COMM.NET.200 Computer Networking I

Remote laboratory exercise

Enna Augustin

50235634

enna.augustin@tuni.fi

1 Introduction

In this laboratory exercise a small communications network was set up. In the exercise the network simulator GNS3 was used. The GNS3 was connected to a remote server and the connection was established via OpenVPN. In the exercise routers, switches, and Linux hosts were set up.

2 Switching

In this task, a basic local area network was created. In the network all the workstations will be directly reachable via a switch. Four Linux Workstations were connected to a switch.

After adding the needed devices to the network, IP addresses to all the workstations' eth0 interfaces. The used address range was 10.0.4.0/24. The selected IP addresses are presented in table 1.

Table 1 The selected IP addresses for each device

Device	**IP address/mask**
A	10.0.4.1/24
B	10.0.4.2/24
C	10.0.4.3/24
D	10.0.4.4/24

After this the workstations had a link layer address (MAC) and a network layer address (IP).

Capturing network traffic was performed after adding IP addresses. Ping command was used to verify reachability to other workstations.

Analyze Wireshark's output from the capture. Which packets are sent by the ping command (i.e. which protocol)?

- In the ping command ICMP protocol packets were sent.

Why are there ARP protocol packets sent right before the ping packets? Which device sends the ARP queries?

- When computer A wants to send a ping request to computer B on the network and knows B's IP address but not its MAC address, it sends an ARP request, which is broadcasted to all devices [1]. In the ARP request, it asks the network: "Who owns this IP address X?" This way, it attempts to find the MAC address corresponding to the given IP address. The switch forwards ARP requests to all ports in the network, allowing all devices to respond if they have that IP address and their MAC address matches it [2]. This helps determine the corresponding MAC address for the target device and allows the ping request to succeed [1].

Why do we need the MAC address to send the packet? In other words, why isn't the IP address enough?

- IP addresses help route packets across a network. MAC addresses are physical addresses that are unique to each network device. The MAC address is required to send a message to the correct physical device within the same network segment. [3]

Briefly explain how the switch works. Helper questions: On what basis does the switch make forwarding decisions? And what if the switch does not know where the destination address is located?

- A switch operates at the second layer of the OSI model (data link layer) [3] and learns MAC addresses, building a MAC address table based on ports [4]. It forwards packets based on this MAC address table: if it knows the MAC address of the receiving device, it sends the packet directly to the correct port. If the destination is unknown, the switch floods (broadcasts) the packet to all ports. [4]

Ping from workstation A to workstation C. In the Wireshark capture on workstation A, inspect a ping packet going from A to C and note the IP and MAC addresses included in the packet.

- The addresses and matching devices are presented in table 2.

Table 2 Addresses and matching devices.

	Address	**Device**
Source IP	10.0.4.1	Workstation A
Destination IP	10.0.4.3	Workstation C
Source MAC	d6:73:0f:2b:6f:34	Workstation A
Destination MAC	fe:db4c:f5:cc:2f	Workstation C

Next a second switch was added to the network.

Are there any significant changes to the functionality of the network with the adding of the second switch?

- When another switch is added to the network, it can increase the available bandwidth of the network, it can help in reducing workload on individual host PCs, it can increase the performance of the network and the network can have less frame collisions. On the other hand, network connectivity issues are difficult to be traced through the network switch and broadcast traffic may be troublesome. [5]

3 Subnetting

In this task as small subnetworks as possible from our IP address range 10.0.4.0/24 were created. Subnetworks had to be able to contain 31 devices.

How many addresses are available in the smallest subnetwork that fulfils the criteria?

- In network mask /27 there is 32 addresses, but since two of those are reserved for network address and broadcast address, there are only 30 addresses for devices [6]. Since we want subnets that can contain 31 devices, we need to use network mask /26 which has 64 available addresses and in it there are 64-2=62 available addresses for devices [6].

How many different subnetworks that meet the criteria can be formed from your original IP address range? List the network addresses of all possible subnetworks.

- In the original IP range 10.0.4.0/24 there are 256 available addresses so when it is divided into subnets of mask /26 there are 256/64=4 subnetworks that meet the criteria. These subnets are for example:
  - 10.0.4.0-63
  - 10.0.4.64-127
  - 10.0.4.128-191
  - 10.0.4.192-255

In the report, write down the requested IP addresses for any two subnetworks that meet the criteria. Use a table or list clearly.

