

Facultat Informàtica de Barcelona (FIB)

Computer Networks Xarxes de Computadors (XC) Problems

Llorenç Cerdà, Jorge García, Jordi Iñigo, Josep Maria Barceló, Josep Sunyol, Davide Careglio, Eduard Lara.

February 2008

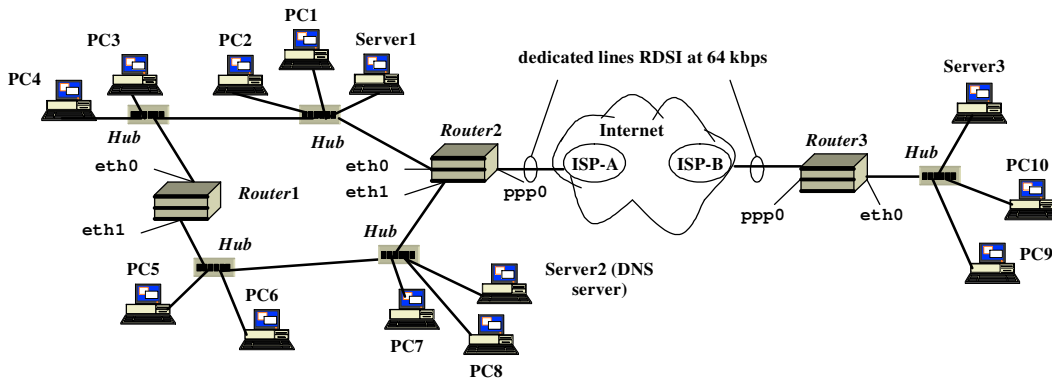
Summary

CHAPTER 2:	IP.....	3
CHAPTER 3.a:	ARQ protocols	12
CHAPTER 3.b:	Transport UDP/TCP.....	13
CHAPTER 4:	Local Area Networks	25
CHAPTER 5:	Data Transmission.....	27

CHAPTER 2: IP

Problem 1.

Consider the network in the figure. The entire network uses *ethernet* 10BaseT, except the Internet area.



When initializing the router ethernet interfaces, in the figure's network, the following commands are executed:

```
Router1:  ifconfig eth0 10.0.0.1 netmask 255.255.255.0;
          ifconfig eth1 10.0.1.1 netmask 255.255.255.0;
Router2:  ifconfig eth0 10.0.0.2 netmask 255.255.255.0;
          ifconfig eth1 10.0.1.2 netmask 255.255.255.0;
Router3:  ifconfig eth0 10.0.2.1 netmask 255.255.255.0;
```

Routers Router2 and Router3 are configured to do **"tunneling"**. Remember that tunneling consists of in sending IP datagrams encapsulated inside other IP datagrams. PPP interfaces in Router2 and Router3 have the following public addresses assigned: 147.0.0.1 and 150.0.0.2, respectively.

Notice that the network address 10.0.0.0 is included in the range of **private IP addresses**.

- Explain briefly which is the use of the PPP protocol.
 - Say which is the use of the protocols LCP and IPCP that are used in PPP.
 - State if a PPP protocol is established between the routers and the Internet Service Providers (ISP), (that is to say, between Router2 and ISP-A and between ISP-B and Router3) or between the routers (between Router2 and Router3). Justify your answer.
 - Explain which is the difference between private and public IP addresses.
 - Explain why do you think it is necessary to use a tunnel between Router2 and Router3.
- MTU for ethernet networks is 1500 bytes and for ppp links is 250 bytes. Answer the following questions (notice that in there would be two headers in the tunnel):
- Which will be the MSS that PC and Server3 need to specify when asking to establish a TCP connection?
 - Assume that PC3 sends an IP datagram of 1500 bytes to Server3 with DF flag (*don't fragment*) deactivated. Router2 will fragment the IP datagrams and Router3 will reassemble (tunnels end):
 - justify why the reassemble is done in Router3 and not at the destiny.
 - how many fragments will be generated
 - the header registers that will be modified when doing the fragmentation
 - and the values to initialize these registers in each fragment
 - What will happen if PC3 sends an IP datagram of 1500 bytes to Server3 with DF flag activated?

CHAPTER 2: IP

From PC1 (from the problem above-mentioned) we execute `tracert Server3` and get the following output:

```
PC1:~>tracert Server3
tracert to Server3 (10.0.2.116), 30 hops max, 40 byte packets
 1 Router2 (10.0.0.2)  0.874 ms  0.753 ms  0.830 ms
 2 Router3 (10.0.2.1)  2.346 ms  1.435 ms  1.731 ms
 3 Servidor3 (10.0.2.116)  3.482 ms *  3.613 ms
```

- a) Explain briefly how `tracert` works
 - i) Reason out why the output to the above command does not include the routers between Router2 and Router3.
- Command `ifconfig -i eth0` is executed in PC1, PC2 and PC5. The following are the outputs to these executions:

```
PC1:
eth0  Link encap:Ethernet Hwaddr 00:10:5A:F7:E3:11
      inet addr: 10.0.0.3 Bcast:10.0.0.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:11186142 errors:0 dropped:0 overruns:1
      TX packets:20731023 errors:0 dropped:0 overruns:0
      Interrupt:5 Base address:0x6800

PC2:
eth0  Link encap:Ethernet Hwaddr 00:10:5A:F7:E3:22
      inet addr: 10.0.0.4 Bcast:10.0.0.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:31486100 errors:0 dropped:0 overruns:1
      TX packets:10631073 errors:0 dropped:0 overruns:0
      Interrupt:5 Base address:0x6800

PC5:
eth0  Link encap:Ethernet Hwaddr 00:10:5A:F7:E3:55
      inet addr: 10.0.1.3 Bcast:10.0.1.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:11566000 errors:0 dropped:0 overruns:1
      TX packets:1531073 errors:0 dropped:0 overruns:0
      Interrupt:5 Base address:0x6800
```

- j) Assume that PC1 executes “ping 10.0.0.4”. Assume that neither PC1 nor PC2 have any information in their ARP tables and that during the working time, there are no more frames circulating than the derived from the afore-mentioned command. Describe the sequence of Ethernet frames, IP datagrams, ARP packets and ICMP packets that will appear in the network since the execution starts until the first answer from the pings addressee is received.
- k) Now, assume that PC2 executes “ping 10.0.1.3”. Assume that initially, PC5 has no information in its ARP table. Again, describe the Ethernet frames, IP datagrams, ARP packets and ICMP packets that circulate around the involved networks.

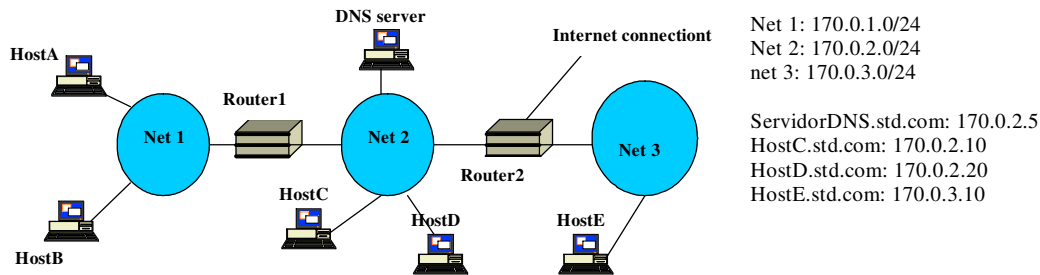
Notes:

1. To describe frames, datagrams and packets the following structures will be used.
2. Notice that in all cases all information must be shown, if an ethernet frame encapsulates an ARP message, the information for the both of them must be shown.

ETHERNET FRAME HEADER	IP DATAGRAM HEADER	ARP PACKET	ICMP MESSAGE
@Physical DESTINO @Physical FUENTE	@IP DESTINY @IP ORIGIN	TIPO DE COMANDO @Physical ORIGIN @IP ORIGIN @Physical ASKED @IP ASKED	MESSAGE TYPE ICMP

Problem 2.

Assume the network in the figure:



- HostA is a PC running Linux. We want to configure it so its Ethernet interface has the following IP address: 170.0.1.30. We execute the command `ifconfig eth0 170.10.1.30 netmask 255.255.255.0`. Once this is done, will we have connectivity in other machines of the network or should we execute another command? If it is necessary to execute another command, say which one and why it is necessary.
- Assume that we have executed all the needed commands to configure hostA. Due to an error, the assigned IP address of HostA is the same that HostB uses. From HostA we execute `ping 170.0.2.10` and observe if there is connectivity. Say which packets are transmitted.
- A few seconds later we execute `ping 170.0.2.10` from HostB. Say which packets are transmitted. Which output will the user get after executing the ping command?
- A few seconds later from HostC we execute `ping HostB.std.com`. Say which packets are transmitted. Which output will the user get after executing the ping command?
- Which mechanism could be used to automatically detect the error of duplicated IP addresses? Explain how this mechanism works.
- We have corrected the previous error (we have assigned HostA the address 170.0.1.31), but when configuring HostD, new problems have been detected. We have executed (from HostD) the following commands:

```
ifconfig lo 127.0.0.1
ifconfig eth0 170.0.2.20
```

