

# Introduction to Computer Networks

# Introduction to Computer Networks

- Methods by which computers are linked together
- -Types of network defined by means of their geographical proximity
- **LAN** (local area network) - network which is confined to a building.
- **Ring** network which may have a diameter of approximately 5 miles.
- **WAN** (wide area network) - network connecting machines from different parts of the country to different parts of the world/ use telephone lines and satellite links.

# Why have a Network

- To meet the need of transferring data between computers, without the need to physically transport storage media
- Allows one to share resources, e.g. files, printers
- Allows for communication, e.g. Email
- Centralized control, useful for updates, backups etc..
- Remove the need for the purchase of very large single machines e.g. mainframe
- Cost effective, this is a result of the advantages listed above

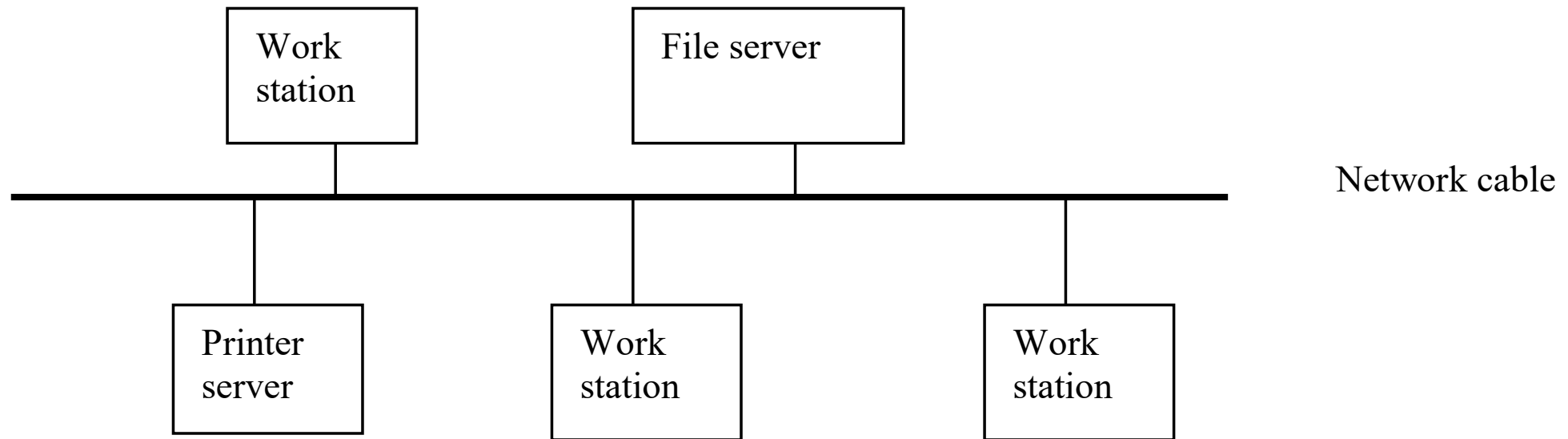
# Main Types of Architectures

- LAN Local area Network
- WAN Wide Area Network

# LAN Architecture

- Limited to local geographical area
- Hardware
  - i) transmission medium
  - ii) controlling mechanism or protocol
  - iii) interface
- The components
  - Workstation - where one works from e.g. a P.C, up to several hundred workstations
  - File server - can have one or more
  - Print server - can have one or more
  - network cabling – wire, allowing high transmission rates

# Typical Architecture of a bus network



# File Server

- Specially configured computer
- contains a network card
- has more memory and disk storage in comparison to a workstation
- has a very powerful processor in cmp. to a workstation
- controls exchange of files/data between users
- controls shared storage, directories and files
- support of several disks allowing storage capacity to be greater than that of just the file server.
- can have more than one file server on a LAN

# Printer Server

- Can be a Configured computer
- accepts and queues jobs from workstations
- may provide print management functions, sets priorities to jobs
- support the use of printers

