AQA Computer Science AS Level

3.9.2 Networking

Advanced Notes

Specification:

3.9.2.1 Network topology:

Understand:

- physical star topology
- logical bus network topology

and:

- differentiate between them
- explain their operation

3.9.2.2 Types of networking between hosts:

Explain the following and describe situations where they might be used:

- peer-to-peer networking
- client-server networking

3.9.2.3 Wireless networking:

Explain the purpose of WiFi

Be familiar with the components required for wireless networking

Be familiar with how wireless networks are secured

Explain the wireless protocol Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with and without Request to Send/Clear to Send (RTS/CTS)

Be familiar with the purpose of Service Set Identifier (SSID)

Network topology

Topology refers to the structure of a network. There are two types of topology to consider: physical and logical.

Physical network topology

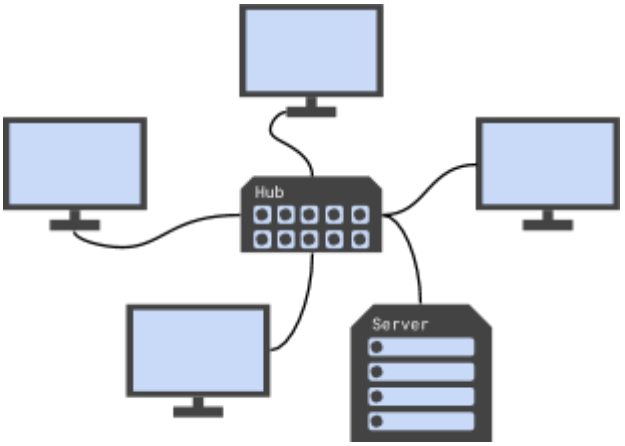
Physical network topology refers to the actual architecture of a network. Networks using one physical topology will interconnect components differently to those networks that use another physical topology.

There are two types of physical network topology to learn: star and bus.

Physical star network topology

In a physical star network, each client (that is, a device connected to the hub) has its own direct connection to the central hub. The hub receives packets for all of the clients connected to it and is responsible for delivering them to the correct recipient.

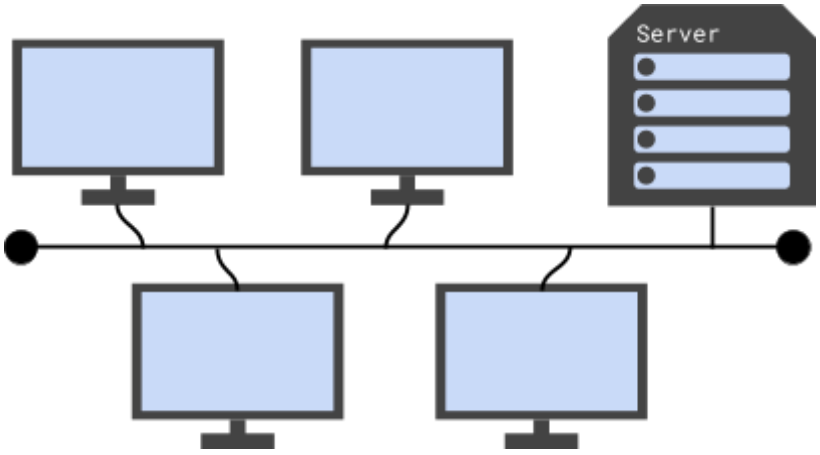
A server can be added to the network in the same way that clients are connected to the central hub.



Advantages	Disadvantages
Packets are sent directly to their recipient, over a cable that is connected only to the recipient. Other clients on the network cannot see packets that aren't intended for them.	Should the central hub fail, all communication over the network is stopped.
It is easy to add and remove clients to and from the network.	Expensive to install thanks to the amount of cable required.
Each cable has just one device communicating over it, eliminating the possibility of collisions.	
The failure of one cable does not affect the performance of the rest of the network.	

Physical bus topology

A physical bus connects clients to a single cable called a backbone. A device called a terminator is placed at either end of the backbone.



There is no need for a central hub like in physical star networks and a server can be connected to the backbone just like a client.

Advantages	Disadvantages
There is no central hub, reducing the chances of a network failure and decreasing the cost of installation.	Packets are sent through the shared backbone, allowing every client on the network to see packets that aren't intended for them.
Inexpensive to install as a minimum length of cable is required.	The backbone is used for communication by multiple clients, introducing the risk of collisions.
	Should the backbone fail, the entire network becomes unusable.

Logical network topology

In contrast to a network's physical topology, a network's logical topology refers to the flow of data packets within a network. A logical bus network delivers packets to all clients on the network whereas a logical star network delivers packets only to their recipient.

Mixing topologies

If a network is set up as a physical star, it can still behave as a logical bus. Even if the physical connections between clients and the central hub follow that of the physical star topology, running a bus protocol on the hub allows it to distribute packets to all of the connected clients so as to act like a bus network.

Types of networking between hosts

A host is a device on a network that provides services. This is often a server, which can provide services such as file storage, printer sharing and internet access but can also be the clients on a network themselves.

Client-server networking

In a client-server network, one or more central servers provide services to the clients on the network. Servers are connected to the network in the same way as clients, but are often more powerful machines than the clients.

The clients on the network request services from the servers, which then respond to the client with the requested service. Services provided by servers in a client-server network could include file storage as well as management of emails, user accounts and print queues.

