# Networks and Transmitting Data

## Networks

- Networks are collections of connected computing devices. They consist of a number of devices known as nodes: mostly computers but also shared peripherals like printers and scanners.

- Devices need to be connected to networks by **network interface cards (NICs)** or by using equivalent circuitry embedded in their electronics. Each device must be uniquely identifiable so that messages intended for it are delivered correctly.

**Reasons for Having Networks**

- Most organisations and individuals have networks. They have become important because of the need to communicate and share data.

- A central store of data enables all the users of the system to see the same up-to-date version of the data they need.

**Private Networks**

- Most organisations still have their own private networks. The advantages of having these include:

- Control over security.

- Complete control over who has access to what resource.

- Control over what software is provided.

- Confidence of availability.

- However, these conveniences come at a cost. A large network needs specialist staff to keep it running all the time and also to maintain security.

- Most organisations are completely dependent on their networks so if it loses functionality this could be a major disaster.

- Various methods are utilised to minimise this risk:

**- Redundancy** - Where essential equipment is duplicated.

**- A sensible backup regime** - So that there is always a copy of essential data stored somewhere else.

**- Failover System** - These detect abnormalities and automatically transfer operations to an alternative system.

**- A Disaster Recovery Plan** - This is necessary so that in the event of a major failure procedures are in place to limit the impact of the failure and remedies are applied effectively.

## **Hardware**

Networks are built on certain common items of hardware. These are concerned with generating, transmitting and interpreting electric signals.

**Network Interface Cards (NICs)**

- Circuits that in the past were plugged into the computer’s bus to produce signals that are placed on the transmission medium and also receive signals from it.

- NICs are designed to work with particular networks standards, and by far the most widespread is Ethernet. So common most computers have Ethernet circuitry built onto their motherboards rather than requiring cards as add-on.

- NICs work as the physical and data link layers of the OSI network model.

**MAC Addresses**

- These are 48 bit identifiers allocated to network devices by the manufacturer. Normally they are quoted in human readable groups as 6 bytes or octets and displayed as Hex digits. A typical MAC address could be 08:01:27:OE:B8.

- The first three octets identify the manufacturer the others are allocated to make each one unique.

**Routers**

- A router is a device that connects networks. It receives data packets from one network and forwards them to another network based on the address information in the packet.

- Routers determine where to send a packet according to either a table of information about neighbouring networks or by using algorithms.

- More advanced than a switch as a router can analyse the packets of data, change how they’re packed and send packets to another network.

**Hubs**

- A network component that forwards all packets to all clients, has multiple ports.

**Switch**

- A network component that stores the IP addresses of clients, and only forwards packets to the right client.

**Wireless Access Point**

- A device that allows clients to connect to the network wirelesslly. WAPs can be protected by hiding the SSID so only people who know of its existence can connect.

- Encryption between client and WAP use standards like WPA2 and limiting connections to certain MAC addresses.

**Repeaters**

- A device that takes a signal and repeats it to extend the range of a network.

**Gateway**

- Serves as an entrance from one network protocol to a different one.

**Bridge**

- Connect a LAN to another LAN using the same protocol.

**Types of Network**

**Peer to Peer**

- All computers are equal, no one has priority over another.

- All computers are controlled by the individual owner.

- Often makes use of a hub to connect the computers together.

**Cons**

- No network wide security in place.

- A user may restart their machine when its being accessed by another.

- Harder to back up as its not centralised.

**Client-Server**

- The server provides services to the rest of the machines on the network, such as storage, computational power, and services.

**Pros**

- Allows for central control of security.

- Easier to supervise network performance.

- Easier to upgrade software.

- Faster performance as fewer data collisions and server is likely to be optimised to serve multiple clients simultaneously.

**Cons**

- A system admin is needed to manage the server.

- There is more infrastructure needed.

- If the server goes down, the impact would be greater than one machine going down on a peer to peer server.

**Parallel and Serial Transmission**

**Parallel Transmission**

- A group of bits are transmitted at the same time over the same number of paths.

**Serial Transmission**

- All the bits that comprise the data are transmitted one bit after another in a continuous line. Slower than parallel. Examples are **USB, Bluetooth and Firewire.**

**Transmission Direction**

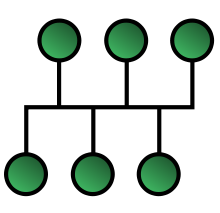
- Data transmission may also be characterised by the direction in which signals travel.

**Simplex (One way):** Television and teletext are examples. The signal travels only in one direction, away from the broadcaster towards the audience.