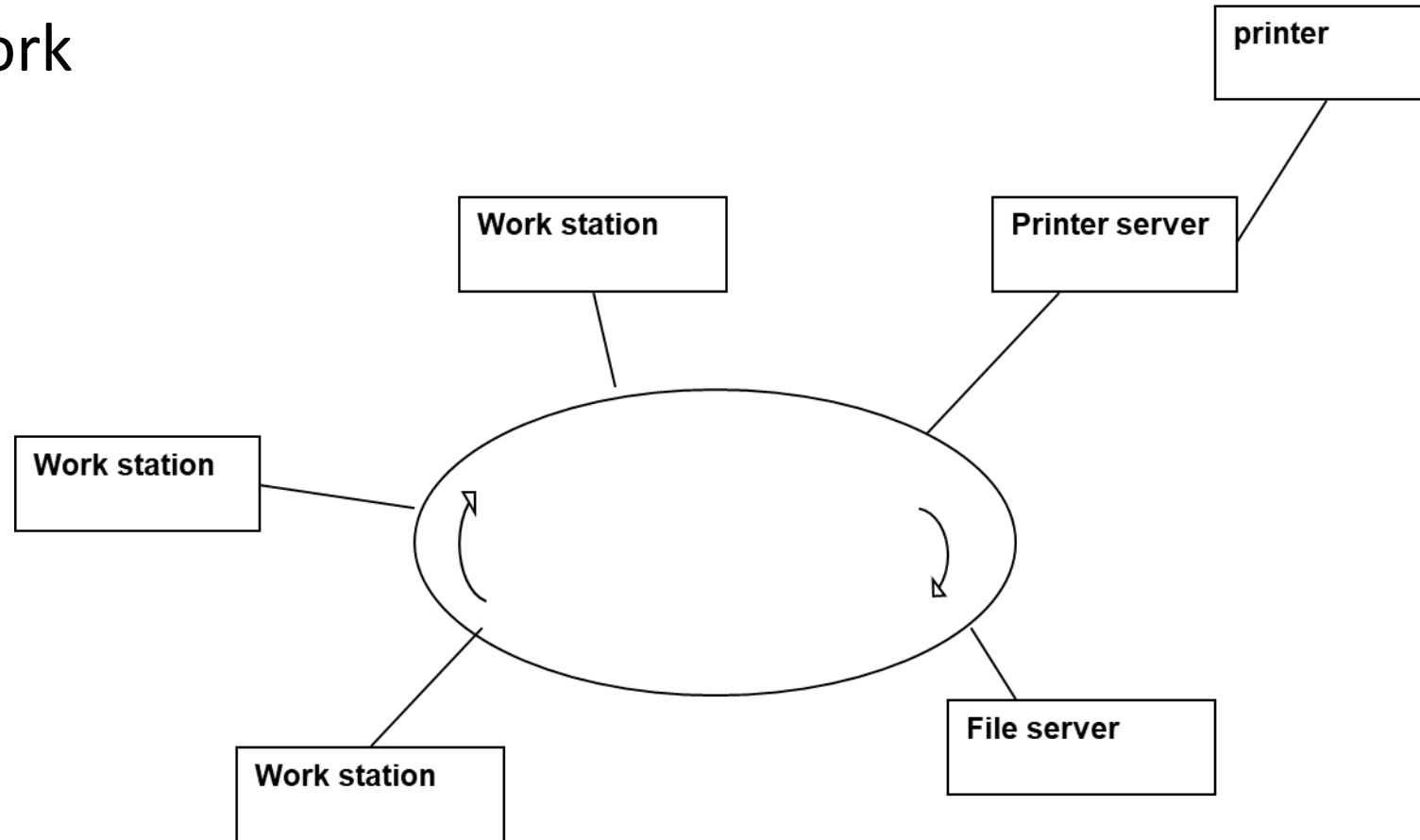


# key terms in Networking

- NODE – this is defined as the workstation within the LAN
- LINK – this is the circuit between two adjacent nodes
- PATH – this is the route which is taken by the messages from sender to receiver
- ROUTING – this is the process of determining the path for a given message, this is managed by the OSI Network layer
- SESSION – is a communication dialogue between two users on the network, and is managed by the OSI session layer

