Solutions network lecture 3 (lecture 8)

R3

3. A UDP socket is fully identified by the destination IP address and the destination port. A TCP socket, instead, is fully identified by the source IP address, the source port, the destination address, and the destination port. This happens as TCP establishes a bi-directional full-duplex session between the sender and the receiver.

This applies when TCP has established the connection (thus needing to perform demultiplexing). Before, less information may be attached to a socket (eg "welcome socket")

R7

7. Yes, both segments will be directed to the same socket. For each received segment, at the socket interface, the operating system will provide the process with the IP addresses to determine the origins of the individual segments.

R8

8. For each persistent connection, the Web server creates a separate "connection socket". Each connection socket is identified with a four-tuple: (source IP address, source port number, destination IP address, destination port number). When host C receives and IP datagram, it examines these four fields in the datagram/segment to determine to which socket it should pass the payload of the TCP segment. Thus, the requests from A and B pass through different sockets. The identifier for both of these sockets has 80 for the destination port; however, the identifiers for these sockets have different values for source IP addresses. Unlike UDP, when the transport layer passes a TCP segment's payload to the application process, it does not specify the source IP address, as this is implicitly specified by the socket identifier.

R12

12.

a) The packet loss caused a time out after which all the five packets were retransmitted.

b) Loss of an ACK didn't trigger any retransmission as Go-Back-N uses cumulative acknowledgements.

c) The sender was unable to send sixth packet as the send window size is fixed to 5.

R13

13.

a) When the packet was lost, the received four packets were buffered the receiver. After the timeout, sender retransmitted the lost packet and receiver delivered the buffered packets to application in correct order.

b) Duplicate ACK was sent by the receiver for the lost ACK.

c) The sender was unable to send sixth packet as the send window size is fixed to 5

When a packet was lost, GO-Back-N retransmitted all the packets whereas Selective Repeat retransmitted the lost packet only. In case of lost acknowledgement, selective repeat sent a duplicate ACK and as GO-Back-N used cumulative acknowledgment, so that duplicate ACK was unnecessary.

13b) Since the sender does not get an ACKnowledgement back it sends packet0 again after the timeout. The receiver recognizes that packet0 is a duplicate it just sends back a duplicate ACKnowledgement.

Problems:

P9

Problem 9

Suppose the protocol has been in operation for some time. The sender is in state "Wait for call from above" (top left hand corner) and the receiver is in state "Wait for 0 from below". The scenarios for corrupted data and corrupted ACK are shown in Figure 1.

