Chair of Distributed Systems and Security
School of Computation, Information and Technology
Technical University of Munich

Computer Networking and IT Security (INHN0012)

Tutorial 10

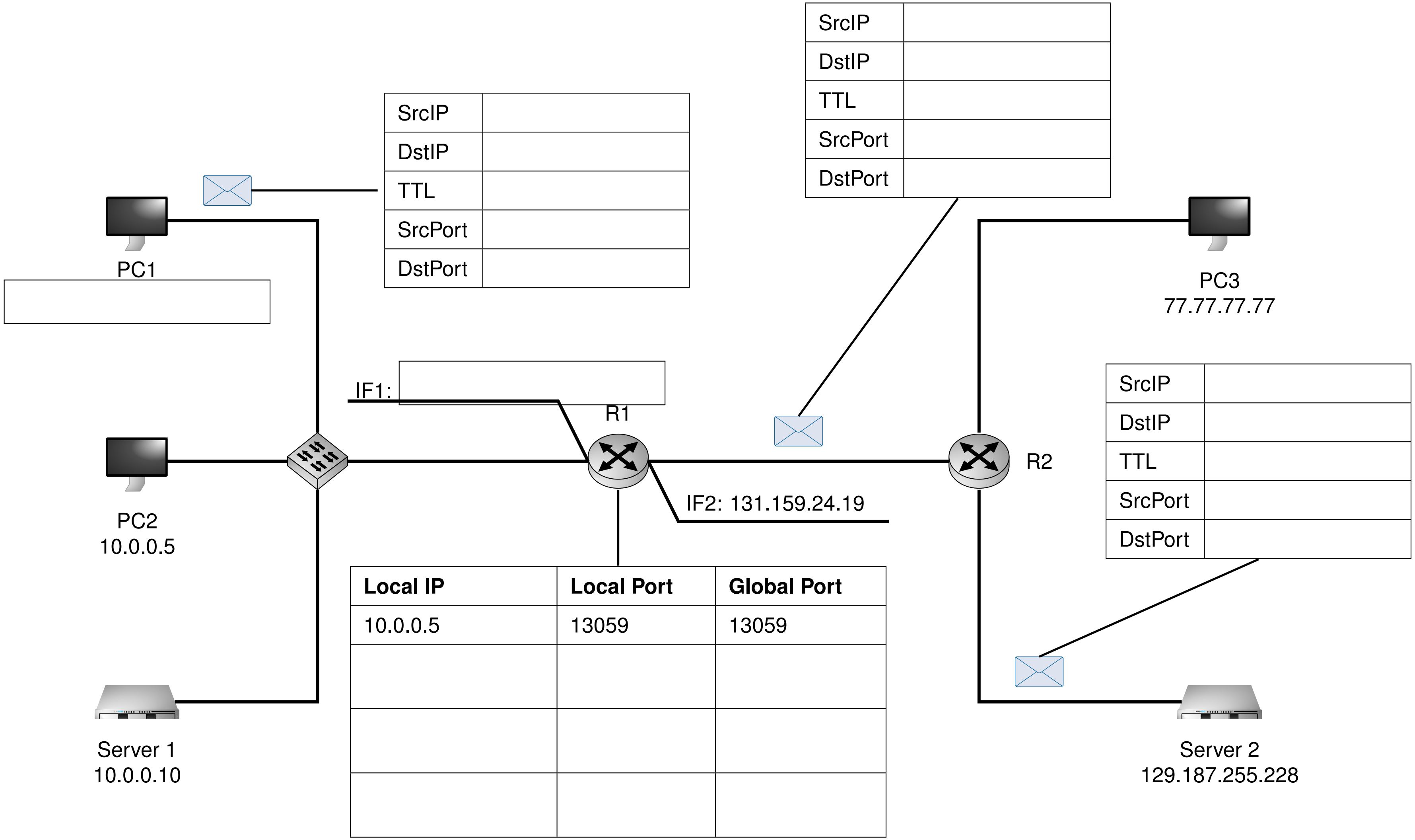
Problem 1 Network Address Translation

This task will look at the forwarding of IP packets (IPv4) when using a NAT-enabled router. For the mapping between public and private IP addresses, a NAT-enabled router has a mapping table that stores the relationship between the local and the global port. Many NAT-enabled devices also store additional information such as the remote IP address or the router's own global IP address (e.g., if the router has more than one global IP). We will refrain from doing this here.
Figure 1.1 shows the network topology. Router R1 has NAT enabled, using a private IP address on IF1 and a public IP address on IF2. Router R2 does not use NAT. PC2 had already communicated with server 2, which created the entry in R1's NAT table (see the 1.1 figure). Where you have the freedom, choose sensible values for the IP addresses and port numbers.

