ETH zürich

Networked Systems
ETH Zürich — seit 2015

Communication Networks

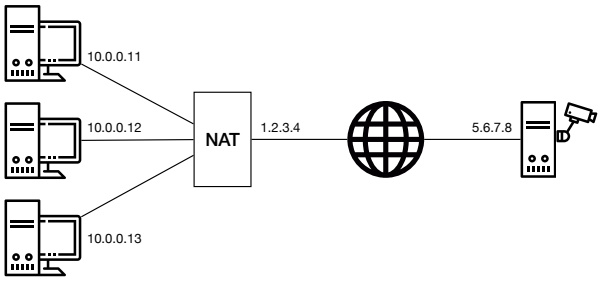
Prof. Laurent Vanbever

Solution: Exercise 5 – Internet Protocol (IP) & Forwarding

Internet Protocol (IP)

5.1 NAT (Exam Question 2018)

Consider the network topology below. Alice has multiple PCs at home (10.0.0.11–13) which share a single public IP address (1.2.3.4) via a NAT device. Further, she operates a surveillance camera server which is directly connected to the Internet with a public IP address (5.6.7.8). The camera transmits the live video signal as a stream of UDP packets with source port 1000 to a configurable destination IP address and port.



Alice operates three PCs and one camera server

a) Alice wants to receive the live video stream on one of her PCs and thus configures the camera to send the video signal to IP 10.0.0.11 and port 1234. However, she does not receive it on her PC. Why? Where is this traffic sent to?

Solution: All IP addresses in the 10.0.0.0/8 prefix are private and not routed in the Internet. As 10.0.0.11 is one of these internal IPs, the camera has no route to this address. Consequently, that traffic is dropped.

b) Now Alice configures the camera to send the video signal to IP 1.2.3.4 and port 1234. But she still does not receive it on any of her PCs. Why? Where is this traffic sent to?

Solution: The IP address 1.2.3.4 is a globally routed address and therefore, the traffic arrives at the NAT box. However, as there is no corresponding address translation rule in the NAT for that specific destination port, the NAT does not know how to rewrite the packet and where to forward the traffic to. The traffic is dropped at the NAT box.

c) What can Alice do such that she receives the video signal at her PC with IP address 10.0.0.11 and at port 1234 assuming that she *cannot* modify the configuration of the NAT? Describe step-by-step what she can do if she has the following possibilities:

- send one single UDP packet with arbitrary source and destination addresses and ports from each of her PCs;
- observe the received packets at each of her PCs and the camera server;
- specify the destination IP address and port for the video signal.

Solution: First, you want to "open a hole" in the NAT box for the video stream to enter your network. To do this, you send a packet from an internal host, for example 10.0.0.11:1234, to the camera 5.6.7.8:1000. This leads the NAT box to install an address translation rule.

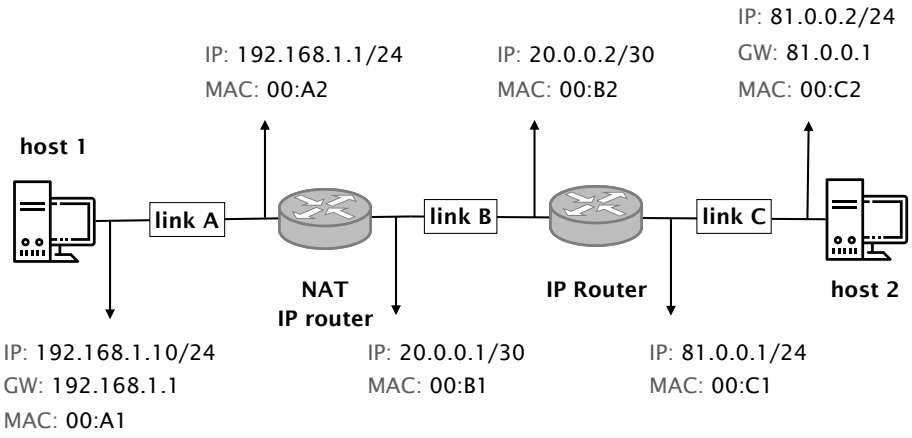
Now, you have to configure the camera with the correct destination IP address and port. The destination IP address is clear: it is the one of the NAT box (1.2.3.4). The port, however, you do not know yet.

Therefore, you start observing the packets arriving at the camera while sending packets from the interal host to the camera, from 10.0.0.11:1234 to 5.6.7.8:1000. At the camera, you will see to what port the NAT changed the source port of the packet.

Finally, configure the camera to send the video stream to the IP address of the NAT box and set the destination port to the port observed previously.

5.2 Changing addresses (Exam Question 2019)

Consider the network depicted in the Figure below which is composed of two hosts along with two routers, one of which acts as Network Address Translator (NAT). Host 1 is located in a private subnet (192.168.1.0/24) and uses 192.168.1.1 as gateway, while host 2 is located in a public subnet (81.0.0.0/24) and uses 81.0.0.1 as gateway. The Figure below also depicts the MAC address of each of the 6 interfaces connected at either end of the three links. The NAT/router performs address translation between the private and the public subnets, translating traffic originating from private IPs to its public one (here, 20.0.0.1), and vice-versa.



