Networks, Information Systems, Software Engineering and Web Technology

UNIT 8

Part A Network

Chapter 1

OSI Layers

LEARNING OBJECTIVES

- *Computer network*
- *LAN*
- *LAN topologies*
- *CSMA/CD*
- *WAN*
- *The OSI reference model*
- *LAN technologies*
- *Physical layer*
- *Data link layer*
- *Types of error*
- *MAC sub layer*
- *FDM/TDM*

Computer Network

Computer network is the collection of two or more computers that are interconnected with each other to perform data communication using the data communication protocol through communications media (wired or wireless) .So these computers can share information, data, programs, and use of hardware together. Data communications that can be done include text data, images, video and sound.

Or

A computer network, often simply referred, as a network is a collection of computers and devices interconnected by communication channels that facilitate communication and allow sharing of resources and information among interconnected devices. There are different networks:

1. LAN
2. MAN
3. WAN

LAN

A Local Area Network (LAN) is a network that is confined to a relatively small area. It is generally limited to a geographic area such as a lab, school, or building. LAN Computers rarely spans more than a mile apart.

In a typical LAN configuration, one computer is designated as the file server. It stores all the software that controls the network, as well as the software that can be shared by the computers attached to the network. Computers connected to the file server are called workstations. The workstations can be less powerful than the file server, and they may have additional software on their hard drives. On many LANs, cables are used to connect the network interface cards in each computer. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves.

Most LANs connect workstations and personal computers. Each node (individual computer) in a LAN has its own CPU which executes programs and it is also able to access data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use LAN to communicate with each other, by sending e-mail or engaging in chat sessions.

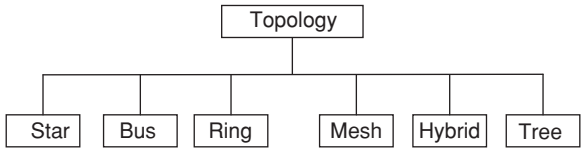
Three characteristic features of LAN

1. The size of a LAN network.
2. The topology of the local area network.
3. The technology used for transmission.

In simple LAN configuration, a single cable runs through the entire set up and the peripherals and computers are attached to the cable. Traditional LAN speeds are 10 Mbps to 100 Mbps. Modern LAN cables are capable of much higher data transfer per second.

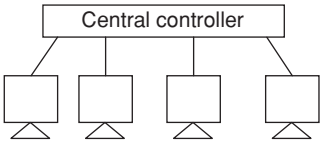
In case two or more systems need to use the LAN at the same time, then an arbitration mechanism is deployed to resolve the conflict. A first come first serve policy or a prioritized approach may be chosen.

LAN topologies



Star Topology Each device has a dedicated point-to-point link to a central controller called a hub. Most used LAN topology.

If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device as shown in the figure.



Each device needs only one link and one I/O port to connect it to any number of others.

Advantages

1. Robust, if one link fails, only that link is affected. All other links remain active.
2. As long as hub is working, it can monitor link problems and by pass defective links.

Disadvantages

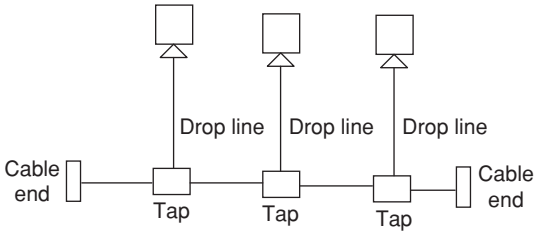
1. If hub goes down, the whole system dead.
2. More cabling is required in a star than ring or bus.

Bus Topology A bus topology is multipoint. One long cable acts as a backbone to link all the devices in a network.

Carrier Sense Multiple Access/Collision Detection (CSMA/CD) is the accessing technique used.

The traffic can go in either direction, i.e., it is bidirectional.

Nodes are connected to the bus cable by drop lines and taps as shown in the figure.



Advantages

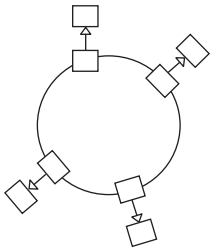
1. Ease of installation.
2. Require less cabling than mesh or star topologies.

Disadvantages

1. Difficult to add new devices.
2. A fault in the bus cable stops all transmission. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

Ring Topology Each device has a dedicated point-to-point connection with only the two devices on either side of it.

Each device in the ring incorporates a repeater; when a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



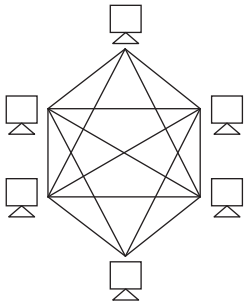
Advantages

1. Easy to install and reconfigure.
2. Fault isolation is simplified as it issues alarm which alerts the network operator to the problem and its location.

Disadvantages

1. A break in the ring can disable the entire network.
2. It is not relevant for higher-speed LANs.

Mesh topology Every station is interconnected to every other station as shown in the figure.



$n(n-1)/2$ (duplex mode) links are required for communication in both directions. Each device on the network must have $(n-1)$ I/O ports to be connected to the other $(n-1)$ stations.

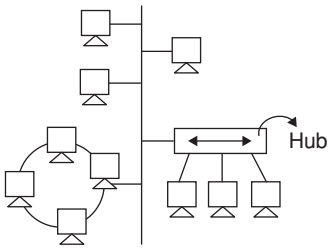
Advantages

1. The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating traffic problems.
2. This topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
3. There is advantage of security, only the intended recipient sees the message on the dedicated line.
4. Fault identification and fault isolation is easy because of point-to-point links.

Disadvantages

1. As the hardware(cables) required for connection is more, it is expensive.
2. Installation and reconnection are difficult.
3. The sheer bulk of the wiring can be greater than the available space.

Hybrid Topology More than one topology in a network.



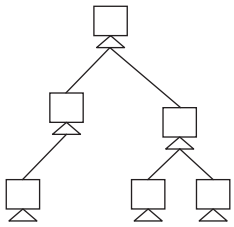
Advantages

1. Fault detection is easier.
2. We can add new stations without affecting the original architecture.

Disadvantages

1. As different topologies are combined so complexity of design increases. Very less practical implementation.
2. The hub which is used to connect different topologies is very costly. Moreover the cost of whole infrastructure is very high.

Tree Topology This topology uses the combination of star and bus topology.



Advantages

1. Expansion is easier; one can add new stations easily.
2. Errors can be easily detected.
3. Robust, if one link fails the remaining system is in communication.

Disadvantages

1. With the increase in the number of nodes, complexity and maintenance become difficult.

Examples: The most common type of local area network is an Ethernet LAN. The smallest home LAN can have exactly two computers; a large LAN can accommodate thousands of computers. Many LANs are divided into logical groups called subnets. An Internet Protocol (IP) 'Class A' LAN can in theory accommodate more than 16 million devices organized into subnets.

MAN

A metropolitan area network is a computer network that usually spans a city or a large campus. A MAN usually interconnects a number of local area networks (LANs) using a high-capacity backbone technology, such as fiber-optical links, and provides up-link services to wide area networks (or WAN) and the Internet.

WAN

Wide Area Networks (WANs) connect larger geographic areas, such as Florida, the United States, or the world. Dedicated transoceanic cabling or satellite uplinks may be used to connect this type of network.

A WAN is complicated; it uses multiplexers to connect local and metropolitan networks to global communications networks like the Internet. To users, however, a WAN will not appear to be much different than a LAN. As the term implies, a WAN spans a large physical distance. The Internet is the largest WAN, spanning the Earth.

A WAN is a geographically-dispersed collection of LANs. A network device called a router connects LAN to a WAN. In IP networking, the router maintains both a LAN address and a WAN address.

A WAN differs from a LAN in several important ways. Most WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management. WANs tend to use technology like ATM, Frame Relay and X.25 for connectivity over the longer distances.

Residences typically employ one LAN and connect to the Internet WAN via an Internet Service Provider (ISP) using a broadband modem. The ISP provides a WAN IP address to the modem, and all of the computers on the home network use LAN (so-called private) IP addresses. All computers on the home LAN can communicate directly with each other but must go through a central gateway, typically a broadband router, to reach the ISP.

The OSI Reference Model

The concept of how a modern day network operates can be understood by dissecting it into seven layers. This seven layer model is known as the OSI Reference Model and defines how the vast majority of the digital networks on earth function. OSI is the acronym for Open Systems Interconnection. The important concept to realize about the OSI Reference Model is that it does not define a network standard, but rather provides guidelines for the creation of network standards.

Physical Layer

The first layer of a network is the Physical Layer. The Physical Layer is literally what its name implies: the physical infrastructure of a network.

This includes the cabling or other transmission medium and the network interface hardware placed inside computers

and other devices which enable them to connect to the transmission medium.

The purpose of the Physical Layer is to take binary information from higher layers, translate it into a transmission signal or frequency, transmit the information across the transmission medium, receive this information at the destination and finally translate it back into binary before passing it up to the higher layers.

Transmission signals or frequencies vary between network standards and can be as simple as pulses of electricity over copper wiring or as complex as flickers of light on optical lines or amplified radio frequency transmissions.

The information that enters and exits the Physical Layer must be bits; either 0s or 1s in binary. The higher layers are responsible for providing the Physical Layer with binary information. Since almost all information inside a computer is already digital, this is not difficult to achieve.

The Physical Layer does not examine the binary information nor does it validate it or make changes to it. The Physical Layer is simply intended to transport the binary information between higher layers located at points A and B.

Data Link Layer

The second layer in the OSI Model is the Data Link Layer, the only layer in the OSI model that specifically addresses both hardware and software.

The Data Link Layer receives information on its software side from higher layers, places this information inside 'frames', and finally gives this frame to the Physical Layer, Layer 1, for transmission as pure binary.

A frame essentially takes the information passed down from a higher layer and surrounds it with Physical Address information. This information is important for the Data Link Layer on the receiving end of the transmission.

When the frame, in binary form, arrives at the destination node, it is passed from the transmission medium to the Data Link Layer (Layer 2) by the Physical Layer (Layer 1).

The Data Link Layer on the receiving node checks the frame surrounding the information received to see if it's Physical Address matches that of its own. If the Physical Address does not match, the frame and its encapsulated data is discarded. If the Physical Address is a match, then the information is removed from the frame and passed up to the next highest layer in the OSI Model.

The Physical Addressing system allows multiple nodes to be on the same network medium, but retain the ability to address only a specific node with a transmission.

The Physical Address used in the Data Link Layer's Physical Addressing system is known as a MAC address and is embedded physically into the node's Network Interface Card during manufacturing.

Every NIC's MAC address is unique in order to prevent addressing conflicts. It is this relationship that causes the Data Link Layer to be known as the only layer that addresses both hardware and software.

In this layer the information on the network makes the move from the physical infrastructure of the network into the software realm. The remainders of the OSI reference model's layers are entirely software.

Network Layer

OSI Layer 3 is known as the Network Layer. The purpose of the Network Layer is to direct network traffic to a destination node who's Physical Address is not known. This is achieved through a system known as Logical Addressing.

Logical Addresses are software addresses assigned to a node at Layer 3 of the OSI Model. Since these addresses are able to be defined by software rather than being random and permanent like Physical Addresses, Logical Addresses are able to be hierarchical. This allows extremely large networks to be possible.

A smart device working at Layer 3 that handles network signals from each node directly rather than nodes just blindly repeating packets at Layer 1 until they happen to reach their destination. Such a device is known as a network router.

A network router sits in the center of a network with all nodes having a direct link to it rather than being linked to each other. This strategic position allows the router to intercept and direct all traffic on the network.

A routed network can be illustrated by a star formation, as shown in Diagram 1. On a routed network, Layer 3 packets are no longer broadcasted to all nodes, but rather received by the router and passed on only to the appropriate node. This is a valuable concept because it allows for the collision free-transport of packets across a network.

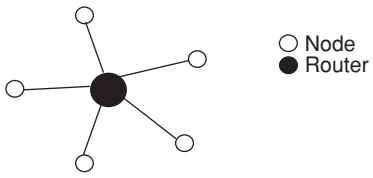


Figure 1

As being linked directly to all nodes in a local network, a router can be linked directly to other routers. This allows groups of nodes separated by distance to communicate with each other in a practical way.

It would not be practical to have nodes separated by a great distance all connected to a single router. The amount of cabling required would be immense and depending on the number of nodes involved, the router may not posses the required number of physical connections.

Routers can be chained in a line, or as shown in Diagram 2, can be connected by a central router. This concept is virtually infinitely scalable and is very efficient.

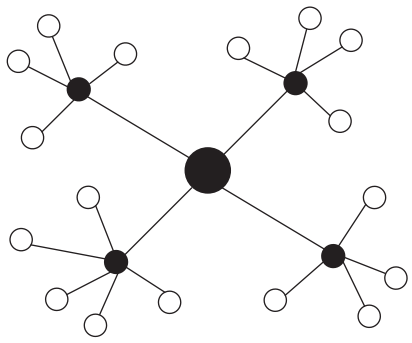


Figure 2

When a node starts a transmission, the OSI Layer 3 protocol takes the information passed down from higher layers and encapsulates it with the logical address of the destination node in a unit called a packet.

This packet, then passes through the remaining lower layer protocols, is transmitted over the network medium from the node to the router. This router reads the logical address that the packet contains and compares it to a list of physical addresses of nodes that are directly connected to it.

If the packet's destination address matches an entry in this list, the packet is transmitted directly on the line that leads straight to the destination node.

If the router does not know of a direct connection to the destination node, the packet is transmitted on a line leading directly to another router. This router then treats the packet much like the first router did upon receipt.

The packet's logical address is checked for matches against the list of logical addresses belonging to nodes directly connected to the router.

If the packet reaches a router with connections only to other routers, as shown in Diagram 2, the router uses the logical address's orderly numbering scheme to try and determine the closest router to the destination node and then transmits the packet to that router.

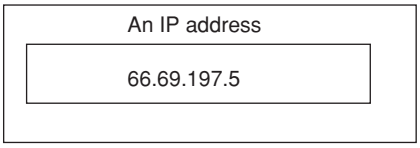


Figure 3

In IP, logical addresses look like four sets. Diagram 3 shows an example of an IP address. IP addresses are orderly on four levels, from left to right. The first section of the IP address refers to a top level router, or a router that is at the highest level of this particular branch of the network. In Diagram 3, the first number is 66. Therefore all IP addresses between 66.0.0.1 and 66.255.255.255 are managed by this router. Only one router is required in a routed network, but more may exist. A router may have a maximum of 255 nodes, which may be either ordinary nodes or other routers. This effectively means that each branch of a network, a group of nodes that have the first set of numbers in their IP address in common, could theoretically have over sixteen million end nodes.

Transport Layer

OSI Layer 4 is known as the Transport Layer, all information transferred is assumed to be at the correct destination node and is being passed up to Layer 4.

The Transport Layer is responsible for the reliability of the link between two end users and for dividing the data that is being transmitted by assigning port numbers to its Layer 4 packages, known as segments.

Ports can be thought of as virtual destination mailboxes or outlets. When information reaches a Layer 4 protocol, the segment is examined to determine the destination port of the data it contains. Once the port is determined, just as all of the past layers have done, the wrapper is discarded and the payload data passed up to the next layer's protocol.

Higher layer protocols that provide services such as email, web browsing, text chat, file transfer and more, each operate on their own unique Layer 4 port, allowing all of these protocols to be operated at once without interference.

On the reliability front, Transport Layer protocols are be capable of running a checksum on the payload data, which they carry. This allows the protocol to determine the integrity of incoming payload data. If this data has been corrupted, the Layer 4 protocol will request the segment to be retransmitted.

Session Layer

OSI Layer 5, known as the Session Layer, still serves a purpose in the OSI Reference Model. The Session Layer draws the outline for protocols that manage the combination and synchronization of data from two separate higher layers.

Layer 5 protocols are responsible for ensuring that the data is Synchronized and consistent before transmitted. A good example is the streaming of live multimedia audio and video, where perfect synchronization between video and audio is desired.

Presentation and Application Layers

The sixth and seventh layers in the OSI Reference Model are the Presentation Layer and the Application Layer. The primary purpose of these layers is to facilitate the movement of formatted information between applications interacting with end users on nodes.

Commonly used top layer protocols are HTTP (for the secure transfer of web page related files), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP, used for sending email messages), and SSH (Secure Shell), used to secure remote shell access for a computer operating system.

OSI reference model concept

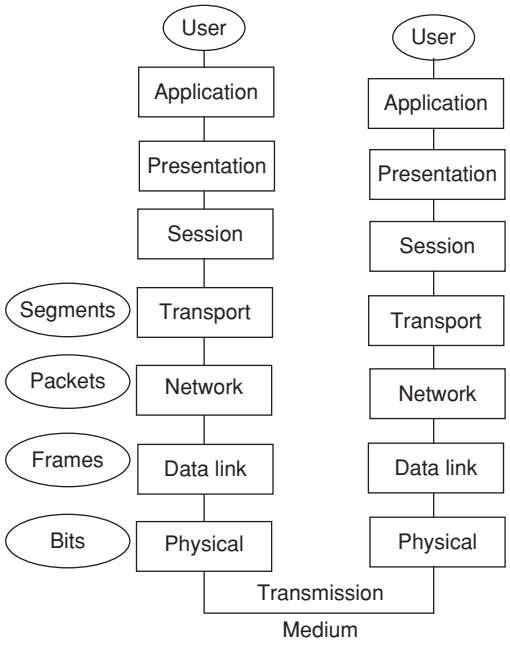


Figure 4

The OSI Reference Model exists not to make hard rules or to shape the industry, but to provide a logical, well-researched, and tested model after which the world's best communication protocol stacks are modeled. The TCP/IP stack is very well-known for being the driving force behind most of the internet, and represents the third (IP) and fourth (TCP) layers of the OSI Model. Every layer in the OSI Model is a reference for a protocol which must facilitate communication between both higher and lower layers. The 'U-shaped' example shown in Diagram 4 provides a visual concept of how two users may be linked on a given network in reference to the OSI Model. Data starts and ends with the user. From the Application Layer of the first user, it must travel down through layers 7 to 1, across the transmission medium, then back up to layers 1 to 7 to be presented at the Application Layer to the user on the end of the transmission. Diagram 4, shows an example of a path between two nodes. Protocols defined by this reference are dependent on the next lowest layer protocol. So, for example, one could not run an Application Layer protocol on a node without the presence of Layer 1 through 6, protocols also being utilized on the node.

LAN TECHNOLOGIES

IEEE standard for networking

IEEE standard project 802 is designed for the enter – connectivity between LAN's

IEEE 802 maps to physical and data link layer

Example: Ethernet, Token ring etc, the IEEE standards for the different groups are

802.1 – Higher layer LAN Protocol
802.3 – Ethernet
802.11 – Wireless LAN
802.15 – WPAN
802.16 – Broad band wireless Access
802.17 – Resilient packet Ring
802.18 – Radio Regulatory TAG
802.19 – Co existence TAG
802.20 – Mobile Broad band wireless access
802.21 – Media independent Hand off

} Active working grourp

802.2 – Logical link control working group
802.4 – Token Bus
802.5 – Token Ring
802.7 – Broad band area Network
802.8 – Fiber optic TAG
802.9 – Integrated service LAN
802.10 – Security working group
802.12 – Demand priority working group
802.14 – Cable modern working group

} In active or dis-banded working groups

Ethernet

We have

10 Mbps – Ethernet
100 Mbps – Fast ethernet
1 Gbps – Gigabit Ethernet
10 GE – 10 Gigabit Ethernet

Best suited for LAN because it is capable of handling high speed bandwidth.

- Ethernet medium:
  Thick wire – 10B5
  Thin wire – 10B2
  Twisted pair – 10BT, 100BT, 1000BT
  Fibre – 10BF, 100BF, 1000BF
  CAT 4 – 10 Mbps
  CAT 5 – 10/100 Mbps
  CAT 6 – 10/100/1000 Mbps
- Fundamental is CSMA/CD, Standard is 802.3.
- It defines two categories:
  1. Base band. 2. Broad band
- Baseband uses digital manchester encoding techniques.
- IP communication in ethernet is of 3 types:
  (i) Unicast
  (ii) multi cast
  (iii) broadcast
- When user sends data he puts destination and source address.
  (i) In unicast, only intended users responds, however all can get the signal (individual MAC).
  (ii) In multicast, group of users will get the data (group MAC).
  (iii) In broadcast, all users on Ethernet can see the data (all MAC).
- Every computer accepts 3 types of packets, to his own, to the group it belongs, to all.

CSMA/CD

CSMA (Carrier Sense Multiple Access)

CSMA protocols performance is better than ALOHA—Monitor the channel before and/or during data transmission.

1-Persistent Check whether the channel is free before transmitting the data. If busy, wait until it becomes free and then immediately start Re-transmitting.

Non-Persistent When the channel is busy, wait for a random period of time before trying again

If the waiting time is too long, the channel utilization decreases.

P-Persistent Used in slotted systems, If the channel is idle during the current slot, transmit with probability P, and defer until next slot with probability $(1 - P)$

Two or more computers can get connected on same physical medium. All computers can communicate whenever they feel like. Any computer want to communicate, it senses the medium, if medium is free and not used by anyone it captures the medium and puts its data on to the channel.

All computers listens to the sent data but only intended computer/system will respond. At this instance, sending computer is owner of the medium; no other system can be owner or can send the data. When two or more computers try to send data at same time by sensing the medium, collision occurs, which will be sensed by all the computers, then they keep integral wait unit of time for next transmission of data. Once the sending machine gets the corrupted collision message it retransmits using integral time.

MAC sublayer

The medium Access control (MAC) sub layer is the bottom half of the Data link layer. The upper half is commonly called logical link control (LLC) sublayer.

Frame format

Preamble	SFD	Destination address	Source address	Length or type	Data and padding	CRC
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 to 1500 bytes	4 bytes

Preamble The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating 0's and 1's that alerts the receiving system to the coming frame and enables it to synchronize its input timing.

Start frame delimiter (SFD) The second field (1 byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that, this is the last chance for synchronization. The last 2-bits is 11 and alerts the receiver that the next field is the destination address.

Destination address (DA) The DA field is 6 bytes and contains the physical address of the destination station to receive the packet.

Source address (SA) The SA field is also 6 bytes and contains the physical address of the sender of the packet.

Length field The original ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard uses it as the length field to define the number of bytes in the data field.

Data This field contains data encapsulated from the upper layer protocols. It is of minimum 46 bytes and a maximum of 1500 bytes.

Ethernet follows **binary exponential back off** algorithm to give waiting time for stations, which are involved in collisions. After collisions, waiting time for the stations will be K * 51.2 μ sec, where K is randomly picked up from 0 to $2^n - 1$, 'n' is the collision number. But after 10 collisions, the randomization internal is frozen at a maximum of 1023 slots.

If each station transmits during a contention slot with probability p, the probability A that some station acquires the channel in that slot is

$A = Kp\ (1 - p)^{k-1}$

A is maximized when $p = 1/k$, with $A \rightarrow 1/e$ as $K \rightarrow \infty$

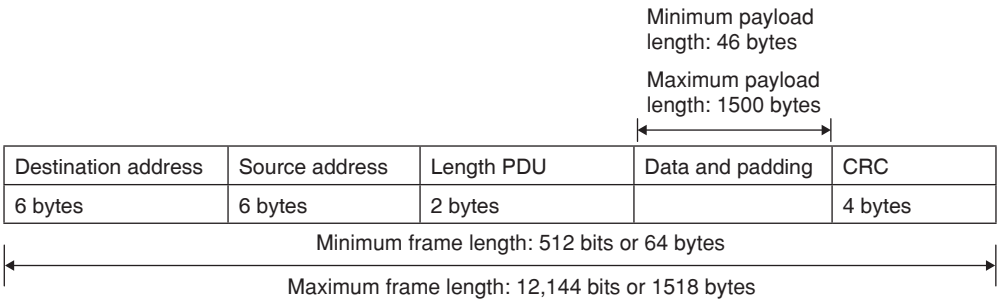
The probability that the contention internal has exactly j slots in it is $A(1 - A)^{j-1}$, hence mean number of slots per contention is given by

$$\sum_{j=0}^{\infty} jA(1-A)^{j-1} = \frac{1}{A}$$

CRC The last field contains error detection information.

Frame length

Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame, as shown in figure below:.



Minimum length of frame is 512 bytes or 64 bytes. If we count 18 bytes of header and trailer, then minimum length of data from the upper layer is 64 – 18 = 46 bytes.

If the upper layer packet is less than 46, padding is added to make up the difference and used to find out collision. Maximum length of the frame is 1518 bytes. If we substract 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes.

- The maximum length restriction has two reasons.
- First, memory was very expensive when ethernet was designed, a maximum length restriction helped to reduce the size of the buffer.
- Second, the maximum length restriction prevents one station from monopolizing the shared medium, blocking other stations that have data to send.

Since each slot has a duration $2T$, the mean contention internal, w, is $2T/A$. Assuming optional p, the mean number of contention slots is never more than e, so w is atmost $2Te = 5.4$ T.

$$\text{Channel efficiency} = \frac{p}{p + 2T/A}$$

$$= \frac{1}{1 + 2B\dfrac{Le}{cF}}$$

Where F = Frame length
B = Network bandwidth
L = Cable length
C = Speed of signal propagation
E = Contention slots per frame

802.5 TOKEN Ring

Here ring topology is used and devices are physically arranged to form a ring. A token is passed among stations. If a station wants to send data, it must wait and capture the token. Only the token holders are permitted to transmit frame. Token ring allows each station to send one frame per turn.

Frame formats

SD	AC	FC	Destination address	Source address	Data	CRC	ED	FS
1 byte	1 byte	1 byte	2-6 bytes	2-6 bytes	Up to 4500 bytes	4 bytes	1 byte	1 byte

SD	AC	ED

Token frame

SD	ED

Abort frame

802.5 Token ring uses differential Manchester digital signal encoding. It supports data rates upto 16 mbps. Tokens ring protocol specifies three types of frames: Data, token, and abort.

The token and abort frames are both truncated data frames.

Data frame

Start delimiter (SD) It is one byte long and is used to alert the receiving station for the arrival of a frame as well as to synchronize it's timing.

Access control (AC) It is one byte long and includes subfields. It has the format PPPTMRRR. First 3-bits are priority field. T denotes whether this is a data frame, token or an abort frame. Token bit is followed by monitor bit. The last 3 bits are the reservation field that can be set by stations wishing to resume access to ring.

Frame control This field is one byte long and contains two fields. The first is a one bit field used to indicate the type of information (whether it is a control information or data). The second uses the remaining seven bits of the byte and contains information used by the token ring logic.

Destination address (DA) The six byte DA field contains the physical address of the frame's next destination.

Source address (SA) The six byte SA field contains the physical address of the sending station.

Data contains LLC data unit Data contains 0 or more bytes, maximum size of the data depends upon taken holding time.

CRC The CRC field is 4 byte long and contains a CRC – 32 bit error detection sequence.

End delimiter (ED) ED is a second flag field of one byte and indicates the end of the sender's data and control information.

Frame status It is one byte long

A/C			A/C		

A: Addressed recognized bit
C: Copies bit

It can be set by the receiver to indicate that the frame has been read/copied etc.

When a frame arrives at the station with the destination address, the station turns A bits to 1. If station copies the frame to the station it also turns on the C bit. A station might fail to copy a frame due to lack of frame buffer or other reason.

When the sending station receives the frame, it examines the A and C bits.

Three combinations are possible:

1. $A = 0$, $C = 0$: destination not ready /present.
2. $A = 1$, $C = 0$: destination present byte frame not accepted.
3. $A = 1$, $C = 1$: destination present and frame copied.

Token frame

It includes only 3 fields: SD, AC and ED

1. The SD indicates, the frame is coming
2. The AC indicates that the frame is a token and includes priority and reservation fields. $T = 0$ for token in AC.
3. The ED indicates the end of the frame.

Abort frame

An abort frame contains no information at all just starting and ending delimiters. It can be generated by the sender to stop its own transmission. Each station has a priority code, as a frame passes by, a station waiting to transmit may reserve the next open token by entering its priority code in the Access control field (AC) of the token or data frame. A station with a higher priority may remove a lower priority reservation and replace it with its own. Among stations of equal priority, the process is first come, first served. Through this mechanism, the station holding the reservation gets the opportunity to transmit as soon as the token is free, whether or not it comes next physically on the ring.

Monitor station Several problems may appear to disrupt the operation of a token ring network. If the token is destroyed by noise there will be no token on the ring and no station can send data. To solve such a problem, one station on the ring is designated as a monitor. The monitor sets a time, each time the token passes. If the token does not appear in the allotted period of time, it is assumed to be lost and the monitor generates a new token and introduces it to the ring. The monitor detects the orphan frames, by setting the monitor bit in the access control byte.

As the frame passes, the monitor checks the status field. If the monitor bit is set, something is wrong since the frame has passed the monitor twice, so monitor discards it. The monitor then destroys the frame and puts a token on the ring. If monitor fails, the protocol ensures that another station is quickly selected as monitor. Every station has the capability of becoming the monitor. While the monitor is functioning properly, it alone is responsible for seeing that the ring operates correctly.

When station notices that either of its neighbors appears to be dead it transmits BEACON frame giving the address of the dead station.

Physical Layer

Physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1-bit, it is received by the other side as 1-bit and not as 0 bit. In physical layer we deal with the communication medium used for transmission.

Types of Medium

Medium can be classified into two categories:

1. Guided Media: Guided media means that signals are guided by the presence of physical media i.e., signals are under control and remains in the physical wire. For example, copper wire.
2. Unguided Media: Unguided media means that there is no physical path for the signal to propagate. Unguided media has essentially electromagnetic waves. There is no control on flow of signal. For example, radio waves.

Transmission Media

In Guided transmission media, generally two kinds of materials are used.

1. Copper
   - Coaxial cable
   - Twisted pair
2. Optical Fiber

Coaxial cable

Coaxial cable consists of an inner conductor and an outer conductor which are separated by an insulator. The inner conductor is usually copper. The outer conductor is covered by a plastic jacket. It is named coaxial because the two conductors are coaxial. Typical diameter of coaxial cable lies between 0.4 inches to 1 inch.

Twisted pair

A twisted pair consists of two insulated copper wires, typically 1mm thick. The wires are twisted together in a helical form, the purpose of twisting is to reduce cross talk interference between several pairs. Twisted pair is much cheaper than coaxial cable but it is susceptible to noise and electromagnetic interference and attenuation is large.

Optical fiber

In optical Fiber light is used to send data. In general terms presence of light is taken as bit-1 and its absence as bit 0. Optical fiber consists of either glass or plastic core which is surrounded by cladding of the same material but of different refractive index. This cladding is surrounded by a plastic jacket which prevents optical fiber from electromagnetic interference and harshly environments. It uses the principle of total internal reflection to transfer data over optical fibers. Optical fiber is much better in bandwidth as compared to copper wire, since there is hardly any attenuation or electromagnetic interference in optical wires. Hence there is

less requirement to improve quality of signal, in long distance transmission. Disadvantage of optical fiber is that end points are fairly expensive.

Communication Links

In a network nodes are connected through links. The communication through links can be classified as

Simplex Communication can take place only in one direction.
Example: TV broadcasting.

Half duplex Communication can take place in one direction at a time. Suppose node A and B are connected then half duplex communication means that at a time data can flow from A to B or from B to A but not simultaneously.
Example: Two persons talking to each other such that when one speaks the other listens and vice versa, walkie-talkies, citizens band radios.

Full duplex Communication can take place simultaneously in both directions.
Example: telephone network.

Links can be further classified as:

Point-to-Point In this communication only two nodes are connected to each other. When a node sends a packet then it can be received only by the node on the other side and none else.

Multi-Point It is a kind of sharing communication in which signal can be received by all nodes. This is also called broadcast.

Digital Data to Digital Signals

A digital signal is sequence of discrete, discontinuous voltage pulses. Each pulse is a signal element. Encoding scheme is an important factor in knowing that how successfully the receiver interprets the incoming signal.

Encoding techniques

Following are several ways to map data bits to signal elements:

Non-return-to-zero (NRZ): NRZ codes share the property that voltage level is constant during a bit interval. High level voltage = bit 1 and low level voltage = bit 0. A problem arises when there is a long sequence of 0's and 1's and the voltage level is maintained at the same value for a long time.

This creates a problem on the receiving end because now, the clock synchronization is lost due to lack of any transitions and hence, it is difficult to determine the exact number of 0's and 1's in this sequence.

The two variations are as follows:

1. *NRZ–Level*: In NRZ–L encoding, the polarity of the signal changes only when the incoming signal changes from a '1' to a '0' or from a '0' to a '1'. NRZ – L method, looks just like the RZ method, except for the first input one data bit. This is because NRZ does not consider the first data bit to be a polarity change, where NRZ–L does.
2. *NRZ–Inverted*: Transition at the beginning of bit interval = bit 1 and no transition at the beginning of bit interval = bit 0 or vice versa. This technique is known as differential encoding.

