3. Communication

Networks

A network consists of a number of computer systems connected together. There are many advantages and disadvantages of using a computer network over a stand-alone computer.

Advantages	Disadvantages
• Share hardware • Share software • Share data/files • Easier for internal communication/can send email • Central backup • Easier to monitor network activity • Centrally controlled security • Can access data from any computer	• A network manager may need to be employed – expensive • Security problems – files sent between computers could spread a virus • Hackers can gain access to data more easily • If the server is down, all workstations on the network are affected • Initial cost of servers, communication devices, etc. can be expensive

There are two main types of network, namely a **Local Area Network (LAN)** and a **Wide Area Network (WAN)**.

A LAN is a network in which the computer systems are all located relatively close to each other, for example, in the same building or on the same site, such as a school.

A WAN is a network, in which the computers systems are all located relatively distant from each other, for example, in different buildings all over the country or in different countries. The Internet is an example of a WAN. You will note that many LANs could be linked using a WAN.

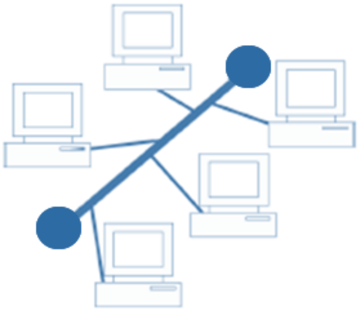
Computer networks use agreed upon protocols to communicate, i.e. common methods of sending data and consistent data formats. If they did not agree on the protocols to be used, the individual computer systems would not be able to communicate with each other.

Network topologies

A network topology is the theoretical layout of computer systems on a network. There are a number of different network topologies. Common network topologies include:

- bus network
- ring network
- star network

Bus network

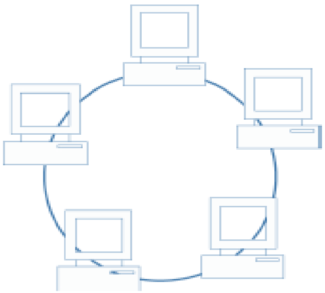


The computer systems, also called *nodes* of the network, are each connected to a single cable on which data can be sent, called the bus. A bus network has terminators on each end, which is needed to ensure that the network functions correctly.

The bus carries packets along the cable. As the packets arrive at each computer system, it checks the destination address contained in the packet to see if it matches its own. If the address does not match, the computer system ignores the packet. If the address of the computer system matches that contained in the packet, it processes the data.

Advantages	Disadvantages
● Easy to implement and add more computer systems to the network ● Quick to set up – well suited for temporary networks ● Cost-effective – less cabling	● It is difficult to troubleshoot the bus ● Limited cable length and number of stations – performance degrades as additional computers are added ● If there is a problem with the main cable or connection, the entire network goes down ● Low security – all computers on the bus can see all data transmissions ● Proper termination is required ● Data collisions are more likely, which causes the network to slow down. A collision is when two computers try to send a packet at the same time

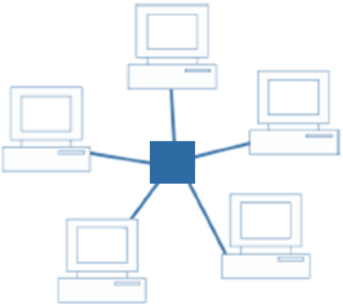
Ring network



In a ring network, computer systems are connected in a ring or a loop. Packets are sent around the ring, being passed from one computer system to the next until they arrive at their destination.

Advantages	Disadvantages
• Data is quickly transferred without a bottleneck – consistent data transfer speeds • The transmission of data is relatively simple as packets travel in one direction only • Adding additional nodes has very little impact on bandwidth • It prevents network collisions.	• If any of the computer systems fail, the ring is broken and data cannot be transmitted efficiently • If there is a problem with the main cable or connection, the entire network goes down • It is difficult to troubleshoot the ring • Because all nodes are wired together, to add a another you must temporarily shut down the network

Star network



In a star network, each computer system is connected to a central node, also known as a hub.

