Unit 2 Communication and Internet Technologies

WAN: network connecting computers on different sites, possibly thousands of kilometers apart.

The benefits of having the computers connected by a WAN were:
- a task could be run on a remote computer.
- a data archive that was stored on a remote computer could be accessed.
- a message could be transmitted electronically to a user on a remote computer.

WAN has following features.
- It will be used by an organization or a company to connect sites or branches.
- It will not be owned by the organization or company.
- It will be leased from a public switched telephone network company (PSTN).
- A dedicated communication link will be provided by the PSTN.
- The transmission medium will be fiber-optic cable.
- Transmission within the WAN will be from switch to switch.
- A switch will connect the WAN to each site.
- There will not be any end-systems connected directly to the WAN.

LAN: a network connecting computers in a single room, in a single building or on a single site.

The benefits of connecting PCs in a LAN included the following.
- The expense of installing application software on each individual PC could be saved.
- A file server could be attached to the LAN that allowed users to store larger files and also allowed files to be shared between users.
- Instead of supplying individual printers to be connected to a user’s PC, one or more printers could be attached to a print server.
- Managers in organizations could use electronic mail to communicate with staff rather than sending round memos on paper.
- The ‘paper-less off ice’ became a possibility.

LAN has following features
- It will be used by an organization or a company within a site or branch.
- It will be owned by the organization or company.
- It will be one of many individual LANS at one site.
- The transmission medium will be twisted pair cable or WiFi.
- The LAN will contain a device that allows connection to other networks.
- There will be end-systems connected which will be user systems or servers.

Wired Media

Twisted pair cabling is a type of wiring in which two conductors (wires) are twisted together for the purposes of cancelling out electromagnetic interference from external sources or other twisted pairs.

Coaxial cable has mainly been replaced for use in long-distance telephone cabling but is still used extensively by cable television companies and is often used in metropolitan area networks.

Fiber optics is a technology that uses glass (or plastic) threads (fibers) to transmit data. A fiber optic cable consists of a bundle of glass threads, each of which is capable of transmitting messages modulated onto light waves.

Fiber optics has several advantages over traditional metal communications lines:
1. Fiber optic cables have a much greater bandwidth than metal cables. This means that they can carry more data.
2. Fiber optic cables are less susceptible than metal cables to interference.
3. Fiber optic cables are much thinner and lighter than metal wires.
4. Data can be transmitted digitally (the natural form for computer data) rather than analogically.

The main disadvantage of fiber optics is that the cables are expensive to install. In addition, they are more fragile than wire and are difficult to splice.
Fiber optics is a particularly popular technology for local-area networks. In addition, telephone companies are steadily replacing traditional telephone lines with fiber optic cables. In the future, almost all communications will employ fiber optics.

Wireless Media

Wireless network refers to any type of computer network that is not connected by cables of any kind. It is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using a transmission system called radio waves.

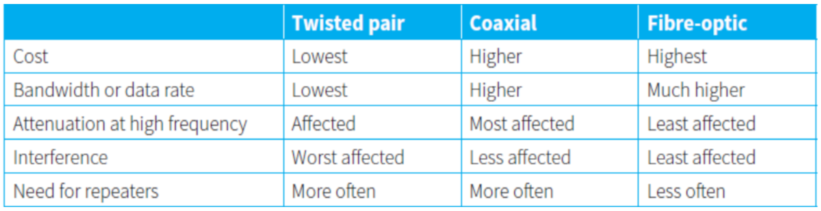
Radio waves are an electromagnetic radiation with differing wavelengths. Radio waves are used for many processes. For example, they are used to broadcast TV, in communication between satellites and it enables computers to share information without wires. However, since they do not have a high frequency, they cannot transmit as much data.

Microwave radio also carries computer network signals, generally as part of long-distance telephone systems. Microwave transmission refers to the technology of transmitting information by the use of electromagnetic waves whose wavelengths are measured in centimeters. Microwaves are widely used for point-to-point communications. The attenuation of microwave is less than twisted pair or coaxial cable. A disadvantage is that microwaves cannot pass around hills or mountains as lower frequency radio waves can. It is also affected by anything blocking the line of sight, such as rainfall.

A satellite is any object that revolves around a planet in a circular or elliptical path. These satellites are typically between 100 and 24,000 miles away. Satellites have many purposes including data communications, scientific applications and weather analysis. Satellite transmission requires an unobstructed line of sight. Microwave signals from a satellite can be transmitted to any place on Earth which means that high quality communications can be made available to remote areas of the world without requiring the massive investment in ground-based equipment.

