Lab Exercise Sheet 2

IP Version 6 Topology

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 sets the foundation of the course Practical Computer Networks and Application in this semester! Therefore the setup of the presented network with its topology is mandatory for successful participation in this course!

In the previous exercise, you configured a network using the **IP Version 4** address format. This technology is deprecated and is set to be replaced by **IP Version 6**. Since IPv6 is very different from IPv4 in the first task inspect the literature and the internet[1] for information regarding IPv6. For the lab exercise, you should disable the Network Manager if it is not already disabled by default and enable IPv6 via `sysctl`!

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] `https://en.wikipedia.org/wiki/IPv6`

1. **General questions on IPv6**

   Get familiar with the **IP Version 6** address format! Try to answer the following questions and tasks to test your understanding:

   a) Explain the format that is used for IPv6 addresses and give the maximum number of devices that can be addressed!

   b) Explain the difference between Unicast, Multicast, and Broadcast in IPv6! (Prepare a diagram)

   c) Explain the structure of IPv6 addresses and the terms Network Identifier, Interface Identifier, and Prefix Length! (Prepare a diagram)

   d) What is an IPv6 address scope? Name and explain the different scopes of IPv6! (Prepare a table and diagram)

   Demonstration Exercise 1

   You should be able to explain the following things:

   - IPv6 addresses and their characteristics!
   - The difference between Unicast, Multicast, and Broadcast in IPv6 and their purpose! Where is Broadcast used in IPv6?
   - The structure of IPv6 addresses and the difference to IPv4 addresses! What about subnet masks and broadcast addresses in IPv6?
   - The different scopes of IPv6 addresses and their purpose!

2. **Static IPv6 addresses**

   a) **Network Topology for this lab exercise**

   IPv6 addresses have a different structure compared to IPv4 addresses and the addressing scheme is also very different. For this task, you are asked to assign **unique local addresses** (**ULA**) to the interfaces of **Host [1-3]** and **Router 1** according to the static RFC 4193[2] scheme. The IP address of **Router 1** and **Host [1-3]** are listed in table 3 where the number `i` is a placeholder for your **group number**! Table 1 demonstrates the scheme for the assignment of IP addresses:

[2]Source: `https://en.wikipedia.org/wiki/Unique_local_address`

Table 1: RFC 4193 Addressing Scheme

Prefix/L	Global ID	Subnet ID	Interface ID
fd00::/8	40 bits	16 bits	64 bits
fd00::/8	12:3456:789a	0001	0000:0000:0000:0001

Resulting IPv6 address: fd12:3456:789a:0001:0000:0000:0000:0001
Short IPv6 address: fd12:3456:789a:1::1

For your setup, you are asked to use the following scheme presented in table 2:

Table 2: RFC 4193 Lab Exercise 2

Machine	Prefix/L	Global ID	Subnet ID	Interface ID
Router 1	fd00::/8	xx:xxxx:xxxx	**i**	0000:0000:0000:0001
Host 1	fd00::/8	xx:xxxx:xxxx	**i**	0000:0000:0000:0010
Host 2	fd00::/8	xx:xxxx:xxxx	**i**	0000:0000:0000:0020
Host 3	fd00::/8	xx:xxxx:xxxx	**i**	0000:0000:0000:0030

The machines should have the following configuration:

Table 3: Addresses of machines

Host	IPv6 Address
Router 2 –	`fd12:3456:789a:ffff::ffff`
Router 1 – `eth0`	`fd12:3456:789a:i::1`
Router 1 – `eth1`	`fd12:3456:789a:ffff::i`
Host 1 – `eth0`	`fd12:3456:789a:i::10`
Host 2 – `eth0`	`fd12:3456:789a:i::20`
Host 3 – `eth0`	`fd12:3456:789a:i::30`

b) **Configuring the machines**

Configure the machines using the command-line tool `ip`! Get familiar with the `ip` tool and configure the interface `eth0`[3] of machines **Host [1-3]** with **IP addresses** according to the network topology shown in figure 1! Use `ping6` on the multicast address `ff02::1` of the hosts to discover the router and all other participants in the network. Configure the interface `eth0` of **Router 1** in such a way, that it becomes the router in the **private network 1** `fd12:3456:789a:i::0/64`. Make sure that **Host [1-3]** can reach the router and vice versa. Furthermore, configure the interface `eth1` of **Router 1** in such a way, that **Host [1-3]** have a route to the **private network 2** `fd12:3456:789a:ffff::/64`! Document your setup and list the commands and steps performed!

