Homework 2, David Rasoly.

Question 1:

A. On Ethernet, and under half duplex assumption, a collision will occur if two (or more) machines will attempt to send packets at the same time via shared link of the network. The network segment on which collusion can occur is deemed a Collision Domain.
A broadcast is an ethernet function which allows broadcasting packets to a network, to all of the machines at the network, have to listen to this broadcast. The network of computers which will receive these packets is called Broadcast Domain.
Both Broadcast Domain and Collision Domain exists when using a Hub, and therefore it is less ideal. On Switch, each port is different, and therefore it is a Collision Domain separator. A Router, is the more ideal as it acts both as Collision Domain and Broadcast Domain separator.

B. I will assume that the desktop computers don't support a wireless communication. In that case, I will purchase another 8 physical slots router from the ISP or any vendor. And will attach it to router provided by the ISP. Then, my choice will be to plug the file and mail servers to the original ISP router, and plug the rest of the 10 computers to the 2 more allotted spots at the original router, and 8 slots of the router that I bought. The reason I chose the servers to be connected to the original ISP router, is due to a point of failure at the connection between the two routers, which could be prevented if servers aren't connected to the new router.

C. I will attempt to answer this question from the course perspective and from my experience - a desktop machine is a working unit which will send and receive data packets only to an office or home router, and from there it will travel via the internet to its destination. A server serves multiple desktop or other server and therefore has to "know" more address, and serve more machine in it's network. From the course material at the past week, I'd imagine that a switching forwarding table of a server is substantially richer than a desktop's.

Question 2:

Traceroute is a command that is used to show technical details about the route that a packet takes from one's computer to the address given as a parameters. It is supported on most modern and common operating systems such as Windows, Linux and Mac OS.

An example of traceroute command from my personal computer to a common website in my country :

```
traceroute to www.google.com (216.58.207.68), 64 hops max, 52 byte packets
 1  192.168.0.1 (192.168.0.1)  3.273 ms  35.070 ms  43.706 ms
 2  10.14.4.1 (10.14.4.1)  40.186 ms  19.144 ms  13.291 ms
 3  172.18.8.66 (172.18.8.66)  19.775 ms  15.572 ms  13.932 ms
 4  212.199.139.153.static.012.net.il (212.199.139.153)  15.296 ms  13.504 ms  14.052 ms
 5  * * *
 6  82.102.132.78 (82.102.132.78)  14.617 ms  14.584 ms  19.952 ms
 7  edge-fra-01-ae3-42.ip4.012.net.il (80.179.166.50)  79.245 ms  101.472 ms
    80.179.166.142.static.012.net.il (80.179.166.142)  84.224 ms
 8  72.14.216.121 (72.14.216.121)  83.493 ms  83.630 ms  83.041 ms
 9  * * *
10  72.14.234.114 (72.14.234.114)  87.727 ms
    172.253.64.118 (172.253.64.118)  82.422 ms
    216.239.48.42 (216.239.48.42)  99.491 ms
11  108.170.252.19 (108.170.252.19)  79.663 ms
    72.14.234.227 (72.14.234.227)  82.167 ms  79.780 ms
12  108.170.228.255 (108.170.228.255)  96.028 ms
    209.85.252.77 (209.85.252.77)  87.122 ms  68.846 ms
13  fra16s25-in-f4.1e100.net (216.58.207.68)  80.210 ms  68.193 ms
    108.170.226.2 (108.170.226.2)  85.310 ms
```

The machine will send three UDP datagrams with time to live (TTL) value which will expire once the first router encountered. Then it will send another sequence of datagram with incremented value to the TTL, and will continue to do so until it arrives to the host input.
The first line suggests that three packets has been sent to to 192.169.0.1, it took the 1st packet 3.273ms to arrive to this router, and the 2nd and 3rd packet took 35.07ms and 43.706ms, respectively. Then, three packets with a TTL of 2, were sent to the next address, until arriving to www.google.com.

