Assignment 1

Data communication

Assignment 1

Q1.

A.

Managed (learned about managed switches in practical class week 8)

In any network, switches play the role of connecting devices and making sure packets in traffic are sent to the right destination. Managed switch gives control over how the relavent network behaves. One of its main advantages is the ability to create VLANs, which separate a single network into isolated groups. For example, in a university, lecturers could be placed in VLAN 15 and students in VLAN 100. This stops one group from seeing the other's traffic and keeps the network more secure. Managed switches also let administrators set up security measures such as limiting how many devices can connect to a port, or using access lists to filter unwanted traffic. They also reduce unnecessary broadcast traffic and make it easier to grow a network without having to add extra hardware.

Unmanaged (learned about Unmanaged switches in practical class week 8)

An unmanaged switch works very differently. It uses a plug and play device with zero configuration needed. You can connect a PC or any other device, and it will start working right away. To check the connection, you can simply use the ping command to test between devices. While this is quick and convenient, unmanaged switches offer no way to separate traffic or control how the network is used. In small spaces like a café, where you may only need to connect a PC, a CCTV camera, and a POS system, this is usually fine. But in a large organization, unmanaged switches are not secure or efficient, since every device ends up in the same network with no control over traffic.

B.

Managed (learned about managed switches in practical class week 8)

With a managed switch, things work differently. Here, I can create VLANs that split one physical switch into several logical networks. Each VLAN usually has its own IP range. For instance, computers in VLAN 15 might use addresses like 192.168.15.Y. while those in VLAN 100 might use 192.168.100.Y. Devices inside the same VLAN can talk to each other, but if a device from VLAN 15 wants to talk to one in VLAN 100, that traffic must go through a router/Layer 3 switch to reach the destination. This makes addressing more structured and gives administrators more control over security and performance

Unmanaged (learned about Unmanaged switches in practical class week 8)

Network with an unmanaged switch, all the connected electronic devices are kept in a same group/broadcast domain. This means every computer, printer, or phone connected through it will normally share the same subnet and receive their IP addresses from the home router. It is simple to set up because there is no configuration involved, but this also means there is no control over how addressing is organised. All devices can freely communicate with each other, which is fine for homes or very small offices, but it becomes messy and less secure when the network grows.

C

A manufacturer is simply the company that builds a network device, like a router, switch, or even the network card inside a computer. Every network card or Wi-Fi adapter comes with its MAC address, which is a distinct code used to identify it on a network. The first part of that code is made up of the first six characters, which is called the Organizationally Unique Identifier (OUI). For example, if you look up the OUI, you might find out to which company.

I referred to these two websites to get the manufacturers of the respective MAC addresses (**publicly available websites**)

https://standards.ieee.org/products-programs/regauth/mac/

https://chatgpt.com/c/68cfb5c2-2f94-8323-ab94-e95a1862c277 (for learning about manufacturers)

https://wireshark.askapache.com/tools/oui-lookup.html

When looking at the manufacturer table, you can see that the network is made up of equipment from a wide range of companies. In the Sydney CBD office, there are older machines such as a PC from Acorn Computers Limited and another from Commodore, while Nortel Networks and Avaya provide the phones and a couple of PCs. There is also an Atari Corporation PC listed, which shows the mix of legacy devices still connected. Switching at this site is handled by an unmanaged Netgear switch with several ports, and the routing is done by The Linksys Group, Inc.

At the Mascot site, most of the core infrastructure is built on Cisco-Linksys routers and HP ProCurve managed switches. The servers are a mix of Dell and Digital Equipment Corporation, alongside a Next, Inc. printer, a Canon PC, and even an IoT device registered under The Coca Cola Company.

Across the WAN, most of the routers come from Cisco Systems, Inc., but there are also entries from Juniper Networks and 3Com. Finally, at the Macquarie Park data centre, Cisco continues to provide the routing, while Pica8 and Big Switch Networks handle switching. The servers here are again mostly Dell, and a full set of training PCs are manufactured by Apple, Inc.