Digital Data Communication Techniques

For two devices linked by a transmission medium to exchange data, a high degree of co-operation is required. Typically data is transmitted one bit at a time. The timing (rate, duration, spacing) of these bits be same for transmitter and receiver. There are two options for transmission of bits.

Parallel All bits of a byte are transferred simultaneously on separate parallel wires. Synchronization between multiple bits is required which becomes difficult over large distance. Parallel communication gives large bandwidth but expensive, possible only for devices which are close to each other.

Serial Bits transferred serially one after other. Serial communication gives less bandwidth but cheaper, suitable for transmission over long distances.

Manchester encoding

Manchester encoding is used in Ethernet (IEEE 802.3) it is a line code in which bit encoding has at least one transition and consumes the same time.

It ensures frequent line voltage transitions, which are directly proportional to clock rate

It is not dependent on data, so it will not carry any information.

Transmission Techniques

Asynchronous

Small blocks of bits (generally bytes) are sent at a time without any time relation between consecutive bytes. When no transmission occurs a default state is maintained corresponding to bit 1, due to arbitrary delay between consecutive bytes, the time occurrences of the clock pulses at the receiving end need to be synchronized for each byte. This is achieved by providing two extra bits, start and stop.

Start Bit It is prefixed to each byte and equals 0. Thus it ensures a transition from 1 to 0 at onset of transmission of byte. The leading edge of start bit is used as a reference for generating clock pulses at required sampling instants. Thus each onset of a byte results in resynchronization of receiver clock.

Stop Bit To ensure that transition from 1 to 0 is always present at beginning of a byte it is necessary that default state be 1, but there may be two bytes one immediately following the other and if last bit of first byte is 0, transition from 1 to 0 will not occur. Therefore a stop bit is suffixed to each byte equaling 1. It's duration is usually 1, 1.5, 2 bits. Asynchronous transmission is simple and cheap but requires an overhead of 3 bits i.e., for 7 bit code 2(start, stop bits) + 1 parity bit implying 30% overhead. However this percentage can be reduced by sending larger blocks of data but then timing errors between receiver and sender cannot be tolerated beyond [50/number. of bits in block]%. It will not only result in incorrect sampling but also misaligned bit count. i.e., a data bit can be mistaken for stop bit if receiver's clock is faster.

Synchronous

Larger blocks of bits are successfully transmitted. Blocks of data are either treated as sequence of bits or bytes. To prevent timing, drift clocks at two ends need to be synchronized. This can be done in two ways.

1. Provide a separate clock line between receiver and transmitter. (or)
2. Clocking information is embedded in data signal i.e., Biphase coding for digital signals.

Still another level of synchronization is required so that receiver determines beginning or end of block of data. Hence each block begins with a start code and end with a stop code. These are in general same, known as flag that is unique sequence of fixed number of bits. In addition some control characters encompass data within these flags. Data and control information is called a frame. Since any arbitrary bit pattern can be transmitted, there is no assurance that bit pattern for flag will not appear inside the frame, thus destroying frame stuffing.

Channel Allocation A large class of networks is built on broadcast channels, a number of stations will share the same channel, if one station sends, all other stations have to hear it.

Problem occurs when, 2 stations want to start data transmission at the same time, in this situation 2 fames collide.

To avoid frame collision, allocate the channel to one of the stations.

There are 3-strategies for channel allocation:

1. Let a station try to use the channel, and when the collision occurs, that is taken care of later.
2. Each station in turn is allowed to use the channel. This is applied in token-based systems. Only the station that has the token can use the channel.
3. Reserve the channel in prior, It is used in slotted systems. The problem is how to make a reservation.

Data Link Layer

Data link layer provides interface to the network layer, determines the number of bits of the physical layer to be grouped into frames, detects transmission error and regulates the flow of frames.

Functions of data link layer:

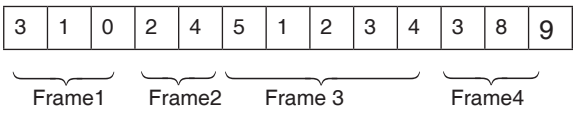
1. Framing
2. Physical addressing
3. Flow control
4. Error control
5. Access control

Various methods of Framing are

1. Time gaps
2. Character count
3. Starting and ending characters, with character stuffing
4. Starting and ending flags, with bit stuffing
5. Physical layer coding violations

Time gaps Framing is done by inserting time gaps between frames, very similar to the way of spacing between words in ordinary text. It is risky to count on timing to mark the start and end of each frame.

Character count It uses a field in the header to specify the number of characters in the frame. Thus at the destination by seeing the character count it knows how many characters follows and where the end of the frame exists.



Problem If count of any frame changes, destination will get out of synchronization and is unable to locate start of next frame.

Starting and ending characters, with character stuffing Each frame starts with the ASCII character sequence DLESTX and ends with the sequence DLEETX. If destination looses track of the frame boundaries, all it has to do is to look for DLESTX or DLEETX character

Starting and ending flags, with bit stuffing

Bit Stuffing: Suppose ou r flag bits are 01111110. So the transmitter will always insert an extra 0 bit after each occurrence of five 1s (except for flags). After detecting a starting flag the receiver monitors the bit stream. If pattern of five 1's appear, the sixth bit is examined and if it is 0 it is deleted; else if it is 1 and next bit is 0 the combination is accepted as a flag. Similarly byte stuffing is used for byte oriented transmition. Here we use an escape sequence to prefix a byte similar to flag and two escape sequences if byte itself is an escape sequence.

Has arbitrary number of bits and allows character codes with an arbitrary number of bits per character. Every frame begins and ends with a special bit pattern, 01111110, called a flag byte.

As soon as the sender's data link layer encounters five consecutive one's in the data, it stuffs a 0 bit into the outgoing bit stream.

Receiver de-shifts the 0 bit of the five consecutive incoming 1 bits, followed by a 0 bit.

If the user data is 01111110, transmitted as 011111010 but stored at receiver as 01111110.

Physical layer coding violations Applied to the networks in which the encoding on the physical medium contains some redundancy.

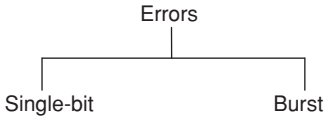
1 → high – low pair

0 → low – high pair

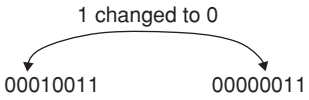
Here high-high, low-low not used for data.

Every data bit has a transition in the middle, thus easy for the receiver to locate the bit boundaries.

Types of Errors



Single bit error The term single bit error means that only one bit in the data unit has changed, it can either be from 1 to 0 or from 0 to 1.



Single bit error correction

A single bit error occurs when a bit changes in value from 0 to 1 (or) from 1 to 0 while storing (or) while performing read (or) write operation. If that error bit is identified, that can be corrected by complementing.

Hamming codes

In hamming codes, K parity bits are added to an n-bit data word, that forms a new word of $(n + k)$ bits. The bit positions are numbered in sequence from 1 to $n + k$. These positions numbered with powers of 2 are reserved for the parity bits; the remaining bits are the data bits.

Example: Consider the given 8-bit data word 11000100, we include four party bits with this word and arrange the bits as follows.

Bit position

1	2	3	4	5	6	7	8	9	10	11	12
$P1$	$P2$	1	$P4$	1	0	0	$P8$	0	1	0	0

The parity bits are in positions, 1, 2, 4, 8. Each parity bit is calculated as

$P1$ = XOR of bits (3, 5, 7, 9, 11) = $1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 = 0$

$P2$ = XOR of bits (3, 6, 7, 10, 11) = 0

$P4$ = XOR of bits (5, 6, 7, 12) = 1

$P8$ = XOR of bits (9, 10, 11, 12) = 1

⇒ If there is odd number of 1s, XOR gives 0

⇒ If there is even number of 1s, XOR gives 1

The values $P1 = 0$, $P2 = 0$, $P4 = 1$, $P8 = 1$ are substituted in 12-bit composed word

Bit position

1	2	3	4	5	6	7	8	9	10	11	12
0	0	1	1	1	0	0	1	0	1	0	0

Check for errors:

$C1$ = XOR of bits (1, 3, 5, 7, 9, 11)

$C2$ = XOR of bits (2, 3, 6, 7, 10, 11)

$C4$ = XOR of bits (4, 5, 6, 7, 12)

$C8$ = XOR of bits (8, 9, 10, 11, 12)

Since the bits were written with even parity, the result $C = C8\ C4\ C2\ C1 = 0000$

∴ Indicates that no error has occurred.

- The code can be used with words of any length.

Burst Error The term burst means that two or more bits in the data unit have changed, either changed, from 1 to 0 or changed from 0 to 1.

Sent:

010011010000-sent bits corrupted by burst error

010001111000 Received

Parity bit

Parity bit is an error detecting code. This bit is added to data words depending on number of 1's in the data word; It could be even parity and odd parity.

n-bit data word is transformed to $(n + 1)$ bit code word with the addition of a bit. Even parity makes even number of 1's in a code word, similarly odd parity makes odd number of 1's in a code word.

Let us illustrate with example

Data word – 1 0 1 1 Parity bit

Code word – 1 0 1 1 1 parity bit (even parity)

Code word: 1 0 1 1 0 (odd parity)

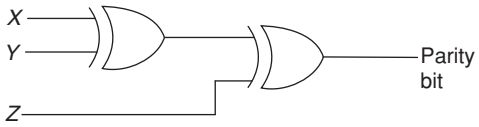
At the receiver side, when the code is received, the receiver checks the same as it is done by the generator. But here it adds all the bits which results in syndrome. If the syndrome is 0 then the number of 1's in code word is even, else number of 1's is odd.

Decision logic analyzer will decide, whether the code word is correct or not, based on syndrome value.

Parity bit generator

The parity bit generator for a 3-bit data word is given below.

The message is in the form of $X\,Y\,Z$



Parity bit generator

When the message is passed through the above circuit, the parity will be generated accordingly.

Error correction code

When data is transmitted form the source to destination, there is a chance of error introduction into the data. Error detection will detect the errors in data, while error correction will rebuild the original data,

Error correction code can be implemented in 2 ways

1. Forward error correction (FEC)
2. Automatic repeat request (ARQ)

In FEC, when sender is sending data, sender adds redundant data (encoded information) to the original data. At the receiver side this redundant data is used to recover the original data, when original data is tampered [error data].

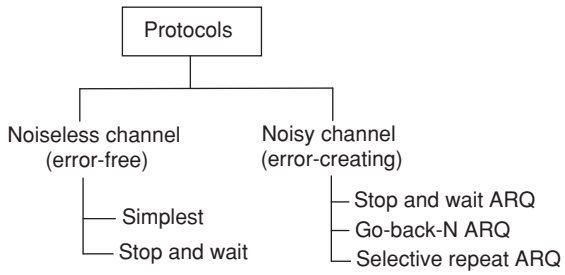
In ARQ, the receiver requests for the retransmission of the data packets, which are corrupted. Receiver will check the data using some error detection code.

Flow Control

It regulates the flow of frames so that slow receivers are not affected by the fast sender or vice versa.

It tell the sender how much data it should transmit before it waits for an acknowledgement from the receiver. Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgement.

Error control in the data link layer is often implemented simply. Any time an error is detected in an exchange, specified frames are retransmitted. This process is called automatic repeat request (ARQ).



All the protocols we discuss as unidirectional in the sense that data frames travels from sender to receiver. Although special frames called acknowledgment (ACK) and negative acknowledgment (NAK) can flow in the opposite direction for flow and error control purposes, data flow is in only one direction. In real life network, the data link protocols are implemented as bidirectional, data flow in both directions. In these protocols flow and error control information such as ACKs and NAKs are included in the data frames in a technique called piggybacking.

Stop and wait Sender sends one frame, stops until it receives confirmation from the receiver. Error correction in stop and wait ARQ is done by keeping a copy of the sent frame and retransmitting the frame when the timer expires.

Only 2 sequence numbers 0 and 1 are used.

Window size is 1.

No ACK for lost or damaged frames.

$$\text{Throughput} = \frac{\text{One packet}}{RTT}$$

$$\text{Utilization} = \frac{L}{L + BR}$$

L = packet length

B = Bandwidth

R = RTT

If $L < BR$, Efficiency > 50

$L > BR$, Efficiency = 50

$$\mu = \frac{1}{1+2a},\quad a = \frac{\text{propagation time}}{\text{Transmission time}}$$

Link utilization is low in stop and wait.

GBN protocol We can send several frames before receiving acknowledgements; we keep a copy of these frames with the acknowledgment.

- Sequence numbers ranges from $2^m - 1$.
- m – number of bits for sequence numbers.
- The sender window slides one or more slots when a valid acknowledgment arrives.
- It uses cumulative acknowledgement or piggy backing wherever possible to acknowledge the frames.
- It discards duplicate and out of order packets.
- Receiving window size is 1.
- If the sender receives a NAK, it resends all frames in the sender window.

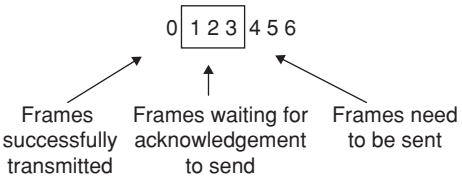
If a single packet is lost, damaged or acknowledgement is lost, it will resend all the packets.

$$\text{Link efficiency} = \frac{1-p}{1-p+p^w}$$

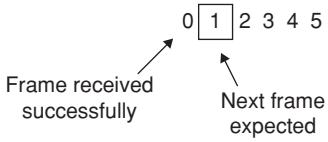
Where, p is the packet loss probability

w is the sender's window size.

Sender:



Receiver:



- If N is maximum sequence number, then sender window size = N, Receiver window size = 1.
- If N is the number of sequence number, sender window size = $N-1$, Receiver window size = 1.

Selective repeat More efficient for noisy links but processing at the receiver is more complex. Receiver window size is same as of sender window size. Sender window maximum size is 2^{m-1}, receiver window maximum size is 2^{m-1}. Sender and receiver window must be at most one half of 2^m.

Receives out of order packets because receiver's window size is greater than 1.

It uses cumulative or independent or piggyback ACK whenever possible. If sender receives a NAK, it resends just the frame specified by the NAK.

If N is maximum sequence number,

$$\text{Sender window size} = \frac{N+1}{2},$$

$$\text{Receiver window size} = \frac{N+1}{2}$$

If N is the number of sequence numbers, sender window size $= \frac{N}{2}$, Receiver window size $= \frac{N}{2}$.

Medium Access Control Sublayer

Multiplexing

When two communicating nodes are connected through a media, it generally happens that bandwidth of media is several times greater than that of the communicating nodes. Transferring of a single signal at a time is both slow and expensive. The whole capacity of the link is not utilized in this case. This link can be further exploited by sending several signals combined into one. This combining of signals into one is called multiplexing.

Frequency Division Multiplexing (FDM)

This is possible in the case where transmission media has a bandwidth higher than the required bandwidth of signals to be transmitted. A number of signals can be transmitted at the same time. Each source is allotted a frequency range in which it can transfer it's signals, and a suitable frequency gap is given between two adjacent signals to avoid overlapping. This type of multiplexing is commonly seen in the cable TV networks.

Time Division Multiplexing (TDM)

This is possible when data transmission rate of the media is much higher than that of the data rate of the source. Multiple signals can be transmitted if each signal is allowed to be transmitted for a definite amount of time. These time slots are so small that all transmissions appear to be in parallel.

Synchronous TDM Time slots are pre. Assigned and are fixed. Each source is given it's time slot at every turn due to it. This turn may be once per cycle or several turns per cycle, if it has a high data transfer rate, or may be once in a number of cycles if it is slow. This slot is given even if the source is not ready with data. So this slot is transmitted empty.

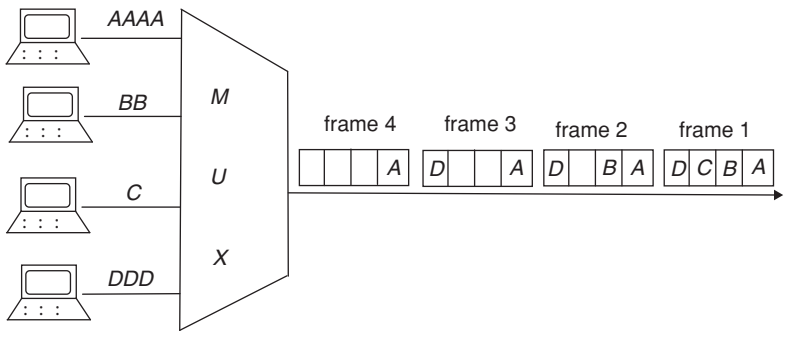


Figure 5 Synchronous TDM: Multiplexing process

Asynchronous TDM In this method, slots are not fixed. They are allotted dynamically depending on speed of sources and whether they are ready for transmission.

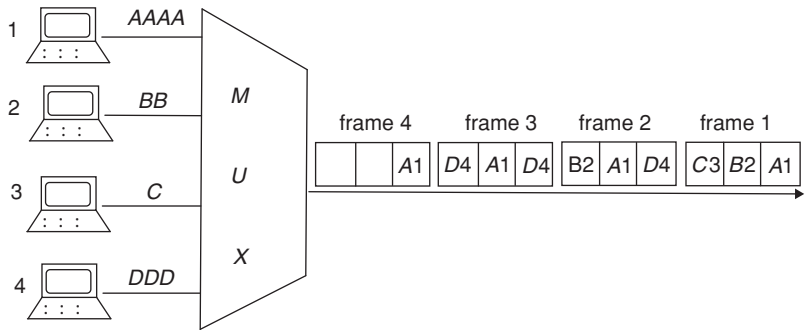


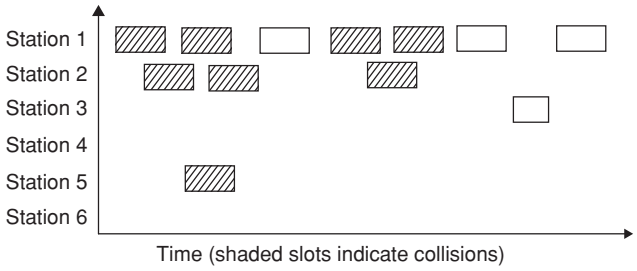
Figure 6 Asynchronous TDM

Aloha Protocols

The Aloha Protocol was designed to provide data transmission between computers on several islands using radio transmission.

Pure aloha

Pure Aloha is an unslotted, fully decentralized protocol. It is extremely simple and trivial to implement. The ground rule is 'when you want to talk, just talk!' So, a node which wants to transmit, will go ahead and sends the packet on its broadcast channel, with no consideration of who so ever to any body else is transmitting (or) (not).

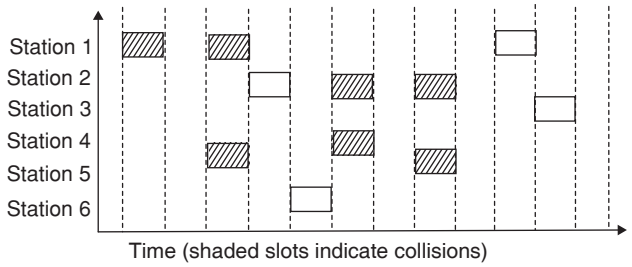


One serious drawback here is that, you don't know whether what you are sending, has been received properly or not. To resolve this in pure Aloha, when one node finishes speaking it expects an acknowledgement in a finite amount of time otherwise it simply retransmits the data. This scheme works well in small networks where the load is not high. But in large, load intensive networks where many nodes may want to transmit at the same time, this scheme fails miserably. This led to the development of slotted Aloha.

Slotted Aloha

This is quite similar to pure Aloha, differing only in the way transmissions take place. Instead of transmitting right at the demand time, the sender waits for some time. This delay is specified as follows–the timeline is divided into equal slots and then it is required that transmission should take place only at slot boundaries. To be more precise, the slotted Aloha makes the following assumptions.

- All frames consist of exactly *L* bits.
- Time is divided into slots of size L/K seconds. (i.e., a slot equals the time to transmit one frame)
- Nodes start to transmit frames only at the beginning of slots.
- The nodes are synchronized so that each node knows when the slots begin.
- If two or more frames collide in a slot, then all the nodes detect the collision event before slot ends.



In this, way the number of collisions that can possibly take place is reduced by a huge margin. And hence, the performance became much better compared to pure Aloha. Collisions may only take place with nodes that are ready to speak at the same time.

Virtual private network

Virtual Private Networking (VPN) Internet protocol security (IP sec) is one of the most complete, secure, standards-based protocol developed for transporting data.

A VPN is a shared network, where private data can be accessed only by the intended recipient.

The term VPN is used to describe a secure connection over the Internet.

VPN is also used to describe private networks such as Frame Relay and Asynchronous Transfer Mode (ATM).

The purpose of data security is that the data flowing across the network is protected by encryption technologies.

IP sec-based VPNs use encryption to provide data security, that increases the networks resistance to data tampering.

IP sec-based VPNs can be created over any type of IP Network, including Internet, ATM, Frame Relay, among all only Internet is inexpensive.

Uses of VPN

Intranets Intranets connect an organization's locations. These locations could be head quarters offices, branch offices, Employees home which is located in some Remote area.

This connectivity is used for e-mails, sharing files etc.

The cost of connecting remote home users is very expensive compared to Internet access technologies because of this organizations have moved their networks to the Internet.

Remote access It enables telecommuters and mobile workers to access e-mail and business applications.

A dial-up connection to an organizations modem pool is one method to access remote workers. It is expensive, because of long distance telephone and service costs.

IP sec

IP sec is an Internet Engineering Task Force (IETF) standard suite of protocols that provide data authentication, integrity, and confidentiality between 2 communication points across IP-Network.

It provides data security at the IP-packet level.

IP sec protects against possible security exposures by protecting data while in transit.

Features

IP sec was designed to provide the following security features when transferring packets across networks.

1. Authentication: Verifies that the packet received is actually from the correct sender or not.
2. Integrity: Ensures that the contents of packet did not change while transmitting data.
3. Confidentiality: Conceals the message content through encryption.

Components of IP sec

ESP: (Encapsulating security payload), It provides confidentiality, authentication and integrity.

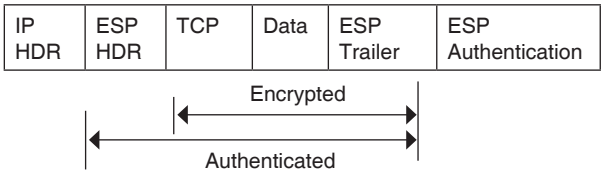
AH: (Authentication Header) provides Authentication and Integrity.

IKE: (Internet key Exchange) provides key management and security Association (SA) management.

ESP:

- Most importantly, it provides message content protection.
- IP sec provides an open frame work for implementing standard algorithms such as SHA and MD5.
- The algorithms IP sec uses produces a unique identifier for each packet, which is a data equivalent to a finger print.
- This Finger Print allows the device to determine whether a packet has been tampered with.
- Packets that are not authenticated are discarded and not delivered to the intended receiver
- ESP also provides all encryption services in IP sec.
- Encryption/decryption allows only the sender and the authorized receiver to read the data.
- The authentication performed by ESP is called ESP authentication.
- ESP provides authentication and integrity for the payload and not for the IP-header

Figure 7 Original packet



The ESP Header is inserted into the packet between the IP-header and any subsequent packet contents.

- ESP encrypts the data, the payload is changed.
- ESP does not encrypt the ESP header, nor does it encrypt the ESP authentication.

AH:

Provides optional anti-replay protection, which protects against unauthorized retransmission of packets.

The authentication header is inserted into the packet between the IP-header and any sub sequent packet contents.

AH does not protect the data's confidentiality.

For added protection in certain cases, AH and ESP can be used together.

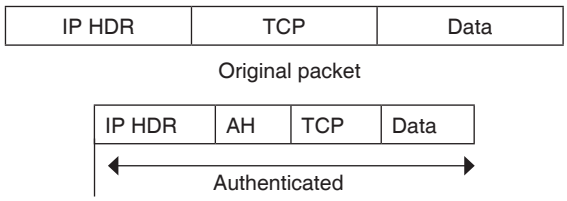


Figure 8 Packet with IP sec Authentication Header.

EXERCISES

Practice Problems I

Directions for questions 1 to 15 Select the correct alternative from the given choices.

1. Assume that, in a stop and wait ARQ system, the bandwidth of the line is 1 mbps, and 1 bit takes 20 ms to make a round trip. What is the bandwidth delay product utilization percentage of the link if we send 1000 bits?

(A) 1% (B) 5%

(C) 10% (D) 50%

2. A channel has a bit rate of 20 kbps and propagation delay of 100 msec. For what size does stop and wait gives an efficiency of 50%?

(A) 2000 bits (B) 3000 bits

(C) 4000 bits (D) 6000 bits

3. CSMA/CD LAN of 1 gbps is to be designed over 1 km cable without repeater. The minimum frame size that Data link layer should consider, if cable support signal speed of 20,000 km/sec

(A) 10 k bits (B) 20 k bits
(C) 30 k bits (D) 40 k bits

4. A 20 mbps satellite link has a propagation delay of 400 μs. The transmitter employs the 'go-back-n ARQ' scheme with n set to 10. Assuming each frame is 100 bytes long. What is the maximum data rate possible?
(A) 1 mbps (B) 2 mbps
(C) 5 mbps (D) 10 mbps

5. A satellite channel has capacity of B bits/sec, the frame size is of L bits, and round trip propagation time of R sec, uses stop and wait protocol, what is the channel utilization?
(A) $\frac{L}{L-BR}$ (B) $\frac{L}{L+BR}$
(C) $\frac{L}{B+R}$ (D) $\frac{L}{B-R}$

6. Find efficiency of the ring where data rate of link is 4 mbps, number of stations are 20 separated by 100 meters and bit delay in each station is 2.5 bits. (velocity of propagation = 2×10^8 m/s)
(A) 60 bits (B) 75 bits
(C) 90 bits (D) 120 bits

7. If you are designing sliding window protocol of 1 mbps which has one way delay of 1.25 seconds. Assuming each frame carries 1 kB of data, what is the minimum number of bits you need for the sequence number?
(A) 8 (B) 9
(C) 10 (D) 12

8. What are the sequence numbers of sender and receiver windows in Go-back-n and selective repeat if m-bits are used?
(A) 2^m–1,1, 2^{m-1}, 2^{m-1} (B) 2^m, 1, 2^{m-1}, 2^{m-1}
(C) 2^m, 2, 2^m, 2^m (D) 2^m–1,1, 2^m, 2^m

9. A 100 km long cable runs at 1.536 mbps. The propagation speed in the cable is 2/3 of speed of light. Number of bits fit in the cable would be?
(A) 428 bits (B) 526 bits
(C) 672 bits (D) 768 bits

10. If the bandwidth of the link is 256 mbps, Assume that sequence number field consists 32 bits. Find the wrap around time for sequence numbers?
(A) 128 sec (B) 256 sec
(C) 512 sec (D) 1024 sec

11. After a series of collisions a station has selected slot 984. In how many successive collisions, the station was a part of communication?
(A) 4 (B) 6
(C) 8 (D) 10

12. There are 10 stations in a LAN always having constant load and ready to transmit. During any particular contention slot each station transmits with a probability of 0.1. If the average frame takes 122 ms to transmit, what is the channel efficiency, if round trip time is 51.2 micro secs?
(A) 0.23 (B) 0.35
(C) 0.48 (D) 0.56

13. Which of the below are issues concerning data link layer?
(i) Ensures that the transmission facility is free of undetected transmission errors
(ii) Regulates the transmission rates so as to match the receiver's capabilities
(iii) Ensures the design of the line such that when a '1' bit is sent it is always received as '1' bit at receivers end.
(A) (i), (ii) (B) (ii), (iii)
(C) (iii), (i) (D) (i), (ii), (iii)

14. An Ethernet LAN has the capability of 100 Mbps. If Manchester encoding is used, what is the rate of signal change?
(A) 20 million times/sec
(B) 200 million times/sec
(C) 50 million times/sec
(D) 500 million times/sec

15. For 10 Mbps LAN it is found that 64 bytes is the minimum frame size to aid in collision detection. What should be the minimum frame size for a 100 Mbps LAN?
(A) 6.4 bytes (B) 64 bytes
(C) 640 bytes (D) 6400 bytes

Practice Problems 2

Directions for questions 1 to 15 Select the correct alternative from the given choices.

1. What is the probability of success for any arbitrary station among 'N' stations to transmit in CSMA/CD?
(A) $Np_s(1-p_s)^N$ (B) $(N-1)p_s\ (1-p_s)$
(C) $Np_s(1-p_s)^{N-1}$ (D) $Np_s(1-p_s)^N$

2. If 4-bits are used to represent sequence numbers for flow control. What are sender and receiver window sizes in Go-back-n and selective repeat?
(A) 16, 1, 8, 8 (B) 15, 1, 8, 8
(C) 15, 2, 8, 8 (D) 15, 1, 16, 8

3. If the available maximum sequence number is 13, compute sender and receiver window sizes in go-back-n and selective repeat?
(A) 4, 1, 4, 4 (B) 4, 1, 7, 7
(C) 13, 1, 7, 7 (D) 13, 1, 4, 4

4. In a gigabit ethernet LAN, the receiver couldn't empty the input buffer on some line for 1 millisecond. What is the maximum accumulation of frames possible neglecting propagation delays?

(A) 1024 frames (B) 2097 frames
(C) 4096 frames (D) 5120 frames

5. A Token ring LAN is using differential Manchester encoding. If the LAN speed is 10 Mbps. What is the baud rate?
(A) 10 M baud (B) 20 M baud
(C) 5 M baud (D) 100 M baud

6. Consider a 100-meter 10 mbps token ring containing 10 stations, each transmitting with equal priority. Each station can transmit 4 bytes before giving up the token. Token holding time per station is 10 ns. Also propagation speed is 200 m/s. Assume that the Ring monitor has created a new token, how long does it take for the token to come back to the Ring monitor if no station uses the token?
(A) 2.55 μsec (B) 3.64 μsec
(C) 4.65 μsec (D) 2.93 μsec

7. In the above question, if only 6 nodes including Ring monitor are active what is total propagation delay in μsec?
(A) 3.60 (B) 3.61
(C) 3.62 (D) 3.63

8. In the above case if bit regeneration time is 1 ns/bit. What is the regeneration overhead caused if a 4 kB token is taken by 1st node and if it uses to transmit 4B data to ring monitor.
(A) 412 ns (B) 544 ns
(C) 640 ns (D) 800 ns

9. Which of the below operation is applied to full-duplex mode operation of gigabit Ethernet?
(i) Traffic is allowed in both directions at any time.
(ii) CSMA/CD protocol is used.
(iii) Maximum length of cable segment used to connect stations is limited by CSMA/CD protocol.
(A) (i) and (ii) (B) (ii), (iii)
(C) (iii), (i) (D) (i), (ii), (iii)

10. Which of the below are not applied to Token Ring networks?
(i) Collisions
(ii) Limits on length of the cable segment
(iii) Time slots for transmission
(iv) Usage of repeaters
(A) (i), (ii) (B) (ii), (iii)
(C) (iii), (iv) (D) (i), (iv)

11. Select the correct statements from below (pertaining to Ethernet):
(i) Frame collisions don't occur at a repeater
(ii) Frame collisions can occur at the hub itself
(iii) Switch frames are never lost due to collisions
(iv) Entire bridge is a point of collisions
(A) (i), (ii), (iii) (B) (ii), (iii), (iv)
(C) (i), (iii), (iv) (D) (i), (ii), (iv)

12. Match the different layers with possible security methods in those layers.

(p) Data link layer	(i) user authentication
(q) Network layer	(ii) use firewalls
(r) Transport layer	(iii) encryption of connections
(s) Application layer	(iv) point to point encryption of data stream

(A) p – i, q – ii, r – iii, s – iv
(B) p – ii, q – iv, r – iii, s – i
(C) p – iv, q – ii, r – iii, s – i
(D) p – iii, q – iv, r – ii, s – i

13. The hamming distance between 001111 and 010011 is
(A) 1 (B) 2
(C) 3 (D) 4

14. Which of the following represents the polynomial $x^5 + x^4 + x^0$ using the CRC?
(A) 110000 (B) 110001
(C) 110010 (D) 110101

15. For a sliding window of size n–1 (n sequence number) there can be maximum of how many frames sent but unacknowledged?
(A) 0 (B) $n - 1$
(C) n (D) $n + 1$

Previous Years' Questions

1. The message 11001001 is to be transmitted using the CRC polynomial $x^3 + 1$ to protect it from errors. The message that should be transmitted is: **[2007]**
(A) 11001001000 (B) 11001001011
(C) 11001010 (D) 110010010011

2. The distance between two stations M and N is L kilometers. All frames are K bits long. The propagation delay per kilometer is t seconds. Let R bits/second be the channel capacity. Assuming that processing delay is negligible, the minimum number of bits for the sequence number field in a frame for maximum utilization, when the sliding window protocol is used, is: **[2007]**

(A) $\left\lceil \log_2 \frac{2LtR + 2\,k}{k} \right\rceil$ (B) $\left\lceil \log_2 \frac{2LtR}{k} \right\rceil$

(C) $\left\lceil \log_2 \frac{2LtR + k}{k} \right\rceil$ (D) $\left\lceil \log_2 \frac{2LtR + k}{2\,k} \right\rceil$

3. Match the following:
(P) SMTP (1) Application layer
(Q) BGP (2) Transport layer

(R) TCP (3) Data link layer
(S) PPP (4) Network layer
(5) Physical layer

[2007]

(A) *P*–2 *Q*–1 *R*–3 *S*–5
(B) *P*–1 *Q*–4 *R*–2 *S*–3
(C) *P*–1 *Q*–4 *R*–2 *S*–5
(D) *P*–2 *Q*–4 *R*–1 *S*–3

4. A layer-4 firewall (a device that can look at all protocol headers up to the transport layer) CANNOT **[2011]**

(A) Block entire HTTP traffic during 9.00PM and 5.00PM
(B) Block all ICMP traffic
(C) Stop incoming traffic from a specific IP address but allow outgoing traffic to the same IP address
(D) Block TCP traffic from a specific user on a multi-user system during 9.00PM and 5.00AM.

