Lab Exercise Sheet 3

Dynamic Host Configuration and Virtual LAN

Document and analyze your experimental procedures by using your Wireshark and terminal recordings. Note all relevant intermediate steps. Mark and explain all relevant information, such as protocol header fields, MAC addresses, IP addresses, port numbers. If you have little experience with Linux, you may need to do some research.

Group number:	
First name:	
Last name:	
Student number:	

This lab exercise uses the network topology from Exercise 1! Therefore the setup of the presented network with its topology form Exercise 1 is mandatory for successful participation in this lab exercise!

In this lab, you will perform variant experiments on Linux machines running the operating system Debian. For the lab exercise, you need to disable the Network Manager if it is not already disabled by default! Your configuration on the hosts needs to be done **dynamically**! The configuration for the **Virtual LAN** needs to be done among others in parts on the switches! For detailed information on the switches please consult the manual of the *TP-Link TL-SG108E* Switch!

Furthermore, the experiments need to be conducted using the Command-Line Interface (CLI) and Wireshark. In the lab exercise, you find boxes with questions regarding the tasks performed. You need to **demonstrate and answer** the questions in the exercise session to pass the lab exercise!

Examination

For every Lab Exercise you need to prepare slides documenting your setup! The slides should contain your network configurations, steps performed and screenshots of relevant captures! Send your slides to your lecturer and present your results in the lecture!

1. **Setting up the initial network**

   Please setup your configuration from lab exercise 1! In lab exercise 1 you were asked to configure a network using IP version 4. The network consisted of **4 Host machines** in a private network. One machine was configured as the router of the private network with the network address `192.168.i.0/24`. The number `i` in the IP address is a placeholder for your **group number**!

   The machines have the following configuration:

   Host machines:

   Router 1 – `eth0` – `192.168.i.1`

   Host 1 – `eth0` – `192.168.i.10`

   Host 2 – `eth0` – `192.168.i.20`

   Host 3 – `eth0` – `192.168.i.30`

   Router 1 interfaces:

   `eth0` – `192.168.i.1`

   `eth1` – `10.16.0.i`

   Router 1 needs to be configured as a router in the network with the IP address `192.168.i.1` on the interface `eth0`[1]. The second network interface `eth1` needs to be configured with the IP address `10.16.0.i`. The interface `eth1` with IP address `10.16.0.i` is the route to a **second** private network with the network address `10.16.0.0/16` and the **Router 2** (address `10.16.0.200`).

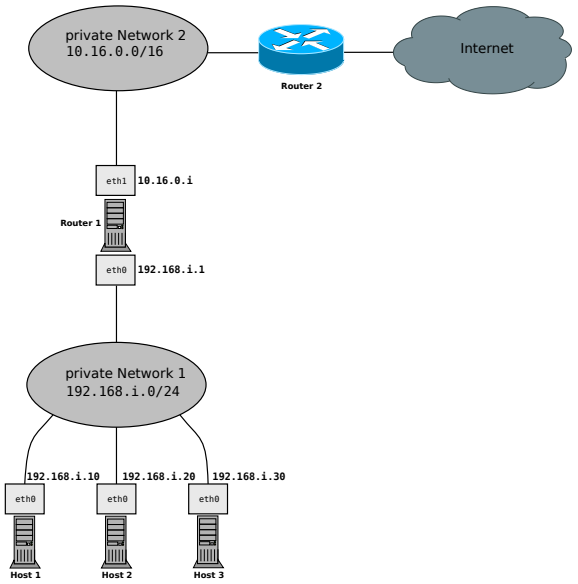

Figure 1: Network Topology of lab exercise 1

[1]The interfaces names can differ on Linux distributions and systems! In the literature the old predictable naming scheme using `ethX` is often found. In newer versions `systemd` uses a different naming scheme!
`https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/`

Configuring the Switch

For this exercise you need to configure the Switch! Log into the Switch with **user:** `admin` and **password:** `admin` and address `http://192.168.0.1`. There you need to disable *Loop Prevention* and turn off DHCP on the Switch!

