Versa Class of Service

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

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

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

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

This lab environment is a shared environment. There may be up to 5 other students in the environment. Each student has their own remote desktop, but the Versa Director is shared. Because of the shared environment, you may see configuration templates, device groups, workflows, and devices that other students have created, or that have been pre-provisioned within Versa Director. It is important that you only modify the configuration components that are assigned to you by your instructor.

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

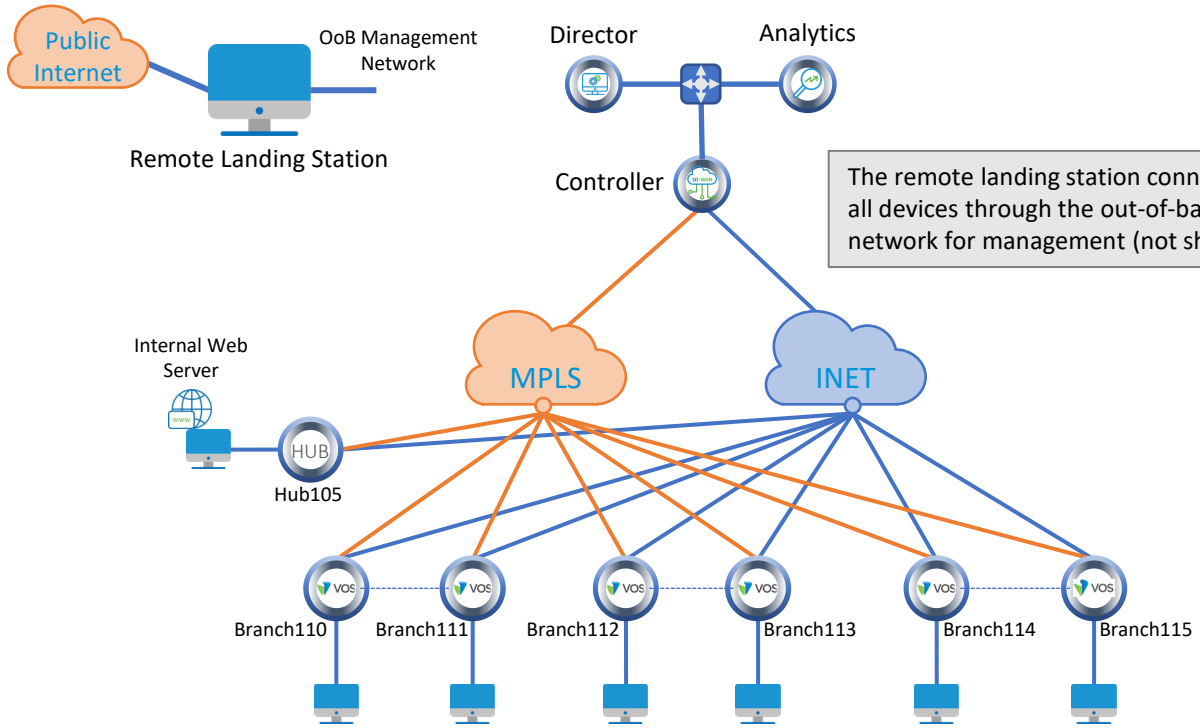
Look for these hints to help you in the labs

This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment. At the end of the lab guide you can find additional help on to how to complete the tasks, so if you have trouble with a task, please refer to the help section. If you still cannot accomplish the task, ask your instructor for assistance. In addition, you will see **hints** placed throughout the lab guide to help you along.

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

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

Lab Topology



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

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

Each branch connects to a local LAN

- vni-0/2

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

- vni-0/3

Remember this! You will use it a lot!

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

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

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

Interface Addresses

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

Controller Addresses

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

Exercise 1: Connect to the remote lab environment

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

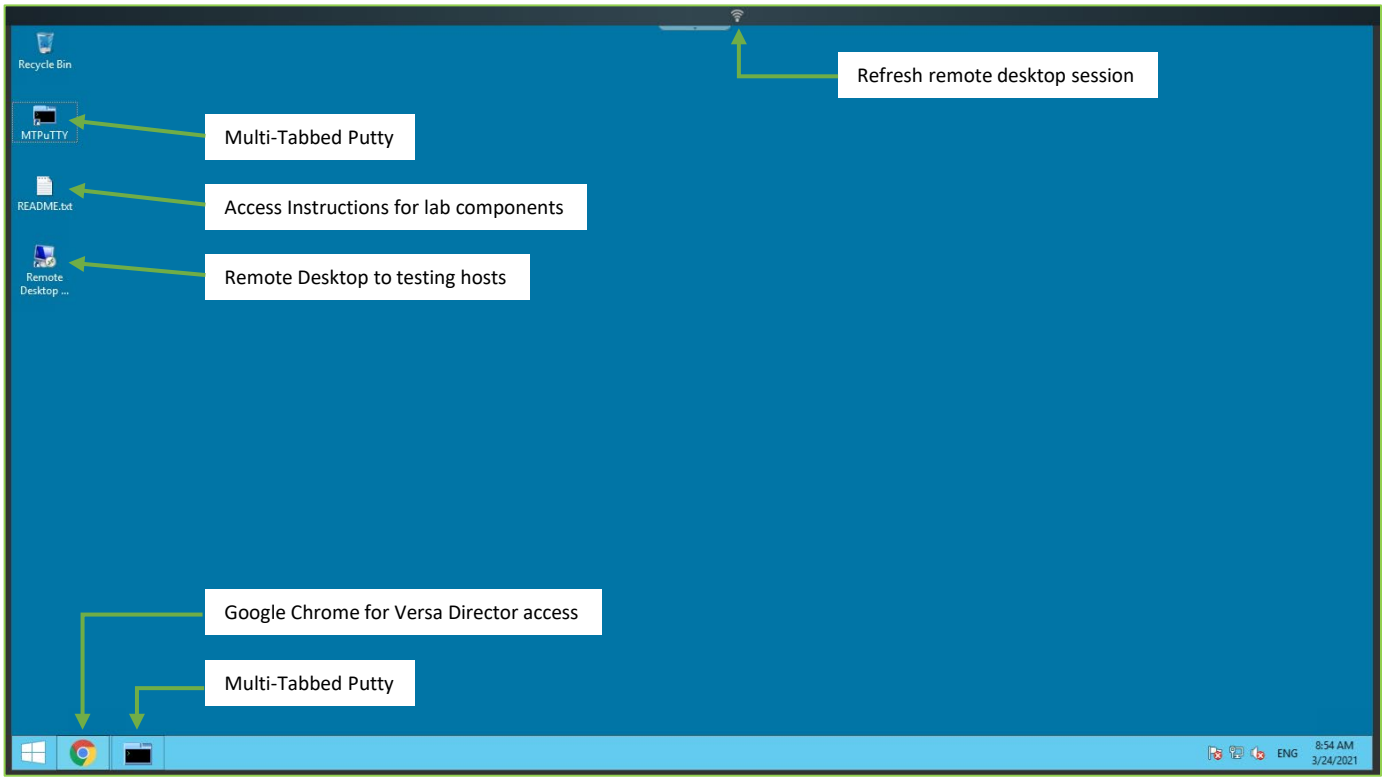
- Branch/Node/CPE Assignment
- Remote Lab Access

