**PART - A**

**UNIT – I**

**1. What is mean by data communication?**

Data communication is the exchange of data (in the form of 1s and 0s) between two devices via some form of transmission medium (such as a wire cable).

**2. What are the three criteria necessary for an effective and efficient network?**

The most important criteria are performance, reliability and security. Performance of the network depends on number of users, type of transmission medium, the capabilities of the connected h/w and the efficiency of the s/w. Reliability is measured by frequency of failure, the time it takes a link to recover from the failure and the network’s robustness in a catastrophe. Security issues include protecting data from unauthorized access and viruses.

3. **What are the three fundamental characteristics determine the effectiveness of the data communication system?**

The effectiveness of the data communication system depends on three fundamental characteristics:

Delivery: The system must deliver data to the correct destination.

Accuracy: The system must deliver data accurately.

Timeliness: The system must deliver data in a timely manner.

**4. What are the advantages of distributed processing?**

Advantages of distributed processing include security/encapsulation, distributed databases, faster problem solving, security through redundancy and collaborative processing.

**5. Why are protocols needed?**

In networks, communication occurs between the entities in different systems. Two entities cannot just send bit streams to each other and expect to be understood. For communication, the entities must agree on a protocol. A protocol is a set of rules that govern data communication.

**6. Why are standards needed?**

Co-ordination across the nodes of a network is necessary for an efficient communication. If there are no standards, difficulties arise. A standard provides a modeler basis for development to which everyone has agreed.

**7. For n devices in a network, what is the number of cable links required for a mesh and ring topology?**

* Mesh topology – n (n-1)/2
* Ring topology – n

**8. What is the difference between a passive and an active hub?**

An active hub contains a repeater that regenerates the received bit patterns before sending them out. A passive hub provides a simple physical connection between the attached devices.

**9. Distinguish between peer-to-peer relationship and a primary-secondary relationship.**

Peer-to-peer relationship: All the devices share the link equally. Primary-secondary relationship: One device controls traffic and the others must transmit through it.

**10. Assume 6 devices are arranged in a mesh topology. How many cables are needed? How many ports are needed for each device?**

* Number of cables=n (n-1)/2=6(6-1)/2=15
* Number of ports per device=n-1=6-1=5

**11. Group the OSI layers by function.**

The seven layers of the OSI model belonging to three subgroups. Physical, data link and network layers are the network support layers; they deal with the physical aspects of moving data from one device to another. Session, presentation and application layers are the user support layers; they allow interoperability among unrelated software systems. The transport layer ensures end-to-end reliable data transmission.

**12. What are header and trailers and how do they get added and removed?**

Each layer in the sending machine adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it. This information is added in the form of headers or trailers. Headers are added to the message at the layers 6,5,4,3, and 2. A trailer is added at layer2. At the receiving machine, the headers or trailers attached to the data unit at the corresponding sending layers are removed, and actions appropriate to that layer are taken.

**13. Discuss the mode for propagating light along optical channels.**

There are two modes for propagating light along optical channels, multimode and single mode.

Multimode: Multiple beams from a light source move through the core in different paths.

Single mode: Fiber with extremely small diameter that limits beams to a few angles, resulting in an almost horizontal beam.

**14. What are the responsibilities of data link layer?**

Specific responsibilities of data link layer include the following.

a) Framing

b) Physical addressing

c) Flow control

d) Error control

e) Access control

**15. Mention the types of errors.**

There are 2 types of errors

* Single-bit error.
* Burst-bit error.

Single bit error: The term single bit error means that only one bit of a given data unit (such as byte character/data unit or packet) is changed from 1 to 0 or from 0 to 1.

Burst error: Means that 2 or more bits in the data unit have changed from 1 to 0 from 0 to 1.

**16. List out the available error detection methods.**

There are 4 types of redundancy checks are used in data communication.

a) Vertical redundancy checks (VRC).

b) Longitudinal redundancy checks (LRC).

c) Cyclic redundancy checks (CRC).

d) Checksum.

**17. Write short notes on VRC.**

The most common and least expensive mechanism for error detection is the vertical redundancy check (VRC) often called a parity check. In this technique a redundant bit4called a parity bit, is appended to every data unit so, that the total number of 0’s in the unit(including the parity bit) becomes even.

**18. Write short notes on CRC.**

The third and most powerful of the redundancy checking techniques is the cyclic redundancy checks (CRC) CRC is based on binary division. Here a sequence of redundant bits, called the CRC remainder is appended to the end of data unit.