2. **Setting up the Switches and VLAN**

In this exercise you are asked to configure the Switch in such a way that you have two separate private networks for your hosts! To achieve that you are asked to setup two **Virtual LANs** on the Switch! The VLANs can be configured in the management GUI of the Switch! Figure 2 shows the setup of the VLAN. Assign addresses according to table 1!

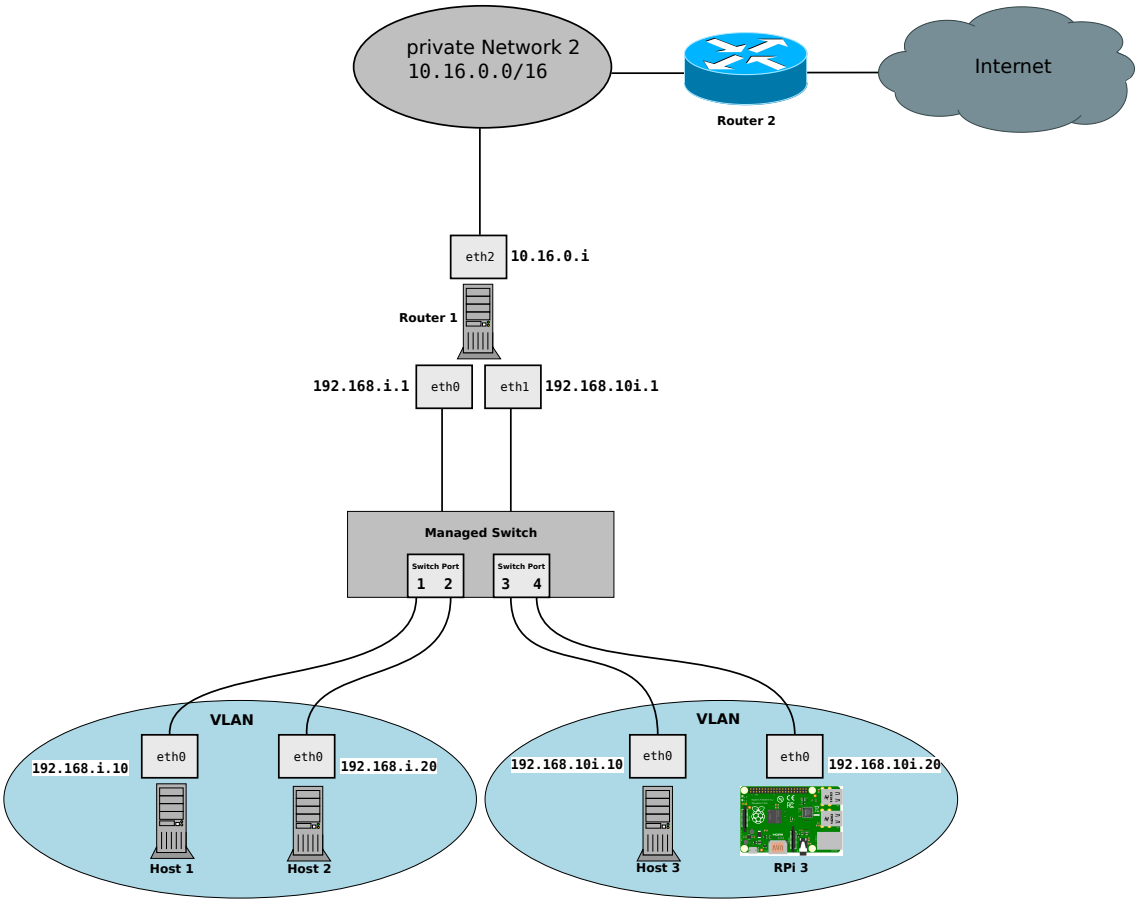

Figure 2: VLAN Setup for the Switches

Table 1: Addresses of machines

Host	Address
Router 2	`10.16.0.200`
Router 1 – `eth0`	`192.168.i.1`
Router 1 – `eth1`	`192.168.10i.1`
Router 1 – `eth2`	`10.16.0.i`
Host 1 – `eth0`	`192.168.i.10`
Host 2 – `eth0`	`192.168.i.20`
Host 3 – `eth0`	`192.168.10i.10`
RPi 3 – `eth0`	`192.168.10i.20`