# Network Topologies

- Ring Network



# Ring Network

- mainly used for LAN and not for WAN's
- ring made up of a series of repeaters
- ring itself can be made of fiber optic cable
- all stations are connected onto the ring
- data is transmitted from node to node (most are unidirectional)
- frame goes round ring, the receiving station copies it
- frame goes back to sender to be removed

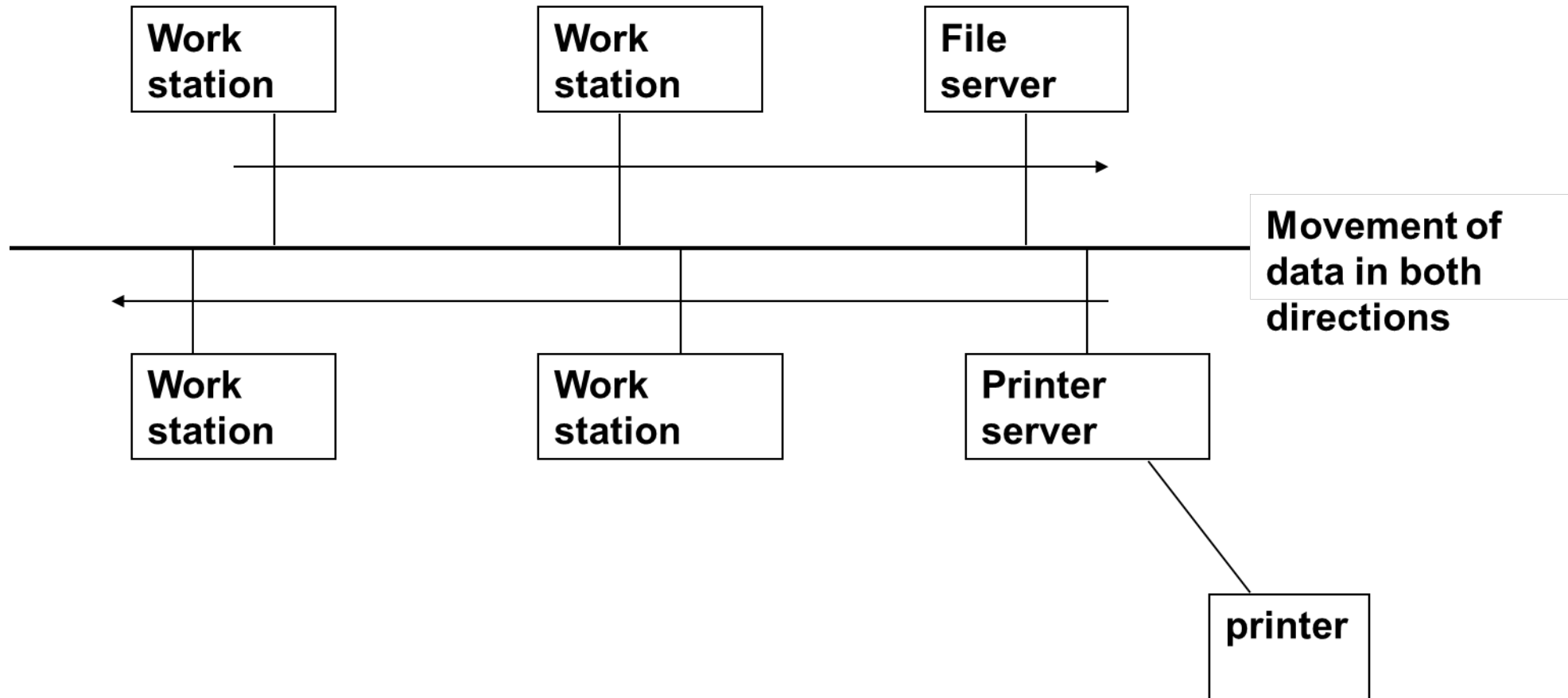
# Advantages of a Ring Topology

- No dependence on a host machine as the transmission of data is supported by all the devices.
- High transmission rates possible
- Data transmission between devices is relatively simple as messages can travel in only 1 direction
- Transmission facility is shared equally among the users

# Disadvantages of a Ring Topology

- System depends on the reliability of ring and repeaters
- Extensions are difficult; any physical installation must make sure that the ring topology is maintained.

