Lab 6: Quality of service. Port mirroring

Contents

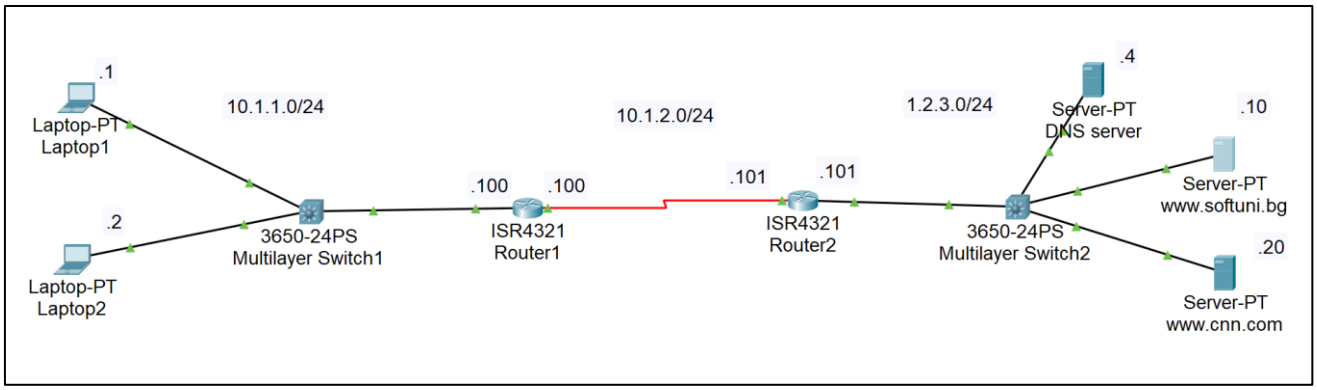
Introduction to LAB 6

This lab has two exercises. In the first one, you are going to configure and explore some of the QoS (quality of service) concepts. In the second exercise, you are going to configure port mirroring, or SPAN (Switched Port Analyzer).

Exercise 1: Quality of service

Task 1: Create the topology

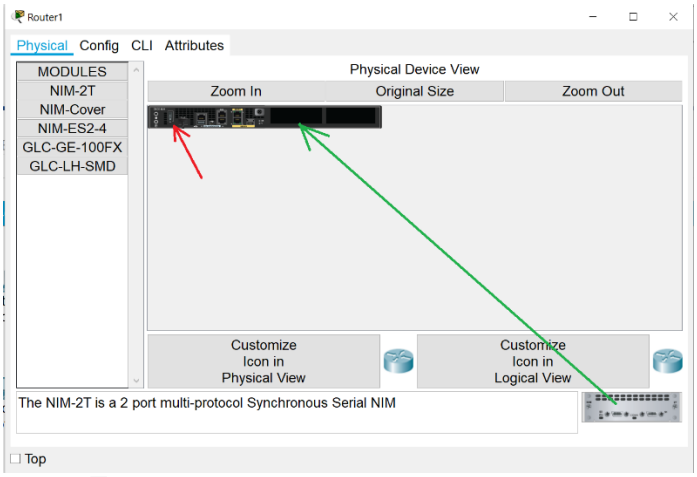
Use the picture below as a reference while creating the topology for this exercise:



Some guidelines to use (please read the whole list first):

- There are 3 networks: 10.1.1.0/24, 10.1.2.0/24 and 1.2.3.0/24
- The last octet of each host/interface address is shown on the picture
- You need to configure end-to-end connectivity between the laptops and the servers. You can use static or dynamic routing for this purpose
- The DNS server (1.2.3.4) should be configured to provide DNS service and "A" records for:
  - www.softuni.bg -> 1.2.3.10
  - www.cnn.com -> 1.2.3.20
- The end devices (the laptops) should have 1.2.3.4 as their DNS server

- Between the routers, use serial links. The reason for this is that they represent much slower connection (1544 kbps), so we need to prioritize the traffic. To do this, you need to have a serial port on the routers. They don't have them by default, so you have to add them. Under the Physical tab, first shutdown the router (hit the **1/0** button, the red arrow on the picture) and then drag the NIM-2T module to the chassis (the green arrow on the picture). Then power on the router again.