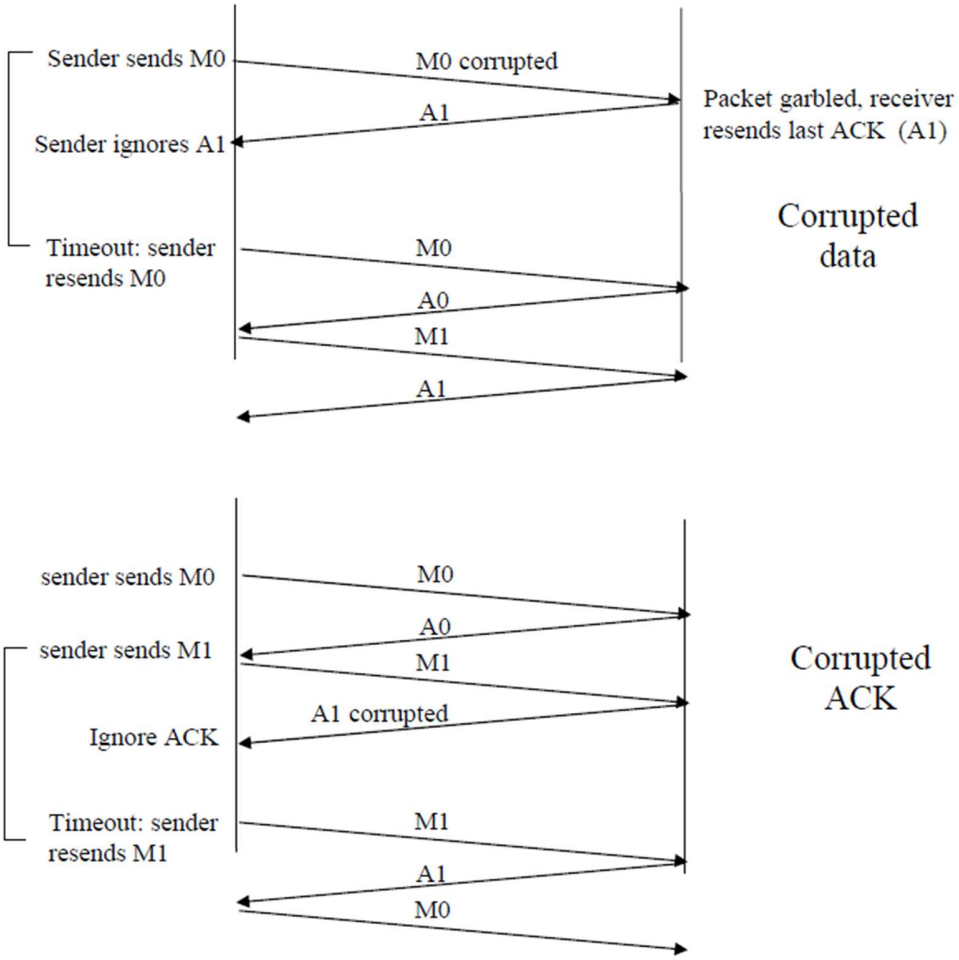
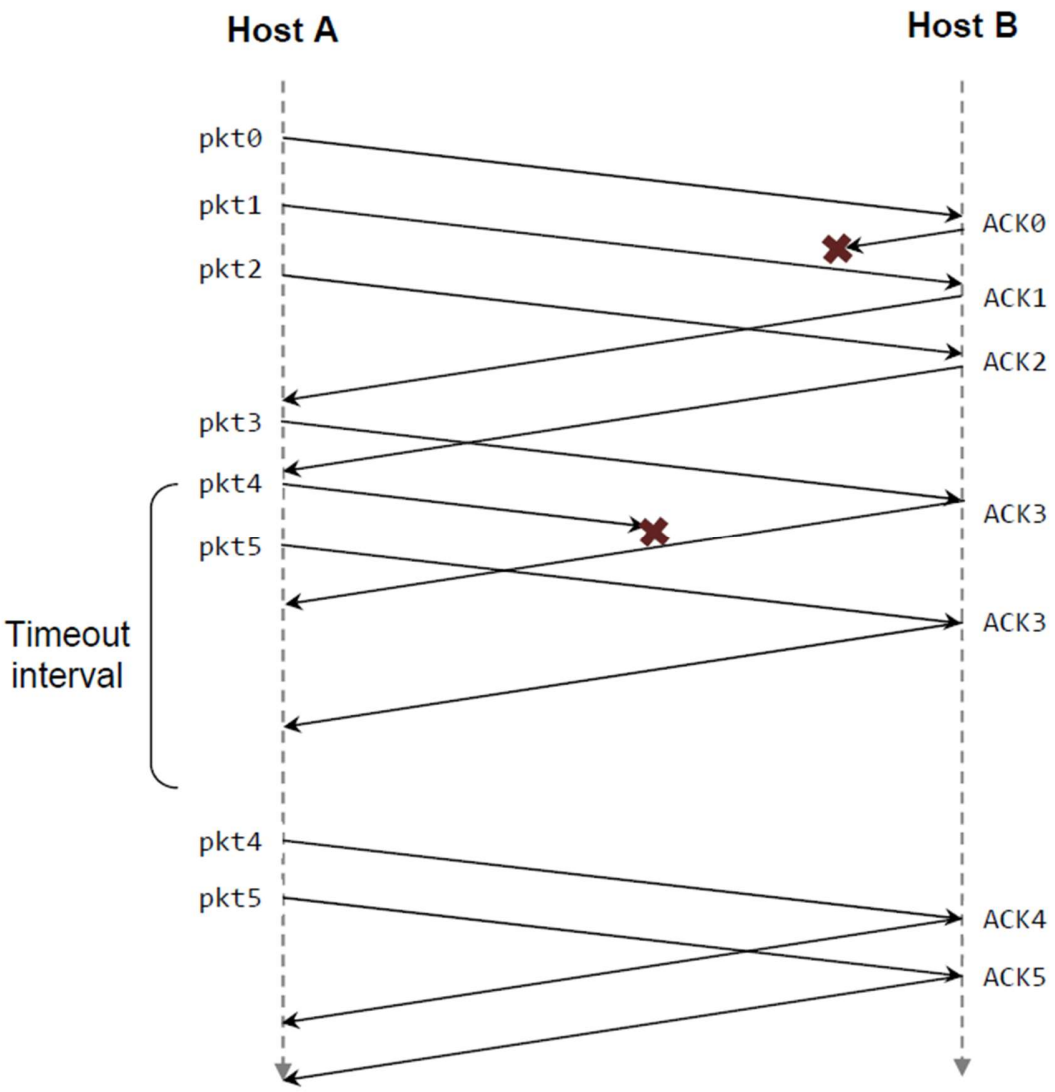


