

Mandatory Assignment 3 - Setting up your router

May 1, 2022

Group 20

Mads Legard Nielsen (s215771)

Mads Gjeraae Eichler Hansen (s205455)

Marcus Wahlers Sand (s215827)

Oscar Maxwell Bjerregaard (s215779)

Nicolai Udbye (s215828)

www.github.com/DTUSoftware/Data-Communication



**Danmarks
Tekniske
Universitet**

Title:

Mandatory Assignment 3 - Setting up your router

Theme:

Data Communication

Project Period:

13. Week Peiod

Project Group:

Group 20

Participant(s):

Mads Legard Nielsen

Mads Gjeraae Eichler Hansen

Marcus Wahlers Sand

Oscar Maxwell Bjerregaard

Nicolai Udbye

Supervisor(s):

Bhupjit Singh

Copies: 1

Page Numbers: 20

Date of Completion:

May 1, 2022

Abstract:

We've been tasked with configuring a network with both dynamically assigned and static hosts. We also got tasked with hosting a webserver which would be accessible by people outside the network.

In the end, the network got configured and the webserver ended up being fully accessible and the project was finished, fulfilling every requirement except for the parts requiring you to visit the websites of other groups.

Contents

1	Introduktion	1
2	Analysis	1
2.1	Provided process	1
2.2	Requirements	2
2.2.1	Priority List (MoSCoW)	2
2.2.1.1	Must have	2
2.2.1.2	Should have	2
2.2.1.3	Could have	2
2.2.1.4	Won't have	2
3	Design	3
3.1	Network Documentation	3
3.2	Topology Diagrams	4
4	Implementation	5
4.1	Winbox Configuration	5
4.1.1	CLI Configuration	5
4.1.1.1	Interfaces	5
4.1.1.2	IP Pool	6
4.1.1.3	DHCP	6
4.1.1.4	DNS	7
4.1.1.5	Firewall Rules	7
4.1.1.6	NAT Forwarding	7
4.1.1.7	System Settings	7
4.1.2	GUI Configuration	8
5	Conclusion	11
A	Appendix	13
A.1	Wireshark Captures	13
A.2	Router Configuration Export	17
B	Bibliography	20

1 Introduktion

We have decided to facilitate our own internet services in our offices. As we only have network out-work installed by the ISP, and getting several new ones would be costly and decrease the network security. We have therefore concluded that we needed to design a private network for our 2 offices. We chose to use a MikroTik router as it came heavily recommended to us.

The designed network will be following the RFC 1918 standards, with a subnet mask at 255.255.255.0. It will furthermore need to be able to handle all of our network devices, such as our pc's, our printer and our web-server.

There will be documentation for all this, as it allows for the network administrator to know what they will be dealing with.

This includes a Topology diagram to visually illustrate how the network is physically connected.

To allow the network administrator to fully know what they are dealing with, they will also be provided with a standard network documentation document, describing relevant information about the: Sub-net Mask, Gateway Address, IP Addresses, Hosts on the Network, Ports, DNS, Firewall and NAT forwarding in detail.

To confirm that our web-server worked as expected, and test that all of the functions, resulted in us requesting help from other web-admins in the building. We were able to get help from office 7, 11, 15, 21 and 22. This confirmed the functions.

The server was ready for production.

2 Analysis

New start-up company (made up of 5 employees) is going to rent 2 offices in new building where there is only one network outlet/modem installed by ISP (telephone) company.

2.1 Provided process

1. Make sure to write needed documentation for the Network Administrator for this network. (Could be Network topology, netmask, gateway address and other relevant info.) Imagine you were given this network to administrate, what information would you like to have.
2. Use a DHCP client on the WAN-port on your router to get an IP address from the ISP. Assign IP address and Gateway address on every host in your network for network mask: with 192.168.xx.0/24 with xx being your group number.
3. Make a script adding a DHCP-server giving up to 40 IP addresses for hosts on the network. Make sure the first 10 IP addresses are reserved for static devices.
IP-address to laptops from port 2 and 3.
Static IPs from port 4 and 5.
Assign DNS-servers.
4. How would you connect all of the machines to the Internet? (there are only 5 ports on the mikrotek router that you will get – but argue for components to be chosen to extend the capabilities.)
(laughs in 10-port router)

5. Set up the website of your group.
For example IIS on a Windows Machine on a machine/laptop.
Publish a webpage -> Port forward to router.
6. Select what you want to have on your website
Publish a group message -> Publish your report/network topology.
Use Wireshark -> Find other groups' router IP -> Visit their website -> Read other groups' message and publish it as their message on your website -> Display captured Wireshark session on your website.
7. Protect your network
Use firewall to block all other ports except dns, https, ntp, dhcp, ssh
8. Take screenshots – and confirm you completed your assignment

2.2 Requirements

2.2.1 Priority List (MoSCoW)

2.2.1.1 Must have

- The network is using RFC1918 addressing <https://tools.ietf.org/html/rfc1918> and has the subnet mask 255.255.255.0
- The ability to assign static devices
- The ability to assign dynamic devices
- The ability to make devices reachable from the internet (web and FTP)
- The ability for devices to reach the internet (PCs)
- The ability for devices to only work on the private network (printer)

2.2.1.2 Should have

- Use the MikroTik Router (5-port or 10-port) as your first hop router in your network.
- A router password that's not the default password.

2.2.1.3 Could have

- Anti-Flooding (Anti-DDoS).
- Its own built in VPN function.
- OpenWRT, Tomato or DD-WRT.

2.2.1.4 Won't have

- Load balancing.

- FTP Server (got told not to, otherwise it would've been a Could have).

3 Design

3.1 Network Documentation

- **Subnet Mask:**
255.255.255.0 [192.168.20.1/24] (Class C Network)
- **Gateway Address:**
192.168.20.1
- **IP addresses:**
Dynamic IP range = 192.168.20.10 - 192.168.20.50
Static IP range = 192.168.20.0 - 192.168.20.9
- **Hosts on the Network:**
Up to 40 dynamically assigned hosts.
Up to 10 statically assigned hosts.
- **Ports:**
WAN is on port 1.
Laptops (dynamic) are on port 2 and 3 - switching is needed to provide internet access to all dynamically assigned hosts through these ports.
Servers (static) are on port 4 and 5.
- **DNS:**
Primary DNS = 1.1.1.1 (Cloudflare)
Secondary DNS = 8.8.8.8 (Google)
- **Firewall:**
Allow SSH, HTTP(S), DNS, NTP, DHCP and pinging
Block everything else
- **NAT Forwarding:**
Forward HTTP(S) requests to Webserver (on port 4)
Forward FTP requests to FTP Server (on port 5)

