9/26/2016

Simon Light

UTC Reading

Unit 9/10

Assignment 1

Contents

[P1 - Describe the types of networks available and how they relate to a particular network standards and protocols 3](#_Toc463266336)

[P2 – Describe why different network protocols and standards are needed. 3](#_Toc463266337)

[M1 – Compare the advantages and disadvantages between peer-to-peer networks and client/server networks 16](#_Toc463266338)

[Definitions 16](#_Toc463266339)

[Peer-to-peer 16](#_Toc463266340)

[Client-server 16](#_Toc463266341)

[P1 – Explain how networks communicate 17](#_Toc463266342)

[P2 – Identify communication protocols and models 17](#_Toc463266343)

[DHCP 17](#_Toc463266344)

[DNS 17](#_Toc463266345)

[WINS 17](#_Toc463266346)

[FTP 17](#_Toc463266347)

[TCP 17](#_Toc463266348)

[IP 17](#_Toc463266349)

[SMTP 17](#_Toc463266350)

[HTTP 17](#_Toc463266351)

[P3 – Identify different types of communication devices 19](#_Toc463266352)

[Switch 19](#_Toc463266353)

[Router 19](#_Toc463266354)

[Bridge 19](#_Toc463266355)

[Hub 20](#_Toc463266356)

[P4 – Describe what data elements are and why they are important 20](#_Toc463266357)

[CRC 20](#_Toc463266358)

[Encapsulation 20](#_Toc463266359)

[Frames 20](#_Toc463266360)

[Packets 20](#_Toc463266361)

[Datagrams 21](#_Toc463266362)

[Addresses 21](#_Toc463266363)

[Sequence Numbers 21](#_Toc463266364)

[M1 – Explain why communication protocols are important 21](#_Toc463266365)

[Example 21](#_Toc463266366)

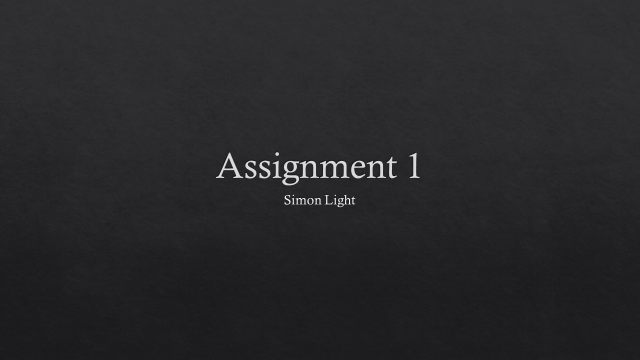
[D1 – Compare the OSI seven-layer model and the TCP/IP. 22](#_Toc463266367)

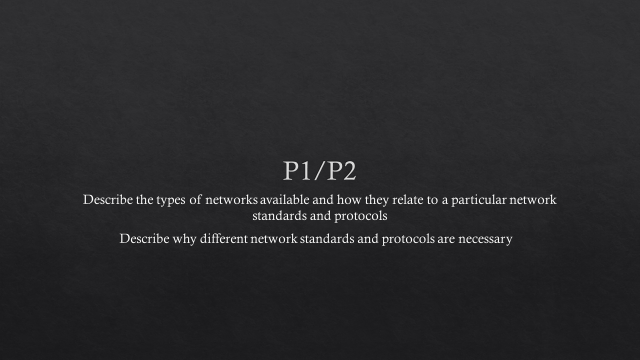
[OSI 22](#_Toc463266368)

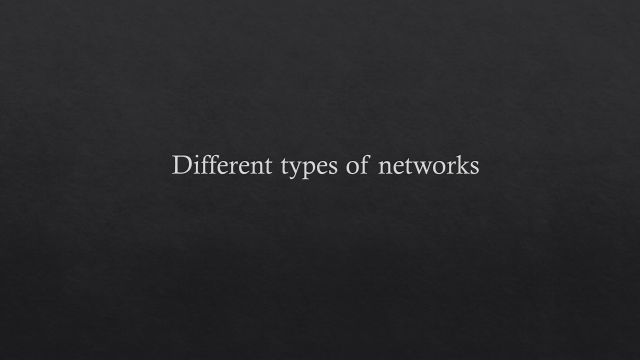
[TCP/IP 22](#_Toc463266369)