Advantages	Disadvantages
• Good performance/fast network speed • Easy to set up • Possible to add more computer systems without taking the network down • Any non-centralised failure will have very little effect on the network • Minimal network collisions • Better security	• Expensive to install – more cabling required • Extra hardware required, such as a hub

Connectivity

To connect a computer system to a network, a Network Interface Card (NIC) is required. A physical hardware port allowing a cable to connect your computer system to the network provides one method of connection. The second method is to connect a computer system using a wireless connection, called a Wi-Fi.

Typical network speeds

A physical connection may be made using:

- a copper cable, with typical data transfer speeds of between 100 Megabits per second (Mbps) and 1 Gigabit per second (Gbps)
- a fibre-optic connection which has typical data transfer speed of between 1-10 Gbps

Wi-Fi connections have typical data transfer rates of 54 – 108 Mbps. However, this can be severely affected by the distance between the device providing the Wi-Fi connection and computer systems. The data transfer rates can also be severely affected by atmospheric conditions, in particular heavy rain.

Circuit switching

Circuit switching is a networking technology that provides a temporary but dedicated link between two stations or nodes regardless of the number of switching devices through which the data has to travel. During the connection no other data can be transmitted along the same route. The landline telephone system is an example of a circuit switched network. When you phone someone and they answer a circuit connection is made and you can pass data along the connection until you put down the telephone to end the connection.

The main advantage of circuit switching is that it is reliable and once the connection is established it is fast and generally error free. However, it takes time to establish the connection. Should anywhere on the route fail then the connection will be broken.

To overcome the problems with circuit switching, packet switching was developed. Rather than relying on a dedicated connection packet switching breaks the data down into small packets that can be sent by more than one route.

Packet

A **packet** is a collection of data that is transmitted over a **packet-switched network.** Packets are provided to a network for delivery to a specified destination. Each packet of data is redirected by a computer system along the network, until it arrives at its destination. Data may be split up into a number of packets. These packets are transmitted over a network and may take different routes to its destination. When all the packets have arrived the data is reassembled. The Internet is an example of a packet-switching network.

Here is a simplified diagram showing what a packet will typically contain:

<table>
<tr><td>The source address</td><td>The destination address</td></tr>
<tr><td colspan="2">Information which enables the data to be reassembled into its original form</td></tr>
<tr><td colspan="2">Other tracking information</td></tr>
<tr><td>The data itself</td><td>A checksum that checks that the data has not been corrupted</td></tr>
</table>

INTERESTING FACT

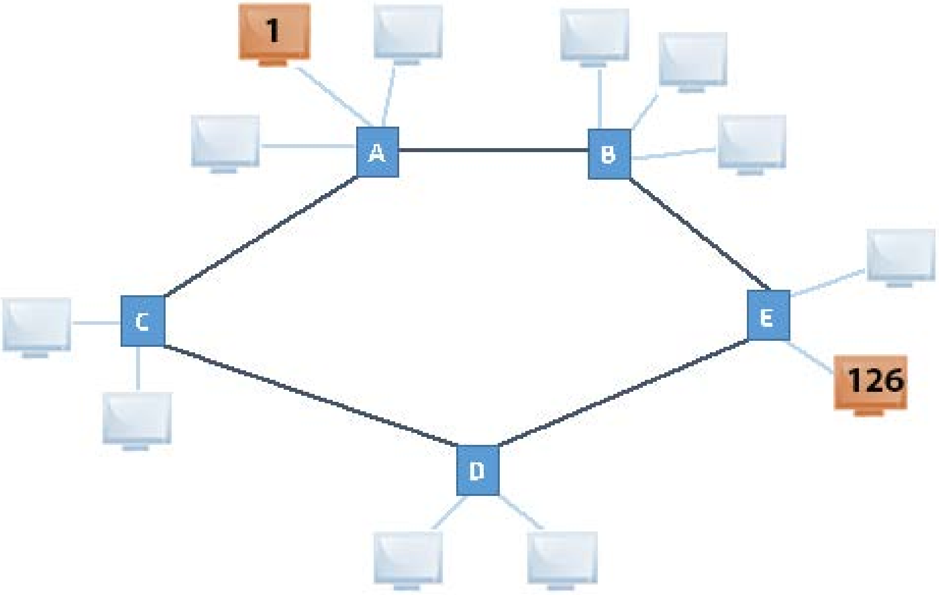
When packets are transmitted over a Wi-Fi network, they can be intercepted by any device, this is called *packet sniffing*. If you perform thorough analysis on a large number of packets, you can often break the encryption. This is why security services, such as National Security Agency, do not allow any Wi-Fi devices on their network.