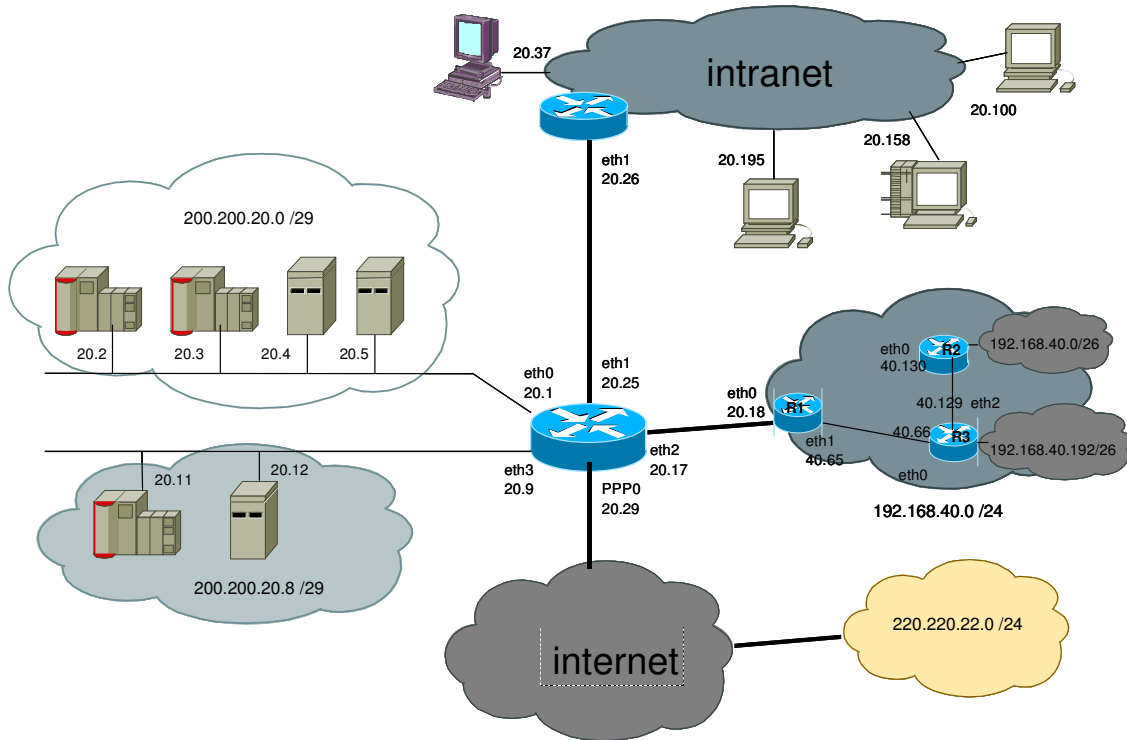
From that host we execute a few "ping" commands. For each case, say if there will be connectivity or not, justifying your answer:

```
ping HostD.std.com
ping HostE.std.com
ping 170.0.3.10
ping www.ac.upc.es
ping HostA.std.com
```

Problem 3.

Assume the network configuration in the figure. To plan the system of IP addressing for the network we have the range of IP addresses: 200.200.20.0/24. This range of address is structured in three main blocks: public servers with free access from the Internet, servers with restricted access and the intranet machines (non-accessible from the Internet).

- The set of servers with restricted access have the subnetwork 200.200.20.0/29 assigned.
- Public servers (http, ftp, smtp, dns) have the subnetwork 200.200.20.8/29 assigned.
- Subranges 200.200.20.16/29 and 200.200.20.24/29 are used to assign addresses to the routers.
- The other addresses in the range 200.200.20.0/24 are free to use in the intranet machines.



- Number of machines that can be connected to the subnetwork 200.200.20.0/29.
- The mask for that subnetwork:
- Its broadcast address.
- How many subnetworks /29 can the range 200.200.20.0/24 include?
- How many subnetworks type /29 are left to be assigned to the intranet?
- Which is the maximum number of machines (hosts) that can be connected inside the intranet?
- If it is necessary to organize the intranet in two subnetworks with a minimum of 50 machines each, which addressing structure will you propose? Indicate all subnetworks of the intranet with the following notation a.b.c.d/m

The questions are independent to the distribution of addresses and subnetworks chosen inside the intranet.

Assume that each time a command is initiated all the ARP tables are empty.

Write the sequence of frames with the corresponding contents for each of the following commands including the pings output.

MAC address will be indicated using the last octet of the IP address (MAC address for the host 200.200.20.2 is 02). Indicate the broadcast MAC address as FF.

Fill the tables with the correspondent information for each frame (Ethernet level, IP level and ICMP protocol level). Leave a blank space if nothing has to be sent.

CHAPTER 2: IP

h) From host 200.200.20.5 we execute: ping 200.200.20.2

Eth @src	Eth @dst	ARP Query / Response	ARP MAC sender	ARP IP sender	ARP MAC receiver	ARP IP receiver	IP @src	IP @dst	ICMP Echo Request / Reply
05	FF	Q	05	20.5					

i) From host 200.200.20.5 we execute: ping 200.200.20.12

Eth @src	Eth @dst	ARP Query / Response	ARP MAC sender	ARP IP sender	ARP MAC receiver	ARP IP receiver	IP @src	IP @dst	ICMP Echo Request / Reply
05	FF	Q	05	20.5					

The number of connected machines increases and it is necessary to use a private range of addresses. The subnetwork 192.168.40.0/24 is defined, and its configuration is shown in the figure.

Routers in the network (the ones in the figure) route the range 192.168.40.0/24 so there is connectivity between the machines with private addressing and the servers and the machines in the intranet.

j) Assume that a DNS query is made from machine 192.168.40.40 to the DNS server (200.200.20.11). Fill in the following table with the information that corresponds to the datagrams at the entrance and the exit of the main router.

	IP	IP	UDP Port	UDP Port	DNS
	origin	destination	origin	destination	
Go:					
Entering eth2	192.168.40.40	200.200.20.11	1100	53	Query
Leaving eth3					Query
Go back:					
Entering eth3					Response
Leaving eth2					Response

In order to provide external connectivity to the network using private addressing it is necessary to configure the NAT (Network Address Translation) functionality in the router. NAT manages the range of ports between 3000 and 3300.

k) Assume that a TCP connection is initiated between machine 192.168.40.40 and a remote webserver 220.220.22.12. Fill in the following table with all the information that corresponds to the entrance and exit of the main router.

CHAPTER 2: IP

	IP	IP	TCP Port	TCP Port	TCP
	origin	destination	origin	destination	Flags
Go:					
Entering eth2	192.168.40.40	220.220.22.12	1030	80	SYN
Leaving PPP0					SYN
Go back:					
Entering PPP0					SYN+ACK
Leaving eth2					SYN+ACK

It is wanted to configure a virtual private network (VPN) between the main division (200.200.20.0/24) and the remote division (220.220.22.0/24). That's why it has been decided to use tunneling between both nets. The ends of the tunnel are the main routers of each division, 200.200.20.29 and 220.220.22.29.

- l) From host 200.200.20.5 we execute a *ping 220.220.22.12*. Fill in the following table with the information that corresponds to the router's exit through PPP0 interface (Internet).

	IP	IP	IP in IP	IP in IP	ICMP
	origin	destination	origin	destination	echo
Go:					
Entering eth0	200.200.20.5	220.220.22.12			RQ
Leaving PPP0					RQ

It is supposed that routers (R₁, R₂ and R₃) belonging to the private subnet 192.168.40.0/24 use RIPv2 protocol as the intern enrouting protocol.

- m) Write the routing table of router R₃ using the following notation:

Acquisition	Destination Net/Mask	Gateway	@IP Exit interface	Metrics

Acquisition is letter **C** if the destination net is directly connected to the router or letter **R** if has learned it using RIP. Fill in the necessary lines for this table.

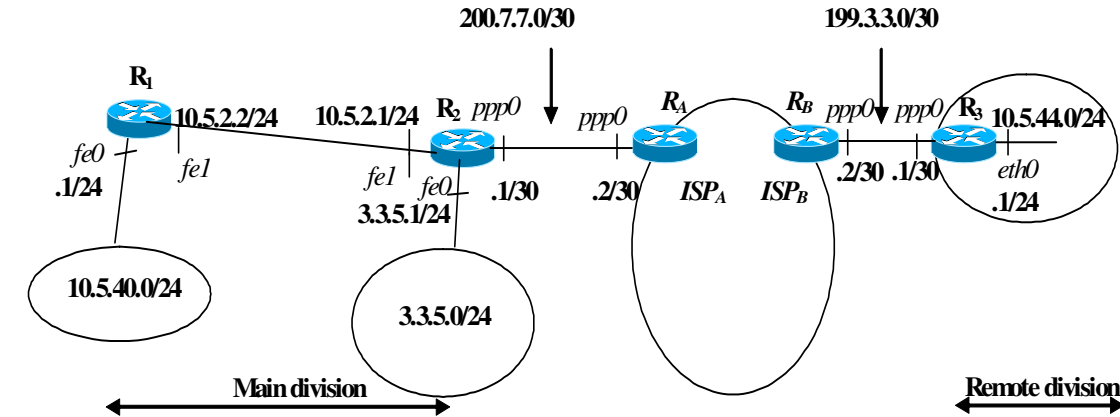
- n) If *split-horizon* is activated in all the routers, write the content of the RIPv2 message that will be sent by router R₃ to router R₁. The message is composed by a list of lines with format:

@IP _{Net}	Mask	Metrics

Problem 4.

Assume the IP network in the figure. The network is divided in two. One is a private net (with addresses 10.0.0/8). The other is a public net (with addresses 3.3.5.0/24). The private part has a remote division (subnet 10.5.44.0/24) that is accessible from the main division through the Internet. The net has a contract with an ISP_A to provide an Internet connection to the main division, and with ISP_B to provide internet connection to the remote net, using IP addresses 200.7.7.0/30 and 199.3.3.0/30 respectively.

From the private side of the net (main and remote divisions) it is possible to access the Internet or net 3.3.5.0/24 through router R₂. To allow the access to the Internet the router is configured by using NAT. In addition, to connect the two divisions in the private network an IP in IP tunnel is configured between R₂ and R₃.



Answer the following questions.