**19. What are the steps followed in checksum generator?**

The sender follows these steps

a) The units are divided into k sections each of n bits.

b) All sections are added together using 2’s complement to get the sum.

c) The sum is complemented and become the checksum.

d) The checksum is sent with the data.

**20. What is error correction.**

It is the mechanism to correct the errors and it can be handled in 2 ways.

a) When an error is discovered, the receiver can have the sender retransmit the entire data unit.

b) A receiver can use an error correcting coder, which automatically corrects certain errors.

**21. What is the purpose of hamming code?**

A hamming code can be designed to correct burst errors of certain lengths. So the simple strategy used by the hamming code to correct single bit errors must be redesigned to be applicable for multiple bit correction.

**22. Mention the categories of flow control.**

There are 2 methods have been developed to control flow of data across communication links.

* Stop and wait- send one from at a time.
* Sliding window- send several frames at a time.

**23. What is a bridge? (May ‘14)**

Bridges operate at the data link layer (Layer 2) of the [OSI model](http://compnetworking.about.com/cs/designosimodel/g/bldef_osi.htm). Bridges inspect incoming traffic and decide whether to forward or discard it. An [Ethernet](http://compnetworking.about.com/cs/ethernet1/g/bldef_ethernet.htm) bridge, for example, inspects each incoming Ethernet frame - including the source and destination *MAC* addresses, and sometimes the frame size - in making individual forwarding decisions.

**24. List the advantage of FDDI. (May ‘14)**

Some of the major advantages of FDDI are

* Token passing topology
* High speed fiber optic transmission
* Dual rings offer improved fault tolerance over other options
* Fiber optic cabling is less susceptible to EMI and noise
* Fiber optic cabling is more secure than copper wire
* It can send data for larger distances than Token Ring or Ethernet

**UNIT II**

**1. Differentiate Physical Address and Logical Address.**

**Physical Address Logical Address**

1. It is implemented by data link layer. It is implemented by n/w layer.

2. It contains 48 bits. It contains 32 bits

3. It is a local addressing system. It is an universal address system.

4. Another name MAC address. Another name is IP address.

5. It is flat in nature Hierarchical in nature

6. Does not give any clue for routing Its structure gives clue for routing

**2. What are the various classes of IP addresses? / Define various levels of addressing in Internet.**

 **Class A :** They use only 1 byte to identify class type and Net Id and 3 bytes to identify host Id

**Range: 0.0.1.1.to 127.255.255.255**

**Class B :** They use only 2 bytes to identify class type and Net Id and 2 bytes to identify host Id

 **Range :128.0.0.0 to 191.255.255.255**

**Class C :** They use only 3 bytes to identify class type and Net Id and 1 byte to identify host Id

 **Range :192.0.0.0 to 223.255.255.255**

 **Class D :** It is reserved for multicast address, Range : 224.0.0.0 to 239.255.255.255

 **Class E :** Addresses are reserved for further use the structure of each IP address class.

 **Range : 240.0.0.0 to 255.255.255.255**

**3.What do you mean by ICMP? To whom ICMP reports error message.**

ICMP is an error reporting mechanism. It does not specify the action to be taken for each possible error. The source must relate the error to an individual application program and take other actions to correct the problem. **ICMP** allows routers to send error messages to other router or hosts. ICMP is an error reporting mechanism. It does not specify the action to be taken for each possible error. It is informing the source that the error has occurred and the source has to take actions to rectify the errors.

**4.Name any two network connecting devices? Can a bridge replace repeater for interconnecting 2 segments of a n/w?** Repeater, Bridges.

**Repeater** repeats the signal to the actual strength so that they can travel and works at physical layer. Repeater operates on the physical layer level. Here collision probability is more.

**Bridge** is an network connecting device. It does forwarding & filtering frames using LAN destination address. Bridges are used to connect LAN or WAN and works at data link layer level. Collision Probability is more. A bridge cannot replace repeater for interconnecting 2 segments of a network because functions of them are entirely different.

**5. List out functions of IP.**

 IP services are unreliable, best-effort, connectionless packet system.

 Unreliable – delivery is not guaranteed

 Connectionless – each pocket is treated independent from others

* Best-effort delivery – it makes an earnest attempt to deliver packets.
* It defines basic unit of data transfer through TCP/IP.
* IP s/w performs routing function – finds a path from source to destination.
* IP includes a set of rules that embody the idea of unreliable packet delivery

**6. What is the use of TTL in IP header? What is the router’s role in controlling the packet lifetime?**

It lets how long that datagram is allowed to live in the network. The source sets that time. Routers and hosts in the path of that datagram should decrement TTL and removes it when TTL = 0 and send an error message to the source. TTL is written hops or time in seconds.

