FINAL EXAM -COMPUTER NETWORKS
Chongqing University of Technology, Fall 2020

NAME: **Md Anower Hossain(安昊铭)**

STUDENT NUMBER: 62017010084
INSTRUCTIONS

This is an open book and notes online exam. You have two days to complete the questions. ***Please write neatly and clearly.*** **To receive credits or partial points, you must show all work and steps for your answers.**

Question	**Grade**
1	____/10
2	____/10
3	____/20
4	____/15
5	____/15
6	____/15
7	____/15
Total	____/100

Score: ____________/ 100

1. [10 Points, each 2 points] True or False (T/F) Questions

(1) If the source's retransmission timeout value RTO is too small, this might lead to unnecessary retransmissions. Answer: T

(2) TCP is a transport protocol for best effort service and cannot guarantees in order delivery of packets. Answer: F

(3) Email SMTP protocol is a transport layer protocol Answer: F

(4) Media Access Control is a function and sublayer of the data-link layer. Answer: T

(5) Forward error correction (FEC) can be more efficient than automatic retransmission request (ARQ) in a wireless broadcast environment with many receivers. Answer: T

2. [10 Points, each 2 points] Single Choice Questions

(1) SIP Session Initialization Protocol is at which layer in the 7-layer OSI model

A. 7th layer B. 3rd layer C. 4th layer D. 5th layer

Answer: D. 5th layer

(2) Which of the following is correct for UDP protocol?

A. Connection oriented and best effort B. Connectionless and reliable C. Connectionless, and best effort D. Connection oriented and reliable

Answer: C. Connectionless and best effort

(3) For TCP protocol, Socket's data format can be represented by which of the following

A. SOCK_STREAM B. SOCK_DGRM C. AF_INET D. PF_INET

Answer: D. PF_INET

(4) When using Socket to send and receive data, timeout and buffer window can be configured by which of the following function

A. getsockopt B. Inet_addr C. getservbyname D. setsockopt

Answer: A. getsockopt

(5) Which of the following IEEE standards best describe LAN and WLAN respectively?

A. 802.16 and 802.3 B. 802.3 and 802.11 C. 802.15 and 802.11 D. 802.16 and 802.15

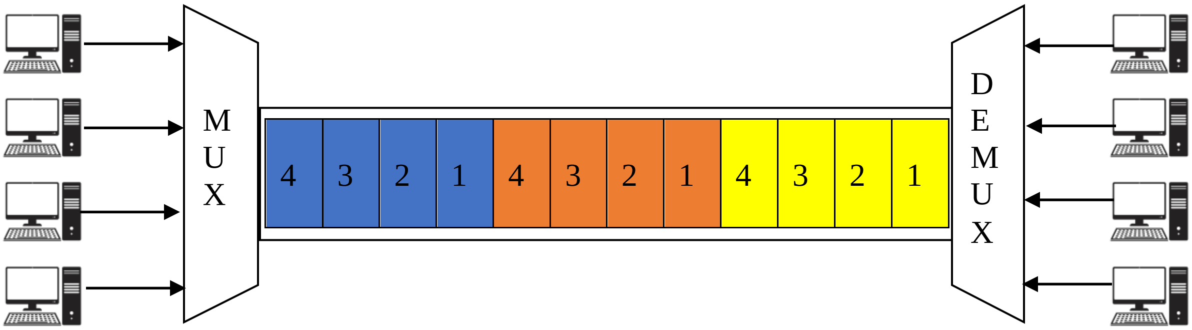
Answer: B. 802.3 and 802.11

3. [20 Points, each 5 points] Brief Questions

(1) Explain major physical layer multiplexing schemes of TDM, STDM, FDM, CDM, and WDM briefly and clearly.

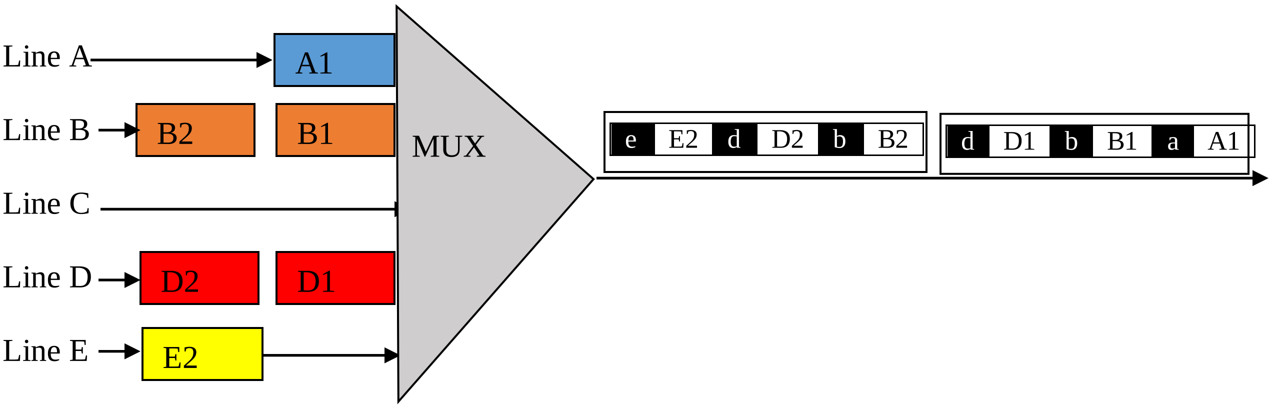
TDM

Answer: TDM is stand for Time Division Multiplexing. TDM is digital multiplexing technique for combining several low rate channel into high rate channel.TDM is mainly useful for analog and digital signals, in which several channels with low speed are multiplexed into high-speed channels used for transmission. Depending on the time and every low-speed channel will be assigned to an exact position, wherever it works in the mode of synchronized. Both the ends of **MUX and DEMUX** are synchronized timely & at the same time switch toward the next channel.