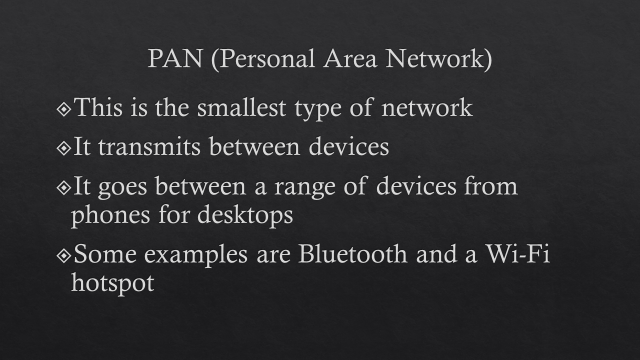
# P1 - Describe the types of networks available and how they relate to a particular network standards and protocols

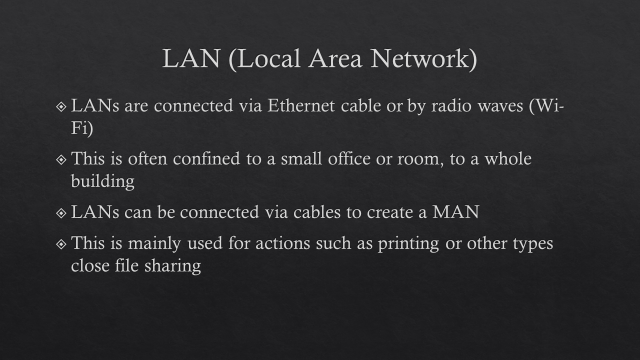
# P2 – Describe why different network protocols and standards are needed.