- Which will be the routing table for R₁?
- We execute a ping from host 10.5.40.10 to host 10.5.44.8. Indicate which are the routers that the packet ICMP ECHO REQUEST crosses. Indicate which are the origin/destiny IP addresses of the packet. In case it is necessary to use a tunnel, indicate the directions for the intern an external header. (It is NOT necessary to indicate other registers from the IP header, ARP packets, etc.)
- IDEM c) what if the ping is from 10.5.40.10 to host 3.3.5.5
- IDEM c) what if the ping is from 10.5.40.10 to machine 147.83.34.90.
- IDEM c) what if the ping is from 10.5.44.8 to machine 147.83.34.90.
- IDEM c) what if the ping is from 3.3.5.5 to host 147.83.34.90

In router R₁ we configure an access list to the incoming traffic in interface fe1. The configured rules allow the following:

- Servers with a port inferior to 1024 of subnet 10.5.40.0/24 are only accessible from the clients in the network 10.0.0.0/8.
- As an exception, webservers (80) from the subnetwork 10.5.40.0/24 are accessible from any client of network 3.3.5.0/24.
- The clients of network 10.5.40.0/24 can access any server of networks 10.0.0.0/8 and subnetwork 3.3.5.0/24. However, they can only connect to webservers through the rest of the Internet.

g) Write the ACL. notation for ACLs is as follows:

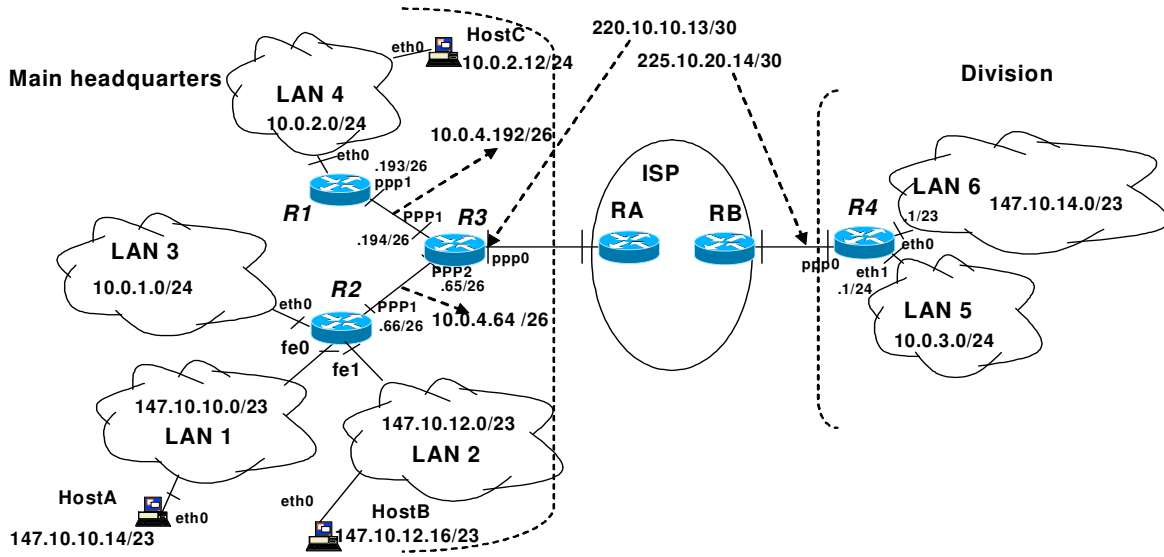
```
access-list #ID {deny/permit} {protocol} {@IPorg WildcardMaskorg}{@IPdst WildcardMaskdst }
{eq/geq/leq}{portdst}
```

where: eq is equal to, leq less than or equal to and geq is greater than or equal to. portdst is referred to the destination port of the packet.

Problem 5.

The figure shows a corporate network of a company that has a main headquarter and a division. PPP interfaces in routers R3 and R4, are assigned to a public address given by the ISP (220.10.10.13/30 and 225.10.20.14/30 respectively). Some of the subnets of the network have assigned private IP addresses (addresses 10.0....) and the others public ones. For doing the last public IP addresses between the range 147.10.8.0/21 have been acquired. The figure shows the assignment between addresses and masks. The main headquarters are composed by LAN1 y LAN2, where public IP addresses are assigned.

Net LAN6 from the division has also assigned public addresses. The rest of the IP addresses are private. HostA is a host belonging to LAN1 and has an IP address 147.10.10.14/23, HostB belongs to LAN2 and has an IP address 147.10.12.16/23, and HostC belongs to LAN4 and has the IP address 10.0.2.12/24. Both routers R3 and R4 have the capacity to do tunneling and NAT.



a) Answer the following questions:

- 1) Assign IP addresses router R2 interfaces fe0 and fe1.
- 2) The routing protocol used by the network routers (main headquarters and division) is RIPv2. Show a possible enrouting table for router R2 that allows a complete connectivity between all the machines in the company and from these to the Internet. Use the following notation. Column Acquisition uses: **C** for the entries that correspond to the networks that are directly connected and **R** for the entries that learn the way using RIP and S for the static entries in the table and column Metrics if there are.

Acquisition	Destination net/ Mask	Gateway	Interface	Metrics
-------------	-----------------------	---------	-----------	---------

b) Answer the following questions:

- 3) Suppose that HostA, in LAN1 executes a ping to HostB in LAN2. Enumerate the frames that circulate through the different subnets until the moment when the first ECHO REPLY arrives to HostA. The ARP caches are empty and the routing tables are stable and correct. For every frame, indicate which are the original physical address -that belongs to each frame-, the content type (ICMP ECHO REQUEST message, ARP request, etc.), and the significant contents to every type in address terms: for ICMP, @IP origin and @IP destination; for ARP, the @IP that corresponds to the origin of the ARP packet, Physical@ of the origin of ARP packet, the target @IP, and the target Physical@ (when recognised).

NOTE: Use the notation @Phys-IdMachine-interfaceName to indicate the physical address of the interface, @Phys-HostA-eth0 indicates the physical direction of interface eth0 in HostA.

- 4) Do the same exercises if HostA executes a ping to HostC.

CHAPTER 2: IP

- c) As said before, routers in the corporate network use the enrouting protocol RIPv2. Assume the format is the indicated below and notice that the metric in a net where you are directly connected is 1. Show the contexts for the RIPv2 message sent by R2 to R3 in the following conditions:

Destination net	Mask	Metrics
-----------------	------	---------

- 5) RIPv2 protocol with split horizon.
- 6) RIPv2 protocol with split horizon with triggered update and poison reverse, when the connection fails in LAN3.
- d) Indicate which routers does the RIPv2 message sent by R4 to R3 crosses. Indicate which are datagram's origin/destination IP addresses. In case tunneling is used, show the addresses for the internal and external header. It is NOT necessary to indicate other registers of the IP header, ARP packets, etc!!
- e) Repeat what you have done in the previous question in case HostC in LAN4 sends a connection request to a webserver located in machine 220.12.20.156.

CHAPTER 3.a: ARQ protocols**Problem 1.**

We want to use a window protocol over a point to point link with the following characteristics:

Distance: 3000 Km.

Propagation speed, $v_p = 0.6 c$. (c is light's speed; $c = 3 \times 10^8$ m/s).

Broadcasting speed, $v_t = 1500$ Kbps.

Frames length, $L = 64$ octets.

Retransmission Go-back-N.

- Which value will you give to the window?
- Which value will you give to the rebroadcasting timing?

Problem 2.

There is a point to point link with propagation 0,5 ms and a speed of 1 Mb/s. To transmit information we use a protocol with error control, Stop & Wait. The frames length is 1000 bits. The recognitions have a length of 32 bits. The average number of transmission N_t is 1.1 frames. The timer of the retransmissions is activated each 10 ms. Which is the number of frames per second ("throughput") that can be broadcasted? Draw a diagram with the times where you can see the protocols behaviour.

Problem 3.

Over a point to point connection, "full duplex", a window protocol is used and the characteristics are the following:

Frame length, $L = 256$ octets

Broadcasting speed, $v_t = 512$ Kbps

Propagation time, $t_p = 100$ ms

Retransmission Go-back-N

The receivers protocol introduce the following variation when sending confirmations, it only sends confirmations each 24 milliseconds, confirming all frames received since the last confirmation sent.

The confirmations can go inside an information frame in the opposite direction or in specific frames of 16 octets.

- Which is the minimum time that has to be assigned to the broadcasting timer to prevent the broadcast of frames before time?
- Which value will you assign to the window?
- If during the time interval lots of consecutive confirmations are lost, the first frame of confirmation that correctly arrives, which maximum number of frames should it confirm?

Problem 4.

A data link between two DTEs has a broadcast speed of 256 Kbps. The propagation time end to end is 0.5 ms. The link is FD_X. The data block has a total of 512 octets and the confirmation block also has 512 octets.

- If the datalink protocol is RS (continuous transmission) type, and noticing that the header of the data block is composed by 8 octets and the detector code of errors is CRC of 32 bits, which is the maximum efficiency?
- Which value must be assigned to the rebroadcasting timer?
- How many blocks must be rebroadcasted whenever an error happens?
- If the average number of broadcasting is $N_t = 1.5$, which is the average efficiency?

Problem 5.

In a link via satellite between two DTEs the propagation time, station to satellite is 250 milliseconds and broadcasting speed is 2 Mbps. Protocol blocks between DTEs, have a total of 1000 octets, from which 2 are from the header and 2 for the intern detector code. Inside the header 4 bits are used to enumerate the frames and 4 bits to confirmations ("piggy-backing").

- Which is the dimension of the optimal transmission window?
- Which is the maximum effective speed if the "stop and wait" protocol is used?
- Which is the maximum effective speed if the "go-back-n" protocol is used?
- Which is the maximum effective speed if the "selective broadcasting" protocol is used?

CHAPTER 3.b: Transport UDP/TCP

Problem 1.

From a personal computer, using a modem, an ftp session with UPC ftp server is established, at the same time its evolution is monitored using a new version of tcpdump (windump) for Windows 95 ®.

Table 1 shows in the 1st column the line number of what is written in the 2nd. The 2nd column shows a screenshot where you can see the interaction between the user and the ftp client. What has been typed by the user is shown in bold and italics (the password and email address have been modified but the number of characters is still the same). As you can see, once the ftp session is established, the user goes to the directory pub/doc/rfc and requests a transference of file ***rfc-index.txt*** that contains a relation of all the existing Internet RFCs. Table 2 shows a screenshot of windump **EXECUTED ON THE PC** (until the moment in which the client sends the password and the ftp server accepts it).

- As you can see in the TCP states graph and the output in table 2, specify in which state are the TCP modules in both sides AFTER EACH of the first four segments that windump captures at the PC.
- Associate the groups of segments that go in one way and the other in the different phases that the FTP session takes, until the password has been accepted by the server (FTP phases: the ftp server accepts the session, login petition, login delivery, password petition and password delivery).

When the user gives the order to transfer the file, a TCP connection between the client and the server is established. So, at that moment there are two TCP connections opened. Table 3 shows important parts of the connection, **captured by windump AT THE FTP SERVER (Notice that in table 2 the capture was done at the PC and now it is done at the FTP server)**.