7. **Write the difference between Distance vector routing and Link state routing.**

|  |  |
| --- | --- |
| **Distance Vector Routing** | **Link state routing** |
| 1. Basic idea is each node sends its knowledge about the entire network to its neighbors.
 | 1. Basic idea is every node sends its knowledge about its neighbors to the entire network
 |
| 1. It is dynamic routing
 | 1. It is dynamic routing
 |
| 1. RIP uses Distance vector routing
 | 1. OSPF uses link state routing
 |

**8.What is the difference between IPV4 and IPV6?**

|  |  |
| --- | --- |
| **IPV4** | **IPV6** |
| IP address is a 32 bit address | 128 bit (16 bytes) IP address |
| IP V4 can potentially address four billion nodes if address assignment efficiency reaches 100%.  | IPv6 can address 3.4×1038 nodes, again assuming 100% efficiency. |
| IP V4 has 5 address classes (Class A, B, C, D and E) and also it provides classless addressing  | IPv6 addresses do not have classes, but the address space is subdivided in various ways based on the leading bits. Eg: 001 - Aggregately Global Uncast Addresses1111 1110 10 - Link local use addresses |

**9. What are the functions of ARP in networking?**

When an incoming packet destined for a host machine on a particular local area network arrives at a [gateway](http://searchnetworking.techtarget.com/definition/gateway), the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply so indicating.

**10. What do you mean by CIDR?**

CIDR (Classless Inter-Domain Routing, sometimes known as *super netting* is a way to allocate and specify the Internet addresses used in inter-[domain](http://searchsoa.techtarget.com/definition/domain) routing more flexibly than with the original system of Internet Protocol (IP) address classes. As a result, the number of available Internet addresses has been greatly increased. CIDR is now the routing system used by virtually all gateway hosts on the Internet's [backbone](http://searchtelecom.techtarget.com/definition/backbone) network.

**11. Define Router.**

* A router operates as the physical, data link and network layer of the OSI model ,
* A router is termed as an intelligent device. Therefore, its capabilities are much more than those of a repeater or a bridge.
* A router is useful for interconnecting two or more heterogeneous networks that differ in their physical characteristics such as frame size, transmission rates, topologies, addressing etc. A router has to determine the best possible transmission path among several available paths.

 **12. What does a router do when it receives a packet with a destination address that it does not have an entry for, in its routing table?**

**Default Router:** If IP Software is not able to find the destination, from routing table then it sends the datagram to default router. It is useful when a site has small set of local address connected to it and connected to the rest of the Internet.

**13. What is fragmentation? Why is it needed?**

Fragmentation is when a datagram has to be broken up into smaller datagram to fit the frame

size of a certain network. Different networks have different MTUs (maximum transfer unit), when a datagram enters a network with a smaller MTU the gateway/router needs to fragment this packet into smaller packets that fit the new MTU.

**14. How many network addresses and host addresses are supported by class A, class B networks?**

Class A: Number of networks = 127 Number of hosts = 224 -1

 Class B : Number of networks = 214 -1 Number of hosts = 216 – 1 = 65,535

**15. Classify the following addresses**

23.8.8.9 ---------- Class A

127.24.34.56 ------------- Class A

159.78.9.10 ------------ Class B

192.20.10.11. ------------ Class C

**16. What does the term ‘cost’ refer to in routing?**

 A hop-count metric simply counts router hops. A bandwidth metric would choose a higher-bandwidth path over a lower-bandwidth link. Load metric reflects the amount of traffic utilizing the links along the path. The best path is the one with the lowest load. Delay is a measure of the time a packet takes to traverse a route. Reliability measures the likelihood that the link will fail in some way and can be either variable or fixed.

**17. What is meant by fixed routing?**

* A route is selected for each source-destination pair of nodes in the network.
* The routes are fixed. Link costs used in designing of routes cannot be based on any dynamic variable such as traffic.
* A **central routing matrix** is created, to be stored perhaps at a network control center. The matrix shows, for each source-destination pair of nodes, the identity of the next node on the route.