5. If two fair coins are flipped and at least one of the outcomes is known to be a head, what is the probability that both outcomes are heads? **[2011]**

(A) 1/3 (B) 1/4
(C) 1/2 (D) 2/3

6. Which of the following transport layer protocols is used to support electronic mail? **[2012]**

(A) SMTP (B) IP
(C) TCP (D) UDP

7. Consider a source computer (S) transmitting a file of size 10^6 bits to a destination computer (D) over a network of two routers (R_1 and R_2) and three links (L_1, L_2 and L_3). L_1 connects S to R_1; L_2 connects R_1 to R_2; and L_3 connects R_2 to D. Let each link be of length 100 km. Assume signals travel over each link at a speed of 10^8 meters per second. Assume that the link bandwidth on each link is 1 Mbps. Let the file be broken down into 1000 packets each of size 1000 bits. Find the total sum of transmission and propagation delays in transmitting the file from S to D? **[2012]**

(A) 1005 ms (B) 1010 ms
(C) 3000 ms (D) 3003 ms

8. Determine the maximum length of the cable (in km) for transmitting data at a rate of 500 Mbps in an Ethernet LAN with frames of size 10,000 bits. Assume the signal speed in the cable to be 2,00,000 km/s. **[2013]**

(A) 1 (B) 2
(C) 2.5 (D) 5

9. Consider a token ring network with a length of 2 km having 10 stations including a monitoring station. The propagation speed of the signal is 2×10^8 m/s and the token transmission time is ignored. If each station is allowed to hold the token for 2 μsec, the minimum time for which the monitoring station should wait (in μsec) before assuming that the token is lost is _____ **[2014]**

10. Consider the store and forward packet switched network given below. Assume that the bandwidth of each link is 10^6 bytes/sec. A user on host A sends a file of size 10^3 bytes to host B through routers R_1 and R_2 in three different ways. In the first case a single packet containing the complete file is transmitted from A to B. In the second case, the file is spilt into 10 equal parts, and these packets are transmitted from A to B. In the third case, the file is spilt into 20 equal parts, and these packets are sent from A to B. Each packet contains 100 bytes of header information along with the user data. Consider only transmission time and ignore processing, queuing and propagation delays. Also assume that there are no errors during transmissions. Let T_1, T_2 and T_3 be the times taken to transmit the file in the first, second and third case respectively. Which one of the following is CORRECT? **[2014]**

(A) $T_1 < T_2 < T_3$
(B) $T_1 > T_2 > T_3$
(C) $T_2 = T_3$, $T_3 < T_1$
(D) $T_1 = T_3$, $T_3 > T_2$

11. In the following pairs of OSI protocol layer/ sub-layer and its functionality the INCORRECT pair is **[2014]**

(A) Network layer and Routing
(B) Data Link Layer and Bit synchornization
(C) Transport layer and End-to-end process communication
(D) Medium Access Control sub-layer and Channel sharing

12. A bit-stuffing based framing protocol uses an 8-bit delimiter pattern of 01111110. If the output bit-string after stuffing is 01111100101, then the input bit-string is **[2014]**

(A) 0111110100 (B) 0111110101
(C) 0111111101 (D) 011111111

13. Suppose that the stop-and-wait protocol is used on a link with a bit rate of 64 kilobits per second and 20 milliseconds propagation delay. Assume that the transmission time for the acknowledgement and the processing time at nodes are negligible. Then the minimum frame size in bytes to achieve a link utilization of at least 50% is _____ **[2015]**

14. A link has a transmission speed of 10^6 bits/sec. It uses data packets of size 1000 bytes each. Assume that the acknowledgement has negligible transmission delay, and that is propagation delay is the same as the data propagation delay. Also assume that the processing delays at nodes are negligible. The efficiency of the stop-and-wait protocol in this setup is exactly 25%. The value of the one-way propagation delay (in milliseconds) is _____ **[2015]**

15. Consider a CSMA/CD network that transmits data at a rate of 100 Mbps (10^8-bits per second) over a 1 km (kilometer) cable with no repeaters. If the minimum frame size required for this network is 1250 bytes, what is the signal speed (km/sec) in the cable? **[2015]**

(A) 8000 (B) 10000
(C) 16000 (D) 20000

16. Consider a LAN with four nodes S_1, S_2, S_3 and S_4. Time is divided into fixed-size slots, and a node can begin its transmission only at the beginning of a slot. A collision is said to have occurred if more than one node transmit in the same slot. The probabilities of generation of a frame in a time slot by S_1, S_2, S_3 and S_4 are 0.1, 0.2, 0.3 and 0.4, respectively. The probability of sending a frame in the first slot without any collision by any of these four stations is _____ **[2015]**

17. Consider a network connecting two systems located 8000 kilometers apart. The bandwidth of the network is 500×10^6-bits per second. The propagation speed of the media is 4×10^6 meters per second. It is needed to design a Go-Back-N sliding window protocol for this network. The average packet size is 10^7-bits. The network is to be used to its full capacity. Assume that processing delays at nodes are negligible. Then, the minimum size in bits of the sequence number field has to be _____ **[2015]**

18. Two hosts are connected via a packet switch with 10^7 bits per second links. Each link has a propagation delay of 20 microseconds. The switch begins forwarding a packet 35 microseconds after it receives the same. If 10000-bits of data are to be transmitted between the two hosts using a packet size of 5000-bits, the time elapsed between the transmission of the first bit of data and the reception of the last bit of the data in microseconds is _____ **[2015]**

19. A sender uses the Stop-and-Wait ARQ protocol for reliable transmission of frames. Frames are of size 1000 bytes and the transmission rate at the sender is 80 Kbps (1 Kbps = 1000 bits/second). Size of an acknowledgement is 100 bytes and the transmission rate at the receiver is 8 Kbps. The one-way propagation delay is 100 milliseconds. Assuming no frame is lost, the sender throughput is _____ bytes/second. **[2016]**

20. In an Ethernet local area network, which one of the following statements is **TRUE**? **[2016]**

(A) A station stops to sense the channel once it starts transmitting a frame.
(B) The purpose of the jamming signal is to pad the frames that are smaller than the minimum frame size.
(C) A station continues to transmit the packet even after the collision is detected
(D) The exponential back off mechanism reduces the probability of collision on retransmissions.

21. Consider a 128×10^3 bits/second satellite communication link with one way propagation delay of 150 milliseconds. Selective retransmission (repeat) protocol is used on this link to send data with a frame size of 1 kilobyte. Neglect the transmission time of acknowledgement. The minimum number of bits required for the sequence number field to achieve 100% utilization is _____. **[2016]**

22. A computer network uses polynomials over $GF(2)$ for error checking with 8 bits as information bits and uses $x^3 + x + 1$ as the generator polynomial to generate the check bits. In this network, the message 01011011 is transmitted as **[2017]**

(A) 01011011010 (B) 01011011011
(C) 01011011101 (D) 01011011100

23. The values of parameters for the Stop-and Wait ARQ protocol are as given below:

Bit rate of the transmission channel = 1Mbps.

Propagation delay from sender to receiver = 0.75 ms.

Time to process a frame = 0.25 ms.

Number of bytes in the information frame = 1980.

Number of bytes in the acknowledge frame = 20.

Number of overhead bytes in the information frame = 20.

Assume that there are no transmission errors. Then, the transmission efficiency (expressed in percentage) of the stop-and-wait ARQ protocol for the above parameters is _____ (correct to 2 decimal places) **[2017]**

24. Consider a binary code that consists of only four valid codewords as given below:

00000,01011,10101,11110

Let the minimum Hamming distance of the code be p and the maximum number of erroneous bits that can be corrected by the code be q. Then the values of p and q are **[2017]**

(A) p=3 and q=l
(B) p=3 and q=2
(C) p=4 and q=1
(D) p=4 and q=2

25. Consider two hosts X and Y connected by a single direct link of rate 10^6 bits/sec. The distance between the two hosts is 10.000 km and the propagation speed along the link is 2×10^8 m/sec. Host X sends a file of 50,000 bytes as one large message to host Y continuously. Let the transmission and propagation delays be p milliseconds and q milliseconds, respectively. Then the values of p and q are **[2017]**

(A) p=50 and q=100
(B) p=*50* and q=*400*

(C) p=100 and q=50
(D) p=400 and q=50

26. Consider a simple communication system where multiple nodes are connected by a shared broadcast medium (like Ethernet or wireless). The nodes in the system use the following carrier-sense based medium access protocol. A node that receives a packet to transmit will carrier-sense the medium for 5 units of time. If the node does not detect any other transmission in this duration, it starts transmitting its packet in the next time unit. If the node detects another transmission, it waits until this other transmission finishes, and then begins to carrier-sense for 5 time units again. Once they start to transmit, nodes do not perform any collision detection and continue transmission even if a collision occurs. All transmissions last for 20 units of time. Assume that the transmission signal travels at the speed of 10 meters per unit time in the medium.

Assume that the system has two nodes P and Q, located at a distance d meters from each other. P starts transmitting a packet at time $t = 0$ after successfully completing its carrier-sense phase. Node Q has a packet to transmit at time $t = 0$ and begins to carrier-sense medium.

The maximum distance d (in meters, rounded to the closest integer) that allows Q to successfully avoid a collision between its proposed transmission and P's ongoing transmission is _____. **[2018]**

Answer Keys

Exercises

Practice Problems I

1. B	**2.** C	**3.** A	**4.** D	**5.** B	**6.** C	**7.** B	**8.** A	**9.** D	**10.** A
11. D	**12.** C	**13.** A	**14.** B	**15.** C					

Practice Problems I

1. C	**2.** B	**3.** C	**4.** B	**5.** B	**6.** B	**7.** A	**8.** B	**9.** D	**10.** B
11. A	**12.** D	**13.** C	**14.** B	**15.** B					

Previous Years' Questions

1. B	**2.** C	**3.** B	**4.** A	**5.** A	**6.** C	**7.** A	**8.** B	**9.** 28 to 30
10. D	**11.** B	**12.** B	**13.** 160	**14.** 12	**15.** D	**16.** 0.40 to 0.46		**17.** 8
18. 1575	**19.** 2500	**20.** D	**21.** 4	**22.** C	**23.** 87.3	**24.** A	**25.** D	**26.** 50

Chapter 2

Routing Algorithms

LEARNING OBJECTIVES

- *Routing algorithm basics*
- *Flooding*
- *Multipath routing*
- *Distance vector routing*
- *Link state routing*
- *Hierarchical routing*
- *Rip*
- *Ospf*
- *Congestion control techniques*
- *Traffic shaping*

Routing Algorithms Basics

The main function of network layer is routing packets from the source machine to the destination machine. The routing algorithms are part of the network layer software, responsible for deciding which output line an incoming packet should be transmitted on.

Routing algorithms can be grouped into two major classes: Non-adaptive and Adaptive.

1. Non-adaptive algorithms do not base their routing decisions on measurements or estimates of the current traffic and topology. Instead, the choice of the route to use is downloaded to the routers when the network is booted. This procedure is called static routing.
2. Adaptive algorithms, in contrast, change their routing decisions to reflect changes in the topology, and the traffic as well.

Store and Forward Packet Switching

In this Technique, the data packet will be stored at the node and it is forwarded to its next appropriate intermediate node. The next intermediate node will first store the packet in the buffer, based on the router decision, it selects an interface, and forwards to receiver.

The technique is most suitable for the networks with unsteady connectivity.

The length of the packet we take shows effect on the file transfer, if the data packet is small, in the store the forward, delay will be less at each node, but causes extra overhead with headers. So, the packet size selection should be done appropriately.

Flooding

Static algorithms, in which every incoming packet is sent out on every outgoing line except the one on which it is arrived. Header contains the hop count of each packet. Hop counter is decremented at each hop, with the packet being discarded when the counter reaches zero.

Another way for damming the flood is to keep track of which packets have been flooded, to avoid sending them out a second time. A variation of flooding that is slightly more practical is selective flooding. In this algorithm the routers do not send every incoming packet out on every line, only on those lines that are going approximately in the right direction.

Multipath Routing

Multipath routing is routing the packets from the source, on multiple paths to the destination. It is nothing but spreading the traffic.

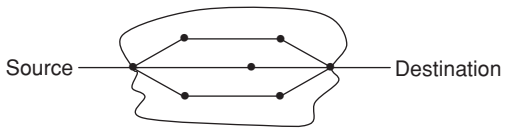


Figure 1 Multipath routing model

Single path routing causes QOS, throughput and delay problems, and multipath routing, improves network performance with sharing of available resources of network.

The components of multipath routing are

1. Multipath calculation algorithm
2. Multipath forwarding algorithm
3. End-Host protocol

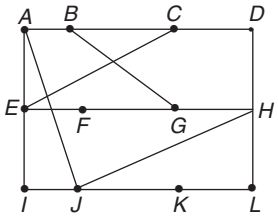
The algorithms specified above are based on Dijkstras shortest path algorithm they generate paths according to path characteristics and ensure path quality and path independence.

The end-host protocol uses the multipath (determined) effectively performance will be improved if end-users use the multiple paths effectively.

Distance Vector Routing

A dynamic routing algorithm, operates by having each router maintain a table (i.e., a vector) giving the best known distance to each destination and which line to use to get there. These tables are updated by exchanging information with the neighbors.

The Metric used might be number of hops, time delay in milliseconds, and total number of packets queued along the path or something similar.



(a)

	New estimated A	I	H	K	Delay from J	
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	-
K	24	22	22	0	6	K
L	29	33	9	9	15	k
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6	New routing table for J Vectors received from J's four neighbours.	

(b)

Figure 2 (a) Subnet, (b) Delay vectors of J

Figure 2(a) 'shows a subnet. The first 4 columns of figure 2(b) shows the delay vectors received from the neighbors of router *J*. A claims to have a 12 m sec delay to *B*, a 25 m sec delay to *C*, a 40 m sec delay to D, etc.

Suppose that *J* has estimated its delay to its neighbour, *A*, *J*, *H* and *K* as 8, 10, 12 and 6 m sec, respectively.

Now *J* computes its new route to router *G*. It knows that it can get to *A* in 8 m sec, and *A* claims to be able to get to *G* in 18 m sec, so *J* knows it can count on a delay of 26 m sec to *G* if it forwards packets bound for *G* to *A*, similarly, it computes the delay to *G* via *I*, *H* and *K* as 41 (31 + 10), 18 (6 + 12) and 37 (31 + 6) m sec, respectively.

The best of these values is 18, so it makes an entry in its routing table that the delay to *G* is 18 m sec and that the route to use is via *H*.

Count to Infinity Problem

It reacts rapidly to good news, but leisurely to bad news. Actual network may be down but routers will exchange routes with one another.

Following measures are taken to avoid count-to-infinity problem:

1. **Hop limit:** Limit number of hops normally 0 hops directly connected, hop 16 is (0–15), 16 hops unreachable.
2. **Split horizon:** Never send information back in direction where it came from.
3. Route poisoning and poison reverse, hold on timer trigger.
4. As soon as network goes down, make metric of root infinity to resolve the immediate instability created because of routing updates from neighbor.
5. When router sends update with infinite metric to neighbor, neighbor will make it down.
6. Now routers will initiate hold on time to learn alternate paths and send update in direction where it came (Poison reverse) from.
7. Routers will incorporate final roots in routing table.

Link State Routing

The idea behind link state routing is simple and can be stated as five parts. Each router must do the following:

1. Discover its neighbors and learn their network addresses.
2. Measure the delay or cost to each of its neighbors.
3. Construct a packet telling all it has just learned.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router.

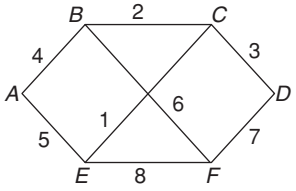
Learning about the neighbors When a router is booted, its first task is to learn who its neighbors are. It accomplishes this goal by sending a special HELLO packet on each point to point line. The router on the other end is expected to send back a reply telling who it is. These names must be globally unique.

Measuring the cost The link state routing algorithm requires each router to know, or at least have a reasonable estimate of, the delay to each of its neighbors.

The most direct way to determine this delay is to send over the line a special ECHO packet that the other side is required to send back immediately.

By measuring the round trip time and dividing it by two, the sending router can get a reasonable estimate of the delay. If two paths with same bandwidth exists and one path is heavily loaded then the path which is not heavily loaded is chosen. But this may oscillate in the choice of best path. So to avoid oscillation in the choice of best path, distribute the load over multiple lines with same known fraction going over each line.

Building link state packets Once the information needed for the exchange has been collected, the next step is, for each router to build a packet containing all the data. The packet starts with identity of the sender, followed by a sequence number and age, and a list of neighbors. For each neighbor, delay to that neighbor is given.



(a)

A	
Seq	
Age	
B	4
E	5

B	
Seq	
Age	
B	4
D	2
E	6

C	
Seq	
Age	
B	2
D	3
E	1

D	
Seq	
Age	
C	3
F	7

E	
Seq	
Age	
A	5
F	8
C	1

F	
Seq	
Age	
B	6
D	7
E	8

(b)

Figure 3 (a) Subnet5, (b) Link state packets for this subnet.

Distributing the link state packets As the packets are distributed and installed, the routers getting the routing packet first will change their routes.

Consequently, the different routers may be using different versions of the topology, which can lead to inconsistencies, loops, unreachable machines, and other problems. The fundamental idea is to use flooding to distribute the link state packets. To keep the flood in check, each packet contains a sequence number that is incremented for each new packet sent. Routers keep track of all the (source router, sequence) pairs they see.

When a new link state packet comes in, it is checked against the list of packets already seen. If it is new, it is forwarded on all lines except the one it arrived on. If it is a duplicate, it is discarded.

If a packet with a sequence number lower than the highest one seen so far ever arrives, it is rejected as being obsolete since the router has more recent data.

If a router ever crashes it will lose track of its sequence number. If its starts again at 0, the next packet will be rejected as a duplicate. Also due to bit error, packets may be rejected as obsolete. Solution to these problems is to include the age of each packet after the sequence number and decrement it once per second.

When the age hits zero, the information from that router is discarded.

Computing new routes Once a router has accumulated a full set of link state packets, it can construct the entire subnet graph because every link is represented. Every link is, in fact, represented twice, once for each direction. The two values can be averaged or used separately. Now dijkstra's algorithm can be run locally to construct the shortest path to all possible destinations.

Hierarchical Routing

Hierarchical Routing is mainly designed for large topologies. With increase in the topology there is proportionate increase in the routing tables, which consume more memory for maintaining tables and requires more bandwidth for the status reports.

In this routing, network topology is divided into hierarchies, these will reduce size of routing table. The node at each hierarchy will know about the nodes present in that level. It forwards the packet to its border router (at its level) if destination is not at its level. Hierarchical routing increases efficiency in routing, less traffic, reduction of table size in an order of about (log n).

RIP

1. It calculates best route based on hop count.
2. RIP cannot handle more than 15 hops, anything above 15 hops away is considered unsearchable by RIP. This fact is used by RIP to prevent routing loops.
3. RIP is a classful routing protocol.
4. Interval between route update advertisements: 30 sec. Time out/hold on times: 180 sec
5. RIP implements the split horizon, route isonning and hold down mechanisms to prevent looping.
6. It is a dynamic distance vector routing protocol.

OSPF

The open shortest path first is an adaptive routing protocol for IP networking. It uses a link state routing algorithm. OSPF keeps track of the state of all the various network connections between itself and a network it is trying to send

data to. OSPF selects the best route by finding the lowest cost paths to a destination. All router interfaces are given a cost. Its domain is an autonomous system.

Backbone routers Backbone routers have one or more interfaces in Area 0 (the backbone area).

Area border router (ABR) Routers that belong to multiple areas, and connect these areas to the backbone area are called ABR. It has interfaces in multiple areas.

Autonomous system boundary router (ASBR) If the router connects the OSPF autonomous system to another autonomous system, it is called an autonomous system boundary router (ASBF).

OSPF elects two or more routers to manage the link state advertisements.

Designated router (DR) Every OSPF will have a DR, a backup DR. The DR is the route to which all other routers within the area, send their link state advertisements.

OSPF areas

OSPF areas are used to impose a hierarchical structure to the flow of data over the network. A network using OSPF will always have atleast one area and if there is more than one area, one of the two areas must be the backbone area. Areas are used to group routers into manageable groups that exchange routing information locally, but summarize the routing information, when advertising the routes externally, ABR's are used to connect the areas.

Congestion Control Techniques

Objective of congestion control technique is to limit queue lengths at the nodes, so as to avoid throughput collapse.

1. Send a control packet from a congested node to some or all source nodes to stop or slow the rate of transmission from source and thus limit the total number. of packets in the network.
2. Allow packet switching nodes to add congestion information to packets as they pass by. The packets carrying such information can go in both the directions i.e., opposite of the congestion and in the same direction of the congestion.

   Packets in the opposite direction of congestion quickly reache the source node which can reduce the flow of packets into the network.

   Packets going in the same direction as the congestion, reaches the destination. The destination asks the source to adjust the load by returning the signal back to the source in the packets.
3. Provides link delay information to other nodes. This information can be used to influence the rate at which new packets are produced. As these delays are influenced by the routing decision, they may vary too rapidly to use effectively for congestion control.

Congestion Control

Congestion control maintains the number of packets within the network below the level at which performance falls dramatically.

Every node has a queue of packets for each outgoing channel. If, rate at which packets arrive and queue up, exceeds the rate of packet transmission, then size of queue grows without bound and thus delay experienced by a packet goes to infinity.

When the packets arrive they are stored in the input buffer, of the corresponding link. The node examines each incoming packet to make a routing decision and then moves the packet to the appropriate output buffer. Packet queued up for output in output buffer is transmitted as soon as possible. When saturation point is reached, one can do any of the following:

1. Discard incoming packet for which there is no available buffer space.
2. Node should exercise some sort of flow control over its neighbors so that the traffic flow remains manageable.
3. Traffic shaping is about regulating the average rate of data transmission.

Leaky Bucket Algorithm

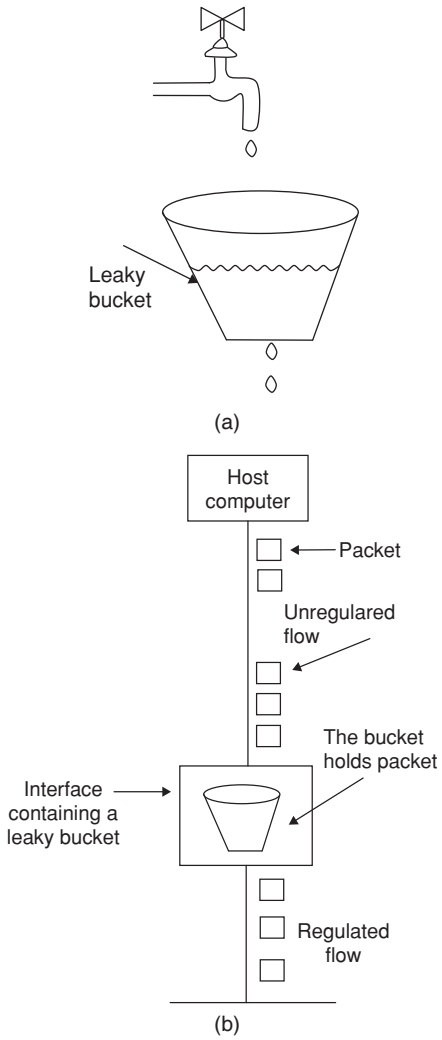
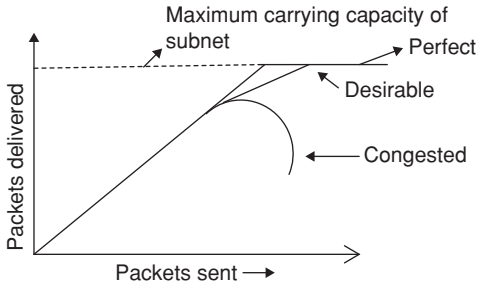


Figure 4 (a) A leaky bucket with water, (b) A leaky bucket with network

A leaky bucket is a bucket with a small hole. No matter at what rate water enters the bucket, the outflow is at constant rate, *S*, when there is any water in the bucket and zero when bucket is empty. Once the bucket is full, any additional water entering it, spills over the sides and it is lost. Each host is connected to the network by an interface containing a leaky bucket (i.e., a finite internal queue) congestion control algorithms.



When too many packets are present in the subnet, performance degrades. This situation is called congestion.

Causes of congestion

1. If all of a sudden, stream of packets are arriving on three or four input lines and all need same output line, a queue will build up.
2. Slow processor.
3. Low bandwidth line.

Token bucket

Tokens are added at a constant rate. For a packet to be transmitted, it must capture and destroy one token.

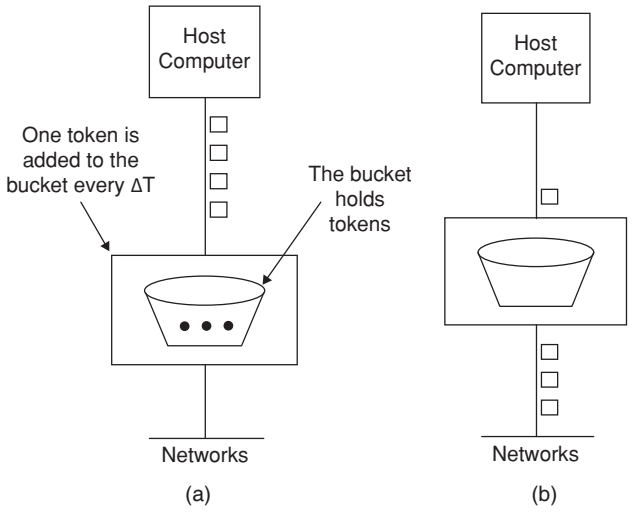


Figure 5 (a) shows that the bucket holds 3 tokens with 4 packets waiting to be transmitted, (b) shows that 3 packets have gotten through but the other one is stuck waiting for tokens to be generated.

Unlike leaky bucket, token bucket allows saving up to maximum size of bucket '*n*'.

The bursts of upto '*n*' packets can be sent at once, giving faster response to sudden bursts.

- Leaky bucket discards packets when the bucket is full, whereas token bucket throws away tokens when the bucket is full but never discards packets.
- Let Token bucket capacity be *c*(bits), token arrival rate ρ(bps), maximum output rate *M*(bps), and burst length *S*(*s*).
- During the burst length of *S*(*s*), tokens generated are ρS(bits), output burst contains a maximum of $C + \rho S$(bits)
- Output in a maximum burst of length *S*(*s*) is MS.
- $C + \rho S = MS \quad (or) \quad S = \frac{C}{M - P}$
- Token bucket still allows large bursts, even though the maximum burst length '*s*' can be regulated by selection of ρ and *M*.
- To reduce the peak rate, put a leaky bucket of a larger rate after the token bucket (To avoid discarding packets)

Traffic Shaping

1. One of the main causes of congestion is, that traffic is often burst.
2. If hosts could be made to transmit at uniform rate, congestion would be less.

This arrangement can be built into the network interface or simulated by the host OS. The host is allowed to put one packet per tick on the network.

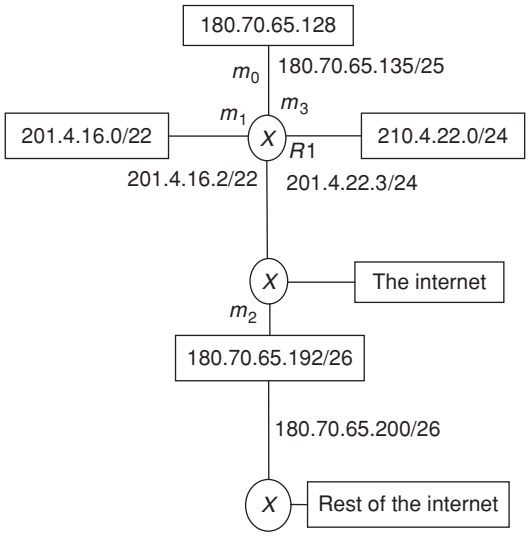
1. When the packets are all of the same size at every clock tick, one packet is transmitted.
2. When variable size packets are used.
   (i) At every tick, a counter is initialized to *n*. If the first packet on the queue has fewer bytes than the current value of the counter, it is transmitted and counter is decremented by that number of bytes.
   (ii) Additional packets may also be sent, as long as the counter is high enough.
   (iii) When the counter drops below the length of the next packet on the queue, transmission stops until the next tick, at that time the residual byte count is overwritten and lost.

EXERCISES

Practice Problems I

Directions for questions 1 to 15: Select the correct alternative from the given choices.

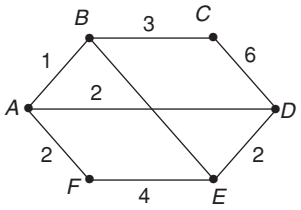
1. Consider below figure:



The network address, 180.70.65.130 goes through which of the following interface?

(A) m_0 (B) m_1
(C) m_2 (D) m_3

2. Consider below graphical representation of a subnet with each node denoting a router. If all the routers are booted at the same time, what is the number of link state packets that are generated having the cost/delay information?

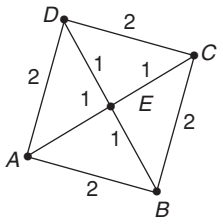


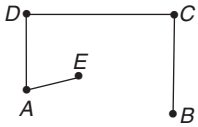
(A) 3 (B) 4
(C) 5 (D) 6

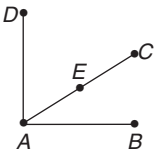
3. In a TCP connection it is found that burst size of 1024, 2048, 4096 have been transmitted while that of 8192 has resulted in a time out. The receiver has earlier set a window size of 4096. As per slow start algorithm which of the below statement is true?

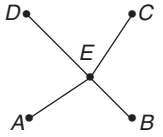
(i) Congestion window is set to 4096.
(ii) Maximum allowed burst size is 8192
(A) (i) only
(B) (ii) only
(C) Both (i) and (ii)
(D) Neither (i) nor (ii)

4. From the below graph select the sink tree(s):



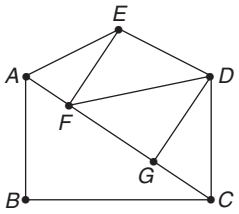
(i) 

(ii) 

(iii) 

(A) (i), (ii) (B) (ii), (iii)
(C) (i), (iii) (D) (i), (ii), (iii)

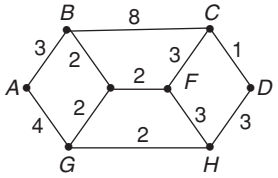
5. Consider the below graph.



It is known that D is the optimal route from A to C and the optimal route from A to C has 3 hops. Which of the below statements is certainly true?

(i) B is not in the optimal route from A to C
(ii) G is not in the optimal route from B to C
(iii) Either E or F is in the optimal route from A to C
(iv) ED, FD are both optimal routes
(A) (i), (ii), (iii) (B) (ii), (iii), (iv)
(C) (i), (iii), (iv) (D) (i), (iv), (ii)

6. The shortest path using Dijkstra's algorithm after 3 iterations is



(A) A G (B) A B E
(C) A B C (D) A G H

7. There are totally 20 links among the routers of a subnet. How many rows are needed in all when link state packets

combined together, which are used to notify each other about cost/delay in transmitting data to immediate neighbours. Assume 1 row is needed for each neighbour?

(A) 10 (B) 20
(C) 40 (D) 80

8. Below are the link state packets generated by routers in a subnet. What is the shortest distance between *A* and *D*?

A	
Seq	
Age	
B	4
E	5

B	
Seq	
Age	
A	4
C	2
F	6

C	
Seq	
Age	
B	2
D	3
E	1

D	
Seq	
Age	
C	3
F	7

E	
Seq	
Age	
A	5
C	1
F	8

F	
Seq	
Age	
B	6
D	7
E	8

(A) 6 (B) 9
(C) 10 (D) 11

9. What are the advantages of reverse path forwarding over other broadcasting algorithms like spanning trees, multidestination routing, broadcasting, and flooding?