- Which is the value of the congestion window of the TCP module in the machine defalla.upc.es in points (1) and (7)?
- Which will approximately be the state of occupation of the buffers of the TCP module in the pc in points (5) and (6)?
- Which will you think must be the minimum value of the congestion window of TCP of defalla.upc.es in point (8)? Why is the segment with byte number 23361 rebroadcasted? Which will be the value of the congestion window in point (9)? How will the congestion control mechanism work? And will it make the congestion window evolve?
- What is happening in point (10)? Is the ftp session over for the user in point (11)? Justify your answers

TABLE 1: FTP CAPTURE: USERS SCREENSHOT

1	C:\>ftp ftp.upc.es
2	Connected to defalla.upc.es.
3	220- O O O
4	220- O O O Servei d'FTP de la UPC
5	220- O O O
6	220- U P C
7	220-
8	220-
9	220 defalla.upc.es FTP server (Thu Dec 23 17:22:07 MET 1999) ready.
10	User (defalla.upc.es:(none)):anonymous
11	331 Guest login ok, send your complete e-mail address as password.
12	Password:aaaaaaaa@aa.aaa.aa
13	230 Guest login ok, access restrictions apply.
14	ftp> cd pub
15	250 CWD command successful.
16	ftp> cd doc
17	250 CWD command successful.
18	ftp> cd rfc
19	250-Please read the file README
20	250- it was last modified on Tue Aug 17 00:00:00 1999 - 508 days ago
21	250 CWD command successful.
22	ftp> get rfc-index.txt
23	200 PORT command successful.
24	150 Opening ASCII mode data connection for rfc-index.txt (452955 bytes).
25	226 Transfer complete.
26	463540 bytes received in 66.73 seconds (6.95 Kbytes/sec)
27	ftp> quit
28	221 Goodbye.

TABLE 2: FTP CAPTURE (INTERACTIVE SIDE: CONNECTION CONTROL)

CAPTURED BY WINDUMP (TCPDUMP)	
20:38:15.444968	193-153-26-166.uc.nombres.ttd.es.1064 > defalla.upc.es.21: S 1086533:1086533(0) win 8192 <mss 1460> (DF)
20:38:33.553968	193-153-26-166.uc.nombres.ttd.es.1064 > defalla.upc.es.21: S 1086533:1086533(0) win 8192 <mss 1460> (DF)
20:38:33.710154	defalla.upc.es.21 > 193-153-26-166.uc.nombres.ttd.es.1064: S
2104269198	:2104269198(0) ack 1086534 win 8760 <mss 1460> (DF)
20:38:33.726773	193-153-26-166.uc.nombres.ttd.es.1064 > defalla.upc.es.21: . ack 1 win 8760 (DF)
20:38:44.147755	defalla.upc.es.21 > 193-153-26-166.uc.nombres.ttd.es.1064: P 1:13(12) ack 1 win 8760 (DF) [tos 0x10]
20:38:44.328946	193-153-26-166.uc.nombres.ttd.es.1064 > defalla.upc.es.21: . ack 13 win 8748 (DF)
20:38:44.523575	defalla.upc.es.21 > 193-153-26-166.uc.nombres.ttd.es.1064: P 13:164(151) ack 1 win 8760 (DF) [tos 0x10]
20:38:44.644831	193-153-26-166.uc.nombres.ttd.es.1064 > defalla.upc.es.21: . ack 164 win 8597 (DF)
20:38:47.157912	193-153-26-166.uc.nombres.ttd.es.1064 > defalla.upc.es.21: P 1:17(16) ack 164 win 8597 (DF)
20:38:47.327138	defalla.upc.es.21 > 193-153-26-166.uc.nombres.ttd.es.1064: . ack 17 win 8760 (DF) [tos 0x10]
20:38:47.342767	defalla.upc.es.21 > 193-153-26-166.uc.nombres.ttd.es.1064: P 164:232(68) ack 17 win 8760 (DF) [tos 0x10]
20:38:47.448858	193-153-26-166.uc.nombres.ttd.es.1064 > defalla.upc.es.21: . ack 232 win 8529 (DF)
20:38:55.059919	193-153-26-166.uc.nombres.ttd.es.1064 > defalla.upc.es.21: P 17:42(25) ack 232 win 8529 (DF)
20:38:55.223013	defalla.upc.es.21 > 193-153-26-166.uc.nombres.ttd.es.1064: P 232:280(48) ack 42 win 8760 (DF) [tos 0x10]
20:38:55.327765	193-153-26-166.uc.nombres.ttd.es.1064 > defalla.upc.es.21: . ack 280 win 8481 (DF)

TABLE 3: CAPTURE (MASSIVE DATA INTERCHANGE: TRANSFERENCE CONNECTION)

CAPTURED BY WINDUMP (TCPDUMP) –NO TEMPORAL INDICATION-
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: S 2116394541:2116394541(0) win 8760 <mss 1460> (DF) [tos 0x8]
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: S 2116394541:2116394541(0) win 8760 <mss 1460> (DF) [tos 0x8]
193-153-26-166.uc.nombres.ttd.es.1075 > defalla.upc.es.20: S 1124670:1124670(0) ack 2116394542 win 8760 <mss 1460> (DF)
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . ack 1 win 8760 (DF) [tos 0x8]
(1)----->
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . 1:1461(1460) ack 1 win 8760 (DF) [tos 0x8]
193-153-26-166.uc.nombres.ttd.es.1075 > defalla.upc.es.20: . ack 1461 win 8760 (DF)
(2)----->
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . 1461:2921(1460) ack 1 win 8760 (DF) [tos 0x8]
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . 2921:4381(1460) ack 1 win 8760 (DF) [tos 0x8]
193-153-26-166.uc.nombres.ttd.es.1075 > defalla.upc.es.20: . ack 2921 win 8760 (DF)
(3)----->
193-153-26-166.uc.nombres.ttd.es.1075 > defalla.upc.es.20: . ack 4381 win 8760 (DF)
(4)----->
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . 4381:5841(1460) ack 1 win 8760 (DF) [tos 0x8]
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . 5841:7301(1460) ack 1 win 8760 (DF) [tos 0x8]
193-153-26-166.uc.nombres.ttd.es.1075 > defalla.upc.es.20: . ack 5841 win 2048 (DF)
(5)----->
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . 7301:8761(1460) ack 1 win 8760 (DF) [tos 0x8]
193-153-26-166.uc.nombres.ttd.es.1075 > defalla.upc.es.20: . ack 7301 win 4096 (DF)
(6)----->
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . 8761:10221(1460) ack 1 win 8760 (DF) [tos 0x8]
193-153-26-166.uc.nombres.ttd.es.1075 > defalla.upc.es.20: . ack 8761 win 8760 (DF)
(7)----->
Se han suprimido líneas
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . 16061:17521(1460) ack 1 win 8760 (DF) [tos 0x8]
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . 17521:18981 (1460) ack 1 win 8760 (DF) [tos 0x8]
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . 18981:20441(1460) ack 1 win 8760 (DF) [tos 0x8]
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . 20441:21901(1460) ack 1 win 8760 (DF) [tos 0x8]
193-153-26-166.uc.nombres.ttd.es.1075 > defalla.upc.es.20: . ack 21901 win 8760 (DF)
(8)----->
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . 21901:23361(1460) ack 1 win 8760 (DF) [tos 0x8]
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . 23361:4821(1460) ack 1 win 8760 (DF) [tos 0x8]
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . 24821:26281(1460) ack 1 win 8760 (DF) [tos 0x8]
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . 26821:27741(1460) ack 1 win 8760 (DF) [tos 0x8]
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . 27741:29201(1460) ack 1 win 8760 (DF) [tos 0x8]
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . 21901:23361(1460) ack 1 win 8760 (DF) [tos 0x8]
193-153-26-166.uc.nombres.ttd.es.1075 > defalla.upc.es.20: . ack 23361 win 8760 (DF)
(9)----->
Se han suprimido líneas
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: F 463133:463541(408) ack 1 win 8760 (DF) [tos 0x8]
(10)--->
193-153-26-166.uc.nombres.ttd.es.1075 > defalla.upc.es.20: . ack 463542 win 8760 (DF)
193-153-26-166.uc.nombres.ttd.es.1075 > defalla.upc.es.20: F 1:1(0) ack 463542 win 8760 (DF)
defalla.upc.es.20 > 193-153-26-166.uc.nombres.ttd.es.1075: . ack 2 win 8760 (DF) [tos 0x8]
(11)--->

Problem 2.