D.

The speed of transfer in this network is decided by the type of port being used. The most common ones are FastEthernet and GigabitEthernet, while FastEthernet transfers at 100 megabits per second, while GigabitEthernet transfers at 1000 megabits per second. So if a PC is connected through a Fa0 port, it will normally work at 100 Mb per second. If it is connected through a Gi port, it will reach 1 Gb per second.

Some devices in the table use Ethernet0, which usually supports either 10 Mb per second or 100 Mb per second, depending on the hardware used. Printers and IoT devices often fall into this category. Hubs, when mentioned they are a bit different because they still work on older technology, usually 10/100 Mb/s, but in half-duplex mode they can either send or receive at one time. On the other hand, switches are full duplex so they allow traffic in both directions at once.

The actual link speed depends on the lowest speed supported at both ends. For example, if you connect a Gigabit router port to a Fast Ethernet switch, the link will only work at 100 Mb/s. Cable type matters too. Cat5 cables may not always handle gigabit, while Cat5e or Cat6 cables are needed for higher speeds.

In short, almost all of the variation in this network comes down to whether the port is FastEthernet/ GigabitEthernet. The only exceptions are a few older Ethernet0 ports and hubs, which may run at lower speeds.

https://www.youtube.com/shorts/csxqTjZbdAk

https://www.geeksforgeeks.org/computer-networks/difference-between-fast-ethernet-and-gigabit-ethernet/

Q2

- VLSM Design for 192.168.23.0/25
- That block contains 128 addresses in total (host range 192.168.23.1-192.168.23.126).
- Allocate the block 192.168.23.0/25, which contains 128 IP addresses (126 usable). My task is to divide this block into smaller subnets for the main office and the suburban offices at Parramatta, Chatswood, and Hurstville. Since each site has a different number of users, I am using Variable Length Subnet Masking (VLSM).

Step 1: Work out the host requirements

I assume the following host counts based on this scenario:

- Head Office (HQ): about 50 devices
- Parramatta: about 30 devices
- Chatswood: about 14 devices
- Hurstville: about 6 devices
- Two point-to-point links for router connections: 2 devices each

Step 2: Match subnets to needs

I now calculate the smallest subnet that fits each group:

- 50 hosts - needs 62 usable - 26 (64 addresses, 62 usable)
- 30 hosts - needs 30 usable - 27 (32 addresses, 30 usable)
- 14 hosts - needs 14 usable - 28 (16 addresses, 14 usable)
- 6 hosts - needs 6 usable - 29 (8 addresses, 6 usable)
- Router links - 2 usable - 30 (4 addresses, 2 usable)

Step 3: Allocate the addresses in order

- HQ - 192.168.23.0/26
  Network: 192.168.23.0 Broadcast: 192.168.23.63 Usable: 192.168.23.1-62
- Parramatta - 192.168.23.64/27
  Network: 192.168.23.64 Broadcast: 192.168.23.95 Usable: 192.168.23.65-94
- Chatswood - 192.168.23.96/28
  Network: 192.168.23.96 Broadcast: 192.168.23.111 Usable: 192.168.23.97-110
- Hurstville - 192.168.23.112/29
  Network: 192.168.23.112 Broadcast: 192.168.23.119 Usable: 192.168.23.113-118
- Point-to-point A - 192.168.23.120/30
  Network: 192.168.23.120 Broadcast: 192.168.23.123 Usable: 192.168.23.121-122
- Point-to-point B - 192.168.23.124/30
  Network: 192.168.23.124 Broadcast: 192.168.23.127 Usable: 192.168.23.125-126

https://www.computernetworkingnotes.com/ccna-study-guide/subnetting-tutorial-subnetting-explained-with-examples.html (referred for subnetting and how to allocate IP accordingly)

Also learned about IP in week 4,5 practical class.

Q3

A.

