Unit 9, Assignment 1 – Computer Networks

Thomas Robinson

SOLIHULL COLLEGE

Task One (P1, P2)

Types of Networks

LAN

A **Local Area Network** connects devices together in a single physical area, for example a home or an office.

WAN

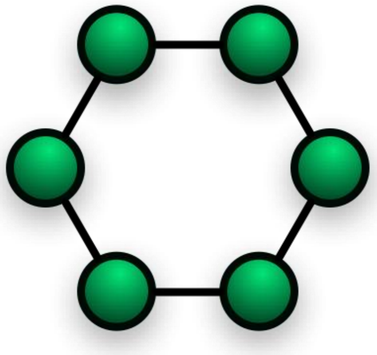
A **Wide Area Network** connects multiple LANs together to allow intercommunication. The internet is an example of a WAN.

PAN

A **Personal Area Network** is limited to the area around a user. An example of a PAN would be a Bluetooth connection to transfer audio data to headphones or a file to another phone or NFC to make a mobile payment at a card terminal.

Topologies

Ring

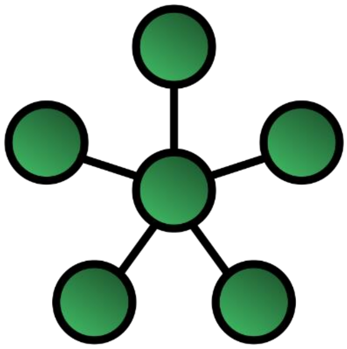


In a ring topology, data travels around the ring, being passed along by each subsequent device (“node”) until it reaches its destination.

In the event of a cable breaking, since data is only sent one way around the ring, some of the devices would no longer be able to receive data from others. This same problem occurs if a computer in the ring were to stop working; the data would not be able to go further along in the ring to reach any devices after it.

A ring network can handle large amounts of traffic since the data only flowing in one direction means there are no collisions (where two devices try to send data at the same time). In the event of excessive traffic, the data could be bottlenecked by a device that is slow to pass the data onto the next device.

Star

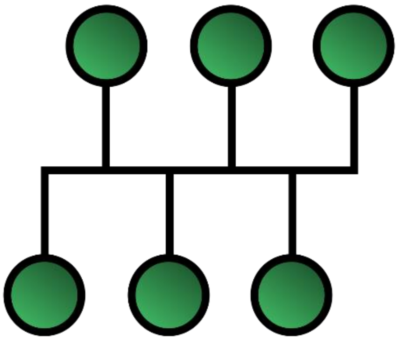


In a star configuration, each device is connected to a central node. An example of this would be an office where each computer is individually connected to a single switch.

If a cable were to break, only the connection to the individual device would be affected. The rest of the network would remain intact. The same holds true for a computer failure; only the affected computer will lose connectivity.

A star network can also handle large amounts of traffic since each device has its own connection, no collisions can occur. Depending on whether a switch or hub is used, excessive traffic could cause the entire network to slow. When a hub is used, all traffic received is passed onto every other device connected. When a switch is used, it could become overloaded and cause the network to slow.

Bus



A bus network sees data sent along a shared central cable that links all devices together. All traffic sent can be read by every device connected.

If the central cable of a bus network were to fail, then the entire network would also cease functioning. Excessive traffic or a large number of devices on a bus network can use significant slowdown since this type of network is prone to collisions.

WAN Technologies

Frame Relay

Frame Relay is a technology that orchestrates data transfer between WAN endpoints. It uses packet switching, which means it breaks data down into packets—also called frames.

MPLS

Multiprotocol Label Switching labels packets with instructions on how it should be sent throughout networks. This means an intermediary does not need to make use of routing tables and can simply be forwarded based on a labels' direction. When the device reaches the final stage of the LSP (layer switched path) network, the label is removed, and normal IP routing takes over.

ATM

Asynchronous Transfer Mode is a transmission-independent standard for the transmission of data, voice and video. Since it makes use of classes that can be attached to each cell (packet) of data, QoS can be used to increase perceived performance and reliability.

Network Access Methods

CSMA

Carrier-Sense Multiple Access is a protocol that controls the sending of data on a network with a shared transmission medium, such as one in a bus configuration. It means that a device will check for the absence of traffic before sending data itself. The device will wait for the ongoing transmission to finish before it sends its data.

Token Passing

With **token passing**, no two devices can transmit a signal at the same time; they must wait until they have the token which allows them to do so.

Standards

Wi-Fi (802.11)

Wi-Fi is a standard set of protocols for communicating data wirelessly using radio waves.

2G, 3G, 4G, 5G

Are standard protocols for mobile telecommunications, used by cellular mobile devices, such as phones, tablets and laptops. Each new generation offers increased bandwidth and capacity.

Ethernet

Ethernet is collection of standards for wired networking technologies, including data transfer specifications, cable specifications and connector specifications.

Protocols

TCP/IP

The **Transmission Control Protocol/Internet Protocol** stack is a collection of protocols that govern how data should be split into packets, routed, sent and received.

DNS

The **Domain Name System** is a way of associating IP addresses with human-readable names. In the context of the internet, a DNS server acts like a phonebook: translating a domain name (solihull.ac.uk) to an IP address (78.109.173.187). DNS servers use port 53.

DHCP

The **Dynamic Host Configuration Protocol** is a method of assigning information and configuration to devices on a network. Most commonly, it is used to assign IP addresses on a LAN or WAN. DHCP servers make use of port 67 which communicates with port 68 of a client.

HTTP

Hypertext Transfer Protocol is designed for transmitting ‘hypermedia’ (websites and associated data/documents), though it can be used for other purposes. Port 80 is used for plaintext traffic and the secure variant (HTTPS) uses port 443 for encrypted communications.

FTP

File Transfer Protocol was introduced in 1971 used for—as the name implies—transferring files between a server and a client. It issues textual commands to a server to manipulate files. Port 21 is used for issuing commands and control and port 20 is used for data transfer.

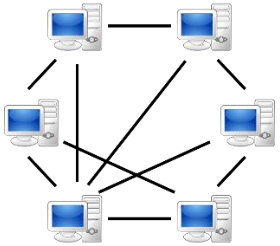
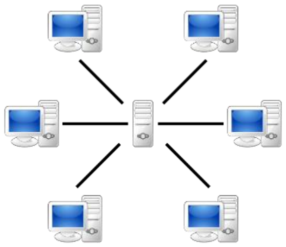
SMTP

Introduced in 1981, the **Simple Mail Transfer Protocol** is a standard for sending and receiving email (though it is often only used for sending). Standard ports include 25 for unencrypted communication and 587 for encrypted.

Why are standards important?

Standards and protocols are important since they dictate how computers, servers and applications can talk to each other and work together. Without a set of common standards, interoperability between devices would be near-impossible since nothing would be able to communicate without being able to speak every possible ‘language’.

Task Two (M1)

Type	Advantages	Disadvantages
 **Peer-to-Peer**	- If an individual computer were to fail, then the whole network does not fail - Cheaper and easier to set up since there is no need for a central server - Can scale well since there is no central server to overutilize	- Files and resources will be distributed across the devices which could make them harder to retrieve - The distributed nature means it is harder to back up files
 **Client-Server**	- A centralised server means it is easier to manage files and accounts/permissions as well as performing backups	- More expensive to set up - If the server fails and there is no redundancy, the network will fail - Requires knowledge to setup and maintain