The following is a captured trace using the command: `tcpdump ip -i eth0 > trace`. The content of the trace file is:

```

12:55:45.92 PC4.local.9088 > Servidor2.local.www: S 3125459530:3125459530(0) win 255 <mss 536>
(1)  ────>
12:55:45.92 Servidor2.local.www > PC4.local.9088: S 2025570752:2025570752(0) ack 3125459531 win 32736 <mss 1460>
(2)  ────>
12:55:45.98 PC4.local.9088 > Servidor2.local.www: . ack 1 win 65534
(3)  ────>
Ara el client envia una comanda HTTP "GET" al servidor...
12:55:45.99 PC4.local.9088 > Servidor2.local.www: P 1:103(102) ack 1 win 65534
El servidor contesta...
12:55:46.00 Servidor2.local.www > PC4.local.9088: P 1:537(536) ack 103 win 32736 (DF)
12:55:46.03 PC4.local.9088 > Servidor2.local.www: . ack 537 win 64998
(4)  ────>
12:55:46.03 Servidor2.local.www > PC4.local.9088: . 537:1073(536) ack 103 win 32736 (DF)
12:55:46.03 Servidor2.local.www > PC4.local.9088: . 1073:1609(536) ack 103 win 32736
12:55:46.07 PC4.local.9088 > Servidor2.local.www: . ack 1073 win 64998
12:55:46.07 PC4.local.9088 > Servidor2.local.www: . ack 1609 win 64998
12:55:46.10 Servidor2.local.www > PC4.local.9088: . 1609:2145(536) ack 103 win 32736
12:55:46.10 Servidor2.local.www > PC4.local.9088: . 2145:2681(536) ack 103 win 32736
12:55:46.10 Servidor2.local.www > PC4.local.9088: . 2681:3217(536) ack 103 win 32736
12:55:46.11 Servidor2.local.www > PC4.local.9088: . 3217:3753(536) ack 103 win 32736
12:55:46.12 PC4.local.9088 > Servidor2.local.www: . ack 2145 win 64998
12:55:46.12 PC4.local.9088 > Servidor2.local.www: . ack 2681 win 64998

12:55:46.12 PC4.local.9088 > Servidor2.local.www: . ack 3217 win 64998
12:55:46.12 Servidor2.local.www > PC4.local.9088: . 3753:4289(536) ack 103 win 32736
12:55:46.13 PC4.local.9088 > Servidor2.local.www: . ack 3217 win 64998
12:55:46.13 Servidor2.local.www > PC4.local.9088: . 4289:4825(536) ack 103 win 32736
12:55:46.13 PC4.local.9088 > Servidor2.local.www: . ack 3217 win 64998
12:55:46.30 Servidor2.local.www > PC4.local.9088: . 4825:5361(536) ack 103 win 32736
12:55:46.32 Servidor2.local.www > PC4.local.9088: . 3217:3753(536) ack 103 win 32736
12:55:46.32 Servidor2.local.www > PC4.local.9088: . 3753:4289(536) ack 103 win 32736
12:55:46.33 PC4.local.9088 > Servidor2.local.www: . ack 5361 win 64998

(5)  ────>
Hem eliminat algunes línies...
12:55:57.32 Servidor2.local.www > PC4.local.9088: . 15217:15753(536) ack 103 win 32736
12:55:57.32 Servidor2.local.www > PC4.local.9088: . 15753:16289(536) ack 103 win 32736
12:55:57.63 PC4.local.9088 > Servidor2.local.www: . ack 15217 win 536
12:55:57.63 Servidor2.local.www > PC4.local.9088: . 16289:16825(536) ack 103 win 32736
12:55:57.63 Servidor2.local.www > PC4.local.9088: . 16825:17361(536) ack 103 win 32736
12:55:58.93 PC4.local.9088 > Servidor2.local.www: . ack 15753 win 0
12:55:58.93 PC4.local.9088 > Servidor2.local.www: . ack 17361 win 536
(6)  ────>
12:55:59.03 Servidor2.local.www > PC4.local.9088: F 17361:17361(0) ack 103 win 32736
(7)  ────>
12:55:59.03 PC4.local.9088 > Servidor2.local.www: . ack 17362 win 32736
(8)  ────>
12:55:59.03 PC4.local.9088 > Servidor2.local.www: F 103:103(0) ack 17362 win 32736
(9)  ────>
12:55:59.05 PC4.local.9088 > Servidor2.local.www: F 103:103(0) ack 17362 win 32736
(10) ────>
12:55:59.06 Servidor2.local.www > PC4.local.9088: ack 104 win 32736

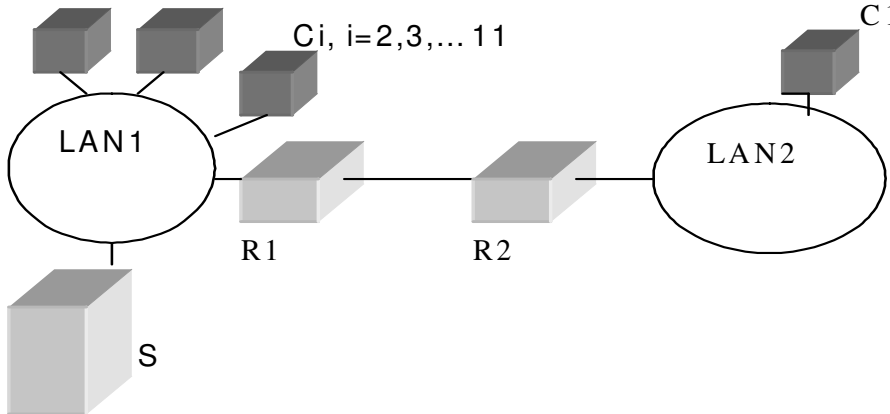
```

- Deduce who is the client and who the server
- Deduce if the trace has been captured from the client or server
- Say in which state is the client and the server in points: (1), (2), (3), (4) and (5).
- Which will be the congestion window for the client in point (4)?

- e) Say which will probably be the occupation of the transmission and reception TCP buffers in the client and server in points (5) and (6).
- f) Why are there 3 ACKs sent by the client to the server just before point (5) that confirm the *same* bytes?
- g) Explain why does the server send an ACK of the byte after the rebroadcasting of segments 3217:3753 and 3753:4283 (point (5)).
- h) Explain in which states are the client and server in points (7), (8), (9), and (10).

Problem 3.

Assume the network in the figure. S is a file server. Clients C_i ($i=1,2,\dots,11$) run an application that reads a file from S and stores it in its local disk.



We will assume that the clients and the server have a CPU with a high processing speed (assume that it is infinitely fast). However, when the access to its disks is limited: the server can read from its disk at a maximum of 8 MBps (64 Mbps) while the clients can write in a continuous way in its disks at a maximum of 2 MBps (16 Mbps).

When a TCP connection is established, the clients and the server reserve transmission and reception buffers of 16 KB.

Routers R1 and R2 have buffers for each output interface with a limited capacity of 12 KB (8 packets of 1500 B).

Both LANs are of big capacity (100 Mbps) while the point to point link is much slower (100 kbps). Propagation delays can be despised.

MTU has a value of 1500 B for all the the entire network.

Losses due to errors in the broadcast between both LANs and the point to point link can also be despised.

Section 1: Assume that client C1 establishes a TCP connection with server S.

- a) Which segments are interchanged between the connection establishment? Which values will the segments have for the following flags: SYN, FIN, RST, ACK? Which will be the MSS?
- b) Explain why the numbers from the initial sequence in TCP are chosen randomly.

We execute the command `netstat -a` from server S and get the following output:

Local Address	Remote Address	State
*.111	*.*	LISTEN
*.21	*.*	LISTEN
147.83.30.10.3045	147.83.30.33.60	ESTABLISHED
147.83.30.10.111	147.83.30.20.3200	SYN_RCVD
127.0.0.1.111	127.0.0.1.3200	ESTABLISHED
147.83.30.10.21	147.83.30.20.2000	FIN_WAIT1

CHAPTER 3: Point-to-point protocols

- c) How many servers are active in S? Why are there two different IP addresses in column "Local Address"? In which connection/s does S take the role of client?
- d) Which sequence of segments interchange has probably happened in a connection in state SYN_RCVD? What if the state is FIN_WAIT1? What will you expect to happen in the following seconds for the previous two connections?

Section 2: Assume now that the network only activates the connection between S and C1.

- a) What limits the transfer speed in long-term, the congestion window or the advertised window? (justify your answer).
- b) Say which will be the occupation (empty/full) in long-term of the following buffers:
 - Transmission and reception buffers from S.
 - Transmission and reception buffers from C1.
 - Buffer linked to the serial interface and buffer linked to the ethernet interface from R1.
 - Buffer linked to the serial interface and buffer linked to the ethernet interface from R2.
- c) Which advertised window will carry segments from S to C1? Idem to the segments from C1 to S.

Section 3: We close the previous connection and open a new one between S and C2.

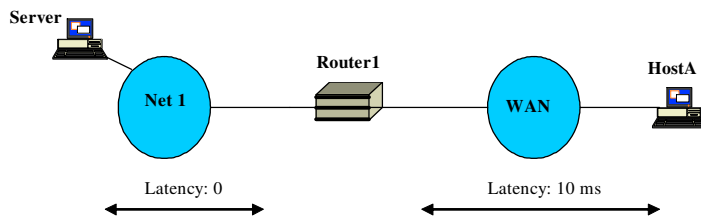
- a) What limits the transfer speed in long-term, the congestion window or advertised window? Say in an approximate way which will be, long-term, the transfer speed that we'll get (bps).
- b) Say which will be the occupation (empty/full) in long-term of the following buffers:
 - Transmission and reception buffers from S.
 - Transmission and reception buffers from C2.
- c) Which advertised window will carry segments from S to C2? Idem to the segments from C2 to S.

Section 4: Assume that we now establish connections between the server S and all the clients in LAN1, C_i , $i=2..11$.

- a) What limits the transfer speed in long-term, the congestion window or the advertised window? Say in an approximate way which will be, long-term, the transfer speed that we'll get (bps) **for each connection**.
- b) Say which will be the occupation (empty/full) in long-term of the following buffers:
 - Transmission and reception buffers from S
 - Transmission and reception buffers from C_i
- c) Which advertised window will carry segments from S to C_i ? Idem to the segments from C_i to S.

Problem 4.

Assume the network in the figure:



HostA is connected to the charger port's server.

The latency introduced by net 1 is despised while the WAN's latency is 10 ms.

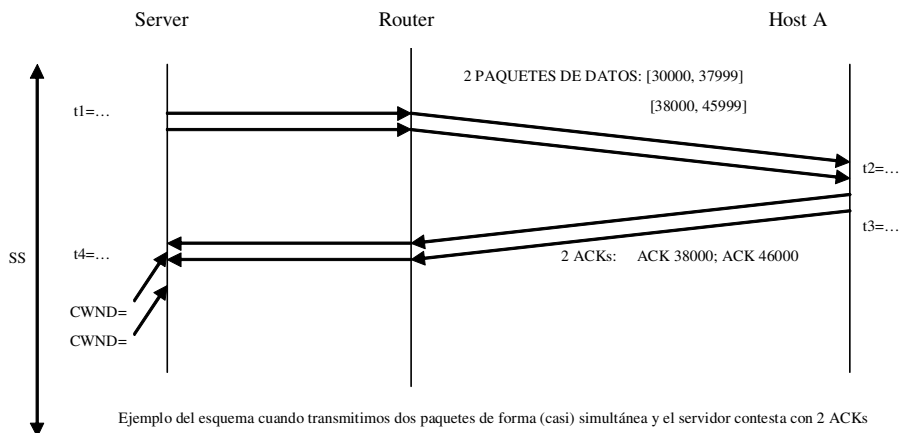
Transmission speed is very high in all the different links, and we will consider it as infinite.

Initially, we will assume that there are no losses, and the routers buffers capacity is infinite.

We will also assume that the processing speed of the server and the Host one is also infinitely large.

When a segment carries data, it has a size of 8 KB and the maximum value for the transmission window is 64 KB. So: transmission window = MIN(64 KB, awnd, cwnd), where awnd is the advertised window and cwnd the congestion window.

