UPPSALA
UNIVERSITET

Homework 4: Scalability

Computer Networks I

Oskar Tegby

November 2022

1 Exercise 1 - Address Aggregation

a) If the clients request 500 hosts each, then we need to be able to encode that in binary. Thus, we need to find the number of bits that are required to encode that. This is given by $\lceil \log_2(500) \rceil \approx 9$ here. This means that the prefix length is 23 bits since those are the bits which we need in order to mask our addresses to leave 9 bits for the hosts. This gives us the address distribution

- Client 1: From 200.23.40.1/23 to 200.23.41.254/23,
- Client 2: From 200.23.42.1/23 to 200.23.43.254/23,
- Client 3: From 200.23.44.1/23 to 200.23.45.254/23,
- Client 4: From 200.23.46.1/23 to 200.23.47.254/23,

which allocates 500 hosts to each client starting with 200.23.40.1/23 and ending with 200.23.47.254/23. Consequentially, the address range of this ISP supports up to 4 clients.

b) The allocation in this case is the same for the first host, but, following the same logic as in the preceding task, we find that $\lceil \log_2(200) \rceil \approx 8$ bits are required to encode 200 hosts, giving a prefix length of 24 bits, and that $\lceil \log_2(100) \rceil \approx 7$ bits are required to encode 100 hosts, giving a prefix length of 25 bits. This gives us

- Client 2: From 200.23.42.1/24 to 200.23.42.254/24
- Client 3: From 200.23.43.1/24 to 200.23.43.254/24
- Client 4: From 200.23.44.1/24 to 200.23.44.254/24

for the clients with 200 hosts, and

- Client 5: From 200.23.45.1/25 to 200.23.45.126/25
- Client 6: From 200.23.45.129/25 to 200.23.45.254/25
- Client 7: From 200.23.46.1/25 to 200.23.46.126/25

for the clients with 100 hosts.

This far we have used $512 + 3 \cdot 256 + 3 \cdot 128 = 1664$ addresses. Thus, we have $2048 - 1664 = 384$ addresses remaining. These may be allocated in the following way

- Client 8: From 200.23.46.129/25 to 200.23.46.254/25,
- Client 9: From 200.23.47.1/25 to 200.23.47.126/25,
- Client 10: From 200.23.47.129/25 to 200.23.47.254/25,

which means that the ISP can provide three more clients with 100 hosts.

2 Exercise 2 - Subnets and Addressing

a) There are two subnets in the figure, as is seen by the router separating the two sets $\{A, B\}$ and $\{C, D, E, F\}$ into subnets.

b) The addresses are distributed in the following ways for the hosts

- A - IP: 192.168.40.1, MAC: 00:1A:2B:3C:4D:5E,
- B - IP: 192.168.40.2, MAC: 10:24:C3:4A:5E:5C,
- C - IP: 192.168.39.1, MAC: 00:10:2A:3F:4D:12,
- D - IP: 192.168.39.2, MAC: 10:12:10:2A:4B:75,
- E - IP: 192.168.39.4, MAC: 11:1A:0B:C3:5F:00,
- F - IP: 192.168.39.5, MAC: 90:94:8A:7B:6C:5D,

and in the following way for the router

- R1L - IP 192.168.40.10, MAC: 00:00:F2:3B:45:12,
- R1R - IP 192.168.39.10, MAC: 00:00:F3:2B:44:10,

where L denotes the left subnet ($\{A, B\}$) and R denotes the right one ($\{C, D, E, F\}$).

c) The purpose of the Address Resolution Protocol (ARP) is to translate between network-layer addresses (such as IP addresses) and link-layer addresses (that is, MAC addresses).

d) In order for host E (192.168.39.4) to send an IP datagram to host B (192.168.40.2) it first of all has to pass it to its adapter. The adapter will then find the MAC address of the destination within the local subnet using the ARP. When it has done that, it creates a frame for the datagram which it sends to the subnet. The MAC address for the frame is that of the adapter for the right subnet (R1R) of the router, which is 00:00:F3:2B:44:10 in this case. The router adapter then detects that the link-layer frame is addressed to it, and passes the frame to the network-layer of the router. The router (R1) then determines the right interface to use for forwarding the datagram using its routing table, which will tell it that the datagram has to be forwarded via the interface 192.168.40.10 in our situation. The interface then passes the datagram to its adapter, which encapsulates the datagram into a new frame that it sends to the subnet. In order to do so, the router again obtains the MAC address to the destination using the ARP, which is 10:24:C3:4A:5E:5C for host B here. That finalizes the procedure.

e) The roles of the sender and the receiver in the preceding scenario are now swapped. That is, it is now host B (192.168.40.2) who is sending to host E (192.168.39.4). In order to do so here, B assigns the source port number 3345 and sends the datagram over the Local Area Network (LAN). The Network Address Translation (NAT) router then receives the datagram, generates the new source port number 5001 for the datagram, replaces the source IP address with its WAN side IP address 192.168.39.10, and replaces the original source port number, 3345, with the new source port number, 5001.

When generating a new source port number, the NAT router can select any source port number that is not currently in the NAT translation table. Moreover, the NAT in the router also adds an entry to its translation table.

Then, host E responds with a datagram whose destination address is the IP address of the NAT router, and whose destination port number is 5001. When the datagram arrives at the NAT router, the router indices the translation table using the destination IP address and the destination port number to obtain the right IP address (192.168.40.2) and destination port number (3345) for the browser in the home network. The router finally rewrites the destination address and port number of the datagram, and forwards the datagram to host B.

f) The problem is that the host in the private network behind the NAT is unable to accept any TCP connections. The situation occurs because the host that is connected to the Internet initiates a TCP connection to the host on the private network which is behind the NAT.

We can solve this by allowing the Internet host to connect to the private host through an intermediate host which is not behind a NAT. The Internet host can then effectively be requested to establish a TCP connection with the private host by using the intermediate host to relay the request, and then communicate thorough it. That is, we end up with the Internet host and the intermediate host communicating back and forth, and the private host communicating with the intermediate host, which simply relays the request between the private host and the Internet host back and forth.