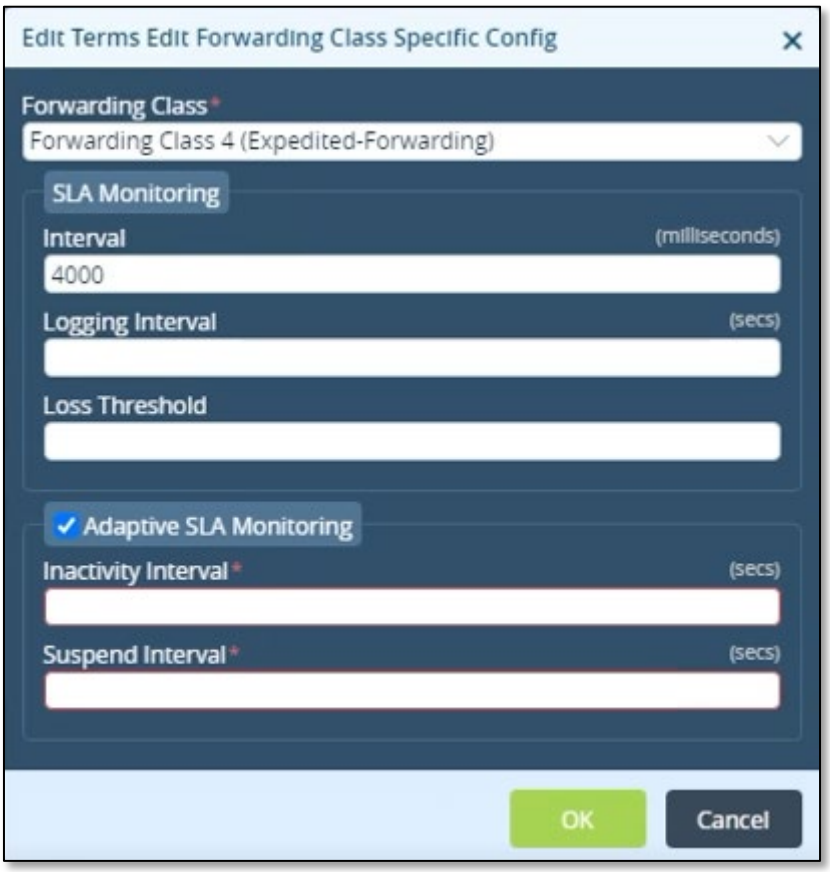
The default timers are built into the system, so they don't appear in the configuration explicitly. Modify the SLA Monitoring interval and set it to 20 seconds (20000ms).

Click OK to accept the new settings, then click OK in the Edit Terms window to finish editing the To_Controller term.

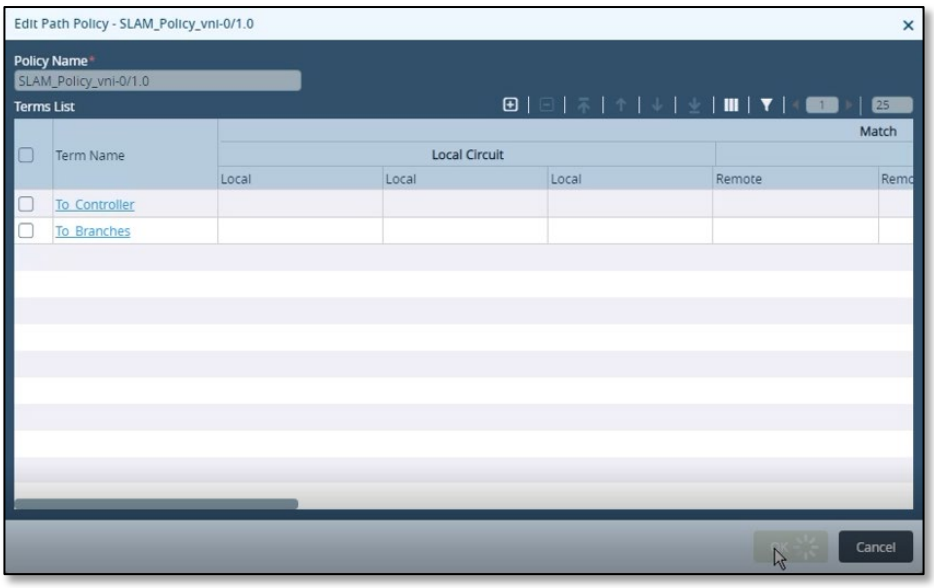


Click the To_Branches term to open and modify the term.