a)* Give PC1 and interface 1 of R1 a suitable IP address. The subnet is 10.0.0.0/24.

b)* PC1 now establishes an HTTP connection to server 2. Specify the source IP, destination IP, source port, destination port, and TTL fields of the IP or TCP header for the packets in the three highlighted locations in Figure 1.1. Also, specify newly created entries in the NAT table of R1.

c) Server 2 now answers PC1. In Figure 1.2, specify the header fields at the three named locations, as well as newly created entries in the NAT table of R1, analogous to the previous subtask.



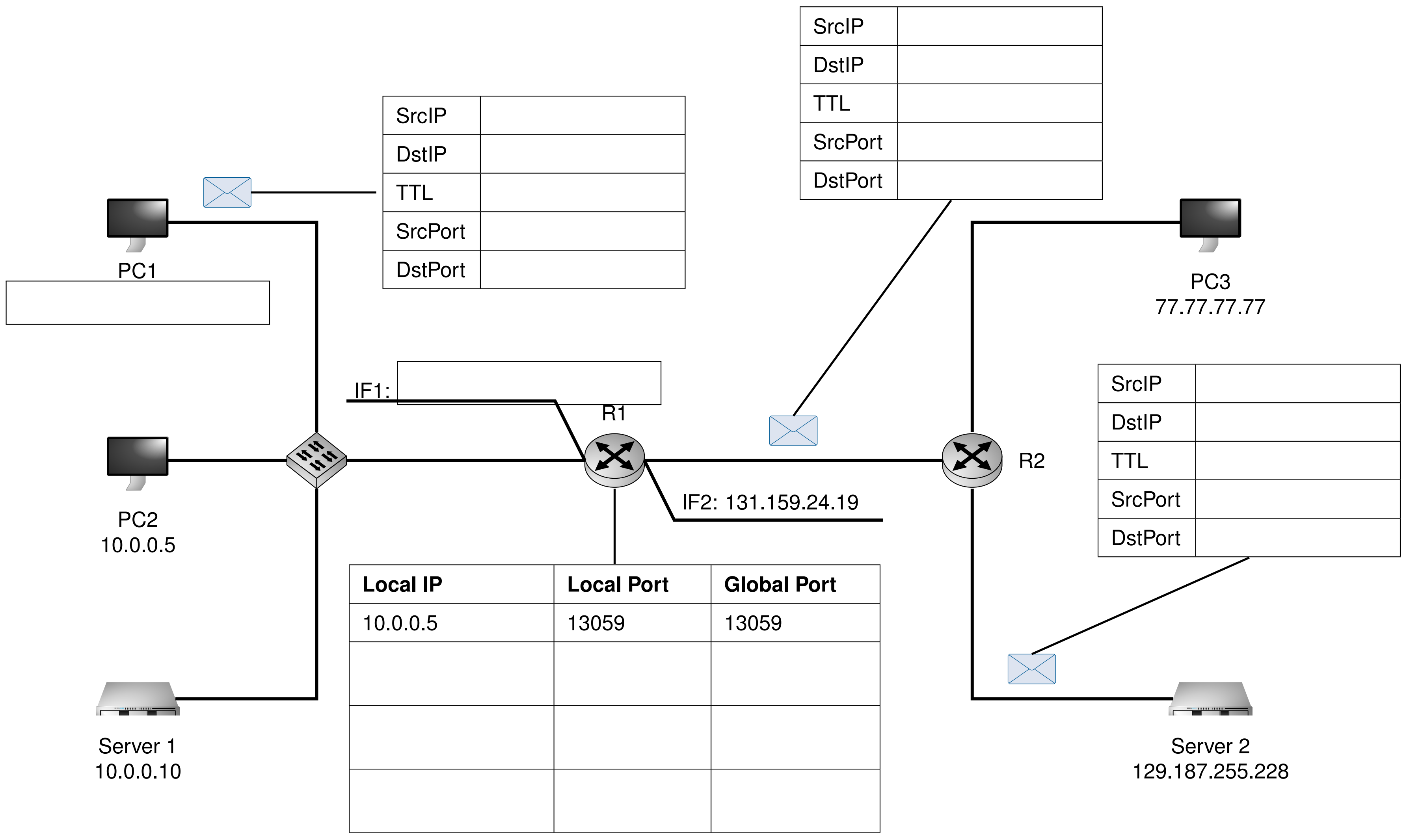
SrcIP	
DstIP	
TTL	
SrcPort	
DstPort	

SrcIP	
DstIP	
TTL	
SrcPort	
DstPort	

SrcIP	
DstIP	
TTL	
SrcPort	
DstPort	

Local IP	**Local Port**	**Global Port**
10.0.0.5	13059	13059

Figure 1.1: Solution sheet for problem 1a)/b)



SrcIP	
DstIP	
TTL	
SrcPort	
DstPort	

SrcIP	
DstIP	
TTL	
SrcPort	
DstPort	

SrcIP	
DstIP	
TTL	
SrcPort	
DstPort	

Local IP	**Local Port**	**Global Port**
10.0.0.5	13059	13059

Figure 1.2: Solution sheet for problem 1c)

d)* Server 1 now also establishes a TCP connection to server 2 on port 80. In doing so, it randomly chooses the sender port 13059. Describe the problem that occurs on the NAT and how it is solved.

e)* R1 receives a packet from PC3 addressed to `131.159.24.19:13059`. What will R1 do with this packet? What problems may arise from it?

f) Does a problem arise for PC2 when it receives a „random“ packet with TCP payload on a port with an existing connection?

g)* What other distinguishing criteria could be used by a NAT router?

h)* What problem arises when PC1 sends an echo request to server 2?

i) Describe a possible solution for the problem which arose in the previous subproblem.

j) What problem arises if a NAT router receives ICMP TTL-exceeded messages and wants to forward it to the intended receiver (sender who caused the problem)? How can this problem be worked around?

k)* Now PC3 wants to establish a HTTP connection with Server 1. Can this happen under the given circumstances? (Explain!)