DCE_DTE Cables.png

  Do the same for the other router. Then, connect them via serial cables. For information about DCE/DTE, please open the attached picture above (DCE_DTE Cables.png)
- You need to power on the 3650-24PS switches. To do this, insert the power supply into the chassis – similar to the way you inserted the serial modules in the routers

Task 2: Configure QoS on both routers

First, ensure that you have L3 connectivity between the laptops and the web servers. Again, you can configure this with static or dynamic routing.

Now that we have the devices and connectivity between them, we can start configuring QoS. We will have 3 types of policies – for voice (which we will not

test), for http traffic, and for icmp. We will use NBAR (network-based application recognition) for traffic classification method (instead of the other classification method – header inspection). This will be done on Router1, so this way it will prioritize the traffic sent over the slow serial link.

On Router1:

class-map voice

match protocol rtp (this leverages NBAR on the router)

exit

class-map http

match protocol http (NBAR again)

exit

class-map icmp

match protocol icmp (NBAR)

exit

policy-map mark

class voice

set ip dcsp ef

priority 100

exit

class http

set ip dscp af31

bandwidth 50

exit

class icmp

```
        set ip dscp af11
        bandwidth 25
        exit
    exit
int s0/1/0
    service-policy output mark
```

Explanations: For the class "voice", we use dscp ef (expedited forwarding), which will ensure that these packets are sent without delay. We also want to limit somehow this, because it may happen that the voice packets utilize the whole bandwidth. That is why we have the "100" limit. The other two classes – http and icmp are identified (with NBAR) and marked with DSCP AF31 and DSCP AF11 respectively. What these values mean?

- DSCP AF31 – Assured Forwarding, Class 3, low drop probability
- DSCP AF11 – Assured Forwarding, Class 1, low drop probability

Also, both of these classes have different minimum bandwidth values (50 and 25).

Finally, we apply our service policy to the outbound interface of Router1.

This is enough for the traffic to be classified, marked and served based on each packet priority when it travels to Router2.

Why do we have QoS configuration or Router2 then? The answer is – to practice what else we can do with QoS. In this example, we are going to remark the **DSCP values** of the packets coming from Router1 with **precedence values** on Router2. Let's say that we have other devices after Router2, which understand only precedence. Again, this is just illustration on some of the capabilities of the QoS configurations.

On Router2:

```
class-map voice
```

```
        match ip dscp ef
        exit
class-map http
        match ip dscp af31
        exit
class-map icmp
        match ip dscp af11
        exit
policy-map remark
        class voice
                set precedence 5
                exit
        class http
                set precedence 3
                exit
        class icmp
                set precedence 0
                exit
int s0/1/0
        service-policy input remark
```

Explanations:

With these policy-map commands we are changing, or re-writing, the DSCP values in the TOS (type of service) field in the IP header of the packets using precedence rather than DSCP values

Now, on Router2 we are just reading the DSCP values from inside the packets and we are not doing NBAR

On Router1 type:

show policy-map interface s0/1/0 – there are no matches for voice, http or icmp

On Router2 type:

show policy-map interface s0/1/0 – there are no matches for voice, http or icmp

Now go and generate some traffic – from the laptops make ICMP requests (pings) and also WEB requests (to www.softuni.bg and www.cnn.com).

Then repeat the above show commands. You should see matches for http and icmp (and not for voice). You can also monitor with Simulation mode.

Note: You can use the attached screenshot for reference how IP precedence and DSCP values correspond.