# Bus Network



# Bus Network

- Workstations connected to main cable/ called the bus or trunk
- End of bus not connected
- Ends are terminated, the terminator absorbs any signal thus removing it from the bus
- Addition of new devices easy
- The bus standard is called Ethernet, now standardized as IEEE 802.3
- No host computer
- All workstations have equal access
- Broken into segments, largest of which is up to 500m and has up to 100 workstations attached
- segments are linked together

# Bus Network

- Data transmitted onto bus and received from bus
- Transmission from one station propagates in both directions and can be received by all workstations
- Simultaneous access may cause collisions, requires Medium Access Control (MAC)



# Advantages and Disadvantages of Bus Network

- Advantages

- If a node breaks down the rest of the system keeps working
- Adding new workstations is easy.

- Disadvantages

- - If a fault occurs on the Ethernet cabling then the whole system
- goes down.

# Components of a network

## Cabling

- 3 main types:
- Twisted pair
  - Cable cheaper than thick Ethernet cabling
  - Transmission rate up to 1 (CAT6 10m) -10 Gbps (CAT6 55m)
  - Bandwidth 100Mhz
  - Easy to install
- Fibre
  - Transmission rate up to 200 Gbps
  - Secure, cannot physically tap in
  - Very good for long distances
  - Better reliability – no electrical interference, no heat losses
- Coaxial
  - Transmission rate max of 100Mbps
  - support greater cable lengths compared to Twisted pair
  - High bandwidth upto 3GHz
  - Used to provide power

# Network Components

## **Repeater**

- Used to continue or extend a length of the Ethernet
- - It reconstructs and amplifies signals received by removing the noise and any distortion
- - Retransmits the signal onto the next segment.

## **Transceiver**

- Used to receive signal and then transform signal to conform with the thin Ethernet cable (change rate)

## **Bridge**

- - Used to connect two LANs of the same type e.g. two token ring
- or two Ethernet LANs, called Local Inter Networking
- - They can divide large networks into smaller segments
- - Can configure bridge to restrict data, and only allow data which needs to enter a network.

# Network Components

## **Hub**

- used to connect computers in a LAN
- Has many ports
- When data is set to port it broadcasts it to ALL other ports
- Not normally programable
- Transmission mode half duplex (1 way at a given time)

## **Switch**

- used to connect computers in a LAN
- Has many ports
- Incoming data packets it uses the destination address and sends it to that device
- Can also multicast, broadcast
- Transmission mode full duplex (2 way) at same time

# Network Components

## **Router**

- Connects different networks together
- Transfers data in the form of IP packets using IP address
- Uses a Routing table and protocol to forward data packets
  - Static Routing Table – table does not get refreshed
  - Dynamic Routing Table – Using Routing Protocols, communicates with other routers to determine path of data packets
- Wifi Router use a WIFI connection but limited to distance
- Broadband Router connect internet through telephone use VoIP protocol, giving high speed access

# Sending Messages through a bus network

## **Carrier sense multiple access(CSMA)**

- Each device is free to transmit data at any time.
- Devices network card test the network patch to make sure that the destination device is free to receive data.

# Sending Messages through a bus network

## **Carrier sense multiple access(CSMA)**

- Two conditions must be satisfied if transmission is to take place:

### **(1) Collision Detection**

- Possibility of colliding with another transmission
- Detection mechanism is used
- If collision occurs transmission is held and it tries again a few milliseconds later.

### **(2) Collision Avoidance**

- The network card checks the path twice
- Once to see if the path is free then it alerts the device that it may use the network
- Then the path is tested a second time before transmission.

