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.

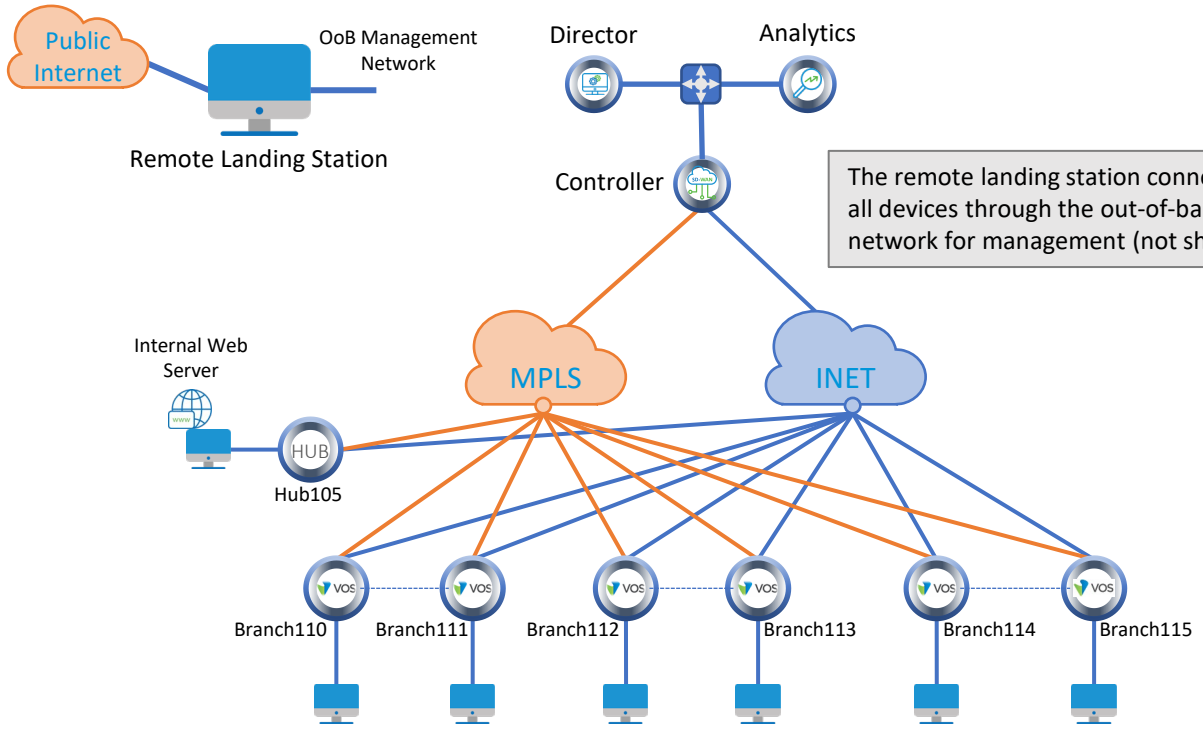
During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not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