3.2 Topology Diagrams

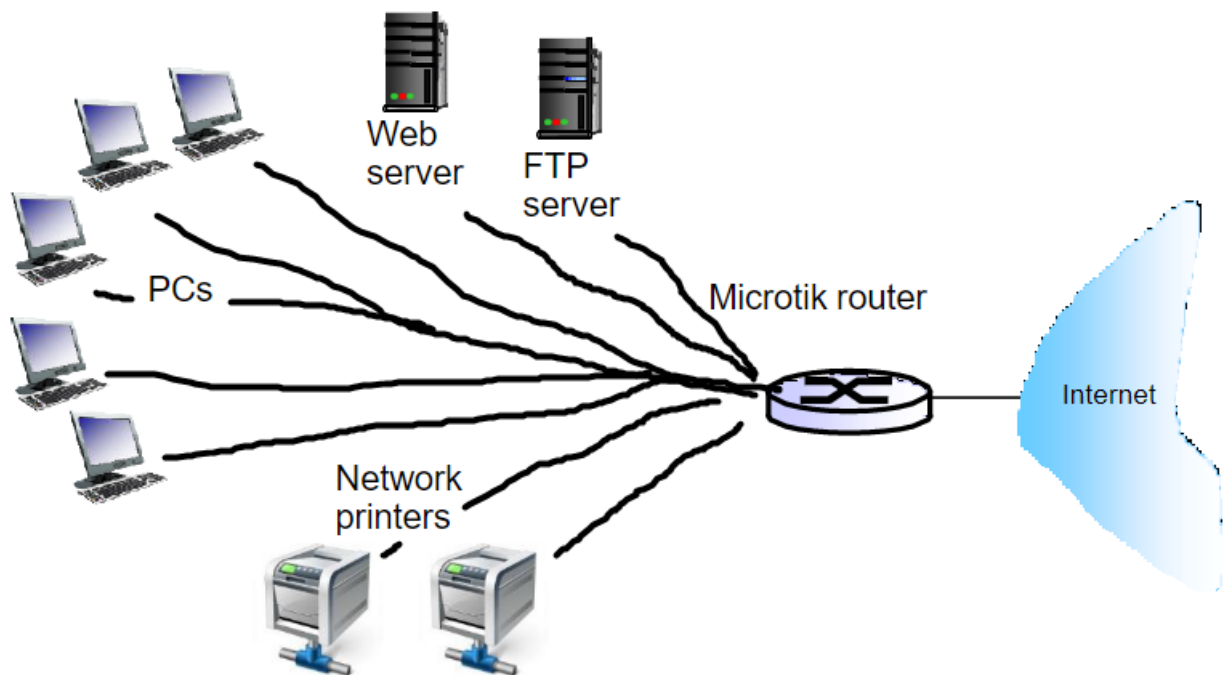


Figure 1: Network graphic filled out with no switches (router has enough ports)

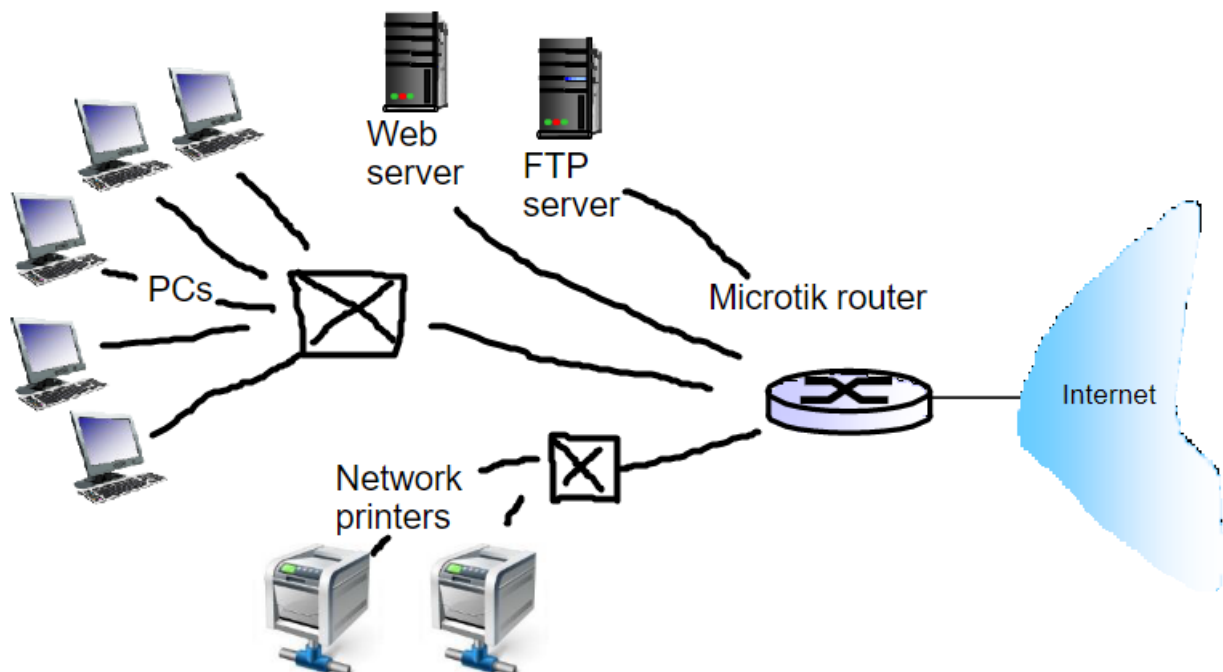


Figure 2: Network graphic filled out with two switches

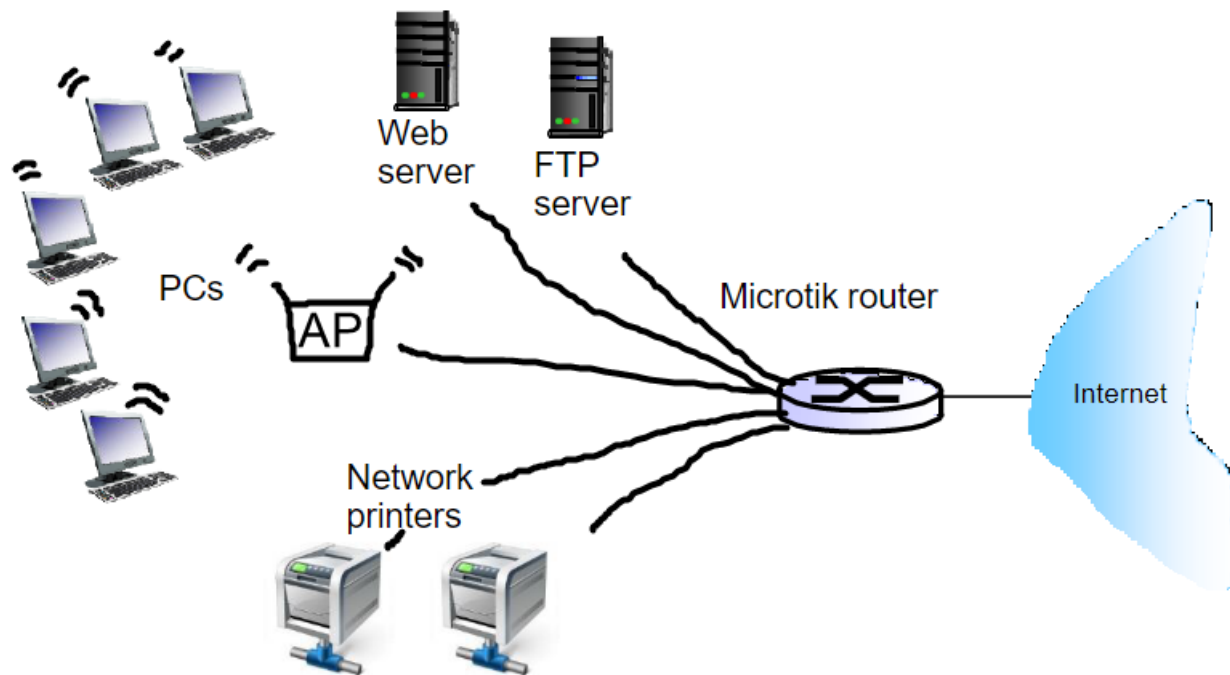


Figure 3: Network graphic filled out with a wireless access point

4 Implementation

4.1 Winbox Configuration

4.1.1 CLI Configuration

4.1.1.1 Interfaces

We setup the different interfaces, which includes the bridge between the two switches. The first switch is consisting of ethernet ports 1-5, as well as the SFP port. The second switch is consisting of ethernet ports 6-10.