When I am using a ping command to communicate from PC1 in Sydney CBD to Printer2 subnet at Mascot. The ping command generates ICMP Echo Request packets that must travel from PC1's subnet in Sydney to the subnet at Mascot, where Printer2 lives. Since this is the very first communication, all ARP caches (on PCs and routers) and all switch tables are empty, so the network has to do some groundwork before the ping succeeds

Step 1:

PC1 creates an echo request containing:

- Source IP = PC1 IP address (Sydney subnet)
- Destination IP = Printer2 IP address (Mascot subnet)
- PC1 quickly checks if the destination Printer is on the same network. Since it is not, the packet must be sent to Router1.

PC1 broadcasts an ARP request

- Ethernet frames need MAC addresses to work on the local LAN
- Every device on the Sydney CBD subnet sees the request (PC0, PC2, IP Phones, Hub, Switch, Router1).
- Only Router1 recognizes that the ARP request is for its IP address.
- Now PC1 knows: Router1-IP <-> Router1-MAC.

ARP cache gets updated:

- PC1 stores this mapping for a certain time.
- This way, PC1 won't need to broadcast ARP again for every ping packet
- When the switch sees PC1's ARP broadcast, it records PC1's MAC on the port where PC1 is connected.
- The switch records when Router1 replies to Router1 MAC on the port where Router1 is connected.

Now PC1 can encapsulate the ICMP Echo Request into an Ethernet frame with:

- Source MAC = PC1 MAC
- Destination MAC = Router1 MAC

Step 2:

Forwarding at Router1

- Router1 strips the Ethernet header to look for the IP header.
- Destination IP = Printer2 (Mascot subnet). Router1 knows the next hop to reach Mascot.
- Router1 must now forward the packet. But like PC1, if Router1 does not know the MAC of the next-hop router, and it sends an ARP broadcast on that subnet

Step 3

ARP updates the MAC table

- At each hop (Router1 -> Router2/Router3 -> Router4/Router7 -> Router6 -> Printer2), the same pattern repeats
- Router checks its routing table.
- When is ARP cache is empty, it sends ARP requests to learn the MAC of the next device.
- Switches in the path update their MAC tables as they see traffic arrive, linking each source MAC to the correct switch port.
- Slowly, all devices along the path build up ARP caches (IP <-> MAC mappings) and switch MAC tables (port <-> MAC mappings).

Arrival at Printer2

- Eventually, the ICMP Echo Request frame reaches Printer2's switch in Mascot.
- The switch has learned where Router6's MAC is and forwards the frame to Printer2.
- Printer2 replies with an ICMP Echo Reply, reversing the process back to PC1.

Step 4:

Now the caches are full:

- PC1 knows Router1's MAC.
- Routers know the MAC addresses of their neighbors.
- Switches know which ports lead to which MACs.

I learned about routers, switches, the network layer, transport layer in my lecture, as well as practiced ping (CLI connecting in a network) in the lab in week 8.

https://www.youtube.com/watch?v=uyRtYUg6bnw (referred for subnetting)

https://www.youtube.com/watch?v=qulRjRFavJI (referred for subnetting)

B. (Learned in lecture and practical class week 4,7, and 8)

- Looking at the appendix, Router1 in Sydney can reach Router6 in Mascot through two paths.
- Path 1 (WAN1): Router1 -> Router2 -> Router4 -> Router6.
- Path 2 (WAN2): Router1 -> Router3 -> Router5 -> Router7 -> Router6.
- WAN1 has fewer hops (only three routers between Sydney and Mascot).

- WAN2 has more hops (four routers in between).
- Because routing protocols usually prefer the shortest or least-cost route, WAN1 is the path that will be chosen under normal conditions.
- WAN2 still serves an important role. If WAN1 fails (for example, Router2 or Router4 goes down), the routing tables will update, and traffic will be rerouted through WAN2. This ensures connectivity is maintained, but at the cost of extra hops and possibly higher delay.