Packet switching (including data redundancy)

Packet switching is the process of delivering packets from one computer system to another using a designated device, such as a *switch* or a *router*. Packets are provided to a network for delivery to a specified destination. Each packet of data is redirected by a computer system along the network, until it arrives at its destination. Data may be split up into a number of packets. These packets are transmitted over a network and may take different routes to its destination. When all the packets have arrived the data is reassembled. The Internet is an example of a packet-switching network.

Routing

Routing is the name given to the method of selecting paths along which packets are sent on a computer network. Specialist computer systems such as routers, switches, bridges, firewalls and gateways construct in their memory a *routing table*, which stores a number of paths along which it is best to send packets to reach a specific destination. Maintaining accurate routing tables is essential for ensuring that packets are delivered as quickly as possible.



In the example shown, computer system 1 is sending a packet to computer system 126. Clearly, the quickest route for the packet to arrive at its destination is to be sent from router A, on to router B followed by router E for delivery to computer system 126. This path would be determined by routing, using a routing table. A poorly constructed routing table may choose to send the packet from router A, on to router C followed by router D and then router E, for delivery to computer system 126. This would take longer and is not a good use of network resources.

Most routers use only one network path at a time, such as the preferred route above (Computer system 1 > Router A > Router B > Router E > Computer system 126). Some multipath routing techniques enable the same packets to be sent using multiple alternative paths at the same time. This means that in the event of Router B failing in the transmission above, the same packet would also have been sent via the alternative longer route set out above (Computer system 1 > Router A > Router C > Router D > Router E > Computer system 126), to ensure that the packet arrives at its destination.

MAC addresses

A MAC address (media access control address), also known as a physical address or a hardware address, is a unique hexadecimal number given to any communication device, such as a network interface card. An example of a MAC address is 74:E1:B6:8E:18:77. The address is usually stored in a communication devices' ROM. Hexadecimal notation is used as it allows for over 281 trillion different combinations of MAC address.

INTERESTING FACT

Although MAC addresses are designed to be unique and unchangeable, some devices or specialised software allow you to change your own MAC address. This is called *MAC address spoofing* and can be used by hackers to trick computer systems into providing data.

Routing tables store the MAC address of communication devices on its network, as the address is permanent and does not change like an IP address. A computer system can have multiple network interface cards, each with its own unique MAC address.

IP addresses

An IP address is an address, which is allocated to a computer system on a network, usually by a DHCP (Dynamic Host Configuration Protocol) server. Alternatively, you may assign your own IP address if you do not wish to rely on the services of a DHCP server. An example of an IP address is 195.10.213.120.

