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

Computer Networking and IT Security (INHN0012)

Tutorial 5

Problem 1 Cyclic Redundancy Check (CRC)

The message `10101100` is secured using CRC as introduced in the lecture. The reduction polynomial $r(x) = x^3 + 1$ is given.

a)* What is the checksum length?

b) Determine the checksum for the given message.

c)* Specify the transmitted bit sequence.

The error pattern `00100000000` now occurs during the transfer.

d)* What is the received bit sequence?

e) Show that the transmission error is detected.

f)* Specify an error pattern that cannot be detected.

g) CRC was explicitly introduced in the lecture as an error-detecting, but not as an error-correcting code. Show that by means of CRC even 1 bit errors are not correctable in the concrete example of this task.

Problem 2 Switching and Forwarding

Given is the example network shown in Figure 2.1. In this problem, we will analyze the network with respect to the collision domains and the behavior of the network devices hub, switch and access point. The notebooks NB1 and NB2 are associated with the access point AP.

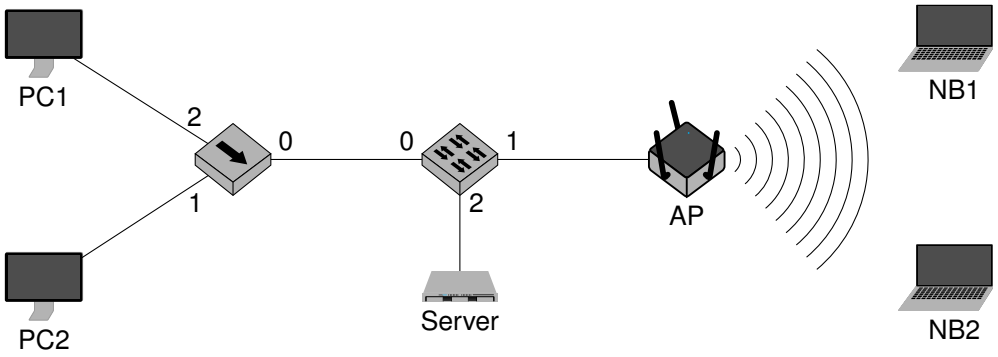


Figure 2.1: Network topology

a)* Draw the borders of all collision domains in the network in Figure 2.1.

b)* The network only consists of one broadcast domain. Why is that the case? Propose a change to the network that results in the presence multiple broadcast domains.

In the following subproblems we consider a message sent by PC1, destined for the server. The switching table of the central switch is given in Table 2.1. As a result of a previous transmission between PC2 and NB2, it already contains some entries.

MAC	Port	Reasoning
PC2.MAC	0	Previous connection
NB2.MAC	1	Previous connection

Table 2.1: Switching table of the switch of Figure 2.1.

c)* What is the state of the switching table, after the switch has forwarded the frame?
Update the table accordingly.

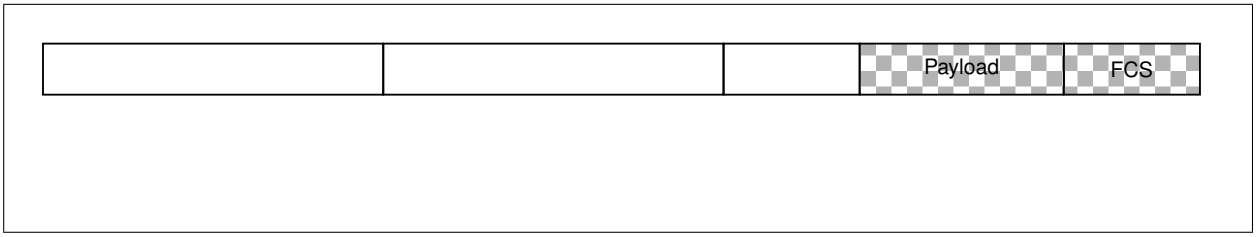
d) The server replies to the request. What is the state of the switching table after the reply reached PC1?
Update the table accordingly.

e) Which nodes will receive the reply sent by the server? What happens if a node that is not the intended destination receives the frame?

Now, we take a look at the connection between PC2 and NB2. NB2 wants to send some new data to PC2 and builds a frame on layer 2.

f)* Which addresses of which nodes must NB2 write into the header of the frame? What roles do these addresses have?

g) Complete the header of the Ethernet frame, which is created by the access point to forward the data in the wired network. If a fields value is not specified in the instructions, choose a sensible value.



h) What would happen if the server was compromised and would send a spoofed frame, where the source address is set to the one of PC1? Update the switching table and explain the effect on the network.