(i) Route does not need to know information regarding spanning tree structures
(ii) Uses destination tables for further forwarding
(iii) Does not need a halt mechanism to stop packets from further getting routed

(A) (i), (ii) (B) (ii), (iii)
(C) (i), (iii) (D) (i), (ii), (iii)

10. Which of the following specifies the correct sequence of steps to route packets to mobile hosts?

(i) Sender is given foreign agent's address
(ii) Packet is sent to mobile host's home address
(iii) Packet is tunneled to foreign agent
(iv) Subsequent packets are tunneled to the foreign agent

(A) (i), (ii), (iii), (iv)
(B) (ii), (iii), (iv), (i)
(C) (ii), (iii), (i), (iv)
(D) (iii), (iv), (i), (ii)

11. What are the different parts of congestion control by closed loop methods?

(i) Design the system in advance to make sure congestion doesn't occur in first place
(ii) Monitor the system to detect when and where congestion occurs
(iii) Pass congestion information to places where action can be taken
(iv) Adjust system operation to correct the problem

(A) (i), (ii), (iii)
(B) (ii), (iii), (iv)
(C) (iii), (iv), (i)
(D) (i), (ii), (iv)

12. In Selective flooding

(A) Packets are sent in all outgoing lines.
(B) Packets are sent in only on those lines that are approximately in the right direction.
(C) Both (A) and (B)
(D) None of these

13. There are 5 routers and 6 networks in an inter-networking, using link state routing, how many routing tables are there?

(A) 1 (B) 5
(C) 6 (D) 11

14. Congestion control for multicasting flows from multiple sources to multiple destinations, the solution that can handle this is

(A) RSVP (Resource reSerVation Protocol)
(B) Load shedding
(C) Both (A) and (B)
(D) None of these.

15. Which of the below are part of backward learning algorithm?

(i) As the bridge starts operating, a hash table to map source addresses to corresponding LANs is constructed.
(ii) It dynamically updates the hash tables when machines are connected and re connected to the LAN.
(iii) It encrypts the frames for security reasons.

(A) (i), (ii)
(B) (ii), (iii)
(C) (i), (iii)
(D) (i), (ii), (iii)

Practice Problems 2

Directions for questions 1 to 15: Select the correct alternative from the given choices.

1. What does a routing algorithm perform?
(A) Decides if incoming packet should be further corrected for transmission errors
(B) Adds checksum bits to packets
(C) Encrypts the packets
(D) Decides the output line on which the incoming packet should be transmitted

2. What happens in session routing?
(A) User's session variables are managed by the network layer
(B) Route remains same throughout the user session
(C) Packets change their route for optimization sake during user session
(D) Provides special routes for important packets

3. What is the type of algorithm that changes their routing decision based on changes in topology and traffic?
(A) Adaptive routing
(B) Static routing
(C) Non-adaptive routing
(D) Network routing

4. Which of the below routing method always ensures the shortest path even though routers crash during course of routing?
(A) Dijkstra Routing
(B) Flooding
(C) Distance Vector Routing
(D) Link State Routing

5. What is the root cause for count-to-infinity problem?
(A) The routing tables are static and are not updated.
(B) The routing tables run out of space to accommodate more entries in table.
(C) When router *X* tells router *Y* that there is a path, it doesn't say if *Y* itself is in the path.
(D) When router *X* tells router *Y* that there is a path (to target route *Z*) it doesn't inform *Z* about the path.

6. In a strict sure security path ABCD, where A, B, C, D are routers, the maximum bandwidth is found to be 500 kbps, 700 kbps, 900 kbps, 300 kbps respectively. What is the effective bandwidth if no buffering is possible?
(A) 600 kbps (B) 900 kbps
(C) 300 kbps (D) 2400 kbps

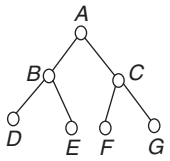
7. What is the characteristic of Distance Vector Routing?
(i) Time taken to reach other routers in the network is maintained in the routing tables.
(ii) Algorithm is susceptible to count-to-infinity problem.
(iii) The preferred outgoing line to be used for a particular destination is also stored in tables.
(A) (i), (ii) (B) (ii), (iii)
(C) (i), (iii) (D) (i), (ii), (iii)

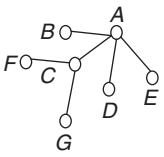
8. A subnet using link state algorithm has router, using link state packets with sequence of 16-bit fixed size. If a link state packet is sent every second, how long would it take before wrap around occurs. Assume starting sequence number is 0.
(A) 24.5 hours (B) 18.20 hours
(C) 17.5 hours (D) 16.4 hours

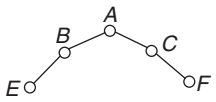
9. Which of the following are features of link state routing?
(i) In the first step discover all the routers in the subnet and find their network addresses.
(ii) Measure cost/delay to the neighbours.
(iii) Transmit the information as obtained in (ii) across the subnet.
(iv) Thus by pass the necessity for shortest path algorithm.
(A) (i), (ii) (B) (ii), (iii)
(C) (iii), (iv) (D) (i), (iv)

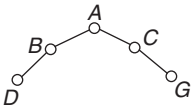
10. In multidestination routing,
(i) Each router makes new copies of the incoming packets.
(ii) It retains the same destination list in all copies.
(iii) It places them on appropriate outgoing lines.
(A) (i), (ii) (B) (ii), (iii)
(C) (iii), (i) (D) (i), (ii), (iii)

11. In a subnet which follows reverse path forwarding, routers *B* and *C* have received packets from *A* which have been further forwarded to *D* and *E* by *B* and to *F* and *G* by *C*. Of this *D*, *G* has always discarded the valid packets. Construct the preferred routing lines in the subnet.

(A) 

(B) 

(C) 

(D) 

12. Which of the following layers accept services from network layer and provides services to session layer?
(A) Data link layer
(B) Presentation layer
(C) Transport layer
(D) Physical layer.

13. Which of the below are different metrics for congestion?
(i) Packets discarded for lack of buffer space
(ii) Packets that are retransmitted
(iii) Average packet delay
(iv) Average queue length
(A) (i), (ii), (iii) (B) (ii), (iii), (iv)
(C) (iii), (iv), (i) (D) (i), (ii), (iii), (iv)

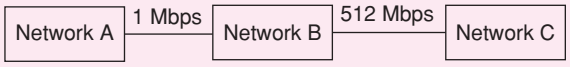
14. What are the ways to decrease congestion?
(i) Put spare routers to use
(ii) Increase bandwidth by routing on alternate lines
(iii) Increase the size of tables in the routers
(iv) Decrease the load
(A) (i), (ii), (iii) (B) (ii), (iii), (iv)
(C) (iii), (iv), (i) (D) (iv), (i), (ii)

15. The algorithm which tells the routers to maintain certain data structures in their memories for congestion control is
(A) Resource Reservation Protocol.
(B) Fair queuing algorithm.
(C) Token bucket algorithm.
(D) None of these

Previous Years' Questions

Common data for questions 1 and 2: Consider three IP networks, *A*, *B* and *C*. Host H_A in network *A* sends messages each containing 180 bytes of application data to a host H_C in network *C*. The TCP layer prefixes a 20 byte header to the message. This passes through an intermediate network *B*. The maximum packet size, including 20 byte IP header, in each network is:
A: 1000 bytes
B: 100 bytes
C: 1000 bytes

The networks *A* and *B* are connected through a 1 Mbps link, while *B* and *C* are connected by a 512 Kbps link (bps = bits per second)



1. Assuming that the packets are correctly delivered, How many bytes, including headers, are delivered to the IP layer at the destination for one application message, in the best case? Consider only data packets. **[2004]**
(A) 200 (B) 220
(C) 240 (D) 260

2. What is the rate at which the application data is transferred to host H_C? Ignore errors, acknowledgements, and other over heads. **[2004]**
(A) 325.5 kbps (B) 354.5 kbps
(C) 409.6 kbps (D) 512.0 kbps

3. In a packet switching network, packets routed from source to destination along a single path having two intermediate nodes. If the message size is 24 bytes and each packet contains a header of 3 bytes, then the optimum packet size is: **[2005]**
(A) 4 (B) 6
(C) 7 (D) 9

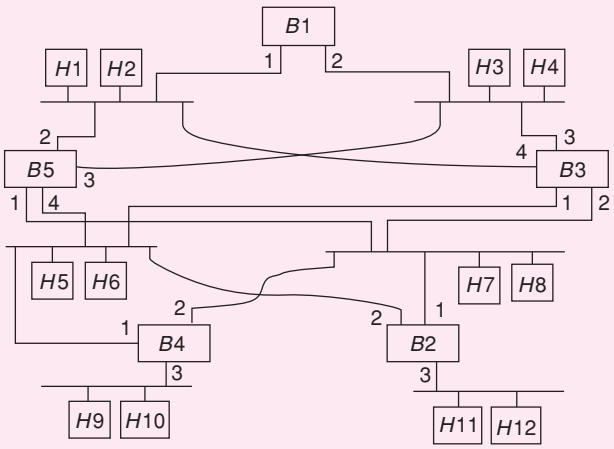
4. Suppose the round trip propagation delay for a 10 Mbps Ethernet having 48-bit jamming signal is 46.4 μs. The minimum frame size is: **[2005]**
(A) 94 (B) 416
(C) 464 (D) 512

5. Station *A* uses 32 byte packets to transmit messages to station *B* using a sliding window protocol. The round trip delay between *A* and *B* is 80 milliseconds and the bottleneck bandwidth on the path between *A* and *B* is 128 kbps. What is the optimal window size that *A* should use? **[2006]**
(A) 20 (B) 40
(C) 160 (D) 320

6. Station *A* needs to send a message consisting of 9 packets to station *B* using a sliding window (window size 3) and go-back-n error control strategy. All packets are ready and immediately available for transmission. If every 5th packet that *A* transmits gets lost (but no acks from *B* ever get lost), then what is the number of packets that *A* will transmit for sending the message to *B*? **[2006]**
(A) 12 (B) 14
(C) 16 (D) 18

Common data for questions 7 and 8: Consider the diagram shown, where a number of LANs are connected by (transparent) bridges. In order to avoid packets looping through circuits in the graph, the bridges organize themselves in a spanning tree. First, the root bridge is identified as the bridge with the least serial number. Next, the root sends out (one or more) data units to enable the setting up of shortest paths from the root bridge to each bridge.

Each bridge identifies a port (the root port) through which it will forward frames to the root bridge. Port conflicts are always resolved in favor of the port with the lower index value. When there is possibility of multiple bridges forwarding to the same LAN (But not through the root port), ties are broken as follows: bridges closest to the root get preference and between such bridges, the one with the lowest serial number is preferred.



7. For the given connection of LANs by bridges, which one of the following choices represents the depth first traversal of the spanning tree of bridges? **[2006]**

(A) B1, B5, B3, B4, B2 (B) B1, B3, B5, B2, B4
(C) B1, B5, B2, B3, B4 (D) B1, B3, B4, B5, B2

8. Consider the spanning tree for the previous question. let Host H1 send out a broadcast ping packet. Which of the following options represents the correct forwarding table on B3? **[2006]**

(A)

Hosts	Port
H1, H2, H3, H4	3
H5, H6, H9, H10	1
H7, H8, H11, H12	2

(B)

Hosts	Port
H1, H2	4
H3, H4	3
H5, H6	1
H7, H8, H10, H11, H12	2

(C)

Hosts	Port
H3, H4	3
H5, H6, H9, H10	1
H1, H2	4
H7, H8, H11, H12	2

(D)

Hosts	Port
H2, H2, H3, H4	3
H5, H7, H9, H10	1
H7, H8, 11, H12	4

9. In a token ring network the transmission speed is 10^7 bps and the propagation speed is 200 metres/μs. The 1-bit delay in this network is equivalent to: **[2007]**

(A) 500 metres of cable.
(B) 200 metres of cable.
(C) 20 metres of cable.
(D) 50 metres of cable.

10. In the slow start phase of the TCP congestion control algorithm, the size of the congestion window **[2008]**

(A) Does not increase
(B) Increases linearly
(C) Increases quadratically
(D) Increases exponentially

11. A computer on a 10 Mbps network is regulated by a token bucket. The token bucket is filled at a rate of 2 Mbps. It is initially filled to capacity with 16 Megabits. What is the maximum duration for which the computer can transmit at the full 10 Mbps? **[2008]**

(A) 1.6 seconds (B) 2 seconds
(C) 5 seconds (D) 8 seconds

12. Let $G(x)$ be the generator polynomial used for CRC checking. What is the condition that should be satisfied by $G(x)$ to detect odd number of bits in error? **[2009]**

(A) $G(x)$ contains more than two terms
(B) $G(x)$ does not divide $1 + x^k$, for any k not exceeding the frame length
(C) $1 + x$ is a factor of $G(x)$
(D) $G(x)$ has an odd number of terms.

Common data for questions 13 and 14: Frames of 1000 bits are sent over a 10^6 bps duplex link between two hosts. The propagation time is 25 ms. Frames are to be transmitted into this link to maximally pack them in transit (within the link).

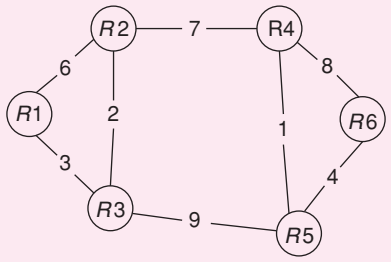
13. What is the minimum number of bits (l) that will be required to represent the sequence numbers distinctly? Assume that no time gap needs to be given between transmission of two frames. **[2009]**

(A) l = 2 (B) l = 3
(C) l = 4 (D) l = 5

14. Suppose that the sliding window protocol is used with the sender window size of 2^l, where l is the number of bits identified in the earlier part and acknowledgements are always piggy backed. After sending 2^l frames, what is the minimum time the sender will have to wait before starting transmission of the next frame? (Identify the closest choice ignoring the frame processing time.) **[2009]**

(A) 16 ms (B) 18 ms
(C) 20 ms (D) 22 ms

Common data for questions 15 and 16: Consider a network with 6 routers $R1$ to $R6$ connected with links having weights as shown in the following diagram



15. All the routers use the distance vector based routing algorithm to update their routing tables. Each router starts with its routing table initialized to contain an entry for each neighbour with the weight of the respective connecting link. After all the routing tables stabilize, how many links in the network will never be used for carrying any data? **[2010]**

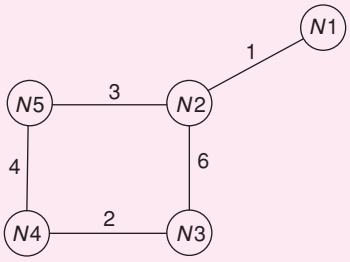
(A) 4 (B) 3 (C) 2 (D) 1

16. Suppose the weights of all unused links in the previous question are changed to 2 and the distance

vector algorithm is used again until all routing tables stabilize. How many links will now remain unused? **[2010]**

(A) 0 (B) 1 (C) 2 (D) 3

Common data for questions 17 and 18: Consider a network with five nodes, $N1$ to $N5$ as shown below.



The network uses a distance vector routing protocol. Once the routes have stabilized, the distance vectors at different nodes are as following.

$N1$: (0, 1, 7, 8, 4) $N4$: (8, 7, 2, 0, 4)

$N2$: (1, 0, 6, 7, 3) $N5$: (4, 3, 6, 4, 0)

$N3$: (7, 6, 0, 2, 6)

Each distance vector is the distance of the best known path at that instance to nodes, $N1$ to $N5$, where the distance to itself is 0. Also, all links are symmetric and the cost is identical in both directions. In each round, all nodes exchange their distance vectors with their respective neighbors. Then all nodes update their distance vectors. In between two rounds, any change in cost of a link will cause the two incident nodes to change only that entry in their distance vectors.

17. The cost of link $N2$-$N3$ reduces to 2 (in both directions). After the next round of updates, what will be the new distance vector at node, $N3$? **[2011]**

(A) (3, 2, 0, 2, 5) (B) (3, 2, 0, 2, 6)

(C) (7, 2, 0, 2, 5) (D) (7, 2, 0, 2, 6)

18. After the update in the previous question, the link $N1$-$N2$ goes down. $N2$ will reflect this change immediatedly in its distance vector as cost, ∞. After the NEXT ROUND of update, what will be the cost to $N1$ in the distance vector of $N3$? **[2011]**

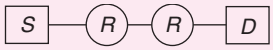
(A) 3 (B) 9 (C) 10 (D) ∞

19. Consider an instance of TCP's Additive Increase Multiplicative Decrease (AIMD) algorithm where the window size at the start of the slow start phase is 2 MSS and the threshold at the start of the first transmission is 8 MSS. Assume that a timeout occurs during the fifth transmission. Find the congestion window size at the end of the tenth transmission. **[2012]**

(A) 8 MSS (B) 14 MSS

(C) 7 MSS (D) 12 MSS

20. Assume that source S and destination D are connected through two intermediate routers labeled R. Determine how many times each packet has to visit the network layer and the data link layer during a transmission from S to D. **[2013]**



(A) Network layer – 4 times and Data link layer – 4 times

(B) Network layer – 4 times and Data link layer – 3 times

(C) Network layer – 4 times and Data link layer – 6 times

(D) Network layer – 2 times and Data link layer – 6 times

21. Consider a selective repeat sliding window protocol that uses a frame size of 1 kB to send data on a 1.5 Mbps link with a one-way latency of 50 msec. To achieve a link utilization of 60%, the minimum number of bits required to represent the sequence number field is _____. **[2014]**

22. Consider the following three statements about link state and distance vector routing protocols, for a large network with 500 network nodes and 4000 links.

[$S1$] The computational overhead in link state protocols is higher than in distance vector protocols.

[$S2$] A distance vector protocol (with split horizon) avoids persistent routing loops, but not a link state protocol.

[$S3$] After a topology change, a link state protocol will converge faster than a distance vector protocol.

Which one of the following is correct about $S1$, $S2$ and $S3$? **[2014]**

(A) $S1$, $S2$ and $S3$ are all true

(B) $S1$, $S2$ and $S3$ are all false

(C) $S1$ and $S2$ are true, but $S3$ is false

(D) $S1$ and $S3$ are true, but $S2$ is false.

23. Let the size of congestion window of a TCP connection be 32 kB when a timeout occurs. The round trip time of the connection is 100 msec and the maximum segment size used is 2 kB. The time taken (in msec) by the TCP connection to get back to 32 kB congestion window is _____. **[2014]**

24. Which one of the following is TRUE about the interior gateway routing protocols-Routing information protocol (RIP) and Open Shortest Path First (OSPF)? **[2014]**

(A) RIP uses distance vector routing and OSPF uses link state routing

(B) OSPF uses distance vector routing and RIP uses link state routing

(C) Both RIP and OSPF use link state routing

(D) Both RIP and OSPF use distance vector routing

25. Consider the store and forward packet switched network given below. Assume that the bandwidth of each link is 10^6 bytes/sec. A user on host A sends a file of size 10^3 bytes to host B through routers R_1 and R_2 in three different ways. In the first case a single packet containing the complete file is transmitted from A to B. In the second case, the file is spilt into 10 equal parts, and these packets are transmitted from A to B. In the third case, the file is spilt into 20 equal parts, and these packets are sent from A to B. Each packet contains 100 bytes of header information along with the user data. Consider only transmission time and ignore processing, queuing and propagation delays. Also assume that there are no errors during transmissions. Let T_1, T_2 and T_3 be the times taken to transmit the file in the first, second and third case respectively. Which one of the following is CORRECT? **[2014]**

(A) $T_1 < T_2 < T_3$ (B) $T_1 > T_2 > T_3$
(C) $T_2 = T_3, T_3 < T_1$ (D) $T_1 = T_3, T_3 > T_2$

26. An IP machine Q has a path to another IP machine H via three IP routers R_1, R_2, and R_3.
$Q - R_1 - R_2 - R_3 - H$
H acts as an HTTP server, and Q connects to H via HTTP and downloads a file. Session layer encryption is used with DES as the shared key encryption protocol. Consider the following four pieces of information.

[*I*1] The URL of the file downloaded by Q
[*I*2] The TCP port numbers at Q and H
[*I*3] The IP addresses of Q and H
[*II*4] The link layer addresses of Q and H

Which of *I*1, *I*2, *I*3 and *I*4 can an intruder learn through sniffing at R_2 alone? **[2014]**

(A) Only *I*1 and *I*2 (B) Only *I*1
(C) Only *I*2 and *I*3 (D) Only *I*3 and *I*4

27. An IP router with a Maximum Transmission Unit (MTU) of 1500 bytes has received an IP packet of size 4404 bytes with an IP header of length 20 bytes. The values of the relevant fields in the header of the third IP fragment generated by the router for this packet are **[2014]**

(A) MF bit : 0, Datagram Length: 1444; Offset: 370
(B) MF bit: 1, Datagram Length : 1424; Offset: 185
(C) MF Bit: 1, Datagram Length: 1500; Offset: 370
(D) MF bit: 0, Datagram Length: 1424; Offset: 2960

28. Identify the correct order in which a server process must invoke the function calls accept, bind, listen, and recv according to UNIX socket API. **[2015]**

(A) listen, accept, bind, recv
(B) bind, listen, accept, recv
(C) bind, accept, listen, recv
(D) accept, listen, bind, recv

29. For a host machine that uses the token bucket algorithm for congestion control, the token bucket has a capacity of 1 megabyte and the maximum output rate is 20 megabytes per second. Token arrive at a rate to sustain output at a rate of 10 megabytes per second. The token bucket is currently full and the machine needs to send 12 megabytes of data. The minimum time required to transmit the data is _____ seconds. **[2016]**

30. Consider the following statements about the routing protocols. Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) in an IPv4 network.

I: RIP uses distance vector routing
II: RIP packets are sent using UDP
III: OSPF packets are sent using TCP
IV: OSPF operation is based on link-state routing

Which of the statements above are CORRECT? **[2017]**

(A) I and IV only (B) I, II and III only
(C) I, II and IV only (D) II, III and IV only

Answer Keys

Exercises

Practice Problems 1

1. A	**2.** D	**3.** A	**4.** B	**5.** A	**6.** A	**7.** C	**8.** B	**9.** C	**10.** C
11. B	**12.** B	**13.** B	**14.** A	**15.** A					

Practice Problems 2

1. D	**2.** B	**3.** A	**4.** B	**5.** C	**6.** C	**7.** D	**8.** B	**9.** B	**10.** C
11. C	**12.** C	**13.** D	**14.** D	**15.** A					

Previous Years' Questions

1. D	**2.** B	**3.** D	**4.** D	**5.** B	**6.** C	**7.** C	**8.** A	**9.** C	**10.** D
11. B	**12.** C	**13.** D	**14.** B	**15.** C	**16.** B	**17.** A	**18.** C	**19.**	**20.** C
21. 5	**22.** D	**23.** 1100 to 1300		**24.** A	**25.** D	**26.** C	**27.** A	**28.** B	**29.** 1.1
30. C									

Chapter 3

TCP/UDP

LEARNING OBJECTIVES

- *Transport layer*
- *User Diagram Protocol (UDP)*
- *TCP/IP*
- *TCP/IP vs OSI reference model*
- *TCP state transition diagram*
- *TCP flow control*
- *Application layer*
- *ICMP, SMTP, POP3, IMAP 4, HTTP, FTP*
- *DNS*
- *Network devices*

Transport Layer

Real communication takes place between two applications programs i.e., processes. For this, process-to-process delivery is needed. A mechanism is required in order to deliver data from one of these processes running on the source host to the corresponding process running on the destination host.

The transport layer is responsible for process-to-process delivery.

Addressing in Transport Layer

Port addresses

- A transport layer address is a port number.
- The destination port number is needed for delivery and the source port number is needed for reply.
- The port numbers are 16-bit integers ranging from 0 to 65535.

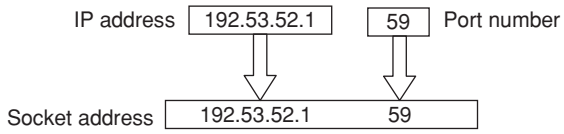
The IANA (Internet Assigned Number Authority) has divided the port numbers as:

- Well-known ports (0 to 1023)
- Registered ports (1024 to 49,151)
- Dynamic or private or ephemeral ports (49,152 to 65,535)

Socket address

Process to process delivery needs two identifiers, IP address and port address at each end to make a connection.

The combination of an IP address and a port number is socket address.



Protocols at transport layer

1. UDP
2. TCP
3. SCTP

User Datagram Protocol (UDP)

- UDP is connectionless protocol.
  - There is no mechanism for connection establishment or connection termination.
  - The packets may be delayed or lost or may arrive out of sequence, i.e., there is no acknowledgement.
  - Each user datagram sent by UDP is an independent program. Even if the user datagram's are coming from the same source program and going to the same destination process, there is no relationship between the different datagrams.

  Thus, user datagrams can travel on a different path.
- Multicasting capability is embedded in UDP.
- It is a simple, unreliable transport protocol.
  - There is no flow control, no window mechanism.
  - There is no error control as well except for the checksum. The sender does not know if a message has been lost or duplicated. When the receiver detects an error through the checksum, the datagram is discarded silently.
- It is used in real-time applications.
  - The header length is fixed, of 8 bytes. Real time applications require a constant flow of data. Moreover, the unreliability (fast and less complex service) of UDP aids in real-time applications like voice over IP, online games etc.
- It encapsulates and decapsulates messages in an IP datagram.

User Datagram

UDP packets have other name called user datagrams. They have a fixed size header of 8 bytes. The datagram is divided into 4 fields.

Source port number (16-bits)	Destination port number (16-bits)
Total length (16-bits)	Checksum (16-bits)

Figure 1 User datagram header format

1. ***Source Port Number*** It is a 16-bit number used by the process running on the source host.
2. ***Destination Port Number*** It is also a 16 bit number used by the process running on the destination host.
3. ***Total length*** It is a 16-bit field, it defines the total length of the user datagram header and data. It can define a total length of 0 to 65535 bytes. A UDP packet is encapsulated in an IP packet.

UDP length = IP length – IP header's length

4. ***Checksum:*** It is optional field, if not available the field is filled with 1's. It is used to detect errors in user datagram (header plus data).

Protocols That Take UDP Services

Following are a few protocols that take the services of UDP:

1. Domain Name Service (port – 53): UDP is used to send small data. If the data is less than 512 bytes, then DNS uses UDP else it goes for TCP.
2. Trivial File Transfer Protocol (port – 69): TFTP is used to transfer simple and small files, it uses UDP service.
3. Routing Information protocol: It uses UDP service on port number 520 to update routers.
4. Simple Network Management Protocol (SNMP): The SNMP agent receives requests on UDP port 161 for management process.
5. Bootstrap protocol (BOOTP): For client (port 68) and for server (port – 67).

UDP Checksum Calculation

- The checksum includes a pseudo header, the UDP header and the data coming from the application layer.

32-bit source IP address		
32-bit destination IP address		
All 0's	8-bit protocol (17)	16-bit UDP total length

Figure 2 Pseudo header of UDP for checksum calculation

- The value of protocol field is 17. If this value is changed during transmission, the checksum calculation at the receiver will detect it and UDP drops the packet.
- If the checksum is not calculated, the field is filled with 0's. This means checksum calculation is optional.
- The calculated checksum can never be all 1's as this implies that the sum is all 0's. But this is impossible because for this the value of fields have to be 0's.

TCP/IP

TCP/IP is a network model which is used for the internet architecture, its main objectives are

- Connecting the multiple networks.
- Maintaining the intact connection between two machines, which are functioning.

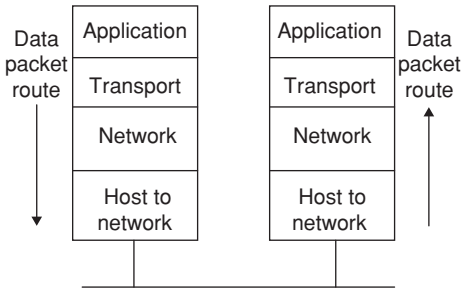


Figure 3 TCP/IP network protocol

TCP/IP vs OSI Reference Model

	OSI		TCP/IP
(1)	There are 7 layers	(1)	There are 5 layers
(2)	There is no definition for multicasting	(2)	Multicasting is clearly defined
(3)	Less flexibility	(3)	Lot of flexibility
(4)	Practically it is not suggestible as it is based on theoretical rules	(4)	It is based on practical rules

- TCP stands for Transmission Control Protocol.
- It is connection-oriented protocol.
  - It creates a virtual connection between two TCPs to send data then data is transferred and at the end the connection is released.
  - There is acknowledgement mechanism for safe and sound arrival of data.
- It is a reliable transport protocol.
  - Uses flow and error control.
  - Slower and more complex service.
  - Duplicate segments are detected, lost segments are resent, the bytes are delivered to the end process in order.
- It is a stream-oriented protocol.

- Allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes.
- TCP offers full-duplex service.
  - Data can flow in both directions at the same time.
  - Each TCP has a sending and receiving buffer.
  - It cannot be used in real time applications as the header length varies from 20-to-60 bytes, moreover it needs reliability.

TCP Header Format

- A packet in TCP is called a segment. The segment consists of a 20-to-60 bytes header.
- If there are no options, the header is of 20 bytes.

Source port address (16-bits)					Destination port address (16-bits)			
Sequence number (32-bits)								
Acknowledgement number (32-bits)								
HLEN (4-bits)	Reserved (6-bits)	URG	ACK	PSH	RST	SYN	FIN	Window size (16-bits)
Checksum (16-bits)					Urgent Pointer (16-bits)			
Options and Padding								

Figure 4 TCP header format

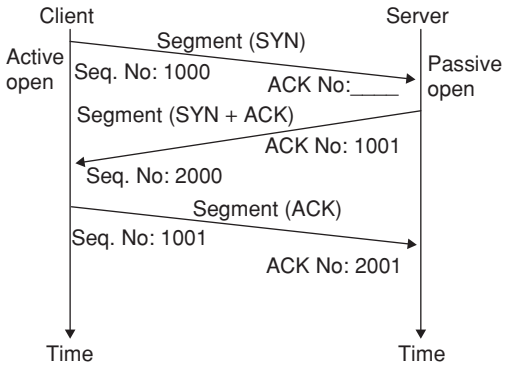
- If there are options, the header goes upto 60 bytes.
- ***Source Port addresses*** A 16-bit field that defines the port number of the application program in the host that is sending the segment.
- ***Destination Port address*** A 16-bit field that defines the port number of the application program in the host is receiving the segment.
- ***Sequence number*** A 32-bit field whose value defines the number of the first data byte contained in that segment. During connection establishment, a random number is generated to create an initial sequence number (ISN) which is usually different in each direction.
- ***Acknowledgement Number*** A 32-bit field whose value defines the number of the next byte, a party expects to receive. If the receiver of the segment has successfully received byte number x from the other party, it defines $x + 1$ as the acknowledgement number. The acknowledgement number is cumulative.
- ***HLEN(Header Length)*** This field is of 4-bit. The header length can be between 20 and 60 bytes. The value of this field can be between $5(5 \times 4 = 20)$ and $15(15 \times 4 = 60)$.
- ***Reserved*** This is a 6-bit field which is reserved for future use.
- ***Control*** This field contains 6 control flags. These are as follows.
  - URG: Urgent pointer. This flag is set when the value of urgent pointer field is valid.
  - ACK: Acknowledgement pointer. This flag is set when the value of acknowledgement field is valid. It is not set at the start of connection during 3-way handshake.
  - RST: Reset pointer. Used to reset the connection, reject an invalid segment or refuse an attempt to open a connection.
  - PSH: Push pointer. When a data is pushed the flag is set.
  - SYN: Synchronization pointer, used to synchronize sequence numbers during connection. If it is set to 1, then it is ISN. If set to 0, then it is the accumulated sequence number of the first data byte of the segment for the current session.
  - FIN: Finish Pointer. It is used to terminate a connection. It indicates that the sender is not interested in sending any more data.
- ***Window size*** The field size is of 16-bits and thus the maximum size of the window is 65,535 bytes. This field is determined by the receiver and thus referred to as the receiving window. The window size is variable.
- ***Checksum*** The inclusion of this 16-bits field is mandatory in TCP. The calculation of the checksum for TCP follows the same procedure as in UDP, only the value of protocol field in TCP is 6.
- ***Urgent pointer*** This 16-bit field, is valid only if the urgent flag is set. This field is used when the segment contains urgent data.
- ***Options and padding*** When the header length is greater than 5, option field is used to make the segment into the multiples of 32. Padding is used to ensure the ending of TCP header, it is composed to 32 zeros.