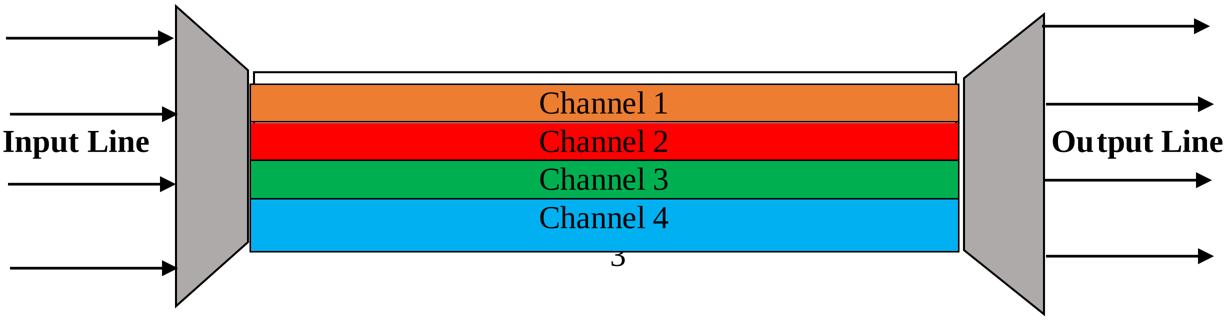
STDM

Answer: STDM is stand for **statistical time division multiplexing.** Statistical time-division multiplexing (STDM) is a form of communication link sharing, which is almost identical to dynamic bandwidth allocation. In STDM, a communication channel is split into a random range of variable bit-rate data streams or digital channels.



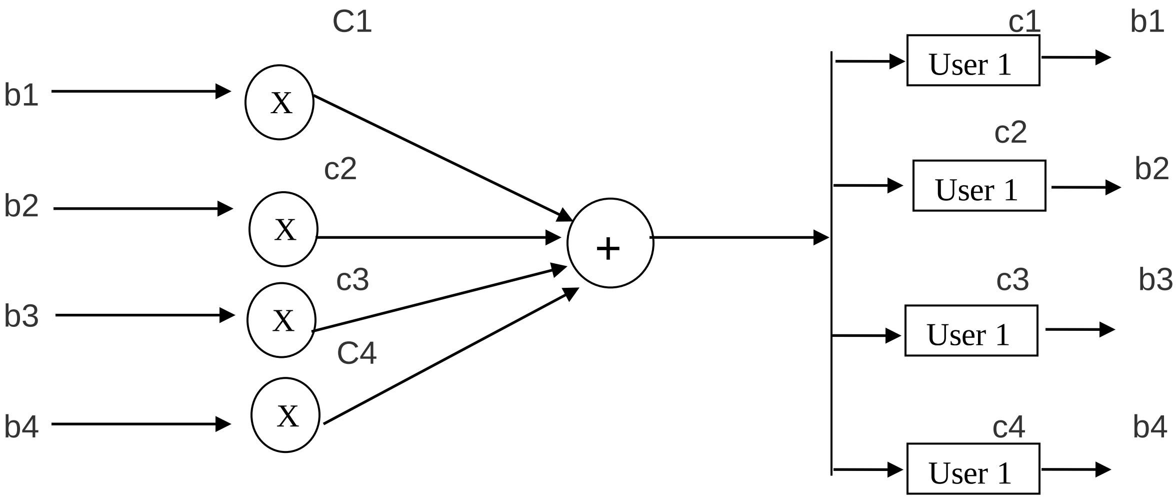
FDM

FDM Stands for Frequency-Division Multiplexing. FDM is a networking technique in which multiple data signals are combined for simultaneous transmission via a shared communication medium. FDM uses a carrier signal at a discrete frequency for each data stream and then combines many modulated signals. Call FDMA When FDM is used to allow multiple users to share a single physical communication.



