Communications and Computer Networks

Prof. Dr. Daniel Spiekermann
ccn@fh-dortmund.de

Summer term 2023

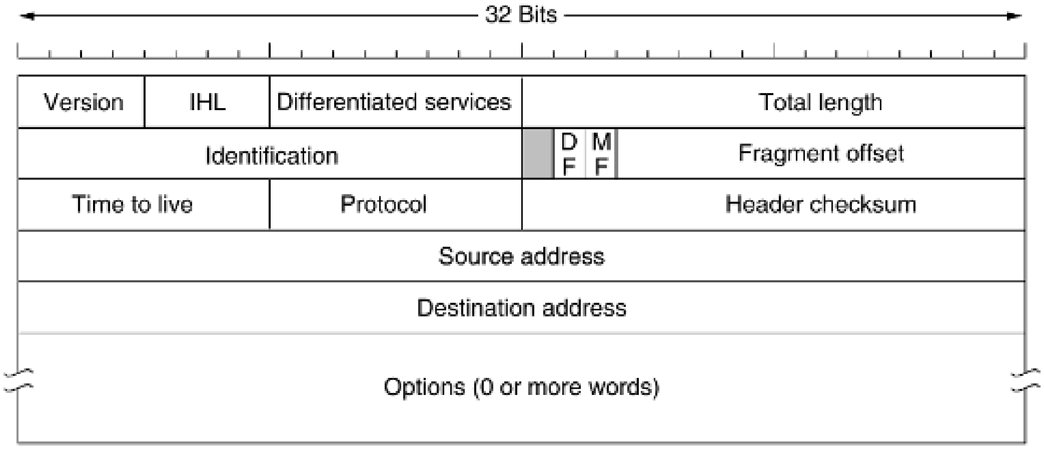
Exercise 4

Information: If necessary, remove the suffix *.sec* of files downloaded from ILIAS.

1 IPv4

1. Sketch the individual fields of an IPv4 datagram and explain their meaning.

Solution:



IHL Internet Header Length:
Consists of 4 bits that indicate how long the datagram header is (specified in 32-bit words, min =5 (20 bytes) max=15 (60 bytes)

Type of Service (TOS): The field can be set and
evaluated for the prioritization of IP data packets (Quality of Service)

Total length:
Specifies the total length of an IP datagram (header and payload), can calculate the actual data length by subtracting IHL and total length (16 bits: total packet in bytes; maximum packet length of 65535 bytes)

Identification:
IP packets are uniquely identified by a number (16 bit)

Flags:
Indicates whether fragmentation of the datagram is possible or fragments follow (DF= Don't Fragment; MF = More Fragments)

Fragment Number (Fragment Offset):
Specifies the relative position of the datagram fragment to the original (specified in 8-byte blocks)

Time to Live:
Contains number of routers to be traversed (decremented by 1 for each traversal). If TTL = 0, the packet is discarded.

Protocol Number:
Identifies the protocol in the data field (e.g. TCP = 6 or UDP = 17)

Header checksum:
Detects changes in the header (not in the payload). Parity check ⇒ sum of all 16 bit words + header checksum; no errors if 0xFFFF.

Source address:
Address of source node; destination address: Address of the destination node

Options (not necessarily present):
Identifies additional services

Fill bits (padding):
Ensure that the length of a datagram header is an integer multiple of 32 bits

Data:
User data

2. You have the following bit stream in the network

```
5c 49 79 8e 23 a3 5c e9  1e ae 7c ef 08 00 45 00
00 54 a8 ac 00 00 40 01  35 d0 c0 a8 0a 51 c1 19
10 1a 08 00 44 a6 2e 1c  00 03 64 4b cf d7 00 0a
66 0a 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15
16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25
26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35
36 37
```

Interpret the blue marked hex code.

Solution: It is a header of an IPv4 packet.

```
v Internet Protocol Version 4, Src: 192.168.10.81, Dst: 193.25.16.26
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xa8ac (43180)
  v 000. .... = Flags: 0x0
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x35d0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.10.81
    Destination Address: 193.25.16.26
```

3. Why is the maximum packet size of an ipv4-packet 65.535?

Solution: The related Total length field is only 16bit long, so $2^{16} = 65,535$.

4. You see an IHL value of 10. How long is the header? What is a reason for this length?

Solution: The length of the IP-header is $10 \cdot 32bit = 320bit \Leftrightarrow 320 \div 8 = 40Byte$
A reason for this is the use of the option field, e. g. the option field is present and has to be considered.