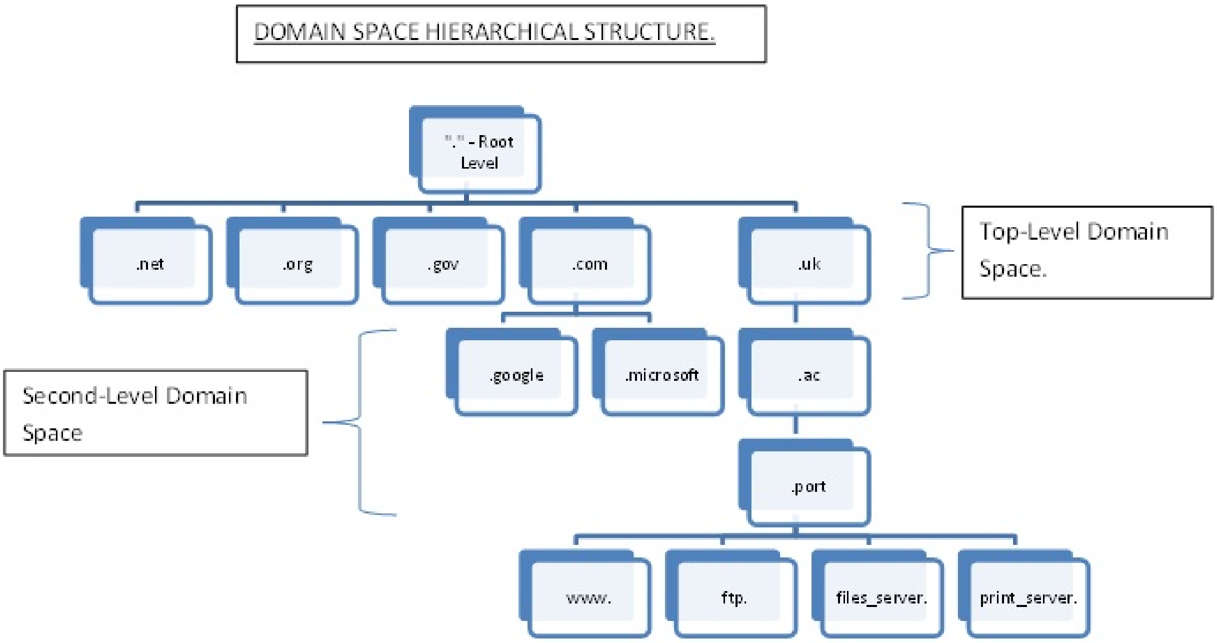
It is used to uniquely identify computer systems on a network, thus allowing communication between them. In routing tables, the corresponding IP address of a unique MAC address is stored and updated as necessary.

Internet Domain Name System (DNS)

A Domain Name System (DNS) is a distributed database that matches IP addresses to computer system resources.

One example of this is to match an IP address to a human friendly domain name. For example, if you wanted to visit the Google search engine, the computer system on which the website is stored has an IP address assigned to it; 173.194.34.191. Try typing this into the address bar of your web browser; you should be able to view the website that you would be more familiar with when accessing the domain name www.google.co.uk. Here your computer system sent a request to its DNS server for the IP address that is mapped to the domain name www.google.co.uk. The DNS server returned the IP address 173.194.34.191, which allowed your computer system to communicate with the computer system where the Google search engine is stored.

Of course there are many different DNS servers located across the world. If your local DNS server does not store the address of the resource you are requesting, it will pass the request along to another higher level DNS server, such as your Internet Server Provider's (ISP) DNS server. If again the address is not found, you ISPs DNS server will pass the request on to a higher level DNS server which may be the DNS server responsible for an entire zone, such as the *.co.uk zone*. This continues until the address is found or the DNS query fails.



Another example where a DNS server is used is where a computer system, on joining a network, would query the DNS server for the IP address of other useful computer systems, such as the logon server, which stores the details of all usernames and passwords.

INTERESTING FACT

In 2015 users of YouTube uploaded 400 hours of video every minute. That means that 1000 days of video are uploaded every hour of the day.