# Open Systems Interconnection (OSI) model.

- Open systems give users of data networks the freedom to choose equipment, software and systems from any vendor/supplier.
- Decomposes one problem into seven more manageable sub problems
- Each layer
  - performs a subset of functions required for communication
  - provides services for the next highest layer
  - sends data down to the next lower layer for more primitive functions
- The reason why we break down the network architectures down into a number of layers is that each smaller unit can be better understood and also designed better.
- In a network design we can implement a number of layers which can talk to adjacent layers. Each layer can be separately tested and we can have different versions or standards in each



# Open Systems Interconnection (OSI) model.

The OSI architecture defines the communication process as a set of 7 layers, these are :

Layer No.	Name	Function
LAYER 7	APPLICATION LAYER	FILE TRANSFER, ACCESS AND MANAGMENT DOCUMENT AND MESSAGE INTERCHANGE
LAYER 6	PRESENTATION LAYER	DATA REPRESENTAION, TRANSFORMATION AND SECURITY
LAYER 5	SESSION LAYER	DIALOGUE AND SYNCHRONISATION CONTROL
LAYER 4	TRANSPORT LAYER	END-TO-END TRANSFER MANAGMENT (Connections, error or flow control segmentation)
LAYER 3	NETWORK LAYER	NETWORK ROUTING AND ADDRESSING
LAYER 2	DATA LINK LAYER	FRAMING, DATA TRANSPARENCY, ERROR CONTROL
LAYER 1	PHYSICAL LAYER	MECHANICAL AND ELECTRICAL NETWORK INTERFACE DEFINITIONS

# Layer 1 Physical Layer

- The lowest level the physical layer is a set of rules that specifies the electrical and physical connections between devices.
  - This level specifies the cable connection and the electrical rules necessary to transfer data between devices.
  - Typically the physical link corresponds to establish interface standards such as the port connectors.
  - The result is a stream of bits which are signalled from one point to another with all the electrical and mechanical properties of the connections being specified.
- 
- Transmission medium including
    - type of media
    - how data is represented
    - speed of transmission
    - electrical connections

# Layer 2 The data link layer

- This level denotes how a device gains access to the medium specified in the physical layer.
- It also defines data formats, to include the framing of data within transmitted messages, error control procedures and other link control activities such that the bits carried by the physical layer have a structure.
- So this layer becomes responsible for reliable delivery of information, thus it carries out any error checks.

# Layer 2 The data link layer

## **Link Management**

- concerned with the initialisation (or link set up) phase and, after the data transfer has taken place, the disconnection phase.

## **Flow Control**

- for assuring that a transmitting entity does not overwhelm a receiving device with data.
- The receiver typically allocates a data buffer of some maximum length for transfers. When data are received, the receiver needs some time for processing, before passing the data to the higher level. Flow control should ensure that enough buffer space is provided.
- Two common flow control mechanisms are:
  - Stop and Wait
  - Sliding Window

# Layer 2 The data link layer

- **Error Control.**
- detect and correct errors that occur in the transmission of frames
- There is the possibility of two types of errors:
  - Lost frames: A frame fails to arrive
  - Damaged frames: Bits of a frame are in error

# Layer 3 The Network layer

- This layer is responsible for arranging a logical connection between a source and a destination on the network to include the selection and management of a route for the flow of information between source and destination based on the available paths in a network.
- The services provided for the movement of data through a network include:-

addressing, routing, switching, sequencing, flow control

- In a complex network the source and destination may not be directly connected by a single path, but instead may require a path to be established that consists of many sub paths, thus routing data through the network onto the correct path,

# Layer 5 The Session layer

- Establishes logical connection between ends.
- Controls the flow of information between ends (dialogue management).
- Recovery: synchronisation points marked to prevent loss of data in case of failure

# Layer 6 The Presentation layer

- This layer is concerned with
- Data encryption/decryption and data compression/decompression are other examples of the functions which are provided by this layer.
- Data is prepared and formatted for transmission
- May involve
  - code conversion (e.g. ASCII to EBCDIC)
  - encryption
  - compression/decompression
  - terminal screen formatting (e.g. Clear Screen, Move Cursor to Home, etc.)