The hosts in the VLANs should get the network configurations as specified in figure 2 in order to connect to **Router 1**! In a first step, configure the interfaces `eth0` and `eth1` on **Router 1** statically! Plug the Ethernet cables from the interfaces `eth0` and `eth1` from **Router 1** to the Switch as depicted in figure 2.

a) **Setting up Port-Based VLAN**

Setup **Port-Based VLAN** on the Switch! Configure the **Ports 1** and **2** of the Switch as the VLAN for machines **Host 1** and **Host 2**! Configure **Ports 3** and **4** of the Switch for the machines **Host 3** and **RPi 3**! Configure **Port 5** of the Switch to connect the interface `eth0` of **Router 1** with the VLAN of **Host 1** and **Host 2**. Configure **Port 6** of the Switch to connect the interface `eth1` of **Router 1** with the VLAN of **Host 3** and **RPi 3**! Test your setup and document the steps performed! Additionally to the machines **Host** [**1-3**] you should attach a Raspberry Pi 3 as host **RPi 3** in your Network! You can log into the **RPi 3** via **SSH** with the **username:** `raspberry` and **password:** `raspberry`.

b) **Monitoring the Port-Based VLAN**

Monitor the configuration from exercise 2a! Send broadcast messages in both VLANs with the command-line option `ping -b` and use Wireshark on the interface `eth0` on **Host 1** and **Host 3**! Also monitor packets on the interfaces `eth0` and `eth1` on **Router 1**! Explain the results of the broadcast messages sent in the network configuration from 2a in your Wireshark captures! What happens if you disable the IP-Forwarding on **Router 1**? Document the requests and responses and list the results and steps performed!