Protocols

A **protocol** is an agreed format, which allows two devices to communicate. The protocol, put simply, is a set of rules. These rules can include the following:

- handshaking, where two devices establish their readiness to communicate
- how the sending device will indicate that it has finished sending a message
- how the receiving device will indicate that it has received a message
- the type of error checking to be used
- agreement on the data compression method to be used

There are many standard protocols used with computer systems. The table illustrates the protocols with which you need to be familiar:

Protocol	Description
TCP/IP (Transmission Control Protocol/Internet Protocol)	Two protocols that combine to allow communication between computer systems on a network. IP is a protocol that sets out the format of packets and an addressing system. TCP is a protocol that allows packets to be sent and received between computer systems
HTTP (Hypertext Transfer Protocol)	HTTP is a protocol than can be used to transfer multimedia web pages over the Internet.
FTP (File Transfer Protocol)	FTP is a protocol that can be used when copying a file from one location to another via a network or the Internet. It is typically used for the transfer of large files, as it allows broken communications to resume transferring a file rather than having to restart.

A **protocol stack** is a set of protocols that work together to provide networking capabilities. It is called a stack because it is designed as a hierarchy of layers, each supporting the one above it and using those below it. The use of a layered approach enables different protocols to be substituted for each other to allow for e.g. new protocols and different network architectures. The number of layers varies according to the particular protocol stack. However, the lowest layer will deal with physical interaction of the hardware, with each higher layer adding additional features, and user applications interacting with the top layer.

INTERESTING FACT

Although the Bluetooth protocol has been agreed, the protocol stack varies considerably from device to device. Try sending a photograph via Bluetooth from one smartphone to another.

TCP/IP 5 layer protocol stack model

TCP stands for *Transmission Control Protocol* and IP stands for *Internet Protocol*. There are five layers to this model:

- Physical layer
- Data link layer
- Network layer
- Transport layer
- Application layer

Physical layer

The physical layer transmits the raw data. It consists of hardware such as switches and routers. The layer deals with all aspects of setting up and maintaining a link between the communicating computers.

Data Link Layer

The data link layer sends data from the network layer to the physical layer. It divides the data to be sent into data frames. A data frame consists of a link layer header followed by a packet. The data link layer handles the acknowledgements sent from the receiver and ensures that incoming data has been received correctly by analysing bit patterns in the frames.

Network layer

The network layer is responsible for the addressing and routing of data. Routers belong to the network layer as they use logical addresses to direct the data from the sender to the receiver. A router determines the path the data should take based on network conditions. Routers manage traffic problems on the network such as the routing of packets to minimise congestion of data.

Transport layer

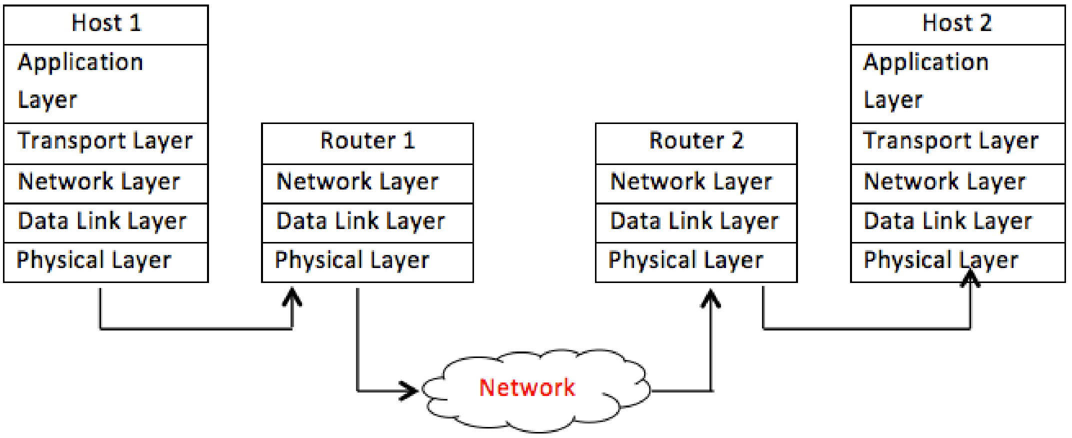
The transport layer ensures that data is transferred form one point to another reliably and without errors. The transport layer is responsible for making sure that data is sent and received in the correct order. The transport layer is implemented in the sending and receiving computers but not in the routers on the path between them. It acts as an interface between the communicating computers and the network.