Ethernet 1 is the port used for connecting to the internet - Ethernet 2 is the port that's used as the master port of all the other interfaces on the router.

```

1 /interface bridge
2 add comment="Bridge between Gigabit and Fast switch" l2mtu=1598 name=bridge1
3 /interface ethernet
4 set [ find default-name=ether1 ] comment=WAN
5 set [ find default-name=ether2 ] comment="GIGABIT LAN MASTER PORT - Ports 2-5
   ↳ and sfp1 are switched"
6 set [ find default-name=ether3 ] master-port=ether2
7 set [ find default-name=ether4 ] master-port=ether2
8 set [ find default-name=ether5 ] master-port=ether2
9 set [ find default-name=ether6 ] comment="FAST LAN MASTER PORT - Ports 7-10 a
   ↳ re switched"
  
```



```

10 set [ find default-name=ether7 ] master-port=ether6
11 set [ find default-name=ether8 ] master-port=ether6
12 set [ find default-name=ether9 ] master-port=ether6
13 set [ find default-name=ether10 ] master-port=ether6
14 set [ find default-name=sfp1 ] comment="Slave to ether2 (part of GIGABIT LAN)"
    ↪ " master-port=ether2
15 /ip neighbor discovery
16 set ether1 comment=WAN
17 set ether2 comment="GIGABIT LAN MASTER PORT - Ports 2-5 and sfp1 are switched"
18 set ether6 comment="FAST LAN MASTER PORT - Ports 7-10 are switched"
19 set sfp1 comment="Slave to ether2 (part of GIGABIT LAN)"
20 set bridge1 comment="Bridge between Gigabit and Fast switch"
21 /interface wireless security-profiles
22 set [ find default=yes ] supplicant-identity=MikroTik
23 /interface bridge port
24 add bridge=bridge1 interface=ether2
25 add bridge=bridge1 interface=ether6

```

4.1.1.2 IP Pool

Our IP-addresses are on 192.168.20.1/24. We assign the range 192.168.20.10-192.168.20.50 for DHCP to dynamically assign to devices on the network, that haven't been set to static.

```

1 /ip address
2 add address=192.168.20.1/24 interface=ether2 network=192.168.20.0
3 /ip pool
4 add name=dhcp ranges=192.168.20.10-192.168.20.50

```

4.1.1.3 DHCP

We assign the DHCP pool that we created above to the DHCP server, and also assign the two static IP's for the devices on Port 4 and 5 (the Web server and the FTP server).

```

1 /ip dhcp-client
2 add dhcp-options=clientid,hostname disabled=no interface=ether1
3 /ip dhcp-server
4 add address-pool=dhcp disabled=no interface=bridge1 name=server1
5 /ip dhcp-server lease
6 add address=192.168.20.5 comment="Port 5 Static" mac-address=98:28:A6:06:29:B
    ↪ 4 server=server1
7 add address=192.168.20.4 comment="Port 4 Static" mac-address=00:E0:4C:68:00:9
    ↪ D server=server1
8 /ip dhcp-server network
9 add address=192.168.20.0/24 dns-server=192.168.20.1 gateway=192.168.20.1

```

4.1.1.4 DNS

We assign Cloudflare's 1.1.1.1 and Google's 8.8.8.8 as DNS servers.

```
1 /ip dns
2 set allow-remote-requests=yes servers=1.1.1.1,8.8.8.8
```

4.1.1.5 Firewall Rules

We create the Firewall rules for allowing SSH, HTTP(S), DNS, NTP, DHCP and ping. Everything else gets denied, saying the port is unreachable.

```
1 /ip firewall filter
2 add chain=forward comment="Allow SSH" dst-port=22 protocol=tcp
3 add chain=forward comment="Allow HTTPS" port=443 protocol=tcp
4 add chain=forward comment="Allow HTTP" port=80 protocol=tcp
5 add chain=forward comment="Allow DNS" dst-port=53 protocol=udp
6 add chain=forward comment="Allow NTP" dst-port=123 protocol=udp
7 add chain=forward comment="Allow DHCP" dst-port=67 protocol=udp
8 add chain=forward comment="Allow ping" protocol=icmp
9 add action=reject chain=forward comment="Deny everything else" reject-with=icmp-port-unreachable
```

4.1.1.6 NAT Forwarding

We do NAT-forwarding to masquerade outgoing packets to the correct devices on the network. We also add forwarding for our Webserver, both on port 80 and 443 - later one could also do forwarding for other servers on the network.

```
1 /ip firewall nat
2 add action=masquerade chain=srcnat out-interface=ether1
3 add action=dst-nat chain=dstnat comment="NAT-forwarding for Webserver (port 4
  ↳ )" dst-port=80 in-interface=ether1 protocol=tcp to-addresses=192.168.20.4
  ↳ \
4     to-ports=80
5 add action=dst-nat chain=dstnat dst-port=443 in-interface=ether1 protocol=tcp
  ↳ to-addresses=192.168.20.4 to-ports=443
```

4.1.1.7 System Settings

And last, but not least, we set the system clock, UPNP, NTP and set a name for the router.

```
1 /port
2 set 0 name=serial0
3 /ip upnp
```

```

4 set allow-disable-external-interface=no
5 /system clock
6 set time-zone-name=Europe/Copenhagen
7 /system identity
8 set name=Group20
9 /system ntp client
10 set enabled=yes

```

4.1.2 GUI Configuration

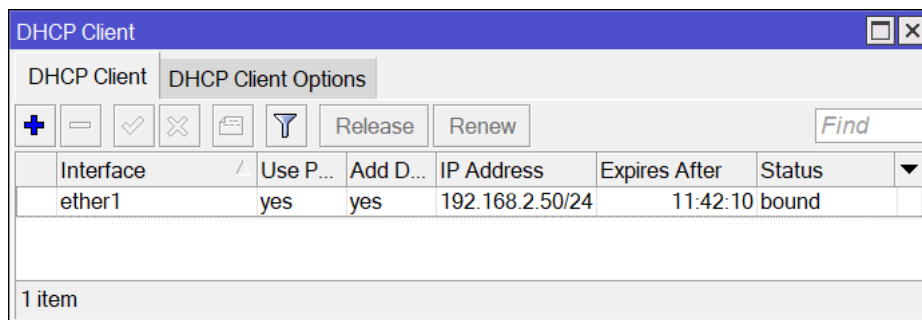
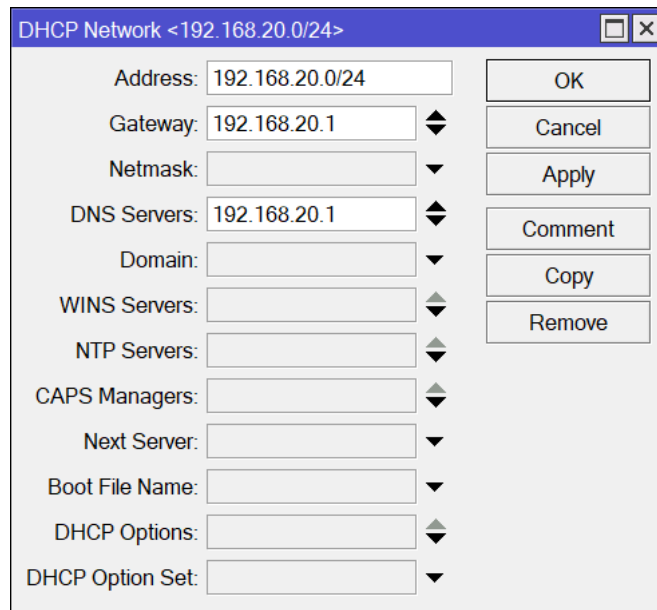