- a) Do a schema that clearly shows the times of arrival and departure to HostA and the server of the TCP segments. Show the first 140ms. If more than one packet is transmitted or received at the same time, show it as in the figure below. After the reception of each segment by the HostA it is necessary to indicate the value of the congestion window. We will assume that HostA sends an ACK for each data segment that receives. It is necessary to indicate for each data segment the numeration to the bytes it carries. For the ACKs indicate the byte until which they confirm. Assume that we start numerating the bytes at 0. (Try to fit the schema in one page).



Which is the maximum value of the transmission window that we will get? Which is the average data transfer speed between the server and hostA that we will have in a stationary state (in Mbps)?

To the following part we will assume that net 1 introduces losses in the segments. Specifically we will assume that the server starts numbering the data in byte 0, and we have a loss the first time that we transmit the segment carrying bytes (32000,39999). We also assume that the packets of size 40 bytes (which are, ACKs, SYNs, etc) that cross the network in either way are never lost.

We will assume the following:

- The servers and router TCP only has the following mechanisms: Slow Start and Congestion Avoidance, but does not include: Fast retransmit, Fast recovery, etc.
- The timer value RTO of TCP keeps a constant value of 22 ms.

Also keep in mind that::

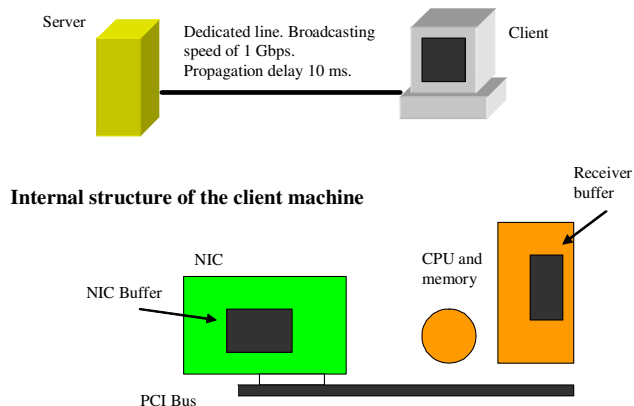
- Duplicated ACKs do not increase the congestion window.
- Accumulated ACKs are taken as an only ACK when increasing the congestion window.
- Transmission window refers to the TCP segments that have been sent but are not yet confirmed.

CHAPTER 3: Point-to-point protocols

- b) Draw a graph similar to the previous one, also until the time 140 ms, that shows the broadcast evolving for this case. Indicate the duration of the phases of Slow Start and the ones of Congestion Avoidance. Also specify the values of $cwnd$ and $ssthresh$.
- c) In the previous part we assumed that the timer RTO of TCP is kept constant. However, in a real environment that won't be true. Explain briefly what mechanism is used to fix the value of the timer. It is NOT necessary to explain the concrete algorithm that is used (Van Jacobson and Karels algorithm).

Problem 5.

Assume that we connect a remote server from our company to a local client through a dedicated line at 1 Gbps. The propagation delay of the signal along the line is of 10 ms (see figure).



The client machine is a PC equipped with a CPU that works at a very high speed (consider infinite) so the client process consumes data from the receiver buffer also at a high speed (consider infinite) The I/O bus of the system, to which the net adapter is connected, is a PCI bus, with a maximum transference speed of 1 Gbps. However, the used bus is also used by other peripherals so the effective speed is decreased so it only uses a 10% of the maximum transference speed.

The operating system of the client reserves 32 KBytes for the receiver buffer of TCP data. The maximum value for the congestion window is 64 Kbytes.

The server is continuously transferring data to the client, sending frames with MSS of 1000 Bytes. The client only sends in the other way TCP ACKs of 40 Bytes.

Assume that we buy a new network adapter with a buffer for packets of a very big capacity (infinite) and the client machine sends an ACK for each TCP segment correctly received.

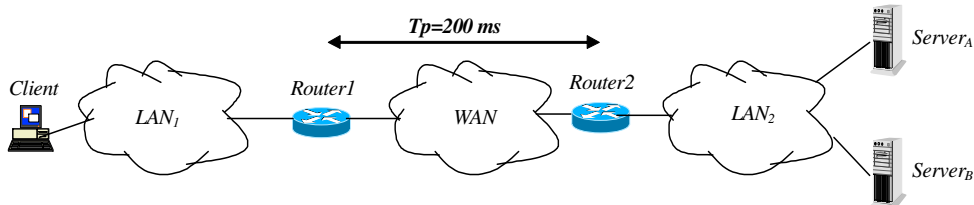
- Draw how will the server's transmission window will evolve, also the advertised window by the client and the transference speed between the server and the client. Consider that time $t=0$ corresponds to the end of the process of connection establishment. Clearly indicate which times in x-axis. Indicate in the graph in which phase of the congestion control is the server.
- Which will be the maximum transfer speed that we will get?.
- How much data is stored in the buffer of the network adapter?
- How do questions b) y c) change if instead of using TCP we use UDP as the transport protocol?

Assume now that the network adapter that we use only has a storing capacity for 3 data packets.

- same question as in a).
- same question as in b)
- same question as in d)

Problem 6.

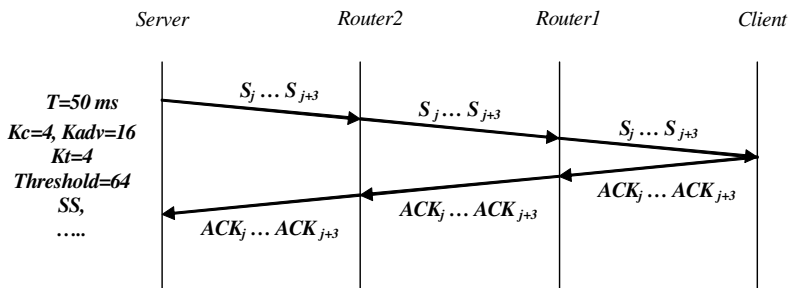
A client is connected to two remote servers (Server_A and Server_B) with a connection through a WAN using a router (router1), as shown in the figure. The propagation in the LANs is despicable and for the WAN is 200 ms. The client will do requests to the server's charger port.



Terminals (clients or servers) access the LANs with a MTU of 1000 Bytes (40 Bytes of TCP ACKs) and a high broadcast speed (for example, 1 Gbps) for both clients and servers. In fact, for simplicity reasons we will consider the speed as infinite. The access to the WAN is of 10 Mbps in both directions. The client reserves 32 Kbytes for the receiver buffer and a maximum value for the congestion window of 64 Kbytes. Routers have buffers of 64 Kbytes for each direction

Initially the client connects to the server A through the charged port.

- a) Draw a temporal schema where the interchange of TCP segments is shown from the start (including 3WHS) of the connection to the broadcast of the segment S_{80} . Follow the notation in the figure (in which the transmission of 4 segments, segment from S_j to S_{j+3} is draw as well as the ACKs in each frame of the communication). Indicate the value for the congestion window (Kc), the threshold, the phase (Slow Start, SS or Congestion Avoidance, CA) that has the TCP at the start of the transmission of each group of segments and all the events you think it is necessary to point out.
- b) Draw the evolution of the transmission window, the advertised window and the congestion one, indicating the values of the advertised window, the congestion and the transmission one in the most significant times.



- c) Which average throughput is obtained once the transitory state is over?

Now the client opens a charged connection with server B keeping the existing connection with A. Assume that the servers share the LAN fairly with an access protocol.

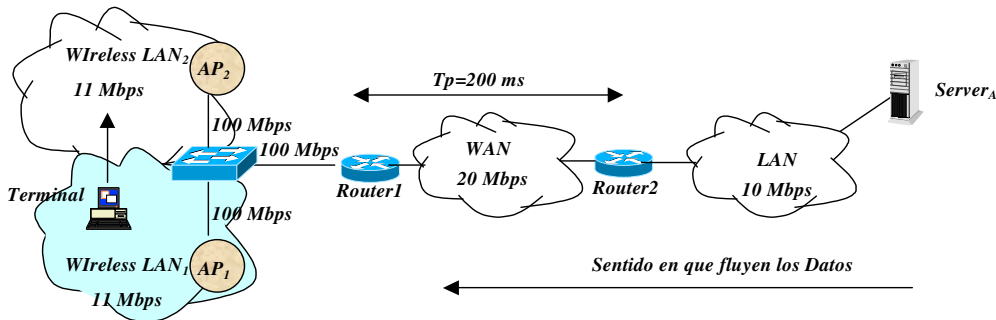
- d) Which is the average throughput obtained for each of the client connections once the transitory state is finished? How will the results change if the propagation time was 500 ms?

Assume now that the connections use the UDP transport protocol and the two servers are non-stop returning data to the client.

- e) Which average throughput for the client's received data will we have for each of the transferences if the router had 32Kbytes? How will this vary if the router had 64Kbytes? Justify your answer.

Problem 7.

There is a terminal connected to a Wireless network type 802.11b (at 11 Mbps). Wireless networks LAN1 and LAN2 are connected to the output router through its Access Points (AP) connected to an Ethernet switch, all ports at 100 Mbps. The router's Internet access is of 20 Mbps. There is a remote server connected to a 10Mbps LAN. The propagation time inside the Wireless LANs or the LAN can be despised and for the WAN the time is 200 ms. The terminal, initially connected to Wireless LAN1, establishes a connection to ServerA's chargen server. The client assigns a receiver buffer of 32KB. The MSS (Maximum Segment Size) is 1000 Bytes. The maximum size of the congestion window is 64 KB so $Kt = \text{MIN}(64\text{KB}, \text{adwnd}, \text{cwnd})$. Switches' buffers, Access Points and routers are considered infinite..



- a) Draw the evolution of the transmission window, advertised window and congestion one, indicating the values of the advertised, congestion and transmission window and the threshold and the state of the congestion control (SS or CA) at the most important moments.
- b) Which is the average throughput once the transitory phase is finished?
- c) Which will be the effect of increasing the receiver buffer from 32KB to 64KB?