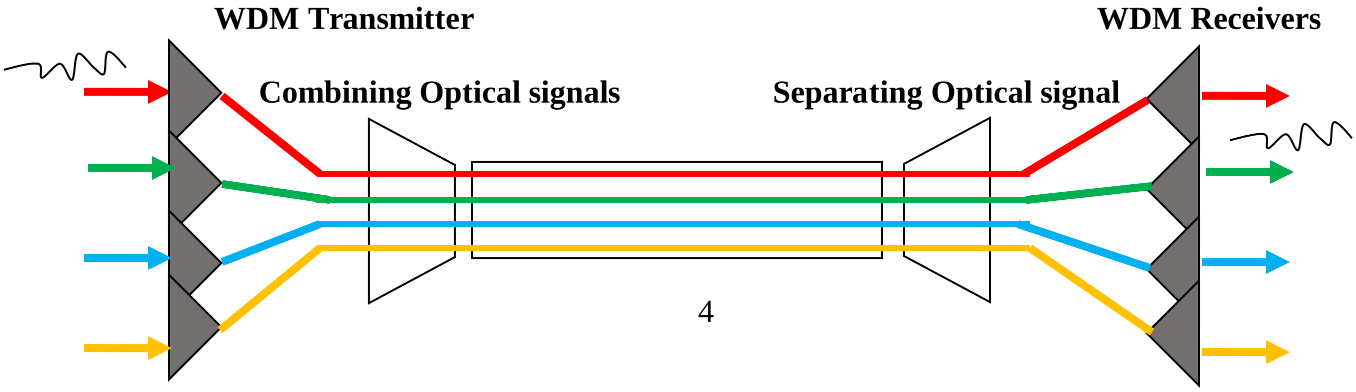
CDM

Answer: CDM is stand for Code division multiplexing. CDM is a networking technique in which multiple data signals are combined for simultaneous transmission over a common frequency band. Call CDMA When CDM is used to allow multiple users to share a single communications channel. A pseudo-random spreading code is used to multiplex the base signal. Multiplexing with a spreading code increases the bandwidth required for the signal, spreading it out over the available spectrum. The receiving device is aware of the spreading code and uses it to DE multiplex the signal. CDMA provides a certain amount of built-in security, as the transmissions of multiple users are mixed together within the frequency spectrum. The spreading code is required to decode a specific transmission. Different variations of CDM and CDMA are used in 2G and subsequent generations of cellphone technology.



WDM

Answer: WDM stands for Wavelength division multiplexing. WDM networks are networks that deploy optical WDM fiber links where each one carries multiple wavelength channels. WDM is a technology that multiplexes several signals over a single optical fiber by optical carriers of different wavelengths which use a laser or a LED. There is a multiplexer and a DE multiplexer at the either end of the WDM. A multiplexer is at the transmitting end to combine several signals together, and a DE multiplexer is at the receiving end to split the signals apart. WDM systems are popular in fiber optic network as they allow to be expanded by simply upgrading the multiplexer and DE multiplexer at each end. And with the help of WDM, there is no need for us to overhaul the backbone network regardless of several generations of technology development.



Transmission on fiber optic line

(2) Explain the following networks PAN, LAN, WLAN, MAN, WAN briefly and clearly.

PAN

Answer: Personal Area Network is the abbreviation is PAN. PAN is the computer network that connects computers/devices within the range of an individual person. As PAN provides a network range within a person's range typically within a range of 10 meters (33 feet) it is called as Personal Area Network. A Personal Area Network typically involves a computer, phone, tablet, printer, PDA (Personal Digital Assistant) and other and other entertainment devices like speakers, video game consoles etc.

Types of Personal Area Network (PAN) :

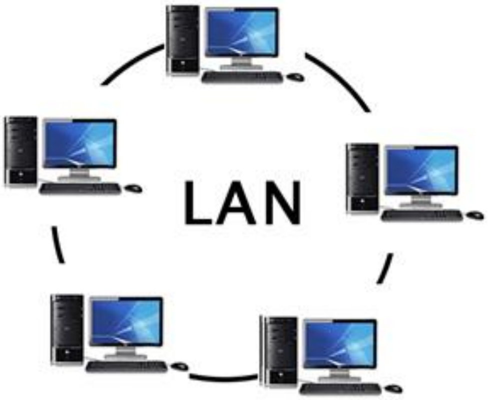
Personal Area Network can be of 2 types depending upon its connection i.e., Wireless PAN, and Wired PAN.

These are explained as following below.

1. **Wireless PAN –**
   Wireless Personal Area Network (WPAN) is connected through signals such as infrared, ZigBee, Bluetooth, Wireless mouse, Wireless keyboard and ultra wideband etc.
2. **Wired PAN –**
   Wired PAN is connected through cables/wires such as Fir wire or USB (Universal Serial Bus).