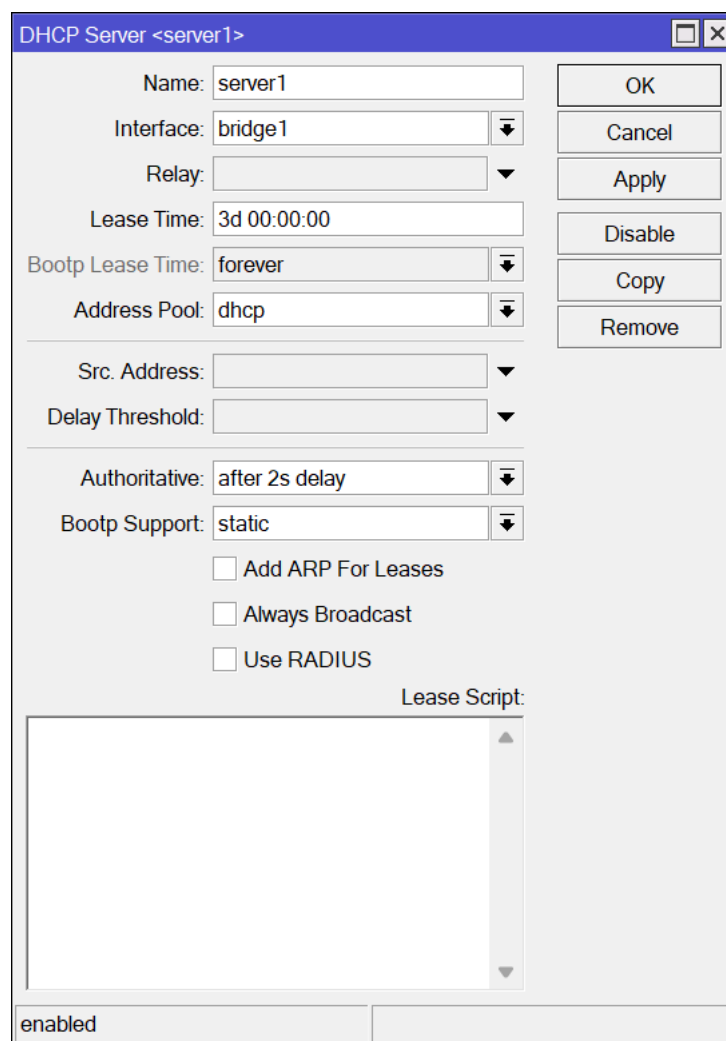
Figure 4: DHCP Client

	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Active Host...	Expires After	Status
D					192.168.20.47	08:97:98:EC:2F:ED	LAPTOP-3...	2d 21:08:32	bound
D					192.168.20.46	38:F3:AB:B7:C0:91	LAPTOP-M...	2d 22:56:11	bound
D					192.168.20.45	B0:0C:D1:46:11:9C	Amadeus	2d 23:46:57	bound
... Port 4 Static									
	192.168.20.4	00:E0:4C:68:00:9D		server1	192.168.20.4	00:E0:4C:68:00:9D	LAPTOP-R...	2d 23:52:42	bound
... Port 5 Static									
	192.168.20.5	98:28:A6:06:29:B4		server1	192.168.20.50	98:28:A6:06:29:B4	HERO-LA...	2d 19:32:38	bound

Figure 5: DHCP Leases

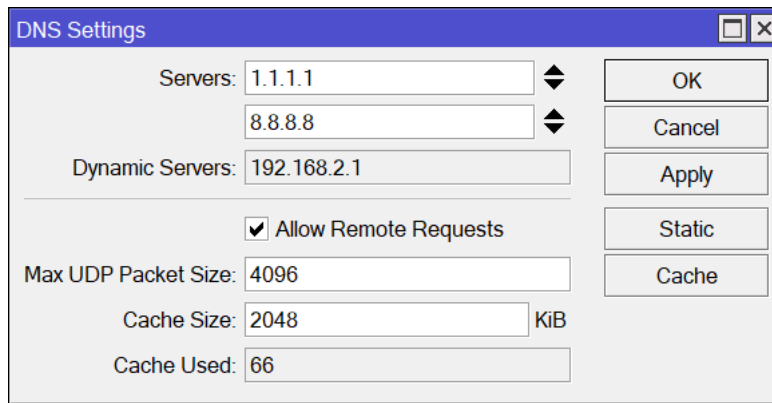


The image shows a window titled "DHCP Network <192.168.20.0/24>". It contains several input fields and a list of buttons on the right. The fields are: Address (192.168.20.0/24), Gateway (192.168.20.1), Netmask (empty), DNS Servers (192.168.20.1), Domain (empty), WINS Servers (empty), NTP Servers (empty), CAPS Managers (empty), Next Server (empty), Boot File Name (empty), DHCP Options (empty), and DHCP Option Set (empty). The buttons on the right are: OK, Cancel, Apply, Comment, Copy, and Remove.

Figure 6: DHCP Network

The image shows a window titled "DHCP Server <server1>". It contains several input fields and a list of buttons on the right. The fields are: Name (server1), Interface (bridge1), Relay (empty), Lease Time (3d 00:00:00), Bootp Lease Time (forever), Address Pool (dhcp), Src. Address (empty), Delay Threshold (empty), Authoritative (after 2s delay), and Bootp Support (static). There are three checkboxes: "Add ARP For Leases", "Always Broadcast", and "Use RADIUS". At the bottom, there is a "Lease Script:" label and a text area. The status at the bottom left is "enabled". The buttons on the right are: OK, Cancel, Apply, Disable, Copy, and Remove.