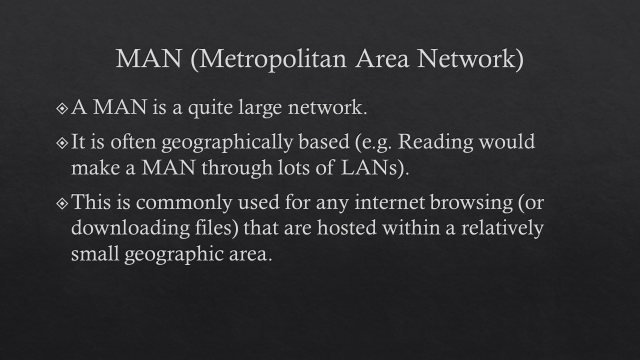


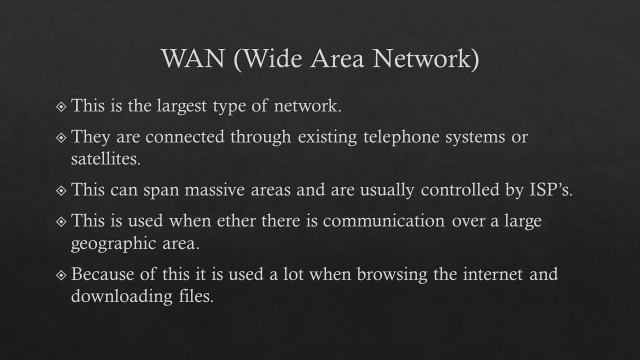


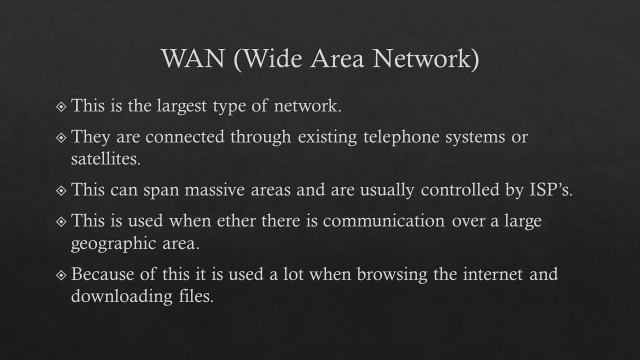


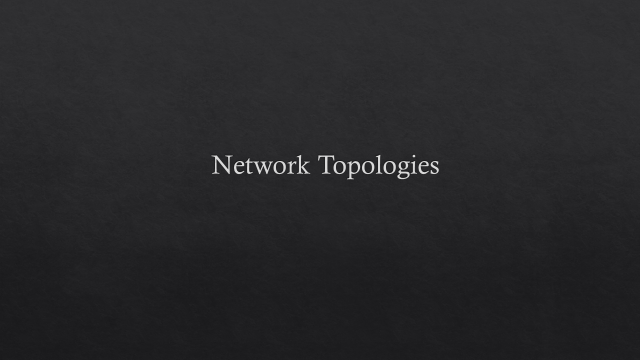


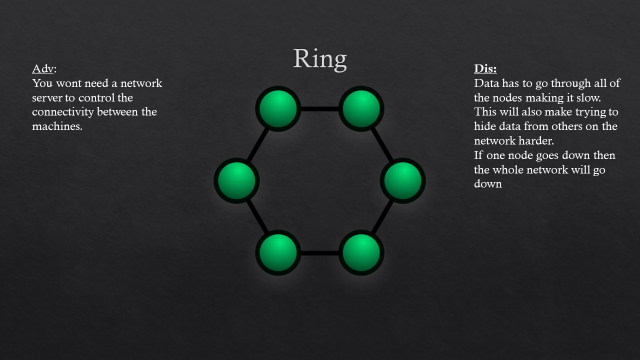


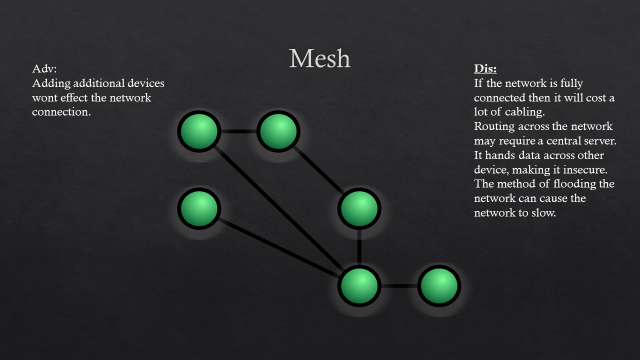


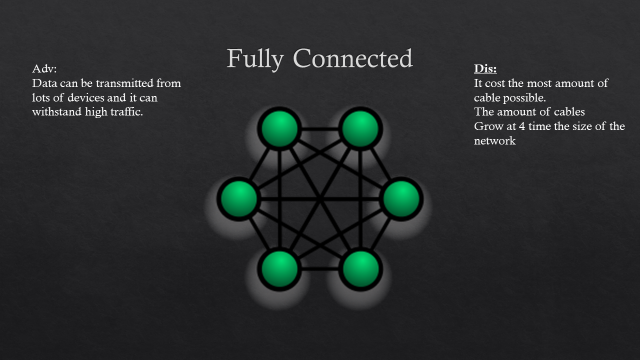


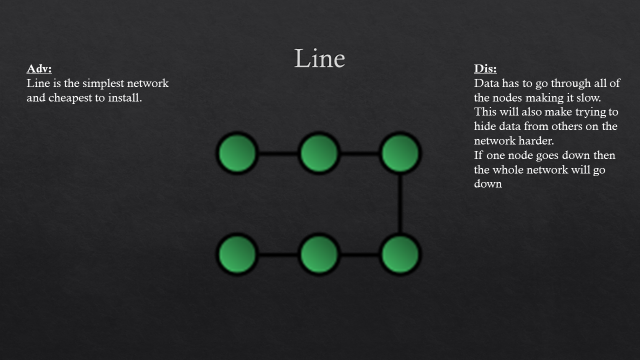


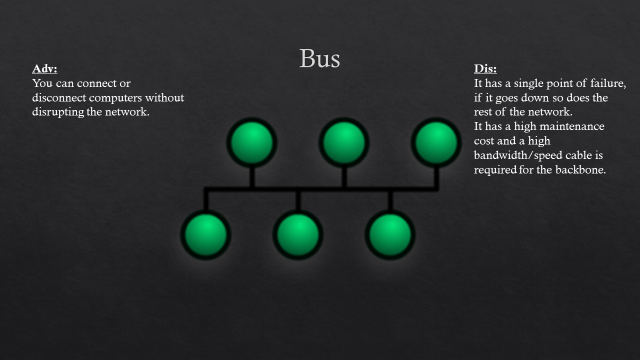


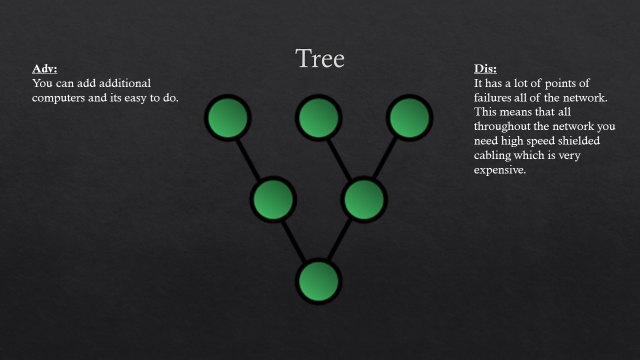


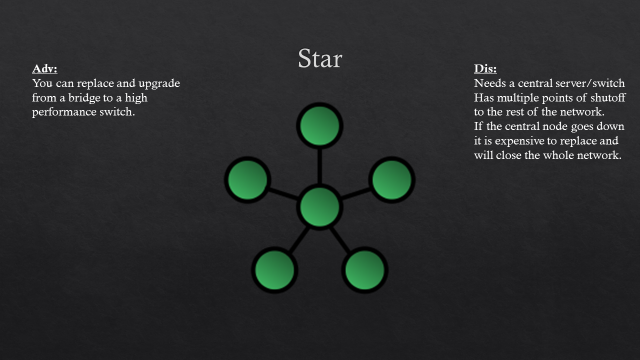




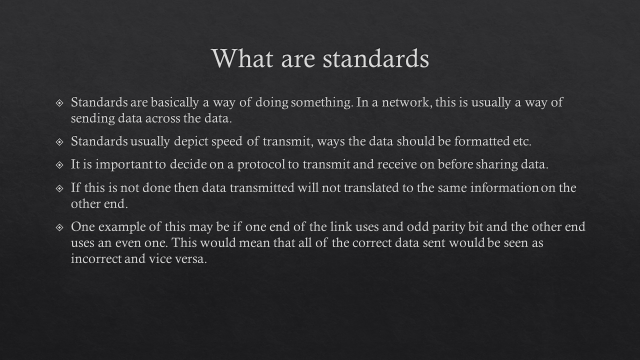