TCP Connection

- TCP is connection-oriented and the connection is virtual not physical.
- TCP operates at a higher level. TCP uses the services of IP to deliver individual segments to the receiver, but it controls the connection itself. Lost or corrupted segments are retransmitted.
- In TCP, connection-oriented transmission requires three phases:
  1. Connection establishment
  2. Data transfer
  3. Connection termination

Connection establishment

- The connection establishment in TCP is called three-way handshaking.
- The process starts with the server. The server program tells its TCP that it is ready to accept a connection. This is a request for a passive open.
- The client program issues a request for an active open. A client that wishes to connect to an open server tells its TCP that it needs to be connected to a particular server. Hence the TCP can start the three-way handshaking process as shown in the figure.



1. The first segment which is a SYN segment is identified by the randomly generated number and is assigned to a 1 byte dummy data indicating the sequence number.
2. Again from the server side a randomly generated number is assigned for the dummy data indicating the first byte.
3. A SYN segment cannot carry data, but it consumes one sequence number.

   A (SYN + ACK) segment cannot carry data, but consumes one sequence number.

   An ACK segment, if carrying no data, consumes no sequence number.
4. Initial Sequence Number (ISN) 1000 is sent from the client to server. Server receives the segment 1000 and is expecting segment 1001 as the next one.

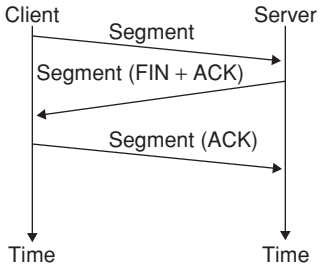
Data transfer

- After the connection is established, bidirectional data transfer can take place. Both the client and server can send data and acknowledgements.
- The data segments sent by the client have the PSH (push) flag set so that the server TCP knows to deliver data to the server process as soon as they are received.
- Sometimes the sending application program wants a piece of data to be read out of order by the receiving application program that means an application program needs to send urgent bytes then in this case the URG bit is set and the segment is send. The sending TCP creates a segment and inserts the urgent data at the beginning of the segment.

Connection termination

There are two options for connection termination.

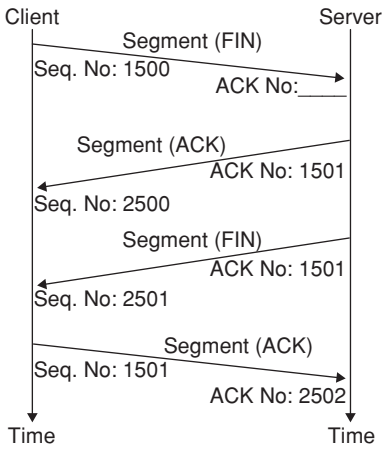
Three-way handshaking



- The client process sends the first segment, a FIN segment in which the FIN flag is set. The FIN segment consumes one sequence number if it does not carry data.
- The server TCP sends the second segment, a FIN + ACK segment, to confirm the receipt of the FIN segment from the client and at the same time announce the closing of the connection in the other direction.
  The FIN + ACK segment consumes one sequence number if it does not carry data.
- The client sends the last ACK segment to the server. This segment contains acknowledgement number which is 1 plus, the sequence number received in the FIN segment from the server.

Four-way handshaking

- ***Half-close**:* In TCP, one end can stop sending data while still receiving data. This is half close.
- The client half-closes the connection by sending a FIN segment.
- The server accepts the half-close by sending the ACK segment. The data transfer from the client to the server stops.
- When the server has sent all the processed data, it sends a FIN segment, which is acknowledged by an ACK from the client.



TCP State Transition Diagram

The functionality of TCP connection setup, communication phase and termination phase can be easily depicted by the state transition diagram where the TCP will be only at one state at a time with respect to server or client.

A change in the state is only observed after receiving a request for change like ACK (acknowledgement).

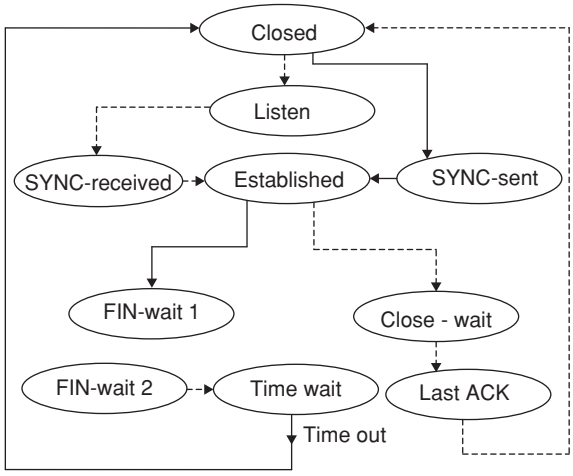


Figure 5 State transition diagram

Here, Solid line '–' is for client states, Break line '---' is for server states

State 'Closed' is common for both client and server. Initially the client and the server are in the closed state where no TCP connection is set. When an application request for a TCP connection then the client changes its state from closed to SYNC-sent state.

Client states

1. SYNC-sent — After the client sends a SYNC-sent and receives an ACK for the sent SYNC segment, it changes its state to ESTABLISHED STATE.
2. Established — In this state the client and the server exchange user data. After the requested application is completed, it sends a FIN segment and changes its state to FIN-wait 1.
3. FIN-wait 1 — FIN-wait 1 changes to FIN-wait 2 after receiving an ACK for sent FIN segment.
4. FIN-wait 2 — The client will remain in this state until it receives a FIN segment from the server. When the last ACK is sent by the client, the client changes its state to Time-wait.
5. Time-wait — A timer is set at this state for any delayed segment from the server which are removed or discarded at the client and after the timeout is reached, the client changes its state from present state to the closed state again.

Server states

1. Listen — This is a passive state where the server always listens for the SYNC request segment on different TCP ports.
2. SYN-received — After receiving the SYNC request from the client, the server acknowledges its state to the Established state.
3. Closed-wait — The server changes its state from Established to close-wait after receiving the finish segment from the client. In this state the server sends an ACK and finish segments. Afterwards it changes the state to last-ACK.
4. Last-ACK — In this state the server expects the last ACK segment from the client, as and when it receives the ACK segment it changes its state to again closed state.

TCP Congestion Control

- Deals with end-to-end delivery.
- Congestion handling in TCP is based on three phases:
  - Slow start
  - Congestion avoidance
  - Congestion detection

Slow start (exponential increase)

1. By default the receiver window size is initially set to 1.
2. In the first instance the transmitter receives an ACK for the window size indicating the receiver window size as 2 segments.
3. After 2 segments are sent it is acknowledged with 4 segments.
4. After 4 segments are sent it it acknowledged with 8 segments.
5. This is exponential growth and this growth continue until the window size reaches the threshold value.
6. If there is delayed ACKs, the increase in the size of the window is less than power of 2.

Congestion avoidance (additive increase)

1. To avoid the congestion before it happens, the exponential growth of slow start algorithm must be slowed down.
2. When the threshold is reached, then the additive phase begins. Here each time the whole window of segments is acknowledged, the size of congestion window is increased by 1.

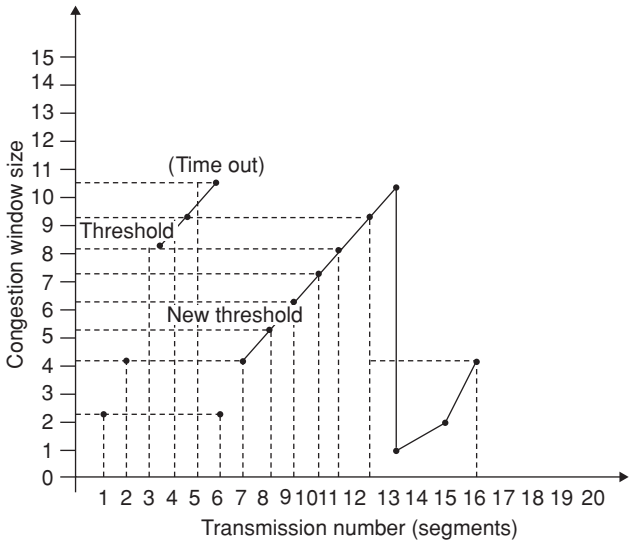
Congestion detection (multiplicative decrease)

1. If congestion occurs, the congestion window size must be decreased. The only way the sender can guess the congestion has occurred is by the need to retransmit a segment.
2. Retransmission can occur in two cases:
   (i) When a timer times out.
   (ii) When 3 ACKs are received.

3. In both the cases the size of threshold is dropped to one-half of the current window size and the window size is decreased to initial window size "1".
   This is multiplicative decrease.

Example: Let us take an example to explain the TCP congestion control.

Consider an instance of TCP additive increase, multiplicative decrease algorithm where the window size at the start of slow-start phase is 2 MSS (Maximum Segment Size) and threshold value is 8 MSS. The timeout occurs at the fifth transmission. Then what is the congestion window size at the end of the tenth transmission?



Window size is 2 MSS initially.

8 MSS is threshold value, after this there is only increase of 1-1 window size till timeout value which is 10.

The new threshold value becomes half of the value of current congestion window i.e., 5.

Timeout remains the same i.e., 10.

At 10th transmission the window size is 7.

After time-out, at 13th transmission window size = 1 and at 14th transmission window size = 2.

TCP Flow Control

- For flow control sliding window protocol is used.
- The window size is set by the receiver and is controlled by the receiver. The window size is not fixed (variable).
- The sliding window protocol in TCP looks like the Go-Back-N protocol because it does not use NAKs; it looks like Selective Repeat because the receiver holds the out-of-order segments until the missing ones arrive.
- A sliding window is used to make transmission more efficient as well as to control the flow of data so that the destination does not become overwhelmed with data. TCP sliding windows are byte-oriented.

TCP Error Control

- TCP provides reliability using error control.
- Error control includes mechanism for detecting corrupted segments, lost segments, out-of-order segments and duplicated segments.
- Error detection and correction in TCP is achieved through the use of three tools:
  - Checksum
  - Acknowledgment
  - Time-out

Checksum

Each segment includes a checksum field which is used to check for a corrupted segment. A 16-bit checksum is mandatory in every segment.

Acknowledgement

- There is no negative ACK in TCP.
- There is no ACK for the received ACK.
- Only the correctly received segments are acknowledged, if any segment if found to be corrupted through checksum such segments are not acknowledged.

Time-out

Different timers are deployed for error control.

1. ***Time-awaited timer:*** This timer is used to handle TCP termination process specially to handle duplicate finish segments.
   Its value is set to twice the life time of a segment.
2. ***Keep-Alive Timer:*** This timer is used to handle long idle TCP connections.
   By default its value is 2 hours, beyond which a probe (1 byte dummy data) is used for 10 consecutive times with a separation of 75 milliseconds. If there is no response beyond this, then the connection is terminated.
3. ***Persistence Timer:*** This timer is used to handle Zero(0) window size scenario.
   The sender sends 1 probe every 60 seconds until it receives a non-zero window size from where the communication resumes.
4. ***Retransmission Timer:*** This timer is used for handling any lost segments. Its value is twice the Round trip time, i.e., $2 \times RTT$.
   RTT is time needed for a segment to reach a destination and for an acknowledgement to be received.

Application Layer

An interface between the networks is called application. This section introduces two important concepts:

- Application Layer: The application layer of the OSI model provides the first step of getting data onto the network.

- Application Software: Applications are the software programs used by people to communicate over the network. Examples of application software, includes HTTP, FTP, e-mail, and others, used to explain the differences between these two concepts.

In the OSI model, information is passed from one layer to the next, starting at the application layer on the transmitting host and proceeding down the hierarchy to the physical layer, then passing over the communications channel to the destination host, where the information proceeds back up the hierarchy, ending at the application layer.

The following six steps explain the procedure:

1. People create the communication.
2. The application layer prepares human communication for transmission over the data network.
3. Software and hardware converts communication to digital format.
4. Application layer services initiate the data transfer.
5. Each layer plays its role. The OSI layers encapsulate data down the stack. Encapsulated data travels across the media to the destination. OSI layers at the destination unencapsulate the data.
6. The application layer receives data from the network and prepares it for human use.

The application layer, layer 7, is the top layer of both the OSI and TCP/IP models. Layer 7 provides the interface between the application you use to communicate and the underlying network over which your messages are transmitted. Application layer protocols are used to exchange data between programs, running on the source and destination hosts.

TCP/IP Application Layer Protocol

The most widely known TCP/IP application layer protocols are those that provide the exchange of user information. These protocols specify the format and control information necessary for many of the common internet communication functions. Among these, TCP/IP protocols are the following.

- Domain name system (DNS) is used to resolve internet names to IP addresses.
- Hypertext transfer protocol (HTTP) is used to transfer files that make up the web pages of the world wide web.
- Simple mail transfer protocol (SMTP) is used for the transfer of mail messages and attachments.
- Telnet, a terminal emulation protocol, is used to provide remote access to servers and networking devices.
- File transfer protocol (FTP) is used for interactive file transfers between systems.

Application Layer Services

Programs such as file transfer or network print spooling, might need the assistance of application layer services to use network resources. Although transparent to the user, these services have interface with the network and prepares the data for transfer. Different types of data whether it is text, graphics or video require different network services to ensure that it is properly prepared for processing by the functions occurring at the lower layers of OSI model. Application layer services establish an interface to the network and protocols provide the rules and formats that govern how data is treated, a single executable program can use all three components. For example, while discussing "Telnet", you could be referring to the Telnet application, the Telnet service, or the Telnet protocol.

Application Layer Protocol Functions

Both the source and destination devices use application layer protocols during a communication session. For the communications to be successful, the application layer protocols implemented on the source and destination host must match.

Protocols perform the following tasks

- Establish consistent rules for exchanging data between applications and services loaded on the participating devices.
- Specifies how data inside the messages is structured and the types of messages that are sent between source and destination. These messages can be requests for services, acknowledgements, data messages, status messages, or error messages.
- Defines message dialogues, ensuring that a message being sent is met by the expected response and that the correct services are invoked when data transfer occurs.

Applications and services can also use multiple protocols in the course of a single conversation. One protocol might specify how to establish the network connection and another might describe the process for the data transfer when the message is passed to the next lower layer.

A single application can employ many different supporting application layer services. Thus, what appears to the user as one request for a web page might, in fact, amount to dozens of individual requests. For each request, multiple processes can be executed. For example, the FTP requires a client to initiate a control process and a data stream process to a server. Additionally, servers typically have multiple clients requesting information at the same time, as shown in the figure below. For example, a Telnet server can have many clients requesting connections to it. These individual client requests must be handled simultaneously and separately for the network to succeed. The application layer processes and services rely on support from lower layer functions to successfully manage the multiple conversations.

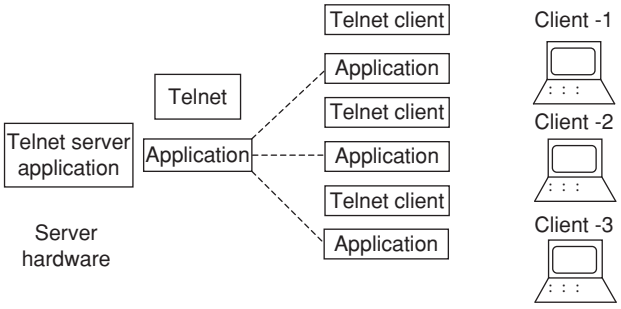


Figure 6 Multiple client's service Requests

Application Layer Protocols

The transport Layer uses an addressing scheme called a port number. Port numbers identify application layer services that are source and destination of data. Server programs generally use predefined port numbers that are commonly known by clients.

Some of these services are

- Domain Name System (DNS): TCP/UDP Port 53
- HTTP: TCP Port 80
- Simple Mail Transfer Protocol (SMTP): TCP Port 25
- Post office Protocol (POP): UDP Port 110
- Telnet: TCP Port 23
- DHCP: UDP Port 67
- FTP: TCP Ports 20 and 21

Internet Control Message Protocol (ICMP)

- Used by hosts and gateways to send notification of datagram problems back to the sender.
- Used for error reporting and query messages.
- Helpful in network debugging.
- Uses the services of TCP and UDP with the port number 7 as the ping command which is used for testing, this testing is done from a source which starts at the application layer and reaches network through transport layer.
- ICMP is encapsulated into an IP datagram and then transmitted into the network, if the protocol filed in the IP datagram is 1 then the IP datagram is said to be carrying ICMP message.

Types of messages

Error reporting

- **Destination Unreachable:** The packet is discarded due to the host not present in the network or the host is not responding to the request.
- **Source Quench:** The packet is discarded due to the congestion in the network.
- **Parameter Problem:** The packet is discarded due to the processing problem observing a change in the header format of the I/P datagram.
- **Time Exceeded:** The packet is discarded because the TTL value is decremented to zero(0).
- Redirection: Here the packet is not discarded but redirected to a network as the host doesn't belong to this network.

Query message

Router solicitation and router advertisement request and reply: Router solicitation is a request generated by the source requesting the router's presence in the network.

The response is a router advertisement generated by the router broadcasting its network id and its presence in the network.

Address mask request and reply: If by any means the node is unable to identify the network bits in its I/P address then this request is used by the source to a router requesting for the network id, the reply is also unicast in this scenario.

Time stamp echo request and reply: This is used to calculate the round trip time of a packet for network diagnose or debugging.

Echo request and reply: This is used to see the presence of a host or a router in the network. For example PING.

SMTP

- SMTP stands for simple mail transfer protocol.
- It uses the services of TCP on port number 25.
- It is a push protocol. Even when the destination is not interested to receive the message this push approach of the SMTP makes the receiver receive the message.
- Components of SMTP:

1. User Agent (UA) :
   (i) It provides Graphical User Interface access to the user.

   Example: Netscape navigation, Mozilla Firefox. It also provides command-driven access in early days.

   (ii) It handles the inbox transactions:
   (a) Composing messages: Helps the user compose the e-mail message to be sent out.
   (b) Reading messages: Helps to read incoming messages by checking the mail in the incoming mail box.
   (c) Replying to messages: Sends the message to the sender or recipients of the copy.
   (d) Forwarding messages: Sends the message to a third party.
   (e) Handling mailboxes: Two mailboxes, an inbox and an outbox are created by the user agent. The inbox keeps all the received e-mails until they are deleted by the user. The outbox keeps all the sent e-mails until the user deletes them.

2. Mail transfer agent (MTA): The actual mail is transferred using MTA.
3. Multipurpose Internet mail extension (MIME): By default SMTP uses ASCII format for transaction. But few languages like Japanese, German etc do not support ASCII format. Hence for carrying non-ASCII form of transactions MIME is used in congestion with SMTP. Thus, MIME is a set of software functions that transforms non-ASCII data (stream of bits) to ASCII data and vice-versa.
4. Mail access protocol (MAP): MAP is a pull approach where the emails of a client are retrieved from the mail server i.e., it is used to retrieve the clients emails from the mail server.

   Two protocol of MAP are

   (i) POP 3 (Post Office Protocol)
   (ii) IMAP4 (Internet MAP)

POP3

1. It is a pull protocol.
2. It uses the services of TCP on port number 110.
3. POP3 has several drawbacks and hence it is currently not in use.
   - A user cannot have different folders on the server.
   - A user cannot partially check the contents of the mail before downloading.
   - A user cannot search a mail with a keyword.
   - The user is not allowed to organize the mail on the server.

(4) Modes of POP3
   (i) Copy mode: The mails are copied from the mail server onto the client.
   (ii) Delete mode: The mails are transferred from the mail server to the client and deleted at the mail server. By default POP3 uses delete mode.

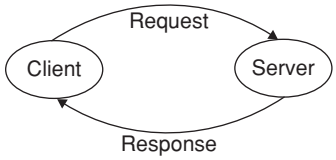
IMAP 4

To overcome the drawbacks of POP3, IMAP4 is in current use. It provides the following functions:

1. A user can create, delete or rename mail boxes on the mail server.
2. A user can create a hierarchy of mailboxes in a folder.
3. A user can partially download e-mail.
4. A user can check the e-mail header before downloading and can search the contents of the e-mail for any specific character prior to downloading.

HTTP

- HTTP stands for Hyper Text Transfer Protocol.
- It uses the services of TCP on well known port 80.
- It is a protocol mainly used to access data on the World Wide Web (www).
- HTTP functions as a combination of FTP and SMTP.
- It uses only one TCP connection, there is no separate control connection, only data is transferred between the client and the server.
- HTTP messages are read and interpreted by the HTTP server and HTTP client (browser).
- It works on two commands request and reply.
- It is a stateless protocol as it does not have any mapping from one transaction onto the other and treats a request and reply as a pair every time.



HTTP1.1 has several request types called methods:

1. GET: Requests a document from the server.
2. HEAD: Requests information about a document but not the document itself.
3. POST: Sends some information from the client to the server.
4. PUT: Sends a document from the server to the client.
5. TRACE: Echoes the incoming request.
6. CONNECT: Reserved.
7. OPTION: Inquires about available options.

- HTTP supports proxy servers. A proxy server is a computer that keeps copies of responses to recent requests. This reduces the load on the original server, decreases traffic and improves latency.
- HTTP Connections:
  (i) *Non-persistence:* In this connection approach for every request and reply (response) as a pair, a separate TCP connection is established every time. It suffers from slow start process. This was present in http version 1.0. Two RTTS are required to fetch each object.
  (ii) *Persistence:* Here a single TCP connection is set on which multiple request and response can be made. This is observed from http version 2.0 onwards (apache http server). For http/1.1 is default. Hence we have reduced network congestion and faster content delivery.

File Transfer Protocol (FTP)

- FTP uses the services of TCP.
- It needs two TCP connections:
  - Uses well-known port 21 for the control connection.
  - Uses well-known port 20 for the data connection.

- Mode of access:

  FTP(TCP) – requires username and password.
  TFTP(UDP) – requires no username and password.
- Types of files supported by FTP:

  i. ASCII: By default FTP follows ASCII mode for file transfer. It is composed of 7-bit + 1 parity bit.
  ii. EBCDIC: If any node supports EBCDIC then this type of technique is used for file transfer. BCDIC supports 8 bits data format and is used in IBM. There is no error control i.e., there is no parity bit.
  iii. Image file: If the file to be sent is very large then continuous streams of 0s and 1s are sent to the transport layer. This is image file. Here FTP does not care of code, it is done by the lower layers.
- **Transmission mode of FTP:** FTP can transfer a file across the data connection by using one of the following three transmission modes:

  i. Stream mode: This is the default mode. Data are delivered from FTP to TCP as a continuous stream of bytes.
  ii. Block mode: Data is delivered from FTP to TCP in blocks. Each block is preceded by a 3-byte header. The first byte is called the block descriptor, the next two bytes define the size of the block in bytes.
  iii. Compressed mode: If the file is big then the data is compressed. The compression method which is mostly used is run-length encoding. Consecutive appearances of a data unit are replaced by one occurrence and the number of repetitions. In a binary file, null characters are compressed.

DNS

- Stands for Domain Name System.
- The DNS is a client/server application that identifies each host on the Internet with a unique user-friendly name i.e., it is used to map an Uniform Resource Locator (URL) to an IP address.
- DNS can use the services of UDP or TCP using the well-known port 53.
- If the size of the response message is more than 512 bytes, it uses the TCP connection.
- When the size of the response message is less than 512 bytes, UDP connection is used. Even though the size of message is not known then also UDP can be used. The UDP server will truncate the message if the message size is more than 512 bytes.
- DNS organizes the namespace in a hierarchical structure to decentralize the responsibilities involved in naming.
- DNS can be pictured as an inverted hierarchical tree structure with one root node at the top and a maximum of 128 levels. Each node in the tree has a domain name.

For example, on the Internet, the domain names, such as http//www. cisco.com, are much easier for people to remember than 198.132.219.25. Also if, cisco decides to change the numeric address, it is transparent to the user, because the domain name will remain http//www.cisco.com. The new address will simply linked to the existing domain name and connectivity is maintained as shown in the figure.

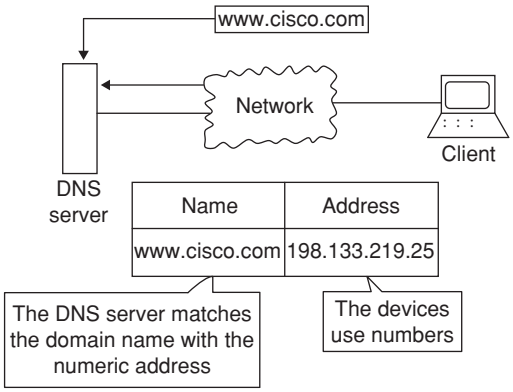


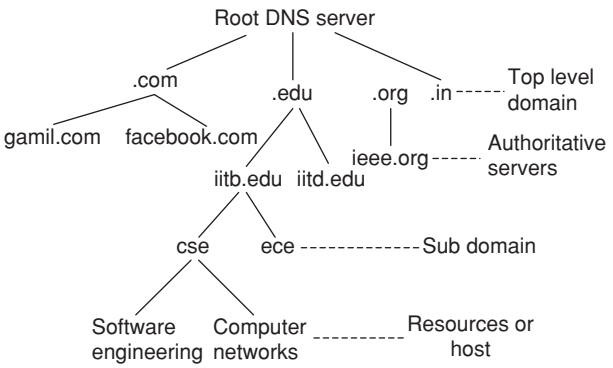
Figure 7 DNS addresses

When networks were small, it was a simple task to maintain the mapping between domain names and the addresses they represent. However, as networks began to grow and the number of devices increased, this manual system became unworkable. DNS was created for domain name to address resolution for these networks. DNS uses a distributed set of servers to resolve the names associated with these numbered addresses.

The DNS protocol defines an automated service that matches resource names with the required numeric network address. It includes the format for queries, responses, and data formats. DNS protocol communications use a single format called a message. This message format is used for all types of client queries and server responses, error messages, and the transfer of resource record information between servers. DNS is a client/server service, however, it differs from the other client/server services. Where as other services use a client that is an application (Web browser, e – mail, client, and so on) the DNS client runs as a service itself. The DNS client, sometimes called the DNS resolver, supports name resolution for the other network applications and other services that need it.

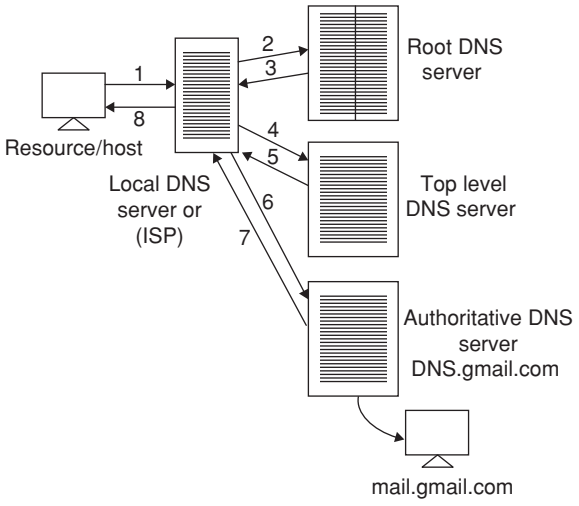
When configuring a network device, you generally provide one or more DNS server addresses that the DNS client can use for name resolution. Usually the Internet Service Provider (ISP) gives you the address to use for the DNS servers. When a user's application requests to connect to a remote device by name, the requesting DNS client queries one of these DNS servers to resolve the name to a numeric address.

- The domain name space consists of a tree of domain names. Each node or leaf in the tree has zero or more resource records, which holds information associated with the domain name. The tree sub-divides into zones beginning at the root zone. A DNS zone consists of a collection of connected nodes authoritatively served by an authoritative name server.



Components of DNS

1. Root DNS Server : Root name servers keep track of all the authoritative name servers of each of the top level domain (TLD) name servers.
2. Top Level Domain: It provides the information regarding the presence of different zone files like
   (i) based on geographical location (country domain): us—for United Statesm, in—for India
   (ii) based on general attributes (generic domain):
   com—used by commercial organization
   Example, gmail.com
   .edu—used by educational institutes
   .org—used by non-profit organizations
   Example, ieee.org
   .gov—used by government institutions
   Example, nasa.gov
   .mil—used by military organizations
   Example, army.mil
3. Zones: The TLD and the domains under TLD are divided into smaller units with the help of delegation. The domain is divided into small units, so that it can be managed easily. These small units are zones.
4. Authoritative DNS servers checks whether authoritative name servers are located in the DNS hierarchy.



Dns Resource Records (RR)

- Every domain, whether it is a TLD, subdomain or single host have a set of resource records associated with it in the DNS distributed data base.
- Resource Records provide the mapping of host name to IP address. When a query is made to the DNS server, the host or server. who sends that query receives a response which is nothing but the resource record associated with it.
- A Resource Record (RR) is a 5 tuple that contains (Name, Time to live, class, Type, Value)
  (i) Name: It is the domain name to which this RR belongs to. More than one resource records may exists for the same domain.
  (ii) Time to live: The TTL is measured in seconds and it is a 32-bit integer.
  (iii) Class: This field contains the value 'IN' which tells whether this record is used by internet or not.
  (iv) Type: Defines type of RR address, name service, canonical name.
  (v) Value: This field can be a number, ASCII strings or any domain.

Networking Devices

Repeater

In digital communication systems, a repeater is a device that receives a digital signal on an electromagnetic or optical transmission medium and regenerates the signal. Repeaters remove the unwanted noise in an incoming signal. Unlike an analog signal, the original digital signal, even if weak or distorted, can be clearly perceived and restored. With analog transmission, signals are re strengthened with *amplifiers* which unfortunately also amplify noise as well as information.

Hub

A hub is the central part of a wheel where the spokes come together. The term is familiar to frequent fliers who travel through airport "hubs" to make connecting flights from one point to another. In data communications, a hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more other directions. A hub usually includes a switch of some kind. (And a product that is called a "switch" could usually be considered a hub as well.)

Switch

In a telecommunications network, a switch is a device that channels incoming data from any of multiple input ports to the specific output port that will take the data towards its intended destination. In the traditional circuit-switched telephone network, one or more switches are used to set up a dedicated though temporary connection or circuit for an exchange between two or more parties.

In the open systems Interconnection (OSI) communications model, a switch performs the Layer 2 or Data-link layer

function. That is, it simply looks at each packet or data unit and determines from a physical address (the "MAC address") which device a data unit is intended for and switches it out towards that device. However, in wide area networks such as the Internet, the destination address requires a look-up in a routing table by a device known as a router. Some newer switches also perform routing functions (Layer 3 or the Network layer functions in OSI) and are sometimes called IP switches. On larger networks, the trip from one switch point to another in the network is called a hop. The time a switch takes to figure out where to forward a data unit is called its latency. The price paid for having the flexibility that switches provide in a network is this latency. In the simplest networks, a switch is not required for messages that are sent and received within the network. For example, a local area network may be organized in a token ring or bus arrangement in which each possible destination inspects each message and reads any message with its address.

Bridge

A bridge is a product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or token ring). You can envision a bridge as being a device that decides whether a message from you to someone else is going to the local area network in your building or to someone on the local area network in the building across the street. A bridge examines each message on a LAN, passing those to be within the same LAN and forwarding those known to be on the other interconnected LAN (or LANs).

In bridging networks, computer or node addresses have no specific relationship to location. For this reason, messages are sent out to every address on the network and accepted only by the intended destination node. Bridges learn which addresses are on which network and develops a *learning table* so that subsequent messages can be forwarded to the right network.

Bridging networks are generally always interconnected local area networks since broadcasting every message to all possible destinations would flood a larger network with unnecessary traffic. For this reason, router networks such as the Internet uses a scheme that assigns addresses to nodes so that a message or packet can be forwarded only in one general direction rather than forwarded in all directions. A bridge works at the data-link (physical network) level of a network, copying a data frame from one network to the next network along the communications path. A bridge is sometimes combined with a router in a product called a brouter.

Routers

Routers operate on the Network layer, which is a higher level in the OSI conceptual model. Routers use a combination of software and hardware, but it is used to route data from its source to its destination. Routers actually have a sophisticated OS that allows them to configure various connection ports. You can setup a router to route data packets from different network protocol stacks, which include TCP/IP, IPX/SPX and AppleTalk.

Routers are also used to connect remote LANs together using different WAN technologies. But, when a router has become large, the large network is divided into logical segments called subnets. This division of the network is based on the addressing scheme related to a particular subnet is kept local. The router only forwards data that is meant for the subnets on the extended network.

Routers also help to decide how to forward data packets to their destination based on the routing table. The protocols built into the router's operating system is used to identify neighboring routers and their network addresses. This allows routers to build a routing table.

Brouter

A brouter is a network bridge and a router combined in a single product. A bridge is a device that connects one local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or token ring). If a data unit on one LAN is intended for a destination on an interconnected LAN, the bridge forwards the data unit to that LAN; otherwise, it passes it along the same LAN. A bridge usually offers only one path to a given interconnected LAN. A router connects a network to one or more other networks that are usually part of a wide area network and may offer a number of paths out to destinations on those networks. A router therefore needs to have more information than a bridge about the interconnected networks. It consults a routing table for this information. Since a given outgoing data unit from a computer may be intended for an address on the local network, on an interconnected LAN, or the wide area network, it makes sense to have a single unit that examines all data units and forwards them appropriately.

