Component 1 | 1.3.3| Networks

Specification & learning objectives

	A Level	Specification point description
	1.3.3a	Characteristics of networks and the importance of protocols and standards
	1.3.3b	Internet structure: -The TCP/IP Stack -DNS -Protocol layering -LANs and WANs -Packet and circuit switching
	1.3.3c	Network security and threats, use of firewalls, proxies and encryption
	1.3.3d	Network hardware
	1.3.3e	Client-server and Peer to Peer

Resources

PG Online textbook page ref: 111-129
Hodder textbook page ref: 203-218
CraignDave videos for SLR 11

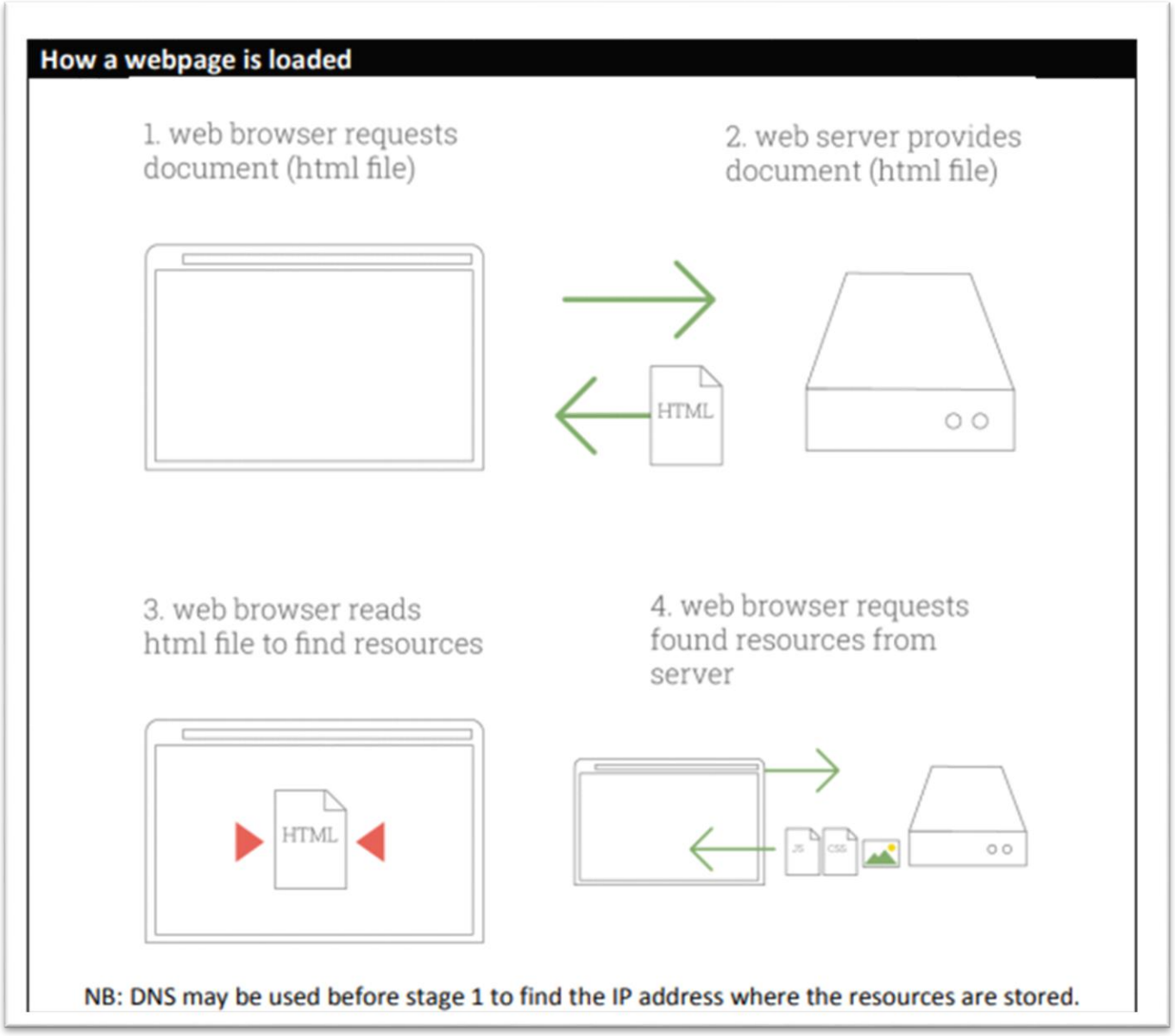
Protocol: Protocols are a set of rules relating to the communication between devices.
TCP/IP Stack: Transmission control protocol: Used with IP to ensure error free transmission and package switching. Internet protocol: Is used to transfer all packets across the internet between routers.
DNS: Domain name system controls your domain names website and email settings. The DNS settings will affect which server your customers goes to when using your domain.
Protocol Layering: Protocols are layered, each layer has a different purpose and when writing a protocol the software can be written appropriately for the given layer.
LAN: Local Area Network is a method of connecting computers together in a small geographical area.
WAN: Wide Area Network is a network that extends over a large geographical distance, connects computers on different sites, towns and continents.
Packet Switching: The data that is to be transmitted is broken up into individual packets by the source computer.
Circuit Switching: Data transmission follows a route between nodes known as a circuit, all the data follows this route until transmission is complete.
Client Server: A device (client) requests services from a central device known as the server.
Peer to Peer: There is no central server all the terminals have equal status.