Transmission Media Comparison

1. The use of specific wireless transmission frequencies is regulated by government agencies and so permission has to be obtained before wireless transmission is used.
2. Outside these frequencies, no permission is needed to use the air for transmission but cables can only be laid in the ground with the permission of landowners.
3. For global communications, the two competing technologies are transmission through fiber optic cables laid underground or on the sea bed and satellite transmission currently neither of these technologies is dominant.
4. Interference is much more significant for wireless transmission and its extent is dependent on which frequencies are being used for different applications.
5. Repeaters are needed less often for wireless transmission.
6. Mobile (cell) phones now dominate Internet use and for these only wireless transmission is possible.
7. For home or small office use, wired or wireless transmission is equally efficient; the lack of cabling requirement is the one factor that favors wireless connections for a small network.

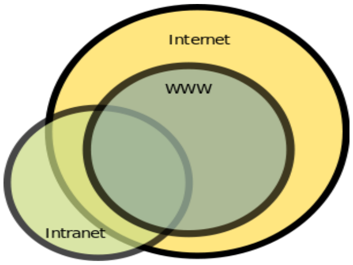


	Twisted pair	Coaxial	Fibre-optic
Cost	Lowest	Higher	Highest
Bandwidth or data rate	Lowest	Higher	Much higher
Attenuation at high frequency	Affected	Most affected	Least affected
Interference	Worst affected	Less affected	Least affected
Need for repeaters	More often	More often	Less often

The Internet: is a global system of interconnected computer networks that use the standard Internet Protocol suite (TCP/IP).

World Wide Web - a system of interlinked hypertext documents accessed via the Internet.

Intranet - a private network within an organization which may offer printer sharing, file sharing, communication, private websites etc...which uses internet technologies such as TCP/IP and web browsers.



The relationships between the internet, intranets and the World Wide Web.

The first thing to notice is that the World Wide Web is not the internet, but a subset of what the internet offers. The internet hosts all forms of data, including games, video, telecommunications etc. while the WWW only transmits hypertext documents. The WWW is accessed through a web browser linking files together using **hyperlinks.**

Server - a computer program running to serve the requests of other programs, the "clients"

Servers are software programs that in most cases run off normal computing hardware. Server software includes:

- Printing
- File sharing
- Game hosting
- Websites
- Other web services

Client - an application or system that accesses a service made available by a server.

Clients are software programs and processes that connect to servers, sending requests and receiving responses. Client examples include:

- Web browser page requests
- Chat systems on mobile phones
- Online games

There are two options for how the client functions.

- A thin-client is one which:
- • chooses an application to run on the server

- sends input data to the server when requested by the application
- receives output from the application.

A thick-client is one which:

- chooses an application provided by the server
- possibly carries out some processing before running the application on the server and also after receiving output from the application.
- alternatively, possibly downloads the application from the server and runs the application itself.

Client-server: an architecture where a client runs an application provided by a server on a network.

Thin-client: a client that only provides input and receives output from the application.

Thick-client: a client that carries out at least some of the processing itself.

The client-server approach is used in following circumstances.

- The server stores a database which is accessed from the client system.
- The server stores a web application which allows the client system to find or, sometimes, supply information.
- The server stores a web application which allows the client system to carry out an e-commerce or financial transaction.

Exercise: Client Servers

Q: Give an example of where a server might be used:

A: Serving websites, hosting games, file sharing, printer sharing

Q: What is a server and what is a client?

A :

- Server - a computer program running to serve the requests of other programs, the "clients"
- Client - an application or system that accesses a service made available by a server

Q: Describe the process involved in a web server delivering a web page to a client:

A :

1. The Client sends a web request to the web server for a web page
2. The server fetches the page items from secondary storage

3. The server sends the page data back to the Client

Q: Describe a situation where having a single server and many client model might not work too well:

A :

1. When all the clients try to access the server at once, it will have too many requests and fail
2. When the clients are a long distance from the server, meaning response times will be slow
3. When the location housing the server suffers a power outage or other disruption, there is no other way for the client to get the data.

File sharing: If a user uploads files to a file server then the client-server operation can be used by another user to download these from the server.

Peer-to-Peer Networking: a peer-to-peer network operates with each peer (networked computer) storing some of the files. Each peer can therefore act as a client and request a file from another peer or it can act as a server when another peer requests the download of a file.

Advantages of Peer-to-Peer Networking:

- it avoids the possibility of congestion on the network when many clients are simultaneously attempting to download files.
- parts of a file can be downloaded separately
- the parts are available from more than one host.

Hardware Connection Devices

Network interface card (NIC): Each NIC has a unique 'physical' address. This is sometimes referred to as the MAC address. The end-system itself has no identification on the network. If the NIC is removed and inserted into a different end -system, it takes the address with it.

HUB: A hub ensures that any incoming communication is broadcast to all connected end-systems.

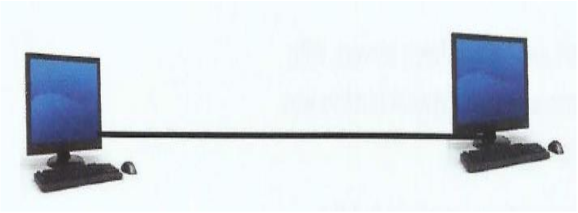
SWITCH: A switch can function as a hub but it is a more intelligent device and, in particular, can keep track of the addresses of connected devices. This al lows a switch to send an incoming transmission to a specific end -system as a unicast. This facility obviously reduces the amount of network traffic compared to that generated by a hub.