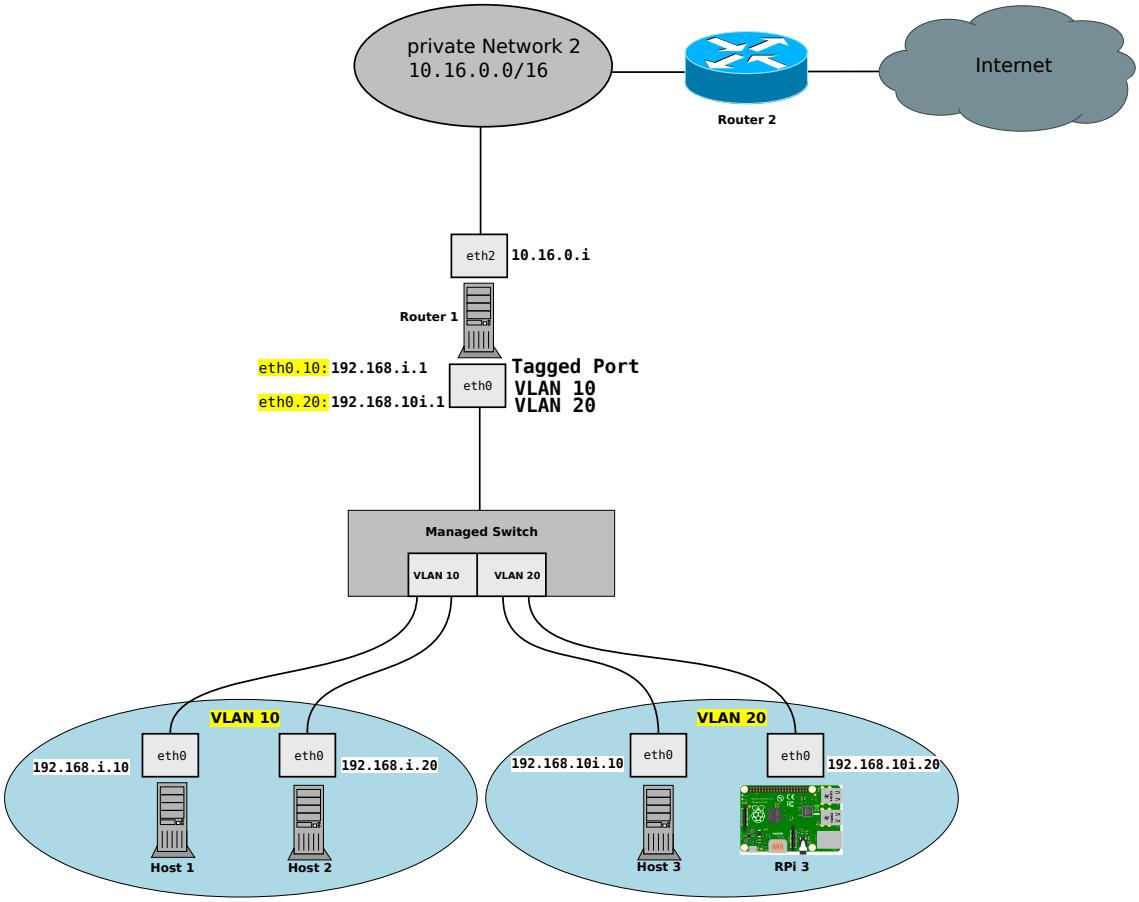

Figure 3: VLAN Setup for 802.1Q

Table 2: Addresses of machines

Host	Address
Router 2	10.16.0.200
Router 1 – eth0.10	192.168.i.1
Router 1 – eth0.20	192.168.10i.1
Router 1 – eth1	10.16.0.i
Host 1 – eth0	192.168.i.10
Host 2 – eth0	192.168.i.20
Host 3 – eth0	192.168.10i.10
RPi 3 – eth0	192.168.10i.20

c) Setting up VLAN according to the 802.1Q standard

Setup the VLAN according to the **802.1Q** standard as depicted in figure 3 with the tool `ip`! The machines **Host 1** and **Host 2** should be configured in the VLAN with Tag **10**. The machines **Host 3** and the **RPi 3** should be configured in the VLAN with Tag **20**! Configure **Port 5** of the Switch to connect the interface `eth0` of **Router 1** with the VLANs! Create the virtual interfaces `eth0.10` and `eth0.20` on the **Router 1** using the tool

`ip`! Configure the Port of the Switch for **Router 1** as **tagged**! Test your setup and document the steps performed!

d) **Monitoring the VLAN according to the 802.1Q standard**

Monitor the configuration from exercise 2c! Send broadcast messages in both VLANs and use Wireshark on the interface `eth0` on **Host 1** and **Host 3**! Also monitor packets on the interfaces `eth0`, `eth0.10` and `eth0.20` on **Router 1**! For the monitoring configure the view of Wireshark with the option `802.1Q VLAN id`[2]! Show the VLAN information from exercise 2c in your Wireshark captures! Document the requests and responses and list the results and steps performed!

e) **Setting up DHCP on the VLAN**

Configure `isc-dhcp-server` on interface `eth0` of **Router 1**. Use the tool `dhclient` on machine **Host** [**1-3**] to receive network configurations from **Router 1**. The configurations on the interface `eth0` of **Router 1** should be made in such a way, that it becomes the router in the network `192.168.i.0/24` serving additional network information such as domain names, DNS-Server, lease times, etc.

Setup **DHCP** in the VLANs from exercise 2d in figure 3! The machines **Host 1** and **Host 2** should be configured in the VLAN with Tag **10**. The machines **Host 3** and the **RPi 3** should be configured in the VLAN with Tag **20**! Configure the Switch to connect the interface `eth0` of **Router 1** with the VLAN of **Host 1** and **Host 2** and the VLAN of machines **Host 3** and the **RPi 3**! For this use the virtual interfaces `eth0.10` and `eth0.20`! Configure `isc-dhcp-server` on the interfaces `eth0.10` and `eth0.20` of **Router 1**, so that it serves the network configurations to the private networks! Configure the Ports as **tagged**! Test your setup and document the steps performed!