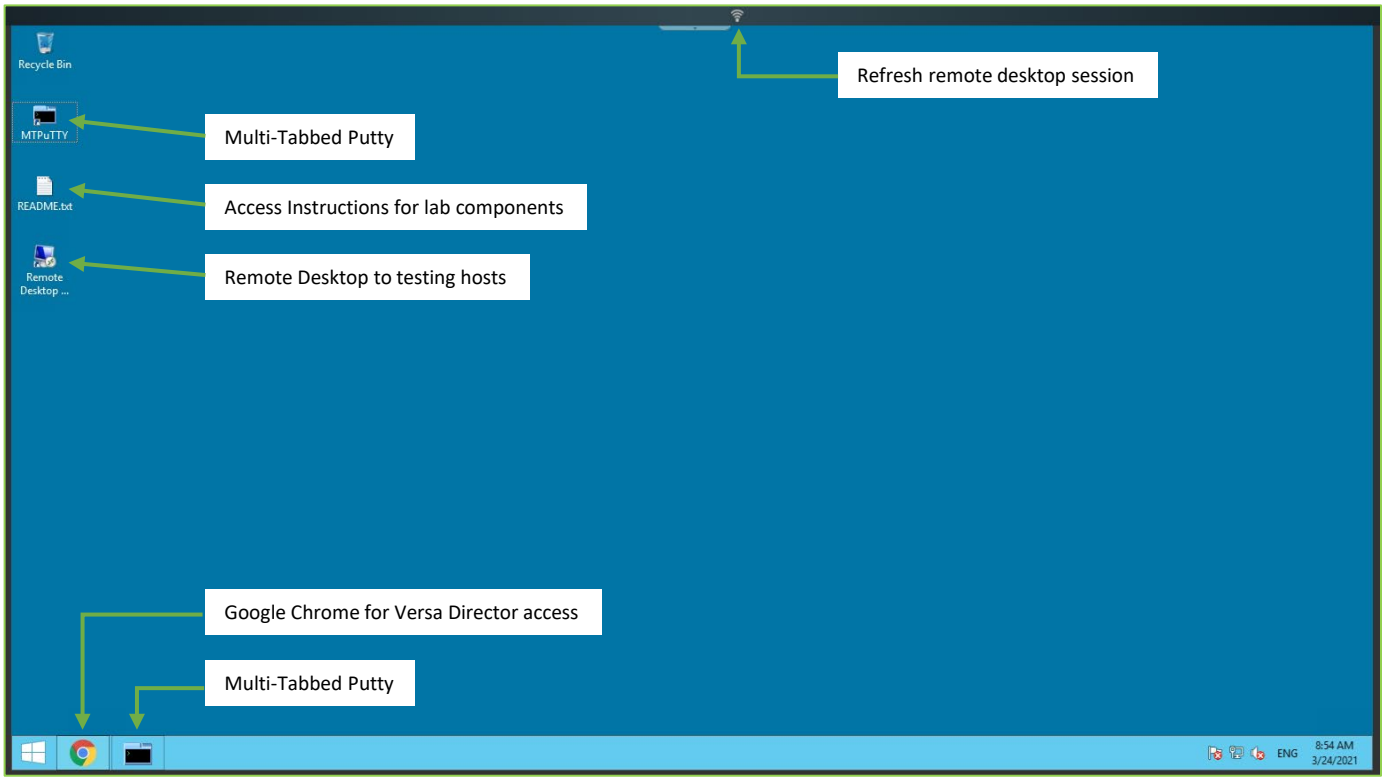
- Branch/Node/CPE Assignment
- Remote Lab Access

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

Exercise 2: Configure Traffic Steering (Application Steering)

In the following lab exercises, you will:

- Locate the SD-WAN Policy and Profile configuration settings
- Configure SD-WAN Forwarding Profiles
- Configure SD-WAN Policies
- Locate the SLA monitoring configuration settings
- Configure SLA profiles and assign them to SD-WAN Forwarding Ptofiles

> **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.

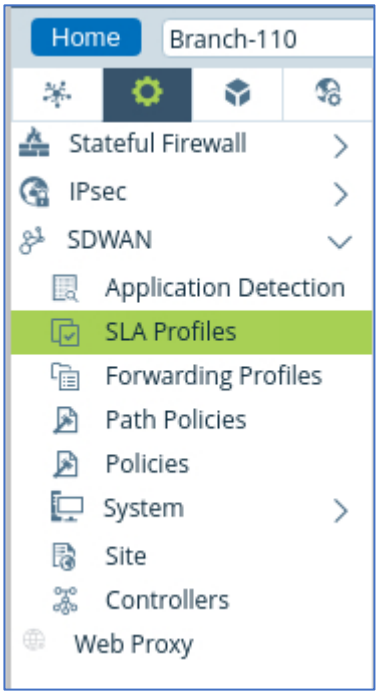
> **Note:** The images in this lab are for demonstration purposes only. Your lab experience may differ from the images provided in the lab guide.