ROUTER: A router is the most intelligent of the connecting devices. It is in effect a small computer.
It can function as a switch but the router can make a decision about which device it will transmit or received transmission to.

Repeater: a device that connects two cables and provides a full-strength signal to the second cable.
Bridge: a device that connects two segments of a LAN.
Wireless Access Point (WAP): the connecting device in a WiFi LAN.
Wireless Network Interface Card (WNIC): provides the NIC function in a WiFi LAN.

Network Topologies:

1- Point-to-point connection: The simplest possible network is where two end-systems are connected by a network link as shown in below figure. This is an example of a point-to-point connection for which there is a dedicated link.



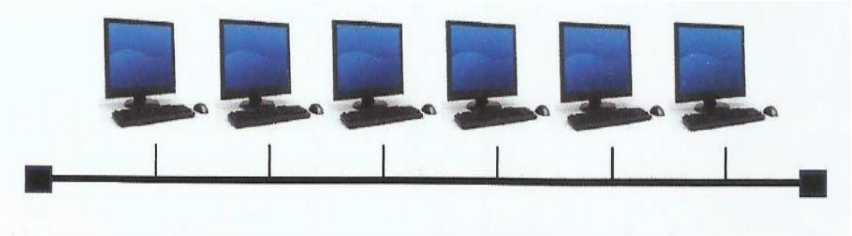
2- Bus Topology: A bus topology also has only one link but it is shared by a number of end -systems and is therefore described as a multi-point connection.

Benefit

- It is easy to set-up and extend bus network.
- Cable length required for this topology is the least compared to other networks.
- Bus topology costs very less.
- Linear Bus network is mostly used in small networks. Good for LAN

Drawbacks

- Lots of traffic down a single spine.
- Great danger of Traffic collision in the network



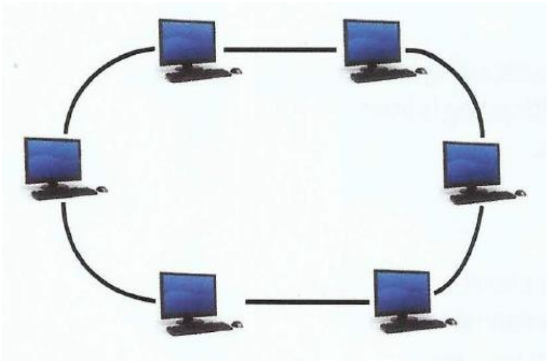
3- A ring Topology: In this configuration, each end-system has a point-to-point connection to the two adjacent end-systems.

Advantages of Ring Topology

- In ring topology all the traffic flows in only one direction at very high speed. Even when the load on the network increases, its performance is better than that of Bus topology.
- There is no need for network server to control the connectivity between workstations.
- Each computer has equal access to resources.

Disadvantages of Ring Topology

- Each packet of data must pass through all the computers between source and destination. This makes it slower than Star topology.
- If one workstation or port goes down, the entire network gets affected.
- Network is highly dependent on the wire which connects different components.



4- Mesh Topology: In this configuration, each end-system has a point-to-point connection to each of the other end systems.

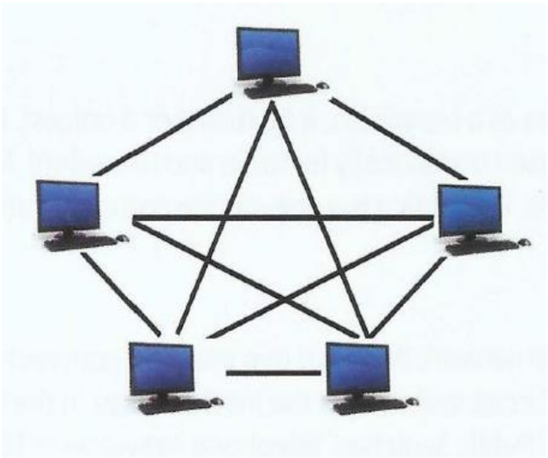
Advantages of Mesh topology

- Data can be transmitted from different devices simultaneously.
- Even if one of the components fails there is always an alternative present. So data transfer doesn't get affected.
- Expansion and modification in topology can be done without disrupting other nodes.

Disadvantages of Mesh topology

- There are high chances of redundancy in many of the network connections as a result a lot of traffic is generated.

- Overall cost of this network is way too high as compared to other network topologies.