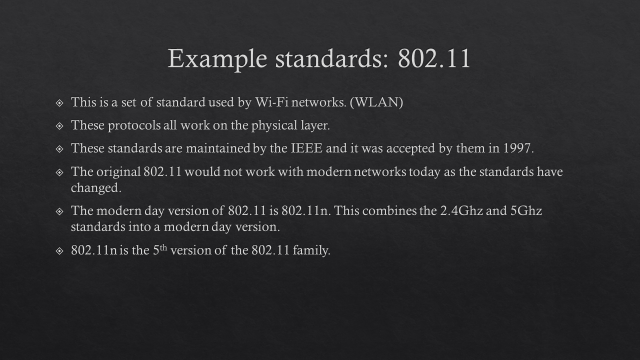


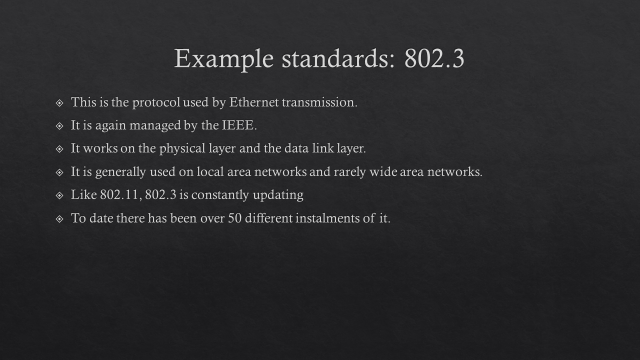


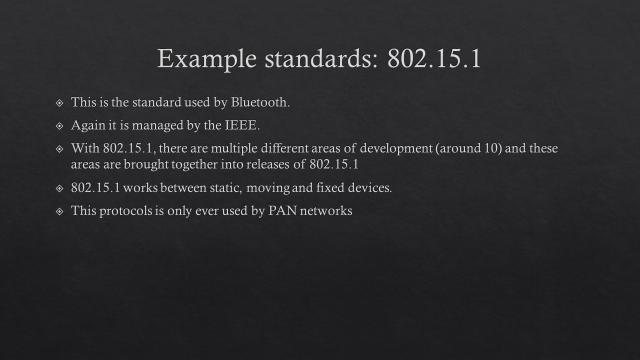




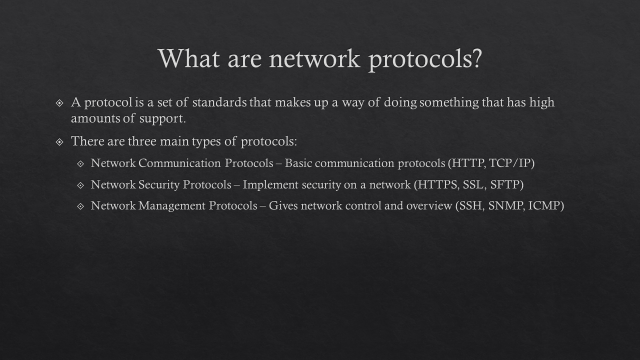


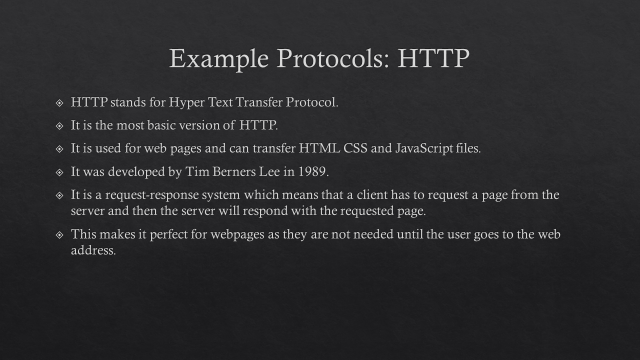




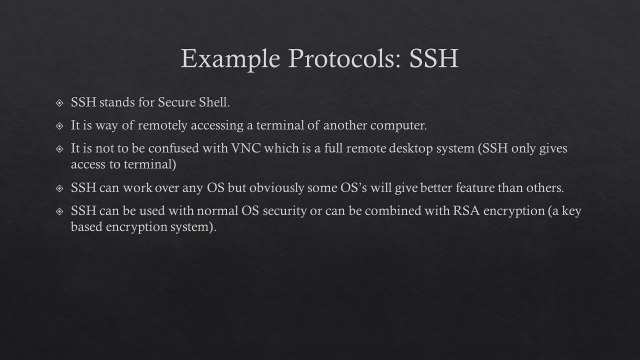












# M1 – Compare the advantages and disadvantages between peer-to-peer networks and client/server networks

## http://core0.staticworld.net/images/idge/imported/article/ctw/2002/04/08/navigatingap2pnetwork-100408562-orig.gifDefinitions

### Peer-to-peer

In the smallest form, a peer to peer server is when two or more computers are connected to each other for the purpose of sharing data. This may be done via some external hardware (switch or hub) but must not contain a server that handles data. In essence, all device in a peer-to-peer network are seen as both the server and the client (depending whether sending or receiving files). A peer to peer network may also be connected to the internet via a router or wireless medium and can also be used to share devices such as printers.