Key question: What are the features of a protocol, and what do we mean by a 'standard'?

Protocols and standards are rules that must be followed when networking computers. It is vital that these are followed as different pieces of hardware and software would not be able to communicate without following the set standards.

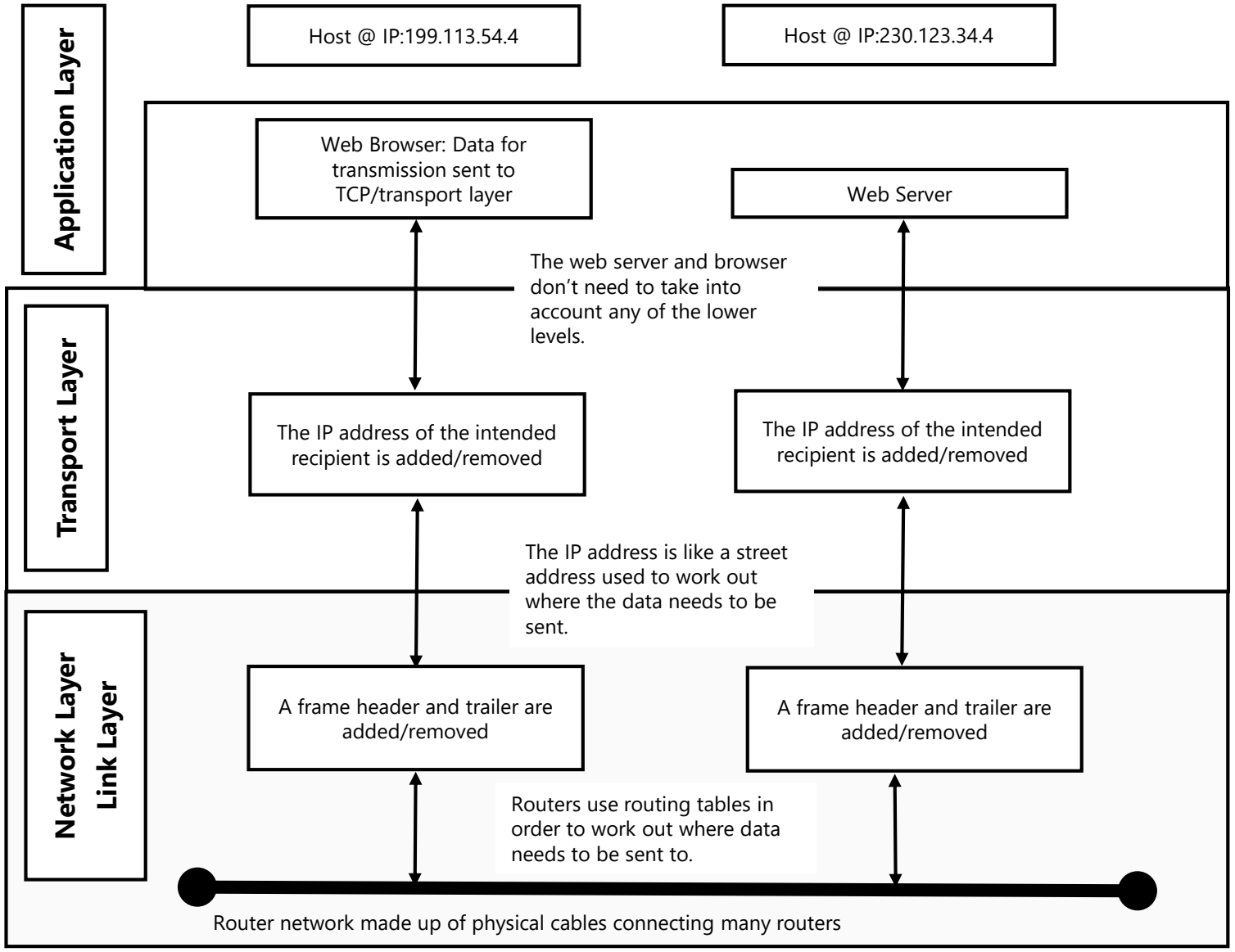
When combining the computers, there are factors that need to be considered which determine the type of network required:

Key question: How does the internet work?