2 Addressing

5. Calculate the network address, broadcast address and address range for the hosts and the number of usable host addresses of the following addresses:
   - 10.0.3.0/8
   - 10.0.3.7/19
   - 171.13.9.47/28
   - 88.94.0.0/21
   - 66.91.119.8/30

Solution:

- 10.0.3.0/8
  - net: 10.0.0.0
  - bc: 10.255.255.255
  - range: 10.0.0.1 - 10.255.255.254
  - number: 16,777,214
- 10.0.3.7/19
  - net: 10.0.0.0
  - bc: 10.0.31.255
  - range: 10.0.0.1 - 10.0.31.254
  - number: 8,190
- 171.13.9.47/28
  - net: 71.13.9.32
  - bc: 71.13.9.47
  - range: 171.13.9.33 - 171.13.9.46
  - number: 14
- 88.94.0.0/21
  - net: 88.94.0.0
  - bc: 88.94.7.255
  - range: 88.94.0.1 - 88.94.7.254
  - number: 2046

- 66.91.119.8/30
  - net: 66.91.119.8
  - bc: 66.91.119.11
  - range: 66.91.119.9 - 66.91.119.10
  - number: 2

3 Fragmentation

6. An ICMP Echo Reply packet with 2000 bytes of user data is sent over a standard Ethernet (MTU = 1500 bytes). What is the size of the associated Ethernet frames (including preamble and FCS)?

Solution: First ethernet frame: Data = 1500 Byte (=20 Byte IP -Header + 1480 IP-Data (=8 Byte ICMP Header + 1472 Byte ICMP Data)) + 14 Bytes ethernet addresses and EtherType + 8 Bytes preamble and SFD + 4 byte FCS = 1526 Bytes

Second ethernet frame: Data = 548 Byte (= 20 Byte IP-Header + 528 IP-Data (=528 Byte ICMP Data)) + 14 Bytes ethernet addresses and EtherType + 8 Bytes preamble and SFD + 4 byte FCS = 574 Bytes

7. Assume you want to transfer an icmp packet with a size of 5800 bytes. Fill in the relevant value in the following fields:

Packet no	Length	DF	MF	Offset	proto

Packet no	Length	DF	MF	Offset	proto

Packet no	Length	DF	MF	Offset	proto

Packet no	Length	DF	MF	Offset	proto

Packet no	Length	DF	MF	Offset	proto

Packet no	Length	DF	MF	Offset	proto

Solution:

Packet no	Length	DF	MF	Offset	proto
1	1500	0	1	0	0x01

Packet no	Length	DF	MF	Offset	proto
2	1500	0	1	1480	0x01

Packet no	Length	DF	MF	Offset	proto
3	1500	0	1	2960	0x01

Packet no	Length	DF	MF	Offset	proto
4	1388	0	0	4440	0x01

4 ICMP

8. *Reconstruct* the path of your host to

- www.google.com
- www.dortmund.de
- www.wireshark.org

What is striking?

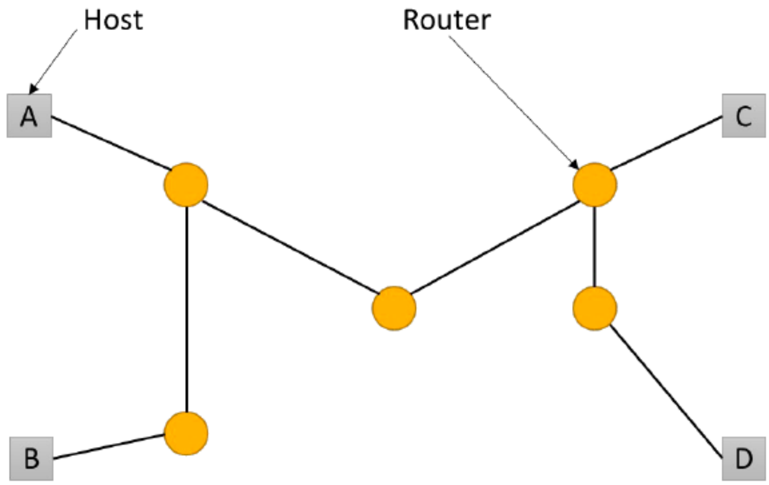
Solution: The beginning of each traceroute should be listing the home router. Depending on the destination, the path might differ.