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

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

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

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



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

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

Exercise 2: Examine the Class of Service Hierarchy

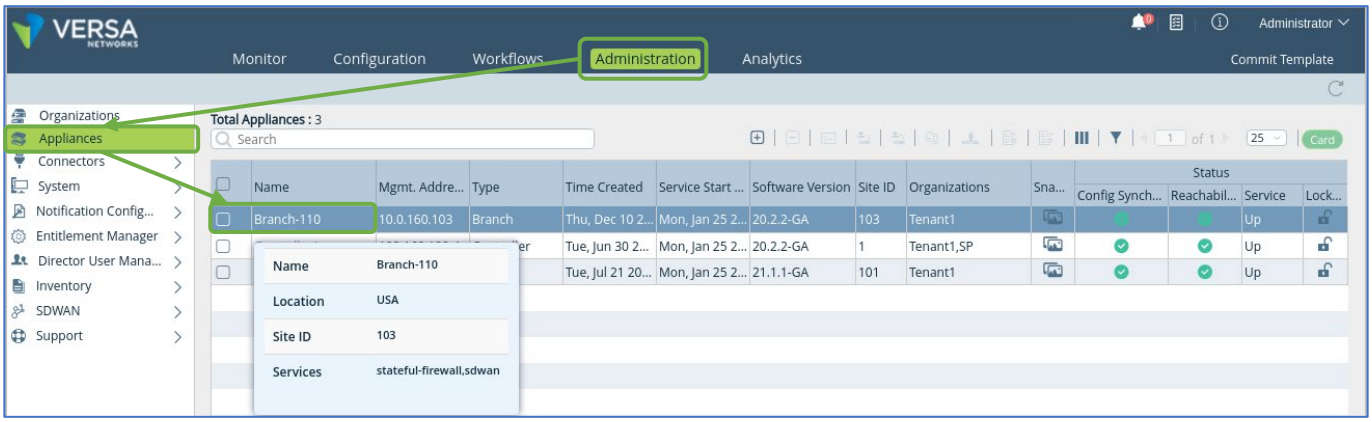
In the following lab exercises, you will:

- 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

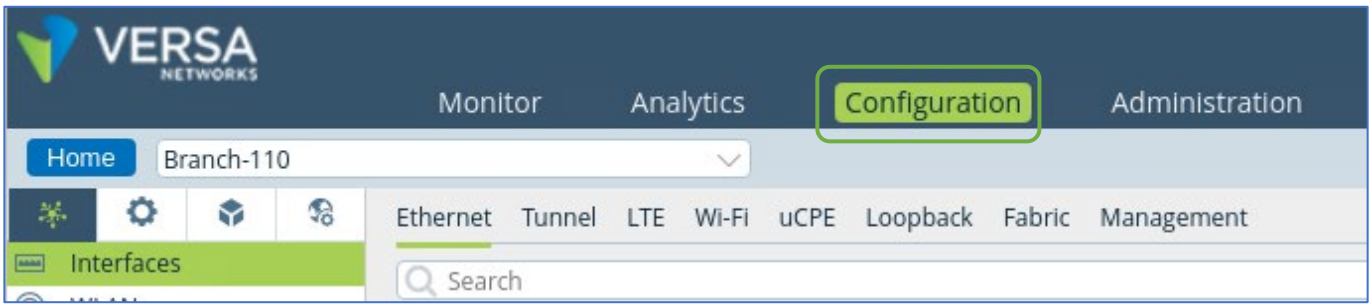
> **Note**: Configuration modifications in this lab will be performed in Appliance Context mode (directly on your device) and will not be performed through device templates.

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

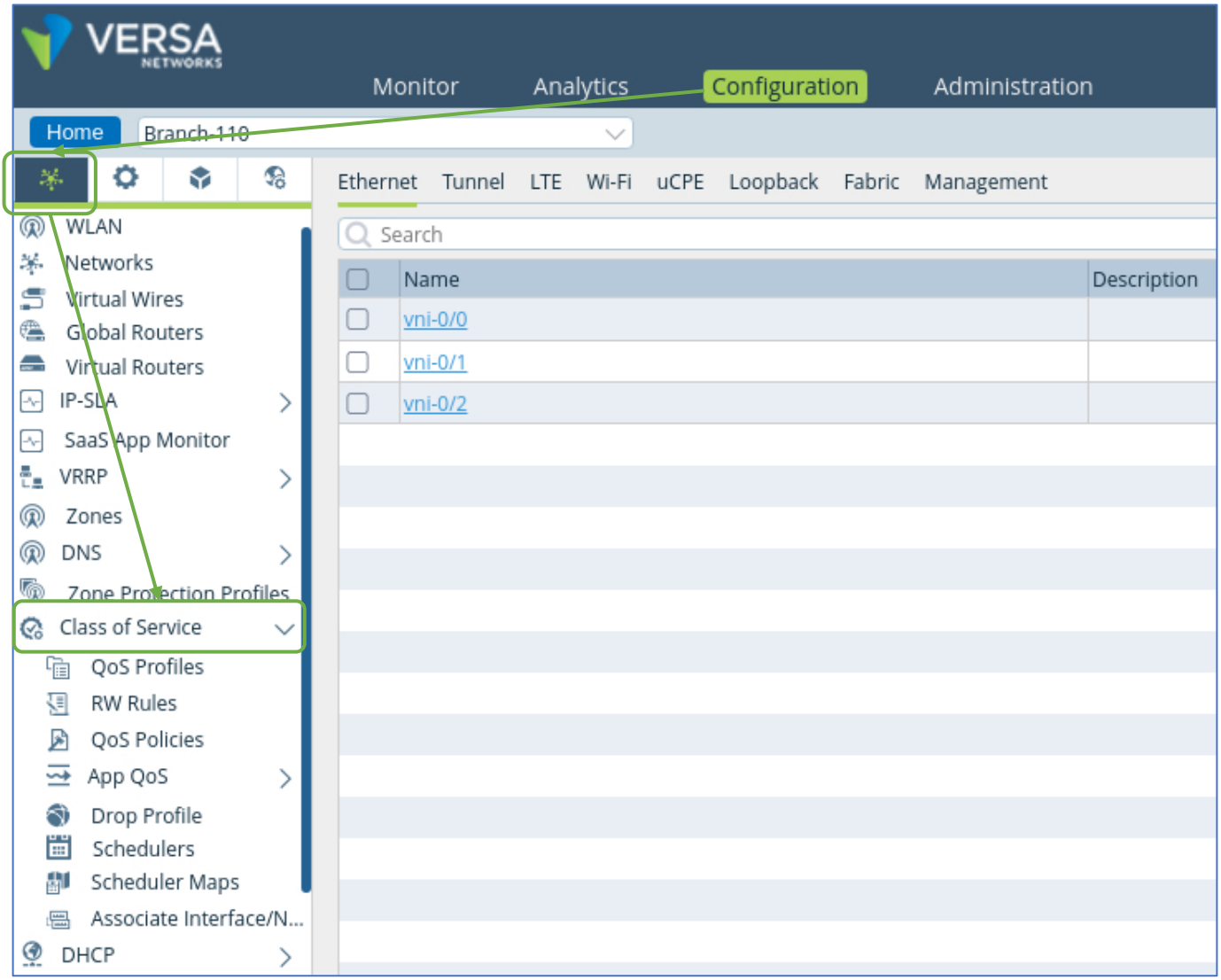
From Versa Director, open the Administration > Appliances dashboard to display the deployed devices. Locate your device in the list and click on the link to your device. This will open the Appliance Context of your device.