The Internet is the world's largest network, consisting of many different machines in different locations. By utilising standards these machines are able to communicate around the world.

Key question: How does the internet work?



Key question: What does ‘protocol layering’ mean and why is it needed?

A set of rules that standardise the way computers communicate with each other are called **protocols.**

The two most major protocols include:

TCP (Transmission Control Protocol): This ensures error free transmission and package switching.

IP (Internet Protocol): This is used to transfer all packets across the internet, between routers.

As these protocols are always used together, these 2 protocols are commonly called the **TCP/IP Stack**.

Other major protocols include:

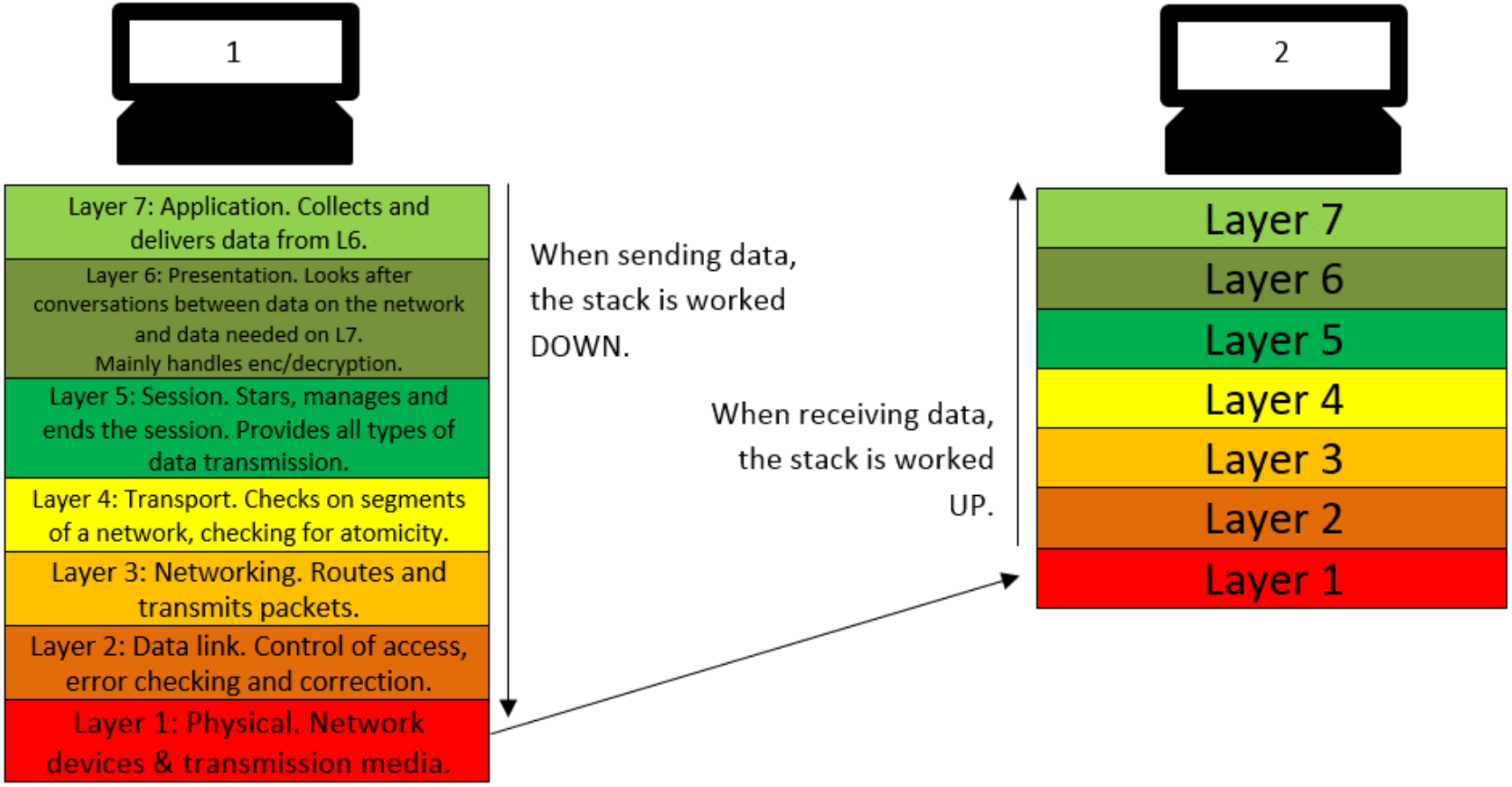
FTP (File Transfer Protocol): This is used by both clients and servers to upload and download files across the internet.