A network topology relying on Network Address Translation.

a) Consider that host 1 tries to open a TCP connection with host 2 on port 80 using 1337 as (random) source port. Write down a possible sequence of packet headers observed at each link for the first two packets (i.e., the SYN sent by host 1, and the SYN/ACK sent by host 2). Fill in the table below to answer. Assume that hosts and routers have the required MAC addresses in their ARP table.

Solution:

	src MAC	dst MAC	src IP	dst IP	src TCP port	dst TCP port
link A	00:A1	00:A2	192.168.1.10	81.0.0.2	1337	80
link B	00:B1	00:B2	20.0.0.1	81.0.0.2	rand	80
link C	00:C1	00:C2	20.0.0.1	81.0.0.2	rand	80
link C	00:C2	00:C1	81.0.0.2	20.0.0.1	80	rand
link B	00:B2	00:B1	81.0.0.2	20.0.0.1	80	rand
link A	00:A2	00:A1	81.0.0.2	192.168.1.10	80	1337

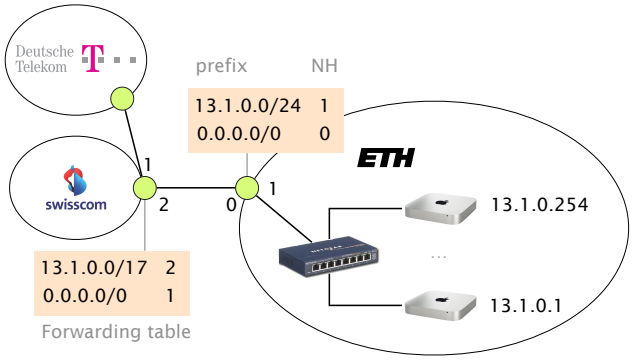
b) Could host 2 initiate a TCP connection to host 1? Briefly explain why/why not.

Solution: That is not possible as host 1 is behind a NAT. Packets that reach the public IP of the NAT will not be forwarded to host 1 as there is no corresponding NAT rule available.

Forwarding

5.3 The Art of Defaulting Properly (Exam Style Question)

Consider this simple network configuration between ETH and Swisscom. Assume that ETH owns a large IP prefix 13.1.0.0/17, but only uses 13.1.0.0/24 to address its internal hosts. For simplicity, we assume that ETH and Swisscom operators configure their forwarding table statically and rely on the use of a default route (0.0.0.0/0).



Where are my IP packets going?

a) How many IP addressable addresses does ETH "own" in total?

Solution: $2^{(32-17)} - 2$

b) Give the first and last IP address that ETH can use for addressing a host.

Solution: 13.1.0.1 and 13.1.127.254

c) Suppose Swisscom receives a packet for 13.1.0.66 from Deutsche Telekom. What is the path taken by this IP packet?

Solution: Swisscom/1 → Swisscom/2 → ETH/0 → ETH/1

d) Suppose Swisscom receives a packet for 13.1.66.1 from Deutsche Telekom. What is the path taken by this IP packet?

Solution: Swisscom/1 → Swisscom/2 → ETH/0 → Swisscom/2 → ETH/0 → ...

e) What eventually happens to the packet for 13.1.66.1? As an attacker observing this, could you use this observation to congest the ETH-Swisscom link more easily? Explain why (or why not).

Solution: It will eventually be dropped as the TTL reaches 0. Permanent forwarding loops can be used to perform a Denial of Service (DoS) attack with few resources. Here an attacker can simply start sending fake traffic to 13.1.66.1 which will start "pilling up" on the Swisscom ↔ ETH link. The actual damages will depend on: *i)* the rate at which the attacker can send; *ii)* the TTL of the packets; as well as *iii)* the actual capacity of the link. Observe that the induced congestion negatively impact *all* traffic, including traffic destined to 13.1.0.0/24.

5.4 Summer Pruning (Exam Question **2018**)

Consider an IP router with a forwarding table composed of the 9 entries depicted on the left. Write down (on the right) an equivalent forwarding table by combining entries together into shorter ones such that the resulting table has the least number of entries. Your reduced forwarding table should be such that the forwarding decision made by the router for any IP packet is equivalent to the initial one.

Solution:

prefix	next-hop
82.130.32.0/20	1
82.130.64.0/20	1
82.130.80.0/20	2
82.130.96.0/20	1
82.130.112.0/21	1
82.130.120.0/21	1
82.130.122.0/24	1
82.130.123.0/24	1
82.130.124.0/24	2

prefix	next-hop
82.130.32.0/20	1
82.130.64.0/18	1
82.130.80.0/20	2
82.130.124.0/24	2

Answer to the same question as above considering the forwarding table below instead (left) in which an extra default route is defined.

Solution:

prefix	next-hop
0.0.0.0/0	1
82.130.32.0/20	1
82.130.64.0/20	1
82.130.80.0/20	2
82.130.96.0/20	1
82.130.112.0/21	1
82.130.120.0/21	1
82.130.122.0/24	1
82.130.123.0/24	1
82.130.124.0/24	2

prefix	next-hop
0.0.0.0/0	1
82.130.80.0/20	2
82.130.124.0/24	2