IP_Precedence-DSCP.png

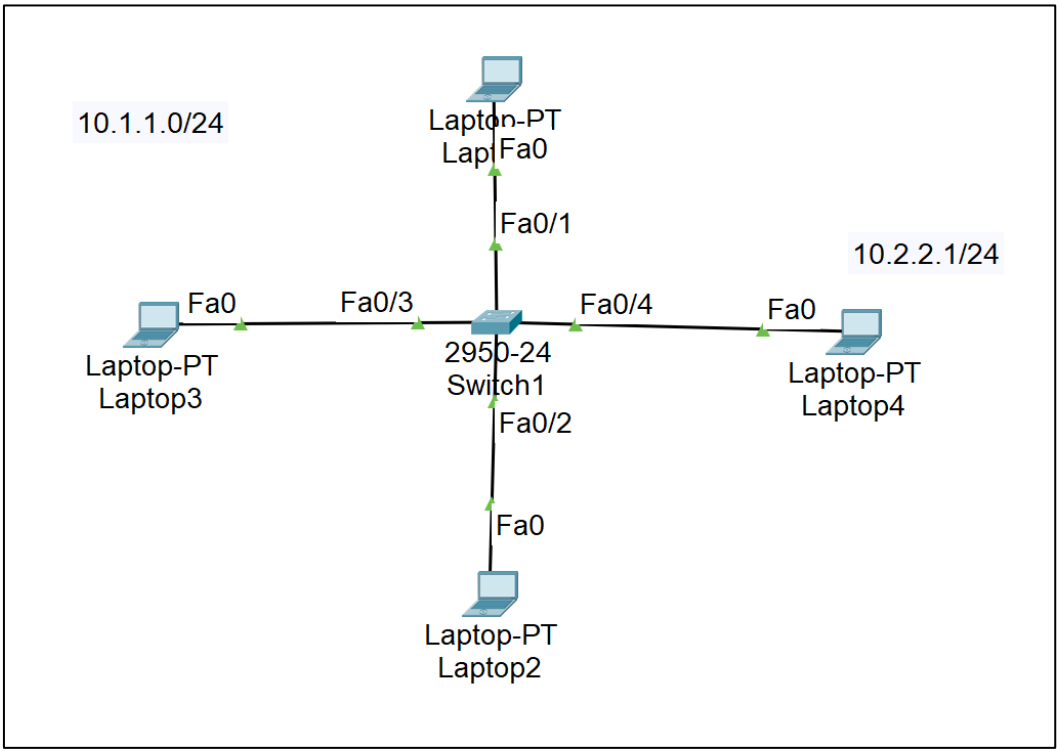
Exercise 2: Port mirroring

Task 1: Configure Local SPAN (Switched Port Analyzer)

In this task, you are going to configure local SPAN, which means that the monitoring station is connected to the same switch as the traffic which is being monitored.

1. Create the topology

   Please connect the devices as per the picture below. Note that you have to use **2950-24** switch.



Please use the following guidelines for your configurations:

- Laptop1, Laptop2 and Laptop3 belong to VLAN 1 and to 10.1.1.0/24 network. Please configure their IP addresses from this IP network
- Laptop4 (Fa0/4) belongs to VLAN 2. Optionally, you can configure its IP address to be 10.2.2.1/24

2. Configure SPAN

In the real world, you can create a source VLAN from which you can copy traffic to a port. Because of the Packet Tracer specifics, here we are going to create source ports from which we are going to copy/mirror the traffic (not a VLAN)

Use the following commands to configure local SPAN:

On Switch1:

- **monitor session 1 source interface fa0/1 both** ("both" here means both ingress and egress traffic for this interface)

do show monitor – check the current SPAN configuration (optional)

- **monitor session 1 destination interface Fa0/4**
  do show monitor – check the current SPAN configuration (optional)