From the Appliance Context mode 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.



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

Exercise 3: Configure Basic Class of Service

In the following exercise you will:

- Configure 3 QoS Profiles
- Configure an AppQoS policy with 3 rules to identify different types of traffic
- Configure 4 Schedulers (1 for each major traffic class)
- Create a Scheduler Map to bundle the schedulers together in a set
- Apply the Scheduler Map to the WAN facing ports (MPLS and INET) of your node

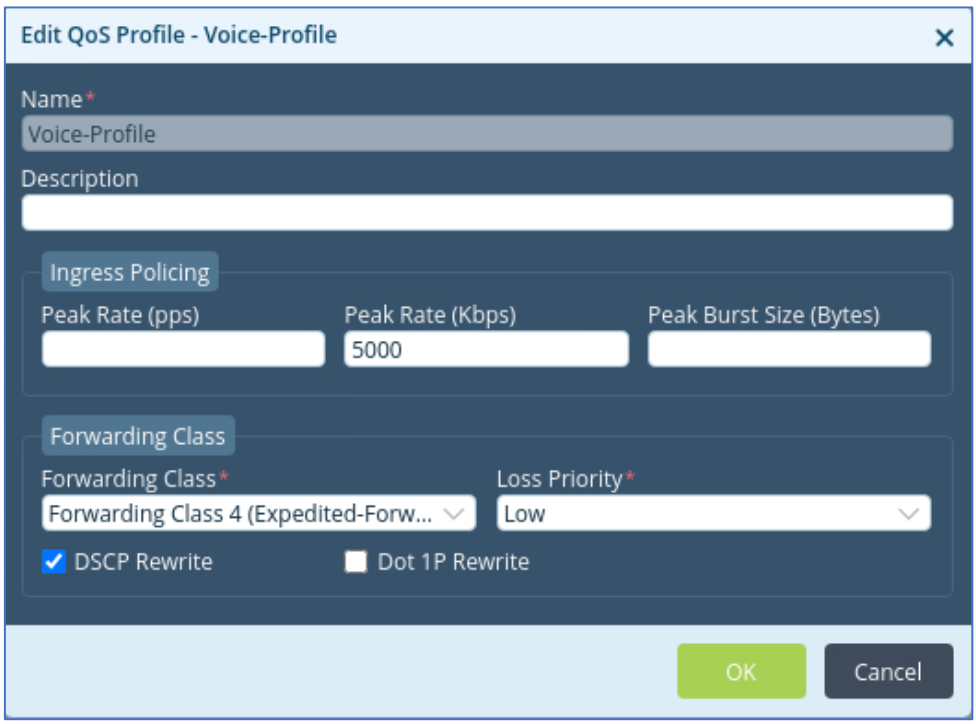
QoS Profiles

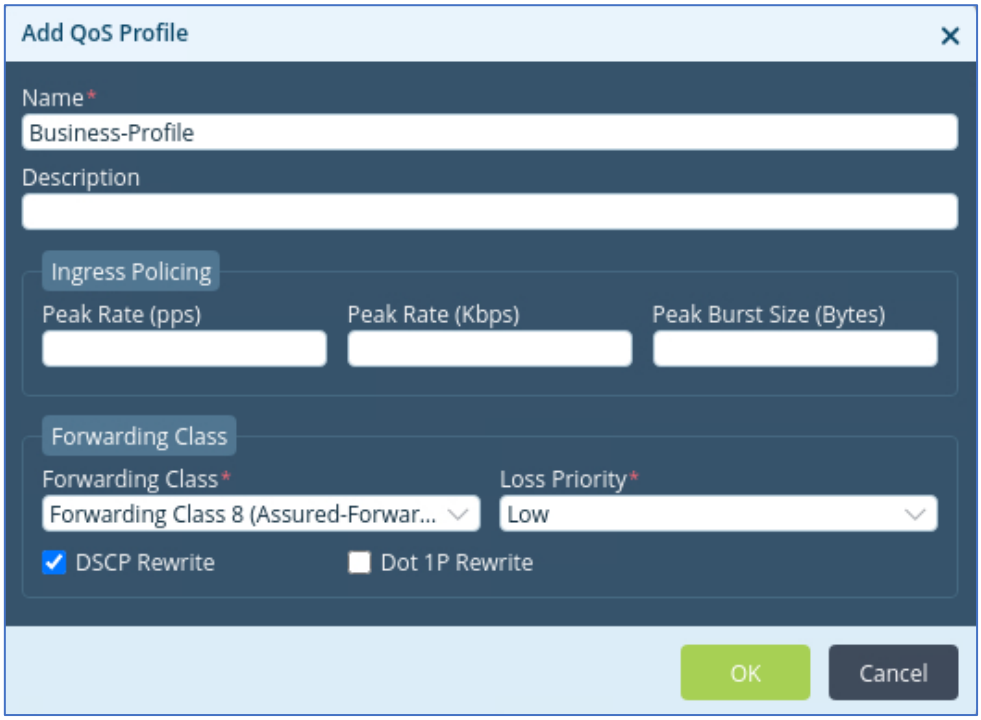
A QoS Profile defines how traffic will be treated that is mapped to that profile. A QoS or AppQoS policy uses the QoS Profile as an enforce action for matching traffic, and therefore the QoS profile must be created before the policy.

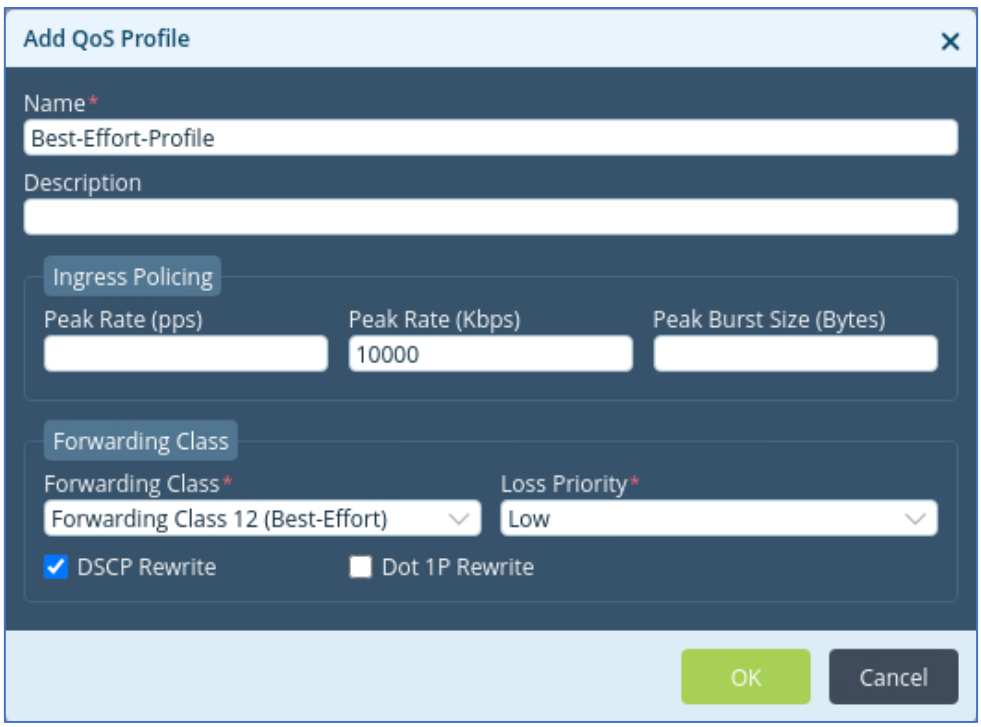
In this lab part you will create 3 QoS profiles:

- Voice-Profile
- Business-Profile
- Best-Effort-Profile

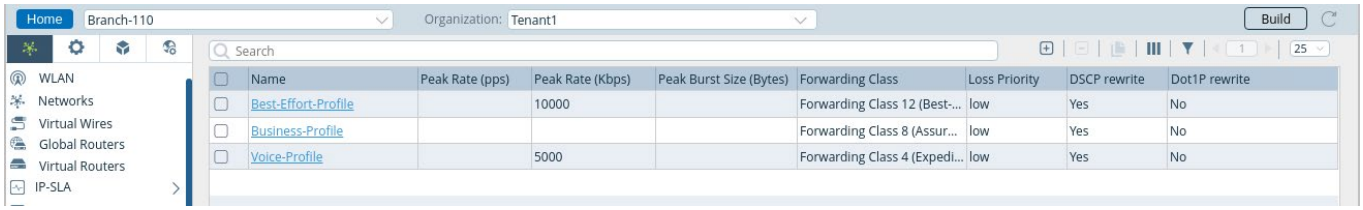
The parameters for each profile are shown below.







When finished, your configuration should resemble the example below.



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.

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.

Ensure that the Rules tab is open and add the following rules to the policy:

Rule 1

General Tab	
Rule Name:	Voice-Traffic
Source/Destination Tab	
Source Zone:	Select the zone associated with your LAN network
Destination Zone:	Select the Intf-MPLS-Zone and Intf-INET-Zone
Source Address:	Leave Blank
Destination Address:	Leave Blank
Headers/Schedule Tab	
Leave all fields empty	

Applications/URL Tab	
Applications:	VOIP, SIP, MS_TEAMS, SKYPE
URL Categories:	Leave Empty
Enforce Tab	
QoS Profile:	Voice-Profile

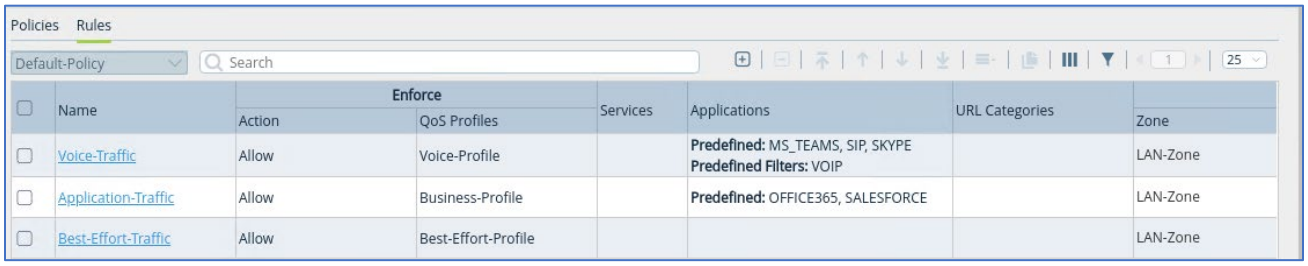
Rule 2

General Tab	
Rule Name:	Application-Traffic
Source/Destination Tab	
Source Zone:	Select the zone associated with your LAN network
Destination Zone:	Select the Intf-MPLS-Zone and Intf-INET-Zone
Source Address:	Leave Blank
Destination Address:	Leave Blank
Headers/Schedule Tab	
Leave all fields empty	
Applications/URL Tab	
Applications:	OFFICE365, SALESFORCE
URL Categories:	Leave empty
Enforce Tab	
QoS Profile:	Business-Profile

Rule 3

General Tab	
Rule Name:	Application-Traffic
Source/Destination Tab	
Source Zone:	Select the zone associated with your LAN network
Destination Zone:	Select the Intf-MPLS-Zone and Intf-INET-Zone
Source Address:	Leave Blank
Destination Address:	Leave Blank
Headers/Schedule Tab	
Leave all fields empty	
Applications/URL Tab	
Applications:	Leave Empty
URL Categories:	Leave empty
Enforce Tab	
QoS Profile:	Best-Effort-Profile

When finished your configuration should look similar to this:



Schedulers

A scheduler defines the algorithm used to determine how frequently packets are pulled from a queue and placed on the wire. Each major traffic class has 4 forwarding classes. Each forwarding class is mapped to a queue, and therefore there are 4 queues in each major traffic class.

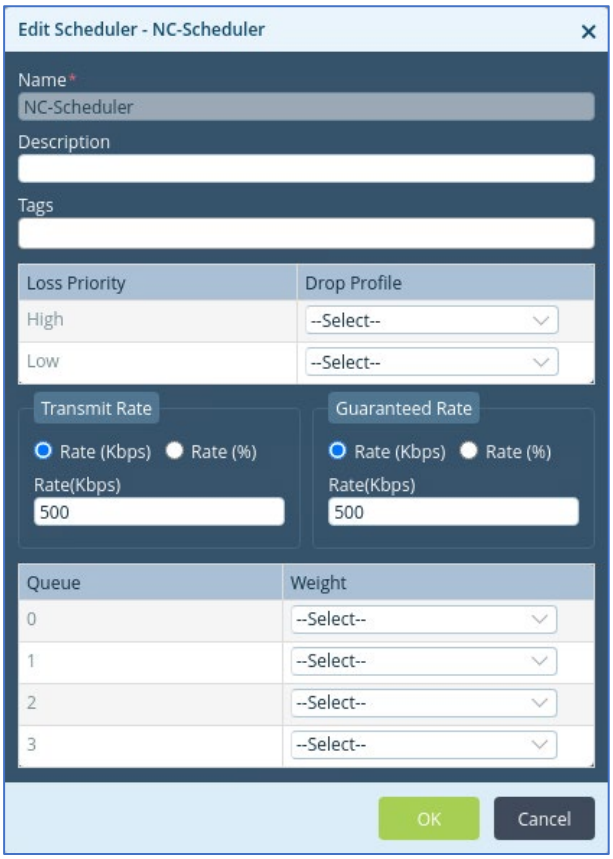
Each traffic class must pull traffic from its 4 queues. The scheduler defines the ratio of traffic that is pulled from each queue to be sent to the outbound interface.