In the Action tab of the To_Branches term, select the Forwarding Class 4 SLA probe option and change the interval to 4 seconds (4000ms).



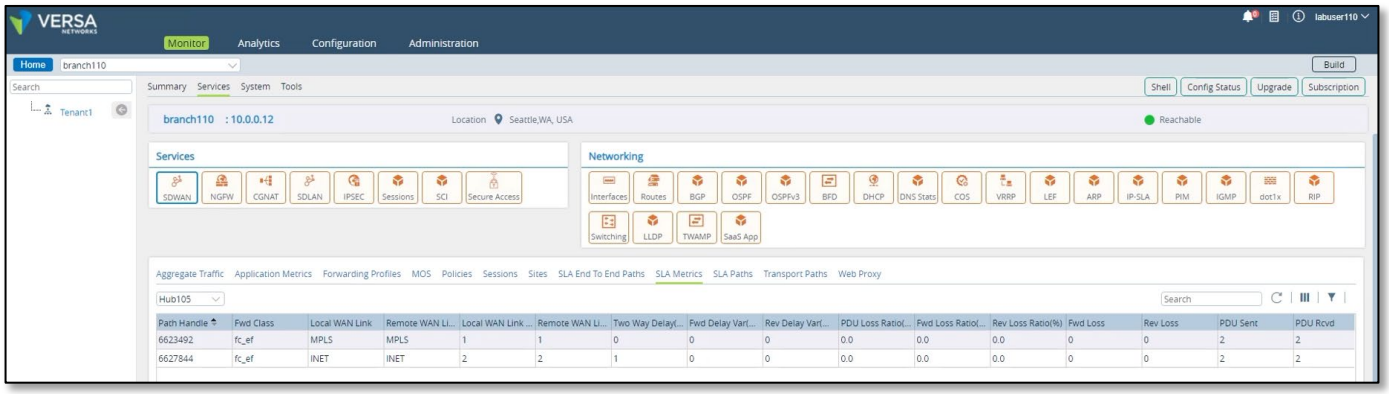
Click OK to accept the parameter change, then click OK in the Edit Terms dialog to finish editing the To_Branches term. Click OK on the Edit Path Policy dialog to apply the changes.



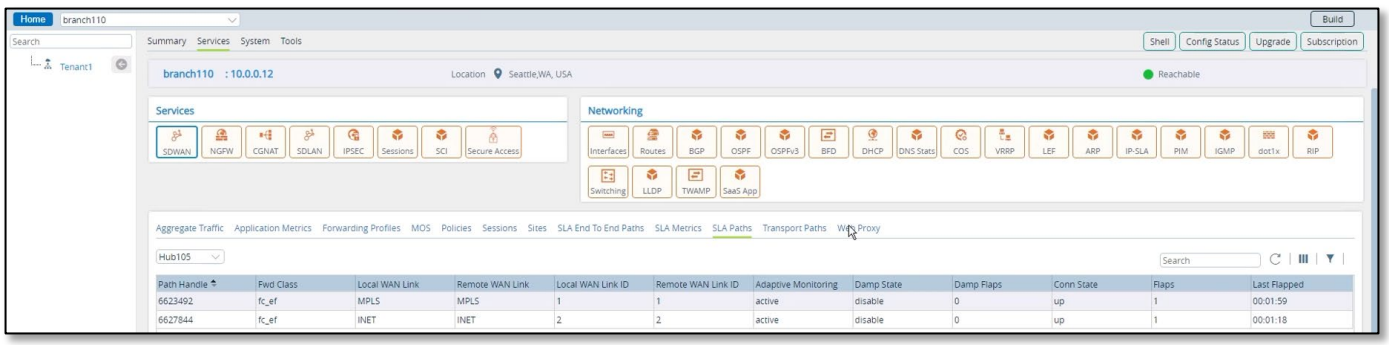
Exercise 3: Analyze and Verify SLA Probe Information

In the following lab exercise you will locate and analyze the SLA probe statistics in the Versa Director Monitor tab for your appliance.