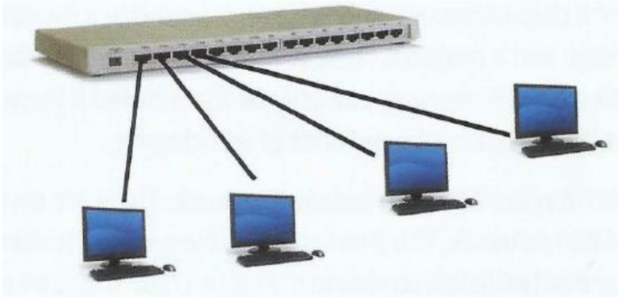
5- Star Topology: In a star topology, each end-system has a point-to-point connection to the 'central' device. So it can be said that every computer is indirectly connected to every other node by the help of “central device” which can be in the form of a hub, router or switch.

Advantages of Star Topology

- As compared to Bus topology it gives far much better performance, signals don’t necessarily get transmitted to all the workstations.
- Easy to connect new nodes or devices.
- Centralized management.
- Failure of one node or link doesn’t affect the rest of network.

Disadvantages of Star Topology

- Too much dependency on central device has its own drawbacks. If it fails whole network goes down.
- The use of hub, a router or a switch as central device increases the overall cost of the network.
- Performance and as well number of nodes which can be added in such topology is depended on capacity of central device.



Ethernet Protocol:

Ethernet is the other dominant protocol in the modern networked world. It is primarily focused on LANs.

The standard for a wired network is denoted as IEEE 802.3 which can be considered to be a synonym for Ethernet.

The standard has evolved through five generations: standard or traditional, fast, gigabit, 10 gigabit and 100 gigabit. The gigabit part of the name indicates the transfer speed capability. Ethernet transmits data in frames. Each frame contains a source address and a destination address. The address is the physical or MAC address, which uniquely defines one NIC. The reason that a unique address can be guaranteed is that 48 bits are used for the definition. The address is usually written in hexadecimal notation, for example: 4A:30:12:24:1A:10

CSMA/CD (carrier sense multiple access with collision detection)

If there were no control on the two end systems of a LAN, two messages sent by two devices at the same time would 'collide' and each message would be corrupted. This protocol defines a time that the end-systems have to wait before they try again. However, because two end-systems could have waited then both decided to transmit at the same time collisions could still happen. Thus, there was also a need to incorporate means for an end-system to detect a collision and to discontinue transmission if a collision occurred.

Public switched telephone network (PSTN)

During the early years of networking the telephone network carried analogue voice data. However, digital data could be transmitted provided that a modem was used to convert the digital data to analogue signals. Another modem was used to reverse the process at the receiving end. Such so-called ‘dial-up’ connections provided modest-speed, shared access when required.

More recently, the PSTNs have upgraded their main communication lines to fiber-optic cable employing digital technology. This has allowed them to offer improved leased line services to ISPs but has also given them the opportunity to provide their own ISP services. In this role they provide two types of service. The first is a broadband network connection for traditional network access. The second is WiFi hotspot technology, where an access point as described in Section 2.04 has a connection to a wired network providing Internet access.

Cell phone network:

For users of devices with mobile (cell) phone capability there is an alternative method for gaining Internet access. This is provided by mobile phone companies acting as ISPs. The mobile phone, equipped with the appropriate software, communicates with a standard cell tower to access the wireless telephone network, which in turn provides a connection to the Internet.

Cloud Storage: Online storage medium used to backup files. Files can be accessed from any device with an internet connection. Data is saved on more than one server so in case of maintenance or repair data is always accessible.

Public Cloud: The storage environment where client and storage provider are different companies.

Private Cloud: The storage environment where client and storage provider are single entity.

Advantages:

- Files can be accessed from any location using an internet connection.
- Users don't have to carry storage devices around with them.
- Offer backup solutions.
- Unlimited storage capacity.

Disadvantages:

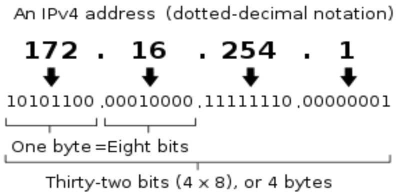
- Files could be hacked.
- Dependent on a good quality internet connection to download and upload files.
- Storage Company can charge the client.

IP Address - numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol.

Every device attached to a network has a number assigned to it. This unique number is called the IP Address, and you might be familiar with the format of:

nnn.nnn.nnn.nnn e.g. 192.168.7.1

Currently the most common form of IP Address $2^{32} = 4,294,967,296$ is IPv4 which uses 32 bits to store an address. This means that there are theoretically different IP Addresses that can exist. However, due to the allocation of IP ranges to different organisations and tasks, the number is lower.


An IPv4 address (dotted-decimal notation)
172 . 16 . 254 . 1
10101100 .00010000 .11111110 .00000001
One byte =Eight bits
Thirty-two bits (4 x 8), or 4 bytes

An IP address (version 4) in both dot-decimal notation and binary code.