Create 4 schedulers (one for each major traffic class

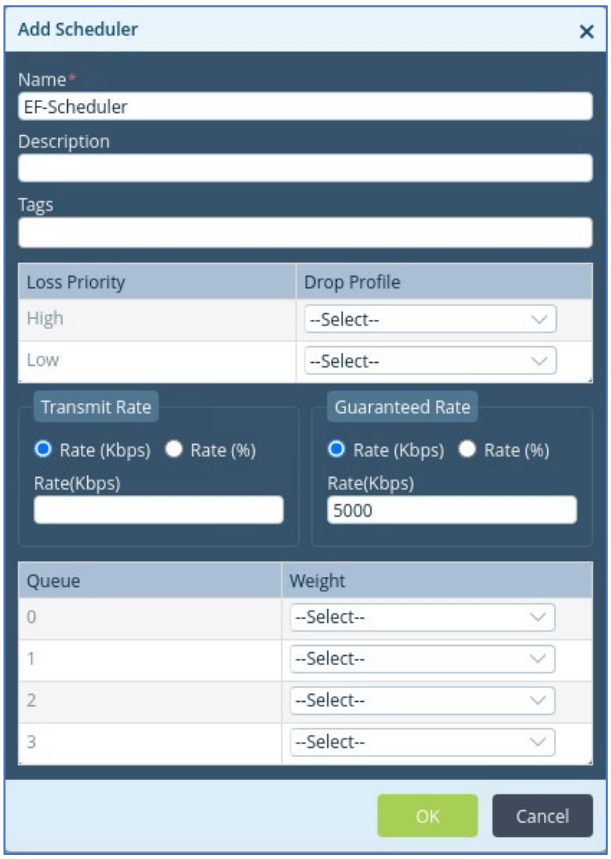
In this lab part you will create 3 QoS profiles:

- Voice-Profile
- Business-Profile
- Best-Effort-Profile

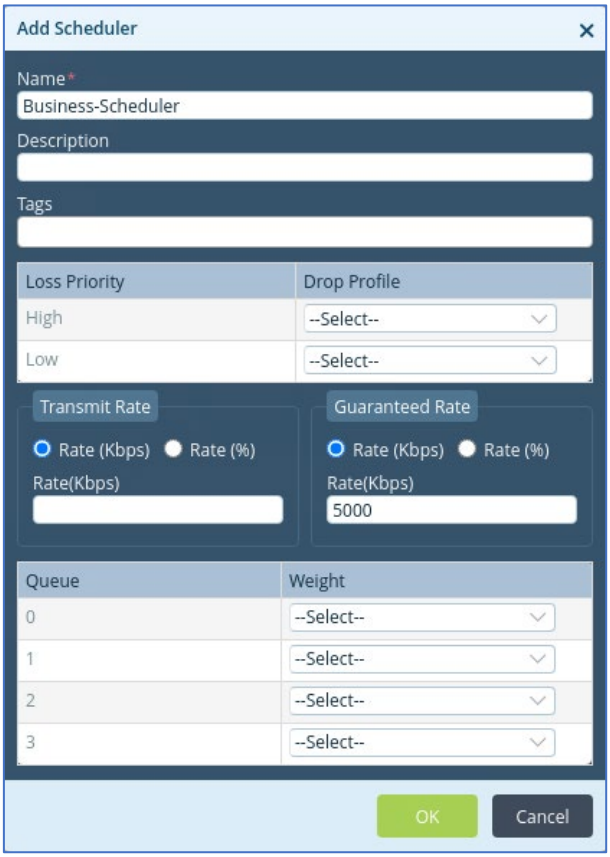
The parameters for each profile are shown below.



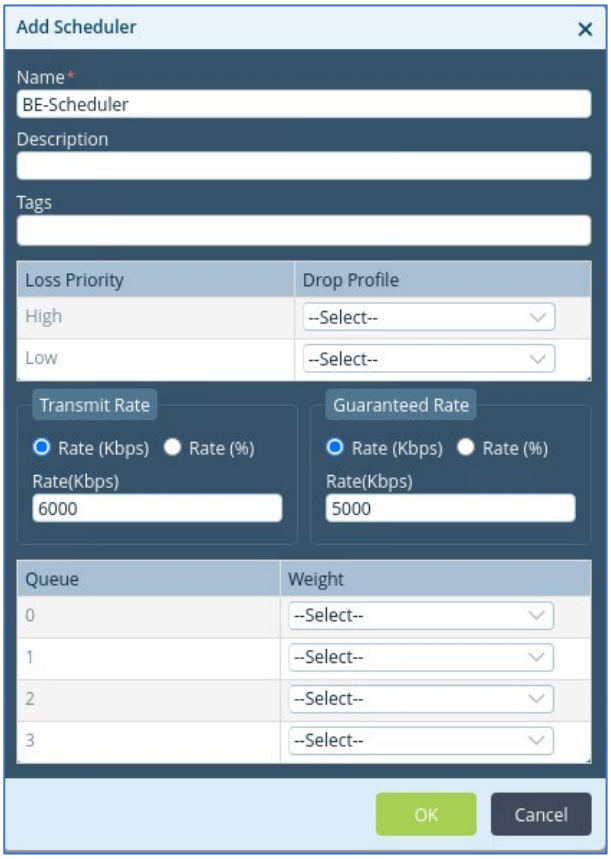
This scheduler guarantees the rate of 500Kbps, but also places a cap on the rate at 500Kbps.



This scheduler guarantees the rate of 5000Kbps, but allows the scheduler to transmit above that rate if other schedulers are not using the interface.



This scheduler guarantees the rate of 5000Kbps, but allows the scheduler to transmit above that rate if other schedulers are not using the interface.



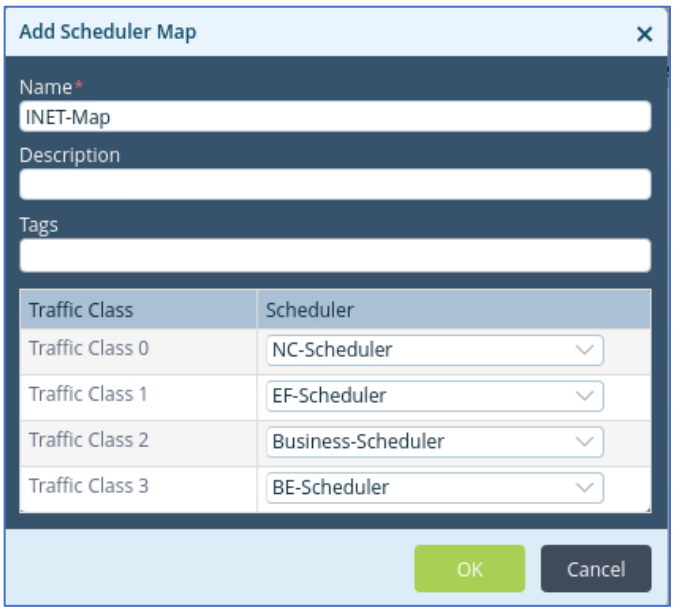
This scheduler guarantees the rate of 5000Kbps, but limits the total rate at 6000kbps, even when other schedules are not using the interface.

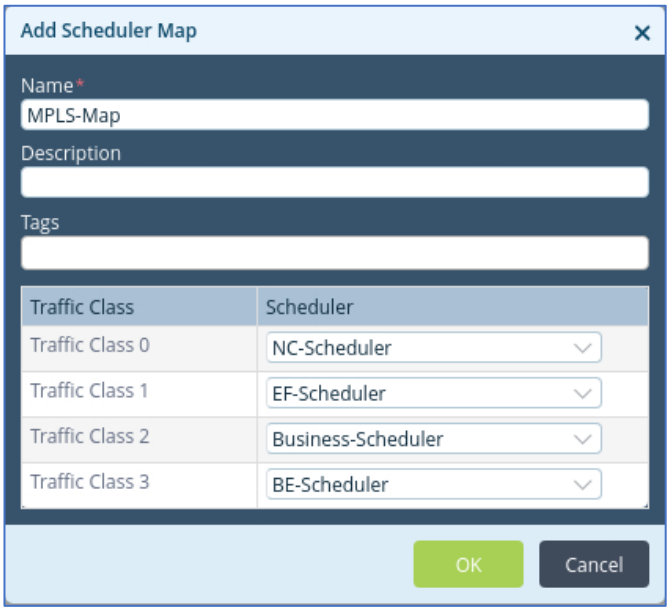
Note: Each of the main schedulers can service up to 4 queues. Because we only mapped traffic into queue 0 of each major traffic class, we do not have to adjust the ratio of packets coming from each forwarding class (queue). If we were to map traffic in the AppQoS policy to multiple forwarding classes within a major traffic class, then we would have to configure the ratio of traffic by selecting a Weight for each queue (or the default values could be left in place, which would service all queues equally). Where a guaranteed rate is configured for the main traffic class, the queues share the guaranteed rate and transmit rate.