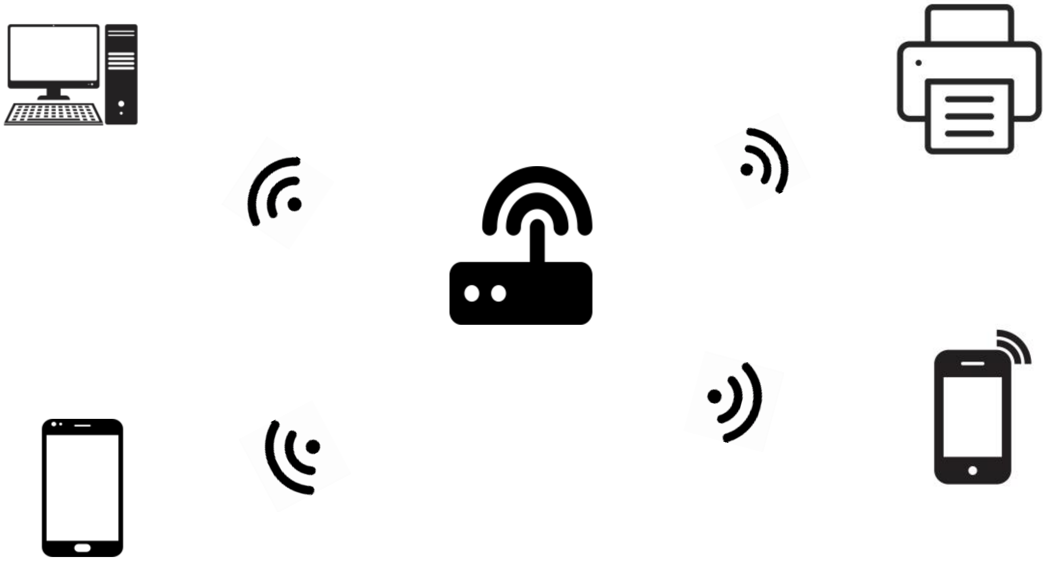
LAN

Answer: A LAN is a computer network that consists of access points, cables, routers, and switches that enable devices to connect to web servers and internal servers within a single building, campus, or home network, and to other LANs via Wide Area Networks (WAN) or Metropolitan Area Network (MAN). Devices on a LAN, typically personal computers and workstations, can share files and be accessed by each other over a single Internet connection. The maximum cable length of a twisted pair is 100 m (328 ft.) while for fiber optic cable, the maximum length ranges from 10 km to 70 km, depending on the type of fiber. Depending on the type of twisted pair or fiber optic cables used, data rates today can range from 100 Mbit/s to 10,000 Mbit/s



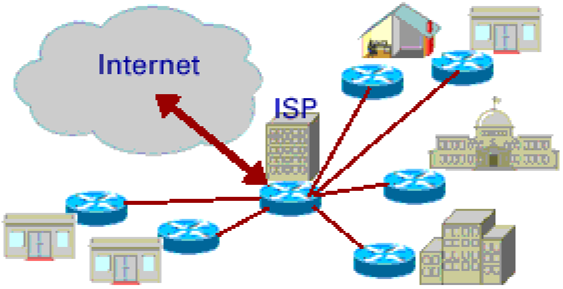
WLAN

Answer: Wireless LAN stands for Wireless Local Area Network**.** It is also called LAWN **(**Local Area Wireless Network**).** WLAN is one in which a mobile user can connect to a Local Area Network (LAN) through a wireless connection. The IEEE 802.11 group of standards defines the technologies for wireless LANs. For path sharing, 802.11 standard uses the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance). Wireless LANs provide high speed data communication in small areas such as building or an office. WLANs allow users to move around in a confined area while they are still connected to the network.



MAN

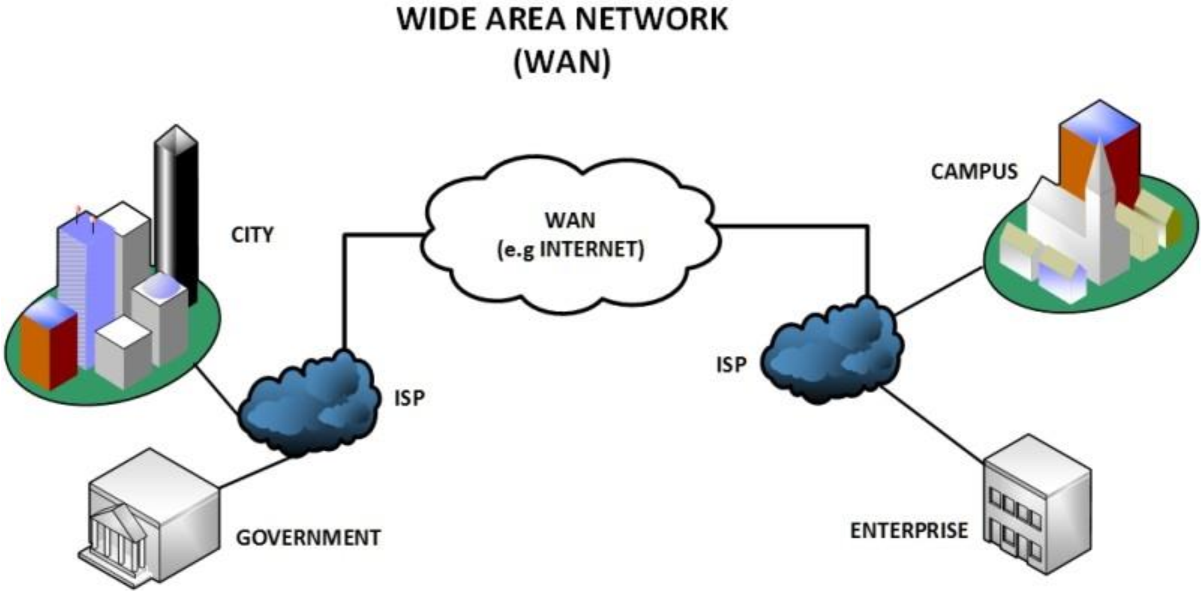
Answer: A metropolitan area network (MAN) is a network with a size greater than LAN but smaller than a WAN. It normally comprises networked interconnections within a city that also offers a connection to the Internet. The distinguishing features of MAN are Network size generally ranges from 5 to 50 km. It may be as small as a group of buildings in a campus to as large as covering the whole city. the Data rates are moderate to high for MAN connection. In general, a MAN is either owned by a user group or by a network provider who sells service to users, rather than a single organization as in LAN. It facilitates sharing of regional resources. They provide uplinks for connecting LANs to WANs and Internet.



Metropolitan Area Network (MAN)

WAN

Answer: WAN stand for Wide Area Network. A wide area network (WAN) is a large computer network that connects groups of computers over large distances. WANs are often used by large businesses to connect their office networks; each office typically has its own local area network, or LAN, and these LANs connect via a WAN.



(3) Explain SDU, PDU, and TPDU briefly and clearly.