**18. What is the RARP?**

RARP (Reverse Address Resolution Protocol) is a [protocol](http://searchnetworking.techtarget.com/definition/protocol) by which a physical machine in a local area network can request to learn its [IP address](http://searchwindevelopment.techtarget.com/definition/IP-address) from a [gateway](http://searchnetworking.techtarget.com/definition/gateway) server's Address Resolution Protocol (ARP) table or cache. A network administrator creates a table in a local area network's gateway [router](http://searchnetworking.techtarget.com/definition/router) that maps the physical machine (or Media Access Control - [MAC address](http://searchnetworking.techtarget.com/definition/MAC-address)) addresses to corresponding Internet

Protocol addresses. When a new machine is set up, its RARP [client](http://searchenterprisedesktop.techtarget.com/definition/client) program requests from the RARP [server](http://whatis.techtarget.com/definition/server) on the router to be sent its IP address.

**19. What is the need for ARP? (May ‘14)**

Address Resolution Protocol (ARP) is a [protocol](http://searchnetworking.techtarget.com/definition/protocol) for mapping an Internet Protocol address ([IP address](http://searchwindevelopment.techtarget.com/definition/IP-address)) to a physical machine address that is recognized in the local network. For example, in IP Version 4, the most common level of IP in use today, an address is 32 bits long. In an [Ethernet](http://searchnetworking.techtarget.com/definition/Ethernet) local area network, however, addresses for attached devices are 48 bits long. (The physical machine address is also known as a Media Access Control or [MAC address](http://searchnetworking.techtarget.com/definition/MAC-address).) A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

**20. How CIDR reduces the number of entries in the routing table? (May ‘14)**

* Restructuring IP address assignments to increase efficiency
* Hierarchical routing aggregation to minimize route table entries

**UNIT - III**

1. **What are the four major aspects of reliable delivery at the transport layer?**

 The four aspects are, Error control Sequence control Loss control and duplication control

1. **What is client process?**
* In the context of a communication session between a pair of processes, the process that initiates

the communication (that is, initially contacts the other process at the beginning of the session) is labeled as the client and the process that waits to be contacted to begin the session is the server.

* A client process makes a request, and a server process responds by returning the requested data.
* Client programs usually manage the user-interface portion of the application, validate data

entered by the user, dispatch requests to server programs, and sometimes execute business logic.

1. **What are the two multiplexing strategies used in transport layer?**
2. **Upward multiplexing**
* Multiplex different transport connections onto one network connection.
* The TL groups transport connections according to their destination and maps

 each group onto the minimum number of network connections.

* Useful when network connections are expensive.
1. **Downward multiplexing**
* Used when high bandwidth connections are needed.
* Open multiple network connections and distribute the traffic among them.
* However, the data links in the subnet must be able to handle this capacity.



1. **What is flow control?**
* In data communications, flow control is the process of managing the rate of data transmission between two nodes to prevent a fast sender from overwhelming a slow receiver.
* It provides a mechanism for the receiver to control the transmission speed, so that the

 receiving node is not overwhelmed with data from transmitting node.

* Preventing senders from overrunning the capacity of the receivers. Flow control is an end to end issue.
1. **Define slow start.**
* Slow-start algorithm is part of the congestion control in TCP, designed to avoid sending more data than the network is capable of transmitting.
* Slow-start algorithm works by increasing the TCP Window by one segment for each acknowledged segment and continues "congestion window" (cwnd) reaches the size of the receivers advertised TCP Receive Window ([RWIN](http://www.speedguide.net/_iframe_term.php?seek=RWIN)), or until [packet loss](http://www.speedguide.net/_iframe_term.php?seek=PACKET%20LOSS) occurs.
* TCP assumes this it is due to network congestion and takes steps to reduce the offered load on the network.
* TCP then enters the linear growth (congestion avoidance) phase. At this point, the window is increased linearly by 1 segment for each [RTT](http://www.speedguide.net/_iframe_term.php?seek=RTT).
1. **List any four QoS parameters.**

 Latency (end- to –end delay.)

 Bandwidth (maximum data transfer rate)

 Throughput. (Rate of successful msg. delivery through a communication channel)

 Jitter

1. **Differentiate flow control from congestion control.**

Flow control: Preventing senders from overrunning the capacity of the receivers. Flow control is an end to end issue.

Congestion Control: Preventing too much data from being injected into the network, thereby causing switches or links to become overloaded. It is concerned with how hosts and network interact.

1. **Differentiate between contention and congestion.**

 Contention occurs when multiple packets have to be queued at a switch because they are competing for the same output link, while congestion means that the switch has so many packets queued that it runs out of buffer space and has to start dropping packets.