Scheduler Map

A scheduler map assigns schedulers to a traffic class. There are 4 main traffic classes. The scheduler is the algorithm used to define how frequently traffic will be pulled from queues. The algorithm is assigned to a traffic class. This means that, if desired, the same algorithm (scheduler) can be used on multiple traffic classes if desired. For our example, a unique scheduler will be assigned to each traffic class.

Create the following scheduler maps. Although the scheduler maps can be unique, for our example both scheduler maps will be the same (one for the INET transport link and one for the MPLS transport link.) A common scenario where the scheduler maps may be unique would be where the MPLS transport and INET transport have different bandwidth capabilities, and therefore the schedulers would have different rates associated with the forwarding classes for each transport link.



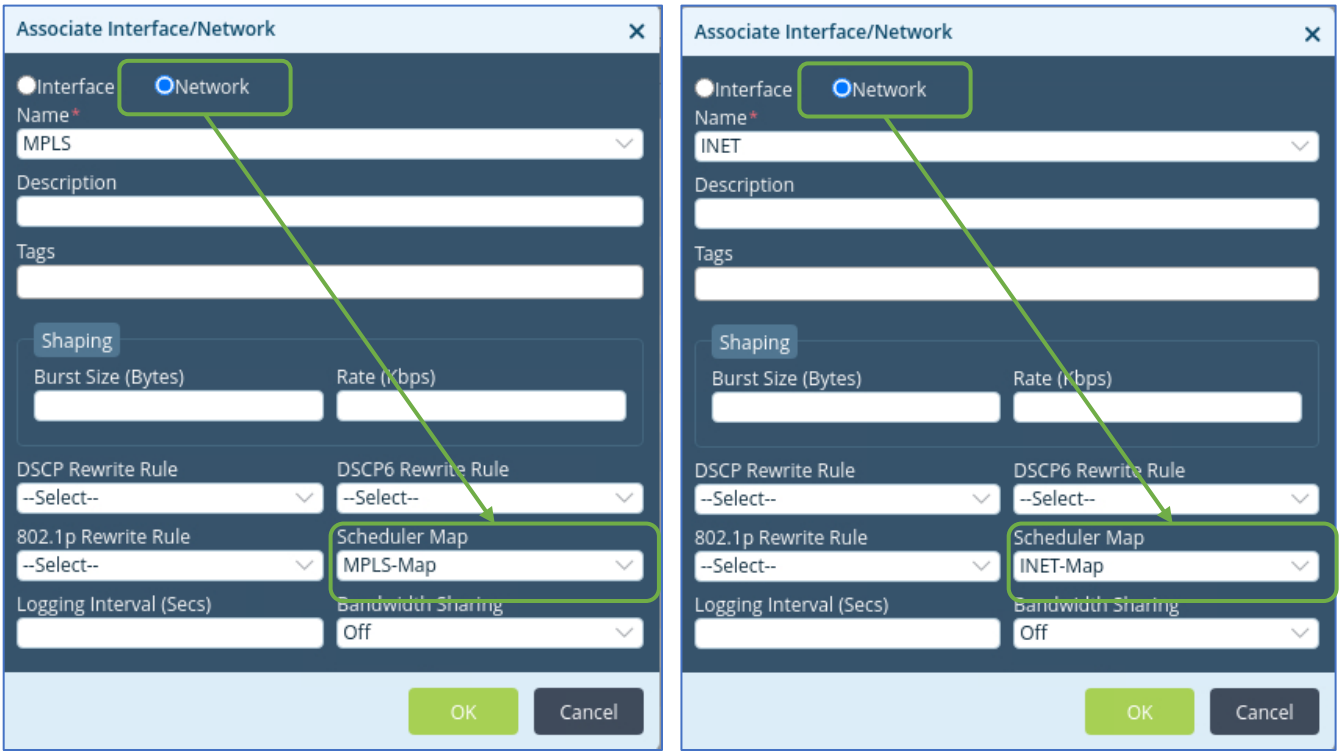


Associate Interface/Network

The final step is to associate the scheduler map, and it's properties, to the outbound interfaces. This step is where all of the previous Class of Service configuration is applied to an interface.

Class of Service parameters (the scheduler map) can be applied to an Interface or a logical network. The Interface association refers to the vni-x/y interface. The Network association refers to the assignment to a network name (LAN, MPLS, INET, etc.)

Create the following Network-to-Scheduler-Map assignments:

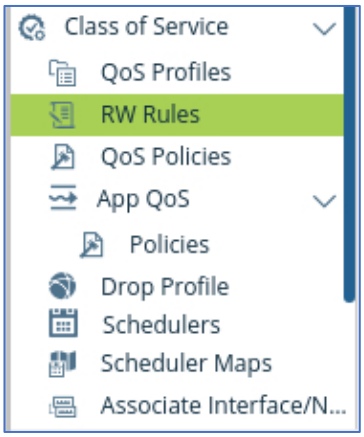


You did not configure any shaping parameters in the Associate Interface/Networks parameters, and therefore the physical interface speed will be used for rate calculations and transmission.

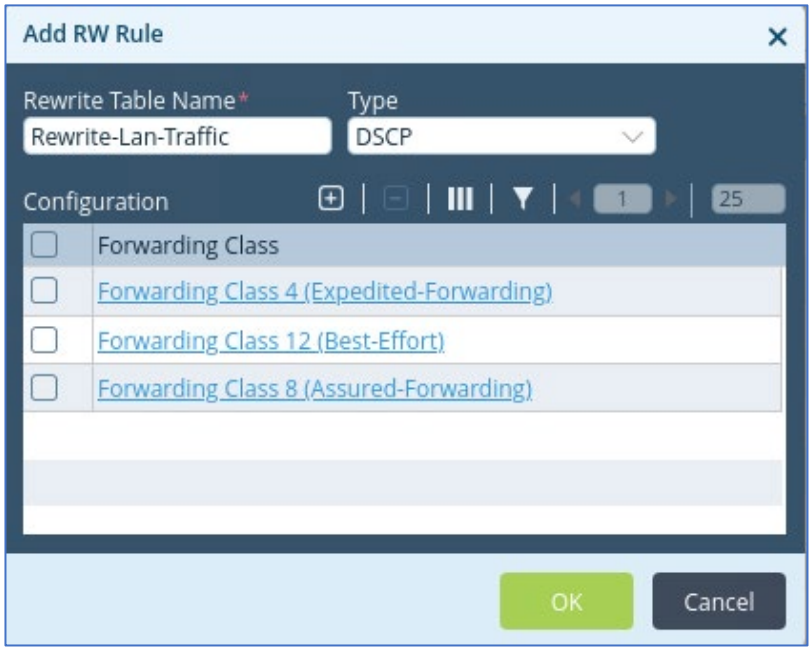
Exercise 4: Configure DSCP Rewrite Rules