Answer:

SDU

Stands for service data unit (SDU). And this is a unit of data that has been passed down from an OSI layer or sublayer to a lower layer. This unit of data (SDU) has not yet been encapsulated into a protocol data unit (PDU) by the lower layer. That SDU is then encapsulated into the lower layer's PDU and the process continues until reaching the PHY, physical, or lowest layer of the OSI *stack*.

PDU

PDU is stands for **protocol data unit** (**PDU**). PDU is a single unit of information transmitted among peer entities of a computer network. A PDU is composed of protocol-specific control information and user data. In the layered architectures of communication protocol stacks, each layer implements protocols tailored to the specific type or mode of data exchange.

TPDU

TPDU is stand for Transaction Protocol Data Unit (TPDU). TPDU is an old-school packet-based protocol designed for transaction-oriented applications. On the OSI model it stands between Transport Layer and the Application Layer. It was originally designed for X.25-based dial up payment devices to provide the ability to concentrate a large number of these into one central host connection. TPDU uses first 5 bytes to store routing information for the payment message and also provides this space for marking up its way back to its origin (source). Having 2 bytes for destination address and 2 bytes for the source address, this system can be effectively set with up to 10^4 routes over 3 router jumps.

(4) What is the difference between the bit rate and baud rate of a signal?

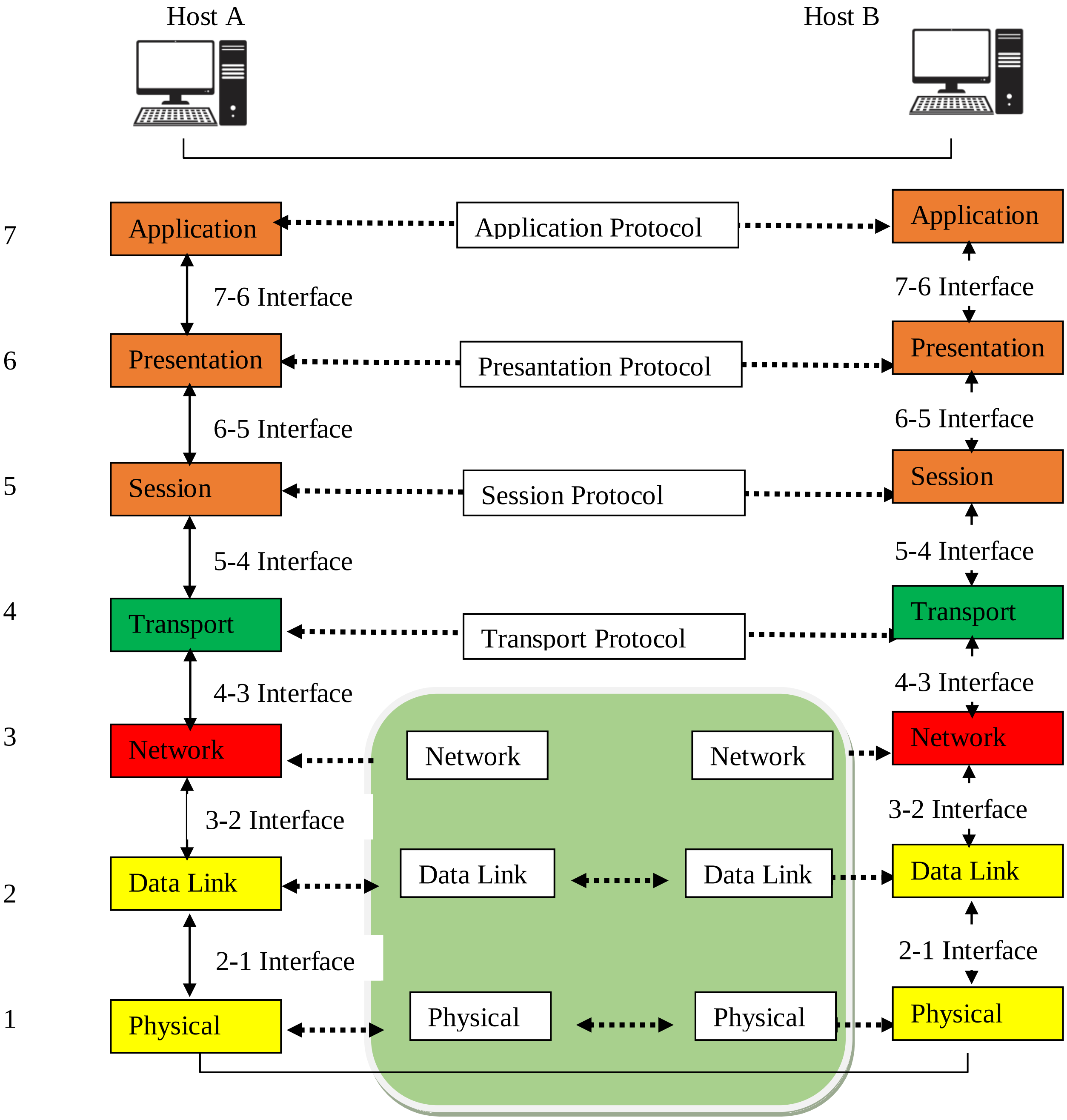
Answer:

Bit Rate	Baud Rate
Bit rate is transmission of number of bits per second.	Baud rate is defined as the number of signal units per second.
Bit rate emphasized on computer efficiency.	While baud rate emphasized on data transmission.
The formula of **Bit Rate** is: = baud rate X the number of bit per baud	The formula of **Baud Rate** is: = bit rate / the number of bit per baud
Bit rate is also defined as per second travel number of bits.	Baud rate is also defined as per second number of changes in signal.

