Computer Networks

Assignment 1

Unit 09

George Hotten

Task 1

What are the different types of networks?

Local Area Network (LAN)

A LAN is a network where 2 or more devices are connected. LANs usually cover a small geographical area. For example, a house/small group of buildings.

Wide Area Network (WAN)

A WAN is a network that contains 2 or more LANs. These networks are usually opened by telecom companies, creating the internet. WANs usually cover a large geographical area.

Personal Area Network (PAN)

A PAN is a network that connects devices close to a user together. These networks usually connect devices such as a wireless mouse, keyboard, and a computer. PANs usually range from a few centimetres to a few meters.

What are the different network topologies?

Star

All devices connect to a switch which connects to a central server which can provide services such as file sharing and account logon.

What if a cable breaks?

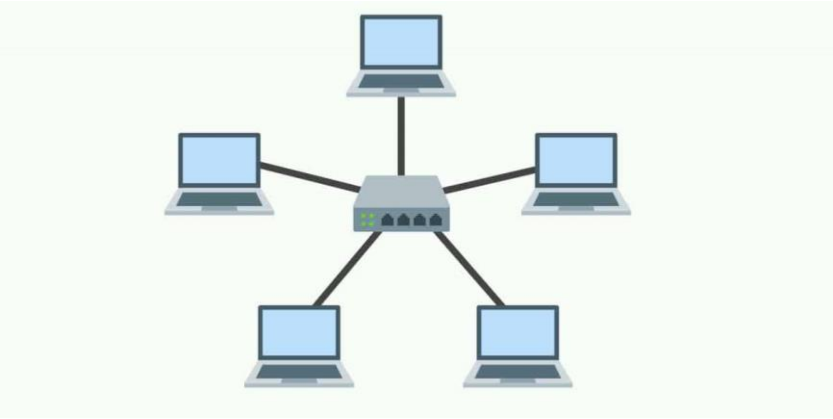
This depends on where the cable is: if the cable is connecting a node to the switch, that single node will go offline. If it’s the cable connecting the switch to the server, all nodes go offline.

What happens if a computer fails?

If the computer is a node of the network, the network will be unaffected. If the server fails, the entire network will go offline.

What if there is excessive traffic?

As the switch knows where to route all packets to each node, the performance shouldn’t degrade too badly when it comes to sending and receiving data. However, if the server must process a large amount of data this may increase load and wait times.



Ring

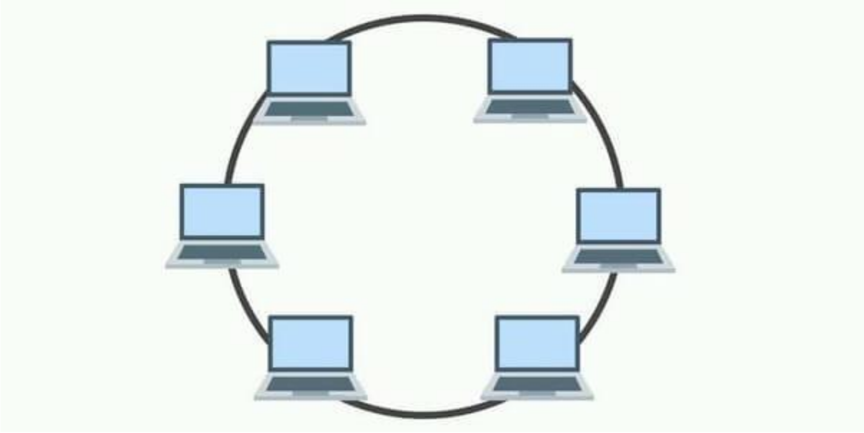
All devices are arranged in a circle and data travels around the circle. Each node has 2 devices connected to it, to send data the data travels to each device until it reaches the one it's intended for.

What if a cable breaks or a computer fails?

As data travels around the circle, if a component fails data will not be able to travel past that node as data can only be transmitted in one direction. This means any nodes after the breakage could be completely isolated.

What if there is excessive traffic?

If there is a lot of traffic it may take longer for data to reach the recipient as all nodes check the packets they receive before they forward them on. When there is lots of data being sent, this can take a long time.



Bus

All devices are connected via a single cable running from one end of the network to the other.

What if the cable breaks?

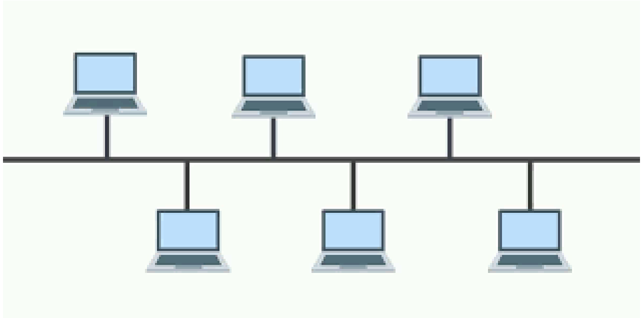
If the cable breaks, it will be impossible to send data meaning the entire network will go offline.

What if a computer fails?

If a computer fails, the rest of the network should be unaffected as data does not need to pass through nodes to be transmitted.

What if there is excessive traffic?