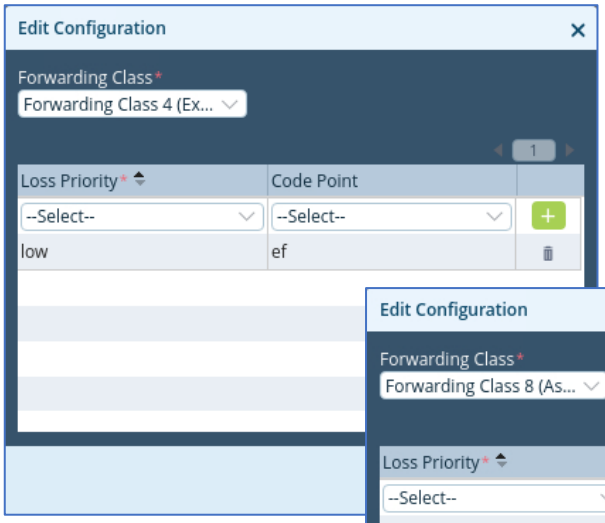
You classified traffic as it entered your device by using a policy, which identified traffic based on application identification properties. In the next lab part you will create a DSCP rewrite rule that will write the DSCP bits in the headers of packets based on the traffic classification assigned to the traffic as it entered the device.

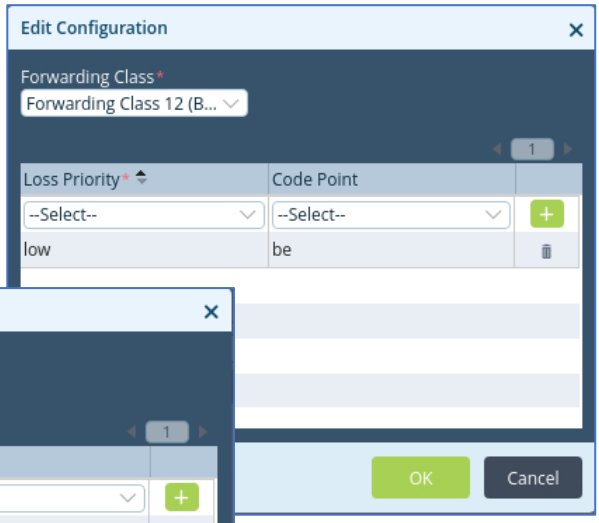
Locate and open the RW Rules configuration.

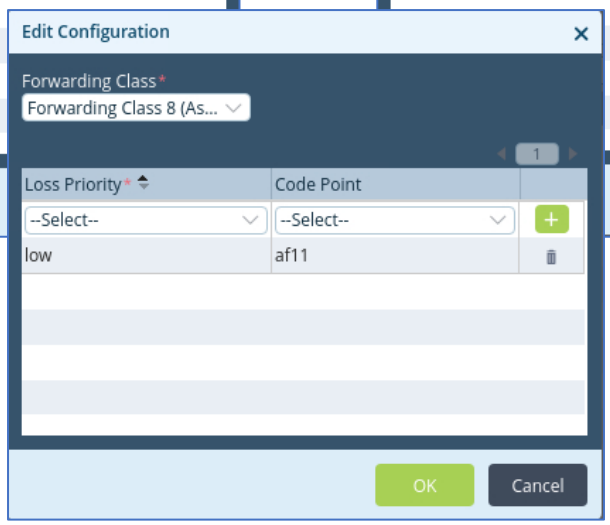


Configure a single Rewrite Rule that rewrites the bits in 3 of the main forwarding classes as shown below:







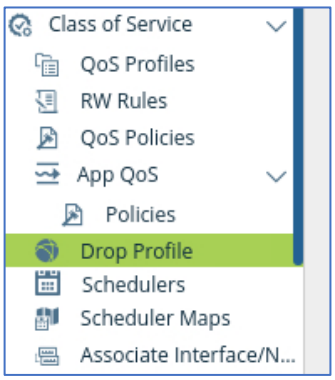


Once the rewrite rules are created, you need to apply the rewrite rules in order for them to take effect. The rewrite rules are applied in the Associate Interface/Network hierarchy, in the same location where the Scheduler Map is applied to outbound traffic.

Exercise 5: Configure Drop Profiles

When an interface queue (buffer) becomes full because the incoming traffic exceeds the outbound circuit speed, packets entering the device must be dropped. Drop profiles allow the administrator to define how deep the buffers are for each queue and when to begin the process of randomly dropping packets to avoid filling the buffer. There are default drop profile properties enabled on the device, but the administrator may want to adjust the buffer depths of queues in order to improve service and control what traffic is dropped during periods of congestion.

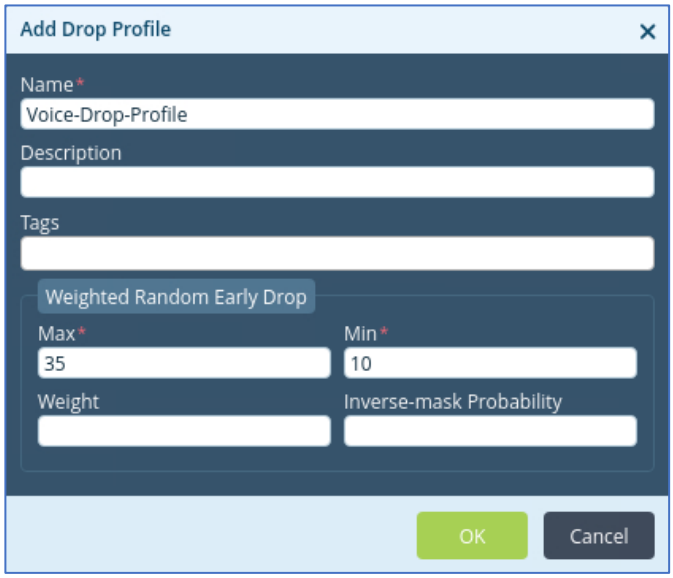
The drop profile parameters are defined under the Drop Profiles configuration hierarchy. They are then assigned to an interface under the Associate Interface/Network configuration.



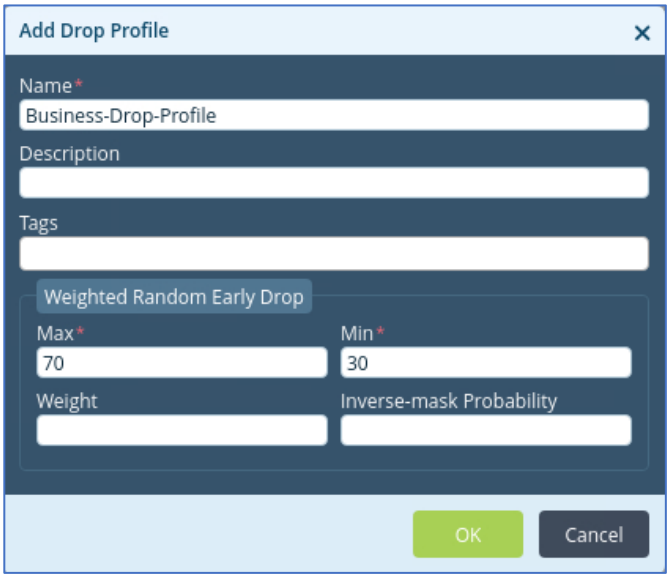
In the next lab part you will configure drop profiles.