# Layer 7 The application layer

- This layer affects the information interchange between two application processes by providing a range of service interfaces for application programs.
- E-mail, file transfer services are typical examples of the interfaces provided at layer 7.
- Interface to the user
- May include network management, diagnostics and statistics gathering,

# TCP/IP Transmission Control Protocol/Internet Protocol.

## TCP/IP Compared to the OSI model

Application	FTP	Telnet	SMTP	DNS	SNMP	OTHER
presentation						
Session						
Transport	TCP			UDP		
Network	IP					
Data link	802 Networks	X.25		Frame Relay	other Applications	
Physical	physical layer					

# FTP File Transfer Protocol

- This supports the transfer of data between hosts.
- It provides the initiation for the bi-directional file transfer, and also it provides a way of looking at file directories, and also provides a method for renaming and deleting files.
- To carry out an FTP session this requires the initiation of 2 connections between hosts
- 1st connection to convey commands and status information
- 2nd connection is for the actual file transfers.

# TELNET and SSH

- Telnet is a protocol
- This represents an interactive remote access terminal protocol, which allows users to log on to a remote computer as if their terminal was directly connected to the remote computer.
- One has to define the host(remote) computer, the port number( normally already set by default), and to define the type of terminal to be emulated.
- SSH is a program similar to telnet for remote terminal access
- More secure than telnet

# Domain Name Service

- The actual addressing on a TCP/IP network occurs through the use of 4 decimal numbers(octets - 8 bits), which range from 0 to 255, each octet is separated by a dot, which collectively represents the 32 bit address
- e.g. 127.248.119.149
- As these numerical addresses are difficult to deal with; TCP/IP also supports a naming conversion.

# The INTERNET PROTOCOL IP

- This is a network layer protocol which supports a datagram gateway service between subnetworks, this allows one to communicate from one network to another.
- To accomplish this the Internet Protocol will fragment large datagrams into data packets just small enough to be transmitted through the network, and then perform the reassembly of the datagrams
- At layer 4 the TCP/IP protocol suite supports two transport protocols, these are the Transport Control Protocol (TCP) and the User Datagram Protocol (UDP).

# TCP Transport Control Protocol

- It provides error detection and correction as well as flow control to regulate the flow of datagrams
- is a connection-oriented reliable protocol which requires a session( a connection via a data terminal such that the transmission path is held open) to be established before the transfer of data is allowed.
- FTP, Telnet and other applications that require the establishment of a session must use TCP.

# UDP User Datagram Protocol

- provides an unreliable connectionless transport service, and so requires higher applications to ensure the message is delivered correctly
- a session does not have to be established for network management information to be transmitted
- provides a degree of flexibility for the transmission of network management information



# IP addressing

- The IP v4 address is 32 bits in length – 4 BYTES
- Represented 4 Decimal numbers separated by a dot
- IP addressing can be broken down into unique network classes

class	Network ID part	Host ID Part	from	To
A	1 <sup>st</sup> byte	3 bytes	0.0.0.0	127.255.255.255
B	1 <sup>st</sup> 2 bytes	2 bytes	128.0.0.0	191.255.255.255
C	1 <sup>st</sup> 3 bytes	1 byte	192.0.0.0	223.255.255.255

IPv6 uses 128 bits as running out of addresses offers  $3 \times 10^{38}$  address

# IP address

- 2 types Private and Public
- Private IP addresses used in a local next work
- Private IP addresses cannot connect to internet directly or be connected to directly from outside the LAN
- Private IP assigned by Network admin
- Private IP are unique within the LAN
- Public IP unique; accessible to and from the internet
- Public IP provided assigned by service provider

# IP address

- A router will have a Public IP
- Each device in your LAN will have a private IP
- The router will use a network address translation (NAT) that maps the private IP addresses to public.
- There are assigned **private IP addresses** that can be freely used:

class	Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

# IP address

Subnet mask

This is used to extract the network ID

It is sometimes given with the IP address e.g.

