

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.

In this lab, you will be assigned a student ID (Student01, Student02, etc.) Each student environment is a tenant on Versa Director and has access to 2 VOS devices and a shared hub. You will perform your operations on the VOS devices.

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. Versa Director is also reachable from the remote desktop at IP address 10.27.1.10 in the remote desktop web browser.

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!

Step 1. Examine the Class of Service Hierarchy

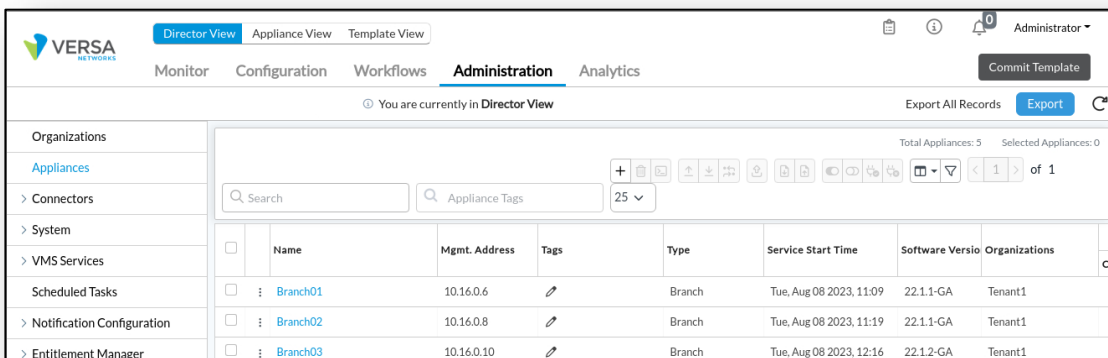
In the following lab exercises, you will:

- Locate the Class of Service configuration parameters
- Identify the components required to implement class of service
- Identify the components that are optional to implement class of service

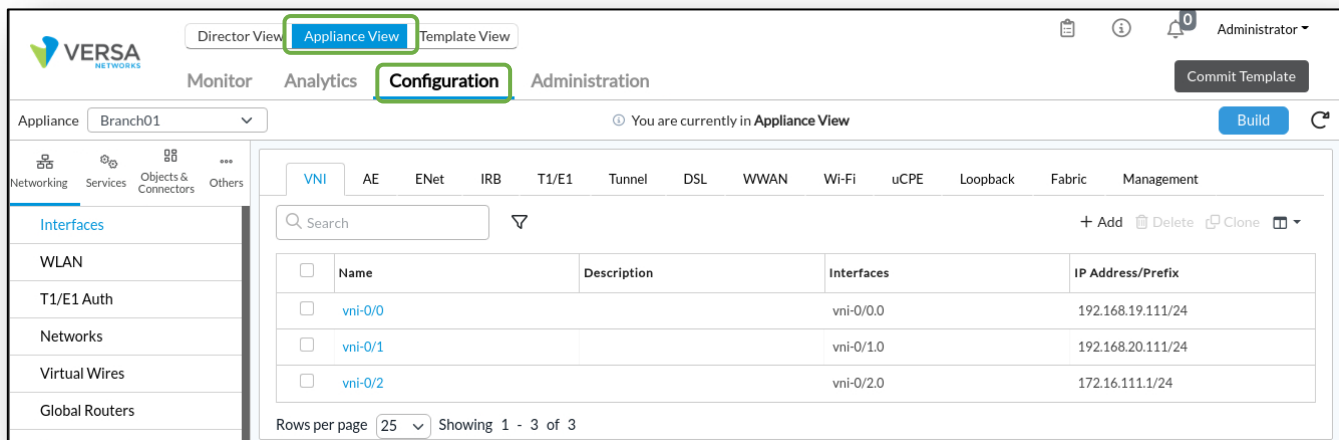
Note: Configuration modifications in this lab will be performed in Appliance Context mode (directly on your device) and will not be performed through device templates.

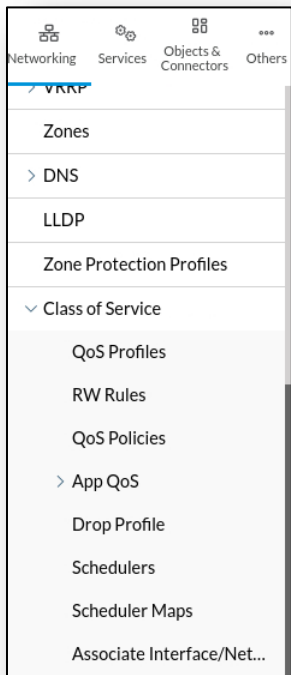
Note: The images in this lab are for demonstration purposes only. Your lab experience may differ from the images provided in the lab guide.

- Open Versa Director on the remote desktop and log in with your assigned student ID.
- From Versa Director, navigate to *Administration* > *Appliances* to display the deployed devices.
- Locate your *SxxB01* device in the list and click on the link to your device. This will open the Appliance Context of your device so that changes that are made take effect immediately on your appliance.



- From the *Appliance View* of your device, select the *Configuration* tab to access the device-specific configuration.





The Class of Service configuration components are located in the Networking tab of the configuration dashboard. Ensure that the Networking tab is selected, locate the Class of Service components, and expand the Class of Service configuration. You may have to scroll down on the networking pane to view the Class of Service configuration section.

The following components are **REQUIRED** for a Class of Service configuration:

- QoS Profile
- Policy (QoS or AppQoS)
- Scheduler
- Scheduler Maps
- Associate Interface

The following components are **OPTIONAL** for a Class of Service configuration:

- RW Rules
- Drop Profile

Step 2. QoS Profiles

A QoS Profile defines how traffic will be treated that is mapped to that profile. A QoS or AppQoS policy uses the QoS Profile as an enforce action for matching traffic, and therefore the QoS profile must be created before the policy.

2.a. In this lab part you will create the following QoS profiles:

- Common-Internet
- Drop-Sensitive-Apps
- External-Business-Apps
- Internal-Business-Apps
- Internet-Streaming
- Realtime-Critical
- Realtime-Non-Critical

The parameters for each profile are shown below. Samples of the GUI dialogs are on the following pages.

<p>QoS Profile name: Common-Internet</p> <ul style="list-style-type: none"> • Peak Rate (Kbps): 2000 • Forwarding Class: 12 • Loss Priority: High 	<p>QoS Profile name: Drop-Sensitive-Apps</p> <ul style="list-style-type: none"> • Forwarding Class: 10 • Loss Priority: Low
<p>QoS Profile name: External-Business-Apps</p> <ul style="list-style-type: none"> • Peak Rate (Kbps): 10000 • Forwarding Class: 9 • Loss Priority: Low 	<p>QoS Profile name: Internal-Business-Apps</p> <ul style="list-style-type: none"> • Peak Rate (Kbps): 10000 • Forwarding Class: 8 • Loss Priority: Low
<p>QoS Profile name: Internet-Streaming</p> <ul style="list-style-type: none"> • Peak Rate (Kbps): 2000 • Forwarding Class: 13 • Loss Priority: Low 	<p>QoS Profile name: Realtime-Critical</p> <ul style="list-style-type: none"> • Forwarding Class: 4 • Loss Priority: Low
<p>QoS Profile name: Realtime-Non-Critical</p> <ul style="list-style-type: none"> • Peak Rate (Kbps): 5000 • Forwarding Class: 4 • Loss Priority: High 	

Edit QoS Profile - Common-Internet

Name *
Common-Internet

Description

Ingress Policing

Peak Rate (pps) 1..4294967295 Peak Rate (Kbps) 2000

Peak Burst Size (Bytes) 128..4294967295

Forwarding Class Per User Policer

Forwarding Class * Forwarding Class 12 (Best-Effort) Loss Priority * High

DSCP Rewrite dot1p Rewrite

OK Cancel

Edit QoS Profile - Drop-Sensitive-Apps

Name *
Drop-Sensitive-Apps

Description

Ingress Policing

Peak Rate (pps) 1..4294967295 Peak Rate (Kbps) 64..4294967295

Peak Burst Size (Bytes) 128..4294967295

Forwarding Class Per User Policer

Forwarding Class * Forwarding Class 10 Loss Priority * Low

DSCP Rewrite dot1p Rewrite

OK Cancel

Edit QoS Profile - External-Business-Apps

Name *
External-Business-Apps

Description

Ingress Policing

Peak Rate (pps) 1..4294967295 Peak Rate (Kbps) 10000

Peak Burst Size (Bytes) 128..4294967295

Forwarding Class Per User Policer

Forwarding Class * Forwarding Class 9 Loss Priority * Low

DSCP Rewrite dot1p Rewrite

OK Cancel

Edit QoS Profile - Internal-Business-Apps

Name *
Internal-Business-Apps

Description

Ingress Policing

Peak Rate (pps) 1..4294967295 Peak Rate (Kbps) 10000

Peak Burst Size (Bytes) 128..4294967295

Forwarding Class Per User Policer

Forwarding Class * Forwarding Class 8 (Assured-Forwarddir) Loss Priority * Low

DSCP Rewrite dot1p Rewrite

OK Cancel

Edit QoS Profile - Internet-Streaming

Name *
Internet-Streaming

Description

Ingress Policing

Peak Rate (pps)	Peak Rate (Kbps)
1 .. 4294967295	2000
Peak Burst Size (Bytes)	
128 .. 4294967295	

Forwarding Class Per User Policer

Forwarding Class *
Forwarding Class 13

Loss Priority *
Low

DSCP Rewrite dot1p Rewrite

OK Cancel

Edit QoS Profile - Realtime-Critical

Name *
Realtime-Critical

Description

Ingress Policing

Peak Rate (pps)	Peak Rate (Kbps)
1 .. 4294967295	64 .. 4294967295
Peak Burst Size (Bytes)	
128 .. 4294967295	

Forwarding Class Per User Policer

Forwarding Class *
Forwarding Class 4 (Expedited-Forwarc

Loss Priority *
Low

DSCP Rewrite dot1p Rewrite

OK Cancel

Edit QoS Profile - Realtime-Non-Critical

Name *
Realtime-Non-Critical

Description

Ingress Policing

Peak Rate (pps)	Peak Rate (Kbps)
1 .. 4294967295	5000
Peak Burst Size (Bytes)	
128 .. 4294967295	

Forwarding Class Per User Policer

Forwarding Class *
Forwarding Class 4 (Expedited-Forwarc

Loss Priority *
High

DSCP Rewrite dot1p Rewrite

OK Cancel

When finished, your configuration should resemble the example below.

<input type="checkbox"/>	Name	Peak Rate (pps)	Peak Rate (Kbps)	Peak Burst Size (Byt	Forwarding Class	Loss Priority	DSCP Rewrite	dot1p Rewrite
<input type="checkbox"/>	: Common-Internet		2000		Forwarding Class 12 (B...	high	Yes	No
<input type="checkbox"/>	: Drop-Sensitive-Apps				Forwarding Class 10	low	Yes	No
<input type="checkbox"/>	: External-Business-Apps		10000		Forwarding Class 9	low	Yes	No
<input type="checkbox"/>	: Internal-Business-Apps		10000		Forwarding Class 8 (As...	low	Yes	No
<input type="checkbox"/>	: Internet-Streaming		2000		Forwarding Class 13	low	Yes	No
<input type="checkbox"/>	: Realtime-Critical				Forwarding Class 4 (Ex...	low	Yes	No
<input checked="" type="checkbox"/>	: Realtime-Non-Critical		5000		Forwarding Class 4 (Ex...	high	Yes	No

Rows per page Showing 1 - 7 of 7

Step 3. AppQoS Policy and Rules

You have created the profiles that associate traffic to input rates (inbound policing) and forwarding classes (which are associated with outbound queues). Next you will create policy rules to identify traffic and direct the traffic to the corresponding QoS profile. To perform this task you will create App QoS policy rules so that you can take advantage of the application identification capabilities of Versa Operating System.

3.a. Expand the *App QoS* configuration hierarchy and select *Policies* from the *App QoS* dropdown.

There should be a pre-created *Default-Policy* that does not have any rules.

3.b. Ensure that the *Rules* tab is open and add the following rules to the policy. The rule parameters are shown below.

General Tab

- Rule Name: Find-Real-time-Critical

Source Tab

- Source Zone: Intf-Student_LAN-Zone

Applications/URL Tab:

- Application List:
 - MS_TEAMS
 - RTP
 - SIP
 - SIP_SOAP

Enforce Tab

- Action: Allow
- QoS Profile Setting: Realtime-Critical

General Tab

- Rule Name: Find-Real-time-Non-Critical

Source Tab

- Source Zone: Intf-Student_LAN-Zone

Applications/URL Tab:

- Application List:
 - FACEBOOK_AUDIO
 - FACEBOOK_MESSENGER
 - FACEBOOK_VIDEO
 - SKYPE

Enforce Tab

- Action: Allow
- QoS Profile Setting: Realtime-Non-Critical

General Tab

- Rule Name: Find-Internal-Business-Apps

Source Tab

- Source Zone: Intf-Student_LAN-Zone

Destination Tab:

- Destination Site Name: Hub_New

Headers/Schedule Tab

- Services: http; https

Enforce Tab

- Action: Allow
- QoS Profile Setting: Internal-Business-Apps

General Tab

- Rule Name: Find-External-Business-Apps

Source Tab

- Source Zone: Intf-Student_LAN-Zone

Destination Tab:

- Destination Zone: Intf-INET-Zone

Applications/URL Tab

- Application List:
 - Amazon-Apps
 - Google-Apps

Enforce Tab

- Action: Allow
- QoS Profile Setting: External-Business-Apps

General Tab

- Rule Name: Drop-Sensitive-Apps

Source Tab

- Source Zone: Intf-Student_LAN-Zone

Applications/URL Tab

- Application List
 - AMAZON_CLOUD_DRIVE

Enforce Tab

- Action: Allow
- QoS Profile Setting: Drop-Sensitive-Apps

General Tab

- Rule Name: Common-Internet

Source Tab

- Source Zone: Intf-Student_LAN-Zone

Destination Tab:

- Destination Site Name: Intf-INET-Zone

Enforce Tab

- Action: Allow
- QoS Profile Setting: Common-Internet

General Tab

- Rule Name: Internet-Streaming

Source Tab

- Source Zone: Intf-Student_LAN-Zone

Destination Tab

- Destination Zone: Intf-INET-Zone

Applications/URL Tab

- Applications:
 - PANDORA
 - SPOTIFY
 - YOUTUBE
- URL Categories:
 - music
 - streaming_media

Enforce Tab

- Action: Allow
- QoS Profile Setting: Internet-Streaming

RULE 1: FIND-REAL-TIME-CRITICAL

Edit App QoS Rule - Find-Real-time-Critical

General Source Destination Headers/Schedule Applications/URL Enforce

Name *
Find-Real-time-Critical

Description Tags

Session Timeout (secs) TCP Keep Alive --Select--

Disable Rule

OK Cancel

Add App QoS Rule

General Source Destination Headers/Schedule Applications/URL Users/Groups Enforce

Source Zone + New
 Intf-Student_LAN-Zone

Source Address + New Address + New Address
Source Address Not Configured

Source Site Name + +
Source Site Name Not Configured

Source Address Negate

Region Region Not Configured State State Not Configured

City City Not Configured

OK Cancel

Edit App QoS Rule - Find-Real-time-Critical

General Source Destination Headers/Schedule Applications/URL Enforce

Applications

Application List + New Application + New Filter + New Group +

MS_TEAMS
 RTP
 SIP
 SIP_SOAP

URL Categories

URL Category List + New URL Category +
URL Category List Not Configured

OK Cancel

Edit App QoS Rule - Find-Real-time-Critical

General Source Destination Headers/Schedule Applications/URL Enforce

Action Setting
 Allow

QoS Profile Setting
QoS Profile *
Realtime-Critical
View QoS Profile

OK Cancel

RULE 2: FIND-REAL-TIME-NON-CRITICAL

Edit App QoS Rule - Find-Real-time-Non-Critical

General Source Destination Headers/Schedule Applications/URL Enforce

Name
Find-Real-time-Non-Critical

Description

Tags

Session Timeout (secs)

TCP Keep Alive
--Select--

Disable Rule

OK Cancel

Add App QoS Rule

General Source Destination Headers/Schedule Applications/URL Users/Groups Enforce

Source Zone
Intf-Student_LAN-Zone

Source Address
Source Address Not Configured

Source Site Name
Source Site Name Not Configured

Source Address Negate

Region
Region Not Configured

State
State Not Configured

City
City Not Configured

OK Cancel

Edit App QoS Rule - Find-Real-time-Non-Critical

General Source Destination Headers/Schedule Applications/URL Enforce

Applications

- Application List
- FACEBOOK_AUDIO
- FACEBOOK_MESSENGER
- FACEBOOK_VIDEO
- SKYPE

URL Categories

- URL Category List

OK Cancel

Edit App QoS Rule - Find-Real-time-Non-Critical

General Source Destination Headers/Schedule Applications/URL Enforce

Action Setting
 Allow

QoS Profile Setting
QoS Profile
Realtime-Non-Critical

View QoS Profile

OK Cancel

RULE 3: FIND-INTERNAL-BUSINESS-APPS

Edit App QoS Rule - Find-Internal-Business-Apps

General Source Destination Headers/Schedule Applications/URL Enforce

Name: Find-Internal-Business-Apps

Description:

Tags:

Session Timeout (secs):

TCP Keep Alive: --Select--

Disable Rule

OK Cancel

Add App QoS Rule

General Source Destination Headers/Schedule Applications/URL Users/Groups Enforce

Source Zone: Intf-Student_LAN-Zone

Source Address: Source Address Not Configured

Source Site Name: Source Site Name Not Configured

Source Address Negate:

Region: Region Not Configured

State: State Not Configured

City: City Not Configured

OK Cancel

Add App QoS Rule

General Source Destination Headers/Schedule Applications/URL Users/Groups Enforce

Destination Zone: Destination Zone Not Configured

Destination Address: Destination Address Not Configured

Destination Site Name: SP-HUB-New

Destination Address Negate:

Region: Region Not Configured

State: State Not Configured

City: City Not Configured

OK Cancel

Add App QoS Rule

General Source Destination Headers/Schedule Applications/URL Users/Groups Enforce

IP Version: --Select--

IP Flags: --Select--

DSCP:

TTL Condition: Greater than or equal to

TTL Value: 1.255

Others Schedules: --Select--

Services: https, http

OK Cancel

RULE 4: FIND-EXTERNAL-BUSINESS-APPS

Edit App QoS Rule - Find-External-Business-Apps

General Source Destination Headers/Schedule Applications/URL Enforce

Name *
Find-External-Business-Apps

Description Tags

Session Timeout (secs) TCP Keep Alive --Select--

Disable Rule

OK Cancel

Add App QoS Rule

General Source Destination Headers/Schedule Applications/URL Users/Groups Enforce

Source Zone Source Address
Intf-Student_LAN-Zone Source Address Not Configured

Source Site Name
Source Site Name Not Configured

Source Address Negate

Region State
Region Not Configured State Not Configured

City
City Not Configured

OK Cancel

Edit App QoS Rule - Find-External-Business-Apps

General Source Destination Headers/Schedule Applications/URL Enforce

Destination Zone Intf-INET-Zone

Destination Address
Destination Address Not Configured

Destination Site Name Custom Geo Circle
Destination Site Name Not Configured Custom Geo Circle Not Configured

Region State City
Region Not Configured State Not Configured City Not Configured

Destination Address Negate Destination Location Negate

OK Cancel

Edit App QoS Rule - Find-External-Business-Apps

General Source Destination Headers/Schedule Applications/URL Enforce

Applications
 Application List
Amazon-Apps
Google-Apps

URL Categories
 URL Category List
URL Category List Not Configured

OK Cancel

Edit App QoS Rule - Find-External-Business-Apps

General Source Destination Headers/Schedule Applications/URL Enforce

Action Setting
 Allow

QoS Profile Setting
QoS Profile *
External-Business-Apps
View QoS Profile

OK Cancel

RULE 5: DROP-SENSITIVE-APPS

Edit App QoS Rule - Drop-Sensitive-Apps

General Source Destination Headers/Schedule Applications/URL Enforce

Name: Drop-Sensitive-Apps

Description: [Empty]

Tags: [Empty]

Session Timeout (secs): [Empty]

TCP Keep Alive: --Select--

Disable Rule

OK Cancel

Add App QoS Rule

General Source Destination Headers/Schedule Applications/URL Users/Groups Enforce

Source Zone: [Empty]

Intf-Student_LAN-Zone

Source Address: [Empty]

Source Site Name: [Empty]

Source Address Negate

Region: [Empty]

State: [Empty]

City: [Empty]

OK Cancel

Edit App QoS Rule - Drop-Sensitive-Apps

General Source Destination Headers/Schedule Applications/URL Enforce

Applications

- Application List
- AMAZON_CLOUD_DRIVE

URL Categories

- URL Category List

OK Cancel

Edit App QoS Rule - Drop-Sensitive-Apps

General Source Destination Headers/Schedule Applications/URL Enforce

Action Setting: Allow

QoS Profile Setting: Drop-Sensitive-Apps

OK Cancel

RULE 6: INTERNET-STREAMING

Edit App QoS Rule - Internet-Streaming

General Source Destination Headers/Schedule Applications/URL Enforce

Name *
Internet-Streaming

Description
[Text Field]

Tags
[Text Field]

Session Timeout (secs)
[Text Field]

TCP Keep Alive
--Select--

Disable Rule

OK Cancel

Add App QoS Rule

General Source Destination Headers/Schedule Applications/URL Users/Groups Enforce

Source Zone
Intf-Student_LAN-Zone

Source Address
Source Address Not Configured

Source Site Name
Source Site Name Not Configured

Source Address Negate

Region
Region Not Configured

State
State Not Configured

City
City Not Configured

OK Cancel

Edit App QoS Rule - Internet-Streaming

General Source Destination Headers/Schedule Applications/URL Enforce

Destination Zone
Intf-INET-Zone

Destination Address
Destination Address Not Configured

Destination Site Name
Destination Site Name Not Configured

Custom Geo Circle
Custom Geo Circle Not Configured

Region
Region Not Configured

State
State Not Configured

City
City Not Configured

Destination Address Negate

Destination Location Negate

OK Cancel

Edit App QoS Rule - Internet-Streaming

General Source Destination Headers/Schedule Applications/URL Enforce

Applications

Application List
PANDORA
SPOTIFY
YOUTUBE

URL Categories

URL Category List
music
streaming_media

OK Cancel

Edit App QoS Rule - Internet-Streaming

General Source Destination Headers/Schedule Applications/URL Enforce

Action Setting
 Allow

QoS Profile Setting
QoS Profile *
Internet-Streaming
View QoS Profile

OK Cancel

RULE 7: COMMON-INTERNET

Edit App QoS Rule - Common-Internet

General Source Destination Headers/Schedule Applications/URL Enforce

Name: Common-Internet

Description: [Empty]

Tags: [Empty]

Session Timeout (secs): [Empty]

TCP Keep Alive: --Select--

Disable Rule

OK Cancel

Add App QoS Rule

General Source Destination Headers/Schedule Applications/URL Users/Groups Enforce

Source Zone: Intf-Student_LAN-Zone

Source Address: [Empty]

Source Site Name: [Empty]

Source Address Negate:

Region: [Empty]

State: [Empty]

City: [Empty]

OK Cancel

Edit App QoS Rule - Common-Internet

General Source Destination Headers/Schedule Applications/URL Enforce

Destination Zone: [Empty]

Intf-INET-Zone

Destination Address: [Empty]

Destination Site Name: [Empty]

Custom Geo Circle: [Empty]

Region: [Empty]

State: [Empty]

City: [Empty]

Destination Address Negate:

Destination Location Negate:

OK Cancel

Edit App QoS Rule - Common-Internet

General Source Destination Headers/Schedule Applications/URL Enforce

Action Setting: Allow

QoS Profile Setting: Common-Internet

View QoS Profile

OK Cancel

When you are finished your configuration should look similar to this:

<input type="checkbox"/>	Rule Num	Name	Rule Disabled	Source				
				Zone	Region	Address	Address Group	Site N
<input type="checkbox"/>	1	Find-Real-time-Critical	False	Intf-Student_LAN-Zone				
<input type="checkbox"/>	2	Find-Real-time-Non-Cr...	False	Intf-Student_LAN-Zone				
<input type="checkbox"/>	3	Find-Internal-Business...	False	Intf-Student_LAN-Zone				
<input type="checkbox"/>	4	Find-External-Business...	False	Intf-Student_LAN-Zone				
<input type="checkbox"/>	5	Drop-Sensitive-Apps	False	Intf-Student_LAN-Zone				
<input type="checkbox"/>	6	Internet-Streaming	False	Intf-Student_LAN-Zone				
<input type="checkbox"/>	7	Common-Internet	False	Intf-Student_LAN-Zone				

Rows per page Showing 1 - 7 of 7

Step 4. Drop Profiles

There are default drop profiles enabled to manage congestion in queues and interfaces. You will add additional drop profiles that can be used to replace the default drop profiles.