l) How can this problem be avoided while mantaining a NAT?

Problem 2 Re-wired shark

Given is the hexdump shown in Figure 2.1 in network byte order of an Ethernet frame, which is to be analyzed in the following.
Note: To solve this task, you will need information from the cheatsheet.
Important: All following subproblems require justification through reasoning or through marking the corresponding header field or fields clearly in the hexdump. In the latter case, note the the subproblems character (e.g. *a)*) next to the marking.

```
0x0000  d0 e1 40 97 ec ea 00 0d   2e 00 40 01 08 00 45 00
0x0010  00 38 00 00 00 00 f1 01   8c 2b 3e 9a 59 2e ac 13
0x0020  f9 bd 0b 00 bf 50 00 00   00 00 45 00 00 3c 15 b2
0x0030  00 00 01 11 ea 81 ac 13   f9 bd 81 bb 91 f1 d4 0f
0x0040  82 be 00 28 de b8
```

Figure 2.1: Hexdump of an Ethernet frame in network byte order

a)* Mark the beginning and end of the Ethernet header in Figure 2.1.

b) Which protocol is used at layer 3.

c) Determine the length of the layer 3 header and mark its end in Figure 2.1.

d) State – if contained in the packet – the TTL or HopCount in decimal **and** hexadecimal notation.

e) Justify to which protocol the L3 SDU belongs.

Given is the SDU of layer 3 shown in Figure 2.2 **of another packet**. It is known that this is ICMPv4.

```
0x0000  0b 00 bf 50 00 00 00 00   45 00 00 3c 15 c6 00 00
0x0010  01 11 ea 6d ac 13 f9 bd   81 bb 91 f1 ec 38 82 c4
0x0020  00 28 c6 89
```

Figure 2.2: ICMP message including ICMP header in network byte order

f)* Determine the type and code of the ICMP message.

g) What causes such a message?

h)* Mark the end of the ICMP header in Figure 2.2.

i) Explain what the payload of such a message fundamentally contains.

j) Was IPv4 or IPv6 used to transmit the original message that triggered this error?

k) What is the length of the original IP packet?

l) Mark the end of the original messages IP header in Figure 2.2.

m) What layer 4 protocol was used in the original message?