HTTP (Hypertext Transfer Protocol): This is used by web servers and browsers to transfer web pages.

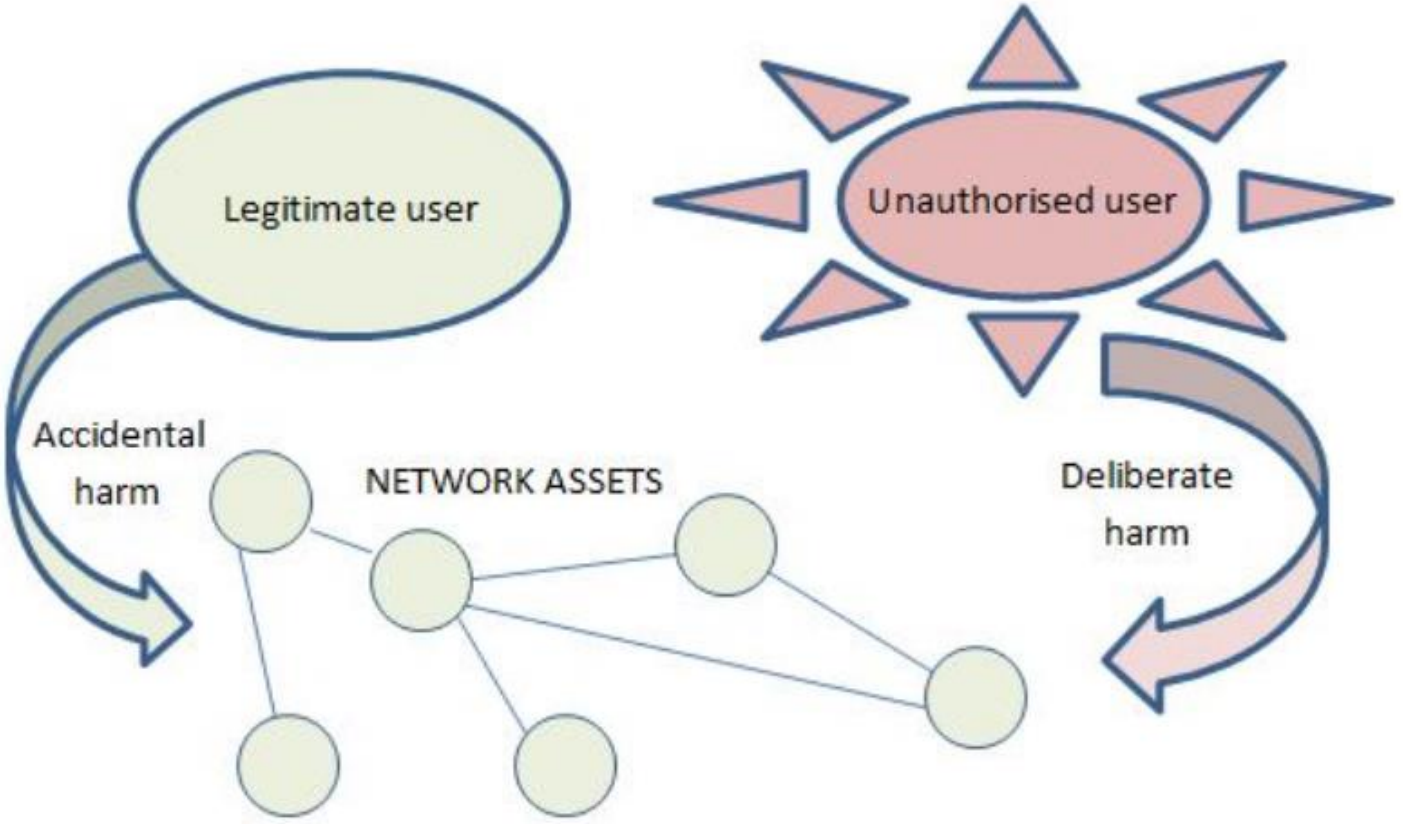
SMTP (Simple Mail Transfer Protocol): Used by mail servers and clients to transfer email across the internet.