4.a. Create 4 drop profiles:

- Deep-Queue-Aggressive
- Deep-Queue-Conservative
- Shallow-Queue-Aggressive
- Shallow-Queue-Conservative

<input type="checkbox"/>	Name	Min	Max
<input type="checkbox"/>	Deep-Queue-Aggressive	10	140
<input type="checkbox"/>	Deep-Queue-Conservative	70	140
<input type="checkbox"/>	Shallow-Queue-Aggressive	10	40
<input type="checkbox"/>	Shallow-Queue-Conservative	20	40

Edit Drop Profile - Deep-Queue-Aggressive ✕

Name *

Description Tags

Weighted Random Early Drop

Max * Min *

Weight Inverse Mask Probability

Edit Drop Profile - Deep-Queue-Conservative ✕

Name *

Description Tags

Weighted Random Early Drop

Max * Min *

Weight Inverse Mask Probability

Edit Drop Profile - Shallow-Queue-Aggressive ✕

Name *

Description Tags

Weighted Random Early Drop

Max * Min *

Weight Inverse Mask Probability

Edit Drop Profile - Shallow-Queue-Conservative ✕

Name *

Description Tags

Weighted Random Early Drop

Max * Min *

Weight Inverse Mask Probability

Step 5. Schedulers

Your device needs to be configured to remove packets from the queues and to forward them out the interface. There are 4 major traffic classes: Network Control, Expedited Forwarding, Assured Forwarding, and Best Effort. Each of these traffic classes has 4 queues. You will create a scheduler for each major traffic class that:

- Defines how much interface bandwidth each traffic class will have for transmitting traffic; and
- Defines which queues to pull traffic from when the traffic class is granted access to the interface.

5.a. Define the following 4 schedulers:

AF-Scheduler

Scheduler Name: AF-Scheduler
Loss Priority High: Deep-Queue-Aggressive
Loss Priority Low: Deep-Queue-Conservative
Guaranteed Rate: 40%
Queue 0 Weight: 1
Queue 1 Weight: 3

BE-Scheduler

Scheduler Name: BE-Scheduler
Loss Priority High: Deep-Queue-Aggressive
Loss Priority Low: Deep-Queue-Conservative
Queue 0 Weight: 1
Queue 1 Weight: 2

EF-Scheduler

Scheduler Name: EF-Scheduler
Loss Priority High: Shallow-Queue-Aggressive
Loss Priority Low: Shallow-Queue-Conservative
Guaranteed Rate: 25%

NC-Scheduler

Scheduler Name: NC-Scheduler
Loss Priority High: Deep-Queue-Aggressive
Loss Priority Low: Deep-Queue-Conservative
Guaranteed Rate: 5%

<input type="checkbox"/>	Name	Loss Priority	Drop Profile	Transmit Rate	Guaranteed Rate	Queue	Weight
<input type="checkbox"/>	AF-Scheduler	low high	Deep-Queue-Conserva Deep-Queue-Aggressiv		40 (%)	0 1	1 3
<input type="checkbox"/>	BE-Scheduler	low high	Deep-Queue-Conserva Deep-Queue-Aggressiv			0 1	1 2
<input type="checkbox"/>	EF-Scheduler	low high	Shallow-Queue-Conser Shallow-Queue-Aggres		25 (%)		
<input type="checkbox"/>	NC-Scheduler				5 (%)		

Edit Scheduler - AF-Scheduler

Name: AF-Scheduler

Description: Tags:

Loss Priority: High Drop Profile: Deep-Queue-Aggressive

Low: Deep-Queue-Conservative

Transmit Rate: Rate (Kbps) Rate (%) Rate(Kbps): 8_10000000

Guaranteed Rate: Rate (Kbps) Rate (%) Rate(%): 40

Queue	Weight
0	1
1	3
2	--Select--
3	--Select--

OK Cancel

Edit Scheduler - BE-Scheduler

Name: BE-Scheduler

Description: Tags:

Loss Priority: High Drop Profile: Deep-Queue-Aggressive

Low: Deep-Queue-Conservative

Transmit Rate: Rate (Kbps) Rate (%) Rate(Kbps): 8_10000000

Guaranteed Rate: Rate (Kbps) Rate (%) Rate(Kbps): 8_10000000

Queue	Weight
0	1
1	2
2	--Select--
3	--Select--

OK Cancel

Edit Scheduler - EF-Scheduler

Name: EF-Scheduler

Description: Tags:

Loss Priority: High Drop Profile: Shallow-Queue-Aggressive

Low: Shallow-Queue-Conservative

Transmit Rate: Rate (Kbps) Rate (%) Rate(Kbps): 8_10000000

Guaranteed Rate: Rate (Kbps) Rate (%) Rate(%): 25

Queue	Weight
0	--Select--

OK Cancel

Edit Scheduler - NC-Scheduler

Name: NC-Scheduler

Description: Tags:

Loss Priority: High Drop Profile: --Select--

Low: --Select--

Transmit Rate: Rate (Kbps) Rate (%) Rate(Kbps): 8_10000000

Guaranteed Rate: Rate (Kbps) Rate (%) Rate(%): 5

Queue	Weight
0	--Select--

OK Cancel

Step 6. Scheduler Map

You have created 4 schedulers that can be used to manage the queues on interfaces. Next you will need to assign a scheduler to each traffic class by using a scheduler map.

- 6.a. Create a scheduler map that will be used to map schedulers to the traffic classes. The same map will be used on all interfaces so that all interfaces receive the same queuing and scheduling parameters
- 6.b. Name the scheduler map WAN-Port-Schedulers.

Use the scheduler name to associate it with the proper traffic class (e.g. NC to Traffic Class 0, EF to traffic class 1, AF to traffic class 2, and BE to traffic class 3)

<input type="checkbox"/>	Scheduler Map Name	Traffic Class : Schedulers
<input type="checkbox"/>	WAN-Port-Schedulers	Traffic Class 0 : NC-Scheduler Traffic Class 1 : EF-Scheduler Traffic Class 2 : AF-Scheduler Traffic Class 3 : BE-Scheduler

Edit Scheduler Map - WAN-Port-Schedulers ✕

Name *

Description Tags

Traffic Class	Scheduler
Traffic Class 0	<input style="width: 100%;" type="text" value="NC-Scheduler"/>
Traffic Class 1	<input style="width: 100%;" type="text" value="EF-Scheduler"/>
Traffic Class 2	<input style="width: 100%;" type="text" value="AF-Scheduler"/>
Traffic Class 3	<input style="width: 100%;" type="text" value="BE-Scheduler"/>

Step 7. Associating the parameters to the interfaces

You have defined the class of service parameters that will be applied to your network. Now you need to associate those parameters to the interfaces, or assign those parameters to the interfaces.

7.a. Assign the following shaping and scheduler map parameters to the physical interfaces (vni-0/0 and vni-0/1) as follows:

Associate Interface vni-0/0

Interface: vni-0/0
Rate: 100000
Scheduler Map: WAN-Port-Schedulers

Associate Interface vni-0/1

Interface: vni-0/1
Rate: 100000
Scheduler Map: WAN-Port-Schedulers

<input type="checkbox"/>	Name	Description	Tag	Shaping		Logging Interval(seconds)	Scheduler Map
				Burst Size (Bytes)	Rate (Kbps)		
<input type="checkbox"/>	vni-0/0				100000		WAN-Port-Sche
<input type="checkbox"/>	vni-0/1				100000		WAN-Port-Sche

Edit Associate Interface/Network - vni-0/0 ✕

Interface Network

Name *
vni-0/0

Description Tags

Shaping ⓘ

Burst Size (Bytes) Rate (Kbps)

DSCP Rewrite Rule DSCP6 Rewrite Rule

802.1p Rewrite Rule Scheduler Map

Logging Interval(seconds) Bandwidth Sharing

Logging CoS FC Stats

Edit Associate Interface/Network - vni-0/1 ✕

Interface Network

Name *
vni-0/1

Description Tags

Shaping ⓘ

Burst Size (Bytes) Rate (Kbps)

DSCP Rewrite Rule DSCP6 Rewrite Rule

802.1p Rewrite Rule Scheduler Map

Logging Interval(seconds) Bandwidth Sharing

Logging CoS FC Stats

Step 8. Verify the Class of Service Parameters

You have configured class of service on the device and applied the configuration parameters to the interface. Next we will verify that the class-of-service parameters have been applied by using the Versa Director Monitor dashboard and the VOS CLI.

- 8.a. In the *Versa Director Monitor* dashboard for your device, navigate to *Networking > COS > App QoS Policies*.
- 8.b. Ensure that you are viewing the *Monitor* dashboard for your *SxxB01* device
- 8.c. Select the *Default-Policy* from the drop-down menu.

The screenshot shows the Versa Director Monitor interface. The 'Monitor' tab is selected. Under 'Devices', 'Branch01' is highlighted. The 'Networking' service is selected, and the 'COS' tab is active. The 'App QoS Policies' dropdown menu is open, showing 'Default-Policy' selected. Below the dropdown is a table with the following data:

Rule Name	App QoS Hit Count	App QoS Drop Packet Count	App QoS Drop Byte Count	App QoS Forward Packet C...	App QoS Forward Byte Count	Dropped Sessions By Per Us...
Find-Real-time-Critical	0	0	0	0	0	0
Find-Real-time-Non-Critical	0	0	0	0	0	0
Find-Internal-Business-Apps	0	0	0	0	0	0
Find-External-Business-Apps	0	0	0	0	0	0
Drop-Sensitive-Apps	0	0	0	0	0	0

Note that because this is a lab environment and no live data is transiting the devices, the counters are listed at 0.

- 8.d. Select the *Interfaces* tab under the COS table. There will be packets listed under the interface that have been processed by the CoS processes. However, the packets listed didn't match the specific policies created, so they were processed with default CoS behavior.

The screenshot shows the 'Interfaces' tab under the COS table. The table lists interface statistics for vni-0/0 and vni-0/1. The data is as follows:

Name	TX Packets	TX PPS	TX Dropped	TX Bytes	TX BPS	TX Bytes Dropped	Queue Length
vni-0/0	233162	0	0	60770355	1064	0	0
vni-0/1	2982	1	0	1078306	1968	0	0

Open the Remmina application. In the Remmina application, open an SSH session to your branch device. If prompted for a username or password, the login is student and password is versa123.

8.e. Type *cli* at the shell prompt to start the CLI process.

8.f. From the CLI, issue the command `show class-of-service interfaces detail` to view the configured class of services properties. The output shows the traffic sent in each traffic class and on each interface.

```
admin@Branch01-cli> show class-of-services interfaces detail
```

```
admin@Branch01-cli> show class-of-services interfaces detail
```

```
Interface: vni-0/0
```

```
Traffic Stats:
```

```
TX Packets      : 233234
TX PPS         : 1
TX Packets Dropped : 0
TX Bytes       : 60784780
TX bps        : 1600
TX Bytes Dropped : 0
```

```
Port Stats :
```

	Traffic Class	TX Pkts	TX Dropped	TX Bytes	Bytes Dropped
tc0	network-control	132052	0	40360896	0
tc1	expedited-fwd	101089	0	20419978	0
tc2	assured-fwd	0	0	0	0
tc3	best-effort	93	0	3906	0

```
Pipe Stat:
```

```
Pipe ID      : 1
Users       : [ Hub:INET:INET:Tenant1:clear ]
```

	Traffic Class	TX Pkts	TX Dropped	TX Bytes	Bytes Dropped
tc0	network-control	0	0	0	0
tc1	expedited-fwd	0	0	0	0
tc2	assured-fwd	0	0	0	0
tc3	best-effort	0	0	0	0

```
Pipe ID      : 2
Users       : [ Hub:INET:INET:Tenant1:secure ]
```

	Traffic Class	TX Pkts	TX Dropped	TX Bytes	Bytes Dropped
tc0	network-control	8	0	1104	0
tc1	expedited-fwd	26241	0	5300682	0
tc2	assured-fwd	0	0	0	0
tc3	best-effort	0	0	0	0

```
Pipe ID      : 0
Users       : [ vni-0/0.0 ]
```

	Traffic Class	TX Pkts	TX Dropped	TX Bytes	Bytes Dropped
tc0	network-control	132044	0	40359792	0
tc1	expedited-fwd	74848	0	15119296	0
tc2	assured-fwd	0	0	0	0
tc3	best-effort	93	0	3906	0

8.g. Use the command `show class-of-services interfaces extensive` to see the shaping parameters in the output.

```
admin@Branch01-cli> show class-of-services interfaces extensive

Interface: vni-0/0
Configuration:
  Burst Size : 125000 bytes
  Rate      : 100000 kbps
  TC0: Network-Control : 5000-100000 kbps
  TC1: Expedited-Forwarding : 25000-100000 kbps
  TC2: Assured-Forwarding : 40000-100000 kbps
  TC3: Best-Effort : 100000-100000 kbps

Traffic Stats:
  TX Packets : 233268
  TX PPS : 1
  TX Packets Dropped : 0
  TX Bytes : 60791575
  TX bps : 2144
  TX Bytes Dropped : 0

Port Stats :
  Traffic Class      TX Pkts      TX Dropped      TX Bytes      Bytes Dropped
tc0 network-control 132062         0                40362843       0
tc1 expedited-fwd  101113         0                20424826       0
tc2 assured-fwd     0              0                 0              0
tc3 best-effort     93             0                 3906           0

Pipe Stat:
  Pipe ID : 1
  Users : [ Hub:INET:INET:Tenant1:clear ]
  Type : SDWAN
  Configuration :
  Rate : 40000 kbps
  TC0: Network-Control : 40000-40000 kbps
  TC1: Expedited-Forwarding : 40000-40000 kbps
  TC2: Assured-Forwarding : 40000-40000 kbps
  TC3: Best-Effort : 40000-40000 kbps

Traffic Stats:
  Queues Cfg      Inferred      TX              TX              TX              Bytes Qlen      Avg      Avg Drop
  Wt             BW kbps       Pkts           Dropped         Bytes           Dropped         Rate bps  rate bps
tc0 network-control:
q0: fc_nc  1  10000-40000  0              0              0              0  0          0          0
q1: fc1    1  10000-40000  0              0              0              0  0          0          0
q2: fc2    1  10000-40000  0              0              0              0  0          0          0
q3: fc3    1  10000-40000  0              0              0              0  0          0          0
tc1 expedited-fwd:
q0: fc_ef  1  10000-40000  0              0              0              0  0          0          0
q1: fc5    1  10000-40000  0              0              0              0  0          0          0
q2: fc6    1  10000-40000  0              0              0              0  0          0          0
q3: fc7    1  10000-40000  0              0              0              0  0          0          0
tc2 assured-fwd:
q0: fc_af  3  20000-40000  0              0              0              0  0          0          0
q1: fc9    1  6666-40000   0              0              0              0  0          0          0
q2: fc10   1  6666-40000   0              0              0              0  0          0          0
q3: fc11   1  6666-40000   0              0              0              0  0          0          0
tc3 best-effort:
q0: fc_be  1  10000-40000  0              0              0              0  0          0          0
q1: fc13   1  10000-40000  0              0              0              0  0          0          0
q2: fc14   1  10000-40000  0              0              0              0  0          0          0
q3: fc15   1  10000-40000  0              0              0              0  0          0          0

[snip]
```



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

ADAPTIVE SHAPING

In the following lab exercises, you will:

- Locate the Adaptive Services configuration parameters
- Configure Adaptive Shaping
- Verify Adaptive Shaping

Note: Configuration modifications in this lab will be performed in Appliance View 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 advertise its local interface speed to the remote devices. Testing of the changes you make on your device will be verified by logging into the Hub device, as changes made on your device will advertise your link rates to the hub, and the hub will apply dynamic shapers towards your device.

The following components are required for a complete adaptive shaping configuration:

- Shaping configured on the local interfaces (in order to apply dynamic shapers towards remote sites)
- The local circuit speeds must be defined (this provides the value that will be used to trigger Advertised Link Rate adjustments)
- Adaptive Shaping function: This adds the Advertised Link Rate value to remote sites using MP-BGP (Versa-Private Route), and defines the circumstances that will trigger an update
- Inbound Shaper: This defines the Advertised Link Rate value that is advertised by the device

The hub already has shaping configured on its WAN interfaces, and therefore will respond to advertised link rate information sent from your site. In this lab you will begin by configuring the local site circuit bandwidth. You will configure a different bandwidth for the MPLS and INET links.

You will perform the lab configuration from the *Appliance View* and not through device templates. To open the *Appliance Context* mode for your device, navigate to *Administration > Appliances* and locate your device in the appliances list. Click on your device to open your appliance. Alternatively, you can click on the *Appliance View* button at the top of the user interface, then select your device from the list of devices in the table.

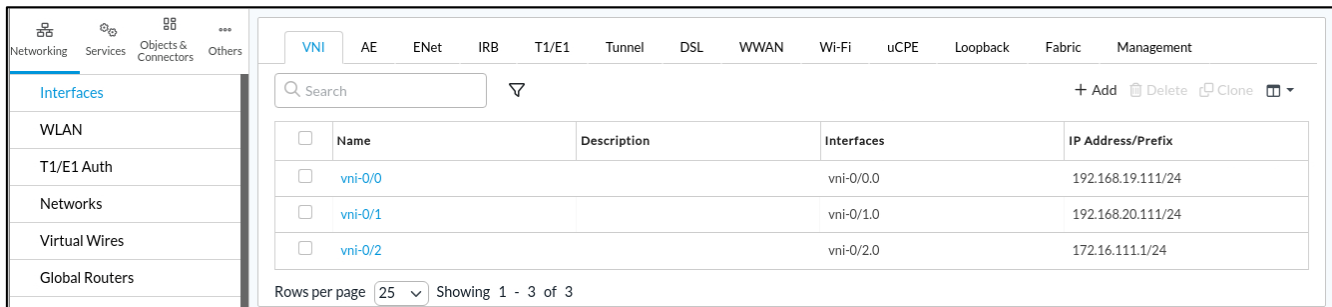
Step 1. Configure Adaptive Shaping

1.a. From your *Appliance View*, click the *Configuration* tab to open your device configuration.

The circuit speeds are configured under the *Networking > Interfaces* configuration.

1.b. Open the *Interfaces* configuration dashboard:

The WAN interfaces are vni-0/0 (INET link) and vni-0/1 (MPLS link).



<input type="checkbox"/>	Name	Description	Interfaces	IP Address/Prefix
<input type="checkbox"/>	vni-0/0		vni-0/0.0	192.168.19.111/24
<input type="checkbox"/>	vni-0/1		vni-0/1.0	192.168.20.111/24
<input type="checkbox"/>	vni-0/2		vni-0/2.0	172.16.111.1/24

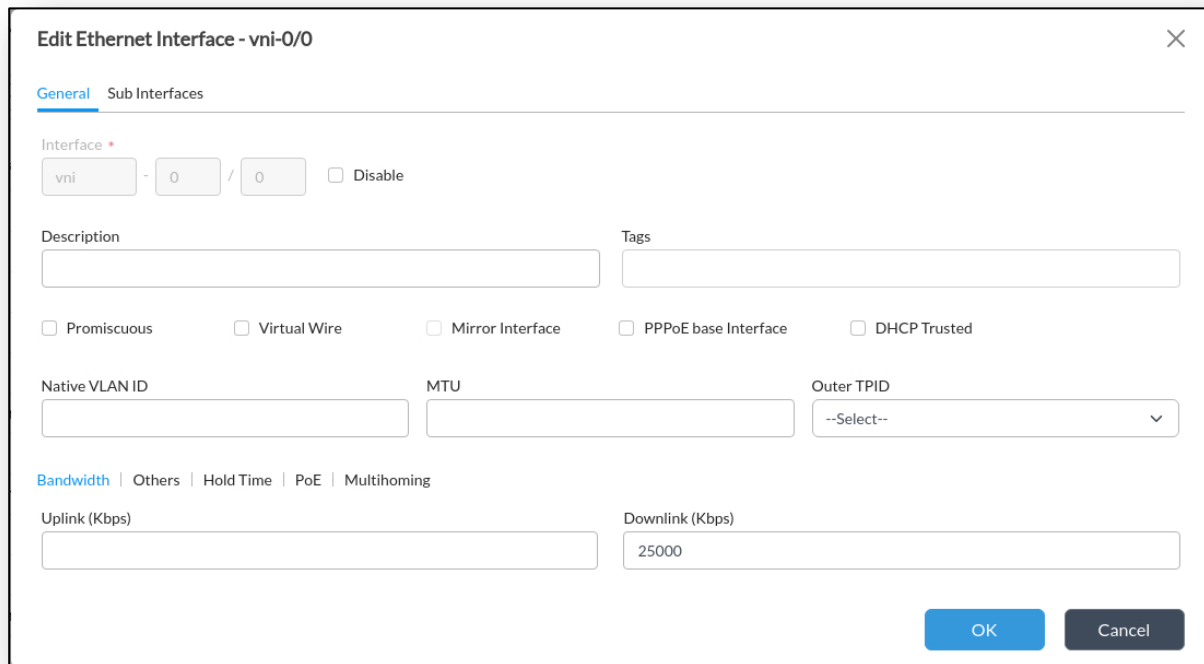
Rows per page: 25 Showing 1 - 3 of 3

1.c. Click on the *vni-0/0* interface to open the interface configuration.

1.d. In the *General* tab, locate the *Bandwidth* setting. It should be empty.

1.e. Set the Downlink bandwidth to 25000Kbps (25mbps)

1.f. Click *OK* to apply the setting.



Edit Ethernet Interface - vni-0/0

General | Sub Interfaces

Interface: vni - 0 / 0 Disable

Description: Tags:

Promiscuous Virtual Wire Mirror Interface PPPoE base Interface DHCP Trusted

Native VLAN ID: MTU: Outer TPID: --Select--

Bandwidth | Others | Hold Time | PoE | Multihoming

Uplink (Kbps): Downlink (Kbps): 25000

OK Cancel

Repeat the process on the vni-0/1 interface.

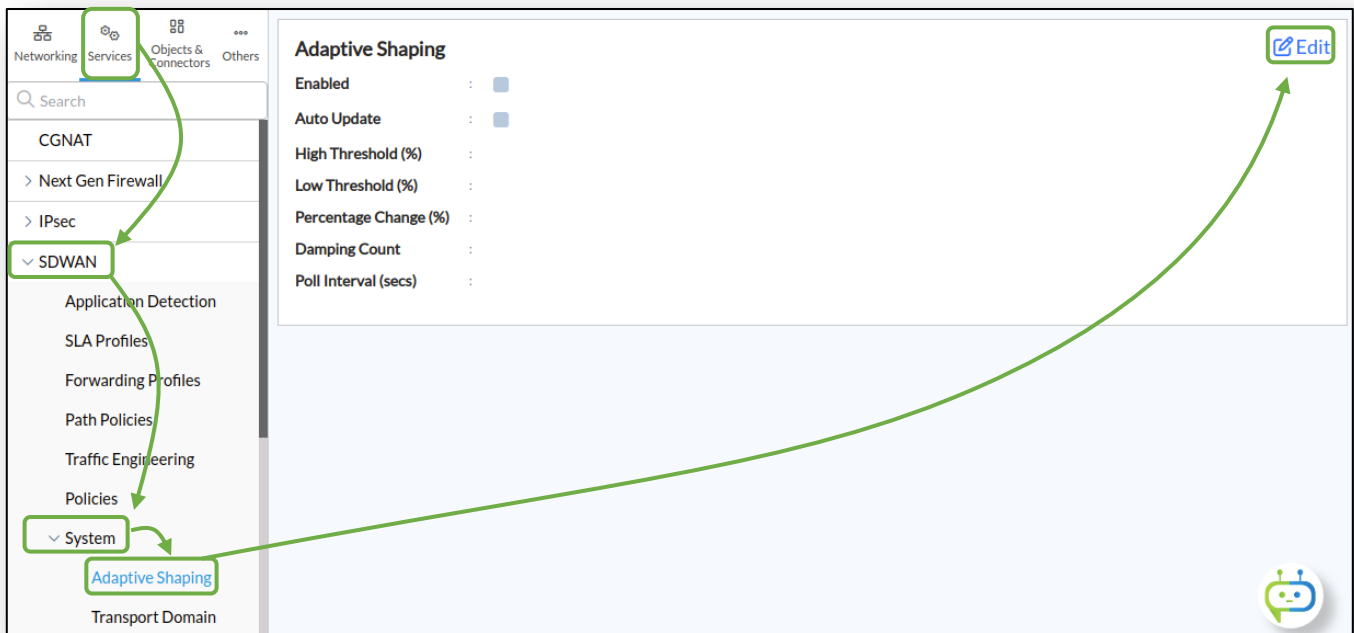
- 1.g. Click on the *vni-0/1* interface to open the interface configuration.
- 1.h. In the *General* tab, locate the *Bandwidth* setting. It should be empty.
- 1.i. Set the Downlink bandwidth to 25000Kbps (25mbps)
- 1.j. Click *OK* to apply the setting.