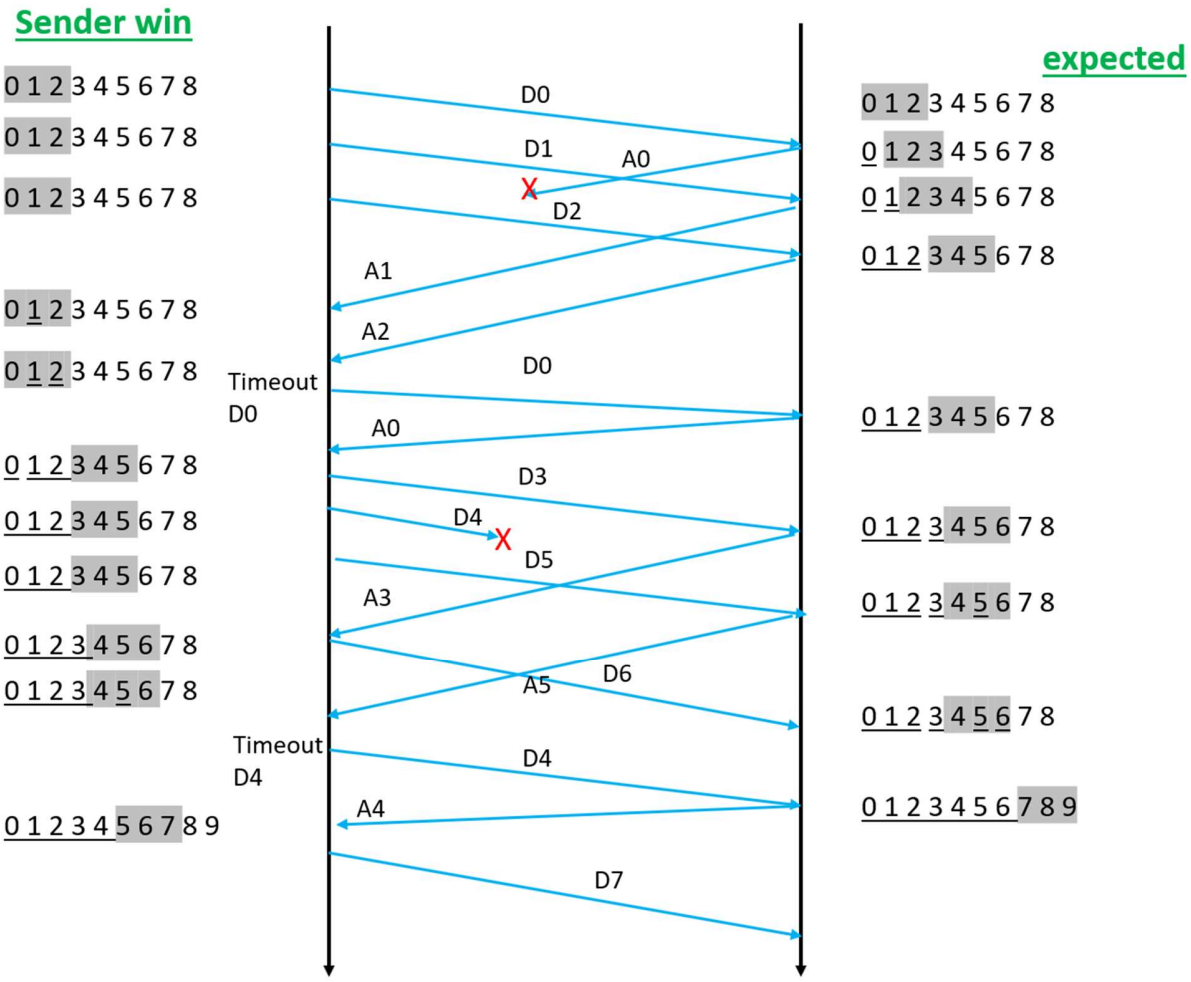
Figure 1: rdt 3.0 scenarios: corrupted data, corrupted ACK