Locate and open the Drop Profiles configuration.

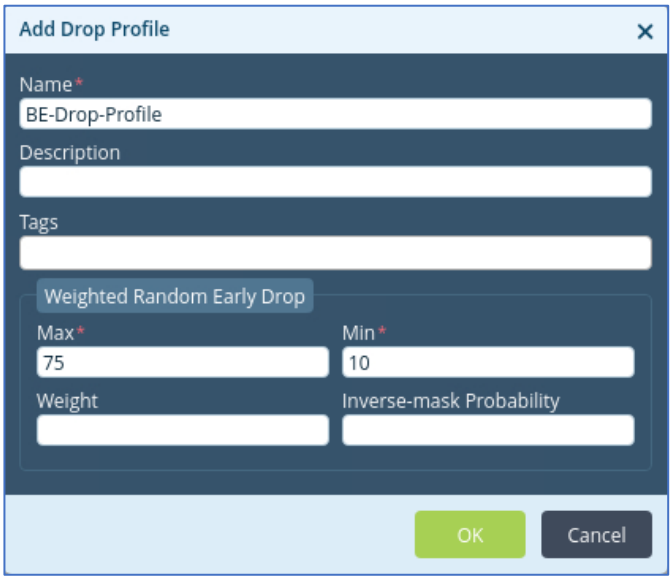
Configure the following drop profiles to define buffer and drop properties. The names of the profiles are descriptive because these profiles will be applied in a later step, and the names will make it easier to identify the proper drop profile.



In this drop profile, the queue depth is kept to a minimum (35 packets) because voice traffic is delay/jitter sensitive. Packets will begin to be dropped when 10 packets are backed up in the associated queue.



In this drop profile, the queue can fill up with 70 packets, and packets won't be dropped until at least 30 packets are buffered. This may help preserve data packets at the expense of more delay or jitter.



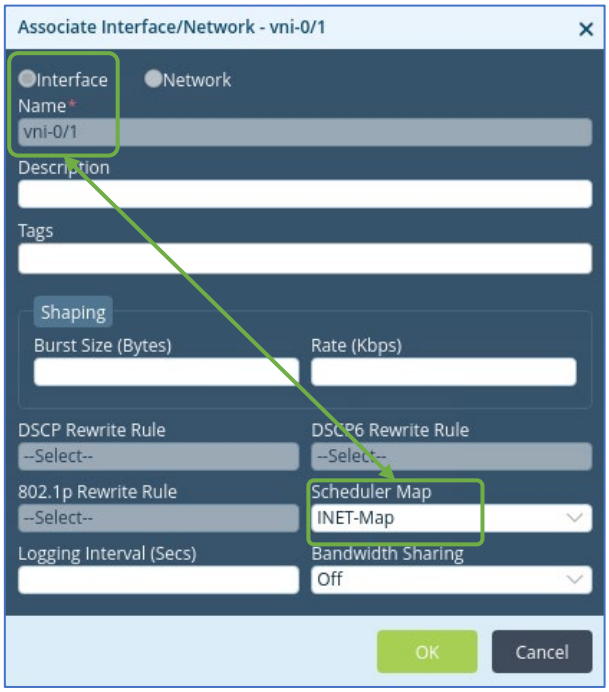
In this drop profile, the queue can fill up with 75 packets, and packets will begin to be dropped once 10 packets are in the buffer.

Now that the drop profile parameters have been defined, the drop profile must be assigned to the outbound traffic processes in the schedulers. However, drop profiles cannot be associated to a Network name, and must be associated with an Interface (vni-x/y).

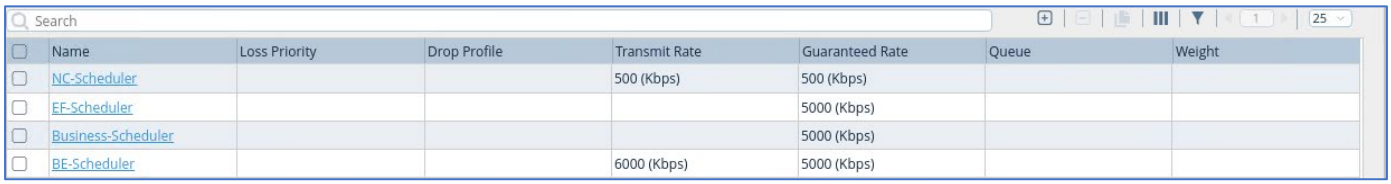
To allow the assignment of a drop profile, you will remove the previous Network association and replace them with interface associations.

In the Associate Interface/Network hierarchy, select and delete the MPLS and INET associations.

After the MPLS and INET associations are removed, create 2 new associations, one for each of the 2 interfaces. Be sure that the associations are to the interface and NOT to the network.



After the new interface associations are complete, you will be allowed to add the drop profiles to the schedulers. If the schedulers/scheduler map is still associated with a network name (instead of an interface) you will receive an error when you try to apply the drop profile to the scheduler.

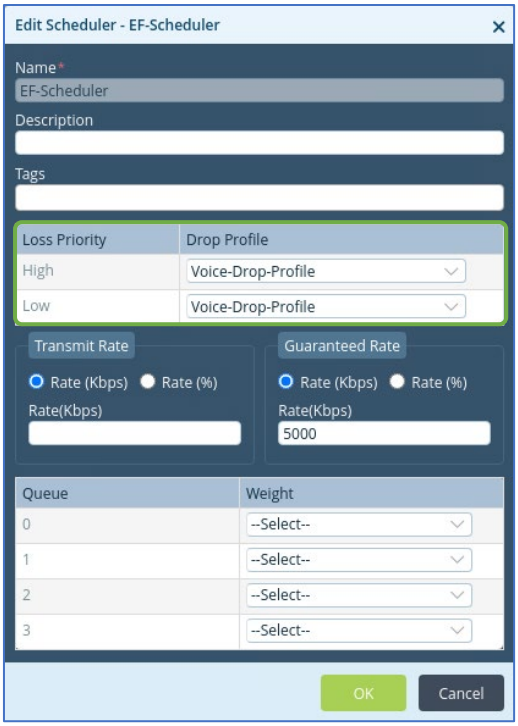


Open the Schedulers

Assign the Voice-Drop-Profile to the EF-Scheduler scheduler.

Assign the Business-Drop-Profile to the Business-Scheduler scheduler.

Assign the BE-Drop-Profile to the BE-Scheduler scheduler.



Search

Name	Loss Priority	Drop Profile	Transmit Rate	Guaranteed Rate
NC-Scheduler			500 (Kbps)	500 (Kbps)
EF-Scheduler	low	Voice-Drop-Profile		5000 (Kbps)
	high	Voice-Drop-Profile		
Business-Scheduler	low	Business-Drop-Profile		5000 (Kbps)
	high	Business-Drop-Profile		
BE-Scheduler	low	BE-Drop-Profile	6000 (Kbps)	5000 (Kbps)
	high	BE-Drop-Profile		

Final Schedulers Results

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