After you have configured the Uplink and Downlink speeds on the interface you need to enable Adaptive Shaping.

- 1.k. To enable Adaptive Shaping, navigate to *Services > SDWAN > System > Adaptive Shaping*.

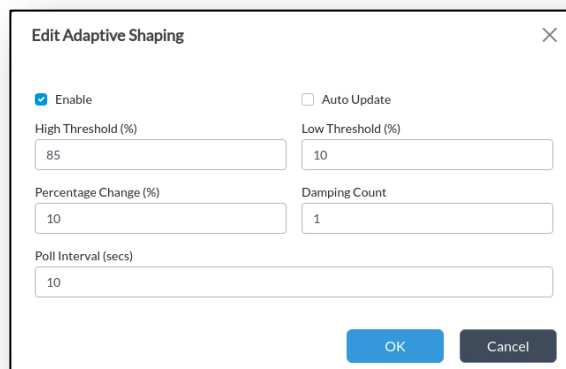
The Adaptive Shaping function is a system function.

- 1.l. Click on the edit (Pencil) button to open the Adaptive Shaping configuration dialog.



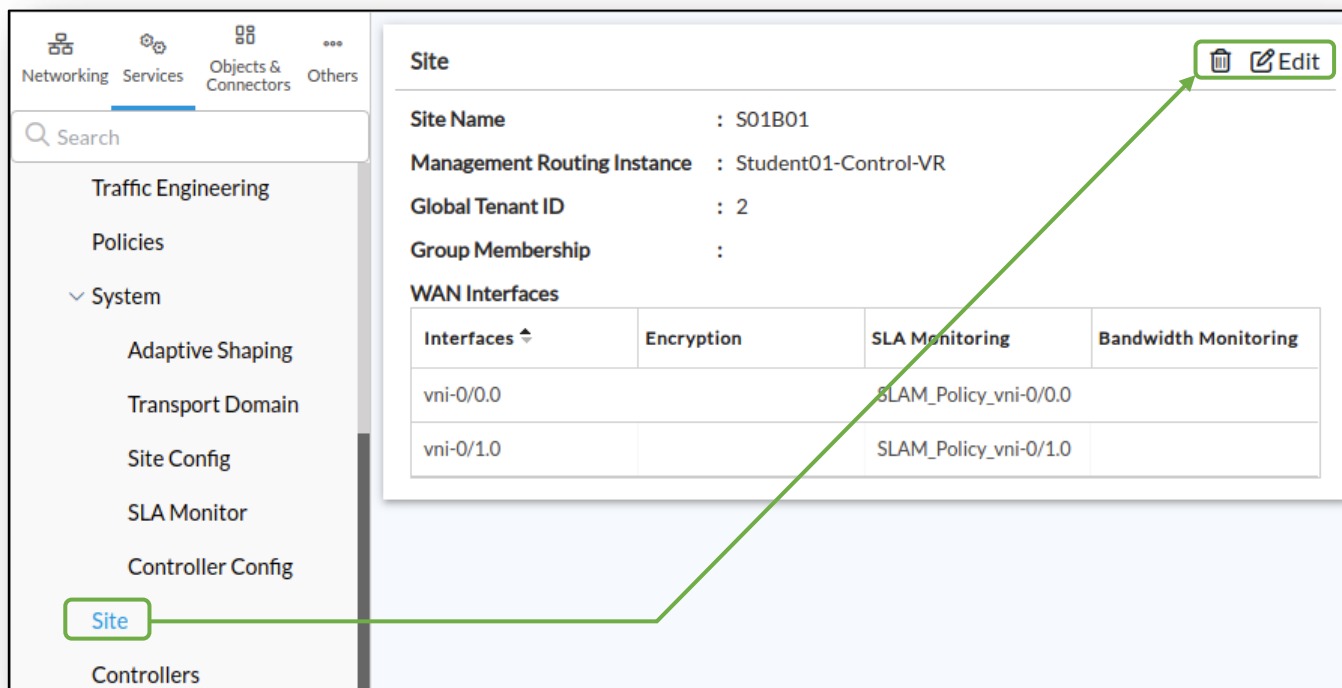
When the Edit Adaptive Shaping dialog appears, the *Enable* setting will automatically be checked. The default settings are shown. For our lab exercise, the default settings will work.

- 1.m. Click the *OK* button to apply the changes and enable the Adaptive Shaping function. The parameters from the dialog should now appear in the Adaptive Shaping information on the main Adaptive Shaping dashboard.

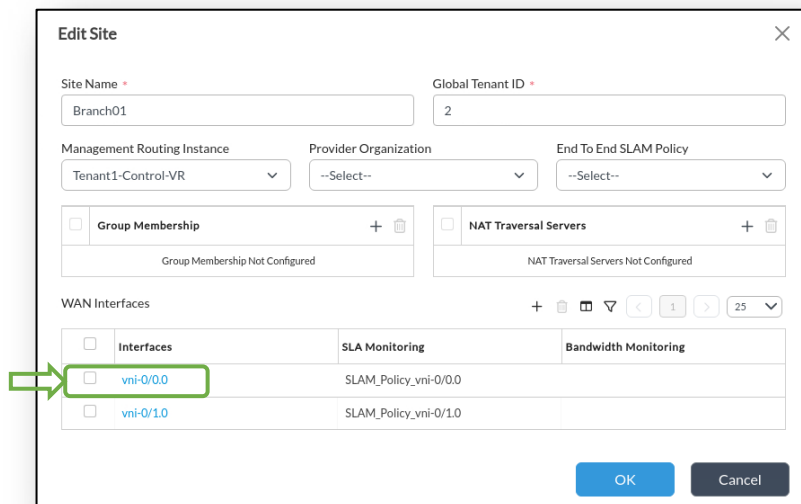


The final step to complete the Adaptive Shaping configuration is to configure the inbound shaping value. This is the value that will be advertised to the remote sites and it is found under the *Services > SDWAN > Site* parameters.

- 1.n. Navigate to the *Services > SDWAN > Site* hierarchy.
- 1.o. Click on the pencil icon to edit the site properties:



- 1.p. In the *Edit Site* dialog, locate the WAN interfaces.
- 1.q. Click on the *vni-0/0.0* interface to modify the interface settings.

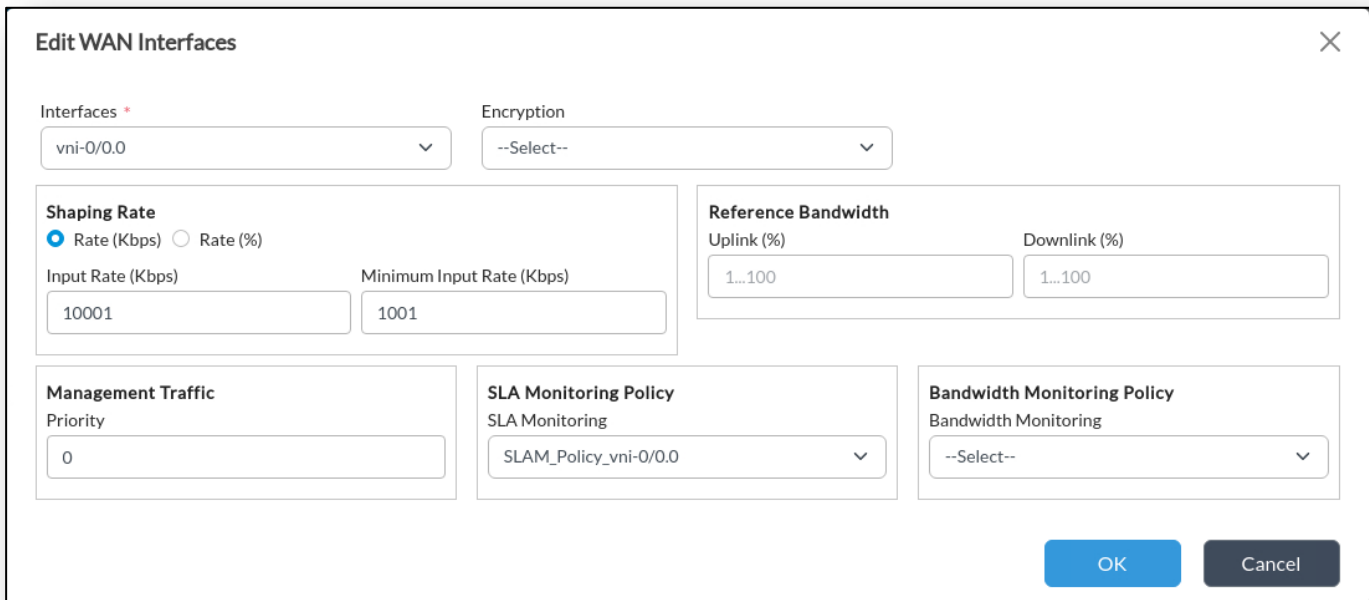


The WAN Interfaces configuration dialog allows you to configure an Input Rate and Minimum Input Rate. The Input rate is the default rate that will be advertised to remote sites. The Minimum Input Rate is the lowest value that will be advertised to remote sites (the lowest value the Adaptive Shaping algorithm can advertise.)

Because of the shared hub, you will configure a unique shaping value on your interface according to your branch/student ID. This will allow you to filter the class of service output on the hub based on your unique bandwidth setting.

- 1.r. Set the Shaping Input Rate of your vni-0/0.0 interface to 100xx, where xx is your student ID (e.g. 10001 for student01, 10002 for student02, 10012 for student 12, 10013 for student 13, etc.)
- 1.s. Set the Shaping Input Rate of your vni-0/1.0 interface to 111xx, where xx is your student ID (e.g. 11101 for student01, 11102 for student02, 11112 for student 12, 11113 for student13, etc.)
- 1.t. Click the *OK* button on each window until you exit the site configuration to apply the configuration to the appliance.

Example for student01:



Edit WAN Interfaces [Close]

Interfaces * Encryption

Shaping Rate
 Rate (Kbps) Rate (%)
Input Rate (Kbps) Minimum Input Rate (Kbps)

Reference Bandwidth
Uplink (%) Downlink (%)

Management Traffic
Priority

SLA Monitoring Policy
SLA Monitoring

Bandwidth Monitoring Policy
Bandwidth Monitoring

You have finished configuring Adaptive Shaping on your branch device.

Step 2. Verify the Advertised Link Rate and dynamic shapers on the Hub device

Your device should now be advertising its local link rates to the other devices in the network. You will verify your advertised link rate by logging in to the hub device. On the hub device you will verify that your advertised link rate has been received, and that the hub device has applied dynamic shapers on the tunnels to your branch device.

- 2.a. Locate the Remmina shortcut on your remote desktop task bar. Open the Remmina application and open an SSH session to the hub device. The hub device management address is 10.27.1.100. The login is *admin/versa123*.
- 2.b. Log into the hub with the username
- 2.c. On the hub device, enter the command *cli* to start the command line interface.

2.d. From the CLI on the hub device, enter the command `show class-of-services`.

You will see output from all of the interfaces and for all of the tunnels. You will need to look for a Pipe ID that has a rate that matches your sites configured Input Shaping rate.

2.e. To help you find your site's Pipe (tunnel), you can use the following command: `show class-of-services | find [your site's bandwidth setting]`: e.g. `show class-of-services | find 10001` for student01, `show class-of-services | find 10002` for student02, `show class-of-services | find 10011` for student 11, etc.)

You should see output that reflects the configured inbound shaping parameter that you configured on your device in an earlier step.

```

dmin@Hub-cli> show class-of-services | find 10001
  Rate      : 10001 kbps
Traffic Stats:
  Queues          TX          TX          TX          Bytes  Qlen
                  Pkts        Dropped      Bytes        Dropped
tc0 network-control:
  q0: fc_nc        0            0            0            0      0
  q1: fc1          0            0            0            0      0
  q2: fc2          0            0            0            0      0
  q3: fc3          0            0            0            0      0
tc1 expedited-fwd:
  q0: fc_ef        0            0            0            0      0
  q1: fc5          0            0            0            0      0
  q2: fc6          0            0            0            0      0
  q3: fc7          0            0            0            0      0
tc2 assured-fwd:
  q0: fc_af        0            0            0            0      0
  q1: fc9          0            0            0            0      0
  q2: fc10         0            0            0            0      0
  q3: fc11         0            0            0            0      0
tc3 best-effort:
  q0: fc_be        0            0            0            0      0
  q1: fc13         0            0            0            0      0
  q2: fc14         0            0            0            0      0
  q3: fc15         0            0            0            0      0

  Pipe ID       : 2
  Users         : [ WAN-103:17:2:secure ]
  Type          : SDWAN
  Configuration :
  Rate         : 10001 kbps
Traffic Stats:
  Queues          TX          TX          TX          Bytes  Qlen
                  Pkts        Dropped      Bytes        Dropped
tc0 network-control:
  q0: fc_nc        0            0            0            0      0
  q1: fc1          0            0            0            0      0
  q2: fc2          0            0            0            0      0
  q3: fc3          0            0            0            0      0

```

You can use the same command to display the dynamic shaper on the hub's MPLS interface by issuing the same command, but substitute the MPLS inbound shaping rate configured on your site (e.g. 11101, 11102, 11103, etc.)

```
admin@Hub-cli> show class-of-services | find 11110
Rate : 11101 kbps
Traffic Stats:
  Queues          TX          TX          TX          Bytes  Qlen
                  Pkts        Dropped      Bytes      Dropped
tc0 network-control:
  q0: fc_nc        0            0            0            0      0
  q1: fc1          0            0            0            0      0
  q2: fc2          0            0            0            0      0
  q3: fc3          0            0            0            0      0
tc1 expedited-fwd:
  q0: fc_ef        0            0            0            0      0
  q1: fc5          0            0            0            0      0
  q2: fc6          0            0            0            0      0
  q3: fc7          0            0            0            0      0
tc2 assured-fwd:
  q0: fc_af        0            0            0            0      0
  q1: fc9          0            0            0            0      0
  q2: fc10         0            0            0            0      0
  q3: fc11         0            0            0            0      0
tc3 best-effort:
  q0: fc_be        0            0            0            0      0
  q1: fc13         0            0            0            0      0
  q2: fc14         0            0            0            0      0
  q3: fc15         0            0            0            0      0

Pipe ID      : 2
Users       : [ WAN-103:34:2:secure ]
Type        : SDWAN
Configuration :
Rate       : 11101 kbps
Traffic Stats:
  Queues          TX          TX          TX          Bytes  Qlen
                  Pkts        Dropped      Bytes      Dropped
tc0 network-control:
  q0: fc_nc        0            0            0            0      0
  q1: fc1          0            0            0            0      0
  q2: fc2          0            0            0            0      0
  q3: fc3          0            0            0            0      0
```



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

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.

In this lab, you will be assigned a student ID (Student01, Student02, etc.) Each student environment is a tenant on Versa Director and has access to 2 VOS devices and a shared hub. You will perform your operations on the VOS devices.

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.

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!

Step 1. Create SLA Profiles to Track Link Status

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.

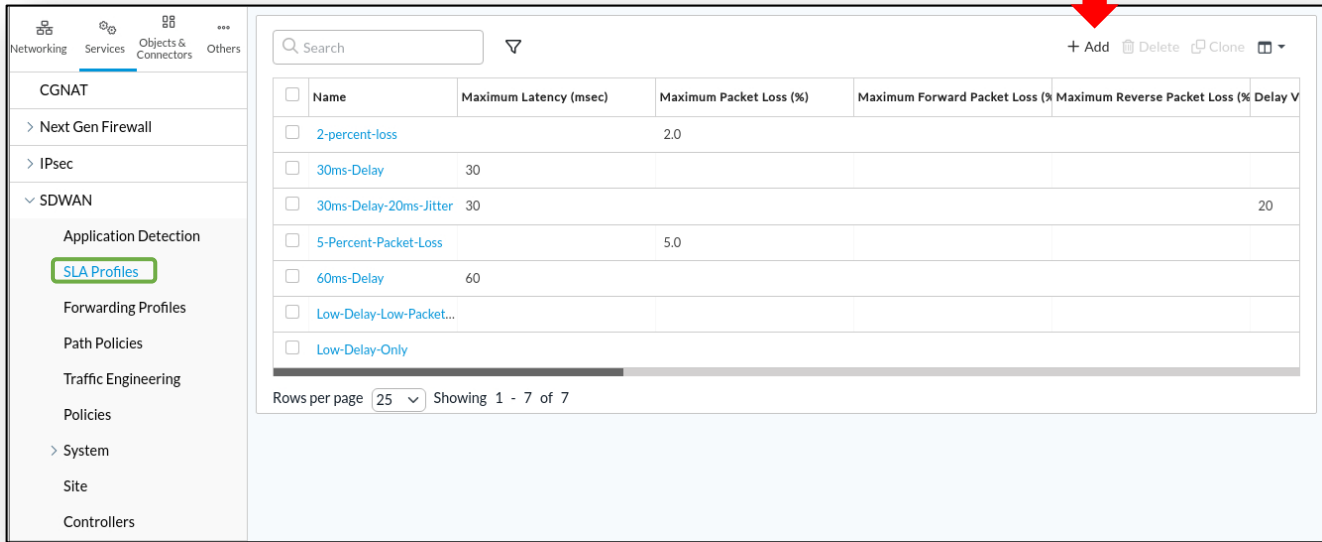
You can configure your device to use the statistics that are gathered to determine whether a transport path is suitable for different types of applications, based on administrative rules. To configure your device to track SLA statistics you configure SLA profiles.

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

- 1.a. Open Versa Director on the remote desktop. Log into Versa Director with the username and password provided by your instructor.
- 1.b. In Versa Director, click on *Appliance View* at the top of the window.
- 1.c. Locate your *SxxB01* device in the appliance table. Click on the appliance to open the appliance view.
- 1.d. In *Appliance View* of your *SxxB01* device, navigate to the *Configuration > Services > SDWAN > SLA Profiles* hierarchy.
- 1.e. Click the *Add* button to create SLA profiles.

Add SLA profiles with the following properties:

SLA Profile Name: 2-percent-loss Maximum Packet Loss: 2.0	SLA Profile Name: 30ms-Delay Maximum Latency: 30
SLA Profile Name: 30ms-Delay-20ms-Jitter Packet Delay Variation (Jitter): 20 Maximum Latency: 30	SLA Profile Name: 5-Percent-Packet-Loss Maximum Packet Loss: 5
SLA Profile Name: 60ms-Delay Maximum Latency: 60	SLA Profile Name: Low-Delay-Low-Packet-Loss Check Low Latency and Low Packet Loss
SLA Profile Name: Low-Delay-Only Check Low Latency	



The screenshot shows the 'SLA Profiles' configuration page in the Versa SD-WAN interface. The left sidebar contains a navigation menu with categories like 'CGNAT', 'Next Gen Firewall', 'IPsec', 'SDWAN', 'Application Detection', 'Forwarding Profiles', 'Path Policies', 'Traffic Engineering', 'Policies', 'System', 'Site', and 'Controllers'. The 'SLA Profiles' item is highlighted in green. The main content area features a table with columns for Name, Maximum Latency (msec), Maximum Packet Loss (%), Maximum Forward Packet Loss (%), Maximum Reverse Packet Loss (%), and Delay (ms). A red arrow points to the '+ Add' button in the top right corner of the table.

<input type="checkbox"/>	Name	Maximum Latency (msec)	Maximum Packet Loss (%)	Maximum Forward Packet Loss (%)	Maximum Reverse Packet Loss (%)	Delay (ms)
<input type="checkbox"/>	2-percent-loss		2.0			
<input type="checkbox"/>	30ms-Delay	30				
<input type="checkbox"/>	30ms-Delay-20ms-Jitter	30				20
<input type="checkbox"/>	5-Percent-Packet-Loss		5.0			
<input type="checkbox"/>	60ms-Delay	60				
<input type="checkbox"/>	Low-Delay-Low-Packet...					
<input type="checkbox"/>	Low-Delay-Only					

Rows per page: 25 Showing 1 - 7 of 7

Edit SLA Profile - 2-percent-loss

General SaaS App Monitor

Name: 2-percent-loss Tags: []

Description: []

Packet Delay Variation (Jitter): [] Circuit Transmit Utilization (%): [] Circuit Receive Utilization (%): []

Maximum Packet Loss (%): 2.0 Maximum Forward Packet Loss (%): [] Maximum Reverse Packet Loss (%): []

Maximum Latency (msec): [] MOS Score: []

Low Delay Variation Low Latency Low Packet Loss

Low Forward Packet Loss Low Reverse Packet Loss

OK Cancel

Edit SLA Profile - 30ms-Delay

General SaaS App Monitor

Name: 30ms-Delay Tags: []

Description: []

Packet Delay Variation (Jitter): [] Circuit Transmit Utilization (%): [] Circuit Receive Utilization (%): []

Maximum Packet Loss (%): [] Maximum Forward Packet Loss (%): [] Maximum Reverse Packet Loss (%): []

Maximum Latency (msec): 30 MOS Score: []

Low Delay Variation Low Latency Low Packet Loss

Low Forward Packet Loss Low Reverse Packet Loss

OK Cancel

Edit SLA Profile - 30ms-Delay-20ms-Jitter

General SaaS App Monitor

Name: 30ms-Delay-20ms-Jitter Tags: []

Description: []

Packet Delay Variation (Jitter): 20 Circuit Transmit Utilization (%): [] Circuit Receive Utilization (%): []

Maximum Packet Loss (%): [] Maximum Forward Packet Loss (%): [] Maximum Reverse Packet Loss (%): []

Maximum Latency (msec): 30 MOS Score: []

Low Delay Variation Low Latency Low Packet Loss

Low Forward Packet Loss Low Reverse Packet Loss

OK Cancel

Edit SLA Profile - 5-Percent-Packet-Loss

General SaaS App Monitor

Name: 5-Percent-Packet-Loss Tags: []

Description: []

Packet Delay Variation (Jitter): [] Circuit Transmit Utilization (%): [] Circuit Receive Utilization (%): []

Maximum Packet Loss (%): 5.0 Maximum Forward Packet Loss (%): [] Maximum Reverse Packet Loss (%): []

Maximum Latency (msec): [] MOS Score: []

Low Delay Variation Low Latency Low Packet Loss

Low Forward Packet Loss Low Reverse Packet Loss

OK Cancel

Edit SLA Profile - 60ms-Delay

General SaaS App Monitor

Name: 60ms-Delay Tags: []

Description: []

Packet Delay Variation (Jitter): [] Circuit Transmit Utilization (%): [] Circuit Receive Utilization (%): []

Maximum Packet Loss (%): [] Maximum Forward Packet Loss (%): [] Maximum Reverse Packet Loss (%): []

Maximum Latency (msec): 60 MOS Score: []

Low Delay Variation Low Latency Low Packet Loss

Low Forward Packet Loss Low Reverse Packet Loss

OK Cancel

Edit SLA Profile - Low-Delay-Low-Packet-Loss

General SaaS App Monitor

Name: Low-Delay-Low-Packet-Loss Tags: []

Description: []

Packet Delay Variation (Jitter): [] Circuit Transmit Utilization (%): [] Circuit Receive Utilization (%): []

Maximum Packet Loss (%): [] Maximum Forward Packet Loss (%): [] Maximum Reverse Packet Loss (%): []

Maximum Latency (msec): [] MOS Score: []

Low Delay Variation Low Latency Low Packet Loss

Low Forward Packet Loss Low Reverse Packet Loss

OK Cancel

Edit SLA Profile - Low-Delay-Only

General SaaS App Monitor

Name: Low-Delay-Only Tags: []

Description: []