P19

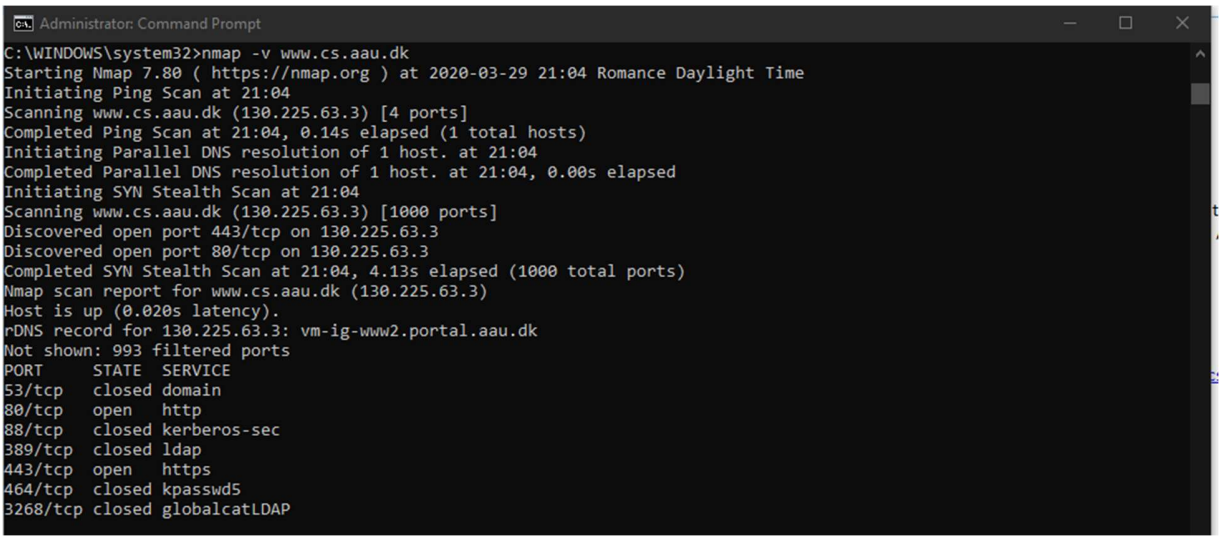
Problem 19

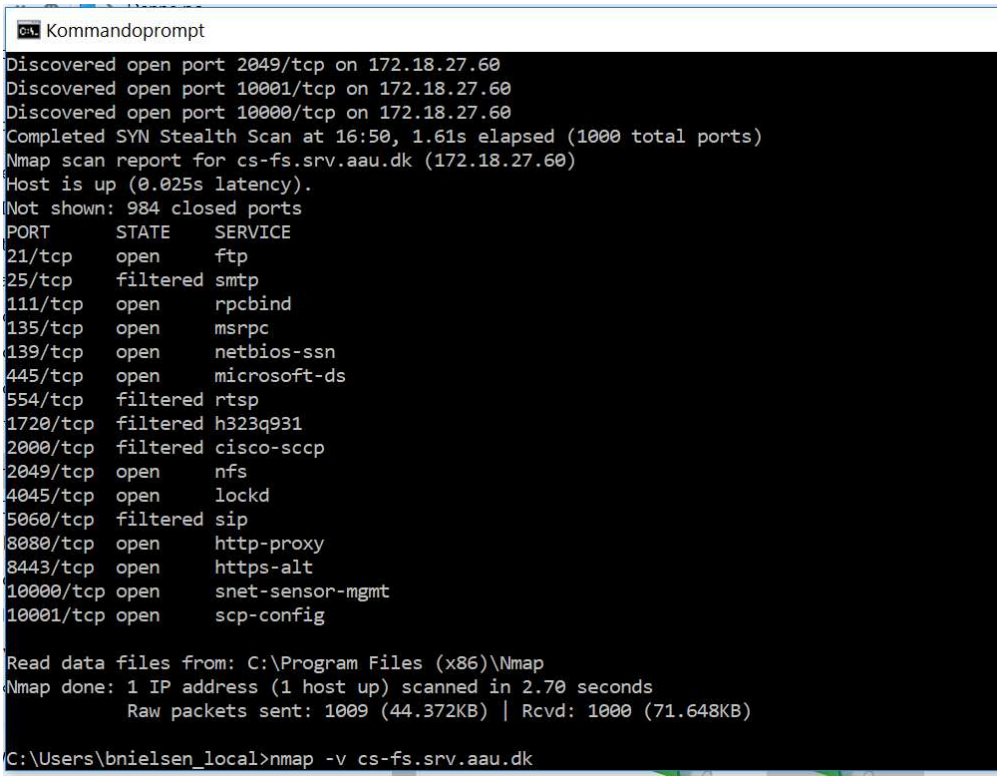