1. **What is the main difference between TCP & UDP?**

|  |  |
| --- | --- |
| **TCP** | **UDP** |
| It provides Connection oriented service | Provides connectionless service. |
| Connection Establishment delay will be there | No connection establishment delay |
| Provides reliable service | Provides unreliable, but fast service |
| It is used by FTP, SMTP | It is used by audio, video and multimedia applications. |

1. **Differentiate between Congestion and collision.**

Congestion occurs when the total traffic generated by the host/input link is greater than output link capacity. Collision occurs when multiple hosts compete for common channel access.

1. **What is the wrap around time for TCP Sequence Number? What is the Wrap around time for T3 link with 45 Mbps data rate?**

 Once a segment with sequence number x survives in Internet, TCP cannot use the same sequence number. How fast 32-bit sequence no space can be consumed? 32-bit sequence no is adequate for today’s network.

Wrap Around Time for T3-45Mbps (232 x 8) / 45 Mbps = 763.55 sec = 12.73 min

1. **Name the policies that can control congestion.**

Additive Increase Multiplicative decrease, slow start mechanism,

 Fast retransmit and fast recovery

1. **Name the two protocols available at transport layer.**

 **TCP- (**Transmission control protocol) UDP **(**User Datagram Protocol)

1. **How do transport services differ from the data link layer services?**
* The data link layer services are at node to node level. But the transport layer services are end to end level.
* Both the layers are having the flow control and error control mechanisms. The data link layer offers at node to node level. But the transport layer offers at end to end level.
* Data link layer is responsible for node to node delivery of the frames while transport layer is responsible for end to end delivery of the entire message.
1. **Name the policies that can prevent congestion.**
	* 1. DEC bit. 2) Random Early Detection (RED) 3) Source based congestion avoidance.
2. **What is the significance of Pseudo Header in UDP?**

 **PSEUDO HEADER TCP/UDP**

 To compute checksum, UDP/TCP pretends a pseudo header to datagram.

|  |
| --- |
| Source IP address |
| Destination IP address |
| Zero | Protocol | UDP Length |

 Pseudo header is not transmitted nor they included in length. To compare checksum,

* Store zeroes in CHECKSUM field
* Entire object (pseudo header, header , data) is divided into 16 bits.
* Added & taken ones complemented.

All destination side, s/w finds out pseudo header from IP datagram and does verification. It is useful to find whether datagram has reached correct destination with correct protocol port. It is misdelivered; it would be detected in checksum calculation.

1. **What is silly window syndrome? What is TINYGRAM?**
* The silly window syndrome occurs when either the sender transmits a small segment or the receiver opens the window to a small amount only. Both involve inefficient use of Bandwidth.
* Suppose receiver buffer is full. It advertises window is zero. Sender will not transmit any data to receiver, finally sender buffer will fill.
* As soon as receiver process starts to read again, its advertised window will become > 0 that allows sender to transmit data out of its buffer.
* The sender obliges and sends 1 byte. The buffer is now full, so the receiver acknowledges the

 1 –byte segments but sets the window to 0.

* This behavior can go on forever. Each byte is sent as TCP segment:

1byte data + 20 byte IP header + 20 byte TCP header=41 byte => known as **TINYGRAM’s** overhead is more. ( - for one byte data over head is 40 byte)

1. **What is smart sender/dumb receiver rule?**

Sending side periodically sends the probe segment to make the receive side easy as possible. It simply responds to segments from the sender and it never initiates any activity on its own.

1. **Which protocol is faster either UDP or TCP? Why?**  **(May’ 14)**

UDP is faster than TCP because it is connectionless and need not wait for connection setup and ACK. so it is not at all having reliability as compared to TCP.

1. **Define congestion.**   **(May ‘14)**

Congestion means that the switch has so many packets queued that it runs out of buffer space and has to start dropping packets.

**UNIT - IV**

1. **What is Data compression?**

Data compression enables [devices](http://www.webopedia.com/TERM/D/device.html) to transmit or store the same amount of data in fewer [bits](http://www.webopedia.com/TERM/B/bit.html). Sometimes application programs need to send more data in a timely fashion than the bandwidth of the network supports. it is often important to first compress the data at the sender, then transmit it over the network, and finally to decompress it at the receiver.

1. **What are the two types of compression algorithms?**

There are two classes of compression algorithms. The first, called *lossless compression*, ensures that the data recovered from the compression/decompression process is exactly the same as the original data. A lossless compression algorithm is used to compress file data, such as executable code, text files, and numeric data, because programs that process such file data cannot tolerate mistakes in the data. In contrast, *lossy compression* does not promise that the data received is exactly the same as the data sent.