Packet Delay Variation (Jitter): [] Circuit Transmit Utilization (%): [] Circuit Receive Utilization (%): []

Maximum Packet Loss (%): [] Maximum Forward Packet Loss (%): [] Maximum Reverse Packet Loss (%): []

Maximum Latency (msec): [] MOS Score: []

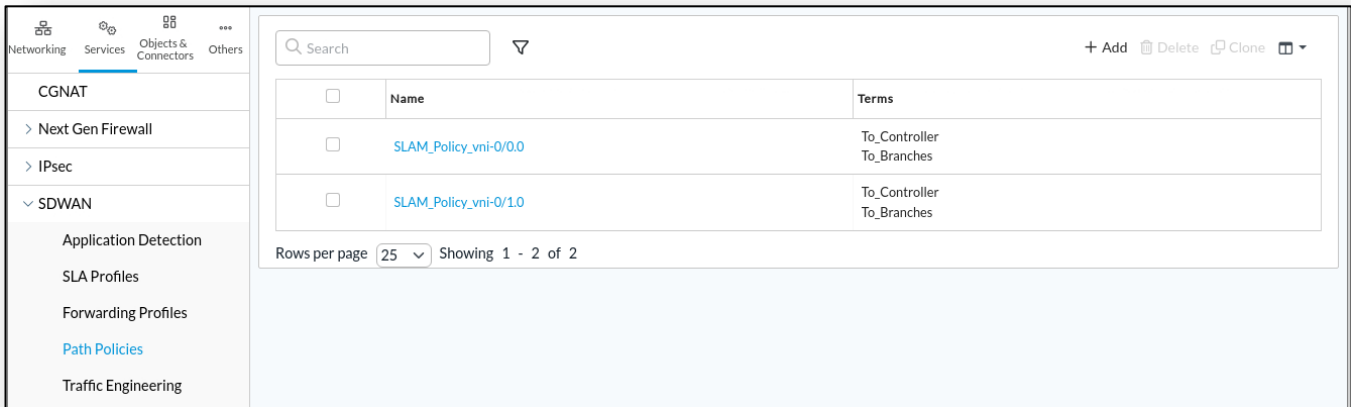
Low Delay Variation Low Latency Low Packet Loss

Low Forward Packet Loss Low Reverse Packet Loss

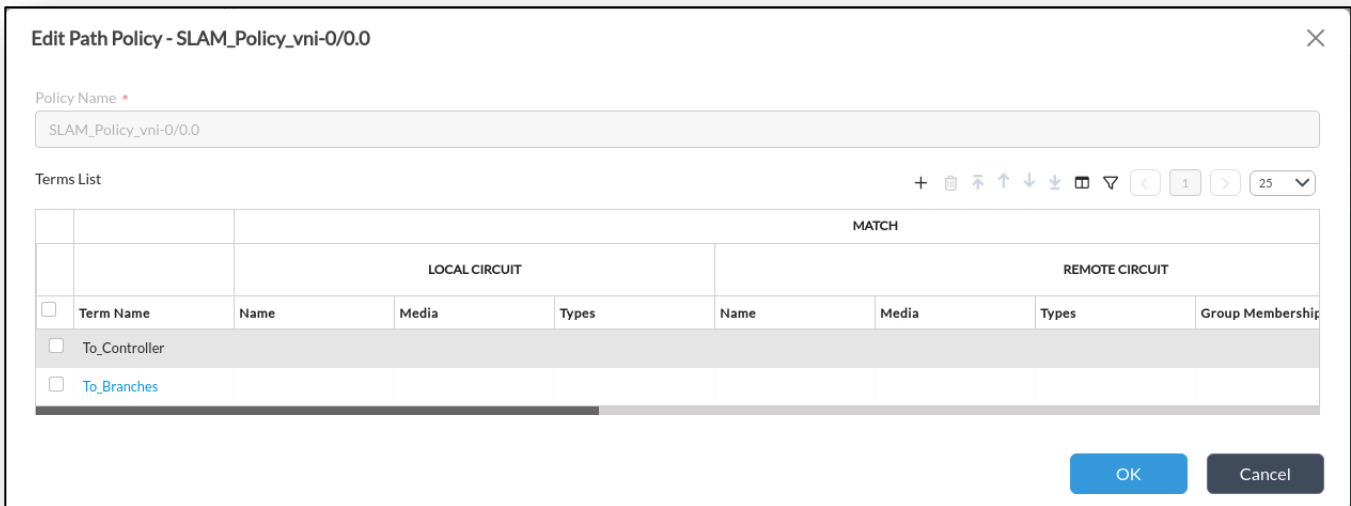
OK Cancel

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.

- 1.f. Navigate to *Configuration > Services > SDWAN > Path Policies* and locate the 2 default path policies.
- 1.g. Click on the *SLAM_Policy_vni-0/0.0* name to open the policy for editing.



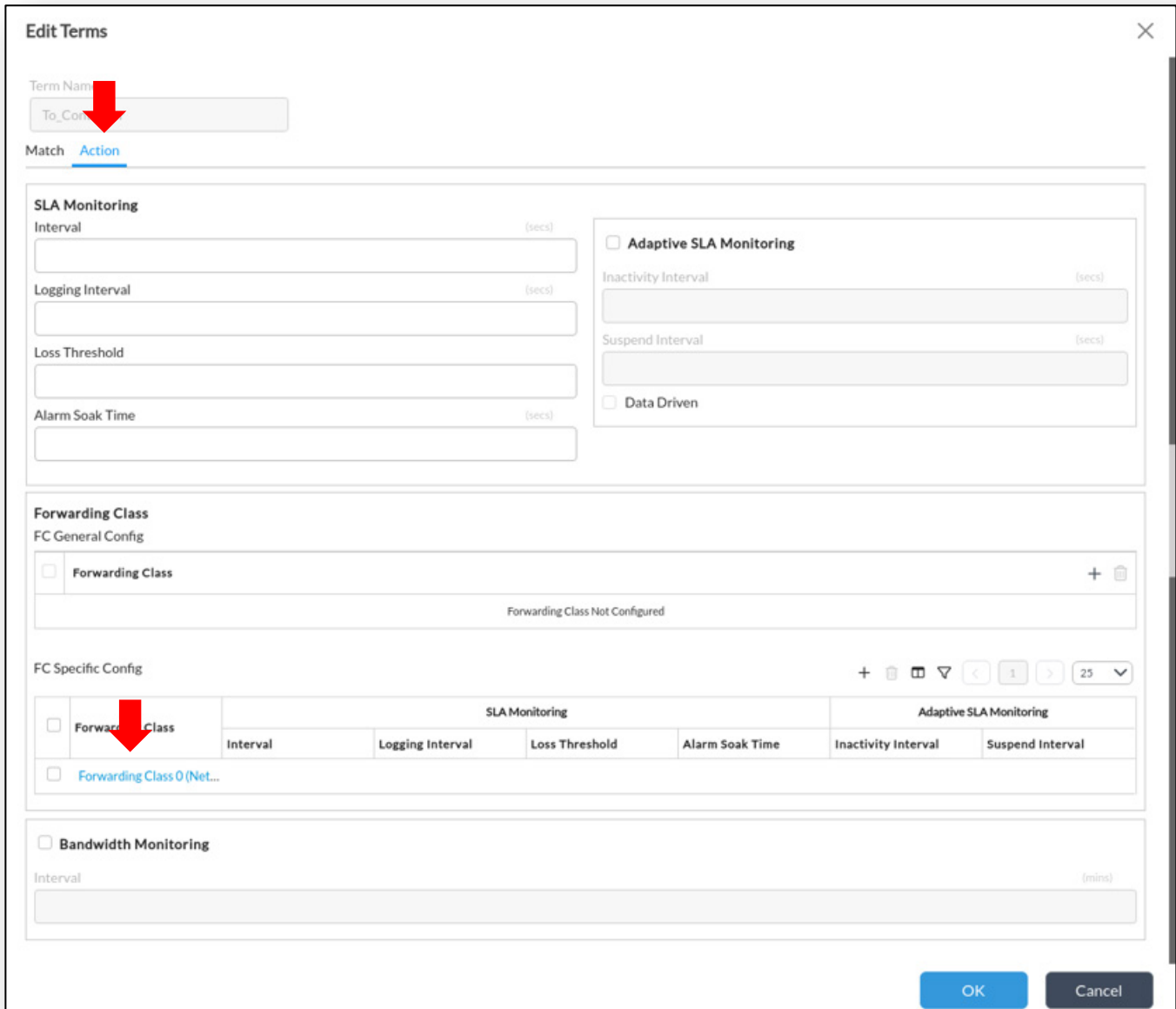
- 1.h. In the *SLAM_Policy_vni-0/0.0*, click the *To_Controller* term to open the term.



1.i. 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.

1.j. Open the *ForwardingClass 0* entry.



Edit Terms

Term Name:

Match: Action

SLA Monitoring

Interval (secs):

Logging Interval (secs):

Loss Threshold:

Alarm Soak Time (secs):

Adaptive SLA Monitoring

Inactivity Interval (secs):

Suspend Interval (secs):

Data Driven

Forwarding Class

FC General Config

Forwarding Class +

Forwarding Class Not Configured

FC Specific Config +

<input type="checkbox"/> Forwarding Class	SLA Monitoring				Adaptive SLA Monitoring	
	Interval	Logging Interval	Loss Threshold	Alarm Soak Time	Inactivity Interval	Suspend Interval
<input type="checkbox"/> Forwarding Class 0 (Net...						

Bandwidth Monitoring

Interval (mins):

The default timers are built into the system, so they don't appear in the configuration explicitly.

1.k. Modify the SLA Monitoring interval and set it to 20 seconds (20000ms).

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

Edit Terms Edit Forwarding Class Specific Config ✕

Forwarding Class *

SLA Monitoring

Interval (milliseconds) Logging Interval (secs)

Loss Threshold Alarm Soak Time (secs)

Adaptive SLA Monitoring

Inactivity Interval (secs) Suspend Interval (secs)

1.m. Click the *To_Branches* term to open and modify the term.

Edit Path Policy - SLAM_Policy_vni-0/0.0 ✕

Policy Name *

Terms List + ✕ ↕ ↑ ↓ 📄 🔍 < 1 > 25 ▾

		MATCH						
		LOCAL CIRCUIT			REMOTE CIRCUIT			
<input type="checkbox"/>	Term Name	Name	Media	Types	Name	Media	Types	Group Membership
<input type="checkbox"/>	To_Controller							
<input type="checkbox"/>	To_Branches							

- 1.n. 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).
- 1.o. Change the *Adaptive SLA Monitoring Inactivity Interval* to 30. The other values should be auto-populated.

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

		MATCH						
		LOCAL CIRCUIT			REMOTE CIRCUIT			
<input type="checkbox"/>	Term Name	Name	Media	Types	Name	Media	Types	Group Membership
<input type="checkbox"/>	To_Controller							
<input type="checkbox"/>	To_Branches							

1.r. Repeat steps g through q on the SLAM_Policy_vni-0/1.0 policy so that adaptive shaping is enabled on both WAN links.

Step 2. 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.

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

The screenshot shows the Versa Director interface for device Branch01. The 'Services' tab is active, and the 'SLA Metrics' sub-tab is selected. A dropdown menu is set to 'Hub'. Below the menu is a table with the following data:

Path Handle	Remote Site N...	Forward Class	Local WAN Link	Remote WAN ...	Local WAN Lin...	Remote WAN ...	Two Way Dela...	Forward Dela...	Rev Delay Var...	PDU Loss Rati...	Forward Loss ...	Rev Loss I
6623492	Hub	fc_ef	INET	INET	1	1	0	0	0	0.0	0.0	0.0
6627844	Hub	fc_ef	MPLS	MPLS	2	2	0	0	0	0.0	0.0	0.0

- 2.d. Select the *SLA Paths* tab to view the SLA probe status between sites.
- 2.e. In the *SLA Paths* dialog, select the *Hub* site from the dropdown menu to view the SLA probe status between your branch and the hub device. If the Adaptive Monitoring status is suspended, wait up to 30 seconds for adaptive monitoring to change to suspend mode. You can click the refresh button to update the display.

Note that the Adaptive Monitoring status should be suspend, meaning the probes are currently suspended to the remote site.

The screenshot shows the Versa Director interface for device Branch01, with the 'SLA Paths' sub-tab selected. A dropdown menu is set to 'Hub'. Below the menu is a table with the following data:

Path Handle	Remote Site N...	Forward Class	Local WAN Link	Remote WAN ...	Local WAN Lin...	Remote WAN ...	Path Mtu	Adaptive Mon...	Damp State	Damp Flaps	Connection St...	Flaps
6623492	Hub	fc_ef	INET	INET	1	1	1500	suspend	disable	0	up	1
6627844	Hub	fc_ef	MPLS	MPLS	2	2	1500	suspend	disable	0	up	1

- 2.f. Open the Remmina application and start an SSH session to your testing host device *Sxx Linux Testing Client*.
- 2.g. From the command line on the testing client, issue the `ping 10.27.13.10 -c 5` command to send 5 ICMP packets to the address 10.27.13.10 (the LAN gateway address on the hub site).
- 2.h. Return to the Versa Director SLA Paths monitoring window.
- 2.i. Refresh the table by selecting a different site from the site dropdown menu, then select the Hub 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	Remote Site N...	Forward Class	Local WAN Link	Remote WAN ...	Local WAN Lin...	Remote WAN ...	Path Mtu	Adaptive Mon...	Damp State	Damp Flaps	Connection St...	Flaps
6623492	Hub	fc_ef	INET	INET	1	1	1500	active	disable	0	up	1
6627844	Hub	fc_ef	MPLS	MPLS	2	2	1500	active	disable	0	up	1

- 2.j. Wait 30 seconds, then refresh the table. The MPLS link Adaptive Monitoring status should return to suspend state.

Path Handle	Remote Site N...	Forward Class	Local WAN Link	Remote WAN ...	Local WAN Lin...	Remote WAN ...	Path Mtu	Adaptive Mon...	Damp State	Damp Flaps	Connection St...	Flaps
6623492	Hub	fc_ef	INET	INET	1	1	1500	suspend	disable	0	up	1
6627844	Hub	fc_ef	MPLS	MPLS	2	2	1500	suspend	disable	0	up	1



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

APPLICATION STEERING AND SLA 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.

In this lab, you will be assigned a student ID (Student01, Student02, etc.) Each student environment is a tenant on Versa Director and has access to 2 VOS devices and a shared hub. You will perform your operations on the VOS devices.

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.

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!

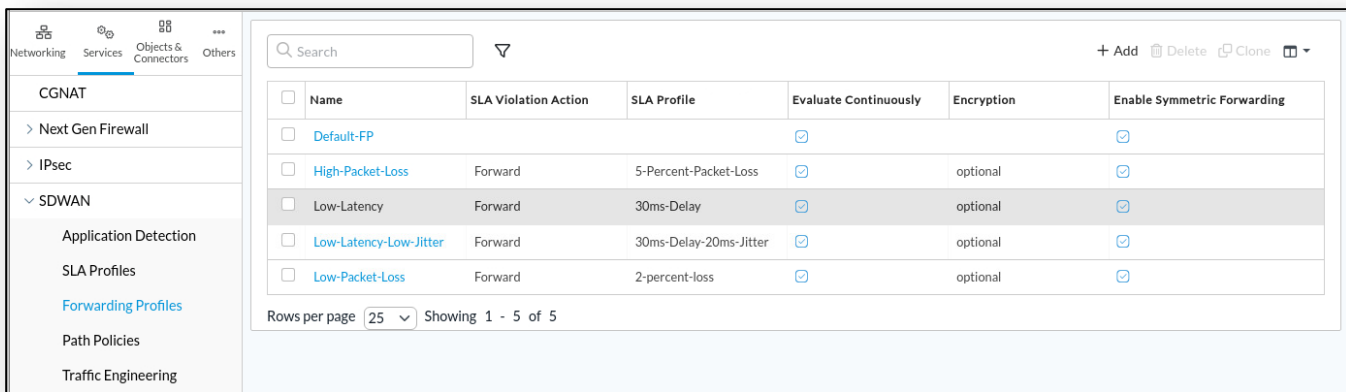
In this lab you will configure SD-WAN Forwarding Profiles set link and path preferences for traffic.

To begin, if you plan to use path statistics to help determine forwarding paths, create SLA profiles that analyze the desired performance statistics. This step should have been completed.

Forwarding profiles create lists of links that will be used to forward traffic. The priority or preference of the links can be influenced or changed by the statistics gathered by the SLA probes. You will create one forwarding profile for each category or type of traffic.

By default, a Default-FP forwarding profile is created. You will add the following forwarding profiles to the device:

- Low-Latency: For traffic that requires low latency links.
- Low-Latency-Low-Jitter: For traffic that requires low latency and low jitter on links.
- Low-Packet-Loss: For traffic that requires low packet loss.
- High-Packet-Loss: For traffic that can tolerate high packet loss.



<input type="checkbox"/>	Name	SLA Violation Action	SLA Profile	Evaluate Continuously	Encryption	Enable Symmetric Forwarding
<input type="checkbox"/>	Default-FP			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
<input type="checkbox"/>	High-Packet-Loss	Forward	5-Percent-Packet-Loss	<input checked="" type="checkbox"/>	optional	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Low-Latency	Forward	30ms-Delay	<input checked="" type="checkbox"/>	optional	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Low-Latency-Low-Jitter	Forward	30ms-Delay-20ms-Jitter	<input checked="" type="checkbox"/>	optional	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Low-Packet-Loss	Forward	2-percent-loss	<input checked="" type="checkbox"/>	optional	<input checked="" type="checkbox"/>

Rows per page 25 Showing 1 - 5 of 5

- 2.a. In Versa Director, click on the *Appliance View* tab at the top of the user interface.
- 2.b. Select your *SxxB01* branch device from the appliance table.
- 2.c. In the *Appliance View* of your *SxxB01* device, click on the *Configuration* tab to open the device configuration.
- 2.d. In the device configuration, navigate to *Services > SDWAN > Forwarding Profiles*.
- 2.e. Click + Add to create a new forwarding profile.

2.f. In the General tab, configure the following parameters:

- Name: Low-Latency
- SLA Profile: 30ms-Delay

Leave other properties at their default values.

Edit Forwarding Profile - Low-Latency

General | Circuit Priorities | FEC | Advanced Settings | Nexthop

Name *
Low-Latency

Tags

Description

SLA Profile: 30ms-Delay

Encryption: Optional

Connection Selection Method: Weighted Round Robin

Recompute Timer (seconds): 300

Path Reconsider Interval (seconds)

SLA Violation Action: Forward

Load Balancing Option: --Select--

Header Compression
Level: Low

Skip HMAC

Replication
 Enable

Replication Factor

Start When: Always

OK Cancel

2.g. Navigate to the *Circuit Priorities* tab

2.h. In the *Circuit Priorities* tab, click the + button to add circuits.

2.i. In the *Add Circuit Priorities* box, set Priority to 1.

2.j. In the *Circuit Names* tab, click + and add both the INET and MPLS circuits. They will have the same priorities.

Edit Forwarding Profile - Low-Latency

General | **Circuit Priorities** | FEC | Advanced Settings | Nexthop

Unmatched Priority: Avoid

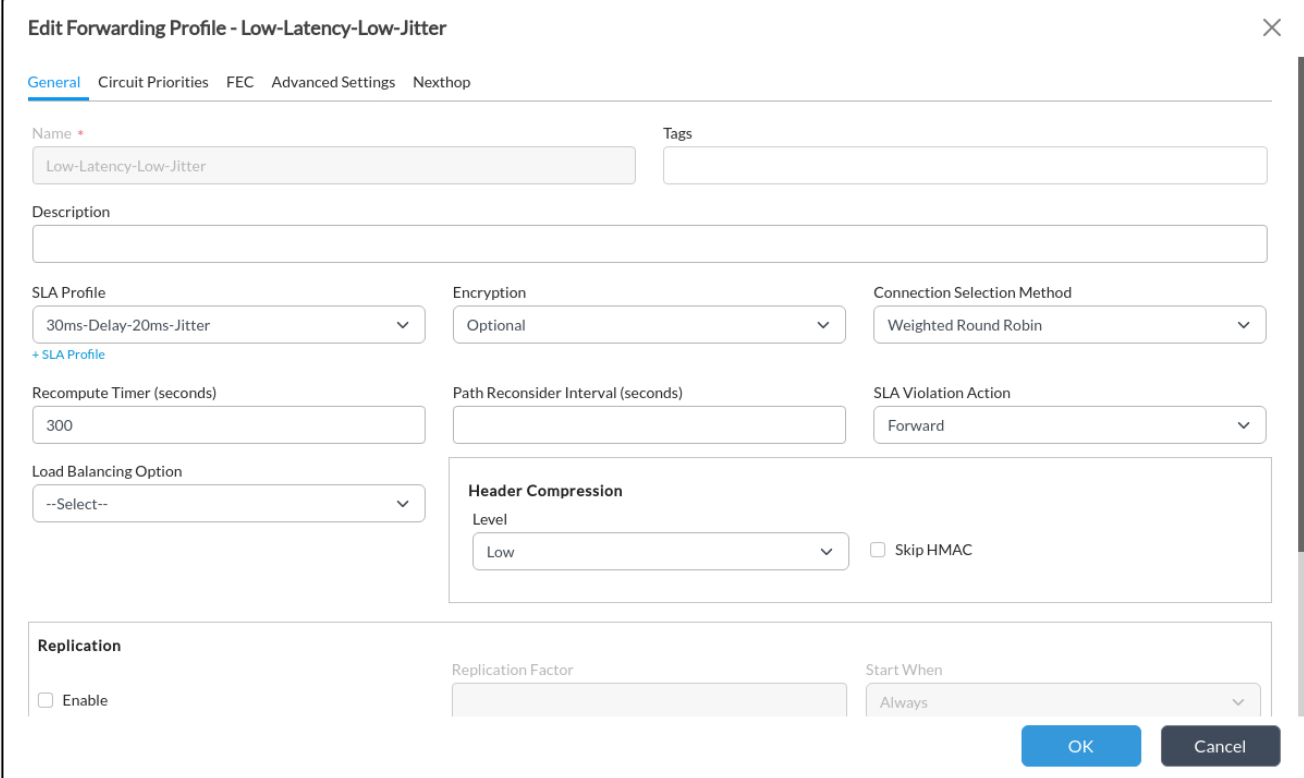
Circuit Priorities List

Priority	Description	Circuit Names		Circuit Types		Circuit Media	
		Local	Remote	Local	Remote	Local	Remote
<input type="checkbox"/> 1		INET	MPLS				

OK Cancel

- 2.k. Click *OK* to finish adding circuits.
- 2.l. Click *OK* on the Forwarding Profile window to finish the configuration of the forwarding profile.
- 2.m. In the Forwarding Profiles window, click the + *Add* button to add another forwarding profile.
- 2.n. In the General tab, configure the following parameters:
 - Name: Low-Latency-Low-Jitter
 - SLA Profile: 30ms-Delay-20ms-Jitter

Leave other properties at their default values.



- 2.o. Navigate to the *Circuit Priorities* tab
- 2.p. In the *Circuit Priorities* tab, click the + button to add circuits.
- 2.q. In the *Add Circuit Priorities* box, set Priority to 1.
- 2.r. In the *Circuit Names* tab, click + and add both the *INET* and *MPLS* circuits. They will have the same priorities.
- 2.s. Click *OK* to finish adding circuits.
- 2.t. Click *OK* on the *Forwarding Profile* window to finish the configuration of the forwarding profile.

Edit Forwarding Profile - Low-Latency-Low-Jitter

General **Circuit Priorities** FEC Advanced Settings Nexthop

Unmatched Priority: --Select--

Circuit Priorities List

Priority	Description	Circuit Names		Circuit Types		Circuit Media	
		Local	Remote	Local	Remote	Local	Remote
1	INET MPLS						

OK Cancel

2.u. In the Forwarding Profiles window, click the + Add button to add another forwarding profile.

2.v. In the General tab, configure the following parameters:

- Name: Low-Packet-Loss
- SLA Profile: 2-percent-loss

Leave other properties at their default values.

