UPPSALA
UNIVERSITET

Homework 3:
Routing and Addressing

Computer Networks I

Oskar Tegby

September 2022

1 Exercise 1 - Forwarding Table

(a) The mandatory fields in an IPv4 forwarding table are header values and output links since they dictate where the packets are sent according to the selected routing algorithm.

(b) Table 1 shows the forwarding table for the router. It is populated by inspecting which addresses the workstations in the subnets use to communicate with the router. The header values are the workstations and the output link is the router that they communicate through.

Header value	**Output link**
223.1.1.1	223.1.1.4
223.1.1.2	223.1.1.4
223.1.1.3	223.1.1.4
223.1.2.1	223.1.2.9
223.1.2.2	223.1.2.9
223.1.3.1	223.1.3.27
223.1.3.2	223.1.3.27

Table 1: The forwarding table for the router connecting the subnets.

(c) Table 2 shows the forwarding table for host **223.1.1.1**. It is populated by inspecting which addresses that the host can communicate to. That is, the workstations in the subnet, the subnet address to the router, as well as the addresses to the other subnets in the network.

Header value	**Output link**
223.1.1.2	223.1.1.1
223.1.1.3	223.1.1.1
223.1.1.4	223.1.1.1
223.1.2.9	223.1.1.1
223.1.3.27	223.1.1.1

Table 2: The forwarding table for the host **223.1.1.1**.

2 Exercise 2 - Longest Prefix Matching

The results of the computation of the the bitwise AND for the destination addresses and subnetwork addresses are found in Table 3.

Mask	Address	Result
255.255.**248**.0	200.23.**16**.0	x.**00010000**.00000000
255.255.248.0	200.23.24.0	x.00011000.00000000
255.255.**248**.0	200.23.**22**.161	x.**00010000**.10100000
255.255.**248**.0	200.23.**24**.170	x.**00011000**.10101000
255.255.**248**.0	200.23.**25**.11	x.**00011000**.00001000
255.255.255.0	200.23.16.0	x.00010000.00000000
255.255.255.0	200.23.24.0	x.00011000.00000000
255.255.255.0	200.23.22.161	x.00010110.10100001
255.255.**255**.0	200.23.**24**.170	x.**00011000**.10101010
255.255.**255**.0	200.23.**25**.11	x.**00011001**.00001011

Table 3: Bitwise AND for the destination and subnetwork addresses, with $x = 11001000.00010111$.

Destination address **200.23.22.161** (a) will be forwarded to subnetwork address **200.23.16.0** (with mask **255.255.248.0**, i.e. link interface 0) since **16** and **22** both mask **248** are **10000** in binary.

Furthermore, destination address **200.23.24.170** (b) will be forwarded to subnetwork address **200.23.24.0** (with mask **255.255.255.0**, i.e. link interface 1) since **25** and **24** both mask **248** are **11000** in binary, but if we change the mask to **255**, then **25** gives **11001** and **24** gives **11000**. That is, only **25** matches completely with **200.23.24.0** using mask **248**. Thus, we assign **200.23.24.170** (b) to **200.23.24.0** with mask **255.255.255.0**, and **200.23.25.11** (c) to **200.23.24.0** with mask **255.255.248.0**.

To summarize, we get the results found in Table 4.

Destination address	Link interface
a	0
b	1
c	2

Table 4: The destination addresses mapped to the link interfaces.

3 Exercise 3 - Subnetwork Addresses

The classification is given in Table 5. Here, we compute the results by first converting the addresses into binary representation, and then masking them both with the netmask, which is the number of one's starting from the most-significant bit and ending with zeroes afterwards. If the masked bits of the address match each other, and if the unmasked bits of the address are within the range of the network, then the address belongs to it.

To be more precise, we provide one example of such a computation. Namely, we go through the steps for case A, and leave the rest as mere results. Converting **10.0.1.0** and **10.0.1.23** into binary gives us

$$10.0.1.0 = 0000\ 1010.0000\ 0000.0000\ 0001.0000\ 0000$$
$$10.0.1.23 = 0000\ 1010.0000\ 0000.0000\ 0001.0001\ 0111$$

and the netmask is 1111 1111 1111 1111 1111 1111 0000 0000. The logical AND for **10.0.1.0** and the netmask **255.255.255.0** is

$$\begin{aligned} &10.0.1.0\ \&\ 255.255.255.0 = \\ &0000\ 1010.0000\ 0000.0000\ 0001.0000\ 0000\ \& \\ &1111\ 1111.1111\ 1111.1111\ 1111.0000\ 0000\ = \\ &0000\ 1010.0000\ 0000.0000\ 0001.0000\ 0000, \end{aligned}$$

and the logical AND for **10.0.1.23** and **255.255.255.0** is

$$\begin{aligned} &10.0.1.23 \ \& \ 255.255.255.0 = \\ &0000\ 1010.0000\ 0000.0000\ 0001.0001\ 0111\ \& \\ &1111\ 1111.1111\ 1111.1111\ 1111.0000\ 0000\ = \\ &0000\ 1010.0000\ 0000.0000\ 0001.0000\ 0000, \end{aligned}$$

where indeed match. Furthermore, the unmasked bits are clearly within the range of the network.

#	Subnetwork / Netmask	Address	Belongs
A	10.0.1.0/24	10.1.1.23	**True**
B	10.0.1.0/24	10.1.1.157	**True**
C	192.168.1.0/28	192.168.1.17	**False**
D	192.168.1.0/28	192.168.1.15	**False**
E	10.1.2.128/25	10.1.2.130	**True**
F	10.1.2.128/25	10.1.2.217	**True**
G	192.168.1.192/26	192.168.1.204	**True**
H	192.168.1.192/26	192.168.1.76	**False**

Table 5: Stating whether the addresses belong to the subnetworks or not.

4 Exercise 4 - Routing Table

The `traceroute` command shows that the packages from the Uppsala workstation first is reaching the Uppsala router (**10.3.0.1**) and then the Stockholm router (**10.10.2.1**), but repeatedly does so since the transmission fails. That is, it keeps trying to send again since it always fails.

The reason is that the gateway is wrong in the Stockholm router for forwarding with Gothenburg (**10.2.0.0**) as the destination. Namely, it says **10.10.2.2**, which is the Uppsala router, and not the intended Gothenburg router (**10.10.1.2**). Furthermore, the interface is wrong since it is `eth2`, but should be `eth1`, as that is the interface for communication between Stockholm and Gothenburg.