In this lab part you will identify the configuration components required that will allow your device to assign preferred transport paths to traffic based on an SD-WAN Forwarding Profile. You will then configure SD-WAN policy rules to identify and map traffic to the SD-WAN Forwarding Profiles.

The main configuration components related to SD-WAN policy and steering are located in the *Services > SDWAN* hierarchy of the configuration.

Navigate to *Administration > Appliances* and locate your appliance in the appliance list. Click your appliance name to open the Appliance Context mode of your device. From the Appliance Context mode of your device, click the *Configuration* tab to open the configuration of your device.

Navigate to the *Services > SDWAN* hierarchy of the configuration and select SLA Profiles.



The first step is define the SLA profiles that will compare the user-defined parameters with the statistics that are being gathered from the transport paths. You will create 3 SLA profiles:

- SLA-Voice
- SLA-Business
- SLA-Best-Effort

The parameters for the profiles are:

- SLA-Voice will examine the jitter, latency, and packet loss of links:
    - Jitter: 10ms
    - Latency: 50ms
    - Packet Loss: 3%

- SLA-Business will examine packet loss:
    - Packet Loss: 2%

- SLA-Best-Effort will examine latency and packet loss:
    - Latency: 100ms
    - Packet Loss: 5%

Name	Maximum Latency (ms)	Maximum Packet Loss (%)	Maximum Forward Packet Loss (%)	Maximum Reverse Packet Loss (%)	Delay Variation (jitter)
SLA-Best-Effort	100	5.0			
SLA-Business		2.0			
SLA-Voice	50	3.0			10

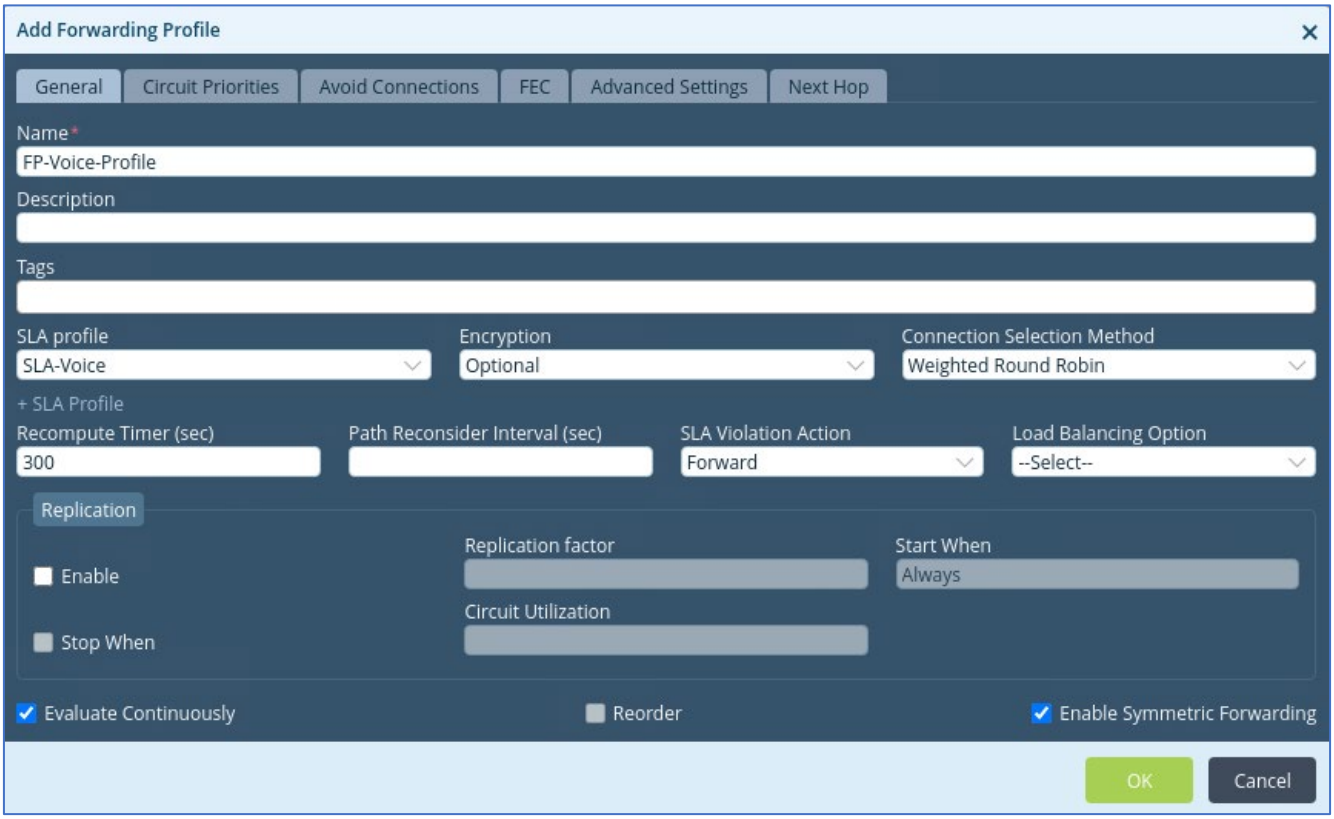
The second step is define the Forwarding Profiles that determine how traffic will be treated. You will configure 3 traffic profiles:

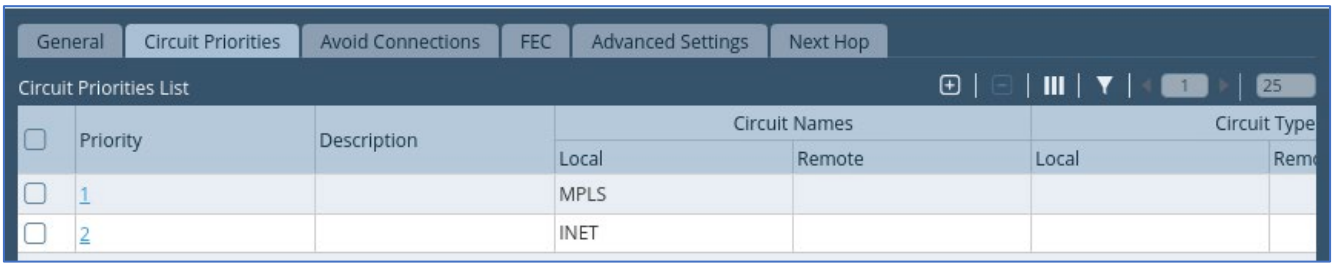
- FP-Voice-Traffic
- FP-Business-Traffic
- FP-Best-Effort

The parameters for the profiles are:

- FP-Voice-Traffic: This profile will utilize the MPLS link as a primary link, and the INET link as a secondary link. If no links are in-profile then this forwarding profile will continue to forward traffic. This profile will use the SLA-Voice SLA profile to determine whether transport paths are in-profile for this type of traffic.
- FP-Business-Traffic: This profile will utilize the MPLS link and INET link equally. If no links are in-profile then this forwarding profile will continue to forward traffic. This profile will use the SLA-Business SLA profile to determine whether transport paths are in-profile for this type of traffic. This Forwarding Profile will enable packet replication when the links are out of profile, and will stop replication when the link utilization reaches 85%.
- FP-Best-Effort: This profile will utilize the INET link as the primary link and will not use the MPLS link. When the link is out of profile, this forwarding profile will drop the traffic. This profile will use the SLA-Best-Effort SLA profile to determine whether transport paths are in-profile for this type of traffic.