Edit Forwarding Profile - Low-Packet-Loss

General **Circuit Priorities** FEC Advanced Settings Nexthop

Name * Low-Packet-Loss Tags

Description

SLA Profile: 2-percent-loss Encryption: Optional Connection Selection Method: Weighted Round Robin

Recompute Timer (seconds): 300 Path Reconsider Interval (seconds): SLA Violation Action: Forward

Load Balancing Option: --Select--

Header Compression
Level: Low Skip HMAC

Replication
 Enable Replication Factor: Start When: Always

OK Cancel

2.w. Navigate to the *Circuit Priorities* tab

- 2.x. In the *Circuit Priorities* tab, click the + button to add circuits.
- 2.y. In the *Add Circuit Priorities* box, set *Priority* to 1.
- 2.z. In the *Circuit Names* tab, click + and add the *MPLS* circuit. Click *OK* to finish adding the circuit.
- 2.aa. In the *Add Forwarding Profile > Circuit Priorities* dashboard, click + to add another circuit.
- 2.ab. In the *Add Circuit Priorities* box, set the *Priority* to 2.
- 2.ac. In the *Circuit Names* tab, click + and add the *INET* circuit. Click *OK* to finish adding the circuit.
- 2.ad. Click *OK* on the *Forwarding Profile* window to finish the configuration of the forwarding profile.

Edit Forwarding Profile - Low-Packet-Loss ✕

General Circuit Priorities FEC Advanced Settings Nexthop

Unmatched Priority

Circuit Priorities List + 🗑️ 📄 🔍 < 1 > 25 ▾

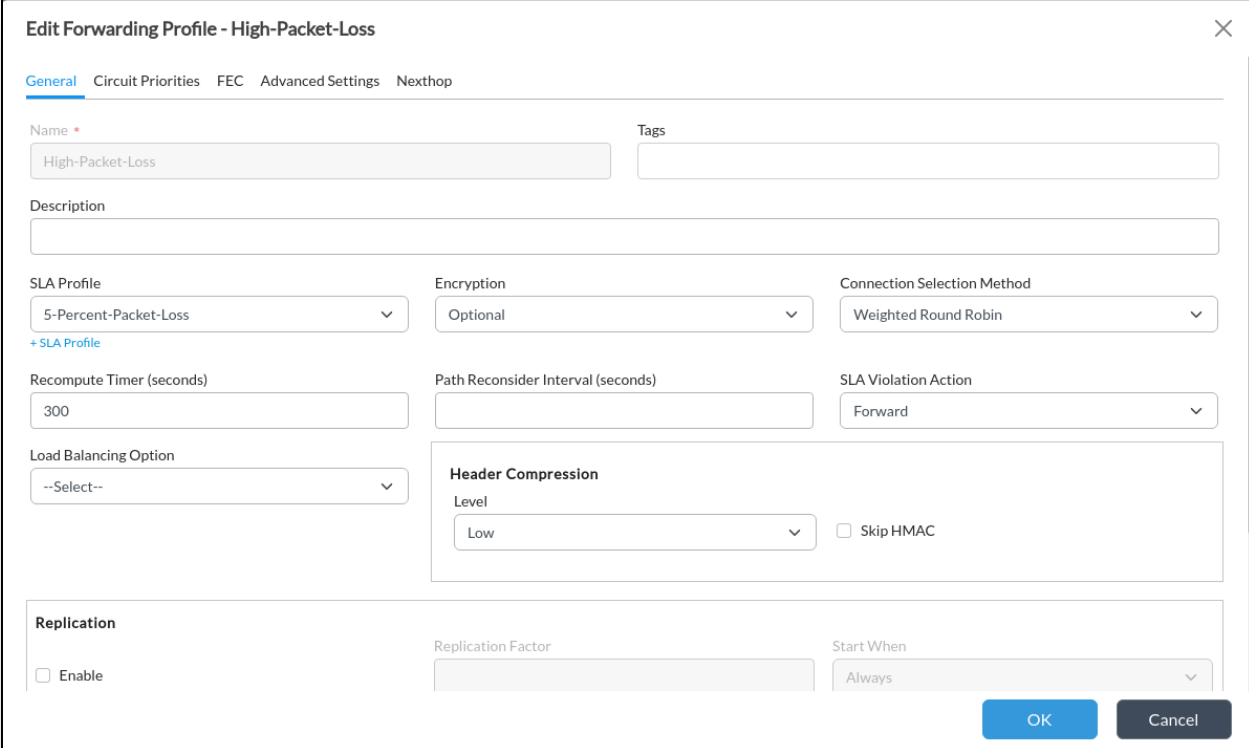
	Priority	Description	Circuit Names		Circuit Types		Circuit Media	
			Local	Remote	Local	Remote	Local	Remote
<input type="checkbox"/>	1		MPLS					
<input type="checkbox"/>	2		INET					

2.ae. In the Forwarding Profiles window, click the + Add button to add another forwarding profile.

2.af. In the General tab, configure the following parameters:

- Name: High-Packet-Loss
- SLA Profile: 5-Percent-Packet-Loss

Leave other properties at their default values.



2.ag. Navigate to the *Circuit Priorities* tab

2.ah. In the *Circuit Priorities* tab, click the + button to add circuits.

2.ai. In the *Add Circuit Priorities* box, set Priority to 1.

2.aj. In the *Circuit Names* tab, click + and add the MPLS and INET circuits. Click *OK* to finish adding the circuits.

2.ak. Navigate to the *FEC* tab.

2.al. In the *FEC* tab, check the *Enable* box. Leave all values at their default settings.

2.am. Click *OK* on the *Forwarding Profile* window to finish the configuration of the forwarding profile.

Edit Forwarding Profile - High-Packet-Loss

General **Circuit Priorities** FEC Advanced Settings Nexthop

Unmatched Priority
--Select--

Circuit Priorities List

Priority	Description	Circuit Names		Circuit Types		Circuit Media	
		Local	Remote	Local	Remote	Local	Remote
<input type="checkbox"/> 1	INET MPLS						

OK Cancel

Edit Forwarding Profile - High-Packet-Loss

General Circuit Priorities **FEC** Advanced Settings Nexthop

Sender

Enable

Duplicate FEC Packet: disable

FEC Packet: Alternate Circuit

Maximum FEC Packet Size: 1400

Number of Packets per FEC: 4

Start When: SLA Violated

Stop When

Receiver

Maximum FEC Packet Size: 1400

Recovery

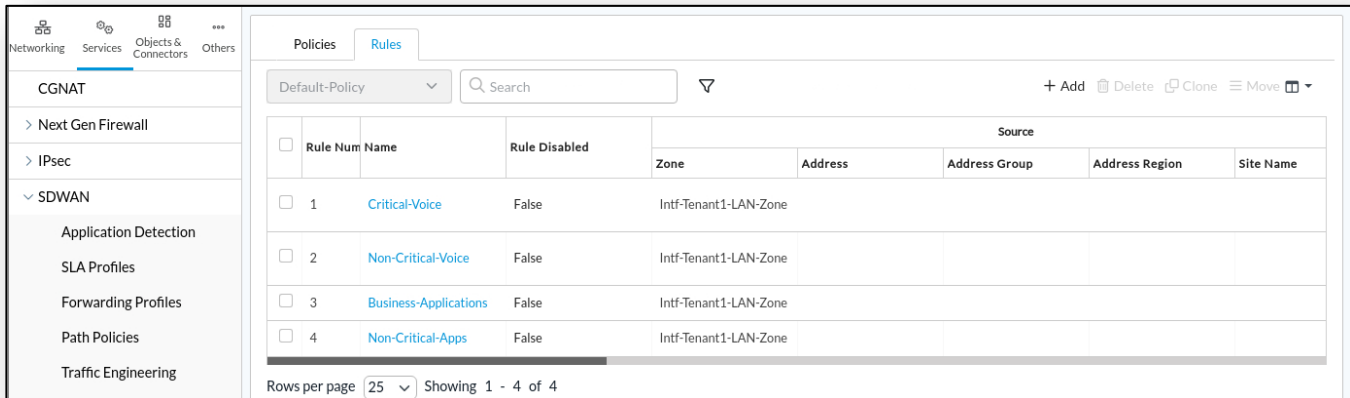
Preserve Order

OK Cancel

Step 3. Define SD-WAN Policy Rules for Traffic Steering and Circuit Assignments

Next you define the SD-WAN Rules. These analyze new sessions and assign them to one of the forwarding profiles based on the traffic requirements.

Note: The rules in this example are for EXAMPLE purposes only to show the functionality and behavior of SD-WAN policies. Every network environment has specific requirements unique to the goals of that environment, and the examples shown are for demonstration purposes only.



In the following steps you will create 4 traffic steering (SD-WAN Policy) rules. The rule names are:

- Critical-Voice
- Non-Critical-Voice
- Business-Applications
- Non-Critical-Apps

3.a. Rule 1: Critical Voice

3.b. In your Sxx-B01 Appliance View, navigate to Configuration > Services > SDWAN > Policies.

3.c. In the Policies dashboard, click on the Rules tab to open the Rules dashboard.

In the Rules dashboard, click the + Add button to add the following rules:

Rule Name: Critical-Voice

Source Tab:

- Source Zone: Intf-Studentxx_LAN-Zone (Click + to add)

Applications Tab:

- VOIP
- MS_TEAMS
- SIP
- SIP_SOAP

Enforce Tab:

- Action: Allow Flow
- Forwarding Profile: Low-Latency-Low-Jitter

Rule Name: Non-Critical-Voice

Source Tab:

- Source Zone: Intf-Studentxx_LAN-Zone (Click + to add)

Applications Tab:

- Audio-Video-Streaming
- YOUTUBE
- ZOOM

Enforce Tab:

- Action: Allow Flow
- Forwarding Profile: Low-Latency

Rule Name: Business-Applications

Source Tab:

- Source Zone: Intf-Studentxx_LAN-Zone (Click + to add)

Applications Tab:

- SaaS Application Groups:
 - Concur-Apps
 - GotoMeeting-Apps
 - Office365-Apps

Enforce Tab:

- Action: Allow Flow
- Forwarding Profile: Low-Packet-Loss

Rule Name: Non-Critical-Apps

Source Tab:

- Source Zone: Intf-Studentxx_LAN-Zone (Click + to add)

URL Tab:

- entertainment_and_arts
- news_and_media
- social_network
- sports

Enforce Tab:

- Action: Allow Flow
- Forwarding Profile: High-Packet-Loss

Example Rule

Add Rules ✕

General Source Destination Headers/Schedule Applications URL IoT Security Users/Groups Forwarding Class Enforce

Name *

Description

Disable Rule

Add Rules

General Source Destination Headers/Schedule Applications URL IoT Security Users/Groups Forwarding Class Enforce

<p><input type="checkbox"/> Source Zone + New Zone + [trash] [refresh]</p> <p><input type="checkbox"/> Intf-Student_LAN-Zone [eye]</p> <p><input type="checkbox"/> Source Address Negate</p> <p><input type="checkbox"/> Region + [trash] [refresh]</p> <p style="text-align: center;">Region Not Configured</p> <p><input type="checkbox"/> Source Location Negate</p> <p><input type="checkbox"/> Custom Geo Circle + [trash] [refresh]</p> <p style="text-align: center;">Custom Geo Circle Not Configured</p>	<p><input type="checkbox"/> Source Address</p> <p style="text-align: right;">Source Address Not Configured</p> <p><input type="checkbox"/> State</p> <p style="text-align: right;">State Not Configured</p> <p><input type="checkbox"/> EIP Profiles</p> <p style="text-align: right;">EIP Profiles Not Configured</p>
--	---

Edit Rules - Critical-Voice

General Source Destination Headers/Schedule **Applications** URL Users/Groups Forwarding Class Enforce

Applications

<input type="checkbox"/>	Application List	+ New Application + New Filter + New Group +
<input type="checkbox"/>	VOIP	
<input type="checkbox"/>	MS_TEAMS	
<input type="checkbox"/>	SIP	
<input type="checkbox"/>	SIP_SOAP	

SaaS Application Groups

<input type="checkbox"/>	SaaS Application Group List	+
SaaS Application Group List Not Configured		

OK
Cancel

Edit Rules - Critical-Voice

General Source Destination Headers/Schedule Applications URL Users/Groups Forwarding Class **Enforce**

Forwarding

Action * Allow Flow Forwarding Profile Low-Latency-Low-Jitter

View Forwarding Profile

NextHop IP Address IP Address Routing Instance --Select--

Enable Symmetric Forwarding of Return Traffic Enable Symmetric L2 Forwarding of Return Traffic

Logging

LEF Profile --Select-- Default Profile

Event Never Rate Limit 10

Monitor

Address IP Address Routing Instance --Select--

Action --Select-- Interval(seconds)

Threshold(Events)

TCP Optimization

Bypass Latency Threshold (msec) Mode --Select--

LAN Profile --Select-- WAN Profile --Select--

OK
Cancel

When you have finished adding the rules you can view the path information and statistics from the VOS command line interface.

- 3.d. In the remote desktop, open the Remmina application.
- 3.e. In the Remmina application, open the SSH session to your SxxB01 device. If prompted, the username is *admin* and the password is *versa123*.
- 3.f. From the VOS shell, enter the *cli* command to start the command line interface.
- 3.g. From the VOS cli, issue the *show orgs org-services Studentxx sd-wan path path-metrics* command, where *Studentxx* is the student ID assigned to you.

```
user@device-cli> show orgs org-services org-name sd-wan path path-metrics
```

REMOTE BRANCH	LOCAL CIRCUIT	REMOTE CIRCUIT	TWO WAY DELAY	FWD DELAY VAR	REV DELAY VAR	FWD LOSS PERCENTAGE	REV LOSS PERCENTAGE	PDU LOSS PERCENTAGE	RX BYTES	TX BYTES	VOICE MOS	AUDIO MOS	VIDEO MOS
Controller01	INET	INET	2	1	0	0.00	0.00	0.00	12626696	16967856	0.00	0.00	0.00
	MPLS	MPLS	2	0	0	0.00	0.00	0.00	157877844	306469548	0.00	0.00	0.00
Hub105	INET	INET	0	0	0	0.00	0.00	0.00	12919004	12919004	0.00	0.00	0.00
	MPLS	MPLS	0	2	0	0.00	0.00	0.00	12921460	12921452	0.00	0.00	0.00
branch111	INET	INET	0	0	0	0.00	0.00	0.00	11127852	11128596	0.00	0.00	0.00
	MPLS	MPLS	1	0	0	0.00	0.00	0.00	11129524	11128796	0.00	0.00	0.00
branch112	INET	INET	0	0	0	0.00	0.00	0.00	11129244	11130236	0.00	0.00	0.00
	MPLS	MPLS	1	0	0	0.00	0.00	0.00	11132096	11131120	0.00	0.00	0.00
branch113	INET	INET	1	0	0	0.00	0.00	0.00	11126700	11126036	0.00	0.00	0.00
	MPLS	MPLS	0	0	0	0.00	0.00	0.00	11127256	11128264	0.00	0.00	0.00
branch114	INET	INET	0	0	0	0.00	0.00	0.00	11127924	11128668	0.00	0.00	0.00
	MPLS	MPLS	1	0	0	0.00	0.00	0.00	11130348	11129604	0.00	0.00	0.00
branch115	INET	INET	0	0	0	0.00	0.00	0.00	11124408	11124956	0.00	0.00	0.00
	MPLS	MPLS	0	0	0	0.00	0.00	0.00	11126472	11126816	0.00	0.00	0.00

- 3.h. From the VOS cli, issue the *show orgs org-services Studentxx sd-wan policies Default-Policy rules path-state brief* command, where *Studentxx* is the student ID assigned to you.

```
user@device-cli> show orgs org-services org-name sd-wan policies Default-Policy rules path-state brief
```

NAME	REMOTE BRANCH	FORWARDING PROFILE	SLA PROFILE	LOCAL CIRCUIT	REMOTE CIRCUIT	FORWARDING CLASS	PRIORITY	
Critical-Voice	Controller01	Low-Latency-Low-Jitter	Latency-50-Jitter-20	INET	INET	fc_nc	Priority 1	
	Hub105	Low-Latency-Low-Jitter	Latency-50-Jitter-20	MPLS	MPLS	fc_nc	Priority 1	
	branch111	Low-Latency-Low-Jitter	Latency-50-Jitter-20	INET	INET	fc_ef	Priority 1	
	branch111	Low-Latency-Low-Jitter	Latency-50-Jitter-20	MPLS	MPLS	fc_ef	Priority 1	
	branch112	Low-Latency-Low-Jitter	Latency-50-Jitter-20	INET	INET	fc_ef	Priority 1	
	branch112	Low-Latency-Low-Jitter	Latency-50-Jitter-20	MPLS	MPLS	fc_ef	Priority 1	
	branch113	Low-Latency-Low-Jitter	Latency-50-Jitter-20	INET	INET	fc_ef	Priority 1	
	branch113	Low-Latency-Low-Jitter	Latency-50-Jitter-20	MPLS	MPLS	fc_ef	Priority 1	
	branch114	Low-Latency-Low-Jitter	Latency-50-Jitter-20	INET	INET	fc_ef	Priority 1	
	branch114	Low-Latency-Low-Jitter	Latency-50-Jitter-20	MPLS	MPLS	fc_ef	Priority 1	
	branch115	Low-Latency-Low-Jitter	Latency-50-Jitter-20	INET	INET	fc_ef	Priority 1	
	branch115	Low-Latency-Low-Jitter	Latency-50-Jitter-20	MPLS	MPLS	fc_ef	Priority 1	
	Non-Critical-Voice-Video	Controller01	Low-Latency	Latency-30ms	INET	INET	fc_nc	Priority 2
		Hub105	Low-Latency	Latency-30ms	MPLS	MPLS	fc_nc	Priority 1
		branch111	Low-Latency	Latency-30ms	INET	INET	fc_ef	Priority 2
branch111		Low-Latency	Latency-30ms	MPLS	MPLS	fc_ef	Priority 1	
branch112		Low-Latency	Latency-30ms	INET	INET	fc_ef	Priority 2	
branch112		Low-Latency	Latency-30ms	MPLS	MPLS	fc_ef	Priority 1	
branch113		Low-Latency	Latency-30ms	INET	INET	fc_ef	Priority 2	
branch113		Low-Latency	Latency-30ms	MPLS	MPLS	fc_ef	Priority 1	
branch114		Low-Latency	Latency-30ms	INET	INET	fc_ef	Priority 2	
branch114		Low-Latency	Latency-30ms	MPLS	MPLS	fc_ef	Priority 1	
branch115		Low-Latency	Latency-30ms	INET	INET	fc_ef	Priority 2	
branch115		Low-Latency	Latency-30ms	MPLS	MPLS	fc_ef	Priority 1	

You can see the current circuit priority between sites. This is the link that will be used to forward traffic for each of the forwarding profiles. If multiple circuits have the same priority, traffic will be load balanced across the links.



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

BGP ROUTING PROTOCOL

In this lab exercise you will configure the BGP routing protocol. Although the lesson focused on BGP configuration on the LAN interface, in this lab exercise you will configure BGP between the two branch devices on the INET WAN link. The configuration processes for BGP are interface independent, meaning the same process is used regardless of what interface or virtual router is used.

In this lab exercise you will:

- Configure an EBGP session in the B01 device INET WAN router to connect to the B02 device INET WAN router.
- Ensure that DIA is configured on the B01 device so that the LAN route is advertised between the LAN and INET WAN virtual routers.
- Verify that the routes in the B01 MPLS virtual router are advertised to branch B02.
- Create a BGP export policy on the B01 device to filter (block) the default route that is advertised to B02.
- Verify that the BGP export policy blocks the appropriate route.
- Reset the devices to the default lab configuration.

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.

In this lab, you will be assigned a student ID (Student01, Student02, etc.) Each student environment is a tenant on Versa Director and has access to 2 VOS devices and a shared hub. You will perform your operations on the VOS devices.

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.

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.

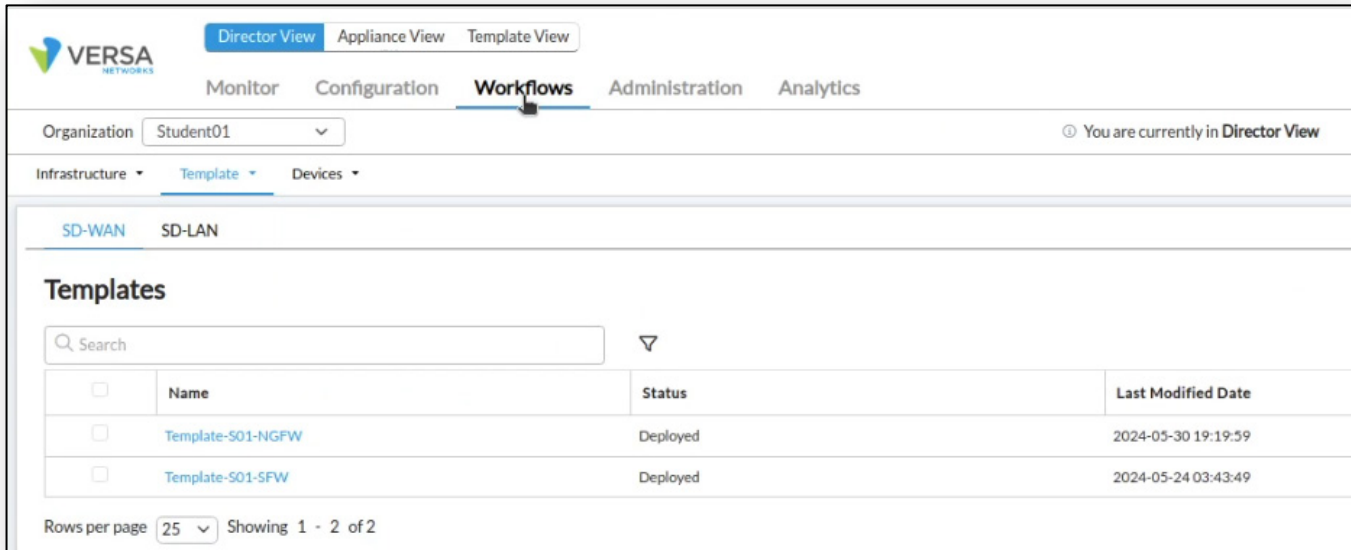
This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

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.

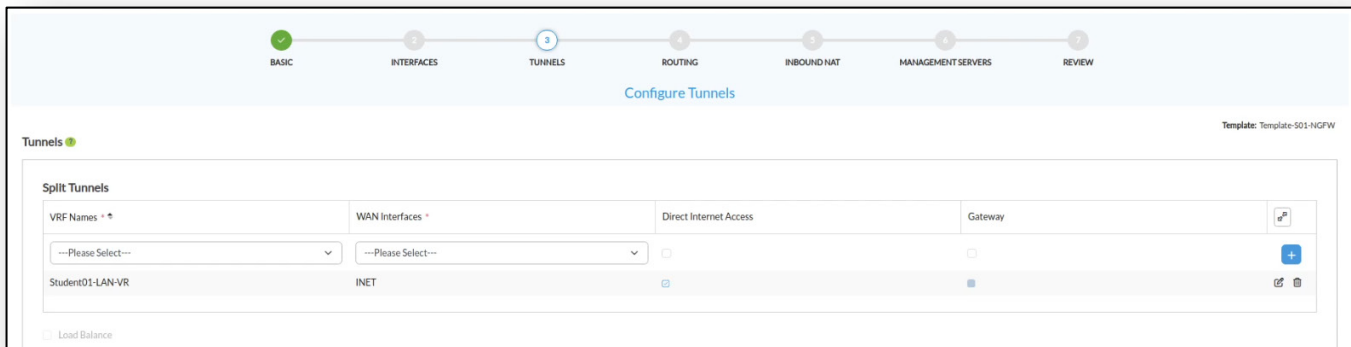
Now that we've discussed what is expected, let's get started!

Step 1. Verify DIA is Configured

- 1.a. The first step is to verify that DIA is configured on the B01 device. When DIA is configured, an EBGP session is automatically created between the LAN VRF and the INET Virtual Router.
- 1.b. Open Versa Director on your remote desktop.
- 1.c. Navigate to *Director View* > *Workflows* > *Template* > *Templates*.
- 1.d. In the *Templates Workflows* menu, locate the *Template-Sxx-NGFW* workflow, where Sxx is your student ID, and open the workflow.



- 1.e. In the *Template-Sxx-NGFW* workflow, navigate to the *Tunnels* step and verify that a DIA tunnel is created between your student LAN-VR and the INET WAN interface.



- 1.f. If a DIA tunnel does NOT exist between the student LAN-VR and the INET WAN interface, create the DIA connection, re-deploy the workflow, and commit the NGFW template to your devices before you continue. If a DIA tunnel already exists, click *Cancel* to exit the workflow and continue with the lab exercises.

Step 2. Create a BGP Session on B01

Next you will create a BGP session on your *B01* device. The session will be created in the INET virtual router.