### http://simplecore.intel.com/itpeernetwork/wp-content/uploads/sites/38/2011/05/client_net.jpgClient-server

A client server network is one that there is a main computer (usually a server) handles some kind of workflow for other clients on the network. This is usually some kind of network load but can be anything from storage to CPU usage. One of the most common uses for this kind of network is a thin client system. This is where there is one localised server that runs multiple instances of an OS. There are then dumb-terminals that then connect to these OS’s as clients.

|  |  |  |
| --- | --- | --- |
|  | Peer-to-peer | Client-server |
| Advantages | * The speed limit is on the network cards and cables (easily upgradeable) * Very easy to set up. * Does not need an expensive server * No need for network technicians * If one computer fails the rest of the network is not effected other than that computer’s files | * Can have delocalised security meaning management is easier * Delocalised storage meaning that users only have to know one file storage system. * If a user goes offline then the rest of the system isn’t effected. |
| Disadvantages | * May give slow performance if on computer is being accessed a lot * Users may have different ways of storing files and so navigation of systems is inconsistent * Security of the system (or lack of) is down to individual users * There is little to no security between systems meaning that if a virus is introduced, it will spread to the whole system. | * It is more expensive to setup * If the server goes down, no information at all can be gathered (single point of failure) * Technicians may be needed to maintain the server |

# Image result for how do networks communicateP1 – Explain how networks communicate

Networks communicate through things called protocols. These are basically ways of communicating so that data gives the same result when it is sent and received. None of this is seen by the user except from the end result. One example of this is a router. When it sends data to another it uses a routing protocols to send the data. Without this, data may clash and make no sense to any other routers.

Different networks use different protocols depending on their purpose. This may change from time to time depending on what data is being sent. For example, a word document would be broken down to different packets than an excel document. If this doesn’t happen then data may get muddled and confused as it goes through the OSI layers.

# P2 – Identify communication protocols and models

## DHCP

This protocol is Dynamic Host Configuration Protocol. Its job is to automatically assign IP addresses to all devices on a network.

## DNS

DNS stands for Domain Name System or Domain Name Service. This protocol connects you to servers (including those on the internet) by locating your IP.

## WINS

WINS stands for Windows Internet Naming Service. WINS is very similar to DNS.

## FTP

FTP stands for File Transfer Protocol. This allows for files to transmitted across a network.

## TCP

TCP stands for Transmission Control Protocol. This protocol makes sure that both parties of any communication are valid (often known as a 3-way handshake).

## IP

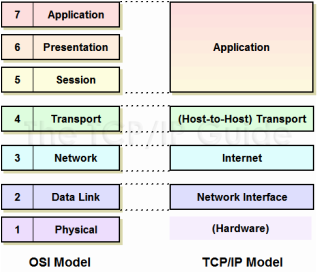
IP stands for Internet Protocol. This allows for internetworking by providing IP addresses within a packet.

## SMTP

SMTP stands for Simple Mail Transfer Protocol. This protocol is used to send emails over the internet.

## HTTP

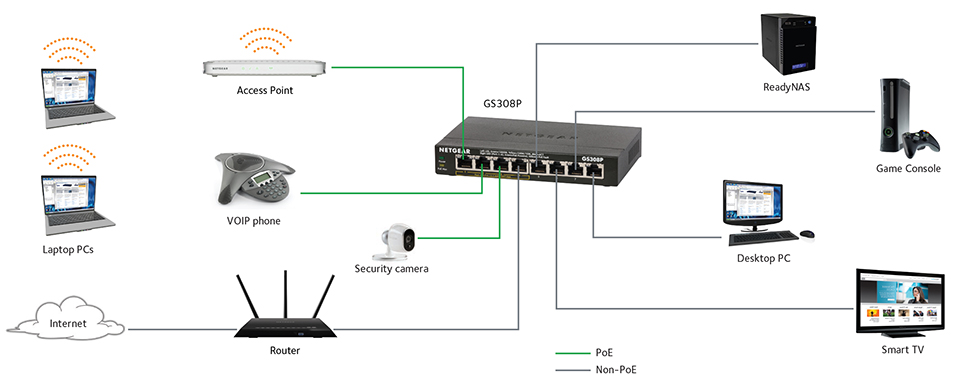
HTTP stands for Hyper Text Transfer Protocol. This protocol is used for requesting and sending web pages. This is used whenever you go to a website.



