SAMPLE NOTES (copied and pasted random info from the main source, no particular order or structure)

What are circuit-switched and packet-switched networks? Why is there a trend away from circuit switched to packet switched?

Circuit-switched networks are connection oriented. This means that before communication can take place a circuit needs to be established. For example a landline telephone call establishes the circuit when you dial the number and when the receiver answers. That number is the destination of the call and is only needed in call establishment. This circuit is then exclusively used for that call.

With a packet switch network, no connections need to be made. Each packet is placed in the network – the important point is that each packet must carry the destination address with it.

Packet-switched networks make more efficient use of resources. Packet switching is more flexible and uses modern technologies. Telephone calls can be sent over a packet-switched network. Thus we have convergence of these technologies, which is actually everything becoming packet switched.

Abstraction, Manipulation, Axiomatisation, Representation

The 4 pillars of design: Not in any particular order, they are not steps or processes. All examples are in regards to the network layer.

1) **Abstraction**: makes things easier to use because it helps us ignore the details. Gives things a higher level of meaning. Handles complexity by only focusing on essential details and ignoring confusing facts. Example: IP itself is an abstraction of a global network over a whole lot of small networks using different technologies.

Example:

Due to the fact that IP addresses were being depleted on the Internet, IPv6 has been developed. IPv6 is a new form of Internet Protocol that has an increased address size of 128 bits as opposed to IPv4's 32 bits. IPv6 has a simpler packet structure that allows a variety of new approaches to routing and addressing. IPv6 also makes it easier to perform routing and supports a greater number of addressable nodes as well as a simplified header format. IPv6 makes it easier for the target audience (users) without supplying the complex information.

2) **Manipulation**: How the information is manipulated and used by the system (basically how it all works). With the IP example, manipulation is what the routers do with the representations to make the whole thing work so they can send packets through the network.

Example:

A good example of manipulation is the way routers connect multiple subnets. The purpose of this is so that each subnet has a separate address. It works perfectly for LANs. However, without routers,

the multiple subnets would not be able to communicate. The routers must have one address in each subnet to allow communication. Any portion of an IP address can be designated as a subnet by using a subnet mask. But it is the routers that allow manipulation.

(Purchase the full notes for the rest of the design pillars!)

Example questions: (hint: these could be exam questions)

Does a switch store the MAC addresses or the IP addresses of the nodes to which it is connected?

Switches only store the MAC addresses. Hubs do not store any MAC addresses - why? Switches only deal with layer 2, thus IP addresses are not known at all, but are just part of the data passed across.

Once CSMA/CD detects a collision how long must the two senders wait before resending their messages? Why?

When a collision occurs, the sending stations must wait until the line is cleared. When the line is clear both stations cannot send again or the collisions will continue to happen. Thus they must wait a different amount of time so that another collision does not occur.

Briefly explain why most LANs use MAC addressing rather than IP addressing for internal messages. Give at least 2 reasons.

LANs operate at layer 2. They are only responsible for sending a message from one node to another – that is a single step on the path. IP addresses are concerned with the entire route that a message takes.

Subnet Mask

Network IDs & host IDs within an IP address are distinguished by using a subnet mask.

A subnet mask is 32 bits that:

- → Mask a portion of the IP address to separate the network ID from the host ID
- → Specify whether the IP address is located on the local or remote network
- → Each host on a TCP/IP network requires a subnet mask

A 32-bit mask uses consecutive bit groups of all ones (1) to identify the network ID and all zeroes (0) to identify the host ID portions of an IP address.