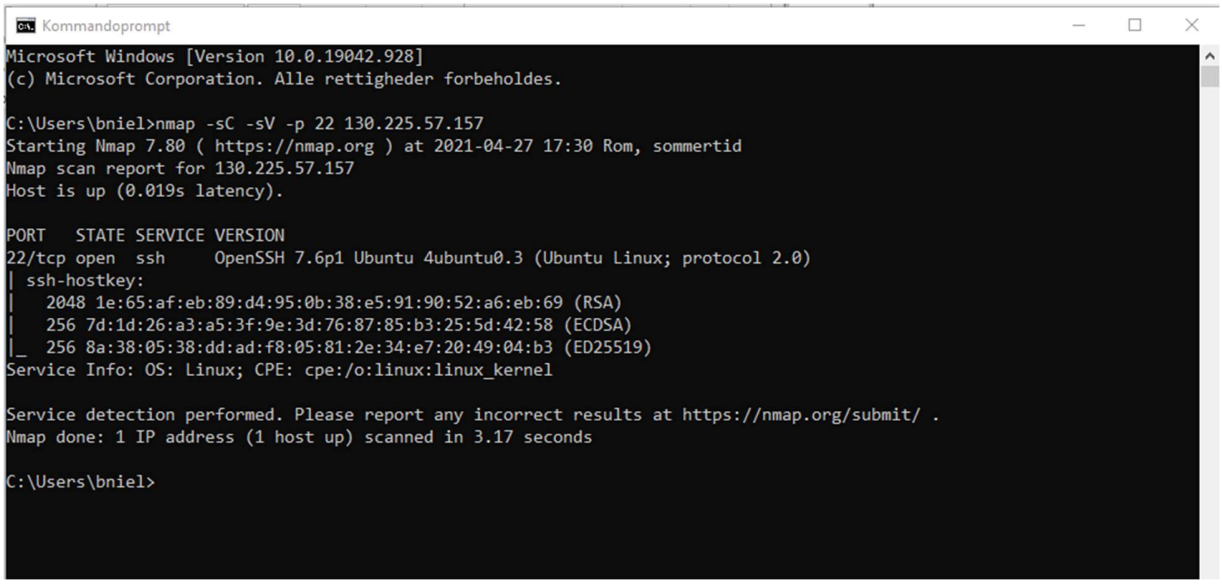
Repeat p19 for using selective repeat.