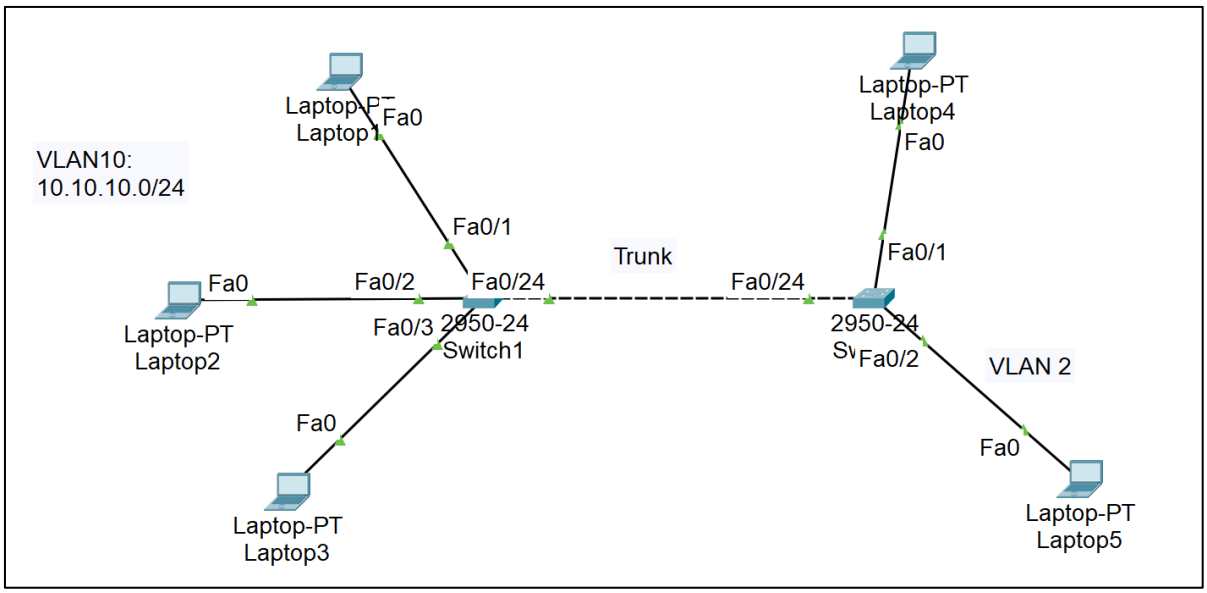
3. Monitor the behavior in Simulation mode
   Make an ICMP (ping) tests by pinging between the laptops in VLAN 1 (Laptop1, Laptop2 and Laptop3). Start the simulation mode in Packet Tracer and observe the behavior – each ICMP packet, originated or destined from/to Laptop1, is also copied to Fa0/4 and goes to Laptop4. The laptop will discard the packet since it will not recognize itself looking at the destination MAC address. (In for this to happen, in the real world, you need to have a packet capturing software, like Wireshark and the network card should be in promiscuous mode).

Task 2: Configure RSPAN (Remote SPAN)

In this task, you are going to configure RSPAN, meaning that the traffic that you are monitoring is copied from one switch to another (over a trunk) and then sent to a computer connected to the remote switch.

1. Create the topology

   Please connect the devices as per the picture below. Note that you have to use **2950-24** switches.



Please use the following guidelines for your configurations:

- Create VLAN 10 on Switch1 (the clients) and VLAN 2 on Switch2 (for the station which will monitor the traffic)
- Create VLAN 99 on both switches. This VLAN will be used for carrying the monitored traffic between the switches
- The Switch1 ports to Laptop1, Laptop2 and Laptop3 should be access ports in VLAN 10
- Assign ip addresses on Laptop1, Laptop2 and Laptop3 from the 10.10.10.0/24 network
- The Switch2 port which goes to Laptop5 should be access port in VLAN 2
- Switch1 to Switch2 link should be configured as trunk and all VLANs should be allowed on it. In the example configuration, these are ports Fa0/24 on both switches
- Choose one port on Switch1 which is going to be used as **reflector port**, meaning that nothing should be connected to it

2. Configure RSPAN
   In order to monitor the communication in VLAN 10 to and from Laptop1 (which is connected to Fa0/1 on Switch1 in this example), use the following configurations on the switches.

On Switch1:

monitor session 1 source interface fa0/1 both ("both" here means both ingress and egress traffic for this interface)

do show monitor – check the current SPAN configuration (optional)

monitor session 1 destination remote vlan 99 reflector-port fa0/23

do show monitor – check the current SPAN configuration (optional)

On Switch2:

monitor session 1 destination interface fa0/2 (the port which goes to Laptop5, which is monitoring the traffic)

monitor session 1 source remote vlan 99

Note: After this configuration, you may start seeing messages that "Native VLAN mismatch discovered". You can ignore this in this particular situation.

3. Monitor the behavior in Simulation mode
   Make an ICMP (ping) tests by pinging between the laptops in VLAN 10 (Laptop1, Laptop2 and Laptop3). Start the simulation mode in Packet Tracer and observe the behavior – each ICMP packet, originated or destined from/to Laptop1, is also copied from Switch1 to Switch2 (tagged) and then goes to Laptop5. Laptop5 is in VLAN 2 and may or may not have an IP address – in either case, the laptop will discard the packet since it will not recognize itself looking at the destination MAC address. (In order for this to happen in the real world, you need to have a packet capturing software, like Wireshark and the network card should be in promiscuous mode).

You have completed LAB 6.