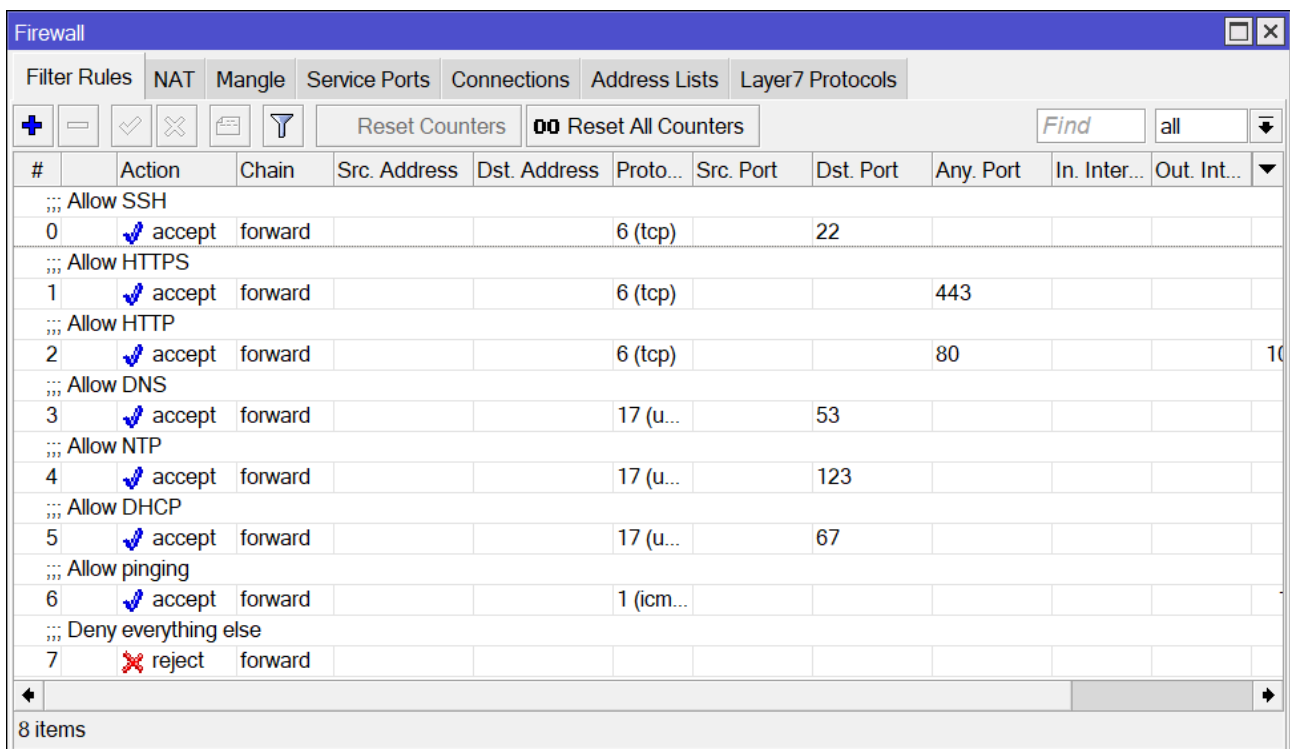
Figure 7: DHCP Server



The DNS Settings window shows the following configuration:

- Servers:** 1.1.1.1, 8.8.8.8
- Dynamic Servers:** 192.168.2.1
- ☒ **Allow Remote Requests**
- Max UDP Packet Size:** 4096
- Cache Size:** 2048 KiB
- Cache Used:** 66

Buttons on the right: OK, Cancel, Apply, Static, Cache.

Figure 8: DNS


The Firewall window shows the Filter Rules tab with the following rules:

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	Any. Port	In. Inter...	Out. Int...
... Allow SSH										
0	✓ accept	forward			6 (tcp)		22			
... Allow HTTPS										
1	✓ accept	forward			6 (tcp)		443			
... Allow HTTP										
2	✓ accept	forward			6 (tcp)		80			10
... Allow DNS										
3	✓ accept	forward			17 (u...		53			
... Allow NTP										
4	✓ accept	forward			17 (u...		123			
... Allow DHCP										
5	✓ accept	forward			17 (u...		67			
... Allow ping										
6	✓ accept	forward			1 (icm...					
... Deny everything else										
7	✗ reject	forward								

8 items

Figure 9: Firewall

Interface List							
Interface Ethernet EoIP Tunnel IP Tunnel GRE Tunnel VLAN VRRP Bonding LTE							
Find							
Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	
... Bridge between Gigabit and Fast switch							
R bridge1	Bridge	1598	145.8 kbps	43.1 kbps	31	48	
... WAN							
R ether1	Ethernet	1598	2.9 kbps	8.1 kbps	5	6	
... GIGABIT LAN MASTER PORT - Ports 2-5 and sfp1 are switched							
RS ether2	Ethernet	1598	0 bps	0 bps	0	0	
S ether3	Ethernet	1598	0 bps	0 bps	0	0	
RS ether4	Ethernet	1598	6.2 kbps	2.4 kbps	4	4	
S ether5	Ethernet	1598	0 bps	0 bps	0	0	
... FAST LAN MASTER PORT - Ports 7-10 are switched							
RS ether6	Ethernet	1598	0 bps	0 bps	0	0	
S ether7	Ethernet	1598	0 bps	0 bps	0	0	
S ether8	Ethernet	1598	0 bps	0 bps	0	0	
S ether9	Ethernet	1598	0 bps	0 bps	0	0	
RS ether10	Ethernet	1598	107.9 kbps	2.5 kbps	12	4	
... Slave to ether2 (part of GIGABIT LAN)							
S sfp1	Ethernet	1598	0 bps	0 bps	0	0	
12 items							

Figure 10: Interface List

IP Pool		
Pools Used Addresses		
Find		
Name	Addresses	Next Pool
dhcph	192.168.20.10-192.168.20.50	none
1 item		

Figure 11: IP Pool

Firewall									
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols									
Reset Counters Reset All Counters Find all									
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Interface	Out. Interface
0	masquerade	srcnat							ether1
... NAT-forwarding for Webserver (port 4)									
1	* dst-nat	dstnat			6 (tcp)		80	ether1	
2	* dst-nat	dstnat			6 (tcp)		443	ether1	
3 items									

Figure 12: NAT Forwarding

5 Conclusion

The company got themselves a very good-looking website, and a "well-working" network.

There were some issues during the exercises, and even though our network configuration and website was up and running prior to the day of the final exercises, it was not possible to visit others' websites, nor for them to visit ours, even though the router configurations was correctly configured. It became possible to visit websites during the last portion of the exercises, but we accidentally captured cached requests with Wireshark, and didn't have enough time to update our own website.

When it became possible to visit other groups' websites, we were able to visit the websites of 5 other groups: 7, 11, 15, 21 and 22 (see Appendix A.1). **We also confirmed that at least 2 other groups were able to visit our website successfully from their networks.**

Basically, we finished the whole project - except for the parts that required you to be able to visit the websites of other groups, which was not the fault of neither our group nor the other groups, but because there was not a large enough time frame for which it was possible to do so, making it extremely difficult to visit other websites and do the captures, especially when you also had to scan for their IP-addresses, and remember to disable your cache (which we forgot, but it was too late when we checked our captures at a later point in time).

A Appendix

A.1 Wireshark Captures

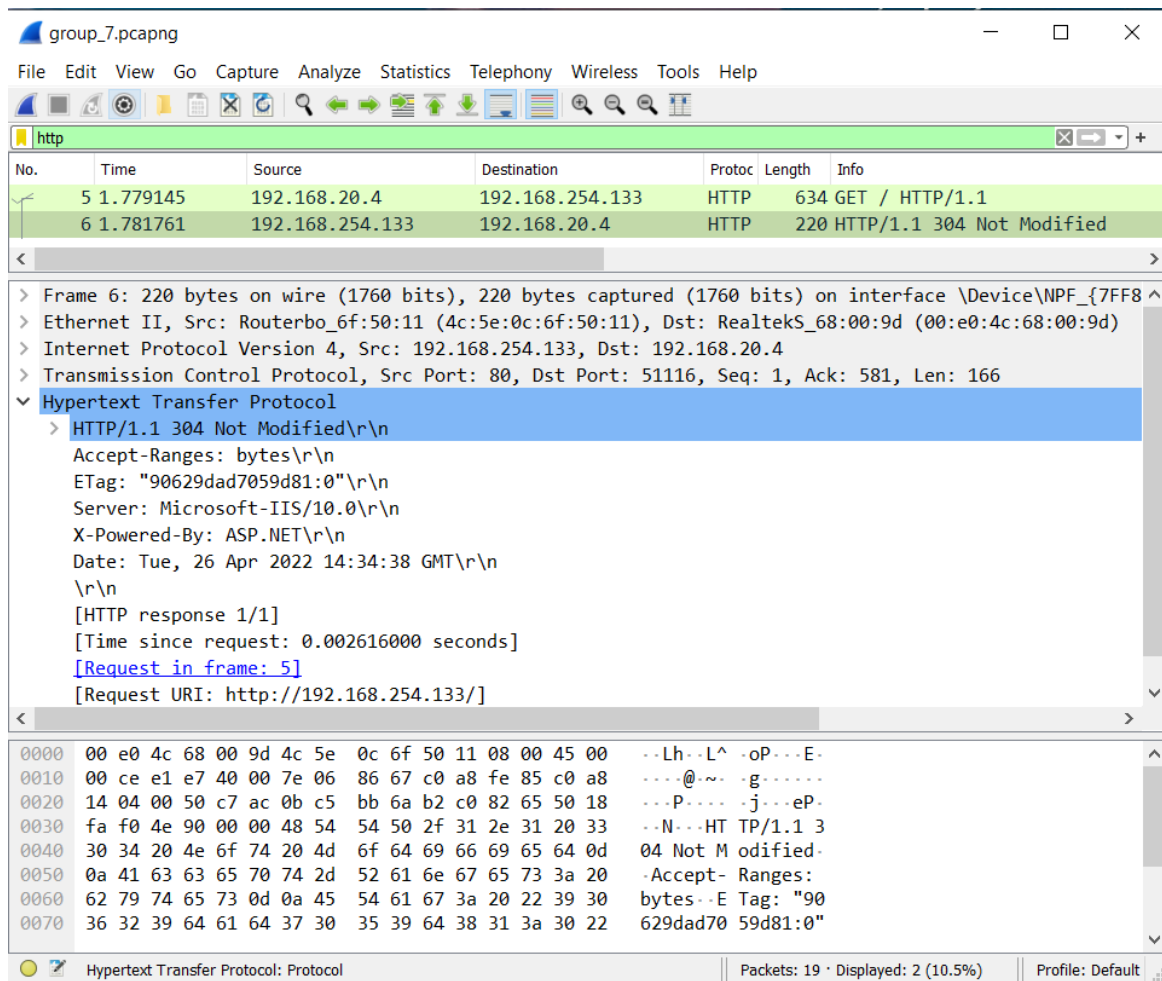


Figure 13: Wireshark capture of group 7

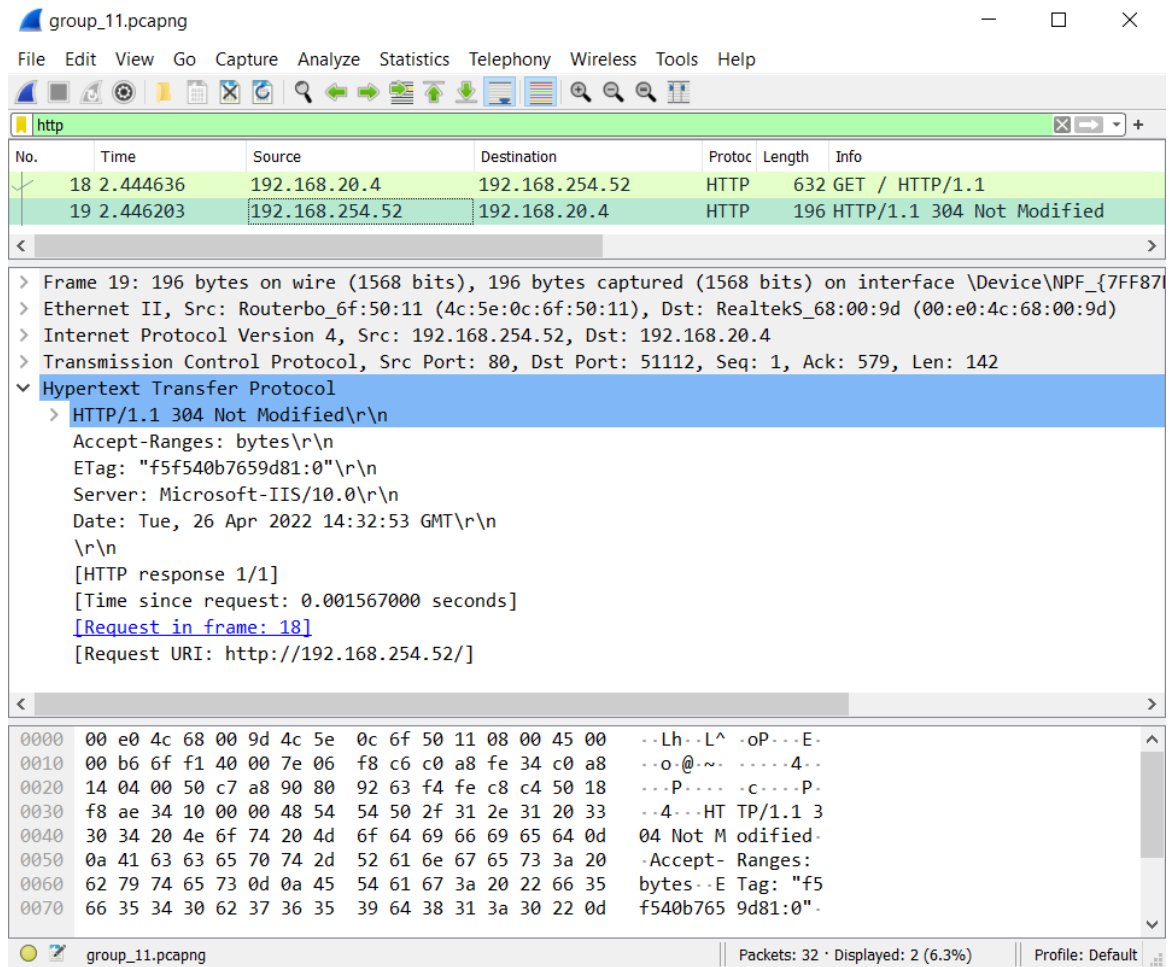
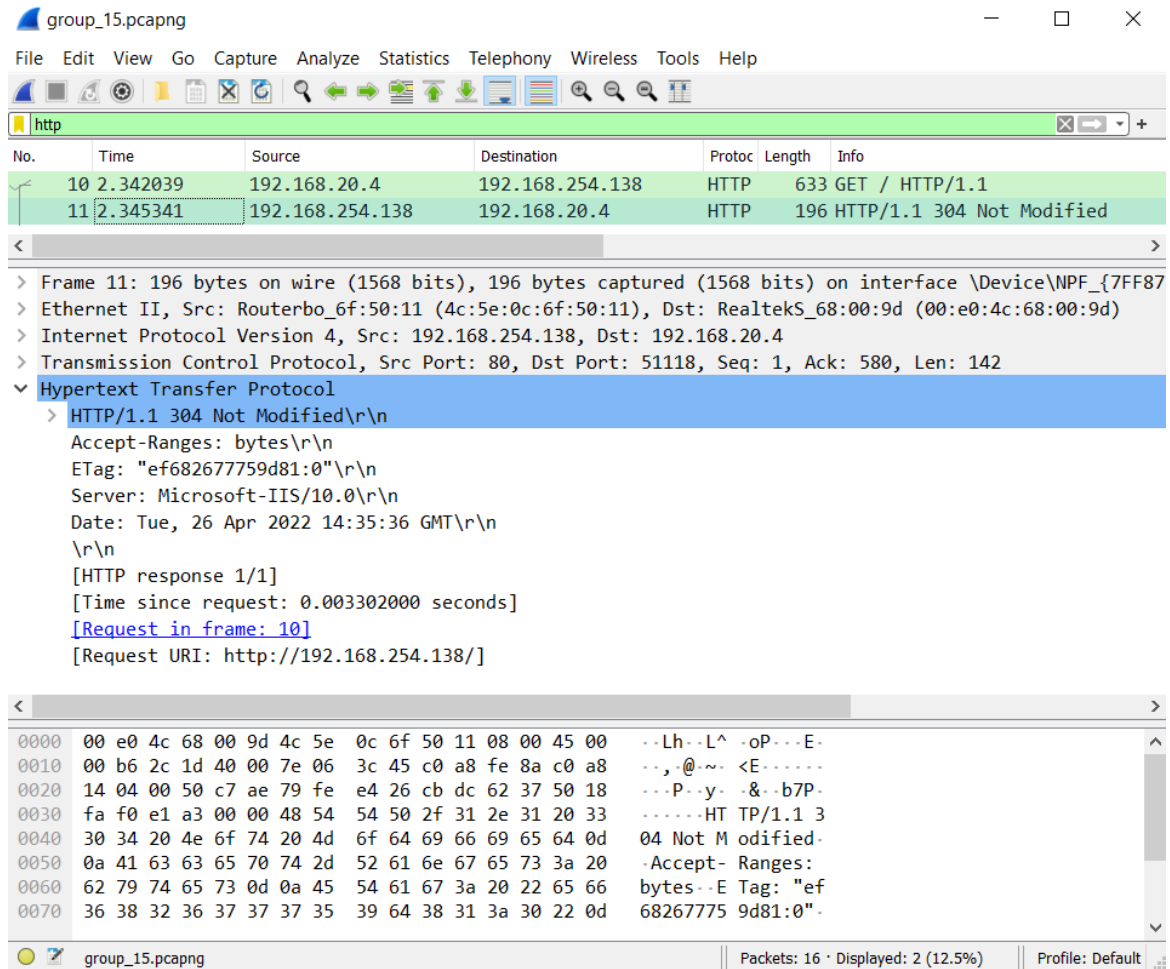


Figure 14: Wireshark capture of group 11



The image shows a Wireshark capture of an HTTP transaction. The packet list shows two packets: a GET request (frame 10) and a 304 Not Modified response (frame 11). The packet details pane shows the structure of the HTTP response, including headers like Accept-Ranges, ETag, Server, and Date. The packet bytes pane shows the raw data of the response.

No.	Time	Source	Destination	Protoc	Length	Info
10	2.342039	192.168.20.4	192.168.254.138	HTTP	633	GET / HTTP/1.1
11	2.345341	192.168.254.138	192.168.20.4	HTTP	196	HTTP/1.1 304 Not Modified

Frame 11: 196 bytes on wire (1568 bits), 196 bytes captured (1568 bits) on interface \Device\NPF_{7FF87...}

Ethernet II, Src: Routerbo_6f:50:11 (4c:5e:0c:6f:50:11), Dst: RealtekS_68:00:9d (00:e0:4c:68:00:9d)

Internet Protocol Version 4, Src: 192.168.254.138, Dst: 192.168.20.4

Transmission Control Protocol, Src Port: 80, Dst Port: 51118, Seq: 1, Ack: 580, Len: 142

Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n

Accept-Ranges: bytes\r\n

ETag: "ef682677759d81:0"\r\n

Server: Microsoft-IIS/10.0\r\n

Date: Tue, 26 Apr 2022 14:35:36 GMT\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.003302000 seconds]

[Request in frame: 10]

[Request URI: http://192.168.254.138/]

0000 00 e0 4c 68 00 9d 4c 5e 0c 6f 50 11 08 00 45 00 ..Lh..L^..oP...E.

0010 00 b6 2c 1d 40 00 7e 06 3c 45 c0 a8 fe 8a c0 a8 ..,.@~<E.....

0020 14 04 00 50 c7 ae 79 fe e4 26 cb dc 62 37 50 18 ...P..y..&..b7P.

0030 fa f0 e1 a3 00 00 48 54 54 50 2f 31 2e 31 20 33HT TP/1.1 3

0040 30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d 04 Not M odified.

0050 0a 41 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 -Accept- Ranges:

0060 62 79 74 65 73 0d 0a 45 54 61 67 3a 20 22 65 66 bytes..E Tag: "ef

0070 36 38 32 36 37 37 37 35 39 64 38 31 3a 30 22 0d 68267775 9d81:0".