- The requested IP addresses for two subnetworks are presented in table 3.

Table 3 Requested IP addresses for subnetworks.

	Subnet 1	**Subnet 2**

Network address	10.0.4.0	10.0.4.192
Network mask	255.255.255.192	255.255.255.192
Broadcast address	10.0.4.63	10.0.4.255
First host address	10.0.4.1	10.0.4.193
Last host address	10.0.4.62	10.0.4.254

Next, the subnets in table 3 were addressed to our switches. Switch 1 was given an address from subnet 1 and switch 2 was given an address from subnet 2.

Try to ping between the workstations. Which workstations can connect to each other?

- Workstations that are in the same subnet can connect to each other. If workstations that are in different subnets are trying to ping, we get an error message "Network is unreachable".
- Workstations A and B can connect, and workstations C and D can connect.

Inspect the routing table on a workstation with the command IP route. Based on the information given in the routing table, explain why the connection doesn't work between certain workstations.

- The results from the command for workstation A and C are presented in figures 1 and 2.

```
root@A:~# ip route
10.0.4.0/26 dev eth0  proto kernel  scope link  src 10.0.4.1
```

Figure 1 IP route command for workstation A

```
root@C:~# ip route
10.0.4.192/26 dev eth0  proto kernel  scope link  src 10.0.4.193
```

Figure 2 IP route command for workstation C

- In the command the first thing that is printed is the subnet's network address. Since workstation A and C are in different subnets their results are different. The workstations cannot connect because they are in different subnets. Since our topology only has switches, we cannot connect devices in different subnets, but for that we will need a router [7].

4 Routing

In this task a Cisco router was added to our topology. The router was added so that the two switches were connected. The default gateway was added to the workstations. After this network traffic capture on links to workstations A and C was started and ping command from A to C was performed.

Why is the default gateway needed?

- Default gateway is needed so that devices in different networks can communicate with one another [8].

The capture on workstation A link should show an ARP query just before the ICMP packets. Which device is sending the query, what is being queried and why?

- An ARP request is sent by workstation A because workstation A needs to discover the MAC address corresponding to the IP address of workstation C. The ARP packet moves through the first switch which does not know either the router's or workstation C's MAC address, so it broadcasts the query to all its ports and receives a response from the router that the workstation is in different subnet. [4] The router receives the ARP request and recognizes it's destined for another subnet. Since the router connects these two subnets, it knows that workstation C is in the other subnet. The router cannot directly respond to the ARP request but can forward it to the workstation C's subnet. [1] Workstation A is querying the MAC address of the router, so it can forward the packet to the router as the next hop. This way the two subnets can communicate with each other.

Inspect a ping packet going from A to C on both captures. Compare the results between the captures and pay attention the IP and MAC addresses included in the packet. What has changed and why? You can optionally include tables here.

- The tables for network captures of the ping command are presented in figures 3 and 4.