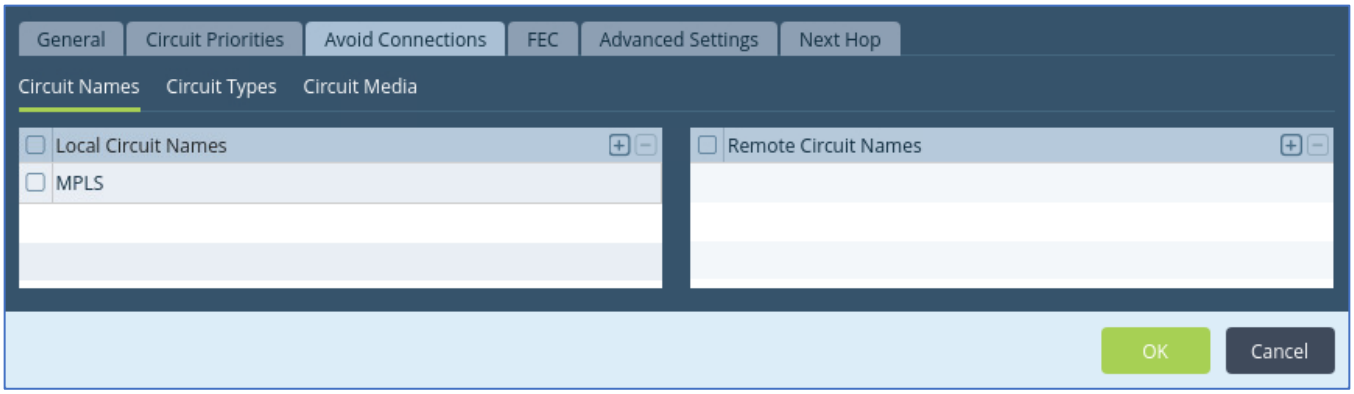
Begin by creating the FP-Voice-Traffic Forwarding Profile. The SLA profile is SLA-Voice, and the SLA Violation Action is Forward.





Next create the FP-Business-Traffic Forwarding Profile. The SLA profile is SLA-Business, and the SLA Violation Action is Forward.

Finally, create the FP-Best-Effort Forwarding Profile. The SLA profile is SLA-Best-Effort, and the SLA Violation Action is Drop. This profile should never use the MPLS circuit.



You have defined the SLA parameters you want to track, and you have defined the forwarding profiles that assign traffic to transport paths based on their priority and SLA status. The final step is to identify traffic that you want to send to the traffic profiles by using an SD-WAN Policy.

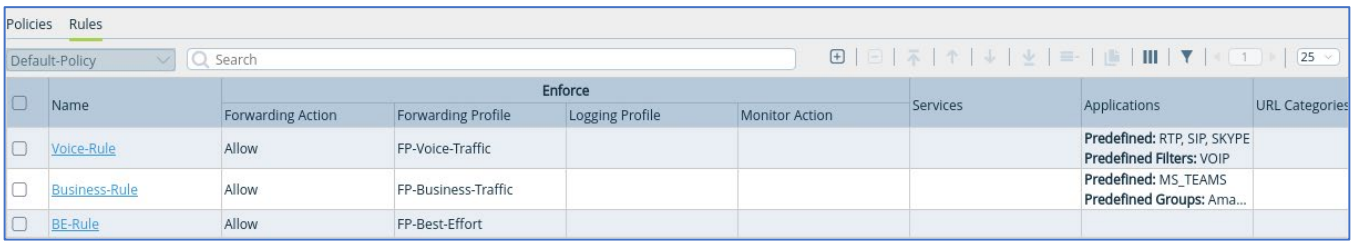
Select *Policies* from the *Services > SDWAN* configuration hierarchy. There should be a pre-configured Default-Policy policy. You will add rules to the default policy.

Rule Description:

Voice-Rule: Identify VOIP, SIP, RTP, SKYPE traffic sourced from the zone associated with the local LAN interface. Direct matching traffic to the FP-Voice-Traffic forwarding profile.

Business-Rule: Identify Microsoft Teams, Salesforce-Apps, and Amazon-Apps traffic sourced from the zone associated with the local LAN interface. Direct matching traffic to the FP-Business-Traffic forwarding profile.

BE-Rule: Direct all other traffic from the zone associated with the local LAN interface to the FP-Best-Effort forwarding profile.



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