The subnet mask used with the class B IP address:

- → 131.107.16.200 is the following 32-bit number:
  - 11111111 11111111 00000000 00000000
  - 255.255.0.0

- → The class A mask is: 255.0.0.0

→ The class B mask is: 255.255.0.0
→ The class C mask is: 255.255.255.0

Once you have the subnet mask, it is easy to get a network address from an IP address. There are 2 methods:

→ Where there are 1s in the subnet mask, copy the IP address
    - Where there are 0s in the mask, put 0s
→ Or use the AND process:
    - Convert the IP to binary, and the AND the IP with the mask
    - 1 AND 1 = 1, anything with 0 = 0.
→ Example:
    - IP address **class B** 189.17.15.4
    - Mask = 255.255.0.0
    - Therefore, network ID = 189.17.0.0 (method 1)
    - Method 2 =
        - 1011 1101 . 0001 0001 . 0000 0111 . 0000 0100
        - AND
        - 1111 1111 . 1111 1111 . 0000 0000 . 0000 0000
        - = 1011 1101 . 0001 0001 . 0 . 0

Other examples of subnet masks include:

→ Subnet: 149.61.10.x. x = 0-255. (x = 0 for mask)
    - Subnet Mask: 255.255.255.0
→ Can't have networks with 2 hosts
    - 2 addresses in each network are the 1st address = all 0s: network ID, last address = all 1s: broadcast address.

Subnet Mask '/' (slash) notation:

Represents where the division between network ID and host ID is.

Examples:

/1 = 128.0.0.0 (can also be written as 128.0/1)

/2 = 192.0.0.0 (or 192.0/2)

/5 = 248.0.0.0 (248.0/5)

/10 = 255.192.0.0 (255.192/10)

/30 = 255.255.255.252 (max)

For each of the following state whether it is a wired or wireless media and give its approximate range:

a) Infrared

- Wireless, a few metres

b) Microwave

- Wireless, line of sight, hundreds of km's

c) Twisted Pair cable

- Wired, 100m+

d) Optic fibre

- Wired, 10-100km

In the context of the physical level of the Internet protocol stack, briefly explain the difference between *bit* and *baud rates.*

The terms bit rate (i.e. the number bits per second transmitted) and baud rate are used incorrectly much of the time. They often are used interchangeably, but they are not the same. In reality, the network designer or network user is interested in bits per second because it is the bits that are assembled into characters, characters into words and, thus, business information.

Because of the confusion over the term baud rate among the general public, the term baud rate be replaced by the term symbol rate. The bit rate and the symbol rate (or baud rate) are the same only when one bit is sent on each symbol. For example, if we use amplitude modulation with two amplitudes, we send one bit on one symbol. Here the bit rate equals the symbol rate.

Define "Bandwidth":

Bandwidth is the difference between the highest and lowest frequencies in a band. In common usage, *bandwidth* refers to circuit capacity; when people say they need more bandwidth, they need a higher transmission speed.

Backbone Networks

A BN is a network that connects other networks together. It connects other LANs, and subnets together. It could apply for different networks in one building.

On a campus there are several buildings, and connection between buildings is don't via a BN. Look at a BN as a campus network and less of a nation-wide network (leave that for WAN).

L3 Switch vs. Router:

Layer 3 switches are routers with fast forwarding done via hardware.
The key difference between Layer 3 switches and routers lies in the hardware technology used to build the unit. The hardware inside a Layer 3 switch merges that of traditional switches and routers, replacing some of a router's software logic with hardware to offer better performance in some situations.

Layer 3 switches often cost less than traditional routers. The major difference between the packet switching operation of a router and a Layer 3 switch is the physical implementation. In general-purpose routers, packet switching takes place using a microprocessor, whereas a Layer 3 switch performs this using application specific integrated circuit (ASIC) hardware.

A Layer 3 switch can support the same routing protocols as network routers do. Both inspect incoming packets and make dynamic routing decisions based on the source and destination addresses inside. Both types of boxes share a similar appearance. Therefore, a L3 switch could route (router functions), and perform as a switch.

Backbone Network Architecture:

Routed Backbone:

A routed backbone is ..... *(all the info is in the full notes!)*

Switched Backbone (or bridged backbone):

Switched backbone networks use a ……. *(all the info is in the full notes!)*

VLAN:

Perhaps that there are some employees from the same department of the company that are not physically connected to the same LAN. This is where the virtual LAN comes into action. In computing terms, virtual ..... *(all the info is in the full notes!)*

Explain the following VLAN types:

- → MAC based
- → IP based
- → Protocol based