Make sure that **Host** [**1-3**] can reach the router and vice versa. Furthermore, configure the interface `eth0.10` and `eth0.20` of **Router 1** **statically**, so that **Host** [**1-3**] have a route to the network `10.16.0.0/16`! Mark the DHCP messages using the filter `bootp` or `dhcp` in Wireshark! Document your setup, the requests and responses and list the results and steps performed!

[2]This can be configured in *Edit->Preferences->Columns* or CTRL+SHIFT+P!

Demonstration Exercise 2

You should be able to demonstrate and explain the following things:

- How does VLAN work? What is its purpose? What are the benefits?
- The successful configuration of the Switch with **Port-Based VLAN** and according to the **802.1Q** standard!
- Pings between **Host 1** and **Host 2** and pings between **Host 3** and **RPi 3** in both configurations!
- What is the difference between a **tagged** and an **untagged** port?
- The Ethernet header information captured with Wireshark in exercise 2d!
- What happens if **Host 1** wants to reach **RPi 3**?
- The successful configuration of the DHCP Server!
- The exchange of DHCP messages and the function of each message!
- The relevant information for the network participants in the DHCP acknowledge message (client IP address, lease time, etc.)!

3. **Quality of Service, Traffic Control and Storm Control**

In this exercise you are asked to configure **Quality of Service** and **Traffic Control** on the Switch for your private networks configured in exercise 2! To achieve that you are asked to experiment with parameters for **QoS Rules** on the Switch and **Bandwidth Control**! The parameters can be configured in the management GUI of the Switch!