The terminal is moved around the Wireless LAN₁ coverage area until it loses connection to Access Point AP₁. When it will enter Wireless LAN₂ coverage area, the terminal registers a new AP₂ and continues the communication. While the terminal registers AP₂, it cannot receive the packets that were sent to AP₁, because there is no coverage with the AP and cannot receive them from AP₂, because the AP is still not registered. The process of moving through one coverage area to another is called "handoff". We will assume that the process takes 0,5 seconds. We will keep our assumptions "infinite buffers for all devices" and "32KB for receiver buffer".

- d) How many segments can get lost through the handoff process (maximum number)?
- e) Draw the evolution of the transmission window, advertised window and congestion one, indicating the values of the advertised, congestion and transmission window and the threshold and the state of the congestion control (SS or CA) at the most important moments in case the receiver buffer at the client has 32KB. Assume that the client has been receiving data for a few seconds and draw the moment before the handoff happens, until the needed time for the connection to stabilize.
- f) Which will be the effect of increasing the receiver buffer from 32KB to 64KB?

We assume that the connection is UDP instead of TCP and all buffers have an infinite size. We transmit 50MB of information from server to client. Just after starting the UDP connection a handoff takes place.

- g) How many bytes are lost due to the handoff?

CHAPTER 3: Point-to-point protocols

```

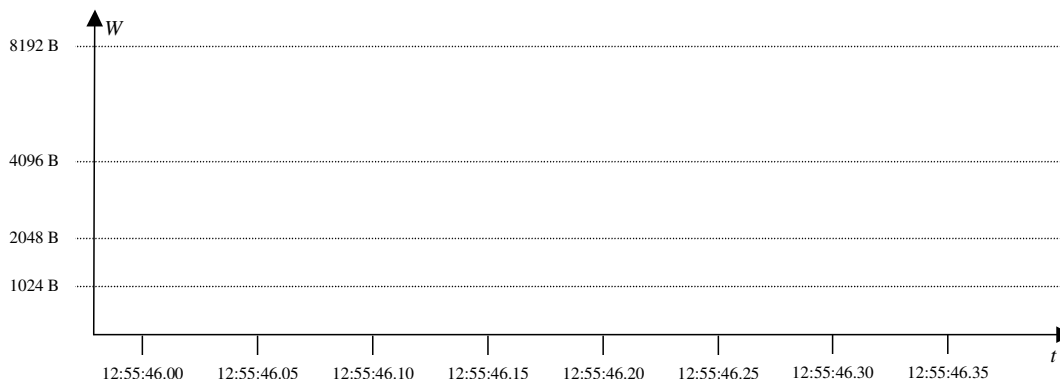
12:55:45.92 PC1:1025 > Serv2:80: S 3125459530:3125459530(0) win 255 <mss 536>
12:55:45.92 Serv2:80 > PC1:1025: S 2025570752:2025570752(0) ack 3125459531 win 32736 <mss 1460>
12:55:45.98 PC1:1025 > Serv2:80: . ack 1 win 65534
12:55:45.99 PC1:1025 > Serv2:80: P 1:103(102) ack 1 win 65534
12:55:46.00 Serv2:80 > PC1:1025: P 1:537(536) ack 103 win 32736
12:55:46.03 PC1:1025 > Serv2:80: . ack 537 win 64998
12:55:46.03 Serv2:80 > PC1:1025: . 537:1073(536) ack 103 win 32736
12:55:46.03 Serv2:80 > PC1:1025: . 1073:1609(536) ack 103 win 32736
12:55:46.07 PC1:1025 > Serv2:80: . ack 1073 win 64998
12:55:46.07 PC1:1025 > Serv2:80: . ack 1609 win 64998
12:55:46.10 Serv2:80 > PC1:1025: . 1609:2145(536) ack 103 win 32736
12:55:46.10 Serv2:80 > PC1:1025: . 2145:2681(536) ack 103 win 32736
12:55:46.10 Serv2:80 > PC1:1025: . 2681:3217(536) ack 103 win 32736
12:55:46.11 Serv2:80 > PC1:1025: . 3217:3753(536) ack 103 win 32736
12:55:46.12 PC1:1025 > Serv2:80: . ack 2145 win 64998
12:55:46.12 PC1:1025 > Serv2:80: . ack 2681 win 64998
12:55:46.12 PC1:1025 > Serv2:80: . ack 3217 win 64998
12:55:46.12 Serv2:80 > PC1:1025: . 3753:4289(536) ack 103 win 32736
12:55:46.13 PC1:1025 > Serv2:80: . ack 3217 win 64998
12:55:46.13 Serv2:80 > PC1:1025: . 4289:4825(536) ack 103 win 32736
12:55:46.13 PC1:1025 > Serv2:80: . ack 3217 win 64998
12:55:46.30 Serv2:80 > PC1:1025: . 4825:5361(536) ack 103 win 32736
12:55:46.32 Serv2:80 > PC1:1025: . 3217:3753(536) ack 103 win 32736
12:55:46.33 PC1:1025 > Serv2:80: . ack 5361 win 64998
# ... deleted lines
12:55:57.32 Serv2:80 > PC1:1025: . 15217:15753(536) ack 103 win 32736
12:55:57.32 Serv2:80 > PC1:1025: . 15753:16289(536) ack 103 win 32736
12:55:57.63 PC1:1025 > Serv2:80: . ack 15217 win 536
12:55:57.63 Serv2:80 > PC1:1025: . 16289:16825(536) ack 103 win 32736
12:55:57.63 Serv2:80 > PC1:1025: . 16825:17361(536) ack 103 win 32736
12:55:58.93 PC1:1025 > Serv2:80: . ack 15753 win 0
12:55:58.93 PC1:1025 > Serv2:80: . ack 17361 win 536
12:55:59.03 Serv2:80 > PC1:1025: F 17361:17361(0) ack 103 win 32736
12:55:59.03 PC1:1025 > Serv2:80: . ack 17362 win 32736
12:55:59.03 PC1:1025 > Serv2:80: F 103:103(0) ack 17362 win 32736
12:55:59.05 PC1:1025 > Serv2:80: F 103:103(0) ack 17362 win 32736
12:55:59.06 Serv2:80 > PC1:1025: . ack 104 win 32736

```

Problem 8.

The previous output corresponds to the download of an HTTP/1.0 web between client PC1 and server Serv2. Answer the following questions justifying your answer and writing down all your assumptions.

- a) Say the size in bytes of the http request sent by the client and the one for the downloaded page.
- b) Which is the downloading effective speed?
- c) Draw a temporal diagram indicating the states taken by the client PC1 and the server Serv2. It is not necessary to specify the different moments, just indicate the states in the diagram and the important segments and their flags.
- d) Say which segments have been lost.
- e) Draw the evolution of the window size from the connection to the suspension points. Indicate which is the slow *start threshold* (*ssthreshold*).



Problem 9.

We have a TCP connection that broadcast from system pcA to pcB with all segments full (filled with MSS bytes) from pcA to pcB . From pcB to pcA the segments are just confirmations.

Notes: Assume the LANs and all links are infinitely fast, TCP does not use the option *window scale* (this option multiplies the advertised window by a factor) and the $MSS=1$ kB. A ping command from pcA to pcB result is 100ms. Answer the following questions justifying your answer and writing down all your assumptions.

- a) Assume there are no losses. Which will be the broadcasting effective speed of a permanent regime?
- b) Now assume that while there is permanent regime a segment is lost each time the congestion window arrives to 4 MSS, and the lost segment is always rebroadcasted because the rebroadcasting timer interrupts. Draw a sketch of the evolution of the window in permanent regime, calculate the approximate effective speed using the draw.

CHAPTER 4: Local Area Networks

Problem 1.

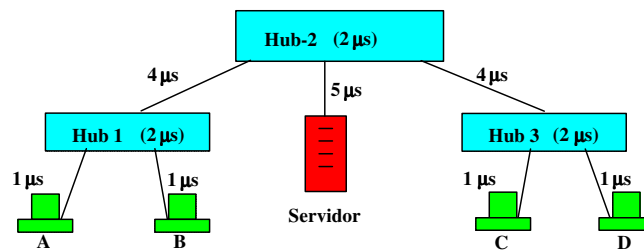
Which is the effect of an accidental disconnection of a 10Base2 bus in a LAN? (Disconnection implies that the bus is split in two halves).

Problem 2.

There is an Ethernet 100BaseT Hub. The network introduces the following delays: $70 T_b$ (Bit Time, $T_b=1/V_t$) for the Hub, $25T_b$ for the stations' network adapters and $0.5 T_b/\text{meter}$ (optical fiber) for the cables. If the collision window (time of vulnerability) is $512 T_b$: Which is the maximum length for the station connection if we keep a margin of $4 T_b$? The margin is an added delay to all the others to ensure a better network running in case the cables length is too adjusted.

Problem 3.

There is an Ethernet network with three 10BaseT hubs each (see figure). The delays in broadcast lines and hubs are indicated in the figure (which are the delays for a bit broadcasted in the network). The duration of a frame is variable ($L_t \geq 64$ octets), the duration of the Jamming signal (interference signal) is 32 bits.



Station A broadcasts a frame at moment T_0 with a request to the server, and the station C does the same at $T_0+10 \mu\text{s}$.

- a) Draw a temporal diagram for the interval time between T_0 and $T_0+200 \mu\text{s}$ indicating what happens to these frames if only stations A and B broadcast and the first back-off applied by the MAC to station A is 0 times the slot of times of CSMA/CD and station C is 1 time the slot of times (remember that the back-off time = $T_{\text{slot}} * \text{RND}(0, 2^{\min(N,10)} - 1) \mu\text{s}$ and T_{slot} is $512 T_b$). Indicate and explain all the events that occur in this interval of $200 \mu\text{s}$.

Problem 4.

Fast Ethernet technology increases the broadcasting speed of the Ethernet from 10 to 100 Mbps. However, it does not modify the level of access to the environment. Gigabit Ethernet technology increases the speed up to 1000 Mbps. However, this one modifies the behaviour at MAC level increasing the minimum frame size from 64 octets to 512 octets. Give a possible explanation to the increase of the minimum frame size. (Note: the typical propagation speed is $2 \times 10^8 \text{ m/s}$)

Problem 5.