Question 3 :

While every Ethernet NIC has a unique Ethernet address, these addresses are part of 2nd layer (DataLink) at the five layer model - a MAC address is used to identify machines at the same broadcast network of the 2nd layer. In order to send messages between computer at the internet, IP protocol should be used, and it is a part of the 3rd layer (Network), at this layer, there is an exposure not for the same network but for external network using routers.

Question 4 :

Since all the hosts are connected to one switch, all of the ports that they are connected to the switch are part of the same switch forwarding table.

1. A creates an Ethernet packet to C, The forwarding table knows now that A maps to port 1, but doesn't know where C is, so it acts like a Hub, and sends the packet to all the other ports, checking their MAC address to see whether they are C or not. Port 3 receives the packet.
2. Host D creates an Ethernet packet and sends a broadcast frame, and sends it. The forwarding table know that D maps to port 4. For the sake of the question, I'd assume that by that time host C received the message from host A.
3. Host C creates an Ethernet packet and send it to A, by that time, the forwarding table knows that A is at port one, and sends it directly to A without checking port 2 and 4.

Question 5 :

To answer this question, I will assume two switches, A and B, each has four ports, from 1 to 4. Switch B, port 4 is connected with a cable to switch A port 1. At ports 3 and 4, Switch A has File Servers that crucial to the business. At ports 1 and 2 of switch B has two desktop computers. If the connection between the two will be broken, the two desktop computer won't have access to the file servers. Therefore, let's connect a cable from Switch B, port 3 to Switch A, port 2. I believe that solution will work, because of the concept we learn regarding switch forwarding table. If two cables are attached, when data packets will travel through the two switch, they will do it only via one of the cables, since only one of them will represent the way to the other. For example, desktop computer of Switch B port 1, will know that the file server is at Switch A port 3, and vice versa. If this connecting cable will be eaten by an evil rat, the desktop computer will look for it once again(this is an assumption which I am not sure that actually works) , and will find the file server, on port 3 of switch B, while traveling through port 2 of Switch A.

Question 6:

A. The three main topologies I chose to describe are these :
    a. Bus - All the machines and devices are connected via backbone cable. The cable should have a terminating point at each end which define the limits of the network and accommodates missed or unrecognized packets. While Bus Topology is easy to install and maintain, it could be hard to troubleshoot errors that happens within it's network.
    b. Star - similar to the answer of the questions 1 and 4, a star has a hub/switch/router which acts as a central point of communication. While it is easy to troubleshoot errors on this topology, it could be more cumbersome to install as it requires more cables.

c. Mesh - All the connecting devices are connected to each other via cable. This topology could only adapt in certain cases of few computers, otherwise there is a waste of bandwidth and it is more difficult to install as the number of computers grows, although these disadvantages, it is easy to troubleshoot errors on Mesh since its a true peer to peer communication.

B. A physical topology describes how the computers and devices are connected within the network physically, that includes the machines themselves, cables and hubs or routers. A logical topology emphasize the way in which the data flows between the network nodes, i.e. switches and routers, instead of the physical machines. A physical ring is a topology in which one computer is connected to two computers, a physical ring of wires could be made of this network. A logical ring is a network on which the computers acts as if they are connected to two computers, and behave as such - but physically they don't have to be connected as a ring.

Question 7 :

Both Cisco Academy & RFC 1122 suggests a 4 layer model, on which the physical layer is missing. In my understanding, the 4 layer model lacks the importance of the electrical "bits" that occur within the network, although it exists within the network access layer.This model is good for understanding the logical and behaviour of the TCP/IP communication. The 5 layer model, or TCP/IP Protocol Suite, separates the physical and data link layer, and give importance of the hardware cables and electrical flow at the model in one hand, and on the other hand let the data link manage the addressing within a network separately. The 7 layer model, also refers as OSI, is extracting the application layer into three layers, and deeply elaborate the inter-communication of data is implemented as presented. In conclusion, it is safe to say that all three models are somewhat built upon the OSI model for TCP/IP, and the 4 and 5 layer models are abstractions which allow to simplify way of allowing connection over TCP IP protocols.