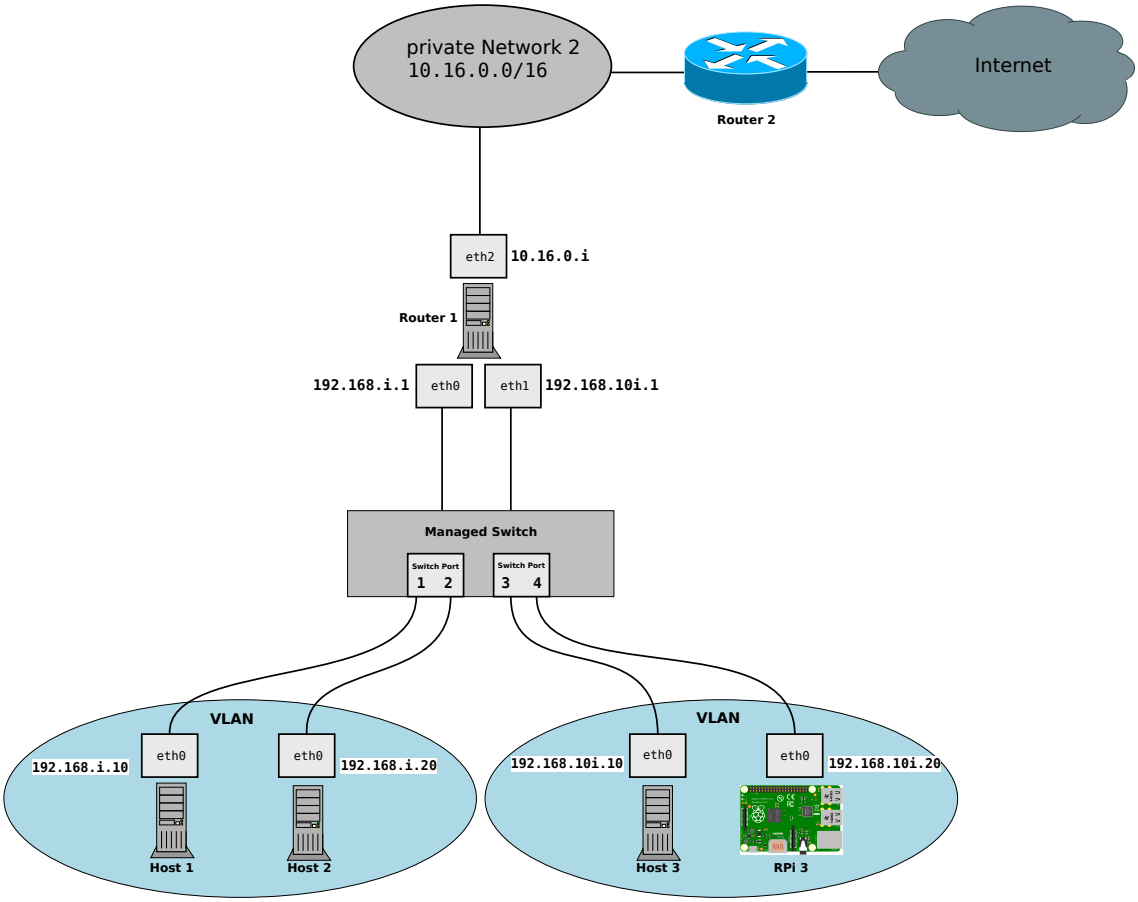

Figure 4: VLAN Setup for the Switches
[a]

[a] It does not matter if you use **Port-based** or **802.1Q** VLAN for this exercise!

a) **Configure Quality of Service**

Setup **Quality of Service** on the Switch! Experiment with the different modes for Quality of Service on **VLAN 10**! Setup **Port-Based QoS**, **802.1p-Based QoS** and **DSCP-Based QoS** on the Switch! Experiment with different values for `ping -Q` and `iperf3 -S`! Test the different setups and document the steps performed!

b) **Monitoring the Quality of Service**

Monitor the configuration from exercise 3a! Send messages in both VLANs and use Wireshark on the interface `eth0` on **Host 1** and **Host 3**! Also monitor packets on the interfaces `eth0` and `eth1` on **Router 1**! For the monitoring configure the view of Wireshark with the option `IP DSCP Value`[3]! Show the priority information of the different methods from exercise 3a in your Wireshark captures! Document the requests and responses and list the results and steps performed!

c) **Configure Bandwidth Control**

Setup **Bandwidth Control** on the Switch! Experiment with rates for **ingress** and **egress rates**[4] on **VLAN 20**! Create a random file with 1 MB in size using the commandline-tool `dd` and send it via `scp` to the machines **Host 3** and **RPi3** in **VLAN 20**! Configure the following bandwidths on the Switch:

- 64 KBit/s
- 1 MBit/s
- 100 MBit/s
- 1 GBit/s

Measure the time for the transmission of the file using the command `time`! What do you observe in the comparison between **Host 3** and **RPi3**? What happens if you increase the file size to 10 MB with bandwidth 1GBit/s? Document and explain your results!

Hint

Use the options `if=/dev/urandom` and `iflag=fullblock` for the file creation!

[3]This can be configured in *Edit->Preferences->Columns* or CTRL+SHIFT+P!
[4]Ingress is the incomming traffic in a network and egress is the outgoing traffic in a network!

d) **Test Bandwidth Control with `iperf3`**

Test your setup from exercise 3c for bandwidth control with `iperf3` and **different metrics for the traffic**! Setup the **Router 1** as a server in `iperf3` using the option `-s` and configure the machine **Host 3** as a client using the option `-c`! Test your setup with the following values and document the results:

- 64 KBit/s
- 1 MBit/s
- 100 MBit/s
- 1 GBit/s

Demonstration Exercise 3

You should be able to demonstrate and explain the following things:

- The successful configuration of **QoS**, **Traffic Control** and **Storm Control** on the Switch!
- Your Wireshark captures for **QoS**, **Traffic Control** and **Strom Control**!
- The priority information in your Wireshark captures and their interpretation!
- What is the relationship between **DSCP values** and the **802.1p PCP priority values**?
- The influence of Traffic Control on the communication with different test cases!
- The measurement results of the bandwidth in your tests!