Sender win
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8 9
Timeout
D0
Timeout
D4
D0
D1
A0
D2
A1
A2
D0
A0
D3
D4
D5
A3
A5
D6
D4
A4
D7
expected
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8
0 1 2 3 4 5 6 7 8 9

Practice


Administrator: Command Prompt
C:\WINDOWS\system32>nmap -v www.cs.aau.dk
Starting Nmap 7.80 (https://nmap.org) at 2020-03-29 21:04 Romance Daylight Time
Initiating Ping Scan at 21:04
Scanning www.cs.aau.dk (130.225.63.3) [4 ports]
Completed Ping Scan at 21:04, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:04
Completed Parallel DNS resolution of 1 host. at 21:04, 0.00s elapsed
Initiating SYN Stealth Scan at 21:04
Scanning www.cs.aau.dk (130.225.63.3) [1000 ports]
Discovered open port 443/tcp on 130.225.63.3
Discovered open port 80/tcp on 130.225.63.3
Completed SYN Stealth Scan at 21:04, 4.13s elapsed (1000 total ports)
Nmap scan report for www.cs.aau.dk (130.225.63.3)
Host is up (0.020s latency).
rDNS record for 130.225.63.3: vm-ig-www2.portal.aau.dk
Not shown: 993 filtered ports
PORT STATE SERVICE
53/tcp closed domain
80/tcp open http
88/tcp closed kerberos-sec
389/tcp closed ldap
443/tcp open https
464/tcp closed kpasswd5
3268/tcp closed globalcatLDAP


Kommandoprompt
Discovered open port 2049/tcp on 172.18.27.60
Discovered open port 10001/tcp on 172.18.27.60
Discovered open port 10000/tcp on 172.18.27.60
Completed SYN Stealth Scan at 16:50, 1.61s elapsed (1000 total ports)
Nmap scan report for cs-fs.srv.aau.dk (172.18.27.60)
Host is up (0.025s latency).
Not shown: 984 closed ports
PORT STATE SERVICE
21/tcp open ftp
25/tcp filtered smtp
111/tcp open rpcbind
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
554/tcp filtered rtsp
1720/tcp filtered h323q931
2000/tcp filtered cisco-sccp
2049/tcp open nfs
4045/tcp open lockd
5060/tcp filtered sip
8080/tcp open http-proxy
8443/tcp open https-alt
10000/tcp open snet-sensor-mgmt
10001/tcp open scp-config
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 2.70 seconds
Raw packets sent: 1009 (44.372KB) | Rcvd: 1000 (71.648KB)
C:\Users\bnielsen_local>nmap -v cs-fs.srv.aau.dk


Kommandoprompt
Microsoft Windows [Version 10.0.19042.928]
(c) Microsoft Corporation. Alle rettigheder forbeholdes.
C:\Users\bniel>nmap -sC -sV -p 22 130.225.57.157
Starting Nmap 7.80 (https://nmap.org) at 2021-04-27 17:30 Rom, sommertid
Nmap scan report for 130.225.57.157
Host is up (0.019s latency).
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 1e:65:af:eb:89:d4:95:0b:38:e5:91:90:52:a6:eb:69 (RSA)
| 256 7d:1d:26:a3:a5:3f:9e:3d:76:87:85:b3:25:5d:42:58 (ECDSA)
|_ 256 8a:38:05:38:dd:ad:f8:05:81:2e:34:e7:20:49:04:b3 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.17 seconds
C:\Users\bniel>