Gateway

A gateway is a network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node.

In the network for an enterprise, a computer server acting as a gateway node is often also acting as a proxy server and a firewall server. A gateway is often associated with a router, which knows where to direct a given packet of data that arrives at the gateway, and a switch, which furnishes the actual path in and out of the gateway for a given packet.

EXERCISES

Practice Problems I

Directions for questions 1 to 15: Select the correct alternative from the given choices.

1. If TCP RTT is currently 40 m/sec and the following acknowledgements come in after 26, 32 and 24 m/sec respectively. What is the new RTT estimate? $\alpha = 0.9$.
(A) 32.69 (B) 24.31 (C) 36.55 (D) 42.23

2. If a TCP connection is transferring a file of 5000 bytes. The first byte is numbered 1001. What are the sequence numbers for each segment if data is sent in five segments, each carrying 1000 bytes?
(A) 1001, 2001, 3001, 4001, 5001
(B) 1000, 2000, 3000, 4000, 5000
(C) 5000, 6000, 7000, 8000, 9000
(D) 5001, 6001, 7001, 8001, 9001

3. Which of the below statements hold good with respect to routing done by a bridge?
(i) they can route packets using IP addresses
(ii) they use data link layer addresses to do routing
(iii) the LAN route IPv4,IPv6,Apple Talk, ATM, OSI packets
(A) (i), (ii) (B) (ii), (iii)
(C) (i), (iii) (D) (i), (ii), (iii)

4. Match the following:

i	Repeaters	p	connects different nodes of a LAN
ii	Hub	q	amplifies the signal between segments
iii	Switch	r	connects different LANs
iv	Bridge		

(A) i – q ii – r iii – p iv – r
(B) i – r ii – p iii – q iv – q
(C) i – q ii – p iii – p iv – r
(D) i – p ii – p iii – q iv – r

5. Match the following.

i	Retransmission timer	p	goes off when a TCP connection is idle for a long time
ii	Keep-alive timer	q	goes off if sender and receiver are waiting for each other
iii	Persistence timer	r	goes off to trigger the delivery of a segment in case acknowledgement is not received for first attempt

(A) i – r ii – q iii – p
(B) i – q ii – r iii – p
(C) i – p ii – r iii – q
(D) i – p ii – q iii – r

6. In T/TCP (Transactional TCP) what does the packet that is sent by client, consist of?
(i) SYN (ii) REQUEST (iii) FIN
(A) (i), (ii) (B) (ii), (iii)
(C) (i), (iii) (D) (i), (ii), (iii)

7. Assume TCP uses 32-bit sequence numbers and sequence numbers are given to each byte that gets transmitted. If data is transmitted at 1 Gbps. What is the wraparound time for sequence numbers?
(A) 14.4 sec (B) 24.24 sec
(C) 34.36 sec (D) 44.45 sec

8. What are the disadvantages of NAT?
(i) NAT forms link between sender and receiver and then link can be broken irreparably during a connection.
(ii) NAT violates architectural model of IP.
(iii) NAT hacks source port field of TCP header which is of limited size.
(iv) NAT alleviates IP shortage.
(A) (i), (ii), (iii) (B) (ii), (iii), (iv)
(C) (i), (iii), (iv) (D) (i), (ii), (iv)

9. What is the main protocol in the transport layer?
(A) TCP (B) UDP
(C) FTP (D) Both (A) and (B)

10. Number of bytes for header in UDP segment and TCP segment are
(A) 8 bytes, 20 bytes (B) 16 bytes, 16 bytes
(C) 32-bits, 20-bits (D) None of these

11. TCP maintains a variable RTT (Round trip time), for determining the time to reach destination and receiving acknowledgement, the formula for RTT is
(A) RTT = RTT + D
(B) RTT = 4RTT
(C) RTT = αRTT + $(1 - \alpha)$ M ($\alpha = 7/8$)
(D) None of these.

12. Maximum segment size is
(A) The size of the segment without header.
(B) The size of the segment with limit.
(C) The transmission link capacity.
(D) Less than maximum transfer unit.

13. What is meant by silly window syndrome that ruins TCP performance?
(A) This occurs when sender sends data in large blocks and receiver receives in large blocks.
(B) This occurs when sender sends data in large blocks and receiver receives in or reads one byte at a time.
(C) Both (A) and (B)
(D) None of these

Common data for questions 14 and 15: A TCP segment begins with a fixed-format, 20-byte header. The header is followed by reader options. After the options, upto 65,495 bytes of data may follow.

14. Number of one bit flags available in the TCP header are
(A) 5 (B) 6
(C) 2 (D) None of these

15. Which of the flags is used for establishing connections?
(A) PSH (B) ACK (C) URG (D) SYN

Practice Problems 2

Directions for questions 1 to 15: Select the correct alternative from the given choices.

1. Which of the below TCP primitives block a port?
(i) LISTEN (ii) CONNECT (iii) RECEIVE
(A) (i), (ii) (B) (ii), (iii)
(C) (i), (iii) (D) (i), (ii), (iii)

2. In the context of TCP sockets how is a symmetric DISCONNECT different from that of an asymmetric one?
(i) In symmetric DISCONNECT each direction is closed separately.
(ii) In asymmetric DISCONNECT each direction is closed separately.
(iii) In asymmetric DISCONNECT transport user can release the connection
(A) (i), (ii) (B) (ii), (iii)
(C) (i), (iii) (D) (i), (ii), (iii)

3. When does RPC/UDP does not make a good combination?
(i) When the caller and callee machines are separated by small network distance.
(ii) When the parameters of the procedures are too huge in size.
(iii) When the procedure requested cannot be repeated safely as needed.
(A) (i), (ii) (B) (ii), (iii)
(C) (i), (iii) (D) (i), (ii), (iii)

4. Which of the following statements below are true with reference to RTP (Real Time Transport Protocol)?
(i) It multiplexes server real time data stream into a single stream of UDP packets.
(ii) RTP has flow control, error control mechanism.
(iii) RTP has no mechanism for retransmission.
(A) (i), (ii) (B) (ii), (iii)
(C) (i), (iii) (D) (i), (ii), (iii)

5. What does RTCP (real time transport control protocol) accomplish?
(i) Provides feedback on delay, jitter etc to sources.
(ii) Handles introstream synchronization.
(iii) Provides a way to name the sources.
(A) (i), (ii) (B) (ii), (iii)
(C) (i), (iii) (D) (i), (ii), (iii)

6. Which of the following are applicable to TCP?
(i) Breaks the data coming from upper layers into 64 kbyte size packets and transmits them.
(ii) Manages the time out and re-uses them.
(iii) Should reassemble the packets in correct order at receiving end.
(iv) TCP supports multicasting.
(A) (i), (ii), (iii) (B) (ii), (iii), (iv)
(C) (i), (iii), (iv) (D) (i), (ii), (iv)

7. Which of the below statements about sockets is/are true?
(i) For sender and receiver to avail TCP service sockets have to be created.
(ii) Each socket is a 16 bit number local to that host.
(iii) Sockets can involve themselves in one connection at a time.
(iv) Ports below 1024 are reserved.
(A) (i), (ii), (iii) (B) (ii), (iii), (iv)
(C) (iii), (iv), (i) (D) (i), (ii), (iv)

8. What are the functions of application layer?
(A) Mail service provides a basis for electronic mails forwarding and storage
(B) File access transfer and management
(C) Creates virtual terminal that allows us to log onto remote host
(D) All the above

9. Which of the following application uses UDP?
(A) Streaming a multimedia
(B) Client–server interaction
(C) Internet telephony
(D) All the above

10. What are the reasons for choosing an UDP by an application?
(A) No connection establishment
(B) No connection state
(C) Small packet header
(D) All the above

11. TCP uses multiple timers to do its work, the timers are
(A) Retransmission timer
(B) Persistence timer
(C) Keep alive timer
(D) All the above

12. Which of the following is supported by TCP connections?
(A) Full-duplex (B) Point-to-point
(C) Multicasting (D) Both (A) and (B)

13. TCP connection is _____ stream.
(A) Byte (B) Message
(C) Packet (D) None of these.

14. If a sender wants to indicate that, it has no data for the receiver, one of the following bits is set.
(A) PSH (B) RST
(C) FIN (D) ACK

15. If the receiver host is responding by sending a primitive SYN (SEQ = y, ACK = $x + 1$) means
(A) The receiver data sequence number is y.
(B) It has received up to $x + 1$ bytes of data.
(C) Both (A) and (B)
(D) None of these

Previous Years' Questions

1. The transport layer protocols used for real time multimedia, file transfer, DNS and email respectively are **[2013]**

(A) TCP, UDP, UDP and TCP
(B) UDP, TCP, TCP and UDP
(C) UDP, TCP, UDP and TCP
(D) TCP, UDP, TCP and UDP

2. Which one of the following socket API functions converts an unconnected active TCP socket into a passive socket? **[2014]**

(A) Connect (B) Bind
(C) Listen (D) Accept

3. Suppose two hosts use a TCP connection to transfer a large file. Which of the following statements is/are FALSE with respect to the TCP connection? **[2015]**

I. If the sequence number of a segment is m, then the sequence number of the sub sequent segment is always $m + 1$.
II. If the estimated round trip time at any given point of time is t sec, the value of the retransmission timeout is always set to greater than or equal to t sec.
III. The size of the advertised window never changes during the course of the TCP connection.
IV. The number of unacknowledged bytes at the sender is always less than or equal to the advertised window.

(A) III only (B) I and III only
(C) I and IV only (D) II and IV only

4. In one of the pairs of protocols given below, both the protocols can use multiple TCP connections between the same client and the server. Which one is that? **[2015]**

(A) HTTP, FTP (B) HTTP, TELNET
(C) FTP, SMTP (D) HTTP, SMTP

5. Assume that the bandwidth for a TCP connection is 1048560 bits/sec. Let α be the value of RTT in milliseconds (rounded off to the nearest integer) after which the TCP window scale option is needed. Let β be the maximum possible window size with window scale option. Then the values of α and β are **[2015]**

(A) 63 milliseconds, 65535×2^{14}
(B) 63 milliseconds, 65535×2^{16}
(C) 500 milliseconds, 65535×2^{14}
(D) 500 milliseconds, 65535×2^{16}

6. Consider the following statements

1. TCP connections are full duplex
2. TCP has no option for selective acknowledgement
3. TCP connections are message streams

(A) Only 1 is correct
(B) Only 1 and 3 are correct
(C) Only 2 and 3 are correct
(D) All of 1, 2 and 3 are correct

7. Which one of the following protocols is **NOT** used to resolve one form of address to another one? **[2016]**

(A) DNS (B) ARP
(C) DHCP (D) RARP

8. Which of the following is/are example(s) of stateful application layer protocols? **[2016]**

(i) HTTP (ii) FTP
(iii) TCP (iv) POP3

(A) (i) and (ii) only
(B) (ii) and (iii) only
(C) (ii) and (iv) only
(D) (iv) only

9. Identify the correct sequence in which the following packets are transmitted on the network by a host when a browser requests a webpage from a remote server, assuming that the host has just been restarted. **[2016]**

(A) **HTTP GET** request, **DNS** query, **TCP SYN**
(B) **DNS** query, **HTTP GET** request, **TCP SYN**
(C) **DNS** query, **TCP SYN, HTTP GET** request
(D) **TCP SYN**, **DNS** query, **HTTP GET** request

10. Consider a TCP client and a TCP server running on two different machines. After completing data transfer, the TCP client calls **close** to terminate the connection and a FIN segment is sent to the TCP server. Server-side TCP responds by sending an ACK, which is received by the client-side TCP. As per the TCP connection state diagram (RFC 793), in which state does the client-side TCP connection wait for the FIN from the server-side TCP? **[2017]**

(A) LAST-ACK
(B) TIME-WAIT
(C) FIN-WAIT-1
(D) FIN-WAIT-2

11. Consider socket API on a Linux machine that supports connected UDP sockets. A connected UDP socket is a UDP socket on which **connect** function has already been called. Winch of the following statements is/are CORRECT? **[2017]**

I. A connected UDP socket can be used to communicate with multiple peers simultaneously.
II. A process can successfully call **connect** function again for an already connected UDP socket.

(A) I only
(B) II only
(C) Both I and II
(D) Neither I nor II

12. Consider the following statements regarding the slow start phase of the TCP congestion control algorithm. Note that cwnd stands for the TCP congestion window

and MSS denotes the Maximum Segment Size.

(i) The cwnd increases by 2 MSS on every successful acknowledgment.

(ii) The cwnd approximately doubles on every successful acknowledgement.

(iii) The cwnd increases by 1 MSS every round trip time.

(iv) The cwnd approximately doubles every round trip time.

Which one of the following is correct? **[2018]**

(A) Only (ii) and (iii) are true

(B) Only (i) and (iii) are true

(C) Only (iv) is true

(D) Only (i) and (iv) are true

13. Consider a long-lived TCP session with an end-to-end bandwidth of 1 Gbps (= 10^9 bits-per-second). The session starts with a sequence number of 1234. The minimum time (in seconds, rounded to the closest integer) before this sequence number can be used again is _____. **[2018]**

Answer Keys

Exercises

Practice Problems 1

1. C	**2.** A	**3.** B	**4.** D	**5.** A	**6.** D	**7.** C	**8.** A	**9.** D	**10.** A
11. C	**12.** D	**13.** B	**14.** B	**15.** D					

Practice Problems 2

1. C	**2.** C	**3.** B	**4.** C	**5.** D	**6.** A	**7.** D	**8.** D	**9.** D	**10.** D
11. D	**12.** D	**13.** A	**14.** C	**15.** C					

Previous Years' Questions

1. C	**2.** C	**3.** B	**4.** A	**5.** C	**6.** A	**7.** C	**8.** C	**9.** C	**10.** D
11. B	**12.** C	**13.** 34							

Chapter 4

IP(v4)

LEARNING OBJECTIVES

- *IP addressing*
- *Class A*
- *Class B*
- *Class C*
- *Class D*
- *Subnet mask*
- *Classless Inter Domain Routing (CIDR)*
- *Network address*
- *Network Address Translation (NAT)*
- *IP-Protocol*

IP Addressing

Every machine on the internet has a unique identification number, called an IP Address. A typical IP address looks like this:

216.27.61.137

To make it easier for humans to remember, IP addresses are normally expressed in decimal format as a "*dotted decimal number*" like the one above. But computers communicate in binary form. Look at the same IP address in binary:

11011000.00011011.00111101.10001001

The four numbers in an IP address are called octets, because they each have eight positions when viewed in binary form. If you add all the positions together, you get 32, which is why IP addresses are considered 32-bit numbers. Since each of the eight positions can have two different states (1 or 0) the total number of possible combinations per octet is 2^8 or 256. So each octet can contain any value between 0 and 255. Combine the four octets and you get 2^{32} or a possible 4,294,967,296 unique values.

Out of the almost 4.3 billion possible combinations, certain values are restricted from use as typical IP addresses. For example, the IP address 0.0.0.0 is reserved for the default network and the address 255.255.255.255 is used for broadcasts.

The octets serve a purpose other than simply separating the numbers. They are used to create classes of IP addresses that can be assigned to a particular business, government or other entities based on size and need. The octets are split into two sections: Net and Host. The Net section always contains the first octet. It is used to identify the network that a computer belongs to. Host (sometimes referred to as Node) identifies the actual computer on the network. The Host section always contains the last octet. There are five IP classes plus certain special addresses. They are

1. Class A
2. Class B
3. Class C
4. Class D
5. Class E

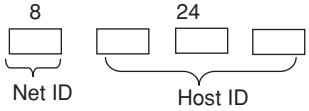
Default Network: The IP address of 0.0.0.0 is used for the default network.

Class A

This class is for very large networks, such as, a major international company. IP addresses with a first octet from 1 to 126 are part of this class. The other three octets are used to identify each host. This means that there are 126 Class A networks each with 16,777,214 ($2^{24} - 2$) possible hosts for a total of 2,147,483,648 (2^{31}) unique IP addresses. Class A networks account for half of the total available IP addresses. In Class A networks, the high order bit value (the very first binary number) in the first octet is always 0.

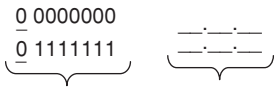
Example:

Net	Host or Node
115.	24.53.107



2^8 – 256 Networks
2^{24} – 1, 67, 77, 216 hosts

- Used for large organizations, e.g., CISCO.
- x.x.x.x/8 – default mask of 8-bits in Network.

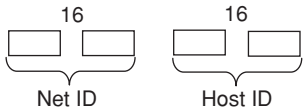


- 1st bit of 1st octet is '0'
- '1' bit is fixed and 2 special addresses are fixed
  ∴ 2^7 – 2 Networks
- All 1's and all 0's are not used in host portion.
  ∴ 2^{24} – 2 hosts

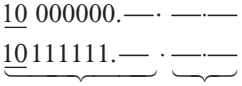
Loopback The IP address 127.0.0.1 is used as the loopback address. This means that it is used by the host computer to send a message back to itself. It is commonly used for troubleshooting and network testing.

Class B

Class B is used for medium-sized networks. A good example is a large college campus. IP addresses with first octet from 128 to 191 are part of this class. Class B addresses also include the second octet as part of the Net identifier. The other two octets are used to identify each host. This means that there are 16,384 (2^{14}) Class B networks each with 65,534 (2^{16} – 2) possible hosts for a total of 1,073,741,824 (2^{30}) unique IP addresses. Class B networks make up a quarter of the total available IP addresses. Class B networks have a first bit value of 1 and a second bit value of 0 in the first octet.



- Used for medium organization eg: universities, medium companies.
- x.x.x.x/16 – default mask of 16 bits in network



- 1st two bits of 1st octet is '10'
- 2 bits fixed. So 2^{14} Networks, 2^{16} – 2 hosts.

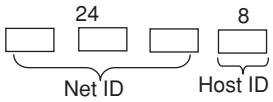
Class C

Class C addresses are commonly used for small to mid-size businesses. IP addresses with a first octet from 192 to 223 are part of this class. Class C addresses also include the second and third octets as part of the Net identifier. The last octet is used to identify each host. This means that there are 2,097,152 (2^{21}) Class C networks each with 254 (2^8-2) possible hosts for a total of 536,870,912 (2^{29}) unique IP addresses. Class C networks make up an eighth of the total available IP addresses. Class C networks have a first bit value of 1, second bit value of 1 and a third bit value of 0 in the first octet.

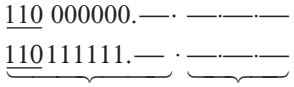
Example:

Net	Host or Node
195.24.53.	107

- Used for small organizations, e.g., colleges



- x.x.x.x/24 – default mask of 24-bits in network.



- 1st 3-bits of 1st octet is '110', So 2^{21} Networks, 2^{24} – 2 hosts.

Class D

Used for multicasts, Class D is slightly different from the first three classes. It has a first bit value of 1, second bit value of 1, third bit value of 1 and fourth bit value of 0. The other 28-bits are used to identify the group of computers the multicast message is intended for. Class D accounts for 1/16th (268,435,456 or 2^{28}) of the available IP addresses.

Example:

Net	Host or Node
224.	24.53.107

- Used for multicasting
- No Net ID or Host ID.
- Whole address is used for multicasting.

Class E

Class E is used for experimental purposes only. Like Class D, it is different from the first three classes. It has a first bit value of 1, second bit value of 1, third bit value of 1 and fourth bit value of 1. The other 28-bits are used to identify the group of computers the multicast message is intended for. Class E accounts for 1/16th (268,435,456 or 228) of the available IP addresses.

Net	Host or Node
240.	24.53.107

Broadcast

- Messages that are intended for all Computers are broadcasted using the IP Address 255.255.255.255.

Notes:

- If we use class of IP address, we waste many IP's So, we use subnetting to save IP's.
- We can use following private addresses to save IP's.
  10.0.0.0 – 10.255.255.255 – class A network
  172.16.0.0. – 172.31.255.255 – 16 class B network
  192.168.0.0 – 192.168.255.255 – 256 class C network.
- Classful addressing is address with default mask.
- Classless address is a address with any other mask that is not default.

Subnet Mask

Mask

The length of the net id and host id is predefined in classful addressing, we can use a mask, also called default mask, which is a 32-bit number made of contiguous 1's followed by contiguous 0's. The masks of classes A, B and C are shown below. Masking is not applicable to class D and class E.

1. Class A mask is
   1111 1111.0000 0000.0000 0000. 0000 0000
   255. 0. 0. 0
   CIDR Representation is '/8'.
2. Class B mask is
   1111 1111.1111 1111.0000 0000.0000 0000
   255. 255. 0. 0
   CIDR Representation is '/16'.
3. Class C mask is
   1111 1111.1111 1111. 1111 1111.0000 0000
   255. 255. 255. 0
   CIDR Representation is '/24'.

The mask will be helpful in finding the netid and the hostid. For Example the mask for class A address has eight 1's, which means the first 8 bits of any address in class A define the netid, the next 24 bits define the hostid.

Subnetting packet structure Internet protocol is layer-3 protocol in OSI, It takes data segments from layer-4 and divides it into packets.

IP packet encapsulates data unit received from above layer and add to its own header information.

IP Header	Layer-4 Data

Figure 1 IP Encapsulation

The encapsulated data is referred to as IP-payload.

Subnetting Each IP-class has its own default mask, which bounds that IP class to have pre fixed number of Networks and prefixed number of Hosts per network.

- CIDR provides the flexibility of borrowing bits of Host part of the IP-address and use them as network within a network, called subnet.
- By using subnetting, one single class A IP-address can be used to have smaller sub networks, that provides better network management.

Class-A subnets

To make more subnets in class A, bits from Host part are borrowed and the subnet mask is changed accordingly.

Table 1 *Possible combination of class-A subnets*

Network bits	Subnet Mask	Bits-borrowed	Subnets	Hosts/ subnet
8	255.0.0.0	0	1	16777214
9	255.128.0.0	1	2	8388606
10	255.192.0.0	2	4	4194302
11	255.224.0.0	3	8	2097150
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
25	255.255.255.128	17	131072	126
27	255.255.255.224	19	524288	30
30	255.255.255.252	22	4194304	2

In case of subnetting also, the first and last IP address of every subnet is used for subnet number and subnet Broadcast IP-address. These 2 IP-addresses cannot be assigned to hosts, subnetting cannot be implemented using more than 30-bits as network bits, because that provides less than 2 hosts per subnet.

Class-B subnets

Class B IP addresses can be subnetted the same way as class-A addresses, that is by borrowing bits from Host bits.

Table 2 *Possible combination of class-B subnets*

Network bits	Subnet Mask	Bits-borrowed	Subnets	Hosts/ subnet
16	255.255.0.0	0	1	65534
17	255.255.128.0	1	2	32766
18	255.255.192.0	2	4	16382
19	255.255.224.0	3	8	8190
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
28	255.255.255.240	12	4096	14
29	255.255.255.248	13	8192	6
30	255.255.255.252	14	16384	2

Class-C subnets

Class C IP-addresses are usually assigned to a very small size network because it can only have 254 Hosts in a network.

Table 3 *Possible combination of class-C subnets*

Network Bits	Subnet Mask	Bits-borrowed	Subnets	Hosts/ subnet
24	255.255.255.0	0	1	254
25	255.255.255.128	1	2	126
26	255.255.255.192	2	4	62
27	25.255.255.224	3	8	30
28	255.255.255.240	4	16	14
29	255.255.255.248	5	32	6
30	255.255.255.252	6	64	2

Classless Inter Domain Routing (CIDR)

The mask shown in the form '/*n*' where '*n*' can be 8, 16, 24 in classful Addressing, This notation is also called slash notation or class less Inter domain Routing (CIDR) notation. This notation is used in class less addressing.

The Internet is rapidly running out of IP addresses. In particular, the problem is with class 'B' network. For most organizations, a class A network, with 16 million addresses is too big, and a class C network, with 256 address is too small.

A class B network with 65, 536, is just right. In reality a class 'B' address is too large for most organizations. It is known that more than half of all class B networks have fewer than 50 hosts.

If the class B address had split, and allocated 20-bits for network number, another problem would have emerged, i.e., the routing table explosion. From the routers point of view, the IP address space is a 2-level hierarchy, with network numbers and host numbers.

One solution is CIDR. The basic Idea behind CIDR, is to allocate the remaining IP addresses in variable – sized blocks, without regard to the classes. If an organization needs 2000 addresses, it is given a block of 2048 address on a 2048-byte boundary.

Dropping the classes makes forwarding more complicated.

In classful addressing system, the forwarding is carried in the following way:

When a packet arrived at a router, a copy of the IP address was shifted right 28 bits to yield a 4-bit class number. A 16-way branch then sorted packet into A, B, C with eight of the cases for class *A*, four of the cases for class B, 2 of the cases for class 'C'. The code for each class then masked off the 8-, 16-, 24-bit network number and right aligned it in a 32-bit word. The network number was then looked up in the A, B or C table, by indexing for *A* and *B* networks and hashing for *C* networks. Once the entry was found, the outgoing line could be looked up and the packet forwarded.

The above described algorithm will not work for CIDR, Instead, each routing table entry is extended by giving it a 32-bit mask. There is only a single routing table for all networks. Consisting of an array of (IP-address, subnet mask, outgoing line) triples.

When a packet comes, its destination IP-address is first extracted. Then the routing table is scanned entry by entry, masking the destination address and comparing it to the table entry looking for a match.

It is possible that multiple entries match, in which case the longest mask is used. Thus, if there is a match for a/20 mask and a/24 mask, the/24 entry is used.

Complex algorithms have been devised to speed up the address matching process.

To overcome address depletion and give more organizations access to the internet, classless addressing was designed and implemented. In this scheme, there are no classes, but the addresses are still granted in blocks.

In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block of addresses. The size of the block varies based on the nature and size of the entity. For example, household may be given only 2 addresses, a large organization may be given thousands of addresses. An ISP(Internet Service Provider) provides addresses to customers.

To simplify the handling of addresses, the Internet authorities impose 3 restrictions on class less address blocks:

1. The addresses in a block must be contiguous.
2. The number of addresses in a block must be a power of 2 (1, 2, 4, 8, 16, …).
3. The first address must be evenly divisible by the number of addresses.

A better way to define block of addresses is to select any address in the block and the mask. In classless addressing the mask for a block can take any value from 0 to 32.

In IPv4 addressing, a block of addresses can be defined as

$$x\,.\,y\,.\,z\,.\,w/n$$

in which *x.y.z.w* defines one of the addresses and the/*n* defines the mask.

The address and the/*n* notation completely define the whole block (First block address, Last address and the number of addresses)

First Address The first address in the block can be found by setting the (32-*n*) right most bits in the binary notation of the address to Zeros.

Solved Examples

Example 1: A block of addresses is granted to a small organization, We know that one of the addresses is 209.17.38.40/28, what is the first address in the block?

Solution 1: The binary representation of the given address is: 209.17.38.40

11010001.00010001.00100110.00101000

If we set (32-*n*) = 32 – 28 = 4 right most bits to '0', we get

11010001.00010001.00100110.00100000

First address:

209. 17. 38. 32

Solution 2: Another way to find the first address is to represent the mask as a 32-bit binary number.
'/28' can be represented as

11111111.11111111.11111111.11110000

(28 ones and 4 zeros)

The first address can be found by ANDing the given address with the mask.
Address: 11010001.00010001.00100110.00101000
Mask: 11111111.11111111.11111111.11110000
First Address:

11010001.00010001.00100110.00100000

209. 17. 38. 32

Last address and number of addresses The last address in the block can be found by setting the $(32-n)$ right most bits in the binary notation of the address to 1's.

Example 2: Find the last address and Number of addresses in the block, for the given CIDR, in the above example?

Solution 1: The binary representation of the given address is

11010001.00010001.00100110.00101111

If we set $(32-n) = (32-28) = 4$ right most bits to 1, we get

11010001.00010001.00100110.00101111

209. 17. 38. 47

Solution 2: Another way to find the last address is by ORing the given address with the complement of the mask. The complement of a number is found by changing each 1 to 0 and each 0 to 1.
Address:11010001.00010001.00100110.00101000
Mask Complement:

00000000.00000000.00000000.00001111

Last Address:

11010001.00010001.00100110.00101111

209. 17. 38. 47

Number of Addresses The number of addresses in the block is the difference between the last and first address. It can be found using formula 2^{32-n}. The value of n is 28, which means that number of addresses is $2^{32-28} = 2^4 = 16$

The number of addresses can also be found by complementing the mask, interpreting it as a decimal number, and adding 1 to it.

Mask Complement:

00000000.00000000.00000000.00001111

Number of addresses: 15 + 1 = 16

Example 3: Suppose that a University-1 needs 2048 addresses and is assigned the addresses 184.26.0.0 through 184.26.7.255, along with mask 255.255.248.0. Next University-2 asks for 4096 addresses. Since a block of 4096 must lie on a 4096-byte boundary, they cannot be given addresses starting at 184.26.8.0. Instead, they get 184.26.16.0 through 184.26.31.255 along with subnet mask 255.255.240.0. University-3 asks for 1024 addresses and is assigned addresses 184.26.8.0 through 184.26.11.255 and mask 255.255.252.0. These assignments are summarized in below table:

University	First Address	Last Address	Number of Addresses	Written as
University-1	184.26.0.0	184.26.7.255	2048	184.26.0.0/21
University-3	184.26.8.0	184.26.11.255	1024	184.26.8.0/22
Available	184.26.12.0	184.26.15.255	1024	184.26.12.0/22
University-2	184.26.16.0	184.26.31.255	4096	184.26.16.0/20

What are the masks for three universities?

Solution:
University-1 Address 184.26.0.0

10111000.00011010.00000000.00000000

Mask: 11111111.11111111.11111000.00000000
University-2 Address 184.26.16.0

10111000.00011010.00010000.00000000

Mask: 11111111.11111111.11110000.00000000
University-3 Address 184.26.8.0

10111000.00011010.00001000.00000000

Mask: 11111111.11111111.11111100.00000000
What happens when a packet comes in addressed to 184.26.17.4?

Solution:
The process has address 184.26.17.4

The binary representation of 184.26.17.4 is

10111000.00011010.00010001.00000100

First it is Boolean ANDed with University-1 mask which gives

10111000.00011010.00010001.00000100
11111111.11111111.11111000.00000000
10111000.00011010.00010000.00000000
184. 26. 16. 0

This value does not match the base address of University-1, so the original address is next ANDed with University-2 mask which gives

10111000.00011010.00010001.00000100
11111111.11111111.11110000.00000000
10111000.00011010.00010000.00000000
184. 26. 16. 0

This value does not match the University-2 base address. Finally original address is ANDed with University-3

10111000.00011010.00010001.00000100
11111111.11111111.11111100.00000000
10111000.00011010.00010000.00000000
= 184. 26. 16. 0

The University-3 entry is used and the packet is sent along the line named in it.

Network Address

When an organization is given a block of addresses, the organization is free to allocate the addresses to the devices that need to be connect to the Internet. The first address in the class is treated as a special address. The first address is called the network address and defines the organization network. First address is the one that is used by routers to direct the message sent to the organization from the outside.

Two-level Hierarchy Without Subnetting

An IP-address can be only 2 levels of hierarchy when not subnetted. The n left most bits of the address $x.y.z.w/n$ define the network (organization network), the $(32-n)$ right most bits define the particular host (computer or router) to the network. The 2 common terms are prefix and suffix. The part of the address that defines the network is called the prefix; the part that defines the host is called the suffix.

Prefix is common to all addresses in the network; the suffix changes from one device to another.

Three-level of Hierarchy with Subnetting

An organization that is granted a large block of addresses may want to create clusters of networks called subnets and divide the address between the different subnets. The rest of the world still sees the organization as one entity. Internally there are several subnets. All messages are sent to the router address that connects the organization to the rest of the Internet; the router routes the message to the appropriate subnets.

The organization, needs to create small sub blocks of addresses, each assigned to specific subnets. The organization has its own mask; each subnet must also have its own.

Example 4: Suppose an organization is given the block 19.18.50.0/26, which contains 64 addresses. The organization has 3 offices and needs to divide the addresses into 3 sub blocks of 32, 16 and 16 addresses. Find the new masks for all the 3 sub blocks?

Solution: First subnet has to be allocated 32 addresses. Suppose the mask for the first subnet is n_1, then 2^{32-n_1} must be 32, which means $n_1 = 27$

$$(\therefore \quad 2^{32-n_1} = 2^5)$$

Second subnet has to be allocated 16 addresses suppose the mask for the second subnet is n_2, then 2^{32-n_2} must be 16, $n_2 = 28$

$$(\therefore \quad 2^{32-n_2} = 2^4)$$

Suppose the mask for third subnet is n_3, then 2^{32-n_3} must be 16, $n_3 = 28$

$$(\therefore \quad 2^{32-n_3} = 2^4)$$

We have the masks 27, 28, 28 with the organization mask being 26.