This image shows the comparison of the OSI Model layer and the TCP/IP Model layer. It also shows what layer from the OSI links with what layer from the TCP/IP by the colour of the boxes and the separation of the dotted lines.  
  
Here's a structure of what happens through this process:  
1. Creation of data at the application layer of the originating source end device  
2. Segmentation and encapsulation of data as it passes down the protocol stack in the source end device   
3. Generation of the data onto the media at the network access layer of the stack  
4. Transportation of the data through the internetwork, which consists of media and any intermediary devices  
5. Reception of the data at the network access layer of the destination end device   
6. Decapsulation and reassembly of the data as it passes up the stack in the destination device   
7. Passing this data to the destination application at the Application layer of the destination end device

# P3 – Identify different types of communication devices

## Switch

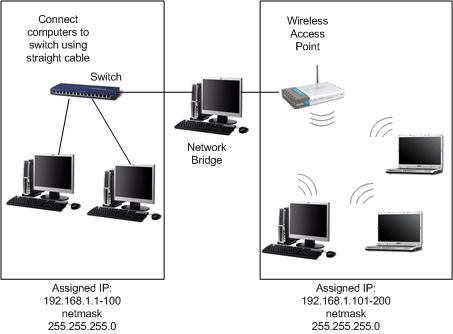


* The main purpose of a switch is to connect different devices within a network.
* It does this by switching packets depending on the destinations MAC addresses.
* A switch can be used to segment up a network (E.G. One switch per room)

## Router

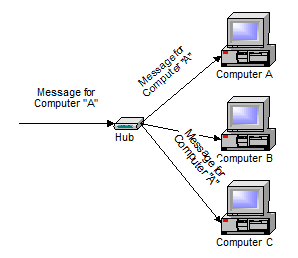
* The main purpose for a router is to forward packets between networks.
* Its sends the data through the network until it gets to the destination node.
* It will also forward any data it receives towards the destination node.
* Modern routers often include antennas as well as Ethernet ports to be able to send and receive over Wi-Fi.

## Bridge



* A bridges main purpose is to connect to networks.
* It is similar to a router as they both have the goal of forwarding packets to the destination.
* It is different to a router as a bridge can only connect 2 networks whereas a router can do this for multiple networks, this happens in the internet.
* A bridge would be used over a router as they are often smaller, cheaper and less power consuming.

## Hub



* A hub is basically a less intelligent version of a switch.
* It still operates on the fact that it switches based on MAC addresses.
* It does not have the ability to separate networks that are connected to the same switch (can’t be managed) and so has a lower price.
* Due to the fact that the price of switches has lowered drastically, the use

# P4 – Describe what data elements are and why they are important

Data element is a data dictionary which can be created or modified by using a process which is called SE11. The purpose of data elements are they are designed to find the characteristics of a table field or a component of a structure. Data element is a term where a process of the functions take place over networks just like protocols.

There are two main types of data elements:

1. Elementary Data Elements – Defined by the data within them (value, length, type).
2. Reference Data Elements - Make use of reference variables mostly used in other ABAP objects.

## CRC

CRC stands for Cyclic Redundancy Check. This is a type of checksum. This is used to check whether the transmission is faulty and if it is, correct it.

## Encapsulation

### Frames

A frame is a way of splitting up a transfer across the network. One example of this is a file transfer. The file would not be sent as one, massive message. Instead it would be split up into lots of different messages, called frames. A frame is mainly used on WANs and LANs.