[3]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/`

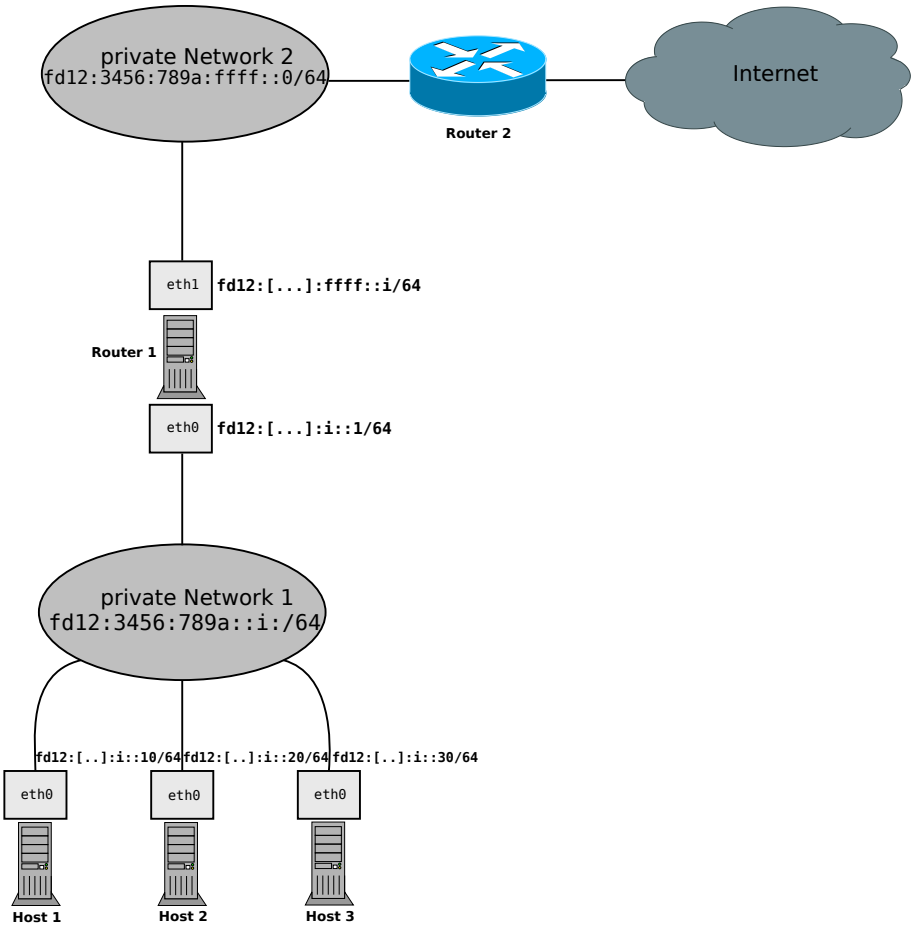

Figure 1: Network Topology of the Lab

c) **Test your network setup**

Test the configuration of your setup with the command-line tool `ping6`! Send ICMP-requests from **Router 1** to the machines **Host [1-3]**. Also Send ICMP-requests from **Host [1-3]** to **Router 1**. Test the communication between **Host [1-3]** and the **private network 2** `fd12:3456:789a:ffff::/64` by sending ICMP-requests to machine **Router 2** (`fd12:3456:789a:ffff::ffff`). Document the tests and list the results and steps performed!

Demonstration Exercise 2

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

- Ping between **Host [1-3]**!
- The routing between **Host [1-3]** and **Router 1**!
- Ping from **Host [1-3]** to **Router 1** and vice versa!
- Ping from **Host [1-3]** to **Router 2** and vice versa!
- The output of the command `ip maddress`!