4. [15 points] Please draw the model figures of 7-layer OSI model and 4-layer TCP/IP, and explain each layer and their differences in detail.

Answer:

The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system. The OSI model characterizes computing functions into a universal set of rules and requirements in order to support interoperability between different products and software. In the OSI reference model, the communications between a computing system are split into seven different abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. Created at a time when network computing was in its infancy, the OSI was published in 1984 by the International Organization for Standardization (ISO). Though it does not always map directly to specific systems, the OSI Model is still used today as a means to describe Network Architecture.



❖ The Physical Layer

This layer includes the physical equipment involved in the data transfer, such as the cables and switches. This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s. The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.

❖ Data Link Layer

At the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames. The data link layer also corrects errors that may have occurred at the physical layer. The data link layer encompasses two sub-layers of its own. The first, media access control (MAC), provides flow control and multiplexing for device transmissions over a network. The second, the logical link control (LLC), provides flow and error control over the physical medium as well as identifies line protocols.

❖ Network Layer

Here at the Network Layer is where you'll find most of the router functionality that most networking professionals care about and love. In its most basic sense, this layer is responsible for packet forwarding, including routing through different routers. You might know that your Boston computer wants to connect to a server in California, but there are millions of different paths to take. Routers at this layer help do this efficiently.

❖ Transport Layer

The transport layer takes data transferred in the session layer and breaks it into "segments" on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

❖ The Session Layer

This is the layer responsible for opening and closing communication between the two devices. The time between when the communication is opened and closed is known as the session. The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting resources. The session layer also synchronizes data transfer with checkpoints. For example, if a 100-megabyte file is being transferred, the session layer could set a checkpoint every 5 megabytes. In the case of a disconnect or a crash after 52 megabytes have been transferred, the session could be resumed from the last checkpoint, meaning only 50 more megabytes of data need to be transferred. Without the checkpoints, the entire transfer would have to begin again from scratch.

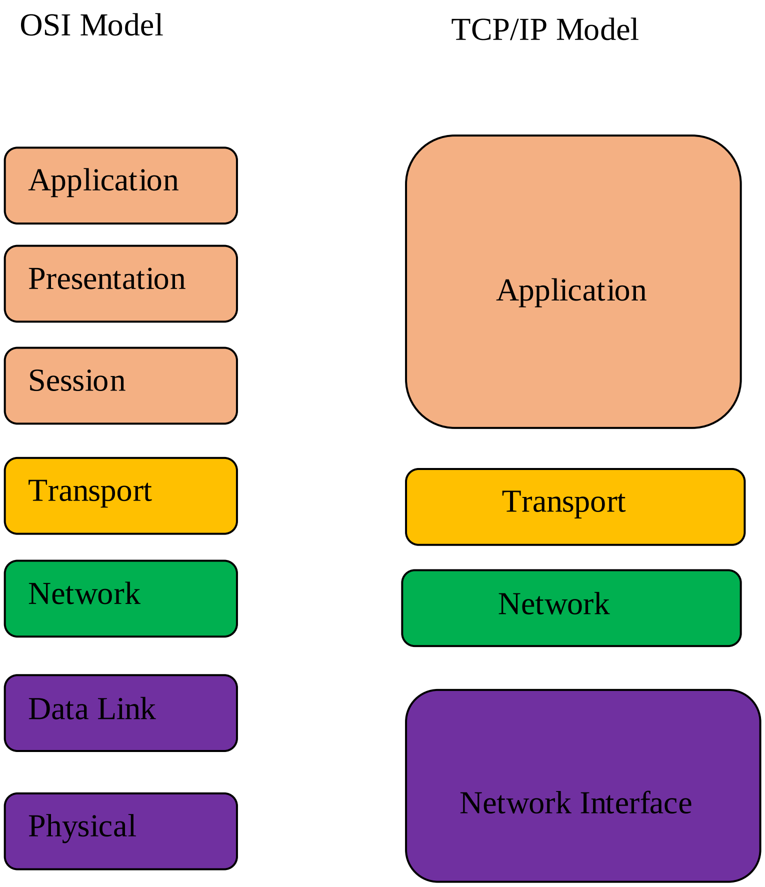
❖ The Presentation Layer

This layer is primarily responsible for preparing data so that it can be used by the application layer; in other words, layer 6 makes the data presentable for applications to consume. The presentation layer is responsible for translation, encryption, and compression of data. Two communicating devices communicating may be using different encoding methods, so layer 6 is responsible for translating incoming data into a syntax that the application layer of the receiving device can understand. If the devices are communicating over an encrypted connection, layer 6 is responsible for adding the encryption on the sender's end as well as decoding the encryption on the receiver's end so that it can present the application layer with unencrypted, readable data.

❖ The Application Layer

This is the only layer that directly interacts with data from the user. Software applications like web browsers and email clients rely on the application layer to initiate communications. But it should be made clear that client software applications are not part of the application layer; rather the application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user. Application layer protocols include HTTP as well as SMTP (Simple Mail Transfer Protocol is one of the protocols that enables email communications).