192.168.3.2/24

192.168.3.0 is the IP address and from its range it's a Class C Private IP address

the **/24** represents the number of MSBs set to 1 out of the 32 bits to be logically AND'ED with the IP address

# IP address

192.168.3.2/24

If we write the MSB 24 bits in decimal we get 255.255.255.0

Then if we carry out a bitwise AND between the IP address and the mask we get

192.168.3.0 – and this is the network ID

The host's mask will be the 0.0.0.255 and if we carry out a logical AND with the IP address and this gives 0.0.0.2

Where the 2 is the host

# SUBNETTING for class C

- Dividing a network into 2 or more networks
- Based on the class you can use within any private ip address
- E.g. 192.168.6.0/24
- Now we can use this and lets assume this was for a company and we wanted 5 different subnets for 5 departments in the LAN and we wished to list the network ID for each along with its subnet mask, the host range, the number of hosts available and the broadcast IP

# SUBNETTING for class C

- Create a table with 3 rows
- Label the rows as follows

Subnet
Host
Subnet mask

# SUBNETTING for class C

- Create 9 further columns for each row
- Populate the rows as follows:
- Subnet row start from 1 and double each time
- Host row start from 256 and halve each time
- For subnet mask start from the one given say for a class C we will have /24 and increment by 1 each time

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet mask	/24	/25	/26	/27	/28	/29	/30	/31	/32



# SUBNETTING for class C

- We have 192.168.6.0/**24** and we wish 5 separate subnets
- Use the table to find the subnet that is just greater or equal to what is required in our case 4 is too small so we need to use 8
- Highlight the column

Subnet	1	2	4	<b>8</b>	16	32	64	128	256
Host	256	128	64	<b>32</b>	16	8	4	2	1
Subnet mask	<b>/24</b>	/25	/26	<b>/27</b>	/28	/29	/30	/31	/32

# SUBNETTING for class C

- We have **192.168.6.0/24** and we wish 5 separate subnets

Subnet	8
Host	<b>32</b>
Subnet mask	/27

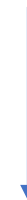
We have the subnet mask for ALL the network ID s i.e. **/27** : 255.255.255.224.

To evaluate each network we start with the private IP given i.e. 192.168.6.0 and for each subnet we add number of hosts from the table in our case **32 and we repeat for each subnet**

We start with  
address given for  
the 1<sup>st</sup> subnet



Network ID
<b>192.168.6.0</b>
192.168.6. <b>32</b>
192.168.6. <b>64</b>
192.168.6. <b>96</b>
192.168.6. <b>128</b>



We increment  
each time by  
adding 32;

# SUBNETTING for class C

- We have **192.168.6.0/24** and we wish 5 separate subnets

Subnet	8
Host	<b>32</b>
Subnet mask	/27

The number of hosts that we can have for each subnet is the host number – 2

The 1<sup>st</sup> and last IP in each host are reserved so should not be as host ids of all zeros or all ones are not allowed

The last address in the range is used for broadcasting

So the number of usable addresses in our example is 30 for each subnet

# SUBNETTING for class C

- We have **192.168.6.0/24** and we wish 5 separate subnets

Subnet	8
Host	<b>32</b>
Subnet mask	/27

To work out the range of addresses for each

Network ID	Starting address + 1 to the host part of address	Last address + (Host-3) from column values to left $32 - 3 = 29$
<b>192.168.6.0</b>	<b>192.168.6.1</b>	<b>192.168.6.30</b>
192.168.6. <b>32</b>	192.168.6. <b>33</b>	192.168.6. <b>62</b>
192.168.6. <b>64</b>	192.168.6. <b>65</b>	192.168.6. <b>94</b>
192.168.6. <b>96</b>	192.168.6. <b>97</b>	192.168.6. <b>126</b>
192.168.6. <b>128</b>	192.168.6. <b>129</b>	192.168.6. <b>158</b>

# ERROR DETECTION AND CORRECTION

- In asynchronous transmission the most common form of error control is the use of a single bit known as the parity bit, for the detection of errors.
- There are two modes that is even and odd parity checking, where the sum of the bits are checked e.g.
  - 1010010 0            odd parity   where the sum of the bits is an odd no.
  - 1010010 1            even parity   where the sum of the bits is an even no.
- The only problem is that if more than two bits change during the transmission then the error would go undetected.