1. **Define security in networking.**
* Network security consists of the provisions and [policies](http://en.wikipedia.org/wiki/Policies) adopted by a [network administrator](http://en.wikipedia.org/wiki/Network_administrator) to prevent and monitor [unauthorized](http://en.wikipedia.org/wiki/Unauthorized) access, misuse, modification, or denial of a [computer network](http://en.wikipedia.org/wiki/Computer_network) and network-accessible resources.
* Network security involves the authorization of access to data in a network, which is controlled by the network administrator.
* Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.

1. **What is MPEG?**
* Moving Picture Experts Group. Typically used to refer to an algorithm for compressing

Video streams developed by the MPEG.

1. **Compare JPEG, MPEG and MP3.**

MPEG is used for video compressing; JPEG is used for picture compressing, and MP3 is for audio compressing they are all file extensions that indicate what programming was used to digitize the file.

1. **What is PGP?**

 Pretty Good Privacy: A collection of public domain software that provides privacy and authentication capabilities using RSA and that use a mesh of trust for public key distribution.

1. **Define cryptography.**
* Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography is closely related to the disciplines of cryptology and cryptanalysis.
1. **What is TLS and name the protocols that use TLS.**

 A protocol is need for establishing a secure connection between a client and a server. TLS (Transport Layer Security) is capable of authenticating both the client and the server and creating a encrypted connection between the two.

 Eg. [HTTP](http://www.faqs.org/rfcs/rfc2818.html), [IMAP](http://www.faqs.org/rfcs/rfc2595.html), [POP3](http://www.faqs.org/rfcs/rfc2595.html), and [SMTP](http://www.faqs.org/rfcs/rfc2487.html)

1. **What is IPSec?**
* Internet Protocol Security (IPSec) is a [protocol suite](http://en.wikipedia.org/wiki/Protocol_suite) for securing [Internet Protocol](http://en.wikipedia.org/wiki/Internet_Protocol) (IP) communications by [authenticating](http://en.wikipedia.org/wiki/Authentication) and [encrypting](http://en.wikipedia.org/wiki/Encryption) each [IP packet](http://en.wikipedia.org/wiki/Packet_%28information_technology%29#Example:_IP_packets) of a communication session. IPSec includes protocols for establishing [mutual authentication](http://en.wikipedia.org/wiki/Mutual_authentication) between agents at the beginning of the session and negotiation of [cryptographic keys](http://en.wikipedia.org/wiki/Key_%28cryptography%29) to be used during the session.
* IPSec can be used in protecting data flows between a pair of hosts (*host-to-host*), between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).
1. **What are the different wireless network security methods?**

Wi-Fi Protected Access – Both authentication and encryption are done.

(WPA and WPA2)

Wired Equivalent privacy (WEP) - older security method- deals with encryption.

802.1X authentication - Enhance security for 802.11 wireless networks and wired

 Ethernet networks.

1. **Compare SSH, TLS/ SSL and IPSec.**

|  |  |  |  |
| --- | --- | --- | --- |
| **SSH**(Secure Shell ) | **TLS**(Transport Layer Security­)  | **SSL**(Secure Socket Layer) | **IPSec****(**Inter Protocol Security**)** |
| Implemented at Application Layer | Implemented at Transport Layer | Implemented at Transport Layer | Implemented atNetwork/Internet layer |
| Used for various shell based protocols such as telnet, and other remote logins as well as file transfer protocols such as FTP | Used for Session Initiation Protocol (SIP), ecommerce solutions such as online banking | Used for http sessions. | Used to secure any transport protocol or any application. |
| Uses public key cryptography | Uses PKI and Symmetric key encryption | Uses PKI and Symmetric key encryption. | Pre-shared key is used. |
| Application dependent. | Application dependent. | Application dependent. | Application independent. |
| Supports TCP only | Supports TCP only. | Supports TCP only. | Supports any packet |

1. **What is digital signature?**

A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender such that they cannot deny sending it ([authentication](http://en.wikipedia.org/wiki/Authentication) and [non-repudiation](http://en.wikipedia.org/wiki/Non-repudiation)) and that the message was not altered in transit ([integrity](http://en.wikipedia.org/wiki/Integrity)).