Tcp/Ip Model



- **Application Layer**

Application layer interacts with an application program, which is the highest level of OSI model. The application layer is the OSI layer, which is closest to the end-user. It means the OSI application layer allows users to interact with other software application. Application layer interacts with software applications to implement a communicating component. The interpretation of data by the application program is always outside the scope of the OSI model. Example of the application layer is an application such as file transfer, email, remote login, etc.

- **Transport Layer**

Transport layer builds on the network layer in order to provide data transport from a process on a source system machine to a process on a destination system. It is hosted using single or multiple networks, and also maintains the quality of service functions. It determines how much data should be sent where and at what rate. This layer builds on the message which are received from the application layer. It helps ensure that data units are delivered error-free and in sequence.
Transport layer helps you to control the reliability of a link through flow control, error control, and segmentation or de-segmentation. The transport layer also offers an acknowledgment of the successful data transmission and sends the next data in case no errors occurred. TCP is the best-known example of the transport layer.

- **Internet Layer**

An internet layer is a second layer of TCP/IP layers of the TCP/IP model. It is also known as a network layer. The main work of this layer is to send the packets from any network, and any computer still they reach the destination irrespective of the route they take. The Internet layer offers the functional and procedural method for transferring variable length data sequences from one node to another with the help of various networks. Message delivery at the network layer does not give any guaranteed to be reliable network layer protocol.

- **The Network Interface Layer**

Network Interface Layer is this layer of the four-layer TCP/IP model. This layer is also called a network access layer. It helps you to defines details of how data should be sent using the network. It also includes how bits should optically be signaled by hardware devices which directly interfaces with a network medium, like coaxial, optical, coaxial, fiber, or twisted-pair cables. A network layer is a combination of the data line and defined in the article of OSI reference model. This layer defines how the data should be sent physically through the network. This layer is responsible for the transmission of the data between two devices on the same network.

Differences between OSI Model and TCP/IP Model

OSI Model	TCP/IP Model
It is developed by ISO (International Standard Organization)	It is developed by ARPANET (Advanced Research Project Agency Network).
OSI is less reliable	TCP/IP is more reliable
OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol.
OSI has 7 layers.	TCP/IP has 4 layers.
Session and presentation layers are not a part of the TCP model.	There is no session and presentation layer in TCP model.
OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
OSI follows a vertical approach.	TCP/IP follows a horizontal approach.
OSI has strict boundaries	TCP/IP does not have very strict boundaries.

5. **[15 points]** Ethernet protocol uses CSMA/CD for multiple access control.
(1) Please explain the three concepts of CS, MA, and CD that are used in CSMA/CD.

Answer: For understanding well how CSMA/CD works, it makes sense to break down the individual components of the CS, MA, and CD:

Carrier sense (CS): The carrier state detection makes sure that all network participants check whether the medium is currently free – only then does the protocol initiate data transmission

Multiple access (MA): Several participants (computers connected to the network) share a transmission medium

Collision detection (CD): The collision detection is an extension of the original protocol and regulates how to proceed in case data packets happen to collide

CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) is a media-access control method that was widely used in Early Ethernet technology/LANs, when there used to be shared. Bus Topology and each Nodes(Computers) were connected by Coaxial Cables. Now a Days Ethernet is Full Duplex and CSMA/CD is not used as Topology is either Star (connected via Switch or Router) or Point to Point (Direct Connection) but they are still supported though.

(2) When a collision is detected, how does Ethernet back off to avoid future collisions? What is the advantage of this scheme compared to random back off?

Answer: How CSMA/CD works, when a frame is ready, the transmitting station checks whether the channel is idle or busy. If the channel is busy, the station waits until the channel becomes idle. If the channel is idle, the station starts transmitting and continually monitors the channel to detect collision. If a collision is detected, the station starts the binary exponential back off algorithm. The station resets the retransmission counters and completes frame transmission.

But if a collision is detected then

- ✓ Step 1) The station continues transmission of the current frame for a specified time along with a jam signal, to ensure that all the other stations detect collision.
- ✓ Step 2) The station increments the retransmission counter, c, that denote the number of collisions.
- ✓ Step 3) The station selects a random number of slot times in the range 0 and $2^c - 1$. For example, after the first collision (i.e. c = 1), the station will wait for either 0 or 1 slot times. After the second collision (i.e. c = 2), the station will wait anything between 0 to 3 slot times. After the third collision (i.e. c = 3), the station will wait anything between 0 to 7 slot times, and so forth.
- ✓ Step 4) If the station selects a number k in the range 0 and 2c – 1, then
  Back_off_time = k × Time slot,
  where a time slot is equal to round trip time (RTT).
- ✓ Step 5) And the end of the back off time, the station attempts retransmission by continuing with the CSMA/CD algorithm.
- ✓ Step 6) If the maximum number of retransmission attempts is reached, then the station aborts transmission.

Advantages

1. The window size where most operations succeed will generally be within a factor of two of the smallest window size where most operations would succeed,
2. Most of the operations which fail at that window size will succeed on the next attempt (since most of the earlier operations will have succeeded, that will leave less than half of them competing for a window which is twice as big), and
3. The total time required for all attempts will end up only being about twice what was required for the last one.

6. **[15 points, each 5 points]** What is the difference between end-to-end delay and packet jitter? What are the causes of packet jitter?
What's the typical means to smooth the packet jitter and make the packet delivery in order?