3. **Autoconfiguration in IPv6**

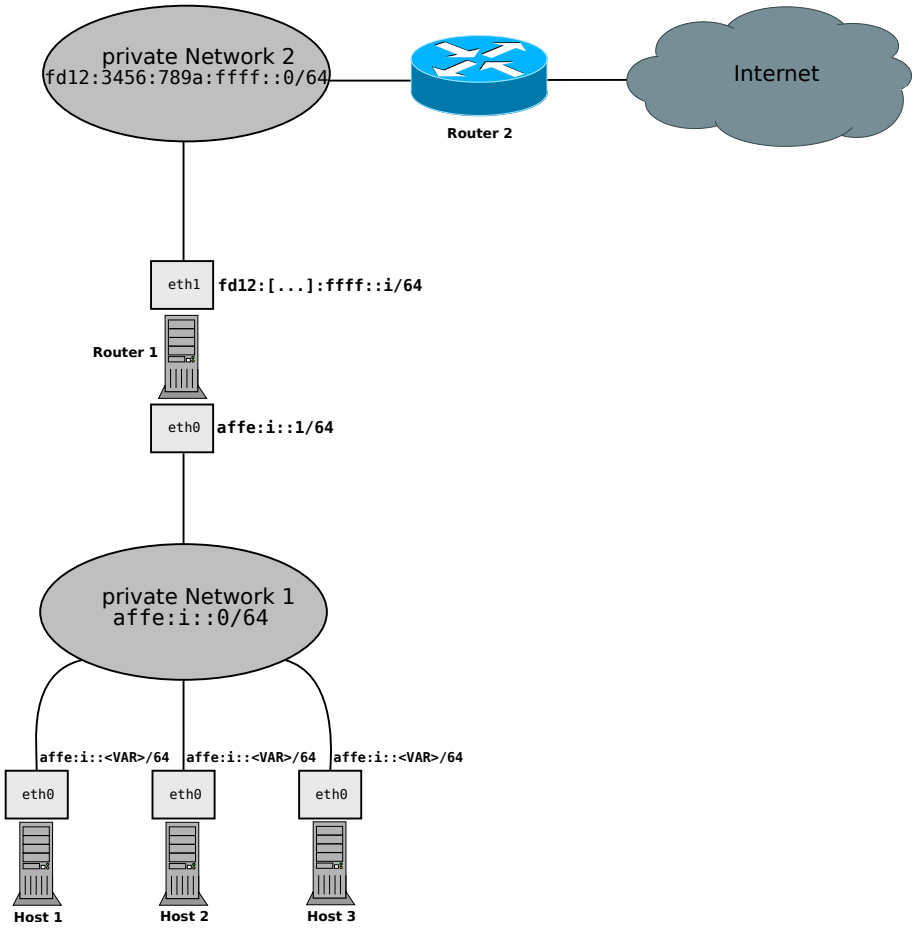

Figure 2: Network Topology with Autoconfiguration of the Lab

For this task, you are asked to configure the network using Autoconfiguration in IPv6. Configure your private network for **Host [1-3]** in such a way, that the network address on interface `eth0` of the router **Router 1** is the gateway address `affe:i::1` in the network `affe:i::0/64`! Make sure that **Host [1-3]** can reach the router and vice versa. Use `ping6` on the

multicast address `ff02::1` of the hosts to discover the router and all other participants in the network. Furthermore configure the interface `eth1` of **Router 1** with the IP address `fd12:3456:789a:ffff::i` in such a way, that the **Host** [**1-3**] have a route to the **private network 2** with the network address `fd12:3456:789a:ffff::0/64` and reach the `Router 2` on the IP address `fd12:3456:789a:ffff::ffff`! Additionally, configure the setups listed in subtask a) - c).

a) **Setup the machines with RFC 4862 – SLAAC**

List the MAC address of the interface `eth0` of **Host** [**1-3**] and calculate the link local address of each host! Check your result by installing and consulting `ipv6calc`. How can duplicate addresses be avoided?

Use `radvd`[4] on the router **Router 1** and configure it to act as an *advertisement daemon* on the interface `eth0`! Configure your hosts **Host** [**1-3**] to receive **Router Advertisements** and `icmpv6` packets from the router! Document your setup and list the commands and steps performed!

b) **Setup the machines with RFC 7217 – Stable Privacy**

Configure your hosts **Host** [**1-3**] to receive IP addresses and network configuration from the router and enable **stable addresses** according to **RFC 7217**[4] on the hosts **Host** [**1-3**]! Document the steps performed for the configuration and list the resulting IPv6 addresses together with the interfaces and the `stable_secret` parameters! Document your setup and list the commands and steps performed!

c) **Setup the machines with Stateful Address Configuration (DHCPv6) and RFC 4941 – Privacy Extension**

Inspect the options of `isc-dhcp-server` on the router **Router 1** and configure the it to act as a DHCP-Server for IPv6 on the interface `eth0`! Configure your hosts **Host** [**1-3**] to receive IP addresses and network configuration from the router and enable **Privacy Extension**[4] on the hosts **Host** [**1-3**]! Experiment with different values for the parameter `use_tempaddr`! What do you observe compared to the IPv6 addresses generated using SLAAC? Document your setup and list the commands and steps performed!

[4] `https://wiki.archlinux.org/title/IPv6`

d) **Test your network setup**

Test the configuration of your setup with the command-line tool `ping6`! Send ICMP-requests from **Router 1** to the machines **Host [1-3]**. Also Send ICMP-requests from **Host [1-3]** to **Router 1**. Test the communication between **Host [1-3]** and the **private network 2** by sending ICMP-requests to machine **Router 2**. Document the tests and list the results and steps performed!