Network Address Translation (NAT)

NAT enables a user to have a large set of addresses internally and one address, or a small set of addresses, externally. To separate the addresses used inside the home or business and the ones used for the Internet, the Internet authorities have reserved three sets of addresses as private addresses.

Range	Total
10.0.0.0 to 10.255.255.255	2^{24}
172.16.0.0 to 172.31.255.255	2^{20}
192.168.0.0 to192.168.255.255	2^{16}

Figure 2 Addresses for private networks

Any organization can use an address out of this set without permission from the Internet Authorities. These reserved addresses are for private networks. They are unique inside the organization, but they are not unique globally.

No Router will forward a packet that has one of these addresses as the destination address.

IP-Protocol

The job of Internet protocol is to provide a best effort to transport datagrams from source to destination, without regard to whether these machines are on the same network or other networks.

- Communication in the Internet works as follows. The transport layer takes data streams and breaks them up into datagrams.
- Datagrams can be upto 64 kbytes each, but in practice they are usually not more than 1500 bytes (so that the datagrams fit in one Ethernet frame). Each datagram is transmitted through the Internet, being fragmented into smaller units as it goes. When all the pieces finally get to the destination machine, they are reassembled by the network layer into the original datagram.
- An IP datagram consists of a header part and a text part. The header has a 20-byte fixed part and a variable length optional part.
- It is transmitted in big endian order: from left to right, with the high-order bit of the version field going first.

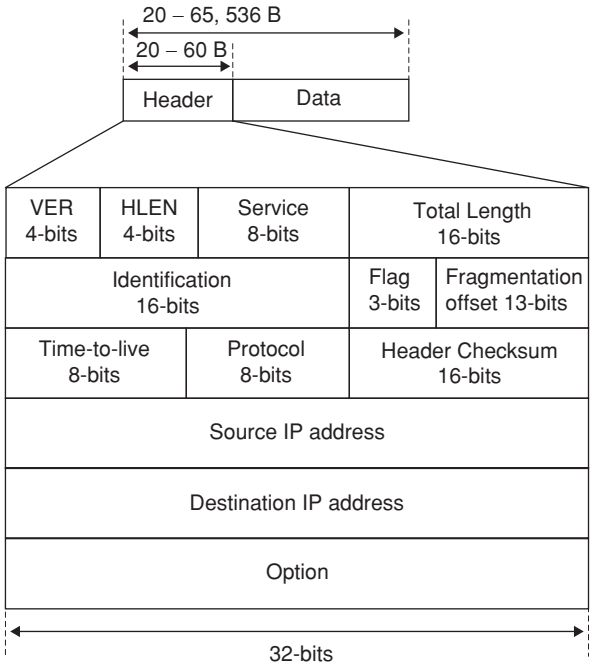


Figure 3 IP(v4) datagram format

The Internet protocol version 4(IPv4) is the delivery mechanism used by the TCP/IP protocols.

- IPv4 is an unreliable and connection less datagram protocol.
- IPv4 provides no error control or flow control (Expect for error detection on the header).
- If reliability is important, IPv4 must be paired with a reliable protocol such as TCP.
- IPv4 is connection less protocol for a packet-switching network that uses the datagram approach. This means that each datagram can follow a different route to the destination. This implies that datagrams sent by the same source to the same destination could arrive out of order. Some of them could be lost or corrupted during transmission. Again, IPv4 relies on a higher-level protocol to take care of all these problems.
- A datagram is a variable-length packet consisting of 2-parts: Header and Data.

The header is 20 to 60 bytes in length and contains information essential to routing and delivery.

The fields of IPv4 are:

Version (VER)

This 4-bit field defines the version of the IPv4 protocol. Currently the version is 4.This field tells the IPv4 software running in the processing machine that the datagram has the format of version 4. All fields must be interpreted as specified in the fourth version of the protocol. If the machine is using some version of IPv4, the datagram is discarded rather than interpreted incorrectly.

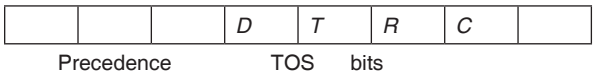
Header Length: (HLEN)

This 4-bit defines the total length of the datagram header in 4-byte words. This field is required because the length of the header is variable (between 20 and 60 bytes). When there are no options, the header length is 20 bytes, and the value of this field is 5($5 \times 4 = 20$). When the options field is at its maximum size, the value of this field is 15($15 \times 4 = 60$).

Services

This 8-bit field, previously called service type, is now called differentiated services. Both Interpretations are given below.

1. Service Type:



D: Minimize delay
R: Maximize reliability
T: Maximize throughput
C: Minimize cost

In this interpretation, the first 3-bits are called precedence bits. The next 4-bits are called Type-of-service (TOS) bits, and the last bit is not used.

Precedence Precedence is a 3-bit sub field ranging from 0(000 binary) to 7(111 binary) precedence is used to give priority to the datagram in issues such as congestion. If a router is congested and needs to discard some datagrams, the datagrams with lowest precedence are discarded first.

Example: A datagram used for network management is much more important than a datagram containing optional information for a group.

The precedence sub field was part of version 4, but never used.

TOS bits It is a 4-bit sub field with each bit having a special meaning. One and only one of the bits can have the value of 1 in each datagram. The bit pattern interpretation and their services are given below.

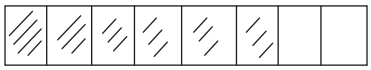
TOS Bits	Description
0000	Default
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

Figure 4 Types of service

- Interactive activities, Activities requiring immediate attention, and activities requiring immediate response need minimum delay.
- Activities that send bulk data require maximum throughput.

- Management activities need maximum reliability
- Background activities need minimum cost.

2. Differentiated Services:



The first 6-bits make up the code point sub field, and the last 2-bits are not used. The code point sub field can be used in two different ways.

1. When the 3 rightmost bits are 0's,the 3 leftmost bits are interpreted the same way as the precedence bits in the service type interpretation.
2. When the 3 rightmost bits are not all 0s, the 6 bits define 64 services based on the priority assignment by the Internet Authorities.

Total length

This is a 16-bit field that defines the total length (header plus data) of the IPv4 datagram in bytes. To find the length of the data coming from the upper layer, subtract the header length from the total length. The header length can be found by multiplying the value in the HLEN field by 4.

∴ Length of data = Total Length – Header Length.

The field length is 16-bits, the total length of the IPv4 datagram is limited to 65,535 ($2^{16} - 1$) bytes, of which 20 to 60 bytes are the header and the rest is data from the upper layer.

- The total length field defines the total length of the datagram including the header.
- If the size of an IPv4 datagram is less than 46 bytes, some padding will be added to meet this requirement. In this case, when a machine decapsulates the datagram, it needs to check the total field to determine how much is really data and how much is padding.

Fragmentation fields

The fields that are related to fragmentation and reassembly of an IPv4 datagram are

1. Identification
2. Flags
3. Fragmentation offset

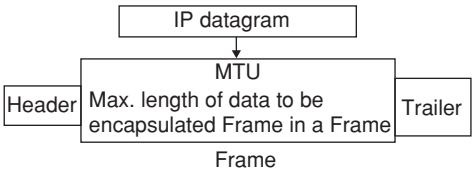
Fragmentation

A datagram can travel through different networks. Each router decapsulates the IPV4 datagram from the frame it receives, processes it, and then encapsulates it in another frame. The size and format of the received frame depends on the protocol used by the physical network through which the frame has travelled. The format and size of the sent frame depend on the protocol used by the physical network through which the frame is going to travel.

Example: If a router connects a LAN to a WAN, it receives a frame in the LAN format and sends a frame in the WAN format.

Maximum transfer unit (MTU)

When a datagram is encapsulated in a frame, the total size of the datagram must be less than this maximum size. The value of the MTU depends on the physical network protocol.



Following table shows MTU's for some networks.

Protocol	MTU
Hyper Channel	65,535
Token Ring(16Mbps)	17,914
Token Ring(4Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

To make the IPv4 protocol independent of the physical network, the designers decided to make the maximum length of the IPV4 datagram equal to 65,535 bytes.

This makes transmission more efficient if we use a protocol with an MTU of this size. But, for other physical network, we must divide the datagram to make it possible to pass through these networks. This is called Fragmentation.

- When a datagram is fragmented, each fragment has it own header with most of the fields repeated.
- A fragmented datagram may itself be fragmented if it encounters a network with an even smaller MTU.
- A datagram can be fragmented several times before it reaches the final destination.
- The host or router that fragments a datagram must change the values of three fields.
  - Flags
  - Fragmentation offset
  - Total length

The rest of the fields must be copied. The value of the checksum must be recalculated regardless of fragmentation.

Identification This 16-bit field identifies a datagram originating from the source host. The combination of the identification and source IPv4 address must uniquely define a datagram as it leaves the source host.

To guarantee uniqueness, the IPv4 protocol uses a counter to label the datagrams.

The counter is initialized to a positive number. When the IPv4 protocol sends a datagram, it copies the current value of the counter to the identification field and increments the counter by 1.

As long as the counter is kept in the main memory uniqueness is guaranteed.

When a datagram is fragmented, the value in the identification field is copied to all fragments.

All fragments have the same identification number, the same as the original datagram.

The identification number helps in reassembling the datagram at destination side.

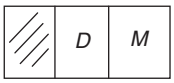
Flags This is a 3-bit field, the first bit is reserved.

The second bit is called the 'do not fragment' bit. If its value is 1, the machine must not fragment the datagram.

If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host.

If its value is '0', the datagram can be fragmented if necessary.

The 3rd bit is called the more fragment bit. If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one. If its value is 0, it means this is the last or only fragment.



D: Do Not Fragment
M: More Fragments

Fragmentation offset This is a 13-bit field, shows the relative position of this fragment with respect to the whole datagram.

Example: A datagram with a data size of 4000 bytes fragmented into three fragments. The bytes in the original datagram are numbered 0 to 3999.

1. The first fragment carries bytes 0 to 1399. The offset for this datagram is 0/8 = 0.
2. The second fragment carries bytes 1400 to 2799; the offset values for this fragment is 1400/8 = 175.
3. The third fragment carries bytes 2800 to 3999. The offset value for this fragment is 2800/8 = 350
   - All fragment datagrams follow different paths to reach destination.
   - Even though each fragment follows a different path and arrives out of order, the final destination host can reassemble the original datagram from the fragments received by using the following strategy:
     - The first fragment has an offset field Value of zero
     - Divide the length of the first fragment by 8.The second fragment has an offset value equal to that result.
     - Divide the total length of the first and second fragments by 8. The third fragment has an offset value equal to that result.
     - The last fragment has a more bit value of 0.

Time-to-live

This field was originally designed to hold a time stamp, which was decremented by each visited router. The datagram was discarded when the value became zero.

This field is used mostly to control the maximum number of hops (routers) visited by the datagram, When a source host sends the datagram, it stores a number in this field. This value is approximately 2 times the maximum number of routes between any 2 hosts.

Each router that processes the datagram decrements this number by 1. If this value becomes zero, the router discards the datagram.

This field limits the lifetime of a datagram and avoids loops (A datagram may travel between 2 or more routers for a long time without ever getting delivered to the destination host)

Protocol

This 8-bit field defines the higher-level protocol that uses the services of the IPv4 layer.

- An IPv4 datagram can encapsulate data from several higher-level protocols such as TCP, UDP, ICMP and IGMP.
- The field specifies the final destination protocol to which the IPv4 datagram is delivered.

Source address This 32-bit field defines the IPv4 address of the source. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.

Destination address

This 32-bit field defines the IPv4 address of the destination. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.

Example 5: An IPv4 packet has arrived with the first 8-bits as shown,

01000100

Will the packet be discarded?

Solution: There is an error in this packet.

The 4 left most bits (0100) show the version, which is correct. The next 4 bits (0100) show an invalid header length (4 × 4 = 16)

The minimum number of bytes in the header must be 20. The receiver discards the packet.

Example 6: In an IPv4 packet, the value of HLEN is 1100 in binary. How many bytes of options are being carried by this packet?

Solution: The HLEN value is 12, which means the total number of bytes in the header is 12 × 4 = 48 bytes. The first 20 bytes are the base header, the next 28 bytes are the options.

Example 7: In an IPv4 packet, the value of HLEN is 5 and the value of the total length field is 0 x 0038. How many bytes of data are being carried by this packet?

Solution: Then HLEN value is 5, which means the total number of bytes in the header is 5 × 4 = 20 bytes (no options). The total length is $(16^1 \times 3 + 16^0 \times 8) = 48 + 8 = 56$.

Which means the packet is carrying 36 bytes of data. ∵ (56 – 20) = 36

Option: The header of the IPv4 datagram is made of 2 parts:

1. Fixed part
2. Variable part

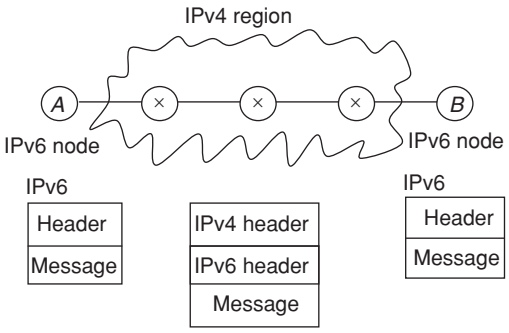
The fixed part is 20 bytes long. The variable part comprises the options that can be a maximum of 40 bytes.

Options, as the name implies, are not required for a datagram. They can be used for network testing and debugging.

Tunneling

If two computers are using IPv6, and want to communicate across the region using IPv4, then Tunneling concept is used.

To pass a packet using IPv6 across a region using IPv4, packet should have IPv4 address. So, IPv6 packet is encapsulated in IPv4 packet, once the packet leaves region it leaves its capsule.



Tunneling cannot be used for translation of IPv6 address to IPv4 address.

Types of tunneling

There are two types of tunneling methods (Corresponding to VPN]

1. End to End tunneling
2. Node to Node tunneling

End to end tunneling acts an interface between LAN and Internet. It is used in Remote access VPN connection.

Node to node tunneling acts as an interface between nodes which are present at an edge of a private network. It is mostly used in the site to site VPN connection.

The other types of tunneling are

1. Layer 2 tunneling (Data link layer)
3. Layer 3 tunneling (Network layer)

Based on the tunneling protocol used for data encapsulation we have different tunneling methods.

Layer 2 tunneling protocol uses frames for encapsulating message it is mostly used in point to point tunnels between client and VPN server.

Layer 3 tunneling protocol adds a new IP header to the packet, it is mostly used for connecting two or more private networks.

Exercises

Practice Problems I

Directions for questions 1 to 15: Select the correct alternative from the given choices.

1. Consider the given IP address, 156.216.24.65 with a subnet mask of 7-bits, what are the number of hosts and subnets?
(A) 512, 128 (B) 510, 126
(C) 511, 127 (D) 509, 125

2. IP address is 198.250.144.23 and mask is 255.255.255.240, find the class, network mask length and broadcast address?
(A) 128,198.250.144.31
(B) 26,198.250.144.63
(C) 30,198.250.144.3
(D) 32,198.250.144.0

3. If subnet addresses are
129.253.4.0, 129.253.8.0, 129.253.12.0, 129.253.16.0
What is subnet mask?
(A) 129.253.7.0 (B) 129.253.31.0
(C) 129.253.192.0 (D) 129.253.252.0

4. For a given source IP 192.16.9.10 and destination network 10.0.0.0, match the following:

i	Network address	P	127.0.0.5
ii	Directed broadcast address	Q	0.0.0.5
iii	Limited broadcast address	R	0.0.0.0.
iv	This host on this network	S	255.255.255.255
v	Specific host on this network	T	10.255.255.255
vi	Loop back address	U	192.16.9.0

Find out all related addresses given above?
(A) i – U, ii – R, iii – Q, iv – S, v – T, vi – P
(B) i – R, ii – Q, iii – P, iv – T, v – S, vi – U
(C) i – U, ii – T, iii – S, iv – R, v – Q, vi – P
(D) i – U, ii – T, iii – S, iv – Q, v – R, vi – P

Common data questions 5 and 6: Consider the routing table below:

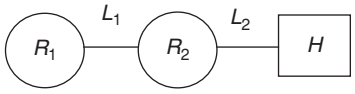
Destination	Gateway	Mask	Flags	Interface
165.230.198.64	165.230.198.119	255.255.255.192	U	eth0
192.168.1.0	192.168.1.1	255.255.255.0	U	eth1
127.0.0.0	127.0.0.1	255.0.0.0	U	Loop back 0
Default	165.230.198.65	255.255.255.255	UG	eth0

5. How many local subnets is this machine attached to?
(A) 0 (B) 1
(C) 2 (D) 3

6. How many IP addresses can this machine reach to (excluding the loop back route)?
(A) 64 (B) 256
(C) 320 (D) 192

7. If a packet is of size 1000 bytes and network span 15 km and speed of propagation is 70% of speed of light. What is the throughput of the system?
(A) 58 Mbps (B) 60 Mbps
(C) 56 Mbps (D) 54 Mbps

Common data for questions 8 and 9: The diagram shows router R_1 sending a datagram to host H through Router R_2.



Link L_1 permits a maximum transfer unit of 1500 bytes. Link L_2 only permits a maximum transfer unit of 1100 bytes. A is an IP datagram which

(i) Has size 4000 bytes (The size of the datagram includes the header of 20 bytes).
(ii) Is not using any of the option field in the header. A must be fragmented as it is sent from R_1 to H. Assume that all datagrams are received successfully.

8. The sizes of IP datagram A is fragmented in sending it from R_1 to R_2 over L_1 are
(A) 1500, 1500, 1500
(B) 1500, 1500, 1060
(C) 1500, 1500, 1100
(D) 1500, 1500, 1040

9. The number of IP datagrams received by H are
(A) 6 (B) 5
(C) 4 (D) 3

Common data for questions 10 and 11: In a network, system packet size is 2 kB, propagation time is 30 milliseconds and channel capacity is 10^6 bits/sec.

10. What will be the transmission time?
(A) 21 microsecond (B) 16.3 microsecond
(C) 18.3 millisecond (D) 16.3 millisecond

11. What is the channel utilization of sender?
(A) 21% (B) 12%
(C) 16% (D) 30%

12. In an IPv4 header fragment offset is set to a size of 13 bits. If the maximum size of datagram is 64 kB, what is the maximum number of fragments possible?
(A) 8191 (B) 8192
(C) 13 (D) 12

13. A packet arriving at main router is addressed to 95.80.15.6. The subnet mask used is 255.255.252.0/22. What is the resultant address?
(A) 95.80.255.0 (B) 95.80.24.0
(C) 95.80.12.0 (D) 95.80.6.6

14. What does 'record route' option signify in an IP header?
(A) Routes that processed the packet, stores the packet details in local memory.
(B) Follow the path already available without further use of any routing algorithm.
(C) Make each router append its IP address to the packet in transit.
(D) Make routers inform the source about the path taken.

15. Which of the following address is used or reserved for loop back testing?
(A) 0. 0. 0. 0
(B) 1. 1. 1. 1
(C) 127.*xx.yy.zz*
(D) None of these

Practice Problems 2

Directions for questions 1 to 15: Select the correct alternative from the given choices.

1. The internet layer of TCP/IP model is similar to _____ layer of OSI model
(A) Transport layer (B) Session layer
(C) Presentation layer (D) Network layer

2. Consider the following statements:

S_1: A system can have multiple IP addresses.

S_2: A system can have multiple physical addresses.

Which one of the following is correct?
(A) Both S_1 and S_2 are true
(B) Both S_1 and S_2 are false
(C) S_1 is true, S_2 is false
(D) S_2 is true, S_1 is false

3. Time to live (TTL) Field in IP header is used
(A) To avoid infinite loops.
(B) To Fragment the packets in the subnet.
(C) To calculate the shortest path from source and destination.
(D) None of these

4. Match the following IP header fields to their functionalities.

i	DF	p	Indicates if there are more fragments
ii	MF	q	Indicates the transport process to which packets need to be given
iii	Protocol	r	If this bit is set routers are not supposed to fragment
iv	Header Checksum	s	Needed to relate all the fragments of a datagram
v	Identification value	t	Can vary from hop to hop

(A) i – q, ii – p, iii – t, iv – r, v – s
(B) i – p, ii – q, iii – s, iv – t, v – r
(C) i – s, ii – p, iii – r, iv – q, v – t
(D) i – r, ii – p, iii – q, iv – t, v – s

5. The header part of IP contains _____ bytes fixed part.
(A) 20 (B) 24
(C) 16 (D) 60

6. The header checksum in the IP header is used to verify
(A) Only header
(B) Only data
(C) Both (A) and (B)
(D) None of these

7. The source address length in IPv4 is
(A) 8 bytes (B) 16 bytes
(C) 32-bits (D) 16-bits

8. The highest IP address in digital notation is
(A) 255 . 0 . 0 . 0
(B) 255 . 255. 0 . 0
(C) 255 . 255 . 255 . 0
(D) 255 . 255 . 255 . 255

9. Which type address class is used for multicast address?
(A) Class A (B) Class B
(C) Class C (D) Class D

10. In the leaky bucket algorithm, the leaky bucket means _____
(A) Infinite buffer.
(B) Finite internal queue.
(C) Constant service time.
(D) Both (B) and (C)

11. The mechanism of leaky bucket algorithm
(A) Reduces congestion.
(B) Turns uneven flow of packet into even flow.
(C) Smoothens out bursts.
(D) All the above.

12. In the IP protocol header we have two one bit flags DF and MF.
What are the uses of DF bit flag?
(A) DF (means don't fragment) orders router not to fragment the packet.
(B) DF is set when the destination is incapable of putting the pieces back together again.
(C) Both (A) and (B)
(D) None of the above

13. In the IPv4 header, what is the maximum value of total length field?
(A) 60 bytes
(B) 255 bytes
(C) 576 bytes
(D) 65535 bytes

14. What are the characteristics of a flow specification input?
(A) Maximum packet size (bytes).
(B) Token bucket rate (bytes/sec).
(C) Token bucket size (bytes)
(D) All the above

15. Standard protocols like HTTP, SMTP, NNTP are part of
(A) Presentation layer
(B) Application layer
(C) Session layer
(D) Not part of any layer

Previous Years' Questions

1. Suppose computers A and B have IP addresses 10.105.1.113 and 10.105.1.91 respectively and they both use the same net mask *N*. Which of the values of N given below should not be used if A and B should belong to the same network? **[2010]**

(A) 255.255.255.0 (B) 255.255.255.128
(C) 255.255.255.192 (D) 255.255.255.224

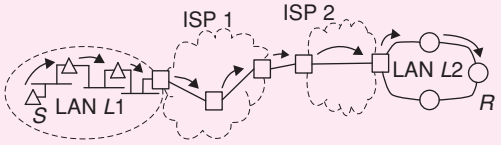
2. In the IPv4 addressing format, the number of networks allowed under class C addresses is **[2012]**

(A) 2^{14} (B) 2^{7}
(C) 2^{21} (D) 2^{24}

3. In an IPv4 datagram, the *M*-bit is 0, the value of HLEN is 10, the value of total length is 400 and the fragment offset value is 300. The position of the datagram, the sequence numbers of the first and the last bytes of the payload, respectively are **[2013]**

(A) Last fragment, 2400 and 2789
(B) First fragment, 2400 and 2759
(C) Last fragment, 2400 and 2759
(D) Middle fragment, 300 and 689

4. In the diagram shown below, *L*1 is an Ethernet LAN and *L*2 is a Token-Ring LAN. An IP packet originates from sender S and traverses to *R*, as shown. The links within each ISP and across the two ISPs, are all point-to-point optical links. The initial value of the TTL field is 32. The maximum possible value of the TTL field when R receives the datagram is ————. **[2014]**



5. Host *A* (on TCP/IPv4 network *A*) sends an IP datagram *D* to host *B* (also on TCP/IPv4 network *B*). Assume that no error occurred during the transmission of *D*. When *D* reaches *B*, which of the following IP header field(s) may be different from that of the original datagram *D*? **[2014]**

(i) TTL (ii) Checksum
(iii) Fragment Offset
(A) (i) only (B) (i) and (ii) only
(C) (ii) and (iii) only (D) (i), (ii), and (iii)

6. An IP router implementing Classless Inter-Domain Routing (CIDR) receives a packet with address 131.23.151.76. The router's routing table has the following entries:

Prefix	Out Interface Identifier
131.16.0.0/12	3
131.28.0.0/14	5
131.19.0.0/16	2
131.22.0.0/15	1

The identifier of the output interface on which this packet will be forwarded is _____. **[2014]**

7. Every host in an IPv4 network has a 1-second resolution real-time clock with battery backup, each host needs to generate up to 1000 unique identifiers per second. Assume that each host has a globally unique IPv4 address. Design a 50-bit globally unique ID for this purpose. After what period (in seconds) will the identifiers generated by a host wrap around? **[2014]**

8. Which one of the following fields of an IP header is NOT modified by a typical IP router? **[2015]**

(A) Checksum (B) Source address
(C) Time to Live (TTL) (D) Length

9. Consider the following routing table at an IP router:

Network No.	Net Mask	Next Hop
128.96.170.0	255.255.254.0	Interface 0
128.96.168.0	255.255.254.0	Interface 1
128.96.166.0	255.255.254.0	R2
128.96.164.0	255.255.252.0	R3
0.0.0.0	Default	R4

For each IP address in Group I identify the correct choice of the next hop from Group II using the entries from the routing table above. **[2015]**

Group I	Group II
i) 128.96.171.92	a) Interface 0
ii) 128.96.167.151	b) Interface 1
iii) 128.96.163.151	c) R2
iv) 128.96.165.121	d) R3
	e) R4

(A) i–a, ii–c, iii–e, iv–d (B) i–a, ii–d, iii–b, iv–e
(C) i–b, ii–c, iii–d, iv–e (D) i–b, ii–c, iii–e, iv–d

10. Host A sends a UDP datagram containing 8880 bytes of user data to host B over an Ethernet LAN. Ethernet frames may carry data upto 1500 bytes (i.e., MTU = 1500 bytes). Size of UDP header is 8 bytes and size of IP header is 20 bytes. There is no option field in IP header. How many total number of IP fragments will be transmitted and what will be the contents of offset field in the last fragment?

(A) 6 and 925 (B) 6 and 7400
(C) 7 and 1110 (D) 7 and 8880

11. In the network 200.10.11.144/27, the fourth octet (in decimal) of the last IP address of the network which can be assigned to a host is _____ **[2015]**

12. An IP datagram of size 1000 bytes arrives at a router. The router has to forward this packet on a link whose MTU (maximum transmission unit) is 100 bytes.

Assume that the size of the IP header is 20 bytes.

The number of fragments that the IP datagram will be divided into for transmission is _____. **[2016]**

13. For the IEEE 802.11 MAC protocol for wireless communication, which of the following statements is/ are **TRUE**? **[2016]**

I. At least three non-overlapping channels are available for transmissions.

II. The RTS-CTS mechanism is used for collision detection.

III. Unicast frames are ACKed.

(A) All I, II and III (B) I and III only

(C) II and III only (D) II only

14. The maximum number of IPv4 router addresses that can be listed in the record route (RR) option field of an IPv4 header is_____. **[2017]**

15. Match the following:

	Field		Length in bits
P.	UDP Header's Port Number	I.	48
Q.	Ethernet MAC Address	II.	8
R.	IPv6 Next Header	III.	32
S.	TCP Header's Sequence Number	IV.	16

[2018]

(A) P-III, Q-IV, R-II, S-I

(B) P-II, Q-I, R-IV, S-III

(C) P-IV, Q-I, R-II, S-III

(D) P-IV, Q-I, R-III, S-II

16. Consider an IP packet with a length of 4,500 bytes that includes a 20-byte IPv4 header and a 40-byte TCP header. The packet is forwarded to an IPv4 router that supports a Maximum Transmission Unit (MTU) of 600 bytes. Assume that the length of the IP header in all the outgoing fragments of this packet is 20 bytes. Assume that the fragmentation offset value stored in the first fragment is 0.

The fragmentation offset value stored in the third fragment is _____. **[2018]**

Answer Keys

Exercises

Practice Problems 1

1. B	**2.** A	**3.** D	**4.** A	**5.** C	**6.** C	**7.** C	**8.** D	**9.** B	**10.** D
11. A	**12.** B	**13.** C	**14.** C	**15.** C					

Practice Problems 2

1. D	**2.** C	**3.** A	**4.** D	**5.** A	**6.** A	**7.** C	**8.** D	**9.** D	**10.** B
11. D	**12.** C	**13.** D	**14.** D	**15.** B					

Previous Years' Questions

1. D	**2.** C	**3.** C	**4.** 26	**5.** D	**6.** 1	**7.** 256	**8.** B	**9.** A	**10.** C
11. 158	**12.** 13	**13.** B	**14.** 9	**15.** C	**16.** 144				

Chapter 5

Network Security

LEARNING OBJECTIVES

- *Network security basics*
- *Terminologies*
- *Cryptographic techniques*
- *Encryptions*
- *Types of keys*
- *Traditional cipher algorithms*
- *Substitution cipher*
- *Traditional cipher*
- *Symmetric key encryption*
- *Asymmetric key encryption*
- *Diffie-hellman*
- *Digital signatures and certificates*

Network Security Basics

It is necessary to define some fundamental terms relating to network security and are the elements used to measure the security of a network. These terms are used to measure the security of a network. To be considered sufficiently advanced along the spectrum of security, a system must adequately address identification, integrity, accountability, non-repudiation, authentication, availability, confidentiality each of which is defined in the following sections:

Identification

Identification is simply the process of identifying one's self to another entity or determining the identity of the individual or entity, with whom you are communicating.

Authentication

Authentication serves as proof that you are who you say you are or what you claim to be. Authentication is critical if there is to be any trust between parties. Authentication is required when communicating over a network or logging into a network. When communicating over a network you should ask yourself two questions.

1. With whom am I communicating?
2. Why do I believe this person or entity is who he claims to be?

Access Control (Authorization)

This refers to the ability to control the level of access that individuals or entities have to a network or system and how much information they can receive. Level of authorization basically determines what you're allowed to do once you are authenticated and allowed access to a network, system or some other resource such as data or information. Access control is the determination of the level of authorization to a system, network or information.

Availability

This refers to whether the network, system, hardware and software are reliable and can recover quickly and completely in the event of an interruption in service. Ideally, these elements should not be susceptible to denial of service attacks.

Confidentiality

This is also be called privacy or secracy to the protection of information from unauthorized disclosure. Usually achieved either by restricting access to the information or by encrypting the information so that it is not meaningful to unauthorized individuals or entities.

Integrity

This can be thought of as accuracy, this refers to the ability to protect information, data, or transmissions from unauthorized, uncontrolled, or accidental alterations.

Accountability

This refers to the ability to track or audit what an individual or entity is doing on a network or system.

Non-repudiation

The ability to prevent individuals or entities from denying (repudiating) that information, data or files were sent or received or that information or files were accessed or altered, when infact they were. This capability is crucial in e-commerce, without if an individual or

entity can deny that he, she or it is responsible for a transaction and that he, she or it is, therefore, not financially liable.

Threats

A threat is anything that can disrupt the operation, functioning, integrity, or availability of a network or system. This can take any form and can be malevolent, accidental, or simply an act of nature.

Vulnerabilities

A vulnerability is an inherent weakness in the design, configuration, implementation, or management of a network or system that renders it susceptible to a threat. Vulnerabilities are what make networks susceptible to information loss and downtime. Every network and system has some kind of vulnerability.

Attacks

An attack is a specific technique used to exploit a vulnerability. For example, a threat could be a denial of service. A vulnerability is in the design of the operating system, and an attack could be a 'Ping of death'. There are two general categories of attacks:

1. Passive
2. Active

Passive attacks These are very difficult to detect because there is no overt activity that can be monitored or detected.

Examples of passive attacks would be packet sniffing or traffic analysis.

These types of attacks are designed to monitor and record traffic on the network. They are usually employed for gathering information that can be used later in active attacks.

Active attacks These employ more overt actions on the network or system. As a result, they can be easier to detect, but at the same time they can be much more devastating to a network.

Examples of this type of attack would be a denial-of-service attack or active probing of systems and networks.

Viruses

A virus, a parasitic program that cannot function independently, is a program or code fragment that is self propagating. It is called a virus, because like its biological counterpart, it requires a 'host' to function. In the case of a computer virus the host is some other program to which the virus attaches itself. A virus is usually spread by executing an infected program or by sending an infected file to someone else, usually in the form of an e-mail attachment.

Worm

A worm is a self-contained and independent program that is usually designed to propagate or spawn itself on infected systems and to seek other systems via available networks. The difference between a virus and a Worm is that a virus is not an independent program.

Trojan horses

A trojan horse is a program or code fragment that hides inside a program and performs a disguised function. A trojan horse program hides within another program or disguises itself as a legitimate program. This can be accomplished by modifying the existing program or by simply replacing the existing program with a new one. The Trojan horse program functions much the same way as the legitimate program, but usually it also performs some other function, such a recording sensitive information or providing a trap door. An example would be a 'password grabber'.