In Versa Director, navigate to the Monitor tab of your device. In your device Monitor tab, navigate to ***Services > SDWAN > SLA Metrics***. Select the Hub105 device from the drop-down to view the SLA statistics between your branch device and the hub device.



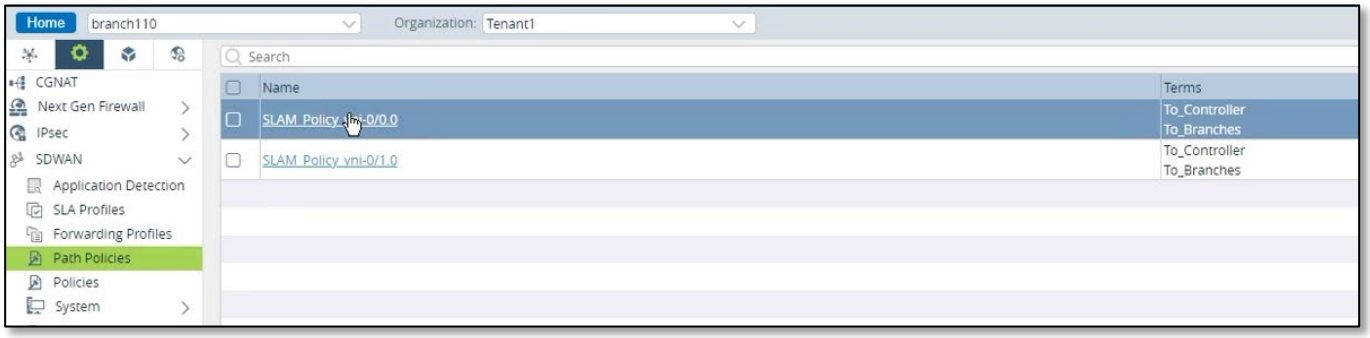
Select the SLA Paths tab to view the SLA probe status between sites. In the SLA Paths dialog, select the Hub105 site from the dropdown menu to view the SLA probe status between your branch and the hub device.



Note that the Adaptive Monitoring status should be active, meaning the probes are actively being sent between sites.

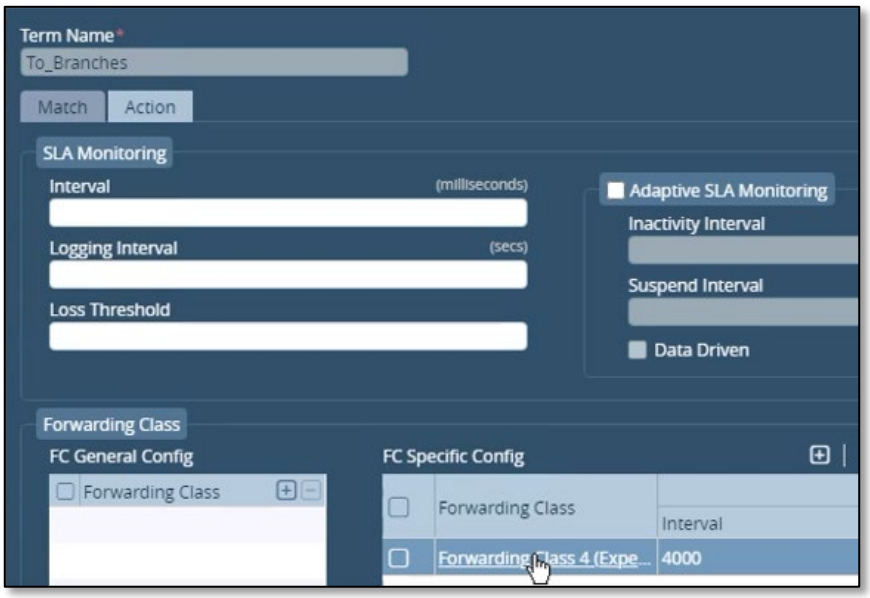
Return to the Configuration > Services > SDWAN > Path Policies hierarchy so that you can modify the adaptive SLA parameters on one of the WAN links.