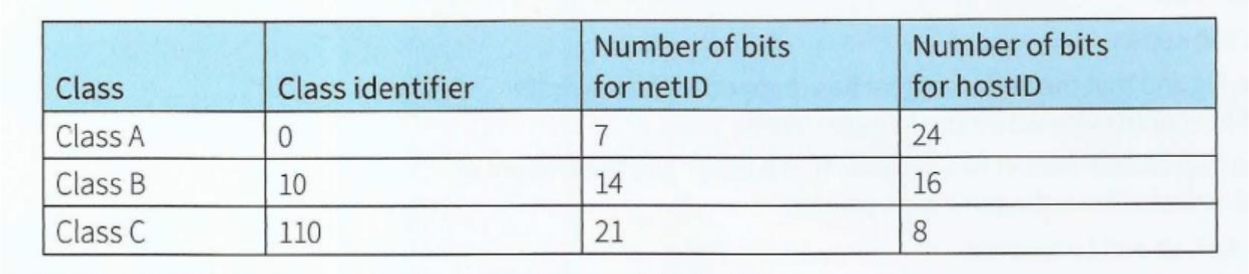
An IPv4 address is typically shown as split into 4 chunks as shown above. Different ranges of IP addresses are categorised differently, with the first part of the IP specifying who or where the IP address is (the **network identifier**), and the second part defining which host/machine it is (the **host identifier**).

$$\underbrace{192 \cdot 168}_{\text{network}} \cdot \underbrace{12 \cdot 162}_{\text{host}}$$

Different sets of IP ranges are allocated to particular networks, geographic areas, companies etc. The table below shows several examples of IP ranges and the uses that they have been put to:

IP range	Description	Example
192.168.___.___ 172.16.___.___ - 172.31.___.___ 10.___.___.___	Private networks, e.g. intranets	192.168.1.23
41.___.___.___ 102.___.___.___ 105.___.___.___	AfriNIC allocations for IP addresses in Africa	102.43.1.65
81.___.___.___ 217.___.___.___ 62.___.___.___	European allocations for IP addresses	81.202.17.89
200.___.___.___	Latin America and the Caribbean	200.100.50.25
9.___.___.___	IBM	9.1.2.3
17.___.___.___	Apple	17.19.23.29

Classful IPv4 Addresses.



Class	Class identifier	Number of bits for netID	Number of bits for hostID
Class A	0	7	24
Class B	10	14	16
Class C	110	21	8

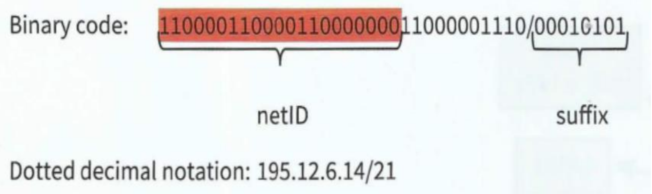
Table 2.02 Address structure for three classes of IPv4 address

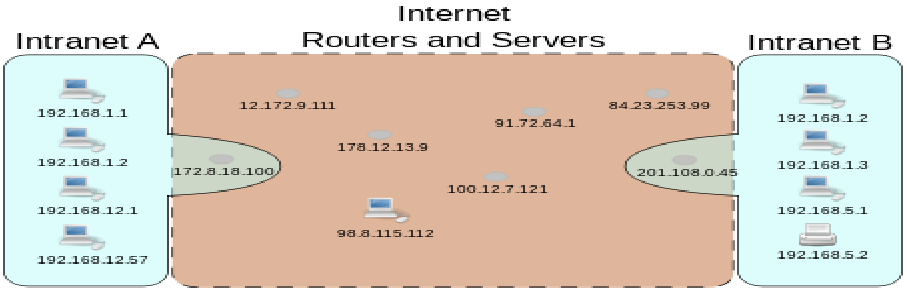
It can be seen from Table that the most significant bit or bits identify the class. A group of the next most significant bits define the netID and the remaining, least significant, bits define the hostID. The rationale was straightforward. The largest organizations would be allocated to Class A. There could only be 2^7 i.e. 128 of these but there could be 224 distinct hosts for each of them. This compared with 2^{21}, approximately two million, organizations that could be allocated to Class C but each of these could only support 2^8 i.e. 256 hosts.

Classless inter-domain routing (CIDR)

The problems with this scheme arose once LANs supporting PCs became commonplace. The number of Class B netIDs available was insufficient but if organisations were allocated to Class C the number of hostIDs available was too small. There have been a number of different modifications made available to solve this problem.

The first approach developed for improving the addressing scheme is called 'classless inter domain rout ing' (CIDR). This retains the concept of a netID and a hostID but removes the rigid structure and allows the split between the netID and the hostID to be varied to suit individual need. The simple method used to achieve this is to add an 8-bit suffix to the address that specifies the number of bits for the netID. If, for instance, we define the suffix as 21, that means that 21 bits are used for the netID and there are 11 bits remaining (of a 32-bit address) to specify hostIDs allowing 2^{11}, i.e. 2048, hosts. One example of an IP address using this scheme is shown in Figure below. The 21 bits representing the netID have been highlighted. The remaining 11 bits represent the hostID which would therefore have the binary value 11000001110.