Protocol Stacks

All protocols, at least loosely, follow the OSI protocol layering system. This is a set of 7 layers that will be gone through in order when sending data across the internet to ensure data is always sent in the same way.



Key question: What are the threats to network security and how can they be mitigated?



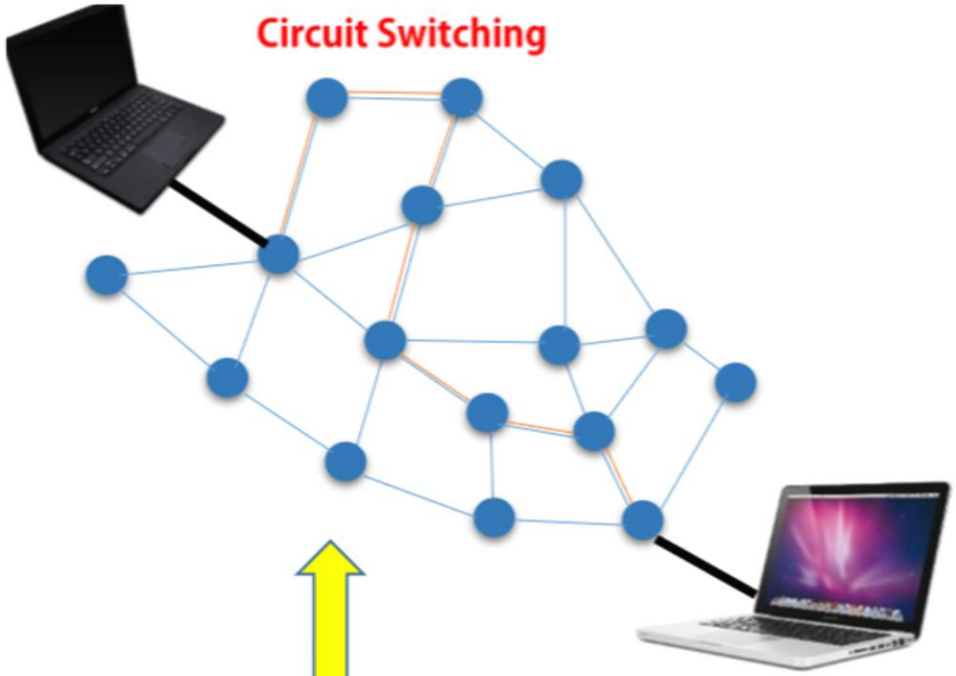
Component 1 | 1.3.3| Networks

Key question: What are the threats to network security and how can they be mitigated?

- Authentication is used to identify legitimate users.
- Authentication includes username-password, two factor authentication and biometric methods.
- User rights can be set to define what areas and files on the network they can access or change.
- Educating users in good network practice improves security.
- A proxy server can block site access, hide IP addresses and provide an encryption service.
- A firewall has a set of rules to define which a proxy server acts as an intermediary between the user browser and a web site or service.
- Packets can and cannot pass between the network and the Internet.
- Encryption is used to keep data private.