In the Path Policies table, click the SLAM_Policy_vni-0/0.0 policy to open the policy for editing.

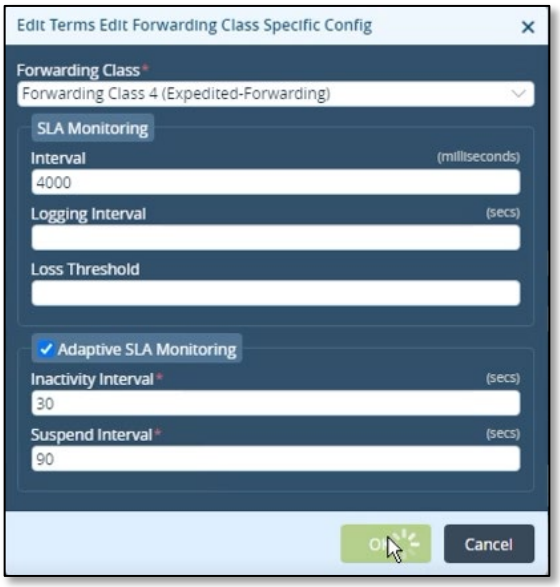


Open the To_Branches term.

Select the Action tab, then select the Forwarding Class 4 options.

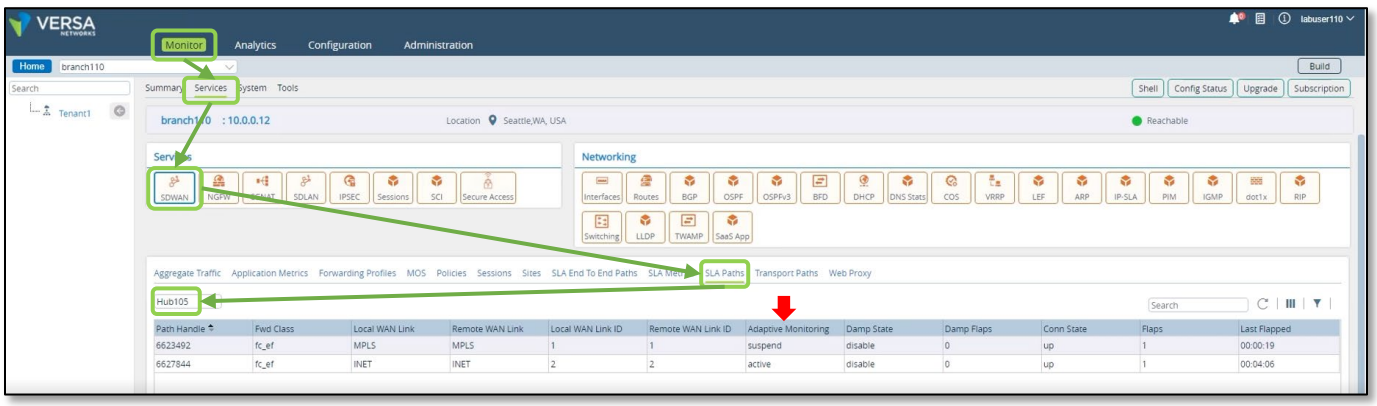


In the Forwarding Class 4 options, enable Adaptive SLA Monitoring and enter a 30 second interval and 90 second suspend interval.



Clock OK on the dialog boxes until you have finished applying the configuration changes.

Once you have applied the adaptive SLA monitoring parameters, return to the Monitor > Services > SDWAN > SLA Paths dialog to view the Adaptive Monitoring status.



