Communication Networks 2

SS 2021

Assignment 3

Group 06

Name	Mat.Nummer
Paul Kloker	12034928
Juan Aramis Oposich	11701238

June 10, 2021

1 Task description

2 Procedure

2.1 Host discovery with nmap

There are different techniques to discover active hosts on a network. One of them is the use of nmap, which is a free and open source tool for network discovery and security auditing. To find the missing host in `10.0.0.0/16` the following command was used:

```
$ nmap --privileged -sn -n -T5 --min-parallelism 100 --min-hostgroup 100
10.0.0.0/16
```

To speed up the discovery process, which can take very long time in large networks, multiple options were added to the bare nmap command `$ nmap 10.0.0.0/16`. This reduced the waiting time to 23 minutes, which is still quite long.

Table 1 shows the result of this nmap host discovery search in `10.1.0.0/8` and `10.0.0.0/8`.

No.	Network	IP address	latency
1	10.0.0.0/8	10.0.4.1	0.0075s
2	10.0.0.0/8	10.0.4.2	0.23s
3	10.0.0.0/8	10.0.120.1	0.20s
4	10.0.0.0/8	10.0.120.2	0.0085s
5	10.0.0.0/8	10.0.132.1	0.024s
6	10.0.0.0/8	10.0.132.68	0.18s
7	10.0.0.0/8	10.0.248.1	0.78s
8	10.0.0.0/8	10.0.248.2	0.16s
9	10.1.0.0/8	10.1.6.1	0.18s
10	10.1.0.0/8	10.1.6.110	0.18s
11	10.1.0.0/8	10.1.7.1	1.5s
12	10.1.0.0/8	10.1.7.123	0.78s

Table 1: Discovered IP addresses

Later research and additional information showed that the 6th found IP address `10.0.132.68` belongs to the missing host.

2.2 Ping measurements

To identify which IP address belongs to the landline and satellite host a simple ping command was sent out to the according DNS names. `landline.cn2lab.cn.tuwien.ac.at` was resolved to `10.1.6.110` and `satellite.cn2lab.cn.tuwien.ac.at` to `10.1.7.123`.

In order to obtain information about the network topology and the Round Trip Time (RTT) and loss rate of each host, the ping command was used as well. For each IP address from table 1 the following command was adapted and executed:

```
$ ping -c 50 -R 10.1.7.123 > 10_1_7_123.txt
```

This delivered 50 individual measurements of the RRT which were then saved to a text file and are discussed in section 3.

With the `-R` the record route option was activated. That means all internet modules that route this message add their IP address to the IP option field. This method is better than just using the command `traceroute` because here the reverse path is recorded as well.

Some recorded routes show that the reverse path can be different from the forward path. This is for example the recorded route of the satellite host:

```
RR:  pc18.cn2lab.cn.tuwien.ac.at (192.168.88.118)
     10.0.120.2 (10.0.120.2)
     10.0.248.2 (10.0.248.2)
     10.1.7.1 (10.1.7.1)
     satellite.cn2lab.cn.tuwien.ac.at (10.1.7.123)
     satellite.cn2lab.cn.tuwien.ac.at (10.1.7.123)
     10.0.4.2 (10.0.4.2)
     border.cn2lab.cn.tuwien.ac.at (192.168.88.2)
     pc18.cn2lab.cn.tuwien.ac.at (192.168.88.118)
```

2.3 Network topology

Using the data of the nmap and ping commands, the network topology could be identified and a network diagram created which can be seen in figure 1. Table 2 shows the routing tables of the three routers. Some entries could not be identified by just using the ping command on the lab pc.

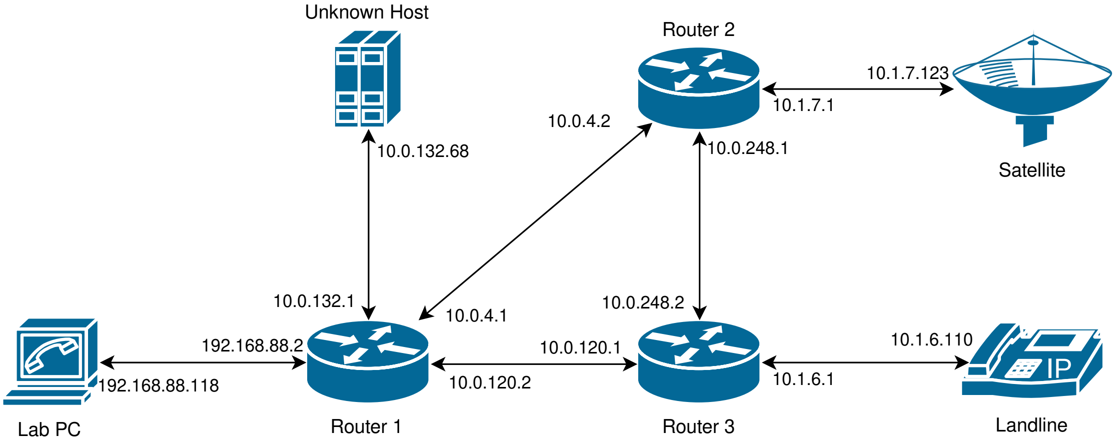

Figure 1: Network diagram

3 Data analysis and comparison

- Welche daten liefert ping

- Grafische Darstellung (besonders Vergleich von Landline und Satellite)

- Vergleich mit den gemessenen Daten von Task 2

4 Conclusion

router	**destination**	**via**
r1	10.0.4.0/24	10.0.4.1
r1	10.0.120.0/24	10.0.120.2
r1	10.0.132.0/24	10.0.132.1
r1	10.0.248.0/24	10.0.120.2
r1	10.1.6.0/24	10.0.120.2
r1	10.1.7.0/24	10.0.120.2
r1	192.168.88.0/24	192.168.88.2
r2	10.0.4.0/24	-
r2	10.0.120.0/24	10.0.120.1
r2	10.0.132.0/24	-
r2	10.0.248.0/24	10.0.248.2
r2	10.1.6.0/24	10.1.6.1
r2	10.1.7.0/24	-
r2	192.168.88.0/24	10.0.120.1
r3	10.0.4.0/24	10.0.4.2
r3	10.0.120.0/24	-
r3	10.0.132.0/24	-
r3	10.0.248.0/24	10.0.248.1
r3	10.1.6.0/24	-
r3	10.1.7.0/24	10.0.7.1
r3	192.168.88.0/24	10.0.4.2

Table 2: Routing table for network A