ALevel CS C17 Communication and Internet (1)

Transmissions models(Circuit switching)

Circuit switching: the method used in the **traditional telephone system**
Public Switch Telephone Networks(PTSNs)**:** largely converted to digital technology. the same method can be provided for data transfer that was traditionally used for voice communication
Circuit switching step:
1. The sender provides the identity of the intended receiver.
2. The system checks whether or not the receiver is ready to accept data.
3. If the receiver is available, a sequence of links is established across the network.
4. The data is transferred.
5. The links are removed.

Circuit switching benefits:
1. **no delay**: delay is minimized and no switching
2. **all bandwidth**: provide with consistent bandwidth, channels, and an ongoing data rate
3. **data in order**: data packets are delivered in their correct order
4. **not sharing channel**

Circuit switching drawback:
1. Dedicating one channel to a single service leaves it unavailable to other services.
2. It is expensive to provision an entire channel to one service and one individual routing path.

Usage: telephone, video conference, live streaming.

Comparison between circuit and packet switching	
Circuit switching	packet switching
Dedicated path	No dedicated path
Path is established for entire conversation	Route is established for each packet
Call setup delay	Packet transmission delay
Overload may block call setup	Overload increases packet delay
Fixed bandwidth	Dynamic bandwidth
No overhead bits after call setup	Overhead bits in each packet

Protocols

Protocol: a set of rules for data transmission which are agreed by sender and receiver
Protocol suite:
1. Each layer can only accept input from the next higher layer or the next lower layer.
2. There is a defined interface between adjacent layers which constitutes the only interaction allowed between layers.
3. A layer is serviced by the actions of lower layers.
4. With the possible exception of the lowest layer the functioning of a layer is created by installed soft ware.
5. A layer may comprise sub-layers.
6. Any user interaction will take place using protocols associated with the highest level layer in the stack.
7.Any direct access to hardware is confined to the lowest layer in the stack.

Why necessary:
1. All data is using the **same rules**
2. All data is using the **same formats**
3. allow communication between devices operating on **different platforms**
4. The communication is independent of the software used
5. The communication is independent of the hardware used

Transmissions models (Packet switching)

Packet Switching:
1. Allows data transmission without a circuit being establish.
2. Data can be sent is divided into packets.
3. Data can travel along different routes.
4. Packets are reassembled in the correct order at the receiver's end
5. Wait until last packet is received, then put the data back together

A packet consists of a **header** which contains instructions for delivery plus the **data body**.

there are two ways that the network can provide a service: **connectionless service** or **connection-oriented service**.
Connectionless service: a packet is dispatched with no knowledge of whether or not the receiver is ready to accept the packet, and has no way of finding out if the transmission has succeeded.
Connection-oriented service: the first packet sent includes a request for an acknowledgement.If the acknowledgement is received, the sender transmits further packets. If no acknowledgement is received, the sender tries again with the first packet. Packet switching are mainly used for data and voice applications requiring non-real time scenarios

Packet switching benefits:
1. **Accuracy**: Ensures accurate delivery of the message
2. **Completeness**: Missing packets can be easily detected and a re-send request sent so the message arrives complete
3. **Resilience**: if a network changes the router can detect this and send the data another way to ensure it arrives
4. **Path also available to other users** // Doesn't use whole bandwidth // allows simultaneous use of channel by multiple users

Packet switching drawback:
1. Time delays to correct errors // Network problems may introduce errors in packets
2. Requires complex protocols for delivery
3. Unsuitable for real time transmission applications

Why packet switching is used in internet?
1. Packet switching makes best use of the available (channel) capacity
2. by using alternative routes
3. which is more secure / robust
4. as packets to / from different sources and destinations can share the same route

Packet switching feature:
1. In packet switching, **station breaks long message into packets**. Packets are sent one at a time to the network. Packets are handled in two ways, viz. datagram and virtual circuit.
2. **In datagram**, each packet is treated independently. **Packets can take up any practical route**. Packets may arrive **out of order** and **may go missing**.
3. **In virtual circuit**, preplanned route is established before any packets are transmitted. The **handshake** is established using call request and call accept messages.In this type, **routing decisions for each packet are not needed**.
4. For a packet-switched network, data is transferred by dividing the data into individual packets and passing it through the circuits to the other host. In packet -switched networks, the route is not exclusively determined when the packets hit the wire. Using routing algorithms, **each packet may actually take a different route** through the network to arrive at the destination host.