Most schools, colleges and businesses use client-server networks to allow for central management of clients on the network. This can improve security but requires a fair degree of expertise to set up and manage.

Peer-to-peer networking

Peer-to-peer networks do away with a shared server. Instead, services are provided by the clients themselves and every client has equal status. For example, one computer on the network might manage print queues, another manage storage and a third manage emails.

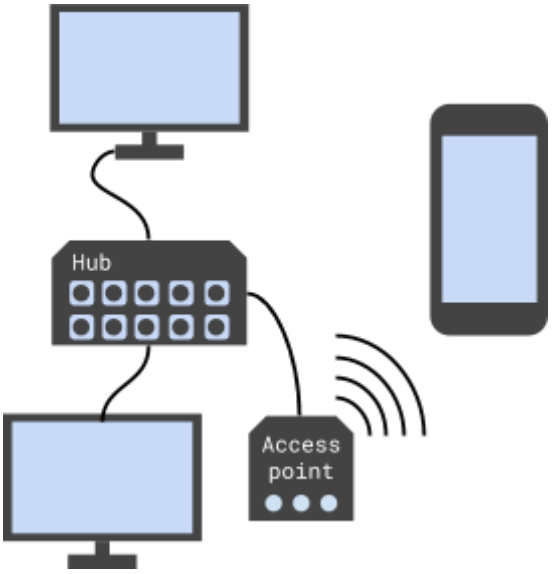
The primary disadvantage of peer-to-peer networking is that all of the clients which provide services must be running in order for the network to be fully operational. If the computer responsible for managing storage is turned off or faulty, none of the clients on the network can access their files.

On the other hand, peer-to-peer networking is more cost effective than client-server networking as there is no need for a powerful server to provide services. Furthermore, peer-to-peer networks are easier to set up and maintain than their client-server counterparts

Large file-sharing networks and multimedia providers use peer-to-peer networking to provide high-performance services without the requirement for a server.

Wireless networking

Wireless networks allow clients to communicate within a network without being physically connected to it.



Wireless networks require a wireless access point, which connects to a wired network just like any other client would, and a wireless network adapter in the device that connects to the wireless network.

WiFi

WiFi is widely used to provide wireless networks and refers to a wireless local area network that is based on international standards. This allows a device made in one part of the world to connect seamlessly to wireless networks all over the world.

Wireless networks are secured by encrypting transmitted data using WPA or WPA2. WPA stands for WiFi protected access and requires that a new wireless client enters a password in order to connect to the network.

Another method of securing a wireless network is disabling SSID broadcast. SSID stands for service set identifier and is the name that identifies a wireless network. Disabling SSID broadcast stops wireless devices within range of the network from displaying that the network is available, only allowing those who know the SSID to connect.

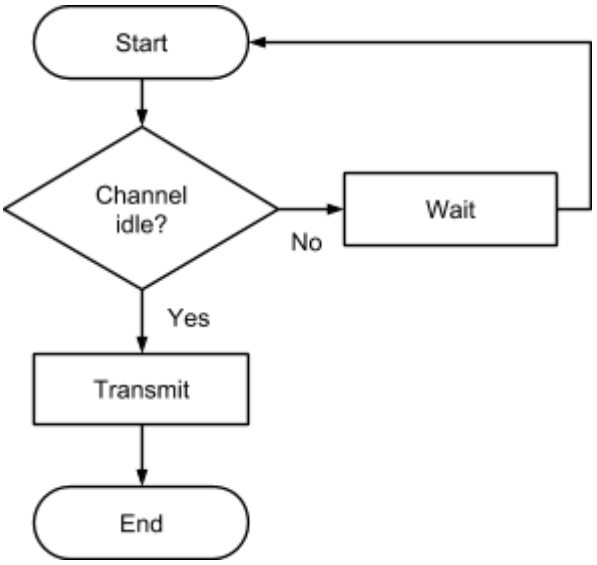
A third method of securing a wireless network is to set up a MAC address filter. MAC (which stands for media access control) addresses are assigned to every wireless device by their manufacturer and are unique to that device. MAC address whitelists can be created to allow only specific devices to connect to a network. Likewise, MAC address blacklists can be used to block specific devices from connecting to a network.

Carrier Sense Multiple Access with Collision Avoidance

Carrier sense multiple access with collision avoidance (CSMA/CA) is a protocol used in wireless networks to avoid data collisions caused by multiple devices communicating simultaneously.

Protocol

A set of rules relating to communication between devices.



When a device is ready to transmit, it listens to its communication channel to check whether it is idle. If so, then the data is transmitted. If the channel is busy, the device waits for a random period of time before checking the channel again. An exponential backoff algorithm can be used to increase the time period for which the device waits with each check of the channel.

While CSMA/CA is effective at eliminating collisions in small networks, it cannot overcome hidden nodes: a problem that arises when the device checking for an idle channel cannot "see" some parts of the network on which communication may be occuring.

To get around the problem of hidden nodes, a protocol called request to send/clear to send (or RTS/CTS) is used. This protocol adds an additional step into the CSMA process. Once the transmitting device has checked whether the channel is idle, it sends a "request to send" message to the server.

If the server is indeed idle, it will respond with a "clear to send" message at which point the transmitting device can begin communication with the server. If no "clear to send" message is received, the server is busy communicating with a hidden node and the transmitting device must wait before starting the CSMA process again.