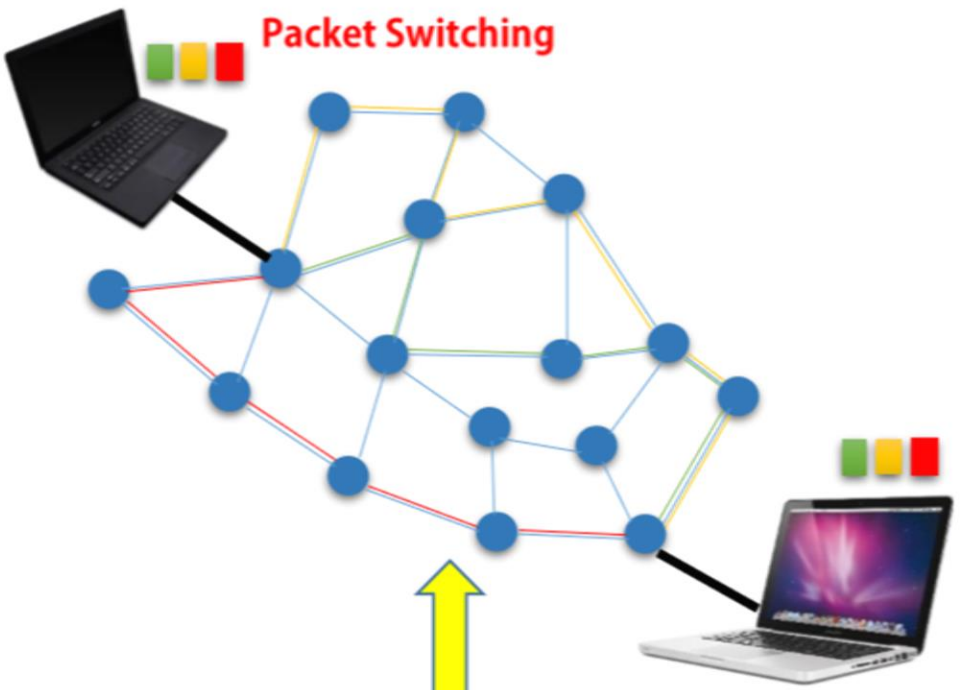
Component 1 | 1.3.3| Networks

Circuit Switching



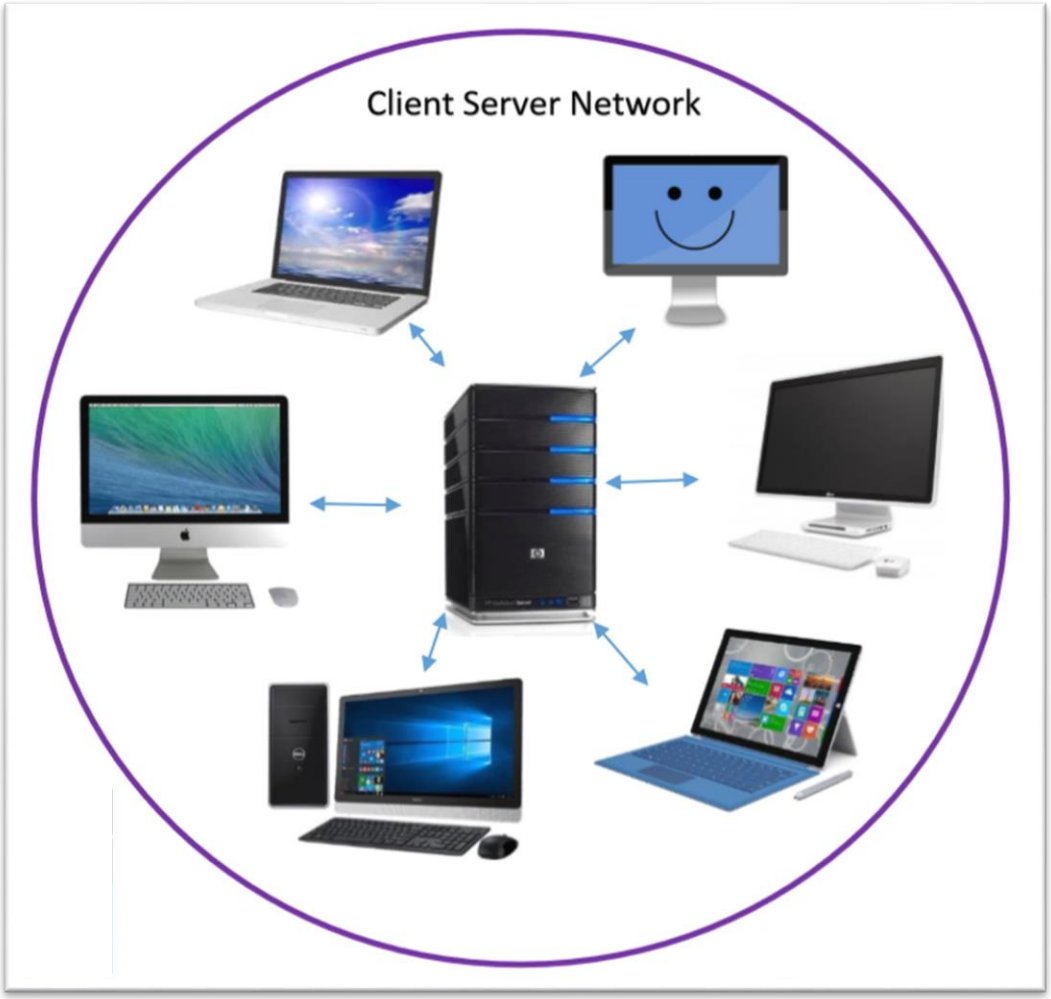
Circuit switching a route is created consisting of several switches or nodes, once this route has been calculated the electronic transmissions can start. During the transmission no other network traffic can use the switches, it is mostly used for telephone calls. Once a user requests the connection and identifies the destination a circuit is established and can be used and in turn electronic transmissions can start.