**Half-Duplex (One direction at a time):** For example intercom systems.

**Full-Duplex (Two directions at same time):** Ethernet and telephones are both examples of a full-duplex systems. Channels may be separated either logically (e.g different frequencies) or physically (e.g different wires).

**Network Topologies**

**Bus**

- A network in which all servers and clients are connected to a common link called the bus.

- All nodes will receive all traffic and all packets have equal priority.

**Pros**

- If one node fails then the network can continue unaffected.

- Easy to connect a new client to the main bus.

- Works well for small networks.

- Easy to extend the network.

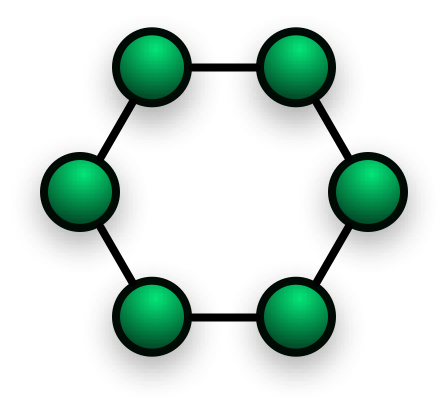
- Requires less cabling than a star.

**Cons**

- Entire network fails if the bus is damaged.

- Large amount of packet collision on network if many people are using it simultaneously so high amounts of packet loss.

**Ring Networks**

- A network in which every node is connected to two other nodes.

- Some implementations allow traffic in only one direction and others allow both directions of travel.

- Unidirectional implementations can have a fallback loop so that in the case of failure of a single node traffic can go the other way.

**Pros**

- Performs better than a bus network under heavy loads.

- Doesn’t need a central server.

- Point to point line makes it easy to identify and replace faulty cables.

**Cons**

- One malfunction can cause problems for the whole network, this can be solved with a bi-directional design.

- Moving and changing the devices can affect the network.

- Poor performance with many clients.

**Star Networks**

- A network where each node is connected to central hub.

**Pros**

- If one node, or cable connecting that node malfunctions then the rest of the network isn’t affected.

- Devices can be added without disturbing the network.

- Good performance as no data collisions.

**Cons**

- Expensive because of the amount of cables needed.

- If the central hub fails then the whole system goes down.

**Mesh Networks**

- A network where each node relays data for the network.

- All nodes cooperate in the distribution of data.

- Often makes use of self-healing algorithms like shortest path bridging, so if a node goes down then the algorithm attempts to find another route.

**Cloud Computing**

- Increasingly organisations and individuals are moving away from maintaining their own networks and devolving many of the responsibilities to outside organisations; so-called outsourcing.

- Providers of such services often supply not only storage space but also software that can be remotely accessed.

- This is called software as a service (SaaS).

**Advantages:**

- Economies of scale – cost of services is shared between many users.

- Removal of the need to install and upgrade software.

- Removal of the need to hire specialist technical staff.

- Removal of the need to back up data.

**Disadvantages:**

- Handing security control to another party could be risky.

- Some risk of losing data.

- Some risk of losing access to the service and having no means of recovering it.

- Trust issues in general but the conveniences are normally worth it.

**More Network Terms**

**SAN –** Storage Area Network. A high speed networked storage device that allows clients to access the same data. It can increase the application performance by offloading heavy read/writes to specifically optimised hardware. SANs appear to be locally attached to clients which allows for easier integration with existing software.

**MAN –** Metropolitan Area Network. A network that connects clients in an area larger than a LAN but smaller than a WAN. These networks may be found in university campuses. The term may also be applied to the interconnection of smaller local networks into a larger network which may in term allow for more efficient connection than a WAN.

**PAN –** Personal Area Network. A network used for transmitting data between devices such as computers, tablets and PDAs. Examples include wireless keyboards and bluetooth.

**Layering**

- Divide and conquer (surprise surprise) is used to decompose the development of networks into components which are each easier to solve than the larger problem.

- This has led to the concept of layering whereby different aspects of the network’s functionality are conceptualised and developed separately.

- Each layer concepts on one aspect without worrying about the others and only communicates with the layers directly adjacent to it.

- One approach is a three layer system:

**1. Application Layer:** Concerned with the collection and dissemination of data that is being sent across the network. Needs to know about the nature of the data being collected so it can be validated and packaged. Application layer does not concern itself with how data will get to intended destination.

**2. Network Layer:** Doesn’t care about what data is being transmitted. It is concerned with the layout of the network, what nodes are there, what topology is being used and how best to get the data efficiently from source to destination.