1. **Distinguish between symmetric / secret key cryptography and asymmetric / public key cryptography.**

|  |  |
| --- | --- |
| **Symmetric / Secret key cryptography** | **Asymmetric /Public key cryptography** |
| Sender and recipient share a common secret key for both encryption and decryption. | Each user has a pair of keys. One of which is public, used for encryption and the other is kept secret, used for decryption. |
| Symmetric encryption is typically faster than asymmetric. | Slower than symmetric cryptography. |
| Distribution of large numbers of keys securely is needed before cryptographic process. | Since public key is used for encryption and private key for decryption, no need to exchange the keys. |
| Ex: Data Encryption standard (DES) Triple DES and the Advanced Encryption Standard. (AES) | Ex :RSA |

1. **How many symmetric keys are needed for n persons to communicate in symmetric key cipher?**

Number of symmetric keys = nc2

1. **What is a session key ?**

A session key is a key used to secure a single, relatively short episode of communication: a session. Each distinct session between a pair of participants uses a new session key, which is always a symmetric-key key for speed.

1. **What are the limitations firewalls?**

A firewall cannot protect against:

* Malicious insiders.
* Connections that circumvent it.
* Completely new threats.
* Some viruses.
* the administrator that does not correctly set it up
1. **What is PKI? What is its purpose?**

A complete scheme for certifying bindings between public keys and identities— what key belongs to whom—is called a *public key infrastructure (PKI)*. A PKI starts with the ability to verify identities and bind them to keys out-of-band.

1. **Mention one protocol that establishes session without any pre distributed keys.**

The Diffie-Hellman key agreement protocol establishes a session key without using any redistributed keys.

1. **What is the principle of symmetric key encryption ?**  **(May’14)**

A symmetric encryption scheme has five ingredients:

– Plaintext - m

– Encryption algorithm - Ek(m)

– Secret Key - k

– Cipher text - C

– Decryption algorithm - Dk(Ek(m))

1. **What is firewall? Specify the use of packet filtering firewall.**   **(May’14)**
* A firewall is a system that is the sole point of connectivity between the site it protects and the

rest of the network.

* It is usually implemented as part of a router, although a personal firewall may be implemented on an end-user machine.

 Uses of Packet filtering firewall:

* Packet filtering prevents attacks from computers outside a local area network (LAN).
* It is standard and cost-effective.
* Filtering with incoming or outgoing interfaces - Ingress filtering of spoofed IP addresses and Egress filtering to restrict the flow of information from one network to another.
* Permits or denies certain services.

 **UNIT-V**

**Part-A**

1. **List the capabilities provided by the Session initiation Protocol**.

The capabilities provided by the SIP can be grouped into five categories:

* User location
* User availability
* User capabilities
* Session setup
* Session management
1. **What is Domain Name System**.

The Domain Name System (DNS) is a [hierarchical](http://en.wikipedia.org/wiki/Hierarchical) distributed naming system for computers, services, or any resource connected to the [Internet](http://en.wikipedia.org/wiki/Internet) or a [private network](http://en.wikipedia.org/wiki/Private_network). It associates various information with [domain names](http://en.wikipedia.org/wiki/Domain_name) assigned to each of the participating entities. The Domain Name System converts domain names (of the form [www.vtubooks.com](http://www.vtubooks.com/)) into IP numbers.

1. **What is Session Description Protocol (SDP)?**

SDP is rather general protocol that can be used in a variety of situation. It conveys the following information:

The name and purpose of the session.

Start and end time of the session.

The media types that comprise the session.

Detailed information needed to receive the session.

1. **What are the four main properties of HTTP?**

Global Uniform Resource Identifier.

Request-response exchange.

Statelessness.

Resource metadata.

1. **List the HTTP Headers.**

The four groups of HTTP headers are General headers, Entity Headers, Request Headers and Response Headers.

1. **Write about World Wide Web.**

The World Wide Web has been so successful and has made the Internet accessible to so many people that sometimes it seems to be synonymous with the Internet. One helpful way to think of the Web is as a set of cooperating clients and servers, all of whom speak the same language: HTTP.

1. **What are advantages of persistent connection?**

Persistent connections have two advantages. First, they obviously eliminate the connection setup overhead, thereby reducing the load on the server, the load on the network caused by the additional TCP packets, and the delay perceived by the user. Second, because a client can send multiple request messages down a single TCP connection, TCP’s congestion window mechanism is able to operate more efficiently.

1. **Give short notes on URL**.