	Time	Source	Destination	Protocol	Length	Info
2	40.788600	d6:73:0f:2b:6f:34	Broadcast	ARP	42	Who has 10.0.4.10? Tell 10.0.4.1
3	40.799763	ca:01:c3:59:00:08	d6:73:0f:2b:6f:34	ARP	60	10.0.4.10 is at ca:01:c3:59:00:08
4	40.799973	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=1/256, ttl=64 (no response found!)
5	41.792060	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=2/512, ttl=64 (reply in 6)
6	41.842191	10.0.4.193	10.0.4.1	ICMP	98	Echo (ping) reply id=0x0042, seq=2/512, ttl=63 (request in 5)
7	42.793744	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=3/768, ttl=64 (reply in 8)
8	42.842823	10.0.4.193	10.0.4.1	ICMP	98	Echo (ping) reply id=0x0042, seq=3/768, ttl=63 (request in 7)
9	43.795219	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=4/1024, ttl=64 (reply in 10)
10	43.843422	10.0.4.193	10.0.4.1	ICMP	98	Echo (ping) reply id=0x0042, seq=4/1024, ttl=63 (request in 9)
11	44.795945	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=5/1280, ttl=64 (reply in 12)
12	44.844616	10.0.4.193	10.0.4.1	ICMP	98	Echo (ping) reply id=0x0042, seq=5/1280, ttl=63 (request in 11)
13	45.797913	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=6/1536, ttl=64 (reply in 14)
14	45.846263	10.0.4.193	10.0.4.1	ICMP	98	Echo (ping) reply id=0x0042, seq=6/1536, ttl=63 (request in 13)
15	46.799610	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=7/1792, ttl=64 (reply in 16)
16	46.817647	10.0.4.193	10.0.4.1	ICMP	98	Echo (ping) reply id=0x0042, seq=7/1792, ttl=63 (request in 15)
17	47.800955	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=8/2048, ttl=64 (reply in 18)
18	47.849866	10.0.4.193	10.0.4.1	ICMP	98	Echo (ping) reply id=0x0042, seq=8/2048, ttl=63 (request in 17)
19	48.802291	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=9/2304, ttl=64 (reply in 20)
20	48.851474	10.0.4.193	10.0.4.1	ICMP	98	Echo (ping) reply id=0x0042, seq=9/2304, ttl=63 (request in 19)
21	49.803850	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=10/2560, ttl=64 (reply in 22)
22	49.854246	10.0.4.193	10.0.4.1	ICMP	98	Echo (ping) reply id=0x0042, seq=10/2560, ttl=63 (request in 21)
23	50.805602	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=11/2816, ttl=64 (reply in 24)
24	50.856773	10.0.4.193	10.0.4.1	ICMP	98	Echo (ping) reply id=0x0042, seq=11/2816, ttl=63 (request in 23)
25	51.201273	ca:01:c3:59:00:08	CDP/VTP/DTP/PAgP/UDLD	CDP	359	Device ID: R1 Port ID: FastEthernet0/0
26	51.807292	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=12/3072, ttl=64 (reply in 27)
27	51.849501	10.0.4.193	10.0.4.1	ICMP	98	Echo (ping) reply id=0x0042, seq=12/3072, ttl=63 (request in 26)

Figure 3 Capture for workstation A

1	0.000000	ca:01:c3:59:00:06	Broadcast	ARP	60	Who has 10.0.4.193? Tell 10.0.4.200
2	0.000220	fe:db:4c:f5:cc:2f	ca:01:c3:59:00:06	ARP	42	10.0.4.193 is at fe:db:4c:f5:cc:2f
3	0.354194	ca:01:c3:59:00:06	CDP/VTP/DTP/PAgP/UD…	CDP	359	Device ID: R1 Port ID: FastEthernet0/1
4	0.961498	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=2/512, ttl=63 (reply in 5)
5	0.961738	10.0.4.193	10.0.4.1	ICMP	98	Echo (ping) reply id=0x0042, seq=2/512, ttl=64 (request in 4)
6	1.962135	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=3/768, ttl=63 (reply in 7)
7	1.962321	10.0.4.193	10.0.4.1	ICMP	98	Echo (ping) reply id=0x0042, seq=3/768, ttl=64 (request in 6)
8	2.962692	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=4/1024, ttl=63 (reply in 9)
9	2.962957	10.0.4.193	10.0.4.1	ICMP	98	Echo (ping) reply id=0x0042, seq=4/1024, ttl=64 (request in 8)
10	3.964041	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=5/1280, ttl=63 (reply in 11)
11	3.964295	10.0.4.193	10.0.4.1	ICMP	98	Echo (ping) reply id=0x0042, seq=5/1280, ttl=64 (request in 10)
12	4.965571	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=6/1536, ttl=63 (reply in 13)
13	4.965879	10.0.4.193	10.0.4.1	ICMP	98	Echo (ping) reply id=0x0042, seq=6/1536, ttl=64 (request in 12)
14	5.967299	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=7/1792, ttl=63 (reply in 15)
15	5.967557	10.0.4.193	10.0.4.1	ICMP	98	Echo (ping) reply id=0x0042, seq=7/1792, ttl=64 (request in 14)
16	6.011680	fe:db:4c:f5:cc:2f	ca:01:c3:59:00:06	ARP	42	Who has 10.0.4.200? Tell 10.0.4.193
17	6.017947	ca:01:c3:59:00:06	fe:db:4c:f5:cc:2f	ARP	60	10.0.4.200 is at ca:01:c3:59:00:06
18	6.969032	10.0.4.1	10.0.4.193	ICMP	98	Echo (ping) request id=0x0042, seq=8/2048, ttl=63 (reply in 19)