# ERROR DETECTION AND CORRECTION

- The modes of error checking used in **synchronous transmission** mainly involve geometric codes.
- Geometric codes try to reduce the deficiency of the parity check by extending it into two dimensions, this involves the forming a parity bit on each individual character as well as on all the characters on the block
- e.g.
- parity bit(odd parity)
- 1011011 0
- 0100101 0
- 0111000 0
- 1000001 1
- 0101010 0
- 1110001 1
- 0100011 1                      Longitudinal Redundancy Check character (odd parity)
- The transmission system using a geometric code for error detection has a slightly better capability to detect errors than that of the sum check.

# CYCLIC CODES

- When a cyclic or polynomial code error detection scheme is employed the message block is treated as a data polynomial  $D(x)$ , which is divided by a predefined generating polynomial  $G(x)$ , resulting in a quotient polynomial  $Q(x)$  and a remainder polynomial  $R(x)$  such that
- $$D(x)/G(x) = Q(x) + R(x)$$
- The remainder of the division process is known as the cyclic redundancy check (CRC) and is normally 16 bits in length, the CRC is appended to the block of data to be transmitted.
- The receiving device then compares the its own generated CRC with that of the transmitted CRC, the receiver then transmits a positive acknowledgement communications control character which informs the transmitting device that the data was received correctly and also informs the device that if additional blocks of data remain to be transmitted the next block can be sent.
- A typical CRC 16 bit polynomial has the form  $X^{16} + X^{15} + X^5 + 1$

# HAMMING CODE

- Here one not only detects the occurrence of an error but also identify its location, and so some errors can be rectified.
- The hammering code uses  $m$  parity bits with a message length of  $n$  bits, where  $n = 2^m - 1$ .
- This permits  $k$  information bits where  $k = n - m$ .
- The parity bits are inserted into the message at bit positions  $2^{j-1}$  where
- $j = 1, 2, \dots, m$ . e.g. if one uses 3 code bits( $m$ ) and 4 data bits( $k$ ), making 7 bits in total ( $n$ ),




# HAMMING CODE

- Message length = 7 bits
- data bits = 4 bits  $\Rightarrow$  1100
- parity = 3 bits  $\Rightarrow P_1, P_2, P_3$
- parity placed in  $P_1$ ,  $j = 1$  pos  $2^{1-1} = 1$
- $P_2$ ,  $j = 1$  pos  $2^{2-1} = 2$
- $P_3$ ,  $j = 1$  pos  $2^{3-1} = 4$
- So we have message : 110  $P_3$  0  $P_2$   $P_1$
- The data and the parity bits are exclusive Ored with all possible data values to determine the value of each parity bit

# HAMMING CODE

- Now considering our example, we 1st

Data position bits		Hamming parity bits			Hamming bit P3 place value of 4
		4	2	1	
7		1	1	1	Sum bits 7, 6,5 and P3 and if we choose odd or even parity then we select the value for P3 to make it so
6		1	1	0	
5		1	0	1	
3		0	1	1	We repeat for P2 and P1
					
		Defines which bits are to be summed with parity bit			

# HAMMING CODE

1	1	0	$P_3$	0	$P_2$	$P_1$
---	---	---	-------	---	-------	-------

If we choose even parity

1      1      0       $P_3$       =      Even      So  $P_3$  has is set to 0

1      1                0       $P_2$       = Even      So  $P_2$  is set to 0

1           0           0            $P_1$       = Even so  $P_1$  set to 1

Transmitted message	1	1	0	0	0	0	1
---------------------	---	---	---	---	---	---	---

# HAMMING CODE

If one of the bits changes in error  
say bit 6 from 1 to 0

1	0	0	0	0	0	1
---	---	---	---	---	---	---

To find the error we repeat the process

1	0	0	$P_3/0$	Test if	Even	= False	set 1
1	0				0	$P_2/0$	Test if Even = False set 1
1		0			0	$P_1/1$	Test if Even = True set 0

Read  
binary  
number  
MSB

LSB

110 (i.e. bit 6 is in error)