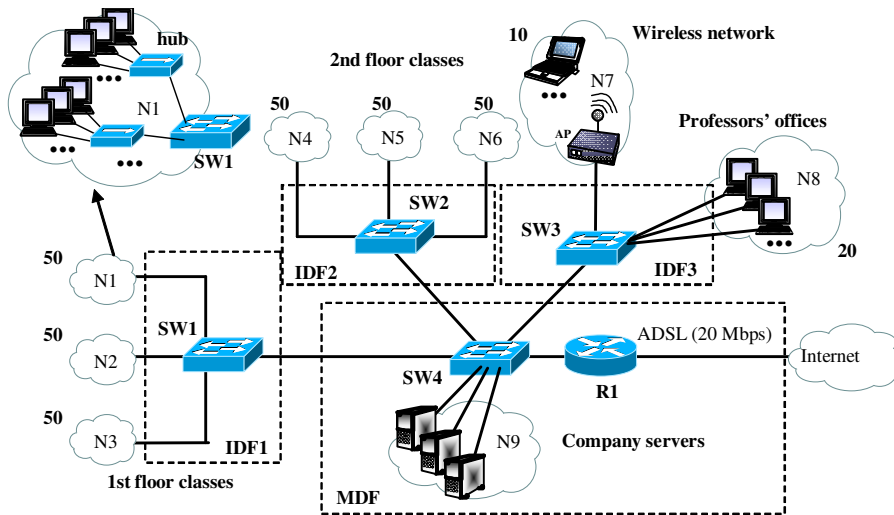
There are two Fast Ethernet switches with 8 ports of 10/100 (Mbps) FDX each and auto negotiation (it detects if the card is a 10 or 100 one). We have 10BaseT hubs of 4, 8, 12, 16 and 24 ports (as many as hubs you want). The network has a router with 2 ports (one is Fast Ethernet and the other to Internet connection) and 6 servers with adapters 10/100. We have to give connectivity to 72 users guaranteeing a minimum of 750 Kbps for each user in the worst case.

- Justify how many hubs of which type do you need to connect 72 users with the indicated speed.
- Design a network drawing a clear schema (an understandable schema will be valued) that follows the described requisites and only uses the listed devices.
- How many collisions domains have you created to the users? Justify your answer.
- If you wanted to guarantee a minimum of 1 Mbps, Which will be the maximum number of users you could connect, to which hubs and how many should you put? (Remember: only use the devices listed before)

Problem 6.

We have two stations over an Ethernet network that have established a Stop & Wait connection. The Ethernet network is composed by a hub. Which will be the effect of substituting the hub by a switch? Do a numeric evaluation in both cases. (Note: Assume that there are no more active stations). Explain the factors that cause the delay introduced by the switch.

Problem 7.



A company that works teaching adults (offers courses to access the university to people over 25 years old, office, accounting, etc) is located in a three floored building. The network is composed by 330 terminals distributed as follows:

- Floor 0 has a meeting room that has an AP at 54 Mbps, wireless network N7, with 10 terminals. There are also shared offices for teachers with 20 terminals directly connected to switch SW3 (net N8) and a room to keep the company servers: web, disk, ft, email, directly connected to switch SW4 (net N9).
 - Floors 1 and 2 are similar. Each floor has 3 classrooms dedicated to theory and practical teaching (nets N1-N6). Each net has 50 terminals connected to fast Ethernet hubs, which are connected to switches (see detail of net N1)
 - Network devices (switches, routers, hubs and servers) are distributed over 4 telecommunication rooms (shown in the diagram as IDF1-IDF3 and MDF). The figure shows all network switches (SW1-SW4) and router (R1). The links between IDFs and between SW4 and R1 are full duplex Gigabit Ethernet made of optic fiber. All servers are connected to SW4 by a full duplex full duplex Gigabit ethernet. All the other switch's ports are UTP full duplex fast Ethernets.
 - Each network N1-N9 builds a subnetwork with different IP addresses. The terminals can communicate with the Internet or the servers.
- a) Keeping in mind that a minimum number of VLANs and trunk links have been defined, say which VLANs (identifying them with the following notation VLAN1, VLAN2...) and trunk links (identified by a switch SW1...) must have been defined in each switch.
 - b) Assume (only for this section) that switches do not do trunking. Explain the changes that should be done to compose a network with just 1 router and the same subnets. Your solution should minimize the number of links between telecommunication rooms and number of devices in the network. Clearly indicate the devices, ports and links that should be added to the figure.
 - c) Calculate how many hubs and ports are necessary in each network N1-N6 in case all the terminals in the same network (for example N1) broadcast a file to the server at the same time, hubs do not become the bottleneck. Indicate which will be the bottleneck in this case. Calculate the effective speed in bps that each terminal will reach. Assume a 100% efficiency (collisions do not affect).
 - d) Assume that using the previous hubs, 330 terminals transfer a file at the same moment to the same server. Explain which is the bottleneck, if there will be losses and which mechanisms will help the different stations to adapt the effective speed to the speed imposed by the bottleneck. Comment all suppositions made.
 - e) Having in mind the previous answer, calculate the effective speed in bps that will reach: (i) one terminal of each network N1-N6, (ii) each professor's terminal and (iii) each terminal in the wireless network. Assume a 100% efficiency (collisions do not affect). Comment all suppositions made.

CHAPTER 5: Data Transmission

Problem 1.

Answer the following questions:

- Define thermic noise and (S/N).
- The receiver has a (S/N) = - 20 db, quantify how high is the power according to the noise.
- Due to having the same bandwidth at the channel, Bw_c , whenever the channel capacity increases the relation S/N increases from 20 dB to 40 dB?

Problem 2.

- Explain how can we increase the modulation speed of the link and which is the theoretical maximum.
- Explain how can we increase the broadcast speed of the link and which is the theoretical maximum.
- Calculate the different values in a channel with bandwidth 1 MHz, relation signal / noise 30 dB, with digital broadcasting of 8 symbols and a time per symbol of 1 μ s.

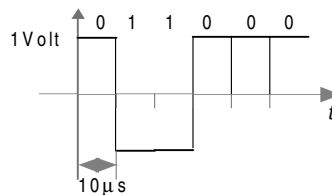
Problem 3.

The receiver of the terminal equipment of the data circuit (DCE) requires a minimum signal power of 1mW (receiver sensibility). The environment attenuation is 2dB/Km and the distance between transmitter and receiver is 100Km

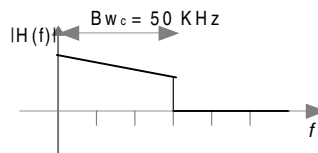
- Which is the necessary power for the transmitter equipment?
- We have repeaters (electronic amplifier) with a sensibility of 1mW and a maximum emitting power of 1W. How many repeaters are needed?

Problem 4.

- Indicate the type of codification, the modulation speed and the broadcast speed of the signal in the figure. The signal has a Bw_s of 50 KHz.



- If a signal is sent through a channel using a transmission function as the one in the figure, having the receiver a sensibility of 1mW and a noise power of 1 μ W, say if there will be distortion and if the bit errors rate will increase due to the maximum broadcasting speed being exceed.



Problem 5.

We have an AMI encoder that transmits symbols at three different potential differences: -10 volts, 0 volts, +10 volts. Each symbol carries a bit of information. The time to transmit a symbol is $t_s = 0,1$ ms.

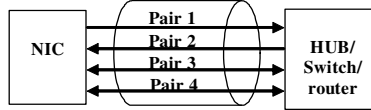
- Draw the signal that results of the transmission of the following sequence of bits: 0101011001. Indicate in the datagram the value of t_s .
- Say which is the broadcasting speed in bps.
- Assume that the environment attenuates 3 dB. Say which will be the 3 different potential differences for the received symbols.
- Say if the signal could be transmitted through an environment that eliminates the continuous component, explain why.
- Assume that the value of t_s can be modified. What value should it take if we want to increase 10 times the broadcasting speed?

CHAPTER 5: Data Transmission

- f) Explain how will the signal's bandwidth will change if the value of t_s takes the value calculated in the previous section.
- g) Assume encoding is used to broadcast 8-bit characters adding a parity bit for each character. Say if the synchronism problem of the encoding bit could be solved adding a parity bit odd or even.

Problem 6.

Fast Ethernet 100BaseT4 standard uses 8B6T codification (each 8 bits are codified with 6 symbols with levels: 0, +V and -V volts). In this Standard, during the broadcast 3 of the 4 twisted pairs of UDP cable are simultaneously used as it is shown in the figure (two pairs are used unidirectionally and two bidirectionally).



Transmission direction of the twisted pairs in a 100 Base T4 UTP cable

- a) Which is the broadcasting speed for each pair?
- b) Which is the modulation speed for each pair?
- c) If a different combination of bits is assigned to each different combination of symbols, how many different combinations of bits there will be? How many symbol combinations are not useful?
- d) In order to have bit synchronism, which symbols combinations you will NOT choose? Why?
- e) Using the Nyquist criterion, estimate the bandwidth of the transmitted signal for each twisted pair
- f) Why do you think that three pairs are used to broadcast instead of one?

Problem 7.

Which is the minimum number of bits that code-words must have in a broadcast code which needs to codify 26 letters, 10 numeric symbols and 20 control signs, and, in addition, must include a parity bit?

Problem 8.

Determine the Hamming distance to the following code: 000000 / 001101 / 110100 / 111111 / 101010 / 110011

Problem 9.

Assume that we want to transmit two bits of information using a detector error code CRC with the generated polynomial: $g(x)=x^3+x+1$. Calculate the valid code-words and deduce which will be the Hamming distance of the code.

Problem 10.

A error detector code consists in adding a bit of odd parity to each broadcasted bit.

- a) Say which are the valid code-words and calculate the Hamming distance for the code.
- b) Calculate the probability of having a non-detected error if code-words are transmitted through a channel with a probability of error of 10^{-3} .

Problem 11.

a) Compare the maximum efficiency that can be obtained using the following two configurations:

- Bit oriented broadcasting using blocks of 100 octets in addition to a header of 2 bits, 16 bits dedicated to synchronism (flags) and a CRC of 16 bits.
- Character oriented broadcasting using 8-bit characters. The blocks have 100 characters in addition to a header of 2 characters, 2 characters dedicated to frame synchronism and 1 character of LRC (horizontal and vertical parity).

b) Calculate how long it takes to broadcast 2 Moctets of information in both cases; the broadcast speed must be 19200 bps.