**3. Physical Layer:** Data has to be transmitted via some medium. Physical layer does not concern itself with the nature of the data or the route being taken it just provides a transport medium to conduct the message as instructed by the network layer.

**Open Systems Interconnection (OSI)**

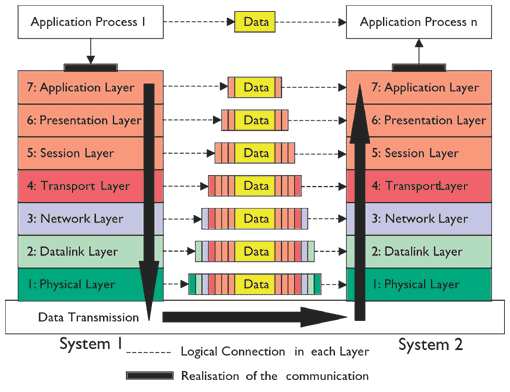
- In reality, most networks are more complex than the three layer model, OSI is an openly available model devices by the International Standards Organisation consisting of a stack of seven layers.

- Further subdivides functionality allowing further refinement and focus on detail.

- Layering is vitally important to get many different manufactures of hardware and different programming languages working together.

- Every piece of hardware and software is designed to fit in one layer and communicate using defined protocols with its adjacent layers.

- The OSI model provides the following abstraction. The layer numbers are normally presented in reverse order so that the applications are shown as high level:



**Sender**

**Receiver**

- A message sent across a network will pass down through the layers of functionality then at the destination will pass back up in reverse order.

- As data moves down through the layers it is encapsulated and additional information is added as headers and trailers.

- As data moves back up the layers of encapsulation are stripped.

- The data itself does not change.

**Acronym**

**P**lease **D**o **N**ot **T**ake **S**ausage **P**izza **A**way

**The Layers**

**1. Physical**: Transmits data on the medium. Network deices and transmission media. Protocols include ethernet, Bluetooth and DSL. Hubs and NICs are in this layer.

**2. Data Link:** Control of access, error detection and correction. Adds the MAC address to the packets. NICs, bridges, repeaters and switches could be in this layer protocols used could be MAC, WAP, WPA.

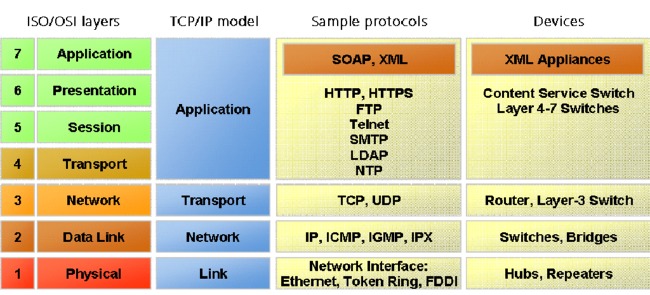
**3. Network:** Transmission of data packets and routing. Adds network addresses to the packets. Maps the network addresses to the devices physical address. Protocol include IPv4 and IPv6 and devices in this layer could be routers.

**4. Transport:** Concerned with keeping track of segments of a network, checking successful transmission, packetisation and flow control. Protocol include TCP and this is the layer where firewalls are.

**5. Session:** Looks after starting, managing and terminating connection sessions. Provides simplex, half-duplex and full duplex operation. Handshaking allows detection of lost packets and re-transmission.

**6. Presentation:** Looks after any conversion between data as sent on the network and data as needed by applications. May involve encryption/decryption operations and compression.

**7. Application:** Layer closest to the user. Collects or delivers data and passes it to and from the presentation layer.



- Because the OSI model is an open standard anyone is free to make use of its ideas. Most networks are based to some extent on the OSI model often mergning some of its layers.

- The most widely used network model is the TCP/IP standard. This stands for Transmission Control Protocol and Internet Protocol. The layers are as such:

**Network Protocols**

- The network protocol establishes the format in which data is transferred, **how to establish and terminate communication,** how to **correct errors** and how to **compress data**.

- Example protocols:

- TCP/IP

- HTTP – used for websites

- FTP

- Telnet – Used to allow users to logon to remote computers.

- WAP

- Another common protocol as well as TCP/IP is http (hyper text transfer protocol) which is used to transmit world wide web pages.

**TCP/IP Stack**

- Complete set of protocols covering data transmission across a network. It governs how data should be formatted, addressed, routed and received.

- Four layers of abstraction.