9. The data packets of a network trace with *Wireshark* are shown below. Which command was used to generate the traffic? Also include any command options that were used.

```
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, id 0
Ethernet II, Src: Apple_ae:7c:ef (5c:e9:1e:ae:7c:ef), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, id 0
Ethernet II, Src: Raspberr_a1:c6:18 (b8:27:eb:a1:c6:18), Dst: Apple_ae:7c:ef (5c:e9:1e:ae:7c:ef)
Address Resolution Protocol (reply)

Frame 3: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id 0
Ethernet II, Src: Apple_ae:7c:ef (5c:e9:1e:ae:7c:ef), Dst: Raspberr_a1:c6:18 (b8:27:eb:a1:c6:18)
Internet Protocol Version 4, Src: 192.168.10.81, Dst: 192.168.10.76
Data (1480 bytes)

Frame 4: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface en0, id 0
Ethernet II, Src: Apple_ae:7c:ef (5c:e9:1e:ae:7c:ef), Dst: Raspberr_a1:c6:18 (b8:27:eb:a1:c6:18)
Internet Protocol Version 4, Src: 192.168.10.81, Dst: 192.168.10.76
Internet Control Message Protocol

Frame 5: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id 0
Ethernet II, Src: Raspberr_a1:c6:18 (b8:27:eb:a1:c6:18), Dst: Apple_ae:7c:ef (5c:e9:1e:ae:7c:ef)
Internet Protocol Version 4, Src: 192.168.10.76, Dst: 192.168.10.81
Data (1480 bytes)

Frame 6: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface en0, id 0
Ethernet II, Src: Raspberr_a1:c6:18 (b8:27:eb:a1:c6:18), Dst: Apple_ae:7c:ef (5c:e9:1e:ae:7c:ef)
Internet Protocol Version 4, Src: 192.168.10.76, Dst: 192.168.10.81
Internet Control Message Protocol

Frame 7: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id 0
Ethernet II, Src: Apple_ae:7c:ef (5c:e9:1e:ae:7c:ef), Dst: Raspberr_a1:c6:18 (b8:27:eb:a1:c6:18)
Internet Protocol Version 4, Src: 192.168.10.81, Dst: 192.168.10.76
Data (1480 bytes)

Frame 8: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface en0, id 0
Ethernet II, Src: Apple_ae:7c:ef (5c:e9:1e:ae:7c:ef), Dst: Raspberr_a1:c6:18 (b8:27:eb:a1:c6:18)
Internet Protocol Version 4, Src: 192.168.10.81, Dst: 192.168.10.76
Internet Control Message Protocol

Frame 9: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id 0
Ethernet II, Src: Raspberr_a1:c6:18 (b8:27:eb:a1:c6:18), Dst: Apple_ae:7c:ef (5c:e9:1e:ae:7c:ef)
Internet Protocol Version 4, Src: 192.168.10.76, Dst: 192.168.10.81
Data (1480 bytes)

Frame 10: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface en0, id 0
Ethernet II, Src: Raspberr_a1:c6:18 (b8:27:eb:a1:c6:18), Dst: Apple_ae:7c:ef (5c:e9:1e:ae:7c:ef)
Internet Protocol Version 4, Src: 192.168.10.76, Dst: 192.168.10.81
Internet Control Message Protocol
```

Solution: ping -s 1600 192.168.10.76 -c2

10. The figure below shows a network with multiple routers (yellow circles) and hosts A, B, C and D. Determine the minimum required TTL for IPv4 communication between A-B, A-C, A-D and B-D. What would happen if the TTL is too small?



Solution:

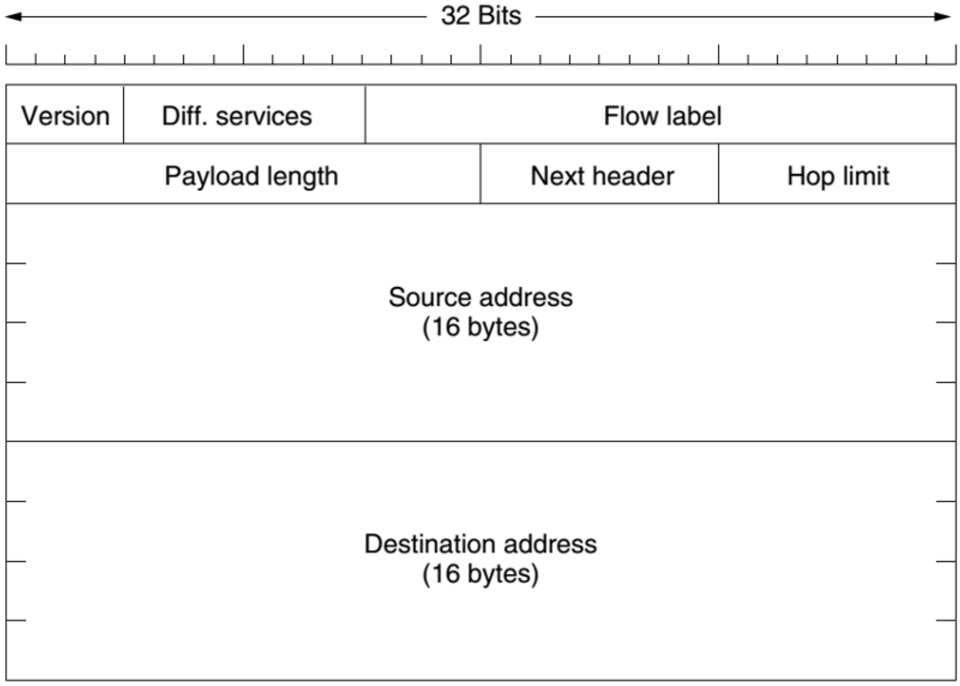
- A-B: TTL = 3
- A-C: TTL = 4
- A-D: TTL = 5
- B-D: TTL = 6

If the TTL is too small, the last router (which drops the packet) sends an ICMP error message to the sender: ICMP Type 11: Time Exceeded with the code: Time to live exceeded in transit

5 IPv6

11. Sketch the individual fields of an IPv6 datagram and explain their meaning.

Solution:



Version:
Version 6

Differential Services (before: Traffic Class):
Quality of Service (Service Type for IPv4)

Flow Label:

identifies a route that meets the requirements of the Traffic Class. Packages bearing the same flow label, are treated equally.

Payload Length:
Length of user data

Next Header:
specifies the type of the next header or, if it does not exist, the type of data. (Protocol for IPv4)

Hop limit:
like TTL for IPv4

Source and destination address:
Addressing of the communication partners

Data:
User data

12. Calculate the address range of the following addresses:

- fe80::/10
- 2001:3211:7600:9/48
- 2001:AABB:4000::0312:6641/28

Solution:

- fe80::/10 ⇒ fe80:: - febf:ffff:ffff...
- 2001:3211:7600::9/48 ⇒ 2001:3211:7600:: - 2001:3211:7600:ffff:ffff...
- 2001:aabb:4000::0312:6641/28 ⇒ 2001:aab0:: - 2001:aabf:ffff...

13. Assign cases A - G to the given IPv6 prefixes/addresses:

    - A: IPv6-Multicast- Address
    - B: IPv6-Link-Local- Address
    - C: Ipv6-Global-Unicast- Address
    - D: IPv6-Loopback-Address
    - E: IPv6-Unique Local Unicast- Address
    - F: IPv6 embedded IPv4 Address
    - G: Unspecified Address
    - H: Reserved

    - 2001:db8::8d3:0:8a2e:70:7344
    - fd6a:291c:f971::/48
    - ff15:faad:7741:88a:874:33::11
    - ::
    - fe80::456:489d:4afa:b00a
    - ::1/128
    - 20a0:faaf:1411:77aa:99::33
    - fdca:9f01:549b::/48
    - 64:ff9b::192.168.0.1

Solution:

- 2001:db8::8d3:0:8a2e:70:7344 - H
- fd6a:291c:f971::/48 - E
- ff15:faad:7741:88a:874:33::11 - A
- :: - G
- fe80::456:489d:4afa:b00a - B
- ::1/128 - D
- 20a0:faaf:1411:77aa:99::33 - C
- fdca:9f01:549b::/48 - E
- 64:ff9b::192.168.0.1 - F

14. Your provider assigns the following subnet to you.

    201f:3300:da11:7000::/56

    You want to create at least 22 networks. Which subnetmask is needed, which are the netaddresses of these networks?