- 2.a. Navigate to *Director View > Administration > Appliances* and locate your B01 device in the *Appliances* table. Alternatively, you can click on the *Appliance View* tab at the top of the user interface.
- 2.b. Click on the B01 device to open the *Appliance View* of the B01 device.

The screenshot shows the Versa Networks Director View interface. The 'Administration' tab is selected, and the 'Appliances' section is active. A table lists three appliances: S01B01, S01B02, and SP-HUB-1. A modal window is open for S01B01, displaying the following details:

Name	S01B01
Location	San Diego, CA, USA
Site ID	101
Serial Number	SN-S01B01
Model	c5.2xlarge
Services	sdwan,nextgen-firewall,cgnat
Time Created	2024-05-24 04:42:09.68
Template Status	IN_SYNC

Below the modal, a table shows the appliance's configuration:

Tags	Type
	Branch
	Branch
	Branch

- 2.c. In the *Appliance View* of your B01 device, navigate to *Configuration > Networking > Virtual Routers* dashboard.
- 2.d. Locate the *INET-Transport-VR* virtual router.
- 2.e. Click on the *INET-Transport-VR* virtual router to open the configuration dialog.

The screenshot shows the Versa Networks Director View interface for the 'Appliance View' of device S01B01. The 'Configuration' tab is selected, and the 'Virtual Routers' section is active. A table lists four virtual routers:

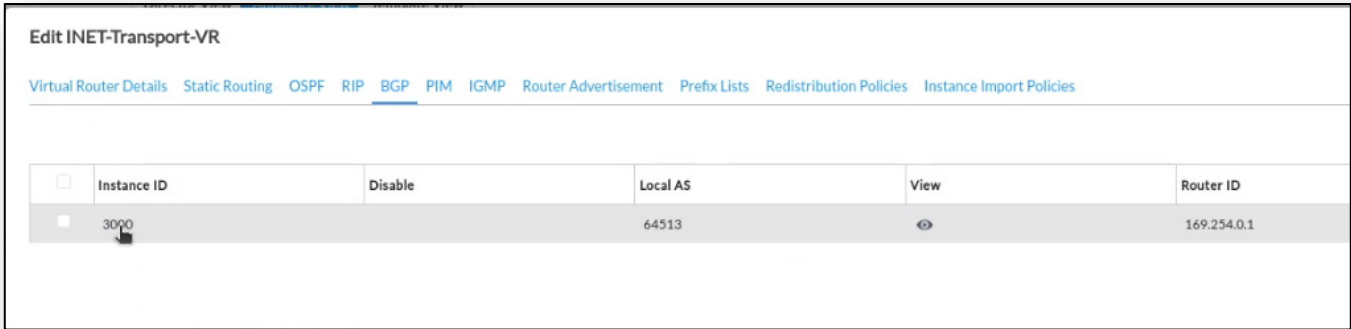
Name	View	Interfaces	Networks	Static Routes
INET-Transport-VR		tvi-0/602.0	INET	0.0.0.0/0
MPLS-Transport-VR			MPLS	0.0.0.0/0
Student01-Control-VR		ptvi514 tvi-0/4.0 tvi-0/5.0		
Student01-LAN-VR		tvi-0/603.0	Student_LAN	

The interface also shows a search bar and a 'Rows per page' dropdown set to 25, displaying 'Showing 1 - 4 of 4'.

2.f. In the *INET-Transport-VR*, click on the *BGP* tab to view the BGP instance configured on the device.

This BGP instance was created by the DIA configuration. A single BGP routing instance is available in the virtual router, but the single instance can manage all BGP peering sessions within the virtual router.

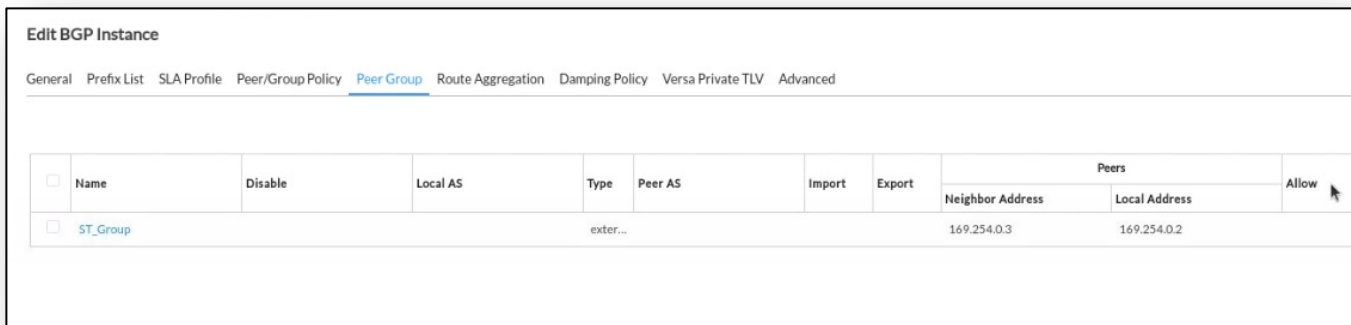
2.g. Click on the BGP instance ID to open the BGP instance.



<input type="checkbox"/>	Instance ID	Disable	Local AS	View	Router ID
<input checked="" type="checkbox"/>	3000		64513		169.254.0.1

2.h. In the BGP instance settings, click on the *Peer Group* tab to open the peer groups.

This is where you will create a new peer group, where the neighbor to the B02 device will be configured.



<input type="checkbox"/>	Name	Disable	Local AS	Type	Peer AS	Import	Export	Peers		Allow
								Neighbor Address	Local Address	
<input checked="" type="checkbox"/>	ST_Group			exter...				169.254.0.3	169.254.0.2	

2.i. In the *Peer Group* window, click the + button to create a new peer group. Name the peer group *BGP-LAB*. Enter the following parameters in the peer group:

- Name: BGP-LAB
- Type: EBGp
- Peer AS: 65002
- Local AS: 65001
- Local Address: vni-0/0.0

An example configuration is below.

Edit BGP Instance Add Peer Group ✕

Name *

Type

Hold Time (seconds)

Local Network Name

Suppress Peer AS
 Fast External Fallover

Description

Peer AS

TTL

Local AS

Relax First AS Check
 Disable Graceful Restart

Local Address

Disable 🟡

Password

Local AS Mode

Soft Reconfiguration
 Disable Extended Message Length Capability

AS Origination Interval

Weight

Next Hop UnChanged

General Neighbors Allow Advanced

Family ⬆	Loop Count	Prefix Limit		Restart Interval	Action	Soft Reconfiguration	Next Hop UnChanged	
		Maximum	Threshold					
<input type="text" value="--Select--"/>	Allowed Range is 1 - 2	Allowed Range is 1 - 2	Allowed Range is 1 - 1	Allowed Range is 30 -	<input type="text" value="--Select--"/>	<input type="checkbox"/> Soft Reconfiguration	<input type="checkbox"/> Next Hop UnChange	+

No Entries Added

2.j. Click on the *Neighbors* tab.

2.k. Click the + button to add a new BGP neighbor.

General **Neighbors** Allow Advanced

🗑️ 📄 📄 🔍 1 25

<input type="checkbox"/>	Neighbor IP	Disable	Local AS	Peer AS	Local Address	Import	Export	Local AS Mode
No Neighbor RECORD Added								

2.1. Enter the Neighbor IP address according to the chart below:

Student	Neighbor IP Address	Student	Neighbor IP Address
S01	10.27.11.102	S11	10.27.11.122
S02	10.27.11.104	S12	10.27.11.124
S03	10.27.11.106	S13	10.27.11.126
S04	10.27.11.108	S14	10.27.11.128
S05	10.27.11.110	S15	10.27.11.130
S06	10.27.11.112	S16	10.27.11.132
S07	10.27.11.114	S17	10.27.11.134
S08	10.27.11.116	S18	10.27.11.136
S09	10.27.11.118	S19	10.27.11.138
S10	10.27.11.120	S20	10.27.11.140

Edit BGP Instance Add Peer Group Add Neighbor ✕

Neighbor IP *

Peer AS

Local Address

Hold Time (seconds)

TTL

Password

Local Network Name

Local AS

Local AS Mode

AS Origination Interval

Weight

Suppress Peer AS

Description

Disable ⓘ

Relax First AS Check
 Soft Reconfiguration
 Next Hop UnChanged
 Fast External Fallover
 Disable Graceful Restart
 Disable Extended Message Length Capability

[General](#) [Advanced](#)

Family ↕	Loop Count	Prefix Limit		Restart Interval	Action	Soft Reconfiguration
		Maximum	Threshold			
--Select--	Allowed Range is 1 - 2	Allowed Range is 1 - 2	Allowed Range is 1 - 1	Allowed Range is 30 -	--Select--	<input type="checkbox"/> Soft Reconfigurati

No Family Added

2.m. Leave all of the remaining fields blank.

The BGP configuration has an inheritance hierarchy, meaning that the individual neighbors inherit the BGP settings of the Peer Group, and the Peer Group inherits the settings of the global BGP configuration. If you need to over-ride a less specific value (for example, the Peer AS value) on a specific neighbor, you can enter the peer-specific value in the neighbor properties, which will over-ride the less specific value. For our example, the Peer Group values that you entered on the previous step will apply to the neighbor.

2.n. When finished, click the *OK* buttons until you exit the Virtual Router configuration dialogs.

2.o. After you finish the B01 configuration, select your B02 device from the Appliance drop-down menu so that you can configure the B02 device.

2.p. In the B02 device, open the INET-Transport-VR virtual router and repeat the BGP configuration steps with the following values for the BGP Peer Group:

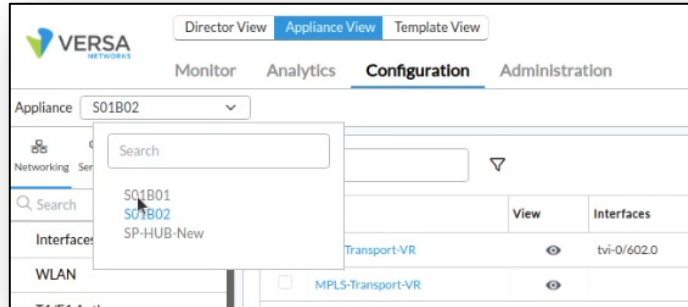
- Name: BGP-LAB
- Type: EBGp
- Peer AS: 65001 << Ensure that this value is correct (the AS values are reversed from the previous step)
- Local AS: 65002 << Ensure that this value is correct (the AS values are reversed from the previous step)
- Local Address: vni-0/0.0
- Neighbor Address from the table below:

Student	Neighbor IP Address	Student	Neighbor IP Address
S01	10.27.11.101	S11	10.27.11.121
S02	10.27.11.103	S12	10.27.11.123
S03	10.27.11.105	S13	10.27.11.125
S04	10.27.11.107	S14	10.27.11.127
S05	10.27.11.109	S15	10.27.11.129
S06	10.27.11.111	S16	10.27.11.131
S07	10.27.11.113	S17	10.27.11.133
S08	10.27.11.115	S18	10.27.11.135
S09	10.27.11.117	S19	10.27.11.137
S10	10.27.11.119	S20	10.27.11.139

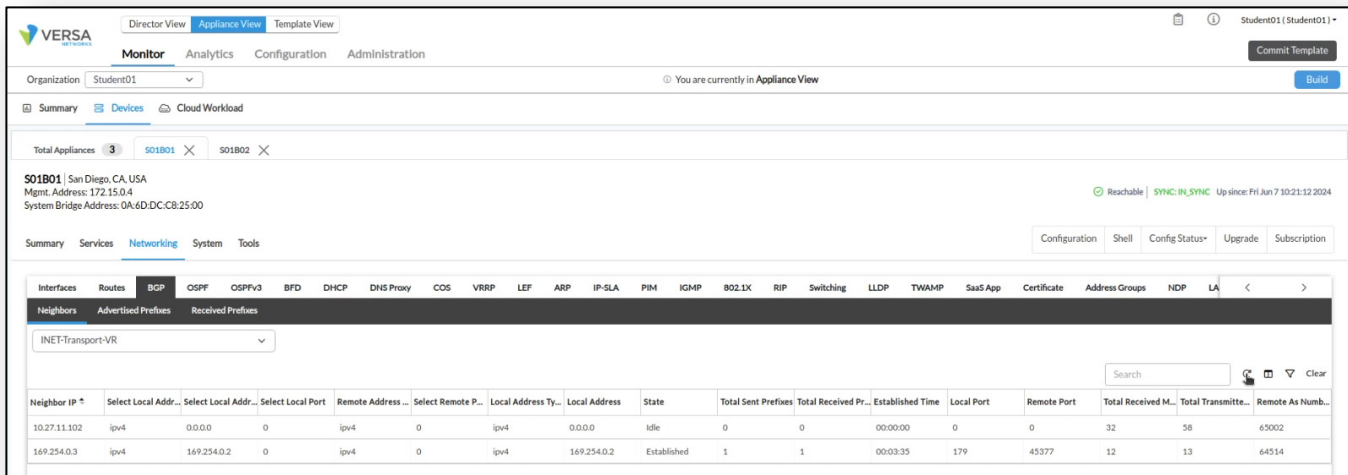
Step 3. Check the BGP Neighbor Status

In this step you will check the BGP peering status, and make a change to fix a problem that is preventing the BGP session from coming up.

- 3.a. Select the B01 device from the Appliance drop-down menu to open the B01 Appliance View dashboard.

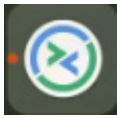


- 3.b. In the B01 Appliance View, navigate to Monitor > Networking > BGP > Neighbors to view the neighbor status. Note that the BGP neighbor status is not *Established* (it may be in Active or Idle mode).

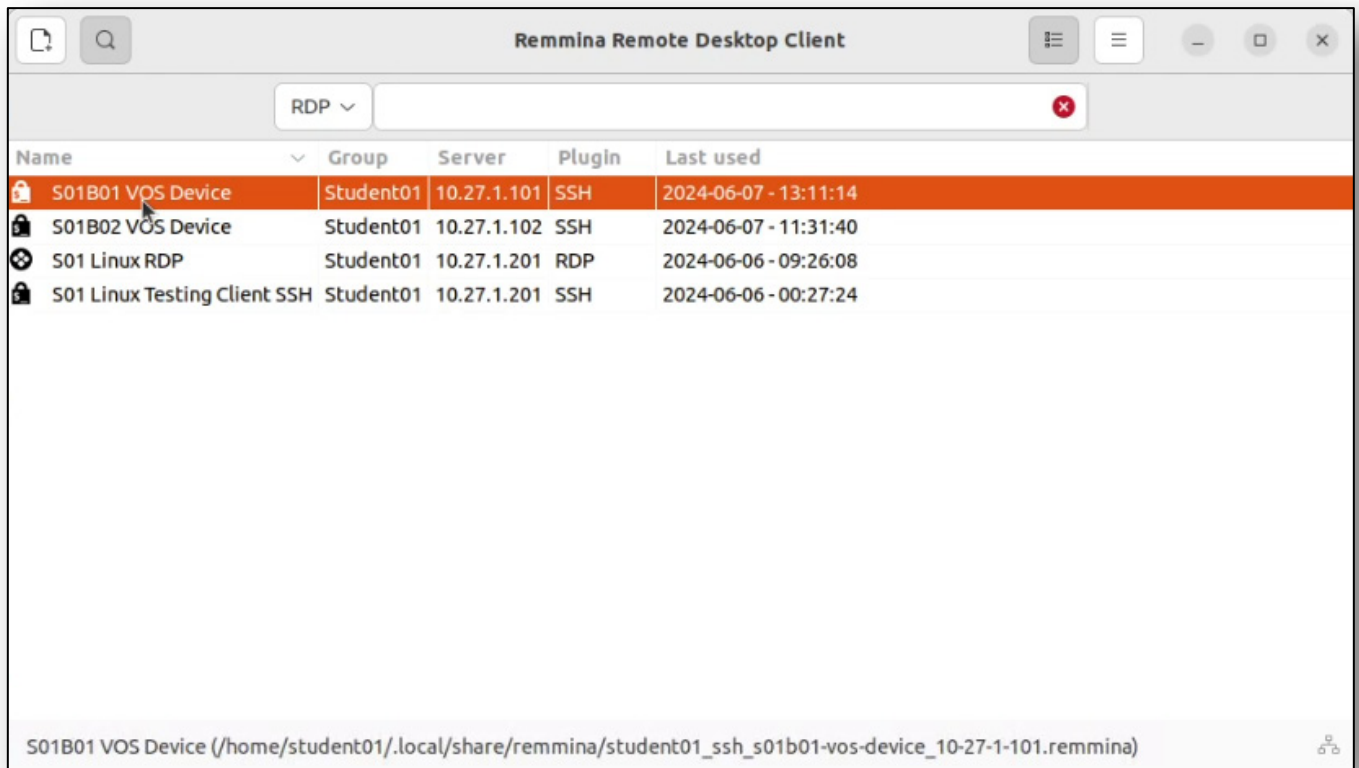


Let's see if we can determine why the BGP session will not establish.

On the remote desktop, open the Remmina Remote Desktop Client. In the Remmina Remote Desktop Client, open the SxxB01 VOS Device session, where Sxx is your student ID.



Remmina Icon on left toolbar



3.c. Log into the B01 VOS device. If prompted, use the username *admin* and password *lab123*.

3.d. In the VOS device shell prompt, type *cli* to start the command line interface.



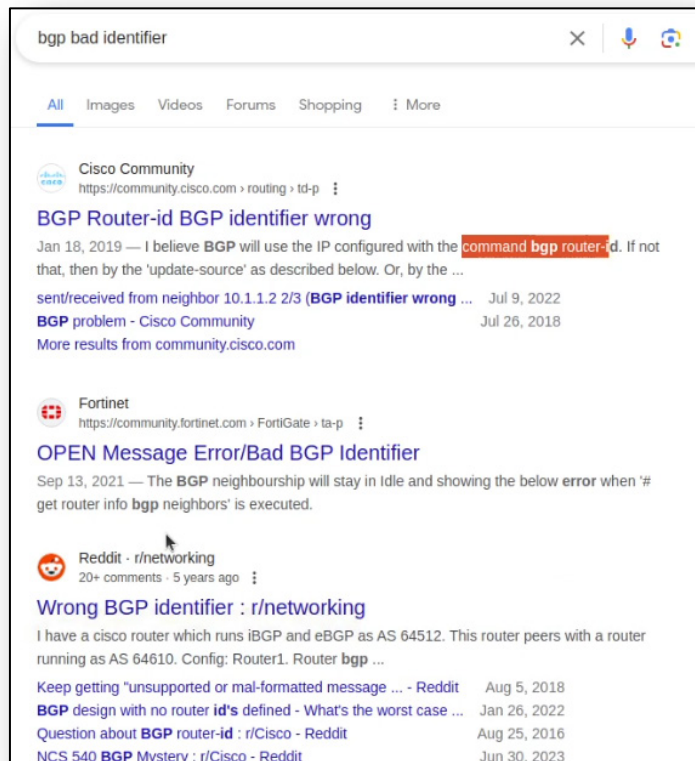
- 3.e. From the command line interface, enter the command `show bgp neighbor detail INET-Transport-VR` to display the detailed neighbor information. You will look for any errors on the session.

In the example you should find an error “OPEN Message Error: Bad BGP Identifier.” in the History Error field.

```

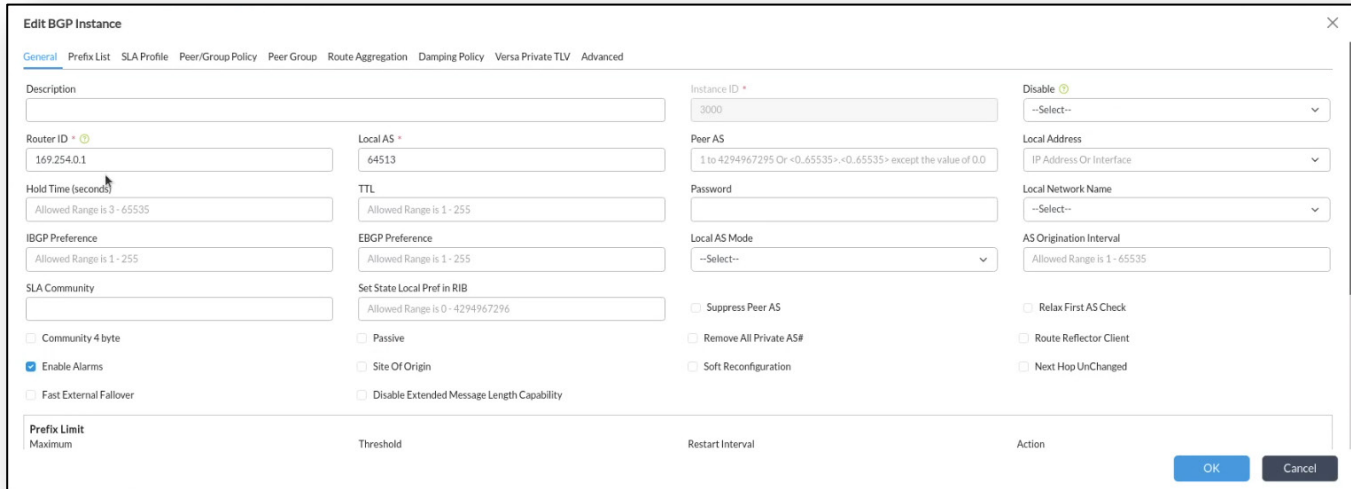
routing-instance: INET-Transport-VR
BGP instance: 3000
Peer: 10.27.11.102+0 AS 65002 Local: 0.0.0.0+0 AS 65001
Site Name:
Type: External State: Idle Up for: n/a
Last State: Opensent Last Event: Closed
Last Error: OPEN Message Error:Bad BGP Identifier.
Last Error Node:
Last Conn up Time Stamp: N/A
Last Conn down Time Stamp: 12:11:27, PDT, 7 June 2024
Last Sent Error: OPEN Message Error:Bad BGP Identifier.
Last Sent Error Time: 12:11:27, PDT, 7 June 2024
Last Received Error: OPEN Message Error:Bad BGP Identifier.
Last Received Error Time: 12:11:23, PDT, 7 June 2024
History Error: OPEN Message Error:Bad BGP Identifier. (History is previous to Last)
History Error Node: local
History Conn up Time Stamp: N/A
History Conn down Time Stamp: 12:11:25, PDT, 7 June 2024
Number of flaps: 0
Holdtime: 90
Peer Router ID: 0.0.0.0 Local Router ID: 169.254.0.1
Keepalive Interval: 30
BFD: disabled, down
NLRI advertised by peer:
NLRI for this session:
Peer does not support Refresh functionality
Peer does not support Restarter functionality
Peer does not support 4 byte AS extension (peer-as 65002)
Peer does not support Outbound Route Filtering functionality
Peer does not support extended message length capability
Input messages: Total 45 Updates 0 Refreshes 0
Output messages: Total 77 Updates 0 Refreshes 0
--More--
    
```

A quick search on the Internet indicates a possible cause for this error. The most likely cause is associated with a Router-ID issue.



Let's examine the Router IDs of the BGP sessions in our VOS branches.

- 3.f. In the *Appliance View* of your B01 branch device, navigate to *Configuration > Networking > Virtual Routers > INET-Transport-VR > BGP*
- 3.g. Open the BGP instance to display the *General* tab of the BGP instance configuration.



- 3.h. Take note of the router ID assigned to the BGP session. It should be a 169.254.0.1 address, or something similar. This is a common local address that VOS assigns to internal processes (usually a tunnel interface).
- 3.i. Click the *OK* button until you return to the main appliance dashboard.
- 3.j. From the main appliance dashboard, select the *SxxB02* appliance from the *Appliance* drop-down menu.
- 3.k. In the *SxxB02* appliance dashboard, navigate to *Configuration > Networking > Virtual Routers > INET-Transport-VR > BGP* and open the BGP instance on the B02 device.



- 3.l. Take note that the Router ID on branch B02 is identical to the router ID on the B01 device. This is because VOS uses the same locally significant IP address on tunnel interfaces, and the router ID is derived from a local logical interface. This is unique to the fact that we are connecting two VOS devices over a WAN connection, where we haven't explicitly configured a loopback interface or router ID.

We will resolve this issue by assigning the IP address of the WAN link to the Router-ID field.