**1. Application:** Concerned with the production, communication and reception of data. Applications need to be concerned that the data they generate is in the format acceptable to application that will make use of it. This layer also includes the means of packing up data and handing to the transport layer. Protocols such as HTTP and FTP operate at this level.

**2. Transport:** This is concerned with the establishment and termination of connections between network entities via routers. It is responsible for providing a reliable flow of data across a network.TCP involved in this layer.

**3. Internet:** Provides links to transmit datagrams across different networks. Not concerned with individual network types and, as such, is the essential feature of the internet allowing exchange of data between any networks. Internet protocol (IP) is the protocol used as this layer and directs datagrams from one router to the next. A datagram is a self-contained, independent entity of data that carries sufficient information to be routed from the source to the destination.

**4. Link:** Not concerned with routers. Concerned with passing datagrams to the local physical network. Designed to make the overall network hardware independent so it can operate over any transmission medium.

**Transmission Control Protocol (TCP)**

- The first part TCP governs how messages are prepared and how they are decoded.

- Can be broken down into two parts: rules for sending data and receiving data.

When sending data TCP rules include:

**Divide the message into chunks of data** called packets.

**Add a sequence number** to each packet. This lets the receiving computer know what order the packets are supposed to be re-assembled in.

**Add error-correction data**, so errors introduced during transmission can be spotted and fixed.

When receiving data TCP protocol includes:

**Examine each packet for errors** by using the extra information that was added to it.

**Fix errors** if possible or request that packet be resent.

**Identify missing packets** and request for them to be resent.

**Reassemble the message** in the correct order, using the sequence number of each packet.

**Send the message on** to the correct application

**Internet Protocol (IP)**

- The second part of the TCP/IP protocol is IP.

- IP allows computers to address their messages to the correct destination, and allows the destination computer to determine whether a message that they received is meant for them.

- Just like TCP, IP is broken down into sending and receiving.

For sending data IP protocol includes:

**Add the destination address** to each data packet so the network knows where the data is going.

**Add the source address** to each data packet so the network knows where the data is coming from.

For receiving data IP protocol includes:

**Accept data packets** that have the computer’s address attached.

**Ignore all data packets** that do not contain its own address, as they are meant for someone else.

**Other Protocols**

**User Datagram Protocol (UDP)**

- Resides in transport layer of four layer model like TCP.

- **Connectionless,** does not do any handshaking to make data transfer more reliable. Instead, it just sends datagrams directly, and assumes it will be error free.

- Used in video conferencing and video games because losing the occasional datagram will not adversely affect them. Faster than TCP.

**Hyper Text Transfer Protocol (HTTP)**

- Protocol underlying the world wide web.

- Web pages are sent and received with this protocol.

- Resides in application layer of four layer model.

- A web page is made up of a collection of individual files – text, images, styling, javascript etc. The http protocol allows a browser to request these individual files from a web server in an orderly way.

**File Transfer Protocol (FTP)**

- Standard network protocol for transfer of files between a client and server on a computer network.