Solution: Subnet is 201f:3300:da11:7000
To create 22 networks, you need at least 5 bits, so possible subnets are:

- 201f:3300:da11:7000:0000::/61
  First: Address 201f:3300:da11:7000:0000:0000:0000:0000
  Last Address 201f:3300:da11:7007:ffff:ffff:ffff:ffff
- 201f:3300:da11:7008:0000::/61
- 201f:3300:da11:7010:0000::/61
- 201f:3300:da11:7018:0000::/61
- 201f:3300:da11:7020:0000::/61
- 201f:3300:da11:7028:0000::/61
- 201f:3300:da11:7030:0000::/61
- 201f:3300:da11:7038:0000::/61
- 201f:3300:da11:7040:0000::/61
- 201f:3300:da11:7048:0000::/61
- 201f:3300:da11:7050:0000::/61
- 201f:3300:da11:7058:0000::/61
- 201f:3300:da11:7060:0000::/61
- 201f:3300:da11:7068:0000::/61
- 201f:3300:da11:7070:0000::/61
- 201f:3300:da11:7078:0000::/61
- 201f:3300:da11:7080:0000::/61
- 201f:3300:da11:7088:0000::/61
- 201f:3300:da11:7090:0000::/61
- 201f:3300:da11:7098:0000::/61
- 201f:3300:da11:70a0:0000::/61
- 201f:3300:da11:70a8:0000::/61

15. After autoconfiguration in the LAN, an interface has the IPv6 address 2001:200:0:8002:203:47FF:FEA5:3085/64 What are the Link-Local IPv6 address and the MAC address (when EUI-64 is used)?

Solution: fe80::203:47FF:FEA5:3085/64 LLA
00:03:47:A5:30:85 MAC-Address (delete FF:FE and invert Bit 7) of 02
02 ⇒ 0000 0010, invert Bit 7 ⇒ 0000 0000

16. Check you local IP-configuration and extract the ip-address and routing configuration. Which commands do you use?

Solution: Configuration differs, necessary tools are

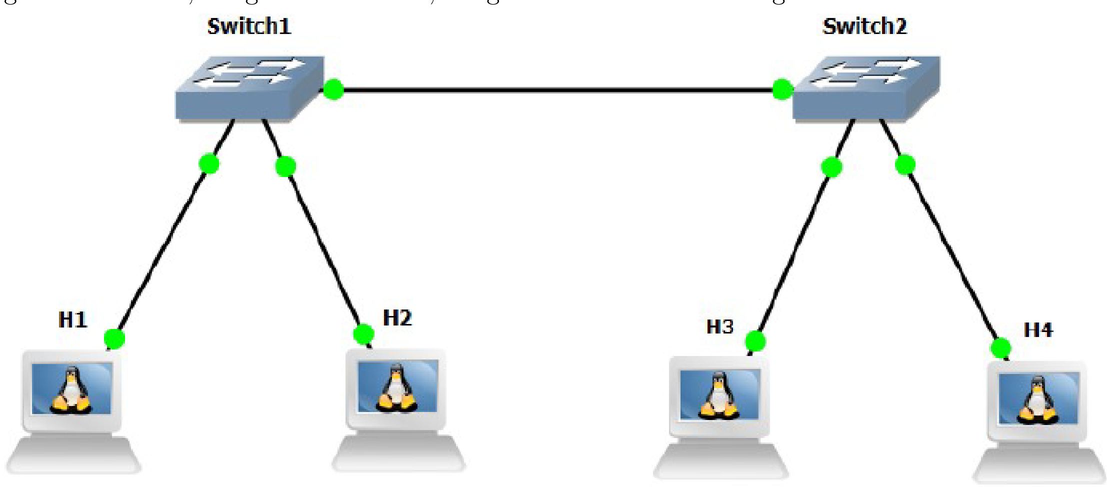
- ip addr show
- ipconfig
- arp
- ndp
- route -n
- ip route show
- ...

6 Tools

17. Create a GNS3 project with two switches and four hosts (no VPCs, please use hosts) and connect the components as shown in the figure. Start a capturing with Wireshark on all connections. Configure different IP addresses on all four hosts in the same network. Add the following code in the file */etc/networking/interfaces*, change the address on each host.

```
auto eth0
iface eth0 inet static
address 192.168.0.1
netmask 255.255.255.0
broadcast 192.168.0.255
```

H1 gets 192.168.0.1, H2 gets 192.168.0.2, H3 gets 192.168.0.3 and H4 gets 192.168.0.4.



Configure a separate broadcast domain for Host 1 and 3 and a separate broadcast domain for host 2 and host 4.

Solution: H1/H3 and H2/H4 have to be in different vlans, created on switch 1 and switch 2 and a trunk between SW1 and SW2.