- 3.m. In the Branch 2 BGP configuration, change the Router ID field to the IP address associated with the WAN IP address shown in the table below:

Student	Neighbor IP Address	Student	Neighbor IP Address
S01	10.27.11.102	S11	10.27.11.122
S02	10.27.11.104	S12	10.27.11.124
S03	10.27.11.106	S13	10.27.11.126
S04	10.27.11.108	S14	10.27.11.128
S05	10.27.11.110	S15	10.27.11.130
S06	10.27.11.112	S16	10.27.11.132
S07	10.27.11.114	S17	10.27.11.134
S08	10.27.11.116	S18	10.27.11.136
S09	10.27.11.118	S19	10.27.11.138
S10	10.27.11.120	S20	10.27.11.140

- 3.n. Click the OK buttons until you exit the Virtual Router configuration to apply the configuration.

At this point the issue should be resolved as the router IDs are no longer the same. However, we will change the Router ID of the B01 devices as well in order to be consistent.

- 3.o. Select the B01 device from the appliance drop-down menu.
- 3.p. In the B01 Appliance View, navigate to *Configuration > Networking > Virtual Routers > INET-Transport-VR > BGP* and open the BGP instance on the B01 device.
- 3.q. Set the B01 Router ID to the value in the table below.

Student	Neighbor IP Address	Student	Neighbor IP Address
S01	10.27.11.101	S11	10.27.11.121
S02	10.27.11.103	S12	10.27.11.123
S03	10.27.11.105	S13	10.27.11.125
S04	10.27.11.107	S14	10.27.11.127
S05	10.27.11.109	S15	10.27.11.129
S06	10.27.11.111	S16	10.27.11.131
S07	10.27.11.113	S17	10.27.11.133
S08	10.27.11.115	S18	10.27.11.135
S09	10.27.11.117	S19	10.27.11.137
S10	10.27.11.119	S20	10.27.11.139

You can now re-check the BGP status.

- 3.r. On the B01 appliance view, navigate to *Monitor > Networking > BGP > Neighbors* and check the neighbor state.

If it does not say Established, click the refresh button at the top right of the neighbor table to refresh the status.

Summary Services **Networking** System Tools

Configuration Shell Config Status+ Upgrade Subscription

Interfaces Routes **BGP** OSPF OSPFv3 BFD DHCP DNS Proxy COS VRRP LEF ARP IP-SLA PIM IGMP BGP.LX RIP Switching LLDP TWAMP SaaS App Certificate Address Groups NDP LA

Neighbors Advertised Prefixes Received Prefixes

INET-Transport-VR

Neighbor IP	Select Local Addr...	Select Local Addr...	Select Local Port	Remote Address ...	Select Remote P...	Local Address Ty...	Local Address	State	Total Sent Prefixes	Total Received Pr...	Established Time	Local Port	Remote Port	Total Received M...	Total Transmisse...	Remote As Numb...
10.27.11.102	ipv4	0.0.0.0	0	ipv4	0	ipv4	10.27.11.101	Established	2	0	00:00:03	179	37047	5	6	65002
169.254.0.3	ipv4	169.254.0.2	0	ipv4	0	ipv4	169.254.0.2	Established	1	1	00:00:03	179	43843	4	5	64514

Once the BGP session is established, it will indicate that 2 prefixes have been sent to the remote branch.

- 3.s. Open the *Monitor* dashboard for the B02 device. Do this by clicking *Devices* and selecting the B02 device from the table. Note that you can have multiple devices open in the Monitor window, and they can appear in different tabs.
- 3.t. In the B02 appliance *Monitor* dashboard, navigate to *Networking > BGP > Neighbors* and check the peering session with the B01 device. Examine the *Total Received Prefixes* count. You should see 0 prefixes received.

Total Appliances 3 S01B01 X S01B02 X

S01B02 | Denver, CO, USA
Mgmt. Address: 172.15.0.6
System Bridge Address: 0A:ED:40:ED:C5:00

Summary Services **Networking** System Tools

Configuration Shell Config Status+ Upgrade Subscription

Interfaces Routes **BGP** OSPF OSPFv3 BFD DHCP DNS Proxy COS VRRP LEF ARP IP-SLA PIM IGMP BGP.LX RIP Switching LLDP TWAMP SaaS App Certificate Address Groups NDP LA

Neighbors Advertised Prefixes Received Prefixes

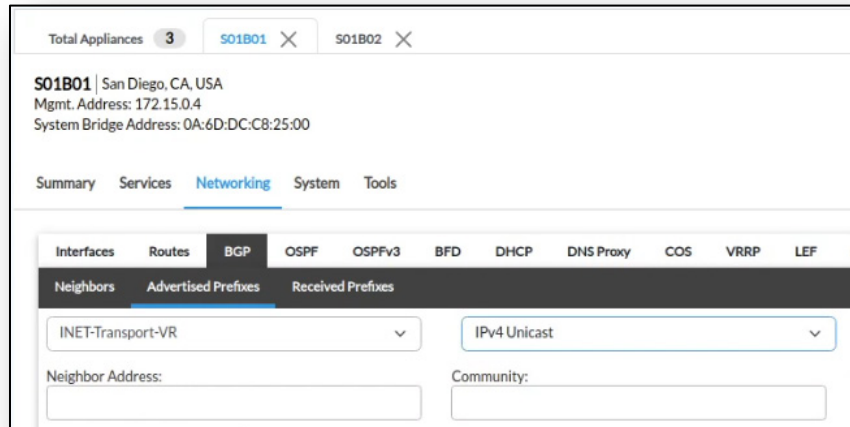
INET-Transport-VR

Neighbor IP	Select Local Addr...	Select Local Addr...	Select Local Port	Remote Address ...	Select Remote P...	Local Address Ty...	Local Address	State	Total Sent Prefixes	Total Received Pr...	Established Time	Local Port	Remote Port	Total Received M...	Total Transmisse...	Remote As Numb...
10.27.11.101	ipv4	0.0.0.0	0	ipv4	0	ipv4	10.27.11.102	Established	2	0	00:00:18	179	35465	5	6	65001
169.254.0.3	ipv4	169.254.0.2	0	ipv4	0	ipv4	169.254.0.2	Established	1	1	00:00:18	179	44423	4	5	64514

Status: B01 states that it is sending 2 prefixes, but branch B02 states that it has not received any prefixes from B01. To understand why this is happening, some knowledge of how BGP works is required. Let's examine the routes to try to determine why the routes do not appear in branch B02.

Step 4. Troubleshoot the BGP Session

- 4.a. Return to the B01 appliance *Monitor* dashboard.
- 4.b. In the B01 Monitor dashboard, navigate to *Networking > BGP > Advertised Prefixes*. Select the *INET-Transport-VR* virtual router, and the *IPv4 Unicast* route type



- 4.c. Locate the LAN address advertised to the remote site (the route that begins with 10.27.1xx.0/24) and click the arrow to expand the route details.

10.27.11.101	10.27.101.0/24	10.27.11.102	0
--------------	----------------	--------------	---

Note: You may have to use the scroll bar on the right side of the routes table or your mouse wheel to view the information.

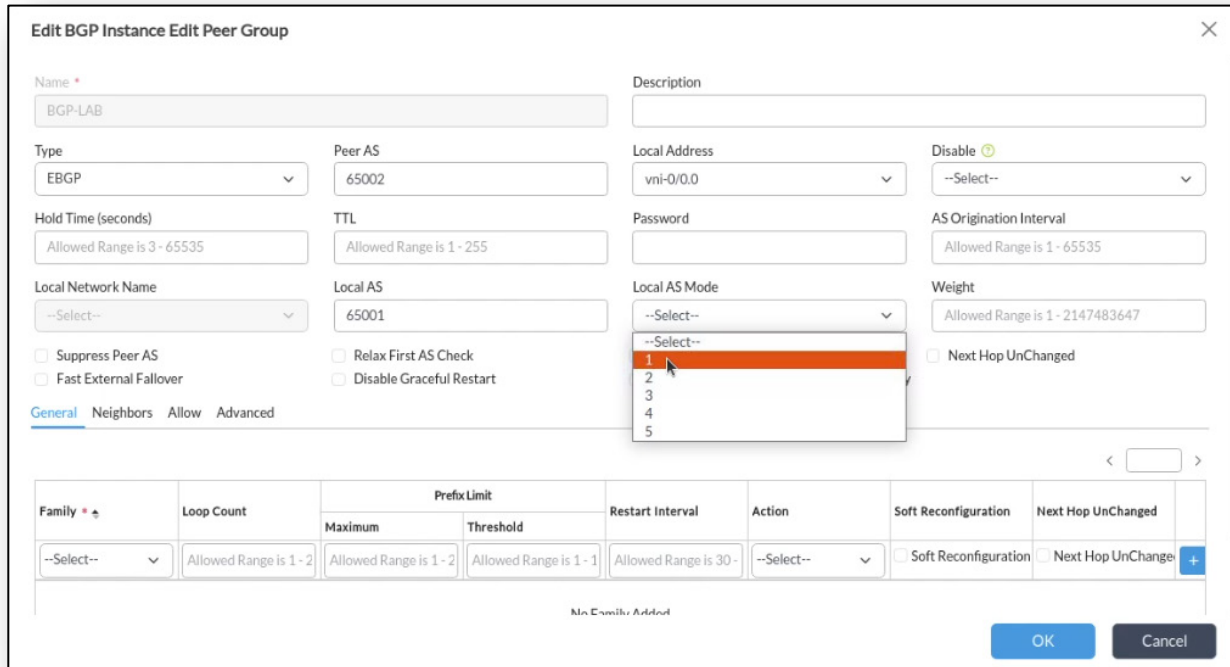
- 4.d. In the routes properties you will see the AS Path property. Note the AS Path advertised with the route.

Nexthop	Prefix	Peer
AS Path: 65001 64513 64514	Admin Distance:	
BGP Show Prefix:	Community: N/A	
Ext Community: N/A	Gateway Address: 10.27.11.101	
IP Address: 10.27.101.0	Local Preference: 0	

The BGP routing protocol detects route advertisement loops by examining the AS-Path property. If a device receives a route that contains its own AS number in the AS-Path property, the route is automatically discarded as a loop.

In the Versa Networks architecture, a private AS number is assigned to all devices as part of the overlay network creation process. In this case, the AS number is 64513. As you can see from the route advertisement, the overlay AS number is included in the AS Path when the route is advertised to branch B02, and therefore the route is discarded due to a perceived loop. This behavior is easily changed, however, by adjusting the properties of the BGP session.

- 4.e. On the B01 *Appliance View*, navigate to *Configuration > Networking > Virtual Routers > INET-Transport-VR > BGP* and open the BGP instance.
- 4.f. In the BGP instance, navigate to *Peer Group* and locate the *BGP-LAB* peer group. Open the *BGP-LAB* Peer Group.
- 4.g. In the *BGP-LAB* Peer Group, select the *Local AS Mode 1* from the drop-down menu. This will change how the BGP peer group behaves with regards to how it treats the local AS.



Edit BGP Instance Edit Peer Group

Name: BGP-LAB

Description:

Type: EBGDP

Peer AS: 65002

Local Address: vni-0/0.0

Disable: --Select--

Hold Time (seconds): Allowed Range is 3 - 65535

TTL: Allowed Range is 1 - 255

Password:

AS Origination Interval: Allowed Range is 1 - 65535

Local Network Name: --Select--

Local AS: 65001

Local AS Mode: --Select-- (1 selected)

Weight: Allowed Range is 1 - 2147483647

Suppress Peer AS

Fast External Fallover

Relax First AS Check

Disable Graceful Restart

Next Hop UnChanged

General Neighbors Allow Advanced

Family	Loop Count	Prefix Limit		Restart Interval	Action	Soft Reconfiguration	Next Hop UnChanged
		Maximum	Threshold				
--Select--	Allowed Range is 1 - 2	Allowed Range is 1 - 2	Allowed Range is 1 - 1	Allowed Range is 30 -	--Select--	<input type="checkbox"/> Soft Reconfiguration	<input type="checkbox"/> Next Hop UnChange +

Max Entries Added

OK Cancel

Because we are only examining the behavior in one direction (from B01 to B02), we will only make this change on branch B01. If you wish to have the behavior changed in both directions, the same change would be required on the B02 device. Listed here are the descriptions of the modes. The default mode is mode 2.

1—Peering session is established with the local AS configured in BGP instance or with a BGP group or neighbor. When importing routes, an AS number is not inserted in the AS path. When exporting routes, the selected local AS number is prepended to the AS path.

2—Peering session is established with local AS configured as a BGP group or neighbor. When importing routes, the local AS number of the group or neighbor is inserted in AS path. When exporting routes, the local AS number configured on the BGP group or neighbor and the local AS number configured for the BGP instance are prepended to the AS path. This is the default.

3—Peering session is established with the local AS configured for the BGP group or neighbor. When importing routes, no AS number is inserted in the AS path. When exporting routes, the local AS configured for the BGP group or neighbor and the local AS number configured for the BGP instance are prepended to AS path.

4—Peering session is established with the local AS number configured for the BGP group or neighbor. When importing routes, no AS number is inserted in the AS path. When exporting routes, the local AS number configured for the BGP group or neighbor is prepended to the AS path.

5—(For Releases 22.1.1 and later.) Peering session is established with the local AS number configured for the BGP group or neighbor. When importing routes, the local AS in the BGP group or neighbor is inserted in the AS path. When exporting routes, the local AS number configured in the BGP group or neighbor is prepended to the AS path.

Once this change is made, only the Local AS number configured within the peer group will be used on the advertised route (the global AS number of the BGP instance is no longer included). This will remove the AS Loop issue.

4.h. Click *OK* to apply the change.

4.i. To verify the change, return to the B01 table and expand the 10.27.11.1xx/24 prefix again.

S01B01 | San Diego, CA, USA
Mgmt. Address: 172.15.0.4
System Bridge Address: 0A:6D:DC:C8:25:00

Summary Services **Networking** System Tools

Interfaces Routes **BGP** OSPF OSPFv3 BFD DHCP DNS Proxy COS VRRP LEF ARP IP-SLA PIM IGMP B02.IX RIP Switching LLDP TWAMP

Neighbors **Advertised Prefixes** Received Prefixes

INET-Transport-VR IPv4 Unicast

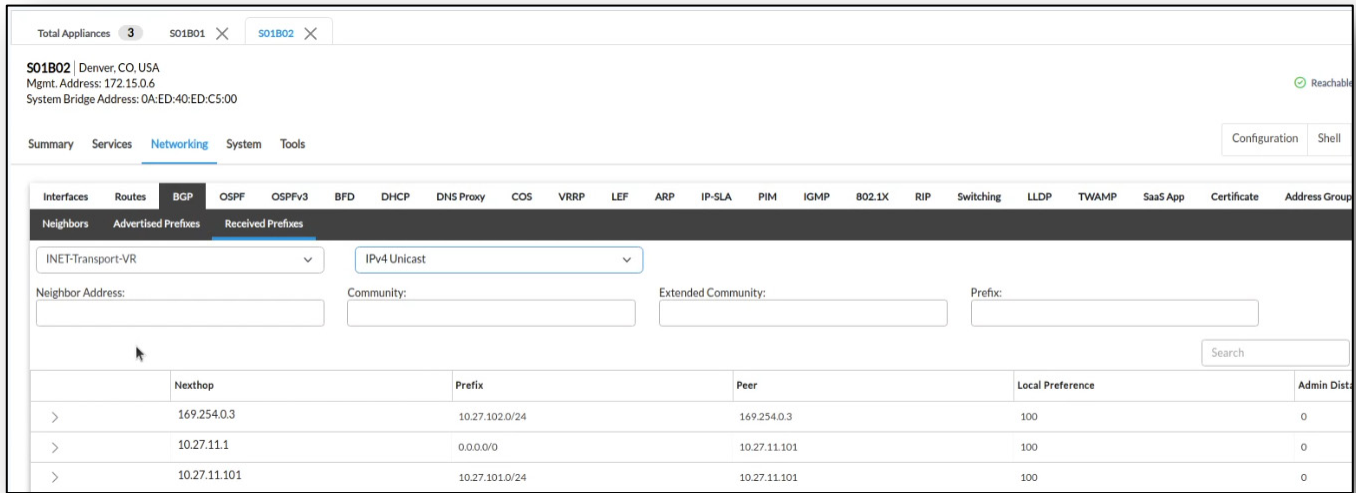
Neighbor Address: Community: Extended Community: Prefix:

	Nexthop	Prefix	Peer	Local Preference
>	169.254.0.2	0.0.0.0/0	169.254.0.3	0
>	10.27.11.1	0.0.0.0/0	10.27.11.102	0
▼	10.27.11.101	10.27.101.0/24	10.27.11.102	0

AS Path: 65001 64514 Admin Distance: AFI: ipv4
BGP Show Prefix: Community: N/A Destination Length: 24
Ext Community: N/A Gateway Address: 10.27.11.101 Instance Name: INET-Transport-VR

Note that the AS Path advertised has been changed. The AS 64514 is added because the route was advertised using EBGp from the LAN VRF to the INET VR, and the AS 64514 is the AS associated with that connection. However, when the prefix is advertised to the remote branch (B02), the global AS number (which was the overlapping AS assigned to all VOS devices) is no longer present in the path. Only the AS number associated with the BGP-LAB instance is added.

- 4.j. To verify the change, open the B02 Monitor dashboard.
- 4.k. Navigate to *Networking > BGP > Received Prefixes > INET-Transport-VR > IPv4 Unicast*. Verify that the prefixes are now present in the B02 routing table.



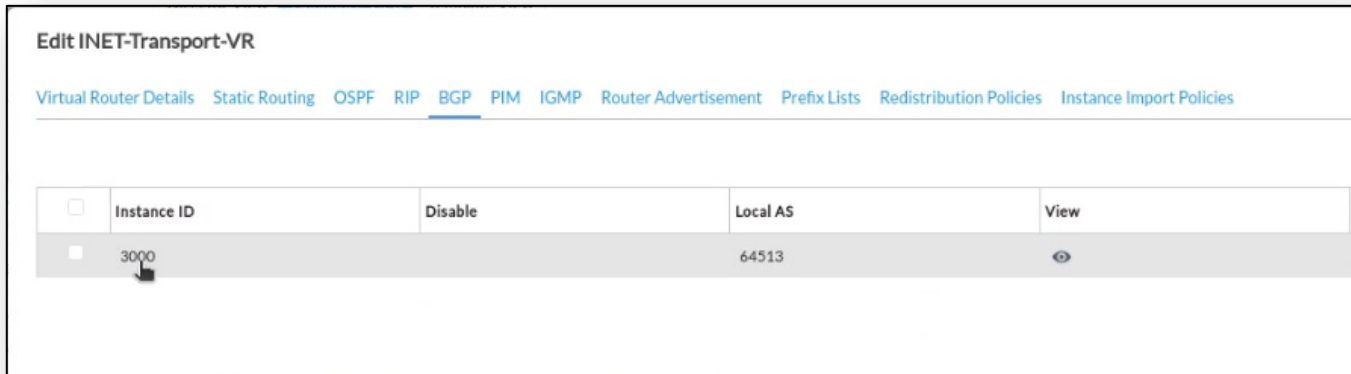
The screenshot shows the 'Received Prefixes' configuration page for S01B02. The 'Neighbor Address' is set to 'INET-Transport-VR' and the 'Prefix' is set to 'IPv4 Unicast'. Below the configuration fields, a table displays the received prefixes:

	NextHop	Prefix	Peer	Local Preference	Admin Dist
>	169.254.0.3	10.27.102.0/24	169.254.0.3	100	0
>	10.27.11.1	0.0.0.0/0	10.27.11.101	100	0
>	10.27.11.101	10.27.101.0/24	10.27.11.101	100	0

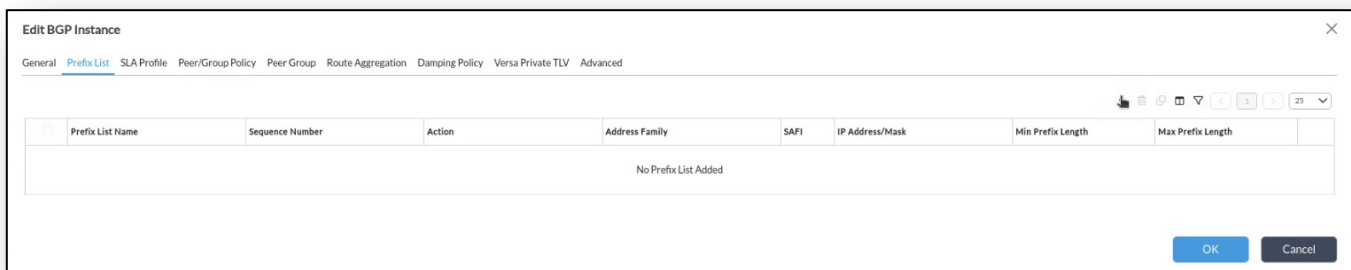
You should have 2 routes from the B01 device listed in the table. One route is a default route, and the other is the remote LAN network.

Step 5. Create a BGP Export Policy

- 5.a. Navigate to the B01 *Appliance View*.
- 5.b. In the B01 *Appliance View*, navigate to *Configuration > Networking > Virtual Routers > INET-Transport-VR > BGP* and open the BGP instance.



- 5.c. In the BGP instance, open the *Prefix List* tab and click the + button to create a new prefix list.



- 5.d. Name the prefix list *BGP-to-B02*, and click the + button to add a prefix to the list.

- 5.e. Add prefix 10.27.0.0/16 to the list with the properties shown below.

- Sequence Number: 1
- Action: Permit
- Address Family: IPv4
- SAFI: Unicast
- IP Address/Mask 10.27.0.0/16
- Max Prefix Length: 24

Edit BGP Instance Add Prefix List Add Sequence ✕

Sequence Number *	Action	Address Family	SAFI *
<input type="text" value="1"/>	<input style="border-bottom: none; border-top: none; border-left: none; border-right: none; background-color: #f0f0f0; width: 100%;" type="text" value="Permit"/>	<input style="border-bottom: none; border-top: none; border-left: none; border-right: none; background-color: #f0f0f0; width: 100%;" type="text" value="IPv4"/>	<input style="border-bottom: none; border-top: none; border-left: none; border-right: none; background-color: #f0f0f0; width: 100%;" type="text" value="Unicast"/>

IP Address

IP Address/Mask	Min Prefix Length	Max Prefix Length
<input type="text" value="10.27.0.0/16"/>	<input type="text"/>	<input type="text" value="24"/>

IP Address Mask is the base prefix. In the example prefixes with the first 16 bits set to 10.27.x.x will match. If you do not include Min and Max lengths, this is an EXACT match. We want to accept the /24 networks within that range, so enter Max Prefix Length 24, which will match all prefixes within the 10.27.x.x network that have up to a /24 prefix length.

5.f. Add another prefix to the list with the following parameters:

- Sequence Number: 2
- Action: Deny
- Address Family: IPv4
- SAFI: Unicast
- IP Address/Mask 0.0.0.0/0

Edit BGP Instance Add Prefix List Add Sequence ✕


Sequence Number *	Action	Address Family	SAFI *
<input type="text" value="2"/>	<input style="border-bottom: none; border-top: none; border-left: none; border-right: none; background-color: #f0f0f0; width: 100%;" type="text" value="Deny"/>	<input style="border-bottom: none; border-top: none; border-left: none; border-right: none; background-color: #f0f0f0; width: 100%;" type="text" value="IPv4"/>	<input style="border-bottom: none; border-top: none; border-left: none; border-right: none; background-color: #f0f0f0; width: 100%;" type="text" value="Unicast"/>

IP Address

IP Address/Mask	Min Prefix Length	Max Prefix Length
<input type="text" value="0.0.0.0/0"/>	<input type="text"/>	<input type="text"/>

5.g. Ensure the action is Deny. This will match the 0.0.0.0/0 route and deny it (will prevent it from being added to the route advertisements).

Your prefix list should resemble the example below when finished.