Figure 4 Capture for workstation C

- The source and destination MAC addresses in the packet change at each network interval. In the packet captured by A, the source is workstation A and the destination is the router. The packet captured by C has the source as the router and the destination as workstation C. Workstation A has set the router's MAC address as the destination MAC because after examining its routing table, it has determined that the packet must be forwarded to the router next. Similarly, the router has determined from its routing table that workstation C is on the same subnet as it, so it marks C's MAC address MAC destination. (If the MAC address of C is not known, it is first queried using an ARP query.) There is also CDP packet that helps us discover Cisco devices on the network [9]. The source and destination IP addresses marked in the packet remain the same in this case. Roughly speaking, the IP addresses in the packet usually indicate the original sender and the final receiver, while the MAC address indicates the previous sender and the next receiver (at the network layer).

5 MicroInternet

In this task a second Cisco router and a Linux workstation were added to the topology to act as a server.

Inspect the routing table of R1 with the command show IP route (exit from config mode first with the command exit, if necessary). Which networks is R1 now aware of?

- The router R1 is now aware of network 10.0.0.0/26 and understands that it is sub netted to subnets 10.0.4.0 and 10.0.4.192 which are directly connected. Figure 5 presents the command's result.

```
    10.0.0.0/26 is subnetted, 2 subnets
       10.0.4.0 is directly connected, FastEthernet0/0
       10.0.4.192 is directly connected, FastEthernet0/1
```

Figure 5 What networks R1 is aware of part 1.

What happens if a packet with an unknown destination network arrives at the router? Hint: You can try this in practice by simply pinging an unknown address from a workstation.

- When a packet with an unknow destination arrives to the router, it sends back an error message "Destination host unreachable" This is presented in figure 6.

```
root@D:~# ping 192.168.52.169
PING 192.168.52.169 (192.168.52.169) 56(84) bytes of data.
From 10.0.4.200 icmp_seq=1 Destination Host Unreachable
From 10.0.4.200 icmp_seq=2 Destination Host Unreachable
From 10.0.4.200 icmp_seq=3 Destination Host Unreachable
From 10.0.4.200 icmp_seq=4 Destination Host Unreachable
```

Figure 6 Pinging an unknown address.

Next, IP addresses for the router 2 and server were added. Also, the router 2 was added as the default gateway for the server.

Which networks is R1 now aware of?

- After the router interfaces have been connected to each other, the router 1 is aware of network 10.0.0.0/8 and says that it is variably sub netted to 10.3.0.0/30 (Gigabit Ethernet), 10.0.4.0/26 (FastEthernet 0/0) and 10.0.4.192/26 (FastEthernet 0/1). The result from the show IP route command is presented in figure 7.

```
  10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
     10.3.0.0/30 is directly connected, GigabitEthernet1/0
     10.0.4.0/26 is directly connected, FastEthernet0/0
     10.0.4.192/26 is directly connected, FastEthernet0/1
```

Figure 7 What networks R1 is aware of part 2.

Next, the router 1 had to be told separately how to connect to the server's network.

At this point, if you try pinging from a workstation to server, where does the query or reply stop? You can answer either based on theory or Wireshark captures.

- When looking at Wireshark captures the responses stop at the router 1. This might mean that the router 2 does not know the way back to the first network which means that data is sent to the second network but lost there.

How should you configure the network so that the ping from a workstation to server works? Implement the configuration. Hint: Adding one thing should be enough.

- The network's router 2 should have addition to its IP route's configuration. The R2 was told how to connect to the first network created with the IP route command. After this ping command from a workstation was successful since the router 2 knew how to connect to the network 10.0.4.0/24.

From workstation A use the command traceroute ADDRESS to inspect the network path to the following devices. How many hops are there in each case? How is a hop defined in networking?

- In networking a hop is defined as an intermediate connection in a string of connections linking two devices. When a packet travels through a router or gateway, a hop occurs. [10]

(a) Workstation B

- The traceroute command to workstation B is presented in figure 8.

```
root@A:~# traceroute 10.0.4.4
traceroute to 10.0.4.4 (10.0.4.4), 30 hops max, 60 byte packets
 1  10.0.4.4 (10.0.4.4)  0.877 ms  0.883 ms  0.889 ms
```

Figure 8 Traceroute to workstation B.