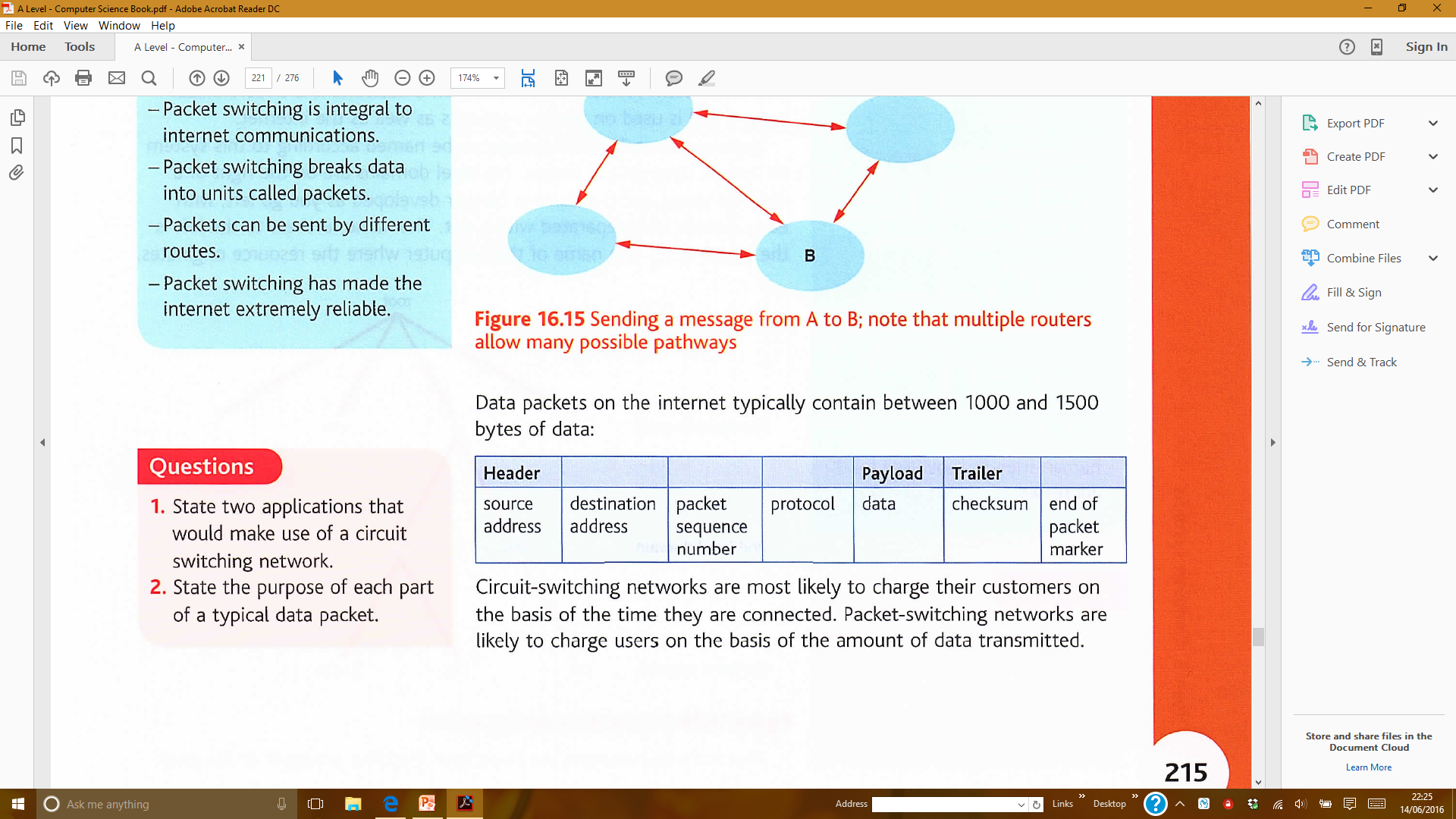
- Application layer.

- Built into modern web browsers to allow you to download or upload files directly from a normal web page.

**Ethernet**

- Belongs in data link/network layer. Family of protocols responsible for sending and receiving data along a network cable.

- Physical protocol.

**Packets**

-Packets are made up of:

- Each packet is sent off via the best available route so each packet can take a different route.

- Much easier to balance the load across various pieces of equipment if data is split into many similarly sized packets.

- If there is a problem with one piece of equipment packets can be routed around the issue.

- Typically 1000-1500 bytes in size.

- Two ways of sending packets across a network: **circuit switching** and **packet switching.**

**Circuit Switching**

- Three phases: connection establishment, data transfer and connection release. The path is reserved for the duration of the message then shut down.

**Advantages:**

- Packets arrive in correct order.

- Performance is predictable.

- Can be used for digital and analogue.

- Simple to create, data can go in one stream rather than in packets.

- Cheap.

- Good for long lasting data transmission.

**Disadvantages:**

- If the single circuit fails the whole transmission fails.

- Doesn’t fully utilise equipment.

- Prevents other users from using routes until transfer is complete.

- Much easier to intercept transmission.

**Packet Switching**

- Packets are sent along the most efficient path at that time, so packets may arrive out of order.

**Advantages:**

- Loss of a small piece of infrastructure may not be critical.

- Better utilisation of equipment.

- Packets can be routed around problems.

- Makes internet much more reliable.

**Disadvantages:**

- Slower message transmission.

- More complex.

- Packets need to be reordered on receipt.

- Can’t be used for analogue data.

- May struggle with time sensitive data in a congested network.

**IP Addressing**

- Messages are directed across a TCP/IP network using IP addressing.

- IPv4 and IPv6 are currently in use.

- IP addresses can be static for a particular machine or assigned dynamically using DHCP.

**Domain Name System (DNS)**

- Top level domains include .com and .uk

- DNS allows user friendly names like google.com to be converted into IP addresses.

- A Domain Name Server is used for this conversion.

**Network Ports**

- A **port** is the endpoint for network communication. It’s the address for a specific application or process within the computer that the message is sent to.

**Sockets**

- A socket is the full destination addressed.

I.e

IP: 192.168.1.1

Port: 80

Socket: 192.168.1.1:80