Lab Exercise

The purpose of this exercise is twofold. First, you will see in action some of the mechanisms described in class so far. Second, you will learn some of the tools network engineers use on a day to day basis to troubleshoot the networking infrastructure.

You will use the following tools:

- `ping`: This is a command-line tool to send ICMP messages.
- tcpdump: This is another command-line tool that captures packets.
- Wireshark: This a GUI based tool. It can be used for packet capture on machines that `tcpdump` is not available. It can also be used for opening, presenting, and navigating a packet capture. You can download Wireshark here.
- `traceroute`: This a command-line tool that prints the route packets take to reach a target host.

To focus on specific mechanisms, we will use a virtual topology that we fully control instead of capturing packets on the NIC your laptop uses to connect to the internet. You can find the scripts to create the topologies here. This repository includes scripts to create, control, and destroy the virtual infrastructure we will use for this exercise. These scripts assume a Linux-based system. Understanding of these scripts is beyond the scope of this class, but feel free to reach out to me if you have questions.

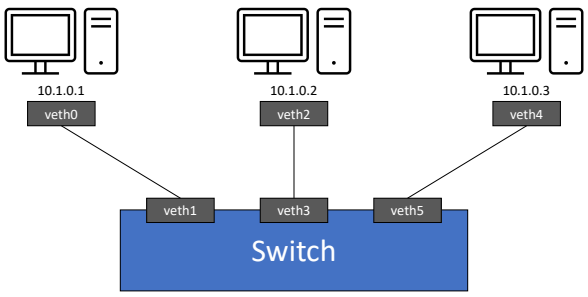

Figure 1: Three machines on the same subnet connected via a subnet

1 Single-Subnet Topology

Assume the topology in Figure 1 in which three machines are on the same subnet `10.1.0.0/24` and connected via a switch.

Run the script `l2/testbed-setup.sh` to create the topology.

1. Ping the IP `10.1.0.3` and capture the traffic on `veth5` using `tcpdump`. Use Wireshark to navigate the trace. Enumerate the different protocols involved.
2. Do the same and capture the traffic on `veth3`. What do you see?
3. Run the script `l2/disable-maclearning.sh` and repeat the previous step.

Run the script `l2/testbed-teardown.sh` to destroy the topology.

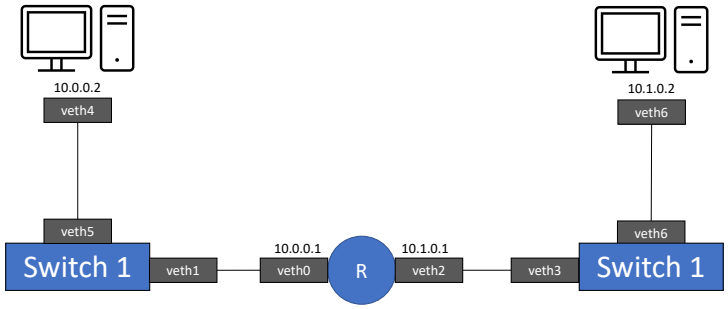

Figure 2: Two subnets connected via a router.

2 Two-Subnet Topology

In this topology, shown in Figure 2, two subnets (`10.0.0.0/24` and `10.1.0.0/24`) are connected to each other via a router. Similarly, run the script `l3/testbed-setup.sh` to create the topology.

1. Use the script `l3/myping.sh` that pings `10.1.0.2` from `10.0.0.2` and observe the traffic on the two router interfaces. Specifically, focus on the IP and MAC addresses, and the ARP protocol.
2. Run the script `l3/mytraceroute.sh` that executes a traceroute from `10.0.0.2` to `10.1.0.2` and capture the traffic on veth5. By observing the traffic, can you understand and explain how `traceroute` works?
3. Use `traceroute` beyond this topology, e.g. to trace your route to `google.com`.

Once done, Run the script `l3/testbed-teardown.sh` to destroy the topology.