- The command says that there is one hop but since the workstations are in the same subnet and connected directly via a switch, are no hops according to the definition we are using. Some definitions count as a hop when a packet passes through other hardware on a network, like switches, access points, and repeaters [11], so if this was the case the number of hops would be 1.

(b) Workstation C

- The traceroute command to workstation C is presented in figure 9.

```
root@A:~# traceroute 10.0.4.193
traceroute to 10.0.4.193 (10.0.4.193), 30 hops max, 60 byte packets
 1  10.0.4.10 (10.0.4.10)  13.633 ms  13.626 ms  13.642 ms
 2  10.0.4.193 (10.0.4.193)  13.452 ms  13.455 ms  13.451 ms
root@A:~#
```

Figure 9 Traceroute to workstation C.

- The command says that there are two hops. In our topology the workstations are in two subnets so when they communicate with each other the packet passes one router, so according to our definition there is one hop. On the other hand, according to the added definition presented in point a, there could be 2 or 3 depending how moving through switches is counted.

(c) The server

- The traceroute command to the server is presented in figure 10.

```
root@A:~# traceroute 192.168.0.6
traceroute to 192.168.0.6 (192.168.0.6), 30 hops max, 60 byte packets
 1  10.0.4.10 (10.0.4.10)  9.128 ms  9.113 ms  9.101 ms
 2  10.3.0.2 (10.3.0.2)  19.367 ms  19.364 ms  19.360 ms
 3  192.168.0.6 (192.168.0.6)  59.672 ms  59.679 ms  59.679 ms
```

Figure 10 Traceroute to the server.

- According to the command there are three hops between workstation A and the server. In our topology there are three different networks 10.0.4.0/24, 10.3.0.0/30, and 192.168.0.0/16. So, when the data moves to the destination it passes two routers but three gateways meaning there are 3 hops.

References

[1] Harmoush, E. (2021) Traditional ARP. Practical Networking. 10.12.2021. Available: https://www.practicalnetworking.net/series/arp/traditional-arp/ (Referred: 9.12.2023)

[2] Netometer. (n.d.) ARP Q&A. Available: https://www.netometer.com/qa/arp.html#A1 (Referred: 9.12.2023)

[3] Cloudflare. (n.d.) What is a network switch? | Switch vs. router. Available: https://www.cloudflare.com/learning/network-layer/what-is-a-network-switch/ (Referred: 9.12.2023)

[4] Cisco Networking Academy. (2020) Ethernet Switching. Cisco Press. 15.7.2020. Available: https://www.ciscopress.com/articles/article.asp?p=3089352&seqNum=6 (Referred: 9.12.2023)

[5] RF Wireless World. (n.d.). Advantages of Switches | disadvantages of Switches. Available: https://www.rfwireless-world.com/Terminology/Advantages-and-disadvantages-of-Switches.html (Referred: 9.12.2023)

[6] Dooley, K. (n.d.) Subnetting: What it is and How it Works. Auvik. Available: https://www.auvik.com/franklyit/blog/subnetting-primer/ (Referred: 9.12.2023)

[7] Rojanala, S. (2022) What Is a Switch, Router, Gateway, Subnet, Firewall & DMZ? (Guest Blog). 4.5.2022. Certified Wireless Network Professionals. Available: https://www.cwnp.com/what-is-a-switch-router-gateway-subnet-firewall-dmz/ (Referred: 9.12.2023)

[8] Mitchell, B. (2021) What Is a Default Gateway in Networking? 8.9.2021. LifeWire. Available: https://www.lifewire.com/what-is-a-default-gateway-817771 (Referred: 9.12.2023)

[9] Networklessons.com (n.d.) Introduction to CDP (Cisco Discovery Protocol). Available: https://networklessons.com/cisco/ccie-routing-switching/introduction-to-cdp-cisco-discovery-protocol (Referred 9.12.2023)

[10] Rouse, M. (2018). Hop. 23.4.2018. Technopedia. Available: https://www.techopedia.com/definition/2411/hop (Referred: 10.2.2023)

[11] Fisher, T. (2023). What Are Hops & Hop Counts? 19.4.2023. LifeWire. Available: https://www.lifewire.com/what-are-hops-hop-counts-2625905 (Referred: 10.12.2023)

Attachments

The configuration files for routers 1 and 2 and Linux workstations A, B, C, D and the server are submitted as a zip folder along the report.