Figure 15: Wireshark capture of group 15

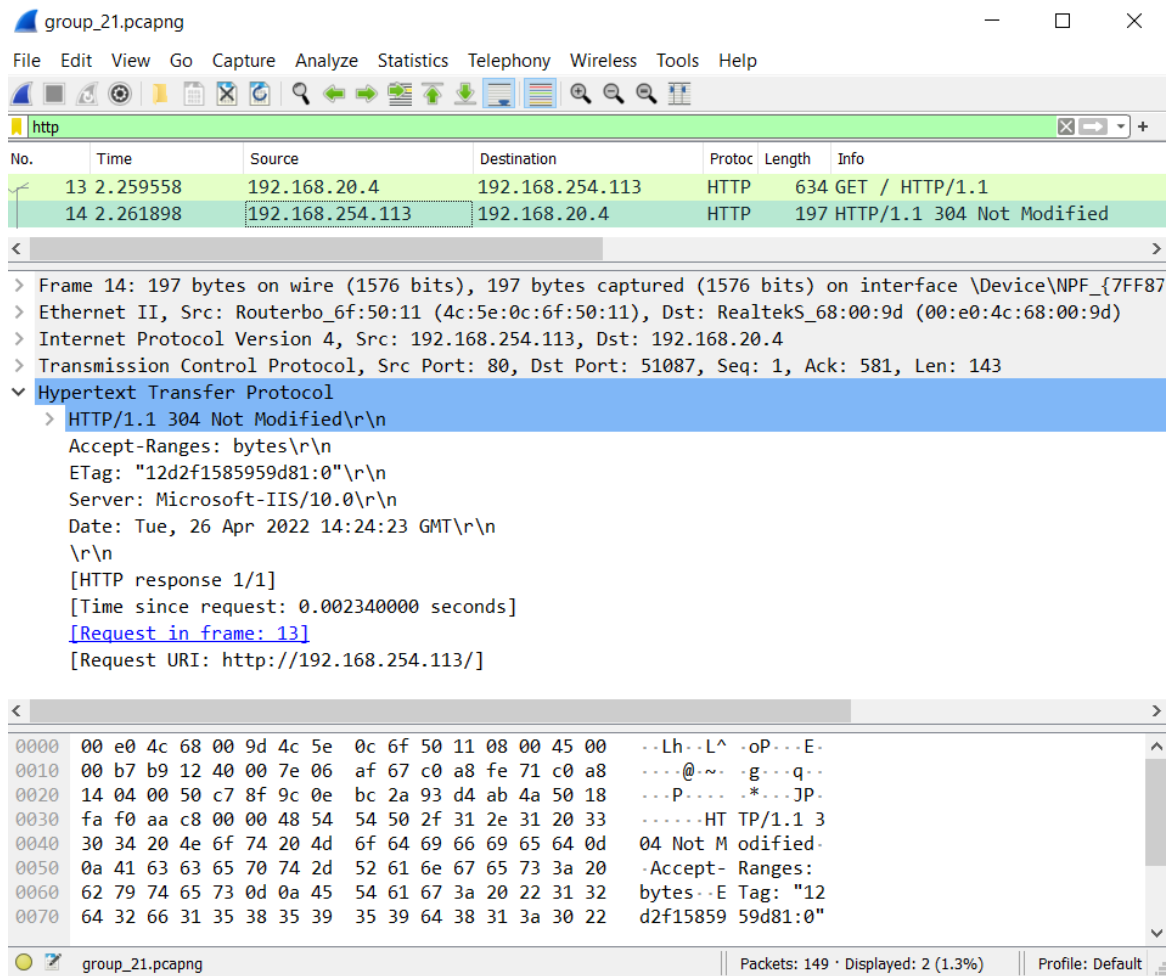


Figure 16: Wireshark capture of group 21

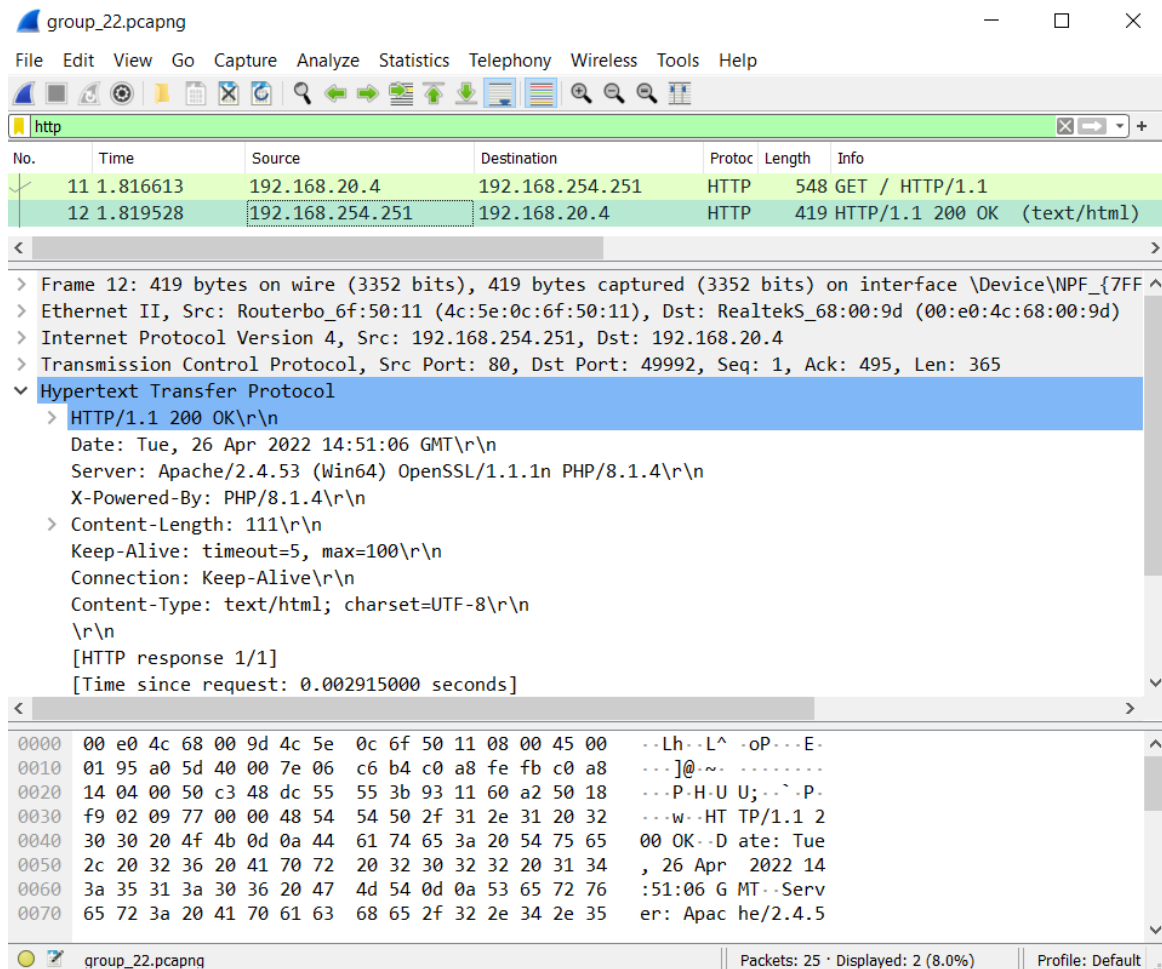


Figure 17: Wireshark capture of group 22

A.2 Router Configuration Export

```

1 # apr/26/2022 15:30:13 by RouterOS 6.18
2 # software id = PLBF-NQ9T
3 #
4 /interface bridge
5 add comment="Bridge between Gigabit and Fast switch" l2mtu=1598 name=bridge1
6 /interface ethernet
7 set [ find default-name=ether1 ] comment=WAN
8 set [ find default-name=ether2 ] comment="GIGABIT LAN MASTER PORT - Ports 2-5
  ↳ and sfpl are switched"
9 set [ find default-name=ether3 ] master-port=ether2
10 set [ find default-name=ether4 ] master-port=ether2
11 set [ find default-name=ether5 ] master-port=ether2
12 set [ find default-name=ether6 ] comment="FAST LAN MASTER PORT - Ports 7-10 a
  ↳ re switched"
13 set [ find default-name=ether7 ] master-port=ether6
14 set [ find default-name=ether8 ] master-port=ether6
15 set [ find default-name=ether9 ] master-port=ether6

```

```
16 set [ find default-name=ether10 ] master-port=ether6
17 set [ find default-name=sfp1 ] comment="Slave to ether2 (part of GIGABIT LAN)"
   ↪ " master-port=ether2
18 /ip neighbor discovery
19 set ether1 comment=WAN
20 set ether2 comment="GIGABIT LAN MASTER PORT - Ports 2-5 and sfp1 are switched"
21 set ether6 comment="FAST LAN MASTER PORT - Ports 7-10 are switched"
22 set sfp1 comment="Slave to ether2 (part of GIGABIT LAN)"
23 set bridge1 comment="Bridge between Gigabit and Fast switch"
24 /interface wireless security-profiles
25 set [ find default=yes ] supplicant-identity=MikroTik
26 /ip pool
27 add name=dhcp ranges=192.168.20.10-192.168.20.50
28 /ip dhcp-server
29 add address-pool=dhcp disabled=no interface=bridge1 name=server1
30 /port
31 set 0 name=serial0
32 /interface bridge port
33 add bridge=bridge1 interface=ether2
34 add bridge=bridge1 interface=ether6
35 /ip address
36 add address=192.168.20.1/24 interface=ether2 network=192.168.20.0
37 /ip dhcp-client
38 add dhcp-options=clientid,hostname disabled=no interface=ether1
39 /ip dhcp-server lease
40 add address=192.168.20.5 comment="Port 5 Static" mac-address=98:28:A6:06:29:B
   ↪ 4 server=server1
41 add address=192.168.20.4 comment="Port 4 Static" mac-address=00:E0:4C:68:00:9
   ↪ D server=server1
42 /ip dhcp-server network
43 add address=192.168.20.0/24 dns-server=192.168.20.1 gateway=192.168.20.1
44 /ip dns
45 set allow-remote-requests=yes servers=1.1.1.1,8.8.8.8
46 /ip firewall filter
47 add chain=forward comment="Allow SSH" dst-port=22 protocol=tcp
48 add chain=forward comment="Allow HTTPS" port=443 protocol=tcp
49 add chain=forward comment="Allow HTTP" port=80 protocol=tcp
50 add chain=forward comment="Allow DNS" dst-port=53 protocol=udp
51 add chain=forward comment="Allow NTP" dst-port=123 protocol=udp
52 add chain=forward comment="Allow DHCP" dst-port=67 protocol=udp
53 add chain=forward comment="Allow ping" protocol=icmp
54 add action=reject chain=forward comment="Deny everything else" reject-with=ic
   ↪ mp-port-unreachable
55 /ip firewall nat
56 add action=masquerade chain=srcnat out-interface=ether1
57 add action=dst-nat chain=dstnat comment="NAT-forwarding for Webserver (port 4
   ↪ )" dst-port=80 in-interface=ether1 protocol=tcp to-addresses=192.168.20.4
   ↪ \
```

```
58     to-ports=80
59 add action=dst-nat chain=dstnat dst-port=443 in-interface=ether1 protocol=tcp
    ↪ to-addresses=192.168.20.4 to-ports=443
60 /ip upnp
61 set allow-disable-external-interface=no
62 /system clock
63 set time-zone-name=Europe/Copenhagen
64 /system identity
65 set name=Group20
66 /system ntp client
67 set enabled=yes
```

B Bibliography