Packet Switching



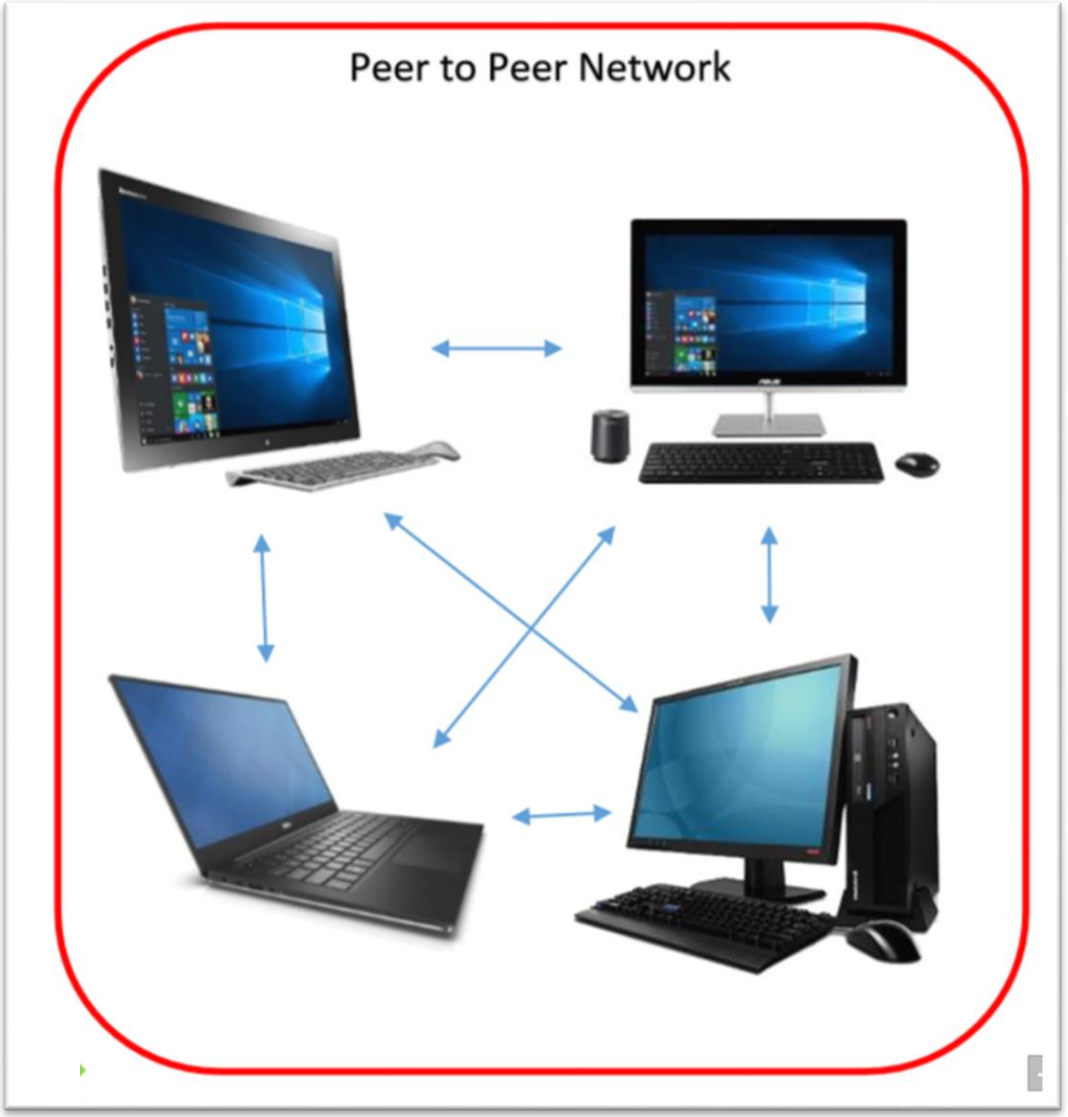
With packet switching the data is separated into packets shown as the green, orange and red above. On the internet network there are millions and millions of routes a file or packet could take, the packets leave the first computer and go the route which is the least busy at the time which means that the packets won't necessarily go the same way. This is also means the packets may arrive out of order but the second computer can sequence them to make the file complete.