Binary code: 11000011000011000000011000001110/00010101
netID
suffix
Dotted decimal notation: 195.12.6.14/21



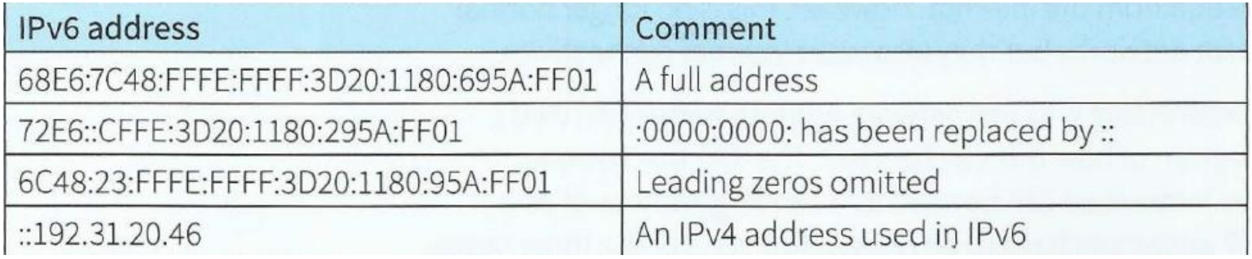
The diagram above shows how two intranets can connect across the internet. If the computer in Intranet A with the IP address 192.168.1.2 wants to send a message to a computer in Intranet B, it will send its message through the Router connected to Intranet A

(IP=172.8.18.100). This router will then route the message onto the internet, going from router to router until it reaches the router attached to Intranet B (IP=201.108.0.45). This router will then pass the message on to the correct machine in Intranet B. Notice that because each intranet is connected to the internet through a router, the computers on each intranet will appear as having the IP of their router when connected to the internet. If you share a house and someone commits a crime online, the finger might be pointed at the whole household! Using IP addresses this way was never the intention of the designers of TCP/IP, they would much prefer that each machine had a distinct IP address, however, with the shortage of IP addresses this isn't possible. What is needed is a system that has more addresses available.

IPv6

As you might have noticed, there is a limit to the number of IPv4 addresses we can have, this limit is well below the current population of the world. If we were in the future to have every inhabitant of the planet connected to the internet, there wouldn't be enough IP Addresses for them to use! This problem is very current and IPv6 is being introduced to try and resolve it. IPv6 uses 128 bits for each address, meaning we have theoretically 2^{128}addresses available = $340,282,366,920,938,463,463,374,607,431,768,211,456$ different possible addresses.

In IPv6, addresses are expressed as a series of eight 4-character hexadecimal numbers, which represent **16 bits** each (for a total of **128 bits**).



IPv6 address	Comment
68E6:7C48:FFFE:FFFF:3D20:1180:695A:FF01	A full address
72E6::CFFE:3D20:1180:295A:FF01	:0000:0000: has been replaced by ::
6C48:23:FFFE:FFFF:3D20:1180:95A:FF01	Leading zeros omitted
::192.31.20.46	An IPv4 address used in IPv6

What is public IP address? A public IP address is the address that is assigned to a computing device to allow direct access over the Internet. A web server, email server and any server device directly accessible from the Internet are candidate for a public IP address.

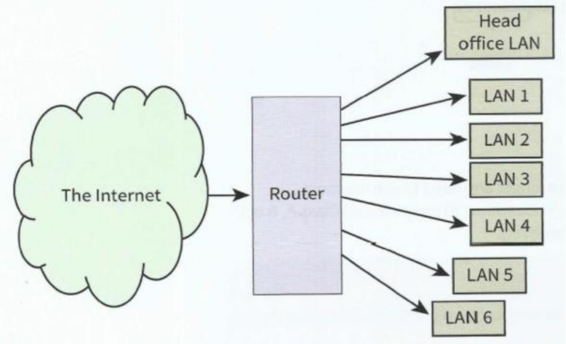
What is private IP address? A private IP address is the address space allocated to allow organizations to create their own private network. The computers, tablets and smartphones sitting behind your home, and the personal computers within an organization are usually assigned private IP addresses. A network printer residing in your home is assigned a private address so that only your family can print to your local printer. When a computer is assigned a private IP address, the local devices sees this computer via its private IP address. However, the devices residing outside of your local network cannot directly communicate via the private IP address, but uses your router's public IP address to communicate. To allow direct access to a local device which is assigned a private IP address, a Network Address Translator (NAT) should be used.

Static IP address: which never changes and can be provided if a user is prepared to pay an extra charge.

Dynamic IP address: the address is available for re-allocation once a user disconnects from the Internet.

"**Subnetting**" is breaking up a single network into smaller networks.