TCP/IP protocol suite

TCP/IP protocol suite: TCP/IP is the protocol suite underpinning the Internet usage.
1. **Application layer**: handless access to service, manage data exchange, defines protocol used
HTTP,SMPT,DNS,FTP,POP3,IMAP
2. **Transport layer**: handles the forwarding of packets
TCP,UDP,SCTP
3. **Network(internet) layer**: handles transmission data, routing, IP address.
IP,IGMP,ICMP,ARP
4. **Link layer(physical layer)**: handles how data is physically send

ALevel CS C17 Communication and Internet (2)

TCP: The TCP protocol operating in the transport layer now has to take responsibility for ensuring the safe delivery of the 'message' to the receiver. Each packet consists of a header plus the user data.

1. **ensure safe delivery**
2. **ensure that any response is directed back** to the application protocol.
3. **connection-oriented**

Tcp function:

1. allows applications to exchange data
2. establishes and maintains a connection
3. until exchange of data is complete
4. determines how to break application data into packets
5. adds sequence / packet number to (TCP) header
6. sends packets to and accepts packets from the network / Internet layer
7. manages flow control // manages congestion avoidance
8. acknowledges all packets that arrive
9. detects when a packet has not arrived at destination
10. handles retransmission of dropped packets
11. reassembles packets into the correct order

TCP/IP data packet have following information:

1. **source** - which computer the message came from
2. **destination** - where the message should go packet
3. **sequence** - the order the message data should be re-assembled
4. **data** - the data of the message
5. **error check** - the check to see that the message has been sent correctly

Route:

1. the frame sent by the data-link layer will arrive at a router during transmission (more likely at several routers).
2. the function of the router software to choose the next target host in the transmission.
3. The routing table for every router has details of any current problems with any of the options for the next transmission step.

The major **distinction** between a switch and a router as a node in a network is that when a frame arrives at a switch, it is transmitted on without any routing decision. A switch operates in the data-link layer but has no access to the network layer.

routing table: network id, routing metric, next hop, interface

IP(Internet Protocol): to ensure correct routing over the Internet. IP protocol takes the packet received from the transport layer and adds a further header. The header contains the IP addresses of both the sender and the receiver.

IP data packet content: IP version number, internet header, total length, protocol, source ip, destination ip address, checksum

IP functions:

1. routes the packets around the network
2. adds to the IP header a source/destination address for each packet
3. encapsulates data into datagram
4. passes datagram to the network access layer (for transmission on the LAN)// passes datagram to the transport layer (on arrival at destination)
5. Defines the addressing method e.g. subnetting, NAT

datagram: The IP packet, which is usually called a 'datagram', is sent to the data-link layer and therefore to a different protocol suite.

IP functions as a **connectionless service**

HTTP(HyperText Transfer Protocol): transfer web pages from servers to the client.

1. transaction-oriented, client-server protocol.
2. define the format of message
3. HTTPS is Hyper Text Transfer Protocol Secure when data is encrypted and send with security.

FTP(File Transfer Protocol): the application-layer protocol that can handle any file transfer between two end-system.

Email protocol

SMTP(simple Mail Transfer Protocol): push protocol, sending a mail

1. largely replaced by the use of web-based mail

POP3(Post Office Protocol version3): pull protocol

1. for emails to be downloaded onto the client computer
2. more secure to cyber-attack because emails are locally stored
3. only accessible from one client system.

IMAP(Internet Message Access Protocol):

1. not download the email to client computer
2. the server can be accessed from any client

P2P (Peer-to-peer) file sharing: no structure and no controlling mechanism. Peers act as both clients and servers and each peer is just one end-system. When a peer acts as a server it is called a 'seed'.

how the bitTorrent protocol allows file to be share:

1. BitTorrent client software made available
2. One computer must keep a complete copy of the torrent/file to be shared
3. Torrent/file is split into small pieces
4. A computer joins (a swarm) by using the BitTorrent software to load a torrent descriptor file
5. The computer can now download a piece of the file
6. Once a computer has a piece it can become a seed and upload (to other members of the swarm)
7. Pieces of the torrent are both downloaded and uploaded (by each member of the of the swarm)
8. A server called a tracker keeps records of all the computers in the swarm
9. The tracker shares their IP addresses allowing them to connect to each other