7 Routing

18. Shown are the routing table and the ARP table of the computer (R) with the two IP addresses of the interfaces eth1 and eth0: 193.25.22.65 and 192.168.44.1

Routing Table

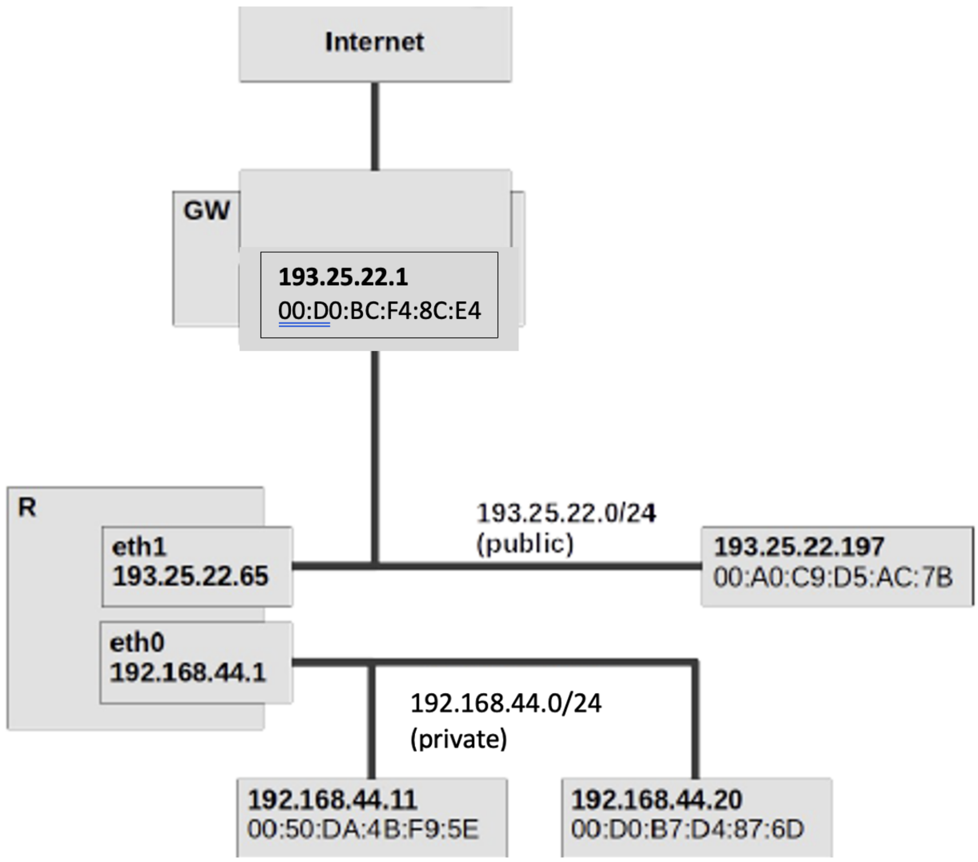
Destination	Gateway	Genmask	Iface
193.25.22.0	0.0.0.0	255.255.255.0	eth1
192.168.44.0	0.0.0.0	255.255.255.0	eth0
127.0.0.1	0.0.0.0	255.255.255.0	lo
0.0.0.0	193.25.22.1	0.0.0.0	eth1

ARP Cache

Address	HWType	HWAddress	Iface
192.168.44.11	Ether	00:50:DA:4B:F9:5E	eth0
192.168.44.20	Ether	00:D0:B7:D4:87:6D	eth0
193.25.22.197	Ether	00:A0:C9:D5:AC:7B	eth1
193.25.22.1	Ether	00:D0:BC:F4:8C:E4	eth1

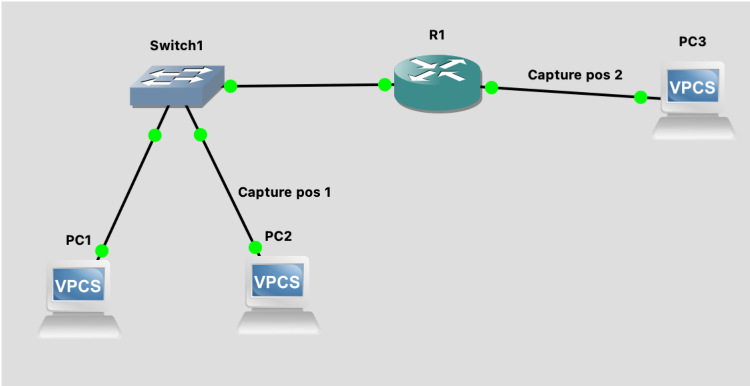
Sketch the network in which this computer is located and the neighbouring networks with hosts and routers.