### Packets

A packet is a collection of frames. A packet is likely to hold more metadata about the information being sent. In an IP packet, 4 bits say whether its IP v4 or v6. 4 bits describe the header size. 8 bits describe quality. 16 bits describe the size. 16 bits describe ID. 3 bits describe whether the packet is whole. 13 bits contain the order of the packets. 8 bits hold the record time. 8 bits hold the protocol. 16 bits contain a checksum. 32 bits contain a source IP. 32 bits contain destination IP.

## Datagrams

A datagram is a less reliable version of a packet. Packets are sent via TCP. This protocol ensures that the packet reaches its destination. This means that when you send a packet, it must reach the destination. Datagrams are sent over UDP. This is where a connection is not guaranteed and is instead seen as a “best effort” approach.

## Addresses

Addresses are as it sounds. They are a way of identifying the location of a device. There are 2 types of address,

1. Physical address – known as a MAC address, this is often hard coded into a device or network card.
2. Logical address – known as IP address, is configured by the owner of the network and can be changed.

Addresses are used so that network hardware knows where to send traffic. Without addresses, data may become jumbled and may reach the wrong destination.

## Sequence Numbers

Sequence numbers are identifiers on packets and datagrams that show what order they were sent in. This is done because if there is any change in the network during transmission, data may reach the destination faster than before. Without this, data would come to a device in the wrong order and therefore assembled wrong. This may cause data to be seen wrong and therefore be useless.

# M1 – Explain why communication protocols are important

A protocol is a set of standards that makes up a way of doing something that has high amounts of support.

There are three main types of protocols:

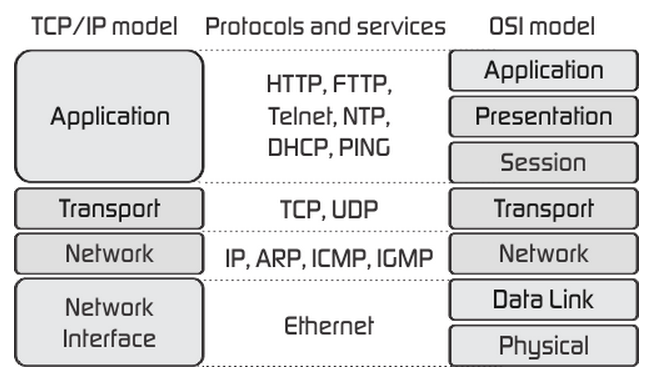
1. Network Communication Protocols – Basic communication protocols (HTTP, TCP/IP)
2. Network Security Protocols – Implement security on a network (HTTPS, SSL, SFTP)
3. Network Management Protocols – Gives network control and overview (SSH, SNMP, ICMP)

Without protocols data may be seen wrong. It may be seen in a correct format with the wrong information or just entirely no readable.

## Example

If one protocol says that transmissions must *start* with the address of the destination and another says that it should *end* with the address, then it could be confusing. The recipient would read its own address as readable data. This could be very damaging, especially over multiple transfers. That is why it is important to decide on a protocol before transmission begins.

# D1 – Compare the OSI seven-layer model and the TCP/IP.



## OSI

The OSI model is the seven layered model shown on the right of the picture above. Its role is to standardise the transmission of data of a telecoms or computing system. Each layer of the model serves the layers above and below depending on whether sending or receiving,

## TCP/IP

The TCP/IP model is the 4-layer model shown above on the left. It is often used to easily split up network communication in a very primitive way.

|  |  |  |
| --- | --- | --- |
|  | Features | Uses |
| OSI | * Has 7 layers * Is more in depth that TCP/IP * It presumes that applications have no direct access to any layer below it | Can be used in most network (mainly telecoms and computing). Is used to break down the infrastructure to make management more straight forward. |
| TCP/IP | * Is easy to break down as only has 4 layers * It can be implemented in *any* network. * It does not need IP addresses to work and so can allow for user friendly names | Can be used in *any* network.  Is used to break down the infrastructure to make management more straight forward. |