Key question: What is the difference between a client-server and peer-to-peer network topology?



In the client server network there is one central network controller or server which controls access to network resources. It also controls the network access and security which is good for use in a school. However they need a special operating system usually installed on the central system.

Key question: What is the difference between a client-server and peer-to-peer network topology?



In a peer to peer network all the computers are equal within the network, the access to the network is not centrally controlled and they don't have to ask the central system to use resources. They have standard operating systems which are installed on each computers, in general they are simpler and have a low cost.

Typical exam questions

1. Describe what is meant by the term Protocol. **[1]**

2. Explain how the TCP/IP stack is a type of protocol, make reference to layering in your answer. **[4]**

3. Explain one advantage and one disadvantage of Client-Server over Peer-to-Peer. **[4]**

Advantage:

Disadvantage:

4. A local business has fallen victim to a string of recent cyber-attacks which has resulted in personal and private data being stolen from their internal network. Explain how each of the following techniques could be used to help mitigate against future attacks. **[6]**

Firewall:

Proxy:

Encryption:

Component 1 | 1.3.3| Networks

Target: Overall grade:

Minimum expectations & learning outcomes

☐	Terms 134-146 from your A Level Key Terminology should be included and formatted.
☐	You must explain the purpose of a protocol (including examples of what it might determine) and standards.
☐	You must include illustrations explaining the difference between packet and circuit switching.
☐	You must show a clear understanding of the main differences between LANs, WANs, client-server and peer to peer.
☐	You must include a diagram which clearly shows your understanding of protocol layering and show how that applies to the TCP/IP protocol.
☐	You must explain how a URL becomes an IP address using a Domain Name System.
☐	You must identify some examples of networking hardware including switch, router, NIC, WAP using an illustration of how a network for a small business might be connected. You should include threats to the network and how these are typically prevented.
☐	Answer the exam questions.

Feedback

Breadth	Depth	Presentation	Understanding
☐ All	☐ Analysed	☐ Excellent	☐ Excellent
☐ Most	☐ Explained	☐ Good	☐ Good
☐ Some	☐ Described	☐ Fair	☐ Fair
☐ Few	☐ Identified	☐ Poor	☐ Poor

Comment & action required

Component 1 | 1.3.3| Networks

Reflection & Revision checklist

Confidence	Clarification
☹ 😐 ☺	Candidates need to understand the definition and purpose of a network.
☹ 😐 ☺	Candidates need to understand the purpose of, and importance of using, protocols.
☹ 😐 ☺	Candidates should be able to discuss examples of protocols that may be used in a network/ the internet (but will not be asked to recall information about any specific protocol).
☹ 😐 ☺	Candidates should understand the term standard, and the purpose and need for standards in a network (or any situation where data is transferred).
☹ 😐 ☺	Candidates need to understand the purpose and benefits of layering protocols, particularly within the TCP/IP stack. Candidates need to know the different layers within the TCP/IP stack and the purpose of each.
☹ 😐 ☺	Candidates need to understand how data is transmitted on the Internet, the use of IP addresses and packets in the transfer of data. (NB: Candidates are not expected to be familiar with the OSI model).
☹ 😐 ☺	Candidates are expected to understand the terms LAN and WAN.
☹ 😐 ☺	Candidates need to understand how the Domain Name System is used to find the IP address of a URL.
☹ 😐 ☺	Candidates need to understand the purpose, function, benefits and drawbacks of both packet and circuit switching.
☹ 😐 ☺	Candidates need to understand the difference between a client-server and peer-to-peer network.
☹ 😐 ☺	Candidates need to know the benefits and drawbacks of each type of network and be able to recommend one for a given scenario.
☹ 😐 ☺	Candidates need to understand that there are a range of security issues and threats involved with networked computers.
☹ 😐 ☺	Candidates need to be aware of threats such as hackers, viruses, unauthorised access, denial of service, spyware, SQL injection, phishing and pharming.
☹ 😐 ☺	Candidates need to know about ways of minimising, or preventing these threats for example firewalls, secure passwords, anti-virus, anti-spyware etc.
☹ 😐 ☺	Candidates need to have knowledge of the hardware required to connect to and/or build a network (e.g. modem, router, cable, NIC, Wireless Access Points, hub, switch etc).
☹ 😐 ☺	Candidates need to understand the purpose of the hardware but are not required to understand how they physically work.