Solution:



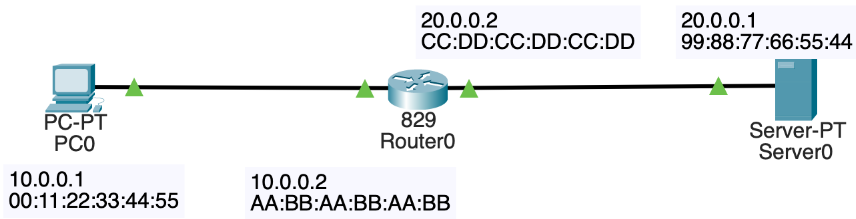
19. Load the pcapng-file *net1.pcapng* with *Wireshark* and determine the involved devices of the network. Draw a plan of the network resting upon the information of the capture file. *Additional information:*

the capture was done on two different positions in the network, and subsequently merged to a single file



Solution:
Information in the pcap:
Two ip-ranges (10.0.0.0 and 11.0.0.0) indicate the need for a router. Different mac-addresses in the packets. ARP request is captured on one position, but not the response (indicates the existence of a switch)

20. Assume you have a network as shown in the next figure. The PC wants to ping the server. Router0



performs routing.
Fill in the missing values in the boxes:

Left of Router0:

source ip-address	
destination ip address	
source mac-address	
destination mac-address	

Right of Router0:

source ip-address	
destination ip address	
source mac-address	
destination mac-address	

Solution: Left of Router0:

- source ip-address: 10.0.0.1
- destination ip-address: 20.0.0.1
- source mac-address: 00:11:22:3:44:55
- destination mac-address: AA:BB:AA:BB:AA:BB

Right of Router0:

- source ip-address: 10.0.0.1

- destination ip-address: 20.0.0.1
- source mac-address: CC:DD:CC:DD:CC:DD
- destination mac-address: 99:88:77:66:55:44

21. Now assume the router0 performs network address translation.
Fill in the missing values in the boxes:
Left of Router0:

source ip-address	
destination ip address	
source mac-address	
destination mac-address	

Right of Router0:

source ip-address	
destination ip address	
source mac-address	
destination mac-address	

Solution: Left of Router0:

- source ip-address: 10.0.0.1
- destination ip-address: 20.0.0.1
- source mac-address: 00:11:22:3:44:55
- destination mac-address: AA:BB:AA:BB:AA:BB

Right of Router0:

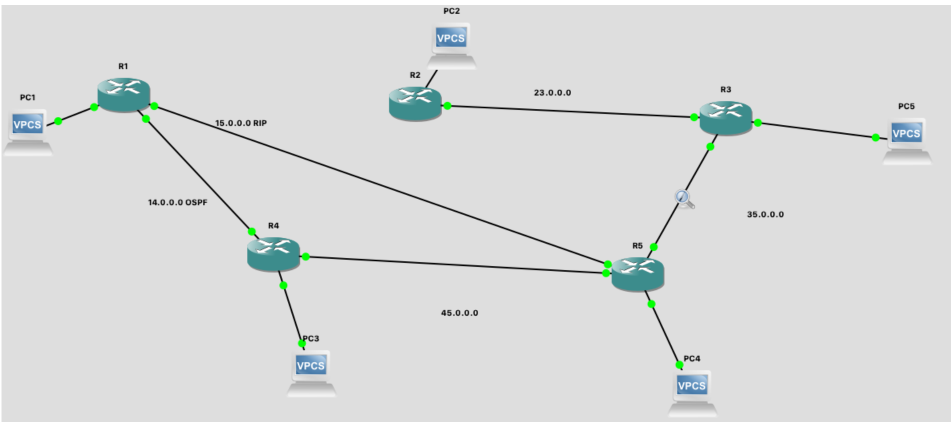
- source ip-address: 20.0.0.2
- destination ip-address: 20.0.0.1
- source mac-address: CC:DD:CC:DD:CC:DD
- destination mac-address: 99:88:77:66:55:44

