IK1203 Networks and Communication

Recitation 3 – Solutions

1.

a) P2, 130.237.160.32
b) P2, 130.237.160.33
c) P1, 130.237.160.132
d) P1, 130.237.160.131
e) P2, 130.237.160.32

2.

a)

IP address	MAC address
10.0.1.1	MAC_A
10.0.1.2	MAC_B
10.0.1.3	MAC_C
10.0.1.4	MAC_{1-1}

b)

Destination	Network mask	Gateway	Interface (port number)
10.0.1.0	255.255.255.0	–	P_1
10.0.2.0	255.255.255.0	–	P_2
0.0.0.0	0.0.0.0	10.0.2.5	P_3

c) Packet received by R_1: IP source 10.0.1.1, IP destination 10.0.2.3, MAC source MAC_A, MAC destination MAC_{1-1}.
Packet sent by R_1: IP source 10.0.1.1, IP destination 10.0.2.3, MAC source MAC_{1-2}, MAC destination MAC_E.

d) All computers will be on the same subnet, so the addresses must be reconfigured. For example, we could use prefix 10.0.0.0/22. Furthermore, all computers will have R_2 as default gateway.

e) A router will divide the network into several subnets, so there will be less traffic within the different parts of network. However, a router requires configuration and is normally more expensive.

3. After processing the message from R_2, R_1 will have the following routing table:

Network	Next router	Distance
N_1	R_2	4
N_2	R_3	5
N_3	R_3	6
N_4	R_2	6
N_5	R_2	6
N_7	R_4	2
N_8	R_3	2

4. The table below presents the solution in accordance with the course book.

Step	N'	D(B),p(B)	D(C),p(C)	D(D),p(D)	D(E),p(E)	D(F),p(F)	D(G),p(G)
0	A	7,A	∞	∞	∞	6,A	∞
1	AF	7,A	∞	∞	14,F		8,F
2	AFB		11,B	∞	14,F		8,F
3	AFBG		10,G	∞	11,G		
4	AFBGC			14,C	11,G		
5	AFBGCE			13,E			
6	AFBGCED						

5.

a) The access control is based on the fact that all frames are long enough to fill the medium during the time it takes for one bit to get to one end of the medium and back. So, to detect collisions the sender must transmit long enough for the collision to propagate all the way back to the sender.
This means that the medium can't be longer than corresponding to the time it takes to send the shortest allowed frame (64 bytes) over the maximum allowed RTT (round trip time). So if the frame size is S (bits), link speed is C (bit/s), length of the medium segment is L (m), and the propagation speed is v (m/s):

$$S/C > 2\,\text{MaxRTT}$$

$$S/C > 2L/v$$

b) Calculate the time it takes to send the smallest allowed frame by dividing the minimum frame size, 64 * 8 bits, with the capacity, 1 billion (10^9) bits per second. The result is the shortest time a sender can spend transmitting on the medium:

$$64*8 \,/\, 10^9 = 512 \,/\, 10^9 = 0.512 * 10^{-6}\,\text{s}$$

Multiply this with the speed of light in the medium. We assume it is 2/3 of the speed of ligth in vacuum: 2/3 c = 200000 km/s or $2*10^8$ m/s, which is close enough for our needs.

$$0.512 * 10^{-6} * 2*10^8 = 1.024 * 10^2 = 102.4\ \text{m}$$

The result is the "length" the frame will have on the medium. We have seen in a) that we need to transmit a longer time than RTT, which means that the medium segment can't be more than half the length of this frame. Thus we need to divide the frame's length with two to get the final result:

$$102.4 \,/\, 2 = 51.2\ \text{m}$$

Or if we do the complete calculation in one step:
$1/2 * 512/10^9 * \ 2*10^8 = (512 * 2 * 10^8) \,/\, (2 * 10^9) = 512 \,/\, 10 = 51.2$ m

6.

a)

Parity: One-dimensional bit parity works as follows. For a group of bits (typically one byte), one bit is added. This bit is set to 1 or 0, depending on if the number of 1s is even or odd (odd or even parity can be used). Accordingly, the number of 1s in the group plus the parity bit is known. If the number of 1s is different at the receiver, the receiver can detect that a bit error has occurred. Single bit errors in the group can always be detected this way.

Checksum: The content of a block of data (frame, packet, etc) is added together by the sender and the sum is appended to the block. The receiver performs the same operation on the received block of data and compares the result to the sum appended by the sender. If the receiver's sum is different than the one appended by the sender, the receiver knows that an error has occurred.

CRC: Data is described as a polynomial and this polynomial is divided by a generator polynomial. The remainder from the division is appended to the data by the sender. By using data+remainder and knowing the generator polynomial, the receiver can verify that the received data matches the sent data.

b)

Parity: The strength with parity is that it is a very simple method which can easily be implemented in both software and hardware. One-dimensional works fine for single/few bit errors. Only an odd number of bit errors a group can be detected with one-dimensional parity.

Checksum: A checksum is straight-forward to implement and it can be done efficiently. Even though multiple bit errors can be detected, a checksum gives limited protection since two or more bit errors in a block of data can cancel out each other so that they are not detected by the checksum.

CRC: This method is more complicated to implement, but efficient hardware-based methods exist today. The method can detect multiple bit errors in a block of data—bit error bursts shorter than the generator polynomial can always be detected. Longer bursts are detected with a high probability if long generator polynomials are used.

c)

Parity: This method is used for instance in serial communication and can also be found in computers as a protection agains bit errors in computer memory.

Checksum: TCP and UDP use this method to validate integrity for segments/packets. The method used by TCP and UDP is relatively weak so additional methods should be applied if data integrity is of high importance.

CRC: Ethernet and wireless LAN use this method to detect bit errors in the frames. Other examples using CRC are archiving programs like WinZip.