As all data is being transferred on one cable, there will be loads of interference causing packets to go missing or get corrupted meaning wait times for data to be processed can take a very long time.



What are the different network technologies?

Frame Relay

Frame Relay is a technology used to connect LANs and transmit data between endpoints in a WAN.

Multiprotocol Label Switching

MPLS is a technology that forwards data – increasing speed and controls the flow of traffic. Data is directed through a path via labels, rather than a using a routing table.

Asynchronous Transfer Mode

ATM is a communication protocol which transfers video and speech data using a fixed length of ATM cells. This protocol depends on an instantaneous bitrate, or a required one set by the receiving server.

What are the different network access methods?

Carrier Sense Multiple Access

CSMA is a protocol that checks to ensure no other data is being transmitted on a network before it begins its own transmission. This is usually implemented in ethernet based networks. Once the CSMA detects the transmission from other devices are finished, it will start transmitting its own data. This is usually used in ethernet networks – for example a star topology.

Token Passing

Token Passing is used to authenticate devices to transmit data on a network. When a node wants to transmit, it waits until it receives an empty token – it then fills the transmission data into that token and sends it to the network. Nodes constantly monitor the tokens around the network to see if it's the recipient of a filled token. This is usually used in a ring topology.

What are the different network standards?

Wi-Fi

Wi-Fi is the technology used to connect millions of devices to the internet via the transmissions of radio waves back and forth between a router. The said router then uses a wired connection to connect to the internet. Wi-Fi usually operates on 2 frequencies: 2.4GHz or 5GHz.

3G

3G, also known as 3rd generation, is the technology used to connect millions of 'cellular' enabled devices across the world – usually phones or tablets. 3G works through 'cellular' technology where signals are passed from phone tower to phone tower until it reaches the recipient.

Ethernet

Ethernet is the technology used to transmit data through cables such as twisted copper pairs or fibre optic. Ethernet is mainly used for networking, connecting end devices such as computer directly to the router (or through a switch). Ethernet is much faster than Wi-Fi as it is often a direct connection to the router.

What are the different network protocols?

Transmission Control Protocol/Internet Protocol (TCP/IP)

This is a set of protocols used to connect network devices on the internet

Domain Name Server (DNS)

A DNS is a server that takes a URL such as google.com and turns it into an IP that the computer can then use to send web requests to that server.

Dynamic Host Configuration Protocol (DHCP)

DHCP is a protocol that assigns IP addresses to nodes in a network to allow it to connect to other devices. This is often seen in a client-server network configuration.

Hyper Text Transfer Protocol (HTTP)

HTTP is the protocol used when requesting resources from a web server, for example a html file or pictures. This is used in a client-server configuration as all requests are initiated from the client and the server responds to them.

File Transfer Protocol (FTP)

FTP is the protocol used to send and receive files between two devices over a network and/or the internet.

Simple Mail Transfer Protocol (SMTP)

SMTP is the protocol used to send and receive emails between two or more mail servers. This is then retrieved using either the Post Office Protocol or the Internet Message Access Protocol.

Why are network standards and protocols needed?

Networks standards and protocols are needed so devices all around the world can connect as they all use the same methods of transmission. This means everything is compatible with everything and data can be sent around the world easily. If the standards and protocols were different everywhere, it would make the internet a lot harder to maintain and it would take a lot of work to support all the different standards.

Task 2
Client-Server vs Peer-to-Peer

Client-Server

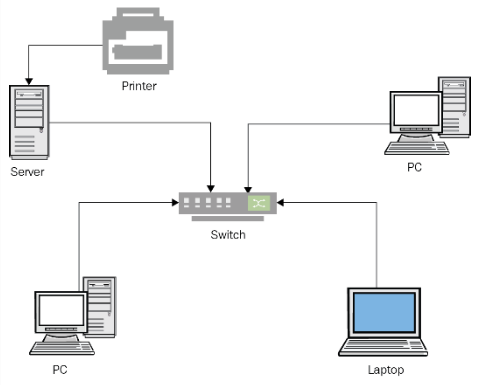
A client-server network is a network that contains a central server which provides services to the clients such as file sharing or authentication. All clients must connect to this central server. This can often be seen in a star topology.

Advantages

- Can handle large amounts of traffic.
- Central administration – security, account privileges, etc.
- Users can log into the network from any client and still have all their data.
- If one client goes down, the rest of the network is unaffected.

Disadvantages

- Depending on the central server – if it goes down the whole network follows.
- Much more expensive than peer-to-peer as a server is required.
- Requires a lot of cabling.



Peer-to-Peer

A peer-to-peer network is a network where all nodes are connected and don't require a central server to operate. This can often be seen in a mesh topology.

Advantages

- Much cheaper than a client-server setup – no need for a central server.
- Each peer can provide a different service – for example one peer could provide printing, whilst another provides shared file storage, etc.
- If a peer goes down, the network is unaffected as traffic can be routed another way.

Disadvantages

- Hard to scale – it will be difficult to support more than 10 clients.
- Files from one machine cannot be asked from another.
- Lack of security – all nodes usually have the same access level.
- Requires lots of cabling as all nodes must be connected to each other.