What is the difference between end-to-end delay and packet jitter?
Answer:

end-to-end delay	packet jitter
A source packet transfer **time** from source to destination through network is called end-to-end delay.	A transferring packet divide into subsequent packets is called packet jitter.
This transmission depends on routers.	This variation depends on path of the network.
The time taken for a packet to go from source to destination across the network is called end-to-end delay.	The variation of End-To-End Delay from packet to subsequent packet is called packet jitter.

What are the causes of packet jitter?
Answer: Packet jitter can be caused by congestion (at routers) in network, low band width links, changes in the travelling path of the packet.

What's the typical means to smooth the packet jitter and make the packet delivery in order?
Answer: jitter doesn't affect sending emails as much as it would a voice chat. So, it depends on what we're willing to accept as irregularities and fluctuations in data transfers. But poor audio and video quality leads to a poor user experience and can impact an organization's bottom line. All networks experience some amount of latency, especially wide area networks. Ideally, over a normally functioning network, packets travel in equal intervals, with a 10ms delay between packets. With high jitter, this could increase to 50ms, severely disrupting the intervals and making it difficult for the receiving computer to process the data. Ideally, jitter should be below 30ms. Packet loss should be no more than 1%, and network latency shouldn't exceed 150 MS one-way (300 MS return).

7. [15 points] Socket and TCP/IP Software and Code
For the following server socket code, please explain
(1) What's the largest number of incoming connection requests from the client for listening socket s of the server in the code?
Answer: A common misunderstanding is that a server cannot accept more than 65,536 (2^16) TCP sockets because TCP ports are 16-bit integer numbers. So A port number uses 16 bits and so can therefore have a value from 0 to 65535 decimal. Finally, the largest number of incoming connection is 65535.

(2) Why socket s can be reused, and why accept() function must create a new socket for the accepted connection in addition to the listening socket s in the code?
Answer:
Reusing socket because You want to run a socket server always on a specific port even after it is closed intentionally or unexpectedly. This is useful in some cases where your client program always connects to that specific server port. So, you don't need to change the server port. The accept() call is used by a server to accept a connection request from a client. When a connection is available, the socket created is ready for use to read data from the process that requested the connection. The call accepts the first connection on its queue of pending connections for the given socket**.**

(3) Why need to close(fd), close(sa), and close(s) in the code?

Answer: once open a file for sent it back for one time it should open and after the file opening session the file should close otherwise the same file will read for the next session so close(fd) function is for close the opened file.

Block connection request, sending the packet when a connection to be requested the function will take it but after sent the specific packet then the block connection will be close otherwise the connection will be alive still. So this is the reason for close Block connection by using close(sa) function.

Once a socket is no longer of interest, it may be discarded by applying a close to the descriptor:

close(s);

If data is associated with a socket that promises reliable delivery (e.g. a stream socket) when a close*()* takes place, the system will continue to attempt to transfer the data. However, if after a fairly long period of time the data is still undelivered, it will be discarded.

(4) Why need to use htonl() and htons() functions in the code?

Answer: The htonl function takes a 32-bit number in host byte order and returns a 32-bit number in the network byte order used in TCP/IP networks (the AF_INET or AF_INET6 address family). The htonl function can be used to convert an IPv4 address in host byte order to the IPv4 address in network byte order. This function does not do any checking to determine if the *hostlong* parameter is a valid IPv4 address.

htons()

The ntohs function takes a 16-bit number in TCP/IP network byte order (the AF_INET or AF_INET6 address family) and returns a 16-bit number in host byte order. The ntohs function can be used to convert an IP port number in network byte order to the IP port number in host byte order.

```
… …
#define BUF_SIZE 4096
#define QUEUE_SIZE 10

int main(int argc, char * argv[])
{
   int s, b, l, fd, sa, bytes, on = 1;
   char buf[BUF SIZE]; / * buffer for outgoing file * /
   struct sockaddr_in channel; / * holds IP address * /
   / * Build address structure to bind to socket. * /
   memset(&channel, 0, sizeof(channel)); / * zero channel * /
   channel.sin family = AF INET;
   channel.sin addr.s addr = htonl(INADDR ANY);
   channel.sin port = htons(SERVER PORT);
   / * Passive open. Wait for connection. * /
   s = socket(AF INET, SOCK_STREAM, IPPROTO_TCP); / * create socket for the server* /
   if (s < 0) fatal("socket failed");
   setsockopt(s, SOL_SOCKET, SO_REUSEADDR, (char * ) &on, sizeof(on));
   b = bind(s, (struct sockaddr * ) &channel, sizeof(channel));
   if (b < 0) fatal("bind failed");
   l = listen(s, QUEUE_SIZE); / * specify queue size * /
   if (l < 0) fatal("listen failed");
   / * Socket is now set up and bound. Wait for connection and process it. * /
   while (1) {
      sa = accept(s, 0, 0); / * block for connection request * /
      if (sa < 0) fatal("accept failed");
      read(sa, buf, BUF SIZE); / * read file name from socket * /
      / * Get and return the file. * /
      fd = open(buf, O RDONLY); / * open the file to be sent back * /
      if (fd < 0) fatal("open failed");
      while (1) {
         bytes = read(fd, buf, BUF SIZE); / * read from file * /
         if (bytes <= 0) break; / * check for end of file * /
         write(sa, buf, bytes); / * write bytes to socket * /
      }
      close(fd); / * close file * /
      close(sa); / * close connection * /
   }
   close(s);
}
```