Logic bombs

A logic bomb is a program or subsection of a program designed with malevolent intent. It is referred to as a logic bomb, because the program is triggered when certain logical conditions are met. This type of attack is almost always perpetrated by an insider with privileged access to the network. The perpetrator could be a programmer or a vendor that supplies software.

Denial of service (DOS)

Denial of service attacks are designed to shut down or render inoperable a system or network. The goal of the denial-of-service attack is not to gain access or information but to make a network or system unavailable for use by other users. It is called denial-of-service attack, because the end result is to deny legitimate users access to network services.

Protection against network threats

Network threats may cause a massive harm to the system, as the network users are increasing, there is a good chance to attack a system protection against threats should be done.

To protect system form virus and worms, a security suite should be installed.

Similarly, to protect a system from Trojan horse, internet security suite prevents from downloading Trojan horse.

SPAM filters should be used to stop SPAM, this is available within the mail servers by default.

A strong encryption should be used to protect against packet sniffers, so that packets become unreadable making packet sniffers useless.

Cryptographic Techniques

For the exchange of information and commerce to be secure on any network, a system or process must be put in place that satisfies requirements for confidentiality, access control, authentication, integrity, and non-repudiation. The key

to the securing information on a network is cryptography. Cryptography can be used as a tool to provide privacy.

Traditionally, cryptography conjures up thoughts of spies and secret codes. In reality, cryptography and encryption have found broad applications in society. Every time you use an ATM machine to get cash or a point-of-sale machine to make a purchase, you are using encryption.

Encryption

Encryption is the process of scrambling the contents of a file or message to make it unintelligible to anyone not in possession of the 'key' required to unscramble it.

A cryptosystem or algorithm is the process or procedure to turn plain text into crypto text. A crypto algorithm is also known as a 'cipher'. Theoretically, all algorithms can be broken by one method or another. However, an algorithm should not contain an inherent weakness that an attacker can easily exploit

Example: Below is an example of a cipher, to scramble a message with this cipher, simply match each letter in a message to the first row and convert it into the number or letter in the second row. To unscramble a message, match each letter or number in a message to the corresponding number or letter in the second row and convert it into the letter in the first row.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

To illustrate how this works see the following where the cipher is used to scramble the message:

'Little green apples'

Cipher text: FCNNF5 AL55H 1JJF5M
Clear text: LITTLE GREEN APPLES

This cipher would not be effective at keeping a message secret for long. It does not comply with one of the qualities of a truly effective cipher. Ciphers usually fall into one to two categories:

1. Block Ciphers
2. Stream Cipher

Stream ciphers

Steam cipher algorithms process plaintext to produce a stream of cipher text. The cipher inputs the plaintext in a stream and outputs a steam of cipher text.

Example:
Plaintext: LET US TALK ONE TO ONE
Cipher text: F5N OM NLFE ITS NI ITS

Stream cipher have several weaknesses. The most crucial short coming of stream ciphers is the fact that patterns in the plain text can be reflected in the cipher text. Knowing that certain words repeat makes breaking the code easier. In addition, certain words in the English language appear with predictable regularity. Letters of the alphabet also appear in predictable regularity. The most commonly used letters of the alphabet in the English language are E, T, A, O, N and I. The least commonly used letters are J, K, X, Q and Z. The most common combination of letters in the English language is '*th*', As a result, if a code breaker is able to find a '*t*' in a code, it doesn't take long to find an '*h*'.

Block ciphers

Block ciphers differ from stream ciphers in that they encrypt and decrypt information in fixed size blocks rather than encrypting and decrypting each letter or word individually. A block cipher passes a block of data or plaintext through its algorithm to generate a block of cipher text. Another requirement of block cipher is that the cipher texts should contain no detectable pattern.

Types of keys

We deal with three types of keys in cryptography:

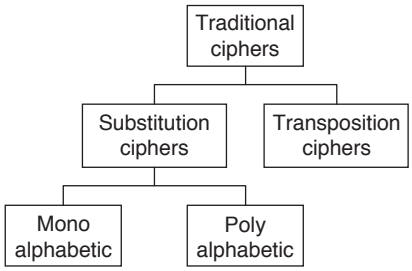
1. Secret key
2. Public key
3. Private Key

- The secret key, is the shared key used in symmetric-key cryptography.
- Public and Private keys are used in asymmetric-key cryptography.
- In symmetric-key cryptography, the same key locks and unlocks the box.
- In asymmetric-key cryptography, one key locks the box, but another key is needed to unlock it.

Traditional Cipher Algorithms

Traditional ciphers are character oriented, these ciphers can be divided into two broad categories:

1. Substitution ciphers
2. Transposition ciphers.



Substitution Cipher

A substitution cipher substitutes one symbol with another. If the symbols in the plain text are alphabetic characters, we replace one character with another. Substitution ciphers can be categorized as either mono-alphabetic or poly-alphabetic ciphers.

- In a mono-alphabetic cipher, a character or symbol in the plaintext is always changed to the same character or symbol in the cipher text regardless of its position in the text. For example if the algorithm says that character '*A*' in the plain text is changed to character '*E*', every character '*A*' is changed to character '*E*'.
- The relationship between characters in the plain text and the cipher text is a one-to-one relationship.
- In a poly-alphabetic cipher, each occurrence of a character can have a different substitute. The relationship between a character in the plain text to a character in the cipher text is a one-to-many relationship.
- To achieve this goal, we need to divide the text into groups of characters and use a set of keys.
- In substitution cipher, if 'a' becomes *D*, '*b*' becomes '*E*' then the word 'corrupt' becomes ETUUXSW, plain text will be given in lower case, and cipher text in upper case.
- A slight generalization of the ceasar cipher allows the cipher text alphabet to be shifted by '*K*' letters, instead of always '3'.
- The next improvement is to have each of the symbols in the plain text, say, the 26 letter for simplicity, map onto some other letter.

Example:

Plain Text	a	b	c	d	e	f	g	h	i	j
Cipher Text	L	N	O	B	R	M	S	U	V	Z

Plain text	k	l	m	n	o	p	q	r	s	t	u
Cipher Text	P	A	K	C	L	H	W	Q	X	Y	J

Plain Text	v	w	x	y	z
Cipher Text	E	F	D	G	J

Plain Text	corrupt
Cipher Text	OIQQJHY

- In this method, if a small cipher is given it can be broken easily. The basic attack takes advantage of the statistical properties of natural languages. For example, In English, '*e*' is the most common letter followed by *t*, *o*, *a*, *n*, *i* etc.
- The most common 2 letter combinations, are *th*, *in*, *er*, *re* and *an*.
- The most common three-letter combinations are are, the, ing, and, and ion.
- By making guesses at common letters, digrams and trigrams and knowing about likely patterns of vowels and consonants, the cryptanalyst builds up a tentative plaintext, letter by letter.

Transposition Ciphers

Substitution ciphers preserve the order of the plaintext symbols but disguise them.

Transposition ciphers, in contrast, reorder the letters but do not disguise them. Following figure depicts a common transposition cipher, the columnar transposition.

- The cipher is keyed by a word or phrase not containing any repeated letters.

Example: 'NETWORKS' is the key.
Plaintext: Transfer ten million dollars to my account.
What is the cipher text using transposition cipher?

Solution: Key: NETWORKS

N	E	T	W	O	R	K	S
3	1	7	8	4	5	2	6
T	r	a	n	s	f	e	r
t	e	n	m	i	l	l	i
o	n	d	o	l	l	a	r
s	t	o	m	y	a	c	c
o	u	n	t	a	b	c	d

The purpose of key is to number the columns, column 1 being under the key letter closest to the start of the alphabet, and so on.

The plain text is written horizontally in rows, padding is required to fill the matrix, if it is not complete'. The cipher text is read out by columns, starting with the column whose key letter is the lowest.

Plain text: Transfer ten million dollars to my account
Cipher Text: rentue laccttososilyafllabrircdandonnmomt.

Symmetric Key Encryption

Symmetric key, also referred to as private key or secret key, is based on a single key and algorithm being shared between the parties who are exchanging encrypted information. The same key both encrypts and decrypts messages.

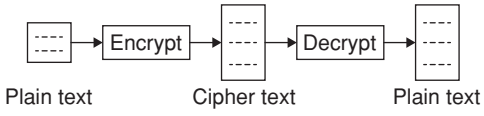


Figure 1 Symmetric key encryption

The strength of the scheme is largely dependent on the size of the key and on keeping it secret. Generally the larger the key, the more secure the scheme. In addition, symmetric key encryption is relatively fast. Private key cryptosystems are not well suited for spontaneous communication over open and unsecured networks. Symmetric key provides on process for authentication or non-repudiation.

Data Encryption Standard: (DES)

DES consists of an algorithm and a key. The key is a sequence of eight bytes, each containing eight bits for a 64 bit key. Since each byte contains one parity bit, the key is actually 56 bits in length. DES is widely used in automated teller machine (ATM) and point-of-sale (POS) networks, so if you use an ATM or debit card you are using DES.

Asymmetric Key Encryption

Asymmetric cryptography is also known as public key cryptography, public key cryptography uses two keys one is public key and the other is private key. The key names describe their function. One key is kept private, and the other key is made public. Knowing the public key doesn't reveal the private key. A message encrypted by the private key can only be decrypted by the corresponding public key. Conversely, a message encrypted by the public key can only be decrypted by the private key.

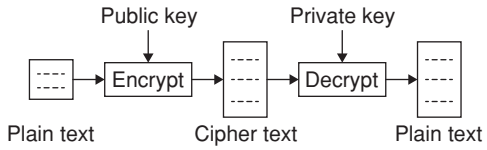


Figure 2 Asymmetric key encryption

With the aid of public key cryptography, it is possible to establish secure communications with any individual or entity when using a compatible software or hardware device.

There are three public key algorithms in wide use today:

1. Diffie–Hellman
2. RSA
3. Digital Signature Algorithm (DSA)

Diffie–Hellman

It was the first usable public key algorithm. Diffie–Hellman is based on the difficulty of computing discrete logarithms. It can be used to establish a shared secret key that can be used by two parties for symmetric encryption. Diffie–Hellman is often used for IPsec key management protocols. For spontaneous communications with Diffie–Hellman, two communicating entities would each generate a random number that is used as their private keys. They exchange public keys they each apply their private keys to the other's. public key to compute identical values (shared secret key). They then use the shared secret key to encrypt and exchange information.

Diffie–Hellman key exchange

The protocol that allows strangers to establish a shared secret key is called the Diffie–Hellman key exchange and works as follows:

- Ana and Brat have to agree on 2 large numbers, 'n' and 'g', where 'n' is a prime.
- $(n-1)/2$ is also a prime and certain conditions apply to 'g'.
- These numbers may be public, so either one of them can just pick 'n' and 'g' and tell the other openly.
- Now Ana picks a large number (suppose 512-bit) 'x', and keeps it secret. Similarly Brat picks a large secret number, 'y'.
- Ana initiates the key exchange protocol by sending Brat a message containing $(n, g, g^x \bmod n)$
- Brat responds by sending Ana a message containing $(g^y \bmod n)$
- Now Ana raises the number Brat sent her to the xth power modulo 'n' to get $[(g^y \bmod n)^x \bmod n]$
- Brat performs a similar operation to get $[(g^x \bmod n)^y \bmod n]$, Both the calculations yield $(g^{xy} \bmod n)$.

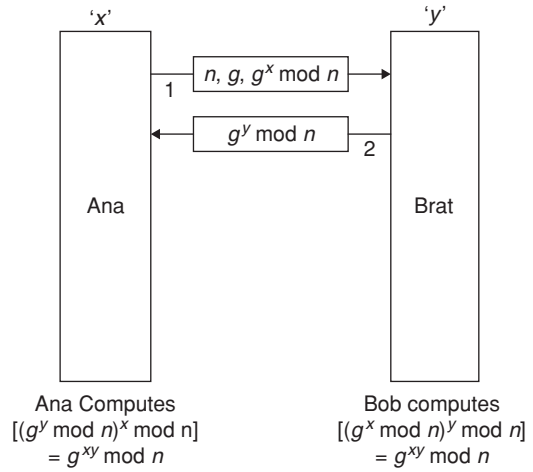


Figure 3 Diffie-Hellman key exchange

RSA (Rivest, Shamir, Adelman)

RSA multiplies large prime numbers together to generate keys. It's strength lies in the fact that it is extremely difficult to factor the product of large prime numbers. This algorithm is the one, most often associated with public key encryption. The RSA algorithm also provides digital signature capabilities.

Example:

- Select two large primes = p, q $p = 17, q = 11$
- $n = p \times q = 17 \times 11 = 187$
- calculate $\phi = (p-1)(q-1) = 16 \times 10 = 160$
- select e, such that LCD $(\phi, e) = 1$, $0 < e < \phi$ say, $e = 7$
- calculate d such that $d \bmod \phi = 1$
- 160k + 1 = 161, 321, 481, 641,
- Check which of these is divisible by 7
- 161 is divisible by 7 giving d = 161/7 = 23
- Key 1 = {7, 187}, key 2 = {23, 187}

Digital Signatures

A digital signature allows a receiver to authenticate (to a limited extent) the identity of the sender and to verify the integrity of the message for the authentication process, you

must already know the senders public key, either from prior knowledge or from some trusted third party. Digital signatures are used to ensure message integrity and authentication. In its simplest from, a digital signature is created by using the senders private key to hash the entire contents of the message being sent to create a message digest. The recipient uses the sender's public key to verity the integrity of the message by recreating the message digest. By this process you ensure the integrity of the message and authenticate the sender.

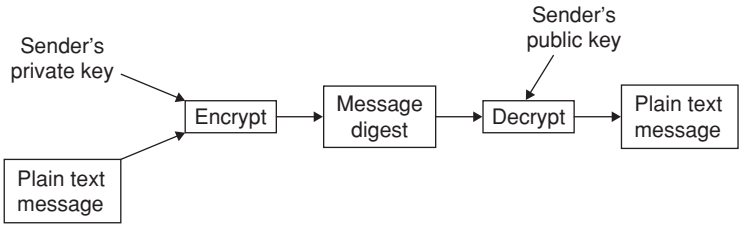


Figure 4 Digital signature

To sign a message, senders usually append their digital signature to the end of a message and encrypt it using the recipient's public key. Recipients decrypt the message using their own private key and verify the sender's identity and the message integrity by decrypting the sender's digital signature using the sender's pubic key. The strength of digital signatures are that they are almost impossible to counterfeit and they are easily verified.

Digital certificate

Digital signatures can be used to verify that a message has been delivered unaltered and to verify the identify of the sender by public key. The problem with authenticating a digital signature, however, is that you must be able to verify that a public key does in fact belong to the individual or entity that claims to have sent it and that the individual or entity is in fact who or what it claims to be.

A digital certificate issued by a certification authority (CA) utilizing a hierarchical public key infrastructure (PKI) can be used to authenticate a sender's identify for spontaneous, first–time contacts. Digital certificates provide a means for secure first time spontaneous communication. A digital certificate provides a high level of confidence in the identify of the individual.

A digital certificate is issued by a trusted/unknown third party (CA) to bind an individual or entity to a public key. The digital certificate is digitally signed by the CA with the CA's private key. This provides independent confirmation that an individual or entity is in fact who it claims to be. The CA issued digital certificates that certify for the identities of those to whom the certificates were issued.

Firewalls

Firewall is a control link between internet and organization intranet. It protects network premises from internet based attacks by providing single choke point. All the network traffic is forced to travel through this fire wall. Firewall allows only authorized traffic to pass through.

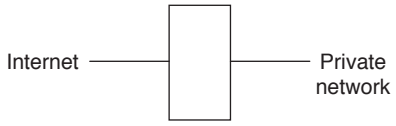
The different types of firewalls are:

1. Packet – filtering router
2. Application level gateways
3. Circuit level gateways
4. Bastion host

Packet filtering router

It filters packets with incoming and outgoing interfaces, and permits or denies certain services. It uses the information of transport layer like IP sources, ICMP message etc.

The drawbacks are IP address spoofing, tiny fragment attack and source routing attacks.



Application level gateway

It provides proxies for each service, when user requests service, it validates the request as legal one and return results to the user.

Application level gateway is more secure than the packet filter.

The drawback of this gateway is processing overhead at each connection.

Circuit-level gateway

It is application level gateway functionality for certain applications. It does not allow end-end TCP connection, rather it maintains two connections, one with the inner host and the other with the outer host. Once the connections are established TCP segment is allowed without examining contents. It only checks the incoming data.

Bastion host

It provides a platform for the application gateway (or) circuit level gateway, it is a critical strong point in network security.

An additional authentication is required for the user who want access to proxy services. Even proxy service authenticates itself before granting the access to user.

Only essential services are installed in the Bastion host which are decided by admin.

EXERCISES

Practice Problems I

Directions for questions 1 to 15: Select the correct alternative from the given choices.

1. In an encryption scheme that uses RSA, values, for p and q are selected to be 5 and 7 respectively what could be the value of d?
(A) 12 (B) 3 (C) 11 (D) 9

2. A person x is supposed to send a document with digitized signature to another person y using public key Cryptography. p is the message. D_x, D_y are private keys of x and y respectively. E_x, E_y are public keys of x, y respectively. Select the best possible sequence of events from below:
(i) $D_x(p)$
(ii) $D_y(p)$
(iii) $E_y(D_x(p))$
(iv) $D_y(D_x(p))$
(v) $D_y(E_y(p))$
(vi) $D_y(E_y(D_x(p))$
(vii) $E_x(D_x(p))$
(viii) $E_y(p)$
(ix) $E_x(D_y(p))$
(x) $D_x(E_y(p))$
(A) (ii), (ix), (viii), (v) (B) (viii), (x), (v), (i)
(C) (i), (iii), (v), (vii) (D) (vii), (v), (iii), (i)

3. Select correct statements about PGP:
(i) Uses existing cryptographic algorithms that have been quite successful.
(ii) Support text compression, digital ignatures.
(iii) Takes plaintext as feed and generates base-64 text.
(iv) No key management capability is rovided.
(A) (i), (ii), (iii) (B) (ii), (iii), (iv)
(C) (i), (iii), (iv) (D) (i), (ii), (iv)

Linked answer questions 4 and 5:

4. Using mono alphabetic substitution a string a b b a c a a b c d is transformed to one of the below strings. Select the most appropriate option:
(A) p q q p r p p s r s (B) j t t x j j i t x t x
(C) u s s u a u u s a b (D) d c c d b b b c b a

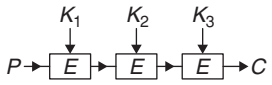
5. Using the mapping obtained above, encrypt the phrase 'bad cab' using same method: Assume space is not encrypted.
(A) q p s r p q (B) t j z x j t
(C) s u b a u s (D) c d a b d c

6. Select the correct statements with regard to packet filters of a firewall:
(i) They are usually driven by a table with information in regards to acceptable sources and destinations.
(ii) Default rules about what needs to be done in regards to packets coming from or going to other machines.
(iii) Can block TCP ports.
(A) (i), (ii) (B) (ii), (iii)
(C) (i), (iii) (D) (i), (ii), (iii)

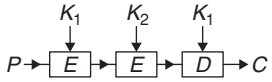
7. What is meant by non-repudiation in the area of digital signatures?
(A) Receiver verifying the signature of the sender.
(B) Receiver concocting the message.
(C) Sender denying having signed digitally.
(D) Receiver changing the contents after receiving the signed document.

8. Which of the following statements about DES is/are true?
(i) DES is public key algorithm.
(ii) DES has 19 distinct stages.
(iii) In the 16 iterations of DES, different keys are used.
(A) (i), (ii) (B) (ii), (iii)
(C) (i), (iii) (D) (i), (ii), (iii)

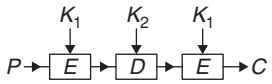
9. Which of the below represents Triple encryption using DES? (P is the unencrypted input, 'C' is encrypted output, k_1, k_2, k_3 are keys used in encryption and decryption, E stands for encryption and D stands for decryption).
(A)



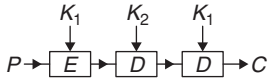
(B)



(C)



(D)



10. Which of the below statements are applied for cipher block chaining?
(i) Each plaintext block is XOR'ed with previous block before encryption.
(ii) Encryption is a mono alphabetic substitution cipher.
(iii) Cipher block chaining can result in same plaintext blocks encrypted to different cipher text blocks.
(A) (i), (ii) (B) (ii), (iii)
(C) (i), (iii) (D) (i), (ii), (iii)

11. Which of the below statements are applied to RSA algorithm?
(i) RSA is a relatively slow algorithm when encrypting large data.
(ii) Mainly used where key is to be distributed.
(iii) The strength of the algorithm lies in the fact that determining the key can take exceedingly long time by brute force.

(A) (i), (ii) (B) (ii), (iii)
(C) (i), (iii) (D) (i), (ii), (iii)

12. The security and usefulness of a digital signature depends on
(A) A public hash function
(B) A two-way hash function
(C) Protection of user's private key
(D) Protection of user's public key

13. Let '*M*' be the message to be encrypted, *E* be Encryption key and *N* be the product of two random prime numbers, then what is the cipher text using RSA algorithm?
(A) $C = E^m \bmod N$ (B) $C = M^E \bmod N$
(C) $C = N^E \bmod M$ (D) $C = E^N \bmod M$

14. Which of the following best describes the decryption in Triple DES?
(A) Plain text $= D_{K_1}(E_{K_2}(D_{k_1}(\text{ciper text})))$
(B) Plain text $= D_{K_1}(E_{K_2}(D_{k_3}(\text{ciper text})))$
(C) Plain text $= E_{K_1}(D_{K_2}(E_{k_1}(\text{ciper text})))$
(D) Plain text $= E_{K_1}(D_{K_2}(E_{k_1}(\text{ciper text})))$

15. In which cipher mode, all cipher blocks will be chained so that if one is modified the cipher text cannot be decrypted correctly?
(A) Electronic Code Book
(B) Cipher Block Chaining
(C) Cipher Feedback Mode
(D) Counter Mode

Practice Problems 2

Directions for questions 1 to 15: Select the correct alternative from the given choices.

1. 'All algorithms must be public only the keys are secret' is
(A) Rijndael Principle
(B) Kerckhoff's principle
(C) Rivest shamir Adleman principle
(D) None of these

2. Pretty Good Privacy encrypts data by using a block cipher called
(A) RSA (B) MD5
(C) IDEA (D) DES

3. E-mail security package is related to
(A) Pretty Good Privacy
(B) DNS spoofing
(C) Secure Socket Layer
(D) Transport Layer Security

4. Which of the following protocols will be proxy, on an application firewall?
(A) IPX (B) FTP
(C) POP (D) SMS

5. A good recommendation is that if a private key is ____ or longer, the key is thought to be secure.
(A) 40 bits (B) 60 bits
(C) 70 bits (D) 80 bits

6. Which issue is related to server side security?
(A) Protection of the server from legitimate web access
(B) Security of the information stored on server
(C) Security of the customer's physical credit card
(D) Security of the customer's computer

7. Which of the following is not an active attack?
(A) Denial of service (B) Traffic Analysis
(C) Replay (D) Masquerade

8. Verifying the true identity of the sender of a message recipient is known as _____.
(A) Authentication (B) fabrication
(C) Cryptography (D) availability

9. In which of the following techniques, letters are arranged in a different order?
(A) Transposition
(B) Substitution
(C) Private key Encryption
(D) None of the above

10. In which type of attack, Algorithm, cipher text, chosen plaintext and cipher text are known?
(A) Cipher text only
(B) Known plain text
(C) Chosen cipher text
(D) Chosen text

11. In which type of ciphers the encryption depends on current state?
(A) Link cipher
(B) Block cipher
(C) Stream cipher
(D) Current cipher

12. Traffic Analysis can be counted using
(A) Encryption (B) Decryption
(C) Replay (D) Data padding

13. DES Algorithm is vulnerable to
(A) Masquerade attack
(B) Replay attack
(C) Denial of service
(D) Brute Force attack

14. What is the size of key in Triple DES?
(A) 168 bits (B) 112 bits
(C) 56 bits (D) Either (A) or (B) or (C)

15. Direct digital signature involves
(A) Source only
(B) Destination only
(C) Communicating parties, sender and receiver.
(D) Everyone including communicating parties.

Previous Years' Questions

1. Suppose that everyone in a group of N people wants to communicate secretly with the $N-1$ others, using symmetric key cryptographic system. The communication between any two persons should not be decodable by the others in the group. The number of keys required in the system as a whole to satisfy the confidentiality requirement is **[2015]**

(A) $2N$ (B) $N(N-1)$
(C) $N(N-1)/2$ (D) $(N-1)^2$

2. Consider that B wants to send a message m that is digitally signed to A. Let the pair of private and public keys for A and B be denoted by K_x^- and K_x^+ for $x = A, B$, respectively. Let $K_x(m)$ represent the operation of encrypting m with a key K_x and $H(m)$ represent the message digest. Which one of the following indicates the CORRECT way of sending the message m along with the digital signature to A? **[2016]**

(A) $\{m, K_B^+ (H(m))\}$ (B) $\{m, K_B^- (H(m))\}$
(C) $\{m, K_A^- (H(m))\}$ (D) $\{m, K_A^+ (m)\}$

3. Anarkali digitally signs a message and sends it to Salim. Verification of the signature by Salim requires **[2016]**

(A) Anarkali's public key.
(B) Salim's public key.
(C) Salim's private key.
(D) Anarkali's private key.

4. A sender S sends a message m to receiver R, which is digitally signed by S with its private key. In this scenario, one or more of the following security violations can take place.

(I) S can launch a birthday attack to replace m with a fraudulent message.
(II) A third party attacker can launch a birthday attack to replace m with a fraudulent message.
(III) R can launch a birthday attack to replace m with a fraudulent message.

Which of the following are possible security violations? **[2017]**

(A) (I) and (II) only (B) (I) only
(C) (II) only (D) (II) and (III) only

5. In a RSA cryptosystem, a participant A uses two prime numbers $p = 13$ and $q = 17$ to generate her public and private keys. If the public key of A is 35, then the private key of A is _____. **[2017]**

Answer Keys

Exercises

Practice Problems 1

1. C	**2.** C	**3.** A	**4.** C	**5.** C	**6.** D	**7.** C	**8.** B	**9.** C	**10.** C
11. D	**12.** C	**13.** B	**14.** B	**15.** B					

Practice Problems 2

1. B	**2.** C	**3.** A	**4.** B	**5.** C	**6.** B	**7.** B	**8.** A	**9.** A	**10.** D
11. C	**12.** D	**13.** D	**14.** D	**15.** C					

Previous Years' Questions

1. C	**2.** B	**3.** A	**4.** B	**5.** 11

Test

Computer Networks

Time: 60 min.

Directions for questions 1 to 30: Select the correct alternative from the given choices

1. What is the Hamming distance between 000, 011?
(A) 0 (B) 1
(C) 2 (D) 3

2. Consider the given data:

Dataword	Codeword
00	00000
01	01011
10	10101
11	11110

Find the minimum hamming distance?
(A) 2 (B) 3
(C) 4 (D) 5

3. In Go-back-n, what should be the Window size?
(A) 2^m (B) 2^{m-1}
(C) 2^{m-2} (D) 2^{2m}

4. If there are 16 sequence numbers, what are the sender and receiver window sizes in go-back-n and selective repeat respectively?
(A) (15, 1) (8, 8) (B) (14, 2) (8, 8)
(C) (15, 1) (7, 8) (D) (15, 1) (8, 7)

5. A code needs to be designed with 8 data bits and r check bits. What is the minimum value of r in order to correct single bit errors?
(A) 1 (B) 2
(C) 3 (D) 4

6. A code has hamming distance of 6. What is the maximum number of bit errors that can be corrected?
(A) 1 (B) 2
(C) 3 (D) 4

7. In the above case what is the number of errors that can be detected?
(A) 3 (B) 4
(C) 5 (D) 6

8. CRC is being used to do error detection and correction. The frame with data 101001001 needs to be sent and the generator polynomial being used is $x^4 + x + 1$. What is the final transmitted frame?
(A) 1010010011110 (B) 1010010010010
(C) 1010010011010 (D) 1010010010000

9. OSI model seven layer is based on which of the following principles:
(A) A layer should be created where a different level of abstraction is needed
(B) Each layer should perform a well defined function
(C) The layer boundaries should be chosen to minimize the information flow across the interfaces
(D) All the above

10. Which of the following is/are the tasks of physical layer?
(A) How to link two or more devices physically
(B) What type of data flow is needed between two devices
(C) Type of topology required
(D) All the above

11. The functions of the data link layer are
(A) It provides services to network layer and accepts services from physical layer
(B) It is responsible for error control and detection within the network.
(C) It regulates the amount of data that can be transmitted on one line
(D) All the above

12. Which one of the following layers deals with problems that arise when packet travels from one network to another?
(A) Transport layer (B) Physical layer
(C) Data link layer (D) Network layer

13. What is the main function of the network layer?
(A) Routing
(B) Congestion control
(C) Both (A) and (B)
(D) None of these.

14. Which layer ensures interoperability among the communicating devices, and also computers to communicate even if their internal representation is different?
(A) Session layer (B) Transport layer
(C) Presentation layer (D) Application layer

15. Which of the following is not a layer in TCP/IP reference model?
(A) Application layer (B) Transport layer
(C) Data link layer (D) Host to Network layer

16. Suppose we want to transmit a character '*C*', the binary value is 1000011 if we pass through an even parity generator then the output is
(A) 10000110 (B) 10000111
(C) 1000011 (D) 1000010

17. What type of frames can be recognized by stop and wait protocols?
(A) Damaged frames
(B) Lost frames
(C) Lost of acknowledgement frames
(D) All the above

18. IEEE project 802 divides the data link layer into two sub layers. What is the upper sublayer?
(A) LLC (B) MAC
(C) PDU (D) HDLC

Common data for questions 19 and 20: When a data frame, arrives at the receiver, instead of sending an acknowledgement separately the receiver rests itself and waits until the network layer passes it the next packet. The acknowledgement is attached to the outgoing data frame.

19. The technique of temporarily delaying outgoing ACK so that they can be hooked onto the next outgoing data frame is called_____
(A) Pipelining (B) Piggybacking
(C) Flooding (D) None

20. Which layer implements technique of piggybacking?
(A) Physical layer (B) Data link layer
(C) Transport layer (D) Session layer

21. What is the protocol used in one bit sliding window protocol?
(A) Unrestricted simplex
(B) Simplex stop and wait
(C) Simplex protocol for noisy channel
(D) Restricted duplex.

22. The technique of keeping the sender window appropriately in such a way, that it can continuously transmit frames for a time equal to the round trip time, so that acknowledgement of first frame will arrive just after transmitting the last frame, is called
(A) Flooding (B) Piggy backing
(C) Pipelining (D) Selective repeat

23. Pick the incorrect statement from the following
(A) Go-Back-*N* method requires more storage at the receiving side.
(B) Selective repeat involves complex logic than Go-back-*N*
(C) Go-back-*N* has better line utilization
(D) Selective repeat has better line utilization

24. In stop and wait flow control, to send '*n*' data packets how many acknowledgements are needed.
(A) n (B) $2n$
(C) $n-1$ (D) $n+1$

25. In sliding window flow control, if the window size is 64 what is the range of sequence numbers?
(A) 0 to 63 (B) 0 to 64
(C) 1 to 63 (D) 1 to 64

26. In Go-Back-*N* Automatic Repeat Request (ARR), if frames 4, 5, 6 are received successfully, the receiver will send which ACK number to the sender?
(A) 5 (B) 6
(C) 7 (D) 4

27. Which of the following are the responsibilities of a token ring monitor station?
(A) Check to see that token is not lost
(B) Taking action when ring breaks
(C) Clearing the ring when garbled frames appear
(D) All the above

Common data for questions 28 and 29:

28. In ISO-OSI reference model the layer that provides necessary translation of different control codes, character set and graphic character and it ensures interoperability among communicating devices.
The above explanation is about which of the following layers?
(A) Session layer
(B) Data link layer
(C) Presentation layer
(D) Application layer

29. What are the other tasks performed by the above layer?
(A) Encryption and compression
(B) Token management and synchronization
(C) Error detection and error correction
(D) None of these

30. The layer that takes a raw transmission and transforms it into a line that appears free of undetected transmission errors and it takes care of traffic regulation to keep fast transmitter from drowning slow receiver. The layer that provides these services is
(A) Physical layer (B) Transport layer
(C) Data link layer (D) Application layer

Answer Keys

1. C	**2.** B	**3.** A	**4.** A	**5.** D	**6.** B	**7.** C	**8.** D	**9.** D	**10.** D
11. D	**12.** D	**13.** C	**14.** C	**15.** C	**16.** B	**17.** D	**18.** A	**19.** B	**20.** B
21. B	**22.** C	**23.** C	**24.** A	**25.** A	**26.** C	**27.** D	**28.** C	**29.** A	**30.** C