A uniform resource locator, abbreviated URL, also known as web address, is a specific [character string](http://en.wikipedia.org/wiki/Character_string) that constitutes a reference to a resource. In most [web browsers](http://en.wikipedia.org/wiki/Web_browser), the URL of a web page is displayed on top inside an [address bar](http://en.wikipedia.org/wiki/Address_bar).

1. **What are the transmission modes of FTP?**

Stream mode: Default mode and data is delivered from FTP to TCP as a continuous stream of data.

Block mode: Data is delivered from FTP to TCP in terms of blocks. Each data block follows the three byte header.

Compressed mode: File is compressed before transmitting if size is big. Run length encoding method is used for compression.

1. **What is a namespace?**

The naming system on which DNS is based is a hierarchical and logical tree structure called the domain namespace. Organizations can also create private networks that are not visible on the Internet, using their own domain namespaces.

1. **Give short notes on URI.**

URI contains location information about the resource (e.g.,Web page). A SIP URI provides complete identification of a user, but does not provide his location, since that may change over time.

1. **What is MIB?**

MIB: Object is a data variable that represents one aspect of the management agent. It represents resources. A collection of objects is known as MIB.A management station performs Monitoring MIB objects, Retrieving MIB objects value, Change MIB object value.

1. **List the Different classification of DNS servers. (May ‘14)**

Internet is divided into many top level domains. Each domain is divided into sub domain and so on. Topmost domains are categorized into generic and countries.

**Generic domain categories are**:

com-commercial

gov-US government

edu-educational

org-profile organization

mil-US military

Net-network providers.

**Country category** uk - United kingdom,jp - Japan,in –India

1. **What is the use of MIME?**

MIME converts binary files, executed files into text files. Then only it can be transmitted using SMTP.SMTP cannot transmit text data including national language characters. MIME translates all these non ASCII codes to SMTP 7 bit ASCII code. Messages – more than certain size can be translated by MIME into SMTP acceptable size.

1. **Describe why HTTP is designed as a stateless protocol.**

Maintaining state across request-response connections significantly increase the initial interactions in a connection since the identity of each party needs to be established and any saved state must be retrieved. HTTP is therefore stateless to ensure that the Internet is scalable since state is not contained in the HTTP request/response pairs by default.

1. **What is the use of web services? (May ‘14)**

A web service is a method of communication between two electronic devices over the [World Wide Web](http://en.wikipedia.org/wiki/World_Wide_Web). A web service is a software function provided at a network address over the web or the cloud, it is a service that is "always on" as in the concept of [utility computing](http://en.wikipedia.org/wiki/Utility_computing).

1. **Describe WSDL.**

The Web Services Description Language is an [XML](http://en.wikipedia.org/wiki/XML)-based [interface description language](http://en.wikipedia.org/wiki/Interface_description_language) that is used for describing the functionality offered by a [web service](http://en.wikipedia.org/wiki/Web_service). A WSDL description of a web service (also referred to as a WSDL file) provides a machine-readable description of how the service can be called, what parameters it expects, and what data structures it returns.

1. **Compare the HTTP and FTP.**

|  |  |
| --- | --- |
| **FTP** | **HTTP** |
| FTP transfers the file from client to server and server to client. | HTTP transfer the file from server to client.(i.e. web pages) |
| It uses two different port connections. (i.e. port 20 and port 21) | HTTP use only one port connection. (i.e. Port 80) |
| Uses TCP protocol. | It also uses TCP protocol. |
| Out – of – band | In – band |

1. **Define NIC and NAT.**

A domain name registry, also called Network Information Centre (NIC), is part of the Domain Name System (DNS) of the Internet which converts domain names to IP addresses.

NAT: In computer networking, network address translation (NAT, also known as network masquerading, native address translation or IP masquerading) is a technique of transcribing network traffic through a router that involves re-writing the source and/or destination IP addresses and usually also the TCP/UDP port numbers of IP packets as they pass through. Most systems using NAT do so in order to enable multiple hosts on a private network to access the Internet using a single public IP address.

1. **Write about SOAP protocol.**

SOAP, originally defined as Simple Object Access Protocol, is a [protocol](http://en.wikipedia.org/wiki/Protocol_%28computing%29) specification for exchanging structured information in the implementation of [Web Services](http://en.wikipedia.org/wiki/Web_Service) in [computer networks](http://en.wikipedia.org/wiki/Computer_network). It relies on [Extensible Markup Language](http://en.wikipedia.org/wiki/XML) (XML) for its message format, and usually relies on other [Application Layer](http://en.wikipedia.org/wiki/Application_Layer) protocols.