Demonstration Exercise 3

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

- The address assignment using RFC 4862 SLAAC!
- The address assignment using RFC 7217 Stable Privacy!
- The address assignment using RFC 4941 Privacy Extension!
- Successful configurations for the schemes in this task!

4. **Monitoring NDP with Wireshark**

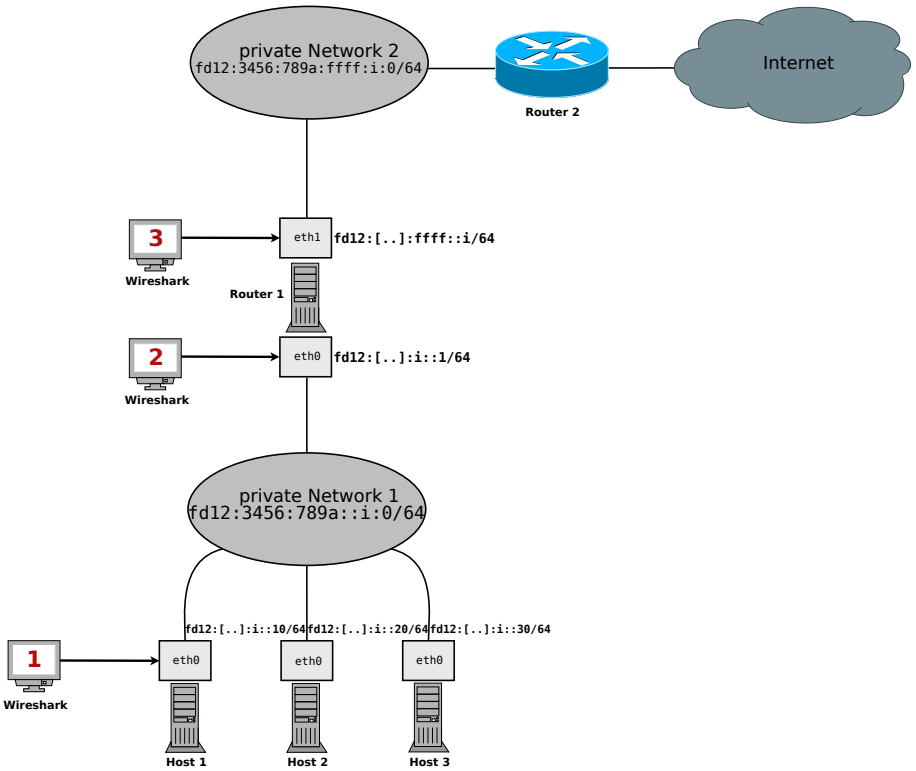

Figure 3: Junction points for monitoring

Monitor and analyze the **Neighbor Discovery Protocol (NDP)**[5] of the IPv6-protocol using Wireshark. Monitor the packets of an IPv6 address resolution process on **junction point 1** (interface `eth0` of **Host 1**) and **junction point 2** (interface `eth0` of **Router 1**). Mark the packets of the discovery in the communication using the filter `icmpv6` in Wireshark! For the execution of the experiment use `ping6` and ping the machine **Router 2**. Solve the following subtasks a) - e) and document the results and steps performed:

a) Monitor and analyze the **Neighbor Solicitation** packets of the traffic. Open the Ethernet II and Internet Protocol view in Wireshark. Inspect the source and destination address of the `icmpv6` packet. What do you observe?

b) Monitor and analyze the **Neighbor Advertisement** packets of the traffic. Open the Ethernet II and Internet Protocol view in Wireshark. Inspect the source and destination address of the `icmpv6` packet. What do you observe?

c) Monitor and analyze the **Router Solicitation** packets of the traffic. Open the Internet Protocol view in Wireshark. Inspect the source and destination address of the `icmpv6` packet. What do you observe?

d) Monitor and analyze the **Router Advertisement** packets of the traffic. Open the Internet Protocol view in Wireshark. Inspect the source and destination address of the `icmpv6` packet. What do you observe?

e) Prepare a diagram showing the exchange of messages in the **Neighbor Discovery Protocol (NDP)** and give a short description and explanation!

Demonstration Exercise 4

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

- The function of the Neighbor Discovery Protocol (NDP)!
- The messages of the Neighbor Discovery Protocol (NDP) in the discovery of machines in a network!
- The contents of the messages and their purpose in the protocol!
- The comparison to the Address Resolution Protocol (ARP) in IPv4! What is the role of ARP in IPv6?

[5] `https://en.wikipedia.org/wiki/Neighbor_Discovery_Protocol`