To illustrate an example of this we can consider a medium-sized organization with about 150 employees each with their own computer workstation. Let's assume that there are six individual department LANs and one head-office LAN. The sub-netting solution for this organisation would require allocating just one Class C netlD. For example, the IP addresses allocated might be 194.10.9.0 to 194.10.9.255 where the netlD comprises the first three bytes, represented by the decimal values 194, 10 and 9.

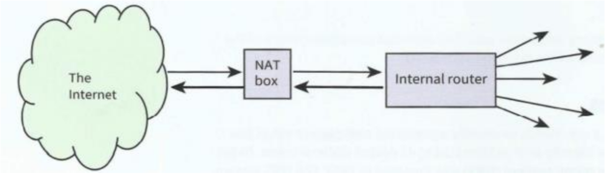


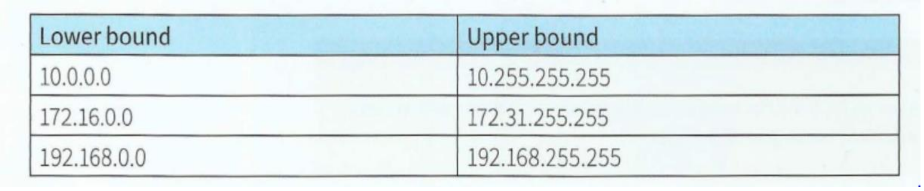
On the Internet, all of the allocated IP addresses have a netlD pointing to the router. The router then has to interpret the hostlD to direct the transmission to the appropriate host on one of the LANS. For example:

1. hostlD code 00001110 could be the address for workstation 14 on the head office LAN (LAN 000).
2. hostlD code 01110000 would be the address for workstation 16 on LAN 3 (LAN 011).

Network address translation (NAT)

Large organizations use INTRANET which use same protocol as those used for the internet. It provides isolation from the internet, however, large organizations also want internet connectivity. The solution for dealing with the addressing is to use network address translation (NAT). As shown in the diagram the NAT box has one IP address which is visible over the internet so can be used as a sending address or as a receiving address. Internally the IP addresses have to be chosen from one of the three ranges of IP addresses shown in the Table. (do not cram these IP addresses). The interface in the NAT box has software installed to examine each incoming or outgoing transmission. There can be a security check before an incoming transmission is directed to the correct internal address. The diagram shows undefined arrows from the router connected to the NAT box. These indicate that the network structure within the organisation could take many different forms.





Lower bound	Upper bound
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

Domain Name - humanly-memorable names for Internet participants such as computers, networks, and servers. One domain name can be connected to multiple IP addresses.

Trying to remember IP addresses is as difficult as trying to remember people's phone numbers. Not many people do it well and you are far more likely to be using a domain name to access a website. A domain name allows us to link to servers and other computers using easily remembered names. The domain name also tells us a bit about the location we are visiting through the use of top level domain names.

Top level domain	**Description**
.com	Commercial
.gov	US governmental organizations
.mil	US military
.org	Organisation
.uk	United Kingdom, country specific website
.pk	Pakistan, country specific website

Sometimes top level domain names might be joined by second level domains, chained together to tell you more detailed information:

bbc.com - there is a commercial organisation called bbc

bbc.co.uk - there is a United Kingdom commercial organisation called bbc.
tfl.gov.uk - there is a United Kingdom governmental organisation, called TFL.

Second level domain names typically tell you the person/company/organisation that owns the address. Finally you have the host or service name, which is the machine/service you are connecting to. For example:

en.wikipedia.org - an organisation, called Wikipedia, requesting the English language version
www.ibm.com - an commercial organisation, called IBM, connecting to the www (World Wide Web) host/service machine

$$\underbrace{windows}_{\text{host}}.\underbrace{microsoft}_{\text{domain name}}.\underbrace{com}_{\text{top level domain}}$$

Trying to remember IP addresses is as difficult as trying to remember people's phone numbers. Not many people do it well and you are far more likely to be using a domain name to access a website. A domain name allows us to link to servers and other computers using easily remembered names. The domain name also tells us a bit about the location we are visiting through the use of top level domain names.

Domain Name System server (DNS server) - translates domain names into IP addresses.

If you have a modern mobile phone it is very unlikely that you will type in the number of your friends each time you want to call or text them. You are far more likely to use the address book, typing in their name, then letting the phone find the number. This is exactly the same principle behind the Domain Name System. A DNS server translates domain names meaningful to humans (such as www.google.com) into IP Addresses for the purpose of locating and addressing these devices worldwide. Domain names are far easier for humans to remember than an IP address.

Internet Registrars - allow organizations and individuals to buy their own domain names.

Internet registrars are responsible for allocating internet domains to anyone who wants one. If someone wanted to own their own website with a domain name, they would have to go to an internet registrar in order to buy the website name. These services typically require payment in order to maintain control over the name of the website. If you do not renew your website, then the internet registrars may sell it to other buyers.