22. You have this routing table of a router in a network.

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

O     10.0.0.0/8 [110/2] via 14.0.0.1, 00:31:16, FastEthernet0/0
      14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        14.0.0.0/8 is directly connected, FastEthernet0/0
L        14.0.0.2/32 is directly connected, FastEthernet0/0
O     15.0.0.0/8 [110/2] via 14.0.0.1, 00:31:16, FastEthernet0/0
      20.0.0.0/24 is subnetted, 1 subnets
O        20.0.0.0 [110/4] via 45.0.0.2, 00:00:03, FastEthernet1/0
O     23.0.0.0/8 [110/3] via 45.0.0.2, 00:00:03, FastEthernet1/0
      30.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C        30.0.0.0/8 is directly connected, FastEthernet1/1
O        30.0.0.0/24 [110/3] via 45.0.0.2, 00:00:03, FastEthernet1/0
L        30.0.0.2/32 is directly connected, FastEthernet1/1
O     35.0.0.0/8 [110/2] via 45.0.0.2, 00:00:03, FastEthernet1/0
      40.0.0.0/24 is subnetted, 1 subnets
O        40.0.0.0 [110/2] via 45.0.0.2, 00:25:28, FastEthernet1/0
      45.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        45.0.0.0/8 is directly connected, FastEthernet1/0
L  _     45.0.0.1/32 is directly connected, FastEthernet1/0
```

Create a GNS3-project resulting in such a routing table.

Solution:



23. Open the GNS3-project static-routing.gnsproject and configure H3 as a router. Configure H1 and H2 with the following ip-addresses:

- H1: 10.0.0.1/24
- H2: 10.3.0.3/24

Configure all hosts to route the traffic properly. After the configuration, H1 should be able to ping H2.

Solution: Commands on H1:

```
ip addr add 10.0.0.1/24 dev eth0
ip route add default via 10.0.0.254
```

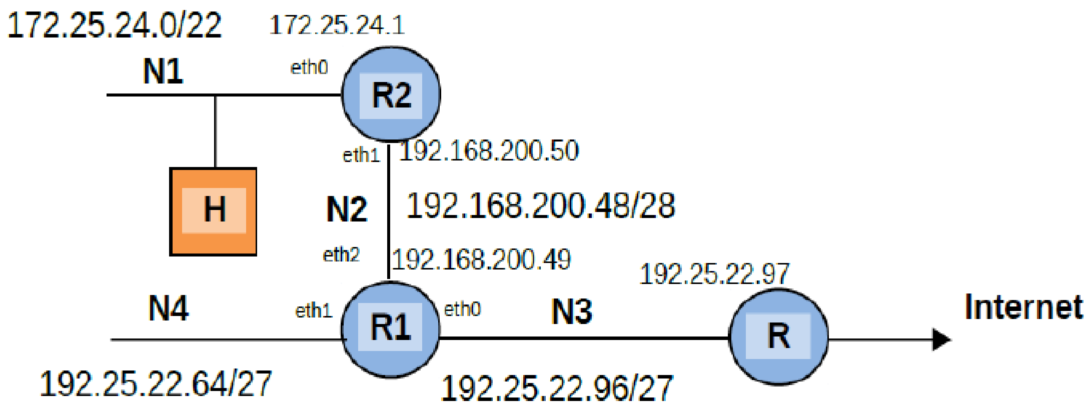
Commands on H2:

```
ip addr add 10.3.0.3/24 dev eth0
ip route add default via 10.3.0.254
```

Commands on H3:

```
ip addr add 10.0.0.254/24 dev eth0
ip addr add 10.3.0.254/24 dev eth1
sysctl -w net.ipv4.ip_forward=1
```

24. Given is the network structure shown with the routers R1, R2 and R as well as the host H.



Specify the routing tables of R1, R2 and H.

R1:

Destination	Mask	Gateway	Interface
N2	/28	0.0.0.0	eth2
N3	/27	0.0.0.0	eth0
N4	/27	0.0.0.0	eth1
N1	/22	R2: 192.168.200.50	eth2
127.0.0.0	/8	0.0.0.0	lo
0.0.0.0	/0	R: 192.25.22.97	eth0

R2:

Destination	Mask	Gateway	Interface
N2	/28	0.0.0.0	eth1
N1	/22	0.0.0.0	eth0
127.0.0.0	/8	0.0.0.0	lo
0.0.0.0	/0	R1: 192.168.200.49	eth1

H:

Destination	Mask	Gateway	Interface
N1	/22	0.0.0.0	eth0
127.0.0.0	/8	0.0.0.0	lo
0.0.0.0	/0	R2: 172.25.24.1	eth0

Solution: