6 Computer Networks & Network Security

1. Concept of Layering

01. In which layer of network architecture, the secured socket layer (SSL) is used?
(a) physical layer (b) session layer
(c) application later (d) presentation layer
[ISRO - 2011]

02. What frequency range is used for microwave communications, satellite and radar?
(a) Low frequency: 30 kHz to 300 kHz
(b) Medium frequency: 300 kHz to 3 MHz
(c) Super high frequency: 3000 MHz to 30000 MHz
(d) Extremely high frequency: 30000 kHz
[ISRO - 2015]

03. Which layers of the OSI reference model are host-to-host layers?
(a) Transport, session, presentation, application
(b) Session, presentation, application
(c) Datalink, transport, presentation, application
(d) Physical, datalink, network, transport
[ISRO - 2015]

04. Assume that Source S and Destination D are connected through an intermediate router R. How many times a packet has to visit the network layer and data link layer during a transmission from S to D?
(a) Network layer – 4 times, Data link layer – 4 times
(b) Network layer – 4 times, Data link layer – 6 times
(c) Network layer – 2 times, Data link layer – 4 times
(d) Network layer – 3 times, Data link layer – 4 times
[ISRO - 2017(Dec)]

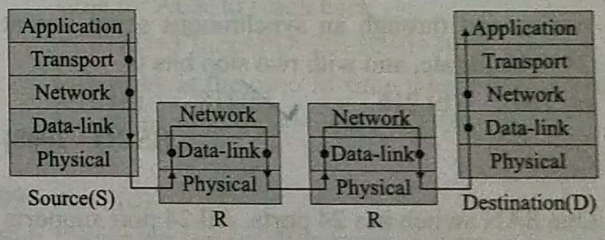
KEY & Detailed Solutions			
01. (d)	02. (d)	03. (a)	04. (b)

01. Ans: (d)
Sol: SSL operates over some reliable transport layer protocols, which places them as application layer protocols in the TCP/IP reference model and as presentation layer protocols in the OSI model.

02. Ans: (d)
Sol: The range of microwave magnetic radiation ranging from 1 meter to 1 millimeter and their corresponding frequency ranges from 3000 MHz to 300 GHz, So an Extremely high frequency will be used like 30000 KHz to communicate with Radar and Satelite.

03. Ans: (a)
Sol: In OSI Model, Physical; Datalink and Network layer are hop-to-hop layers whereas Transport, Session, Presentation and Application layer are end-to-end or host-to-host layers.

04. Ans: (b)
Sol:



2. Network Performance parameters

01. Assume that each character code consists of 8 bits. The number of characters that can be transmitted per second through an synchronous serial line at 2400 baud rate, and with two stop bits is
(a) 109 (b) 216
(c) 218 (d) 219
[ISRO - 2007]

02. If the bandwidth of a signal is 5 kHz and the lowest frequency is 52 kHz, what is the highest frequency
(a) 5 kHz (b) 10 kHz
(c) 47 kHz (d) 57 kHz
[ISRO - 2007]

03. IEEE 802.11 is standard for
(a) Ethernet
(b) Bluetooth
(c) Broadband Wireless
(d) Wireless LANs
[ISRO - 2007]

04. What is the bandwidth of a signal that ranges from 40 kHz to 4 MHz?
(a) 36 MHz (b) 360 kHz
(c) 3.96 MHz (d) 396 kHz
[ISRO - 2008]

05. Assume that each character code consists of 8 bits. The number of characters that can be transmitted per second through an synchronous serial line at 2400 baud rate, and with two stop bits is
(a) 109 (b) 216 (c) 218 (d) 219
[ISRO - 2008]

06. One SAN switch has 24 ports. All 24 port supports 8 Gbps Fiber Channel technology. What is the aggregate bandwidth of that SAN switch?
(a) 96 Gbps (b) 192 Mbps
(c) 512 Gbps (d) 192 Gbps
[ISRO - 2011]

07. What is the maximum number of characters (7 bits + parity) that can be transmitted in a second on a 19.2 kbps line. This asynchronous transmission requires 1 start bit and 1 stop bit.
(a) 192 (b) 240 (c) 1920 (d) 1966
[ISRO - 2013]

08. What will be the efficiency of a Stop and Wait protocol, if the transmission time for a frame is 20ns and the propagation time is 30ns?
(a) 20% (b) 25%
(c) 40% (d) 66%
[ISRO - 2013]

09. Consider a 50 kbps satellite channel with a 500 milliseconds round trip propagation delay. If the sender wants to transmit 1000 bit frames, how much time will it take for the receiver to receive the frame?
(a) 250 milliseconds
(b) 20 milliseconds
(c) 520 milliseconds
(d) 270 milliseconds
[ISRO - 2014]

10. A T-switch is used to
(a) Control how messages are passed between computers
(b) Echo every character that is received
(c) Transmit characters one at a time
(d) Rearrange the connections between computing equipments
[ISRO - 2015]

11. How many characters per sec (7 bits + 1 parity) can be transmitted over a 2400 bps line if the transfer is synchronous (1 start and 1 stop bit)?
(a) 300 (b) 240
(c) 250 (d) 275 **[ISRO - 2015]**

12. 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). What is the minimum number of bits (i) that will be required to represent the sequence numbers distinctly? Assume that no time gap needs to be given between transmission of two frames.

(a) i = 2 (b) i = 3
(c) i = 4 (d) i = 5

[ISRO - 2016]

KEY & Detailed Solutions			
01. (c)	02. (d)	03. (d)	04. (c)
05. (c)	06. (b)	07. (c)	08. (b)
09. (d)	10. (d)	11. (a)	12. (d)

01. Ans: (c)

Sol: Serial port is capable of transferring 2400 bits per second

Character code consist of 8 bit with 1 start and 2 stop bit , therefore total character = 11 bits

Number of character that can be transmitted per second = 2400/11 = 218 (asynchronus mode is considered)

02. Ans: (d)

Sol: Bandwidth = Highest frequency − lowest frequency

52 = Highest frequency − 5

Highest frequency = 57

03. Ans: (d)

Sol:
- 802.3 Ethernet Working Group
- 802.11 Wireless LAN Working Group

04. Ans: (c)

Sol: Bandwidth = $F_h - F_i$

= (4 – 0.4) MHz

= 3.96 MHz

05. Ans: (c)

Sol:

Frame: Size	Start 1bits	Data 5-9 bits	Parity 0-1bits	Stop 1-2bits

"2400 baud" means that the serial port is capable of transferring a maximum of 2400 bits per second."

Therefore, transmission rate here = 2400 bps

An eight bit data (which is a char) requires 1 start bit, 2 stop bits = 11 bits.

So, the number of characters transmitted per second = 2400 / 11 = 218.18.

Since we can only count the fully transmitted ones, we take floor = 218

06. Ans: (b)

Sol: 24 * 8 = 192 gbps full duplex bandwidth

07. Ans: (c)

Sol: 10 bit now is required to send 1 character

Why 10 bit ?

1 character = 7 bit + 1 parity (according to question)

Now, In asynchronous transmission

1 character = (8 bit (we calculated above) + 1 start bit + 1 stop bit)

1 character = 10 bit

Number of character that can be send is 19200/10 = 1920 character.

08. Ans: (b)

Sol: Transmission time = 20ns.

Time for ACK to reach back

=TT+PD+TTack+PD=20+30+0+30=80ns.

Efficiency is the ratio of time where useful data is sent to the total time = 20/80 = 25%

09. Ans: (d)

Sol: Round trip time =2*Propagation time

i.e Propagation time =500/2= 250 ms

Transmission time = Message size / bandwidth

i.e 1000 bits / 50 kbps = 20 ms

Time to receive the frame by the receiver

i.e 250 + 20 = 270 ms

10. Ans: (d)

Sol: The T-Switch is a "passive" in which **information** can be sent in both Input and output directions. Either side of the T-Switch can be the "input" or "output" side.
Also, T-switch is used to rearrange the connection between computing equipment.

11. Ans: (a)

Sol: Size of each character = (7+1)bits = 8 bits
Bandwidth = 2400 bps
Number of characters to be transmitted = 2400/8
= 300

Note: Synchronous mode doesn't use start/stop bits

12. Ans: (d)

Sol: Propagation time is given as 25ms.
Bandwidth $=10^6$bps.
So, to fully utilize the channel, we must send 10^6 bits into the channel in a second, which will be 1000 frames per second as each frame is 1000 bits.
Now, since the propagation time is 25ms, to fully pack the link we need to send at least $1000\times25\times10^{-3}=25$ frames.
So, we need $\lceil \log_2 25 \rceil = 5$bits.

3. LAN Technologies

01. An Ethernet hub
(a) functions as a repeater
(b) connects to a digital PBX
(c) connects to a token-ring network
(d) functions as a gateway
[ISRO - 2007]

02. Phase transition for each bit are used in
(a) Amplitude modulation
(b) Carrier modulation
(c) Manchester encoding
(d) NRZ encoding
[ISRO - 2007]

03. On a LAN, where are IP datagrams transported?
(a) In the LAN header
(b) In the Application field.
(c) In the information field of the LAN frame.
(d) After the TCP header.
[ISRO - 2008]

04. In Ethernet, the source address field in the MAC frame is the _____ address.
(a) original sender's physical
(b) previous station's physical
(c) next destination's physical
(d) original sender's service port
[ISRO - 2008]

05. Which of the following transmission media is not readily suitable to CSMA operation?
(a) Radio (b) Optical fibers
(c) Coaxial cable (d) Twisted pair
[ISRO - 2008]

06. Which Project 802 standard provides for a collision - free protocol ?
(a) 802.2 (b) 802.3
(c) 802.5 (d) 802.6
[ISRO - 2008]

07. In networking, UTP stands for
(a) Unshielded T-connector port
(b) Unshielded twisted pair
(c) Unshielded terminating pair
(d) Universal transmission process
[ISRO - 2009]

08. What is the primary purpose of a VLAN?
(a) Demonstrating the proper layout for a network
(b) Simulating a network
(c) To create a virtual private network
(d) Segmenting a network inside a switch or device
[ISRO - 2009]

09. The encoding technique used to transmit the signal in giga ethernet technology over fiber optic medium is
(a) Differential manchester encoding
(b) Non Return to zero
(c) 4B/5B encoding
(d) 8B/10B encoding **[ISRO - 2011]**

10. The IEEE standard for WiMax technology is
(a) IEEE 802.16 (b) IEEE 802.36
(c) IEEE 812.16 (d) IEEE 806.16
[ISRO - 2011]

11. In the Ethernet, which field is actually added at the physical layer and is not part of the frame
(a) preamble (b) CRC
(c) address (d) location
[ISRO - 2013]

12. Ethernet layer-2 switch is a network element type which gives
(a) different collision domain and same broadcast domain
(b) different collision domain and different broadcast domain
(c) same collision domain and same broadcast domain
(d) same collision domain and different broadcast domain
[ISRO - 2013]

13. A mechanism or technology used in Ethernet by which two connected devices choose common transmission parameters such as speed, duplex mode and flow control is called
(a) Autosense (b) Synchronization
(c) Pinging (d) Auto negotiation
[ISRO - 2014]

14. Which of the following is not a valid multicast MAC address?
(a) 01:00:5E:00:00:00
(b) 01:00:5E:00:00:FF
(c) 01:00:5E:00:FF:FF
(d) 01:00:5E:FF:FF:FF
[ISRO - 2014]

15. In Ethernet CSMA/CD, the special bit sequence is transmitted by media access management to handle collision is called
(a) Preamble (b) Postamble
(c) Jam (d) None of these
[ISRO - 2016]

16. In a token ring network, the transmission speed is 10^7 bps and the propagation speed is 200 m/μs. Then 1 bit delay in this network is equivalent to
(a) 500 m of cable (b) 200 m of cable
(c) 20 m of cable (d) 50 m of cable
[ISRO - 2016]

17. Physical topology of FDDI is?
(a) Bus (b) Ring
(c) Star (d) None of the above
[ISRO - 2017(May)]

18. In network terminology UTP means
(a) Uniquitous teflon port
(b) Uniformly terminating port
(c) Unshielded twisted pair
(d) Unshielded T-connector port
[ISRO - 2017(May)]

19. If there are n devices (nodes) in a network, what is the number of cable links required for a fully connected mesh and a star topology respectively
(a) n(n−1)/2, n−1 (b) n, n−1
(c) n−1, n (d) n−1, n(n−1)/2
[ISRO - 2017(May)]

20. Which media access control protocol is used by IEEE 802.11 wireless LAN?
(a) CDMA (b) CSMA/CA
(c) ALOHA (d) None of the above
[ISRO - 2017(May)]

21. An Ethernet frame that is less than the IEEE 802.3 minimum length of 64 octets is called
(a) Short frame (b) Small frame
(c) Mini frame (d) Runt frame
[ISRO - 2017(May)]

22. The default subnet mask for a class B network can be
(a) 255.255.255.0 (b) 255.0.0.0
(c) 255.255.192.0 (d) 255.255.0.0
[ISRO - 2017(May)]

23. To send same bit sequence, NRZ encoding require
(a) Same clock frequency as Manchester encoding
(b) Half the clock frequency as Manchester encoding
(c) Twice the clock frequency as Manchester encoding
(d) A clock frequency which depend on number of zeros and ones in the bit sequence
[ISRO - 2020]

KEY & Detailed Solutions				
01. (a)	02. (c)	03. (c)	04. (b)	05. (a
06. (c)	07. (b)	08. (d)	09. (d)	10. (a
11. (a)	12. (a)	13. (d)	14. (d)	15. (c
16. (c)	17. (b)	18. (c)	19. (a)	20. (c
21. (d)	22. (d)	23. (b)		

01. Ans: (a)
Sol: An Ethernet hub also known as repeater hub is used for connecting multiple ethernet devices

02. Ans: (c)
Sol: In manchester encoding phase transition for each bit is used
A non-return-to-zero (NRZ) line code is a binary code in which ones are represented by one significant condition, usually a positive voltage, while zeros are represented by some other significant condition, usually a negative voltage, with no other neutral or rest condition.

03. Ans: (c)
Sol: Actually IP datagram is insulated in the payload field of the Ethernet frame
According to option (c) , in the information field of the LAN , IP datagram is present

04. Ans: (b)
Sol: DESTINATION ADDRESS is next physical address
SOURCE ADDRESS is previous source address not the original source address
In 802.3(Ethernet) MAC Frame :
Source Address(SA): Consists of 6 bytes. This is the physical address of the sender of the frame.

05. Ans: (a)

Sol: Radio waves are not suitable for CSMA operation.
Wireless medium is not suitable for collision detection methods
For wireless N/W instead of CSMA it uses CSMA/CA (Carrier sense multiple access/Collision avoidance).

06. Ans: (c)

Sol: IEEE 802.2 is the logical link control of data link layer of OSI model
IEEE 802.6 is the standard govern by ANSI for MetroPolitan Area Network
In IEEE 802.5, the token passing scheme is used in place of Carrier Sense Multiple Access with Collision Detection (CSMA/CD) on a ring topology local area network (LAN).

07. Ans: (b)

Sol: UTP stands for Unshielded twisted pair. It consists of two unshielded wires twisted around each other.
Mainly it is used for LAN and telephone networks.

08. Ans: (d)

Sol: VLAN: Actually the physical system can be placed anywhere but logically they are belonging to a group.
VLANs address issues such as scalability, security, and network management

09. Ans: (d)

Sol: 8B/10B encoding is used, as this layer describes the byte synchronization and the encode/decode scheme which transmits 8 bits as a 10-bit code group. The features of this scheme are low-cost component design and good transition density for easy clock recovery.

10. Ans: (a)

Sol: IEEE 802.16 is used for WiMax technology
WiMax is "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL"

11. Ans: (a)

Sol: The first field(Preamble) of the 802.3 frame contains 7 bytes of alternating 0s and 1s that alerts the receiving system to the coming frame and enables it to synchronize its input timing. Preamble is added at the physical layer and is not part of the frame.

12. Ans: (a)

Sol: A broadcast domain is a logical division of a computer network, in which all nodes can reach each other by broadcast at the data link layer.
A collision domain is the set of LAN interfaces whose frames could collide with each other
Switch is a collision domain separator but not broadcast domain separator.

13. Ans: (d)

Sol: **Ping:** Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network. It measures the round-trip time for messages sent from the originating host to a destination computer that are echoed back to the source.

Autosense: Autosense refers to a feature found in network adapters that allows them to automatically recognize the current local network's speed and adjust its own setting accordingly. It is often used with Ethernet, Fast Ethernet, switches, hubs and network interface cards.

Process synchronization: Process synchronization refers to the idea that multiple processes are to join up or handshake at a certain point, in order to reach an agreement or commit to a certain sequence of action. Data synchronization refers to the idea of keeping multiple copies of a dataset in coherence with one another, or to maintain data integrity, Process synchronization primitives are commonly used to implement data synchronization.

Auto-negotiation: Auto-negotiation is a signaling mechanism and procedure used by Ethernet over twisted pair by which two connected devices choose common transmission parameters, such as speed, duplex mode, and flow control. Auto-negotiation is defined in clause 28 of IEEE 802.3. and was originally an optional component in the Fast Ehternet standard.

14. Ans: (d)

Sol: A multicast addressed frame is either flooded out all ports (if no multicast optimization is configured) or sent out only the ports interested in receiving the traffic.

The range of multicast MAC Address lie between 01-00-5E-00-00-00 to 01-00-5E-7F-FF-FF.

15. Ans: (c)

Sol: The ethernet CSMA/CD,the special bit sequence transmitted by media access management to handle collision, is called Jam signal.

16. Ans: (c)

Sol: Transmission delay for 1 bit $t = 1/(10^7) = 0.1$ microseconds.

200 meters can be traveled in 1 microsecond. Therefore, in 0.1 microseconds, 20 meters can be traveled.

17. Ans: (b)

Sol: FDDI (Fiber Distributed Data Interface) is a set of ANSI and ISO standards for data transmission on fiber optic lines in a local area network (LAN) that can extend in range up to 200 km (124 miles). The FDDI protocol is based on the token ring protocol.

18. Ans: (c)

Sol: UTP is the Unshielded Twisted Pair cable. It consists of 2 unshielded wires twisted together. These are used extensively in LANs and telephone cables.

19. Ans: (a)

Sol: In a fully mesh network every node should be connected to every other node, hence $\binom{n}{2}$ $n(n-1)/2$ links will be there.

In star topology $n-1$ nodes are connected to network at center. Hence $n-1$ links will be there.

20. Ans: (b)

Sol:
- The IEEE 802.11 MAC protocol is a carrier sense multiple access protocols, it also has collision avoidance (CA).
- CSMA/CA is Carrier Sense Multiple Access/ Collision Avoidance.
- In this multiple access protocol, the station senses the medium before transmitting the frame.
- This protocol has been developed to improve the performance of CSMA.
- CSMA/CA is used in 802. 11 based wireless LANs.

21. Ans: (d)

Sol: A runt frame is an Ethernet frame that is less than the IEEE 802.3's minimum length of 64 octets. Runt frames are most commonly caused by collisions. other possible causes are malfunctioning of network card, buffer under run, duplex mismatch or software issues.

22. Ans: (d)

Sol: Default subnet mask of class B network is 255.255.0.0.

23. Ans: (b)

Sol: To send same bit sequence, NRZ encoding requires half the clock frequency as Manchester encoding.

4. Datalink Layer

01. Bit stuffing refers to
(a) inserting a '0' in user stream to differentiate it with a flag
(b) inserting a '0' in flag stream to avoid ambiguity
(c) appending a nibble to the flag sequence
(d) appending a nibble to the use data stream
[ISRO - 2007]

02. Data is transmitted continuously at 2.048 Mbps rate for 10 hours and received 512 bit errors. What is the bit error rate?
(a) 6.9 e–9 (b) 6.9 e–6
(c) 69 e–9 (d) 4 e–9
[ISRO - 2011]

03. If the frame to be transmitted is 1101011011 and the CRC polynomial to be used for generating checksum is x^4+x+1, then what is the transmitted frame?
(a) 11010110111011
(b) 11010110111101
(c) 11010110111110
(d) 11010110111001
[ISRO - 2013]

04. A certain population of ALOHA users manages to generate 70 request/sec. If the time is slotted in units of 50 msec, then channel load would be
(a) 4.25 (b) 3.5
(c) 450 (d) 350
[ISRO - 2015]

05. In CRC if the data unit is 100111001 and the divisor is 1011 then what is dividend at the receiver?
(a) 10011101101
(b) 100111001011
(c) 100111001
(d) 100111001110
[ISRO - 2015]

06. Bit stuffing refers to
(a) Inserting a '0' in user stream to differentiate it with a flag
(b) Inserting a '0' in flag stream to avoid ambiguity
(c) Appending a nibble to the flag sequence
(d) Appending a nibble to the user data stream
[ISRO - 2016]

07. 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
(a) 11001001000 (b) 11001001011
(c) 11001010 (d) 110010010011
[ISRO - 2016]

08. Station A uses 32 byte packets to transmit messages to Station B using a sliding window protocol. The round trip time delay between A and B is 40 ms and the bottleneck bandwidth on the path A and B is 64 kbps. What is the optimal window size that A should use?
(a) 5 (b) 10
(c) 40 (d) 80
[ISRO - 2017(Dec)]

09. 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 ms and the bottleneck bandwidth on the path between A and B is 128 kbps. What is the optional window size that A should use?
(a) 20 (b) 40
(c) 160 (d) 320
[ISRO - 2018]

10. Assuming that for a given network layer implementation, connection establishment overhead is 100 bytes and disconnection overhead is 28 bytes. What would be the minimum size of the packet the

transport layer needs to keep up, if it wishes to implement a datagram service above the network layer and needs to keep its overhead to a minimum of 12.5%. (ignore transport layer overhead)

(a) 512 bytes (b) 768 bytes
(c) 1152 bytes (d) 1024 bytes

[ISRO - 2018]

KEY & Detailed Solutions

01. (a)	02. (a)	03. (c)	04. (b)	05. (b)
06. (a)	07. (b)	08. (b)	09. (b)	10. (d)

01. Ans: (a)

Sol: Insertion of a 0 in user stream to differentiate with a flag is Bit stuffing.

02. Ans: (a)

Sol: Bandwidth is given 2.048 Mbps

We know, The bit error rate (BER) is the number of bit errors per unit time

In 10 hrs , 512 bits per unit time

so in 1 sec, we can send = 0.0142 bit error.

error rate is $0.0142/2.048 \times 10^6$

6.944×10^{-9}

03. Ans: (c)

Sol: Append (number of bits in divisor - 1) number of zeros at the end of data unit

Data unit = 1101011011, Divisor = 10011,

So, append 4 zeros at the end.

= 11010110110000

```
10011) 11010110110000 ( 101000001
       10011
       --------
        10011
        10011
        ---------
          10110
          10011
          --------
           10100
           10011
           --------
            1110
```

1110 must be appended.

04. Ans: (b)

Sol: Channel load = number of request in 1-second ÷ number of slots in 1 second

No. of request - 70 requests/sec

One time slot is of 50 ms then the total number of time slots in 1 second → $\frac{1000\text{ms}}{50\text{ms}}$ → 20 slots

Channel load = $\frac{70}{20} = 3.5$

05. Ans: (b)

Sol: Append (number of bits in divisor − 1) number of zeroes at the end of data unit

Data unit = 100111001, append 3 zeroes at the end

= 100111001000

```
1011) 100111001000 ( 101000001
      1011
      ------
        1011
        1011
        -------
            1000
            1011
            --------
             011
```

= 100111001(000) xor (011)

= 100111001011

06. Ans: (a)

Sol: Bit stuffing refers to inserting a 0 in user stream to differentiate it with a flag

Each frame begins and ends with a special bit pattern called a flag byte

01111110.

Whenever sender data link layer encounters five consecutive ones in the data stream, it automatically stuffs a 0 bit into the outgoing stream.

When the receiver sees five consecutive incoming ones followed by a 0 bit, it automatically destuffs the 0 bit before sending the data to the network layer

07. Ans: (b)

Sol: The polynomial x^3+1 corresponds to divisor is 1001.

11001001 000 ← input right padded by 3 bits

1001 ← divisor

```
1001) 11001001000(
      1001
       1011
       1001
         1000
         1001
           1100
           1001
            1010
            1001
             011
```

08. Ans: (b)

Sol: Transmission delay

= Packet Length/Bandwidth

= 32 Byte/(64 Kbps);

= 32 Byte/(64/8 KBps);

transmission delay = 4ms

Given RTT = 40ms

RTT = 2× propagation delay

Propagation delay = 20ms

a = Propagation delay/ Transmission delay

a = 20/4 = 5

N = 1 + 2a

Therefore,

1 + 10 = 11 Packets.

Usually Some author ignore "1" in "1 + 2a" formulae...

Hence, Answer can be 10 or 11.

09. Ans: (b)

Sol: Efficiency $(\eta) = \frac{N \times T_t}{T_t + 2 \times T_p}$

To get optimal window size: $\eta = 1$

$$N = \frac{T_t + 2 \times T_p}{T_t}$$

$$N = 1 + \frac{2 \times T_p}{T_t}$$

$$N = 1 + \frac{80}{2}$$

$N = 41$

Sometimes 1 is ignored. If 1 is ignored, then

$$N = \frac{2 \times T_p}{T_t}$$

$$N = \frac{80}{2}$$

$N = 40$

The optimal window size that A should use is 40.

10. Ans: (d)

Sol: Let the size of the transport layer packet i.e size of datagram payload be x. Connection Establishment Overhead = 100 Bytes

Disconnection Overhead = 28 Bytes

Total overhead = 100 + 28 = 128 Bytes

Now transport layer wants to keep an overhead to a minimum of 12.5%

So 12.5% of x = 128

$$\frac{12.5}{100} * x = 128$$

$$x = \frac{128 * 100}{12.5}$$

= 1024 Bytes

5. Network Layer(IPv4)

01. Range of IP Address from 224.0.0.0 to 239.255.255.255 are
(a) Reserved for loopback
(b) Reserved for broadcast
(c) Used for multicast packets
(d) Reserved for future addressing
[ISRO - 2007]

02. When a host on network A sends a message to a host on network B, which address does the router look at?
(a) Port (b) IP
(c) Physical (d) Subnet mask
[ISRO - 2007]

03. The subnet mask 255.255.255.192
(a) extends the network portion to 16 bits
(b) extends the network portion to 26 bits
(c) extends the network portion to 36 bits
(d) has no effect on the network portion of an IP address
[ISRO - 2008]

04. The network 198.78.41.0 is a
(a) Class A network (b) Class B network
(c) Class C network (d) Class D network
[ISRO - 2008]

05. The subnet mask for a particular network is 255.255.31.0 which of the following pairs of IP addresses could belong to this network ?
(a) 172.57.88.62 and 172.56.87.23
(b) 10.35.28.2 and 10.35.29.4
(c) 191.203.31.87 and 191.234.31.88
(d) 128.8.129.43 and 128.8.161.55
[ISRO - 2009]

06. The address resolution protocol (ARP) is used for
(a) Finding the IP address from the DNS
(b) Finding the IP address of the default gateway
(c) Finding the IP address that corresponds to a MAC address
(d) Finding the MAC address that corresponds to an IP address
[ISRO - 2009]

07. Which of the following is a MAC address?
(a) 192.166.200.50
(b) 00056A:01A5CCA7FF60
(c) 568, Airport Road
(d) 01:A5:BB:A7:FF:60
[ISRO - 2009]

08. Use of IPSEC in tunnel mode results in
(a) IP packet with same header
(b) IP packet with new header
(c) IP packet without header
(d) No changes in IP packet
[ISRO - 2009]

09. The network protocol which is used to get MAC address of a node by providing IP address is
(a) SMTP (b) ARP
(c) RIP (d) BOOTP
[ISRO - 2011]

10. The broadcast address for IP network 172.16.0.0 with subnet mask 255.255.0.0 is
(a) 172.16.0.255 (b) 172.16.255.255
(c) 255.255.255.255 (d) 172.255.255.255
[ISRO - 2011]

11. IPv6 does not support which of the following addressing modes?
(a) unicast addressing (b) multicast addressing
(c) broadcast addressing (d) anycast addressing
[ISRO - 2011]

12. What is IP class and number of sub-networks if the subnet mask is 255.224.0.0?
(a) class A, 3
(b) class A, 8
(c) class B, 3
(d) class B, 32
[ISRO - 2013]

13. A packet filtering firewall can
(a) deny certain users from accessing a service
(b) block worms and viruses from entering the network
(c) disallow some files from being accessed through FTP
(d) block some hosts from accessing the network
[ISRO - 2013]

14. The process of modifying IP address information in IP packet headers while in transit across a traffic routing device is called
(a) Port address translation (PAT)
(b) Network address translation (NAT)
(c) Address mapping
(d) Port mapping
[ISRO - 2014]

15. A IP packet has arrived in which the fragmentation offset value is 100, the value of HLEN is 5 and the value of total length field is 200. What is the number of the last byte?
(a) 194
(b) 394
(c) 979
(d) 1179
[ISRO - 2014]

16. An IP packet has arrived with the first 8 bits as 0100 0010. Which of the following is correct ?
(a) The number of hops this packet can travel is 2.
(b) The total number of bytes in header is 16 bytes.
(c) The upper layer protocol is ICMP
(d) The receiver rejects the packet
[ISRO - 2014]

17. A supernet has a first address of 205.16.32.0 and a supernet mask of 255.255.248.0. A router receives four packets with the following destination addresses. Which packet belongs to this supernet?
(a) 205.16.42.56
(b) 205.17.32.76
(c) 205.16.31.10
(d) 205.16.39.44
[ISRO - 2014]

18. An organization is granted the block 130.34.12.64 / 26. It needs to have four subnets. Which of the following is not an address of this organization?
(a) 130.34.12.124
(b) 130.34.12.89
(c) 130.34.12.70
(d) 130.34.12.132
[ISRO - 2014]

19. How many bits internet address is assigned to each host on a TCP/IP internet which is used in all communication with the host?
(a) 16 bits
(b) 32 bits
(c) 48 bits
(d) 64 bits
[ISRO - 2015]

20. In a class B subnet, we know the IP address of one host and the mask as given below:
IP address = 125.134.112.66
Mask = 255.255.224.0
What is the first address (Network address)?
(a) 125.134.96.0
(b) 125.134.112.0
(c) 125.134.112.66
(d) 125.134.0.0
[ISRO - 2015]

21. Which statement is false?
(a) PING is a TCP/IP application that sends datagrams once every second in the hope of an echo response from the machine being PINGED
(b) If the machine is connected and running a TCP/IP protocol stack, it should respond to the PING datagram with a datagram of its own
(c) If PING encounters an error condition, an ICMP message is not returned.
(d) PING display the time of the return response in milliseconds or one of several error message
[ISRO - 2015]

22. A router uses the following routing table:

Destination	Mask	Interface
144.16.0.0	255.255.0.0	eth0
144.16.64.0	255.255.224.0	eth1
144.16.68.0	255.255.255.0	eth2
144.16.68.64	255.255.255.224	eth3

A packet bearing a estimation address 144.16.68.117 arrives at the router. On which interface will it be forwarded?

(a) eth0 (b) eth1
(c) eth2 (d) eth3

[ISRO - 2015]

23. Which network protocol Allows hosts to dynamically get a unique IP number on each bootup?

(a) DHCP (b) BOOTP
(c) RARP (d) ARP

[ISRO - 2016]

24. The address of a class B host is to be split into subnets with a 6-bit subnet number. What is the maximum number of subnets and the maximum number of hosts in each subnet?

(a) 62 subnets and 262142 hosts
(b) 64 subnets and 262142 hosts
(c) 62 subnets and 1022 hosts
(d) 64 subnets and 1024 hosts

[ISRO - 2016]

25. Which protocol suite designed by IETF to provide security for a packet at the Internet layer?

(a) IPsec (b) NetSec
(c) PacketSec (d) SSL

[ISRO - 2017(May)]

26. In the IPv4 addressing format, the number of networks allowed under Class C addresses is

(a) 2^{20} (b) 2^{24} (c) 2^{14} (d) 2^{21}

[ISRO - 2017(Dec)]

27. An Internet Service Provider (ISP) has the following chunk of CIDR-based IP addresses available with it: 245.248.128.0/20. The ISP wants to give half of this chunk of addresses to Organization A, and a quarter to Organization B, while retaining the remaining with itself. Which of the following is a valid allocation of addresses to A and B?

(a) 245.248.136.0/21 and 245.248.128.0/22
(b) 245.248.128.0/21 and 245.248.128.0/22
(c) 245.248.132.0/22 and 245.248.132.0/21
(d) 245.248.136.0/24 and 245.248.132.0/21

[ISRO - 2017(Dec)]

KEY & Detailed Solutions				
01. (c)	02. (b)	03. (b)	04. (c)	05. (d)
06. (d)	07. (d)	08. (b)	09. (b)	10. (b)
11. (c)	12. (b)	13. (d)	14. (b)	15. (c)
16. (d)	17. (d)	18. (d)	19. (b)	20. (a)
21. (c)	22. (c)	23. (a)	24. (*)	25. (a)
26. (d)	27. (a)			

01. Ans: (c)

Sol: (a) The IP address range 127.0.0.0 – 127.255.255.255 is reserved for loopback

(b) A broadcast IP address is only assigned once in each network. It is always the last IP address of the subnet. The network address and the broadcast address are not used as computer IP addresses. In a network, the first address field is reserved for the network address and the last for the broadcast address

(c) The IP address that defines a multicast group is a Class D address (224.0.0.0 to 239.255.255.255)

02. Ans: (b)

Sol: Router connects two different network so its operation is based on IP

Mac address used to recognize a unique host over a network in LAN

Port number is required to identify a specific process

03. Ans: (b)

Sol: Subnet mask 255.255.255.192

Default Subnet mask for class C is 255.255.255.192

For first 3 octet 24 bits are fixed and for last octet 2 bits are fixed

24 + 2 = 26 bits

04. Ans: (c)

Sol:

Class	Higher bits	NET ID bits	HOST ID bits	No.of net-works	No.of hosts per net-work	Range
A	0	8	24	2^7	2^{24}	0.0.0.0 to 127.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0 to 191.255.255.255
C	110	24	8	2^{21}	2^8	192.0.0.0 to 223.255.255.255
D	1110	Not De-fined	Not De-fined	Not De-fined	Not De-fined	224.0.0.0 to 239.255.255.255
E	1111	Not De-fined	Not De-fined	Not De-fined	Not De-fined	240.0.0.0 to 255.255.255.255

If you look at class C range , given IP address 198.78.41.0 lies in it.

05. Ans: (d)

Sol: Option (a) 172.57.88.62 and 172.56.87.23

This could not be the answer, as the second octet is not the same .

Option (b) 10.35.28.2 and 10.35.29.4

10.35.28.2 & 255.255.31.0=10.35.28.0

10.35.29.4 & 255.255.31.0=10.35.29.0

Option (c) is not the answer, as same reason as option (a)

Option (d) 128.8.129.43 & 255.255.31.0=128.8.1.0

128.8.161.55 & 255.255.31.0=128.8.1.0

06. Ans: (d)

Sol: The address resolution protocol (ARP) is a protocol used by the Internet Protocol (IP), specifically IPv4, to map IP network addresses to the hardware addresses (MAC Address) used by a data link protocol.

MAC address operates below the network layer.

07. Ans: (d)

Sol: The standard (IEEE 802) format for printing MAC-48 bit addresses form is six octet of two hexadecimal digits

Option (b) and (c) are not any address representation

Option (a) is example of IP address

Option (d) is example of MAC address

MAC address can be represented by either (6 bytes) 48-bit address (or) It can be represented as six pairs of a Hexa decimal values separates with color (6C: 7C: FB: 79: 86: 73)

08. Ans: (b)

Sol: When IPSEC tunnel mode is used, IPSEC encrypts the IP header and the payload, whereas transport mode only encrypts the IP payload. With tunnel mode, an entire IP packet is encapsulated with an AH or ESP header and IP packet, including the header, applies IPSEC security methods to the entire packet, and then adds a new IP header.

09. Ans: (b)

Sol: ARP(address resolution protocol) is used for IP to MAC finding

RARP(reverse address resolution protocol) is used for MAC to IP finding.

10 . Ans: (b)

Sol: Broadcast address - all bits of subnet ID/Network id in host portion will be set to be 1's.

So the broadcast address will be 172.16.255.255.

11. Ans: (c)
Sol: IPv6 does not implement traditional IP broadcast, and therefore does not define broadcast addresses. IPv6 supports unicast, multicast and anycast.

12. Ans: (b)
Sol: Subnet mask is 11111111.11100000.00000000.000 00000.
8 bit assigned for network and Class A contains 8 1's
next 3 ones used for subnet.
Number of subnets is $2^3 = 8$.

13. Ans: (d)
Sol: There are three types of firewalls;-
1. Layer 3 Firewall or Packet Filtering Firewall
2. Layer 4 Firewall
3. Layer 5 firewall or Proxy Firewall

Option (d) deals with IP addresses at Network Layer

14. Ans: (b)
Sol: Network address translation (NAT) is the process of modifying IP address information in IP packet headers while in transit across a traffic routing device.
(Port address Translation) PAT is an extension of NAT which not only changes IP but even assigns port to each address.

15. Ans: (c)
Sol: Data length
=200–4×5=180
Starting number of the first byte of fragment
=100×8=800
Number of the last byte
=800+179=979

16. Ans: (d)
Sol: From the given data the first 8 bits as 01000010. In this the higher nibble will specify the version and the lower nibble will specify header length (which is in the range of (20-60 bytes), So what ever the value we get in the lower nibble, should be multiple with 4 and make sure that the result should be the range of (20-60 bytes) if it is not in this range the receiver will reject the packet since in our question (0010) 2×4 = 8 which is not in the range, So the packet will be rejected.

17. Ans: (d)
Sol: Option (a): 205.16.42.56
Performing bitwise and operation with supernet mask
11001101.00010000.001010101010.0011100
11111111 . 111111111 . 11111000 . 00000000

11001101 .00010000. 00101000. 00000000
≡ 205. 16. 40. 0 ≠ 205.16. 32.0
Hence this is **not the correct** option.

Option (b): 205.17.32.76
Performing bitwise and operation with supernet mask
11001101.00010001.001000000.01001100
11111111 . 111111111 . 11111000 . 00000000

11001101 .00010001. 00100000. 00000000
≡ 205. 17. 32. 0 ≠ 205.16. 32.0
Hence this is **not the correct** option.

Option(c): 205.16.31.10
Performing bitwise and operation with supernet mask
11001101. 00010000. 00011111. 00001010
11111111 . 111111111 . 11111000 . 00000000

11001101 .00010000. 00011000. 00000000
≡ 205. 17. 32. 0 ≠ 205.16. 32.0
Hence this is **not the correct** option.

Option (d): 205.16.39.44
Performing bitwise and operation with supernet mask
11001101. 00010000. 00100111. 00101100
11111111 . 111111111 . 11111000 . 00000000

11001101 .00010000. 00010000. 00000000
≡ 205. 16. 32. 0 = = 205.16. 32.0
Hence this is **the correct** option.

18. Ans: (d)

Sol: Block 130.34.12.64/26 indicates, $2^{32-26} = 2^6$ hosts.

So, addresses from 130.34.12.64 to 130.34.12.127 will be included in this organization.

19. Ans: (b)

Sol: An internet address of 32 bit is assigned to each host on a TCP/IP internet which is used in all communication with the host.

If it is IPV4: 32 bis (4×8 = 32 bits)

If it is IPV6: 128 bits (4×32 = 128 bits)

20. Ans: (a)

Sol: Network address or First address is used for network identification.

The Network address is calculated by Bitwise AND operation of corresponding binary bits of IP Address & Subnet mask.

CALCULATION:

IP Address	**125.134.112.66**	0111101	10000110	01110000	01000010
Subnet Mask	**255.255.224.0**	1111111	11111111	11100000	00000000
Network Address	**125.134.96.0**	01111101	10000110	01100000	00000000

21. Ans: (c)

Sol: PING uses ICMP to check the connectivity of host to the Internet(IP) layer. It send message to host computer to the destination computer and then echoed back from destination to host computer.

Option (c) says - ICMP packet does not return which is false.

22. Ans: (c)

Sol:

Destination	Address (Given)	Mask	Bitwise and (Address & Mask)
144.16.0.0	144.16.68.117	255.255.0.0	144.16.0.0
144.16.64.0	144.16.68.117	255.255.224.0	144.16.64.0
144.16.68.0	144.16.68.117	**255.255.255.0**	**144.16.68.0**
144.16.68.64	144.16.68.117	255.255.255.224	144.16.68.96

23. Ans: (a)

Sol: Dynamic Host Configuration Protocol (DHCP):

- It serves as a bootstrap when a host is booted and supposed to be connected to the Internet, but the host does not know its IP address.
- It is used on UDP/IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.

24. Ans: (*)

Sol: Subnet bits = 6

means 2^6 or 64 subnets are possible.

and, total IP Addresses per subnet = 2^{10}

out of 1024 IP Addresses we need to subtract 2 one for subnet ID and another one for broadcast address, so 1022 hosts are possible.

25. Ans: (a)

Sol: In computing, Internet Protocol Security (IPsec) is a network protocol suite that authenticates and encrypts the packets of data sent over a network. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to use during the session.

26. Ans: (d)

Sol:

Class	PREFIX(bits reserved from 1st byte)	Network ID (bits)	Range of 1st byte	No. of IP address consumed	Number of networks	IP address per network	Host per network	Percentage of IPv4 address consumed
Class A	0	8	0-127	2^{31}	2^{7}	2^{24}	$2^{24}-2$	50%
Class B	10	16	128-191	2^{30}	2^{14}	2^{16}	$2^{16}-2$	25%
Class C	110	24	192-223	2^{29}	2^{21}	2^{8}	$2^{8}-2$	12.5%
Class D	1110	-	224-239	2^{28}	MULTICAST ADDRESS			6.25%
ClassE	1111	-	239-255	2^{28}	RESERVED FOR FUTURE			6.25%

27. Ans: (a)

Sol:

245.248.10000[000.0] → 245.248.100000[00.0] ⇒ 245.248.128.0/22

245.248.10000[000.0] → 245.248.100001[00.0] ⇒ 245.248.132.0/22

245.248.136.0/21

(or)

245.248.10000[000.0] → 245.248.100010 [00.0] ⇒ 245.248.136.0/22

245.248.10000[000.0] → 245.248.100011[00.0] ⇒ 245.248.140.0/22

245.248.128.0/21

6. Routing Algorithms

01. If there are five routers and six networks in an intranet using link state routing, how many routing tables are there?
(a) 1 (b) 5 (c) 6 (d) 11
[ISRO - 2007]

02. What is routing algorithm used by OSPF routing protocol?
(a) Distance vector (b) Flooding
(c) Path vector (d) Link state
[ISRO - 2014]

03. Dynamic routing protocol enable routers to:
(a) Dynamically discover and maintain routes
(b) Distribute routing updates to other routers
(c) Reach agreement with other routers about the network topology
(d) All of the above **[ISRO - 2016]**

04. Match with the suitable one:

List-I
(A) Multicast group membership
(B) Interior gateway protocol
(C) Exterior gateway protocol
(D) RIP

List-II
1. Distance vector routing
2. IGMP
3. OSPF
4. BGP

(a) A-2, B-3, C-4, D-1
(b) A-2, B-4, C-3, D-1
(c) A-3, B-4, C-1, D-2
(d) A-3, B-1, C-4, D-2
[ISRO - 2017(May)]

KEY & Detailed Solutions			
01. (b)	02. (d)	03. (d)	04. (a)

01. Ans: (b)

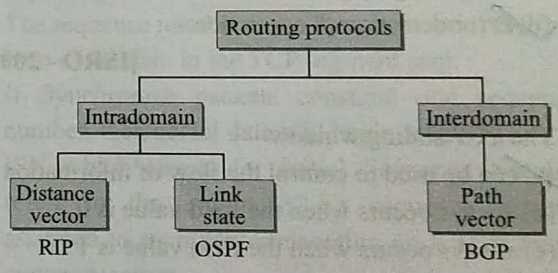
Sol: In a question 5 routers are given, So number of routing tables = 5

02. Ans: (d)

Sol: OSPF is a routing protocol for a IP network Which uses Link State Routing algorithm and falls into a group of Interior Gateway Protocol operated within a single autonomous system. It implements Dijkstra algorithm.

03. Ans:(d)

Sol:



Dynamic routing protocol enables routers:
- To discover and maintain routes
- To distributed routing updates to other routers
- To reach agreement with other routers about the network topology.

04. Ans: (a)

Sol: (a) Multicast group membership IGMP
(b) Interior gateway protocol OSPF
(c) Exterior gateway protocol BGP
(d) RIP Distance vector routing

7. TCP/UDP & Sockets, Congestion control

01. Which of these is not a feature of WAP 2.0
(a) Push & Pull Model
(b) Interface to a storage device
(c) Multimedia messaging
(d) Hashing **[ISRO - 2007]**

02. Silly Window Syndrome is related to
(a) Error during transmission
(b) File transfer protocol
(c) Degrade in TCP performance
(d) Interface problem **[ISRO - 2007]**

03. SSL is not responsible for
(a) Mutual authentication of client & server
(b) Secret communication
(c) Data Integrity protection
(d) Error detection & correction **[ISRO - 2007]**

04. The TCP sliding window
(a) can be used to control the flow of information
(b) always occurs when the field value is 0
(c) always occurs when the field value is 1
(d) occurs horizontally **[ISRO - 2008]**

05. Which algorithm is used to shape the bursty traffic into a fixed rate traffic by averaging the data rate?
(a) solid bucket algorithm
(b) spanning tree algorithm
(c) hocken helm algorithm
(d) leaky bucket algorithm **[ISRO - 2013]**

06. The protocol data unit for the transport layer in the internet stack is
(a) segment
(b) message
(c) datagram
(d) frame **[ISRO - 2013]**

07. Assume the following information.
Original timestamp value = 46
Receive timestamp value = 59
Transmit timestamp value = 60
Timestamp at arrival of packet = 69

Which of the following statements is correct?
(a) Receive clock should go back by 3 milliseconds
(b) Transmit and receive clocks are synchronized
(c) Transmit clock should go back by 3 milliseconds
(d) Receive clock should go ahead by 1 milliseconds **[ISRO - 2014]**

08. An ACK number of 1000 in TCP always means that
(a) 999 bytes have been successfully received
(b) 1000 bytes have been successfully received
(c) 1001 bytes have been successfully received
(d) None of the above **[ISRO - 2015]**

09. What is the maximum size of data that application layer can pass on to the TCP layer below?
(a) Any size
(b) (2^{16} bytes - the size of TCP header)
(c) 2^{16} bytes
(d) 1500 bytes **[ISRO - 2016]**

10. Generally TCP is reliable and UDP is not reliable. DNS which has to be reliable uses UDP because
(a) UDP is slower
(b) DNS servers has to keep connections
(c) DNS requests are generally very small and fit well within UDP segments
(d) None of these **[ISRO - 2017(Dec)]**

11. The persist time is used in TCP to
(a) To detect crashes from the other end of the connection
(b) To enable retransmission
(c) To avoid deadlock condition
(d) To timeout FIN_Wait1 condition **[ISRO - 2020]**

12. Checksum field in TCP header is
(a) ones complement of sum of header and data in bytes
(b) ones complement of sum of header, data and pseudo header in 16 bit words
(c) dropped from IPv6 header format
(d) better than md5 or sh1 methods

[ISRO - 2020]

KEY & Detailed Solutions			
01. (d)	02. (c)	03. (d)	04. (a)
05. (d)	06. (a)	07. (a)	08. (d)
09. (a)	10. (c)	11. (c)	12. (c)

01. Ans: (d)
Sol: WAP is Wireless Application Protocol which provides
Push and Pull
Interface to a storage device
Multimedia messaging

02. Ans: (c)
Sol: Silly window Syndrome is a problem which occurs due to bad implementation of TCP.

03. Ans: (d)
Sol: SSL (Secure Socket layer) is responsible for
Client and server authentication
Secret communication
Data integrity protection

04. Ans: (a)
Sol: TCP used for flow control mechanism
Sender can send any number of frames without worrying about acknowledgment.

05. Ans: (d)
Sol: Leaky bucket algorithm is a method of congestion control by providing a check on data flow and regulating the average rate of data flow.

06. Ans: (a)
Sol: PDU is frame for Data link layer
PDU is datagram for network
PDU is segment for transport
PDU is message for application layer.

07. Ans:(a)
Sol: Sender sent the packet at 46 and receiver should have received it at 56 , but its receiving it at 59, and its 3 ms ahead. So it should set its clock 3 ms behind to sync with sender.

08. Ans: (d)
Sol: The Acknowledgment number (ACK) is the sequence number of the next Byte the receiver is expecting.
The sequence number is the Byte number of the first byte of the data in the TCP segment sent.
If Synchronize packets consume one sequence number, then actual data will begin at ISN+1.
ISN which stands for initial Sequence Number refers to the unique 32-bit sequence number assigned to each new connection on a TCP, based communication.
Since in the given question the ISN is not given , so we cant say anything.

09. Ans: (a)
Sol:

Terminology	TCP/IP Layer	Maximum size (bytes)	OSI layer
Message	Application layer	Any size	Application layer
			Session layer
			Presentation layer
Segment	Transport Layer	1460	Transport Layer
Packet (Fragment)	Internet Layer	1480	Network Layer
Frame	Link Layer	1500	Data Link Layer
			Physical Layer

10. Ans: (c)

Sol: UDP is much faster. TCP is slow as it require 3 way handshake.

UDP is not reliable but reliability can be added on application layer.

11. Ans: (c)

Sol:
- Sender receives an acknowledgment from the receiver with zero window size. This indicates the sender to wait.
- Later, receiver updates the window size and sends the segment with the update to the sender. This segment gets lost.
- Now, both sender and receiver keep waiting for each other to do something. To deal with such a situation, TCP uses a persistent timer.
- Sender starts the persistent timer on receiving an ACK from the receiver with a zero-window size. When persistent timer goes off, sender sends a special segment to the receiver. This special segment is called as probe segment and contains only 1 byte of new data.

12. Ans: (c)

Sol: Checksum field is dropped from IPv6 header format.

8. Application Layer Protocols

01. An email contains a textual birthday greeting, a picture of a cake and a song. The order is not important. What is the content-type ?
(a) Multipart/mixed
(b) Multipart/parallel
(c) Multipart/digest
(d) Multipart/alternative **[ISRO - 2007]**

02. Lightweight directory access protocol is used for
(a) Routing the packets
(b) Authentication
(c) Obtaining IP address
(d) domain name resolving **[ISRO - 2011]**

03. Suppose you are browsing the world wide web using a web browser and trying to access the web servers. What is the underlying protocol and port number that are being used?
(a) UDP, 80 (b) TCP, 80
(c) TCP, 25 (d) UDP, 25
[ISRO - 2014]

04. Consider the following scenario.
A web client sends a request to a web server. The web server transmits a program to that client and is executed at client. It created a web document. What are such web documents called?
(a) Active (b) Static
(c) Dynamic (d) Passive
[ISRO - 2014]

05. The DNS maps the IP addresses to
(a) A binary address as strings
(b) An alphanumeric address
(c) A hierarchy of domain names
(d) A hexadecimal address **[ISRO - 2015]**

06. When a DNS server accepts and uses incorrect information from a host that has no authority giving that information, then it is called

(a) DNS lookup
(b) DNS hijacking
(c) DNS spoofing
(d) None of the mer

07. Which of the fo
transferring electr
machine to another
(a) TELNET
(c) SNMP

08. Consider the set o
A : Send an e-ma
B : Download e-
retrieve mail
C : Checking e-
The application
in the same seq
(a) SMTP, HTT
(b) SMTP, POP
(c) SMTP, IMA
(d) SMTP, IMA

09. Remote Proce
(a) communic
remotely
system
(b) communi
same sys
(c) commun
separate
(d) none of

01. (a)	
06. (c)	

(a) DNS lookup
(b) DNS hijacking
(c) DNS spoofing
(d) None of the mentioned **[ISRO - 2016]**

07. Which of the following protocol is used for transferring electronic mail messages from one machine to another?
(a) TELNET (b) FTP
(c) SNMP (d) SMTP
[ISRO - 2017(May)]

08. Consider the set of activities related to e-mail
A : Send an e-mail from a mail client to mail server
B : Download e-mail headers from mail box and retrieve mails from server to a cache
C : Checking e-mail through a web browser
The application level protocol used for each activity in the same sequence is
(a) SMTP, HTTPS, IMAP
(b) SMTP, POP, IMAP
(c) SMTP, IMAP, HTTPS
(d) SMTP, IMAP, POP **[ISRO - 2017(Dec)]**

09. Remote Procedure Calls are used for
(a) communication between two processes remotely different from each other on the same system
(b) communication between two processes on the same system
(c) communication between two processes on separate systems
(d) none of the above **[ISRO - 2020]**

KEY & Detailed Solutions				
01. (a)	02. (b)	03. (b)	04. (a)	05. (c)
06. (c)	07. (d)	08. (c)	09.(a) & (c)	

01. Ans: (a)
Sol: A multipart/mixed MIME message is composed of a mix of different data types. Each body part is delineated by a boundary.
The purpose of the multipart/parallel content type is to display all of the parts simultaneously on hardware and software that can do so.
The multipart/digest content type is used to send collections of plain-text messages, It is a sub part of MIME
The multipart/alternative content type is used when the same information is presented in different body parts in different forms.

02. Ans: (b)
Sol: The main idea of LDAP is to keep all the information (such as contact details, login, password) of a user in one place, so that it is easier to maintain by network administrators.

03. Ans: (b)
Sol: TCP is the underlying protocol of HTTP. HTTP is used to access the web server ,also the HTTP runs at 80. Its a well-known Port Number.

04. Ans: (a)
Sol: Static:
A static web document resides in a file that is associated with a web server. The author of a static document determines the contents at the time the document is written. Because the contents do not change, each request for a static document results in exactly the same response.

Dynamic:
A dynamic web document does not exist in a predefined form. When a request arrives, the webserver runs an application program that creates the document. The server returns the output of the program as a response to the browser that requested the document. Because a fresh document is created for each request, the contents of a dynamic document can vary from one request to another.

Active:
An active web document consists of a computer program that the server sends to the browser and that the browser must run locally. When it runs, the active document program can interact with user and change the display continuously.

05. Ans: (c)
Sol: DNS, which stands for Domain Name System, maps domain name into Internet Protocol (IP) address.
IP → Domain name
Hence, the DNS maps the IP addresses to a hierarchy of domain names.

06. Ans:(c)
Sol: Spoofing:
It is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.
Therefore when a DNS server accepts and uses incorrect information from a host that has no authority giving that information, then it is called DNS spoofing.

07. Ans: (d)
Sol: SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is an always-on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection through port 25. After successfully establishing a TCP connection the client process sends the mail instantly.

(a) Telnet: Remote log in through port 23
(b) FTP: Secure transmission of files through port 21
(c) SNMP: Used to send command and messages through port 161 and 162

08. Ans: (c)
Sol: SMTP (Simple mail transfer protocol) is push protocol used to send an e-mail from a mail client to mail server.
IMAP (Internet message access protocol) helps download e-mail headers from a mailbox and retrieve emails from server to a cache.
HTTPS(HTTP Secure) it can be used for accessing web-based email.
POP(Post office protocol) is used by the user to list and retrieve the mail messages. POP does not allow the user to partially check the contents of the mail before downloading.

09. Ans: (a) & (c)
Sol: The Remote procedure calls are used in distributed computing, where in a computer program causes a subroutine to execute in a different space (on another computer), which is coded as if it were a local procedure call.

9. Network Security

01. The standard for certificates used on internet is
(a) X.25 (b) X.301
(c) X.409 (d) X.509
[ISRO - 2007]

02. Hashed message is signed by a sender using
(a) his public key
(b) his private key
(c) receiver's public key
(d) receiver's private key
[ISRO - 2007]

03. A public key encryption system
(a) allows anyone to decode the transmissions
(b) allows only the correct sender to decode the data
(c) allows only the correct receiver to decode the data
(d) does not encode the data before transmitting it
[ISRO - 2008]

04. SHA-1 is a
(a) Encryption algorithm
(b) Decryption algorithm
(c) Key exchange algorithm
(d) Message digest function
[ISRO - 2009]

05. Advanced encryption Standard (AES) is based on
(a) Asymmetric key algorithm
(b) Symmetric key algorithm
(c) Public key algorithm
(d) key exchange
[ISRO - 2009]

06. An example of poly-alphabetic substitution is
(a) P-box (b) S-box
(c) Caesar cipher (d) Vigenere cipher
[ISRO - 2011]

07. What will be the cipher text produced by the following cipher function for the plain text ISRO with key k = 7. [Consider 'A' = 0, 'B' = 1, ... 'Z' = 25]
$C_k(M) = (kM + 13) \bmod 26$
(a) RJCH (b) QIBG
(c) GQPM (d) XPIN
[ISRO - 2013]

08. Which of the following encryption algorithms is based on the Fiestal structure?
(a) Advanced Encryption Standard
(b) RSA public key cryptographic algorithm
(c) Data Encryption Standard
(d) RC4
[ISRO - 2013]

09. In a system an RSA algorithm with p = 5 and q = 11, is implemented for data security. What is the value of the decryption key if the value of the encryption key is 27?
(a) 3 (b) 7 (c) 27 (d) 40
[ISRO - 2014]

10. MD5 is a widely used hash function for producing hash value of
(a) 64 bits (b) 128 bits
(c) 512 bits (d) 1024 bits
[ISRO - 2017(May)]

11. Pretty Good Privacy (PGP) is used in
(a) Browser security (b) FTP security
(c) Email security (d) None of the above
[ISRO - 2017(May)]

12. What is WPA?
(a) wired protected access (b) wi-fi protected access
(c) wired process access (d) wi-fi process access
[ISRO - 2017(May)]