Edit BGP Instance Add Prefix List ✕

Prefix List Name *
BGP-to-B02

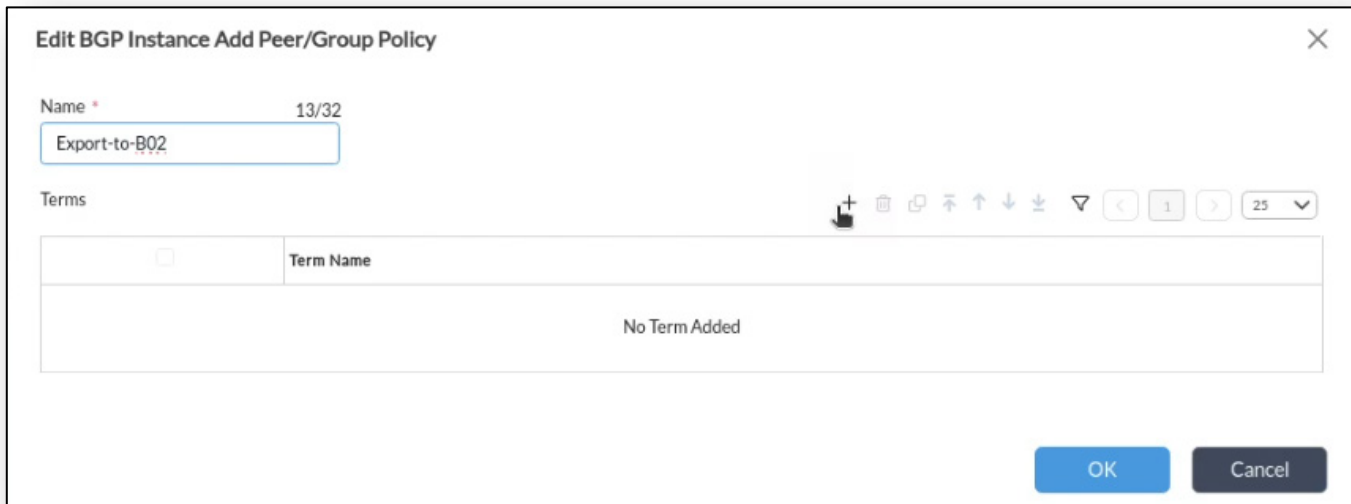
Sequence + - [] [] [] < 1 > 25 ▾

<input type="checkbox"/>	Sequence Number	Action
<input type="checkbox"/>	1	Permit
<input type="checkbox"/>	2	Deny

OK Cancel

5.h. Click *OK* to finish the prefix list configuration.

- 5.i. Navigate to *Peer/Group Policy* to create a peer policy or a peer group policy. This will create the set of rules to apply to BGP updates (the rules will still need to be applied to a peer or peer group later).
- 5.j. Click + to add a new *Peer/Group Policy*. Name the policy *Export-to-B02*.
- 5.k. In the *Export-to-B02* policy, click the + button to add a new policy term (rule).



Edit BGP Instance Add Peer/Group Policy

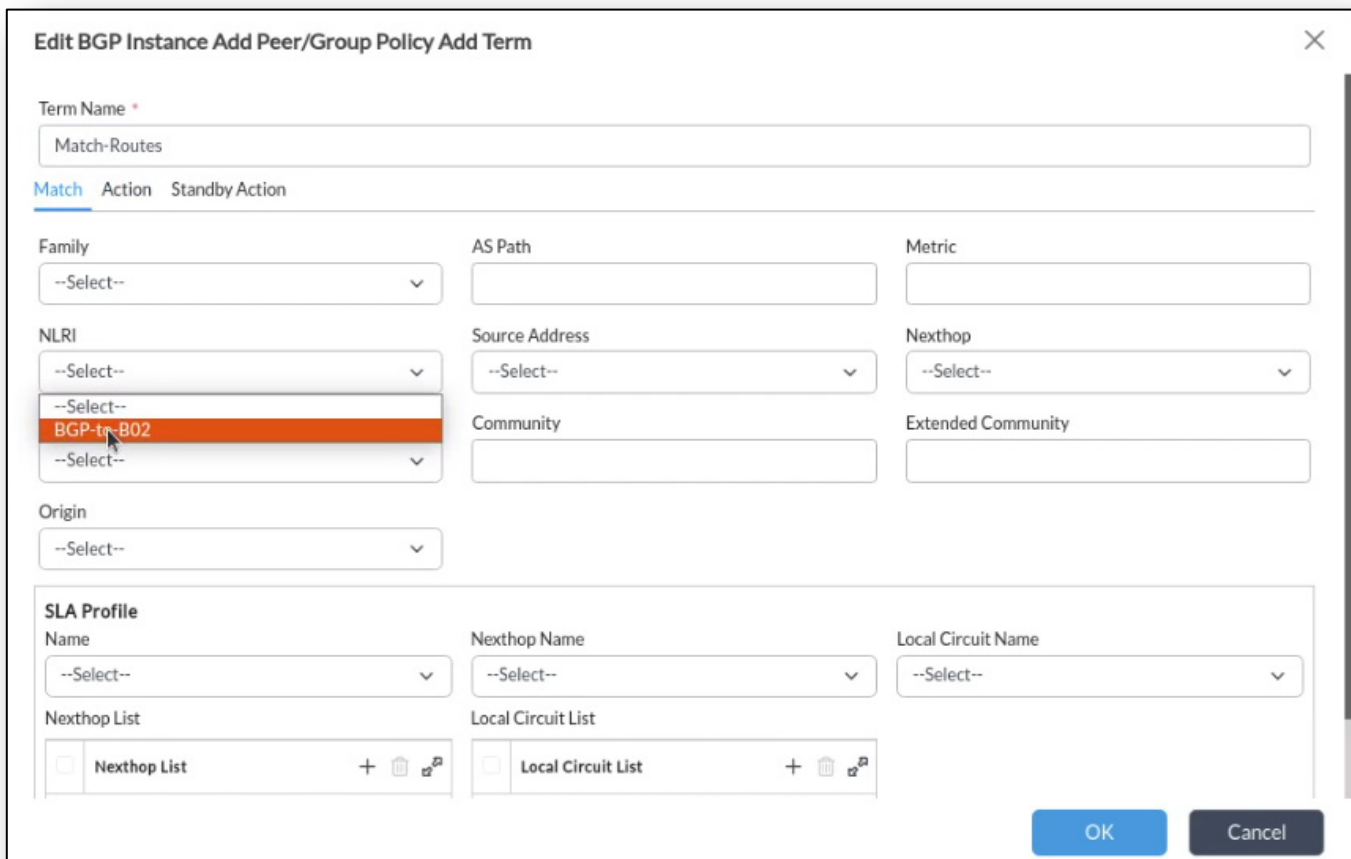
Name * 13/32
Export-to-B02

Terms

<input type="checkbox"/>	Term Name
No Term Added	

OK Cancel

- 5.l. Create a rule named *Match-Routes*, and select the *BGP-to-B02* prefix list in the *NLRI* drop-down. NLRI stands for Network Layer Reachability Information, which is a term that refers to IP prefixes.



Edit BGP Instance Add Peer/Group Policy Add Term

Term Name *
Match-Routes

Match Action Standby Action

Family: --Select--
AS Path:
Metric:

NLRI: --Select-- (BGP-to-B02 selected)
Source Address: --Select--
Nexthop: --Select--

Community:
Extended Community:

Origin: --Select--

SLA Profile

Name: --Select--
Nexthop Name: --Select--
Local Circuit Name: --Select--

Nexthop List: Nexthop List + -
Local Circuit List: Local Circuit List + -

OK Cancel

- 5.m. Click on the *Action* tab and ensure that the *Accept* action is selected. When using prefix lists, the action in the prefix list (Permit or Deny) will be applied to prefixes individually.

Edit BGP Instance Add Peer/Group Policy Add Term ✕

Term Name *

Match-Routes

Match Action Standby Action

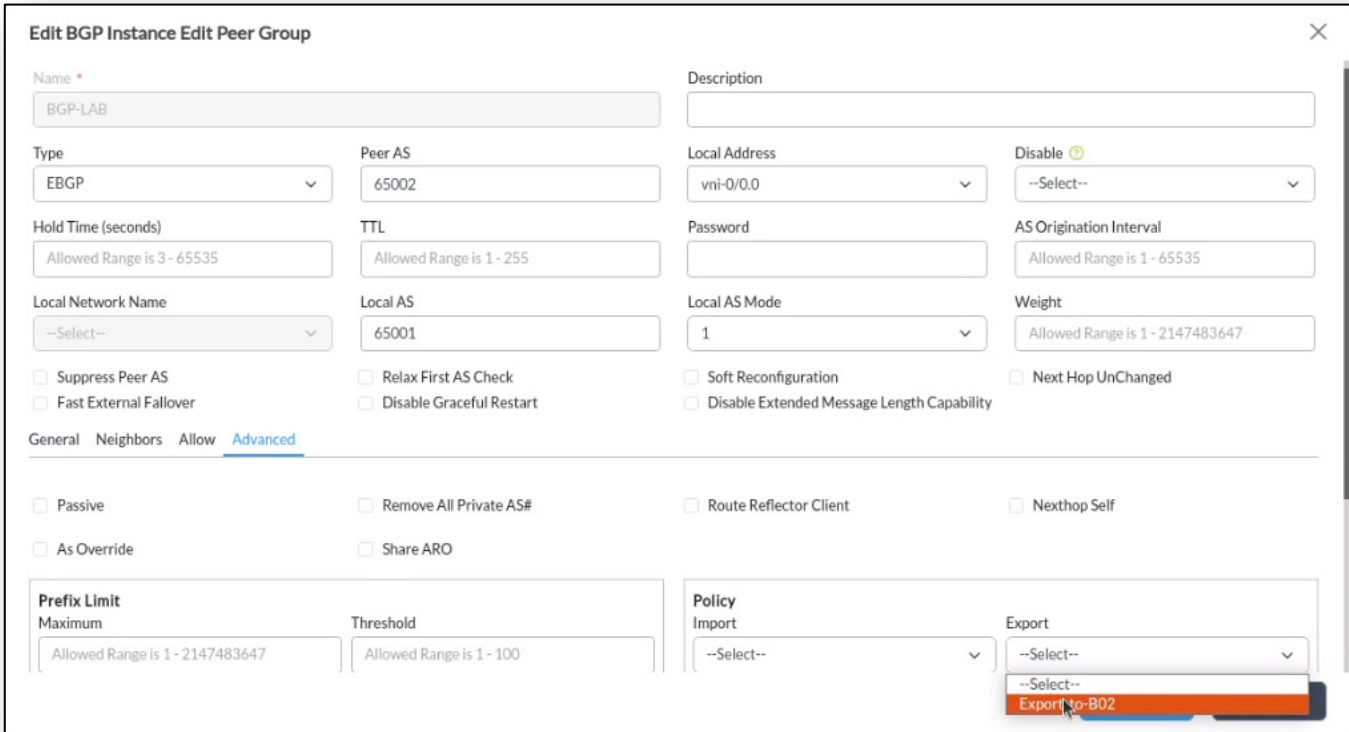
Accept/Reject <input type="text" value="Accept"/>	Damping <input type="text"/>	<input type="checkbox"/> Enable ECMP for BGP Routes in RIB
Origin <input type="text" value="--Select--"/>	Nexthop <input type="text"/>	Local Preference <input type="text" value="Allowed Range is 0 - 2147483647"/>
AS Path <input type="text" value="--Select--"/>	Local AS Prepend Count <input type="text" value="Allowed Range is 1 - 255"/>	AS Path Prepend <input type="text" value="Allowed Range is 1 - 4294967295"/>
Community Action <input type="text" value="--Select--"/>	<input type="checkbox"/> SLA Community Action	Well Known Community <input type="text" value="--Select--"/>
Community <input type="text"/>	Route Preference <input type="text"/>	Extended Community Action <input type="text" value="--Select--"/>
Extended Community <input type="text"/>	Metric Action <input type="text" value="--Select--"/>	Metric <input type="text" value="Allowed Range is 1 - 4294967295"/>
Next Term <input type="text"/>	Weight <input type="text"/>	Next Term Action <input type="text"/>

- 5.n. Click *OK* to add the term, then click *OK* again to finish the policy configuration.

Next you will apply the policy to the BGP session to branch B02.

IMPORTANT NOTE: When you apply a policy to a BGP session, route prefixes are treated in a similar manner as a security policy. This means that all routes will be blocked except routes that are explicitly permitted by the policy. Please ensure that when you apply a BGP Import or Export policy that you explicitly permit any routes you want to include in the sent or received updates.

- 5.o. Navigate to the Peer Group tab and open the BGP-LAB peer group. BGP policies are assigned in the Advanced settings tab. Click the Advanced tab to open the advanced settings.



Edit BGP Instance Edit Peer Group

Name: BGP-LAB

Description: [Empty]

Type: EBGDP

Peer AS: 65002

Local Address: vni-0/0.0

Disable: --Select--

Hold Time (seconds): Allowed Range is 3 - 65535

TTL: Allowed Range is 1 - 255

Password: [Empty]

AS Origination Interval: Allowed Range is 1 - 65535

Local Network Name: --Select--

Local AS: 65001

Local AS Mode: 1

Weight: Allowed Range is 1 - 2147483647

Suppress Peer AS

Fast External Fallover

Relax First AS Check

Disable Graceful Restart

Soft Reconfiguration

Disable Extended Message Length Capability

Next Hop UnChanged

General Neighbors Allow **Advanced**

Passive

As Override

Remove All Private AS#

Share ARO

Route Reflector Client

Nexthop Self

Prefix Limit

Maximum: Allowed Range is 1 - 2147483647

Threshold: Allowed Range is 1 - 100

Policy

Import: --Select--

Export: --Select--
Export-to-B02

- 5.p. In the *Advanced* settings, select the *Export-to-B02* policy in the *Export* drop-down.

This will assign the rules to the BGP sessions in this peer group.

- 5.q. Click the *OK* buttons until you have exited the *Virtual Router* configuration windows. This will save the configuration in Versa Director and automatically apply the changes to the appliance.

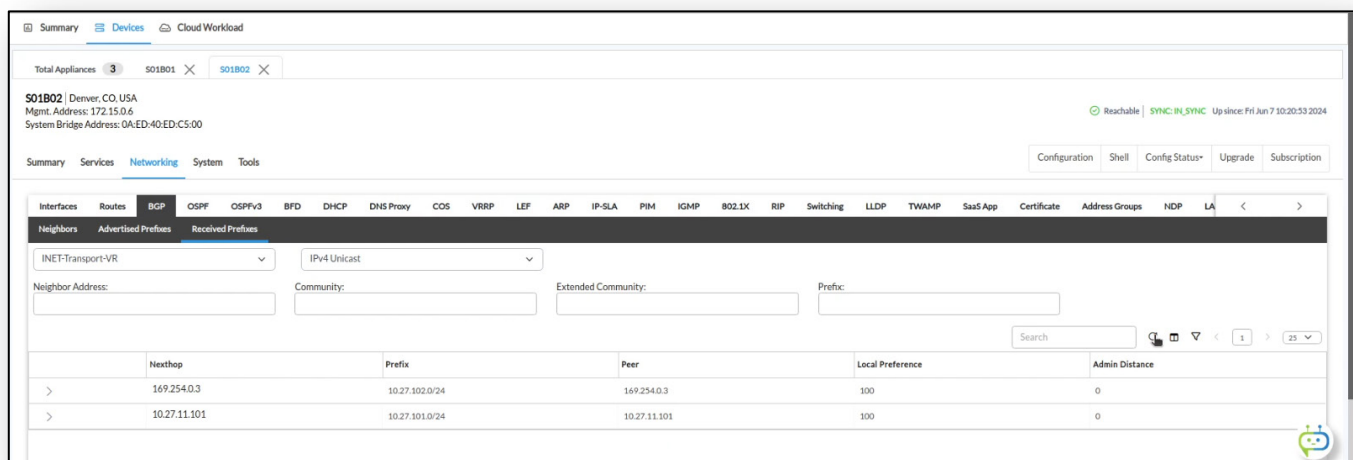
Step 6. Verify the Policy Changes

Next you will verify that the proper routes are sent to branch B02.

- 6.a. Navigate to the B02 *Monitor* view.
- 6.b. In the B02 *Monitor* dashboard, navigate to *Networking* > *BGP* > *Received Prefixes* > *INET-Transport-VR* > *IPv4 Unicast*.

If you had the monitor dashboard open in a different tab, you may need to refresh the route table with the refresh button.

You should now see a route from the DIA connection BGP session and a single route from the B01 device, which is the LAN address connected to the B01 device. The default route from branch B01 should no longer be present in the routing table.



The screenshot displays the Versa Networks GUI for device S01B02. The navigation path is: Summary > Services > Networking > BGP > Received Prefixes > INET-Transport-VR > IPv4 Unicast. The configuration shows two neighbors: 169.254.0.3 and 10.27.11.101. The received prefixes table is as follows:

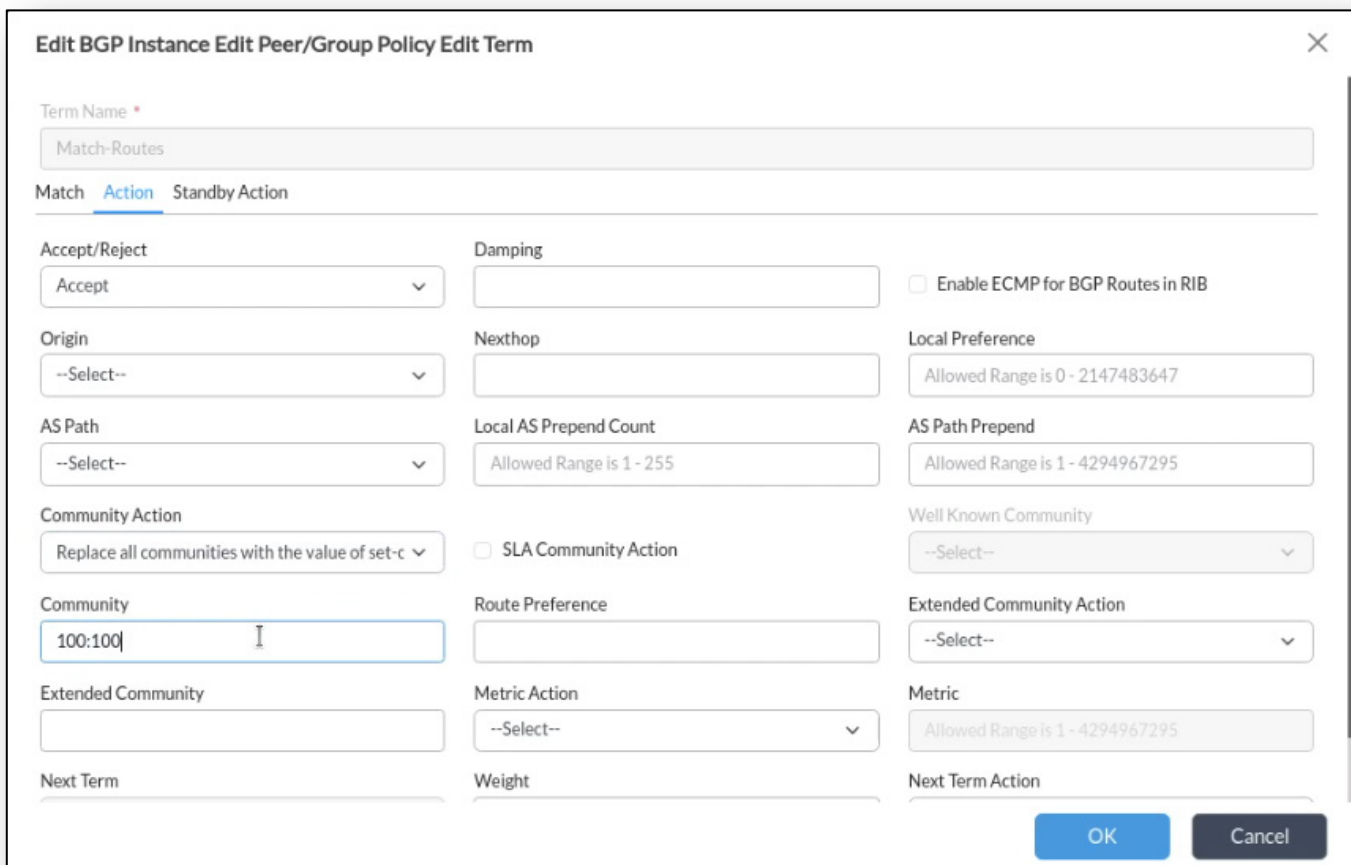
Nexthop	Prefix	Peer	Local Preference	Admin Distance
>	10.27.102.0/24	169.254.0.3	100	0
>	10.27.11.101	10.27.11.101	100	0

Step 7. Make Other Changes and Verify

Next you will make some simple changes to the export policy on appliance B01 and verify the changes by viewing them on branch B02.

- 7.a. Return to the B01 *Appliance View*.
- 7.b. In the B01 *Appliance View*, navigate to *Configuration > Networking > Virtual Routers > INET-Transport-VR > BGP* and open the BGP instance.
- 7.c. In the BGP instance on B01, navigate to *Peer/Group Policy* and open the *Export-to-BGP* policy.
- 7.d. Open the Match-Routes term, and select the Action tab.
- 7.e. In the *Match-Routes Action* window, select the following:
 - Community Action: Replace all communities with the value of set-community
 - Community: 100:100

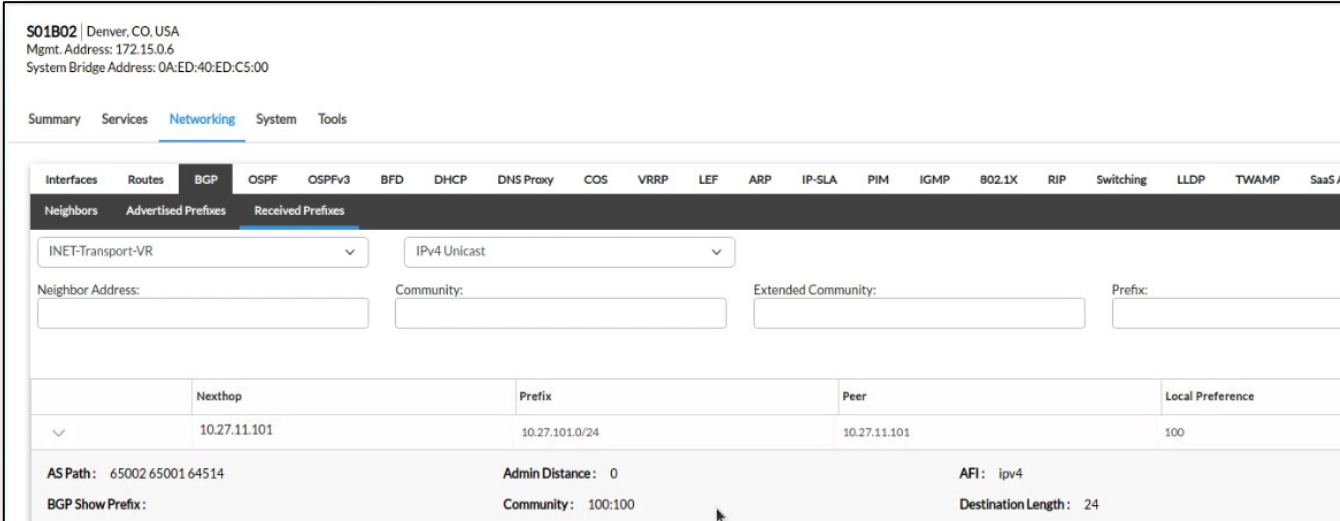
This performs the following actions: any community value associates with the routes matched by the policy will be removed and will be replaced by the community value(s) in the Community field.



- 7.f. Click *OK* to modify the term, then click *OK* until you exit the Virtual Router configuration dialog, which will save and apply the configuration to the appliance.

Step 8. Verify the changes

- 8.a. Return to the B02 *Monitor* dashboard.
- 8.b. In the B02 *Monitor* dashboard, navigate to *Networking > BGP > Received Prefixes > INET-Transport-VR > IPv4 Unicast* and expand the properties of the LAN route received from branch B01.



S01B02 | Denver, CO, USA
Mgmt. Address: 172.15.0.6
System Bridge Address: 0A:ED:40:ED:C5:00

Summary Services **Networking** System Tools

Interfaces Routes **BGP** OSPF OSPFv3 BFD DHCP DNS Proxy COS VRRP LEF ARP IP-SLA PIM IGMP 802.1X RIP Switching LLDP TWAMP SaaS Ap

Neighbors Advertised Prefixes **Received Prefixes**

INET-Transport-VR IPv4 Unicast

Neighbor Address: Community: Extended Community: Prefix:

	Nexthop	Prefix	Peer	Local Preference
▼	10.27.11.101	10.27.101.0/24	10.27.11.101	100

AS Path: 65002 65001 64514 Admin Distance: 0 AFI: ipv4
BGP Show Prefix: Community: 100:100 Destination Length: 24

Note that the Community value in the route matches the value that you set in the BGP export policy on branch B01.



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