Internet Registries - hold domain names which are registered. They allow owners to link domain names to IP addresses. Well known domains usually have their own registry, such as .co, .com,. sch

You may ask why a company would want a domain to link to multiple IP addresses? If you think about a multinational company's website, if someone tries to load your homepage you don't necessarily want them to have to load this webpage from an server at an IP address on the other side of the world. So, depending on their region you would point them at an IP address close to their current location. Typing in www.google.com in Europe and in Asia will send you to different IP addresses even though you have used the same domain name. Sometimes the content of the server won't be the same depending on your region.

Also, big sites not only do geographic IP splitting but load balancing as well. This is when a domain name is undergoing heavy usage, and one particular IP address might be very busy, the domain name will then be pointed to other servers sitting at different IP addresses, balancing the 'load' of users accessing the site.

Internet Service Providers (ISP)- companies which offer customers access to the internet.

Getting a direct connection to the internet is quite costly involving specialist hardware. Most people and organisations pay ISPs to link them to the internet. Examples of Internet Service Providers are : AOL, BT, Sky, TalkTalk and Virgin Media.

Uniform Resource Identifier (URI) - A character string identifying a resource on the internet

Resources such as documents, files and folders sitting on the internet need a method to identify them and access them. URIs provide a way to linking to these resources. There are two types of URI, but you only need to know URL for the exam:

- **Uniform Resource Name (URN)** - the name of a resource, but not its exact location.

e.g. urn:isbn:0486419266
The URN for R.U.R. (1921 play), identified by its book number.

- **Uniform Resource Locator (URL)** - the exact location of a resource.

e.g. http://www.gutenberg.org/catalog/world/readfile?fk_files=85821
The project gutenberg page for the R.U.R. book

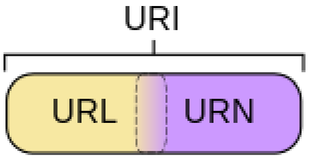


Diagram of URI scheme categories. A Uniform Resource Name (URN) functions like a person's name, while a Uniform Resource Locator (URL) resembles that person's street address. In other words: the URN defines an item's identity, while the URL provides a method for finding it.

Uniform Resource Locator - A character string referring to the location of an internet resource.

A URL is a URI that, "in addition to identifying a resource, provides a means of locating the resource by describing its primary access mechanism (e.g., its network location)". URLs allow us to specify the domain name and exact location of a resource on the internet. For example, the following links to a picture on wiki commons:

http://commons.wikimedia.org/wiki/File:George_Clausen_WWI_poster.jpg

We can break this down into its constituent parts:

$$\underbrace{http://}_{\text{protocol}}\underbrace{commons.wikimedia.org}_{\text{hostname}}\underbrace{/wiki/File:George\_Clausen\_WWI\_poster.jpg}_{\text{location on server}}$$

We can therefore summarise a URL as follows:

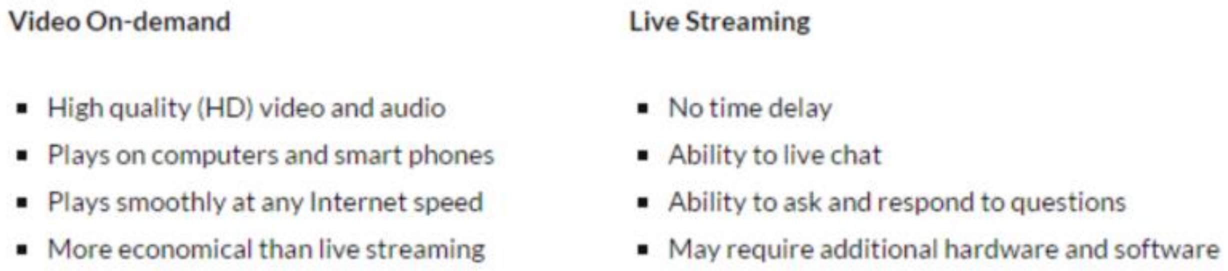
$$protocol://hostname/location\_of\_file$$

Bit Stream

A bit stream is a contiguous sequence of bits, representing a stream of data, transmitted continuously over a communications path, serially (one at a time).

Video on demand (VOD) is a system that may allow users to select and watch/listen to video or audio content when they choose to, rather than having to watch at a specific broadcast time (Live streaming). Some TV VOD systems such as Netflix or Hulu allow users to watch their favorite shows whenever they please.

Real time or Live streaming, as the name suggests, is streaming a video that is happening at that exact moment. Examples may be a football match, a concert, or a lecture happening at your university.



Video On-demand

- High quality (HD) video and audio
- Plays on computers and smart phones
- Plays smoothly at any Internet speed
- More economical than live streaming

Live Streaming

- No time delay
- Ability to live chat
- Ability to ask and respond to questions
- May require additional hardware and software

Bitrate

Bitrate is a term used to describe the amount of data that is being passed within a given amount of time. Depending on the context, common measurements of bitrate include Kbps and Mbps, respectively meaning kilobits per second and megabits per second.