13. Using public key cryptography, X adds a digital signature σ to a message M, encrypts ⟨M, σ⟩ and sends it to Y, where it is decrypted. Which one of the following sequence of keys is used for operations?
(a) Encryption : X's private key followed by Y's private key. Decryption : X's public key followed by Y's public key
(b) Encryption : X's private key followed by Y's public key; Decryption : X's public key followed by Y's private key
(c) Encryption : X's private key followed by Y's public key; Decryption : Y's private key followed by X's public key.
(d) Encryption : X's public key followed by Y's private key; Decryption : Y's public key followed by X's private key.
[ISRO - 2017(Dec)]

14. Which of the following are used to generate a message digest by the network security protocols?
(P) SHA-256 (Q) AES
(R) DES (S) MD5
(a) P and S only (b) P and Q only
(c) R and S only (d) P and R only
[ISRO - 2017(Dec)]

15. In cryptography, the following uses transposition ciphers and the keyword is LAYER. Encrypt the following message. (Spaces are omitted during, encryption)
WELCOME TO NETWORK SECURITY !
(a) WMEKREETSILTWETCOOCYONRU!
(b) EETSICOOCYWMEKRONRU!LTWET
(c) LTWETONRU!WMEKRCOOCYEETS!
(d) ONRU!COOCYLTWETEETSIWMEKR
[ISRO - 2018]

16. Avalanche effect in cryptography
(a) Is desirable property of cryptographic algorithm
(b) Is undesirable property of cryptographic algorithm
(c) Has no effect on encryption algorithm
(d) None of the above
[ISRO - 2018]

17. What is one advantage of setting up a DMZ (Demilitarized Zone) with two firewalls?
(a) You can control where traffic goes in the three networks
(b) You can do stateful packet filtering
(c) You can do load balancing
(d) Improve network performance
[ISRO - 2018]

18. Which one of the following algorithm is not used in asymmetric key cryptography?
(a) RSA Algorithm
(b) Diffie-Hellman Algorithm
(c) Electronic Code Book Algorithm
(d) None of the above
[ISRO - 2018]

19. In a columnar transposition cipher, the plain text is "the tomato is a plant in the night shade family", keyword is "TOMATO". The cipher text is
(a) "TINESAX/EOAHTFX/HTLTHEY/ MAIIAIX/TAPNGDL/OSTNHMX"
(b) "TINESAX/EOAHTFX/MAIIAIX/ HTLTHEY/ TAPNGDL/OSTNHMX"
(c) "TINESAX/EOAHTFX/HTLTHEY/ MAIIAIX/ OSTNHMX/TAPNGDL"
(d) "EOAHTFX/TINESAX/HTLTHEY/ MAIIAIX/ TAPNGDL/OSTNHMX"
[ISRO - 2020]

20. Avalanche effect in cryptography refers
(a) Large changes in cipher text when the keyword is changed minimally
(b) Large changes in cipher text when the plain text is changed
(c) Large Impact of keyword change to length of the cipher text
(d) None of the above
[ISRO - 2020]

KEY &	
01. (d)	02. (
06. (d)	07. (
11. (c)	12.
16. (a)	17.

01. Ans: (d)
Sol: An X.509 c based on th Telecommunic which defines (PKI) certifica

02. Ans: (b)
Sol: Sender has to key, so that data using th

03. Ans: (c)
Sol: Asymetric k private key) private key by using th can decode

04. Ans: (d)
Sol: SHA - 1 is digest whi algorithm. SHA-1 is also called decrypted

05. Ans: (b)
Sol: AES is a is used fo The AES features-

KEY & Detailed Solutions				
01. (d)	02. (b)	03. (c)	04. (d)	05. (b)
06. (d)	07. (a)	08. (c)	09. (a)	10. (b)
11. (c)	12. (b)	13. (c)	14. (a)	15. (b)
16. (a)	17. (c)	18. (c)	19. (a)	20. (a) & (b)

01. Ans: (d)

Sol: An X.509 certificate is a digital certificate based on the widely accepted International Telecommunications Union (ITU) X.509 standard, which defines the format of public key infrastructure (PKI) certificates.

02. Ans: (b)

Sol: Sender has to encrypt the data with its own private key, so that the receiver is capable of extracting data using the sender's public key.

03. Ans: (c)

Sol: Asymetric key encryption uses two keys (public key, private key) public key which is known to every one private key which is known to user only.
by using this encryption only the correct receiver can decode a data by using his private key.

04. Ans: (d)

Sol: SHA - 1 is produces 160 bit hash value or message digest which resembles the Hash value of MD5 algorithm.
SHA-1 is a secure hashing algorithm. Hashing is also called as one-way Encryption (which cannot be decrypted back to the original, plain text)

05. Ans: (b)

Sol: AES is a symmetric key algorithm i.e. the same key is used for encryption and decryption process.
The AES replaced the DES with new and updated features-
Block encryption implementation
128-bit group encryption with 128, 192 and 256-bit key lengths.

06. Ans: (d)

Sol: The Vigenère cipher is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword. It employs a form of poly-alphabetic substitution.

07. Ans: (a)

Sol: A= 0 B=1 C=2 D = 3 so on
I = 8
S= 18
R =17
O = 14
C(I) = (k I+13) MOD 26 =(7*8+13)MOD 26 = 17
i.e R
C(S) = (k S+13) MOD 26 =(7*18+13)MOD 26 = 9
i.e J
C(R) = (k R+13) MOD 26 =(7*17+13)MOD 26 = 2
i.e C
C(O) = (k O+13) MOD 26 =(7*14+13)MOD 26 = 7 i.e H
All these characters matches with option (a)

08. Ans: (c)

Sol: Feistal cipher is a symmetric cipher used in the construction of block cipher.
DES symmetric, based on Feistal structure
RC4 symmetric but not based on Feistal structure
RSA is asymmetric
AES symmetric but not bases on feistal structure.

09. Ans: (a)

Sol: p=5 , q=11 , encryption key(e) = 27
n = p*q = 5*11= 55
$\varphi(n) = (p - 1) * (q - 1) = 4 * 10 = 40$
[e = 27], d such that $(d * e) \% \varphi(n) = 1$
decryption key (d) $\rightarrow (d * 27) \% 40 = 1$
If we put d =3 then 27 * 3 % 40 = 1

10. Ans: (b)

Sol: The MD5 algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption.

11. Ans: (c)

Sol: Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

12. Ans: (b)

Sol: WPA stands for wi-fi protected access. It is a security standard for computing devices equipped with wireless internet connection. WPA provides data encryption and user authentication to the computing devices connected to a wi-fi network.

13. Ans: (c)

Sol: Encryptions: X's private key followed by Y's public key; Decryption: Y's private key followed by X's public key.

14. Ans: (a)

Sol: RSA - It is an algorithm used to encrypt and decrypt messages.

Message Digest 5, or MD5 is a widely used cryptographic hash function

SHA 1 - Secure Hash Algorithm 1, or SHA 1 is a cryptographic hash function.

DES - Data Encryption Standard, or DES is a symmetric key algorithm for encryption of electronic data.

P & S be the message digest option (a) is the final answer

15. Ans: (b)

Sol: Here, $l = 5$,

keyword	L	A	Y	E	R
Key	3	1	5	2	4
Plaintext	W	E	L	C	O
	M	E	T	O	N
	E	T	W	O	R
	K	S	E	C	U
	R	I	T	Y	!

Ciphertext: EETSI COOCY WMEKR ONRU LTWET

16. Ans: (a)

Sol: Avalanche effect is desirable property of cryptography algorithm.

17. Ans: (c)

Sol: Setting up a DMZ with two firewalls has its own advantages.

1. The biggest advantage that you can do load balancing.
2. A topology with two firewalls also helps in protecting internal services on the LAN from denial of the service attacks on the firewall's perimeter.

18. Ans: (c)

Sol: ECB is symmetric key encryption algorithm.

19. Ans: (a)

Sol: In columnar transposition Cipher we writes the plaintext in rows and then reads the cipher text in columns one by one.

5	3	2	1	6	4
T	O	M	A	T	O
T	H	E	T	O	M
A	T	O	I	S	A
P	L	A	N	T	I
N	T	H	E	N	I
G	H	T	S	H	A
D	E	F	A	M	I
L	Y	X	X	X	X

20. Ans: (a) & (b)

Sol: Avalanche effect in cryptography refers

(a) Large changes in cipher text when the keyword is changed minimally

(b) Large changes in cipher text when the plain text is changed.