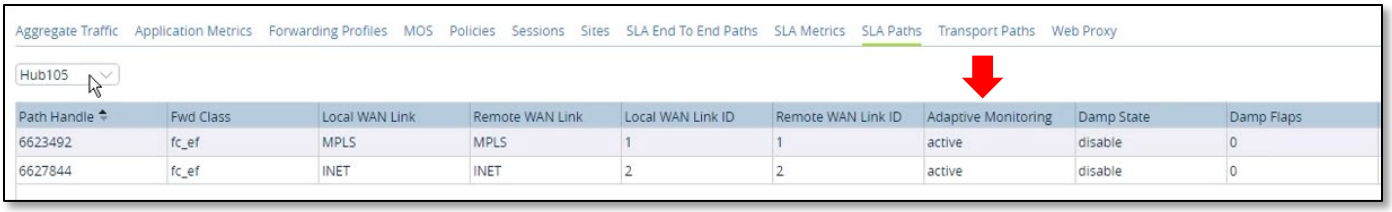
If the status for the MPLS circuit is NOT in suspend mode, wait 10 seconds and then refresh the window. If you refresh the window more than 2 times and the status does not change to suspend, verify that the Adaptive SLA configuration parameters are properly configured.

Open the MT-PuTTY application and start an SSH session to your testing host device (BR-110-PC, BR-111-PC, etc.)

From the command line on the testing PC, issue the **`ping 172.16.105.1 -c 5`** command to send 5 ICMP packets to the address 172.16.105.1 (the LAN gateway address on the hub site.

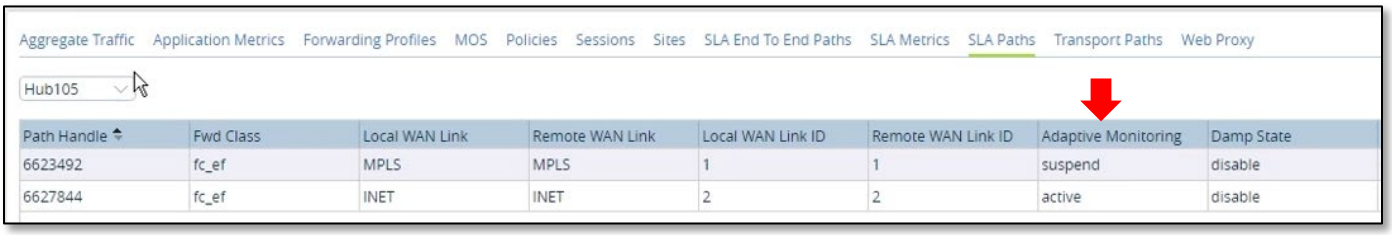
```
labuser@BR-110-PC:~$ ping 172.16.105.1 -c 5
PING 172.16.105.1 (172.16.105.1) 56(84) bytes of data.
64 bytes from 172.16.105.1: icmp_seq=1 ttl=63 time=2.08 ms
64 bytes from 172.16.105.1: icmp_seq=2 ttl=63 time=0.870 ms
64 bytes from 172.16.105.1: icmp_seq=3 ttl=63 time=1.65 ms
64 bytes from 172.16.105.1: icmp_seq=4 ttl=63 time=0.925 ms
64 bytes from 172.16.105.1: icmp_seq=5 ttl=63 time=1.10 ms

--- 172.16.105.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4032ms
rtt min/avg/max/mdev = 0.870/1.327/2.089/0.473 ms
labuser@BR-110-PC:~$
```

Return to the Versa Director SLA Paths monitoring window. Refresh the table by selecting a different site from the site dropdown menu, then select the Hub105 site again. The Adaptive Monitoring status should have changed to active because you sent data packets between the sites with the Ping utility.



Path Handle	Fwd Class	Local WAN Link	Remote WAN Link	Local WAN Link ID	Remote WAN Link ID	Adaptive Monitoring	Damp State	Damp Flaps
6623492	fc_ef	MPLS	MPLS	1	1	active	disable	0
6627844	fc_ef	INET	INET	2	2	active	disable	0

Wait 30 seconds, then refresh the table (select a different remote site, then select Hub105 again). The MPLS link Adaptive Monitoring status should return to suspend state.



Path Handle	Fwd Class	Local WAN Link	Remote WAN Link	Local WAN Link ID	Remote WAN Link ID	Adaptive Monitoring	Damp State
6623492	fc_ef	MPLS	MPLS	1	1	suspend	disable
6627844	fc_ef	INET	INET	2	2	active	disable

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