Application layer

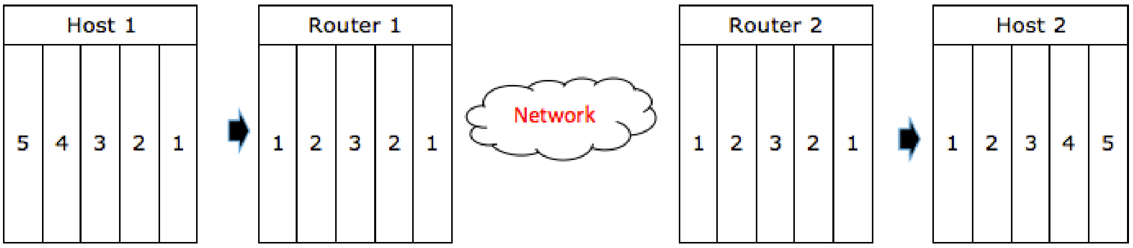
The application layer provides interfaces to the software to allow it to use the network. Examples of software include email, file transfer protocol (FTP) and the World Wide Web (WWW).

Sending data from Host 1 to Host

The diagram shows Host 1 sending a message to Host 2. From Host 1 the data flows down through the 5 layers of protocols and then to Router 1. Router 1 is the gateway to the operating area of Host 1 and therefore only the network, data link and physical layers are involved. Similarly, with Router 2 only the three layers are involved as the data is passed into the operating region of Host 2. Finally the data passes up through the layers to Host 2.



Data flow through layers



Layers and protocols

Layer	Protocol
Application layer	Hypertext Transfer Protocol (HTTP) Simple Mail Transport Protocol (SMTP) File Transfer Protocol (FTP)
Transport layer	Transmission Control Protocol (TCP)
Network layer	Internet Protocol (IP)
Data Link Layer	Ethernet Protocol
Physical Layer	Physical connection using a NIC or router to connect to the Internet

Ethernet protocol

At the data link layer Ethernet protocols describe how network devices can format data for transmission using frames and packets. Ethernet protocols are also used to define standards for types of network cabling used at the physical layer and the corresponding transmission speeds.

Wi-Fi protocol

Wi-Fi is a term for certain types of wireless networks that use 802.11 wireless protocols for transmitting data using electromagnetic waves in place of cables. 802.11 wireless networks use security protocols, such as Wi-Fi Protected Access (WPA), to provide a level of security and privacy comparable to that of a wired network. Bluetooth is another example of a wireless protocol and WAP (Wireless Application Protocol) are protocols to standardise the way that wireless devices can be used for Internet access.

Email protocols

To use email you must have an email client on your computer that has access to a mail server. Your Internet Service Provider (ISP) often supplies this server. The mail client and the mail server exchange information with each other using email protocols to transmit information.

1. **IMAP protocol**

   Internet Messaging Access Protocol (IMAP) is an email protocol that stores email messages on a mail server. It allows the email user to read and handle email messages as though they were stored locally on their own computer. The user can manage their email with facilities such as the ability to create folders to organise their messages, store draft messages in the server and delete unwanted messages.

2. **POP3**

   Post Office Protocol 3 (POP3) is the third version of a protocol for receiving email. POP3 receives email for a client and stores it in a single file on the mail server. When the email client logs onto the mail server the email is transfer to the users computer. There are no copies of the email stored permanently on the server after they have been downloaded.

3. **SMTP**

   The Simple Mail Transfer Protocol (SMTP) is used to deliver email from the sender to an email server or when email is delivered from one email server to another. SMTP can only be used to send emails but not to receive them.

INTERESTING FACT

email existed before the World Wide Web. Early email was very simple – it just put a message in another user's directory in a location they could see when they logged on