I. Data Communication & Computer Networking

1. Write the following for the given IP network address 210.212.140.0/24
    a. Broadcast Address
    b. IP Address of First possible host
    c. IP Address of Last possible host
    d. Subnet Mask
2. List any four Features on IPv6
3. List the methods a machine can obtain an IPv4 address
4. List the methods a machine can obtain an IPv6 address
5. List any four Parameters that affect selection of media for LAN.
6. The reason for terminating the ends of media using resistances in BUS topology
7. List any three reasons to prefer star topology in establishing LANs
8. Reasons for developing networking standards like OSI
9. Purpose of TTL in IP Header
10. What is RTT & its significance for networks

II. Telemetry

11. Define Telemetry
12. Name any three options available for Power Utility Communication
13. List any four required features ofPower Utility Communication
14. Name the components of PLCC.
15. List any four advantages of Optical Fiber Communication
16. Optical Fiber Communication, for long distance transmission, which of SM or MM fibers is used & why?
17. List three limitations of PLCC

III. Cyber security in power sector

18. List three areas of power sector which are vulnerable for cyber attacks
19. Define Cyber Security
20. List any for actions required for cyber security
21. Explain Malicious code attacks
22. What is phishing attack
23. Explain DoS Attack
24. What do we mean by Physical security in reference to cyber security
25. List any four cyber security measures at work
26. What are the consequences if organisation/employees are not aware of cyber threats

IV. Proxy & DHCP

27. Leased IP provided by a DHCP server depends on which factors?
28. Write down the commands in proper order for renewing an IP address provided by DHCP manually using command prompt.

29. Name the four packets used for communication during the IP assignment by DHCP server to a host.
30. Which IP addresses should be excluded from the range of DHCP server in a Network?
31. What are the general guidelines for setting lease duration parameter during a DHCP server configuration?
32. Why a Proxy server is used in LANs?
33. What are the reasons to do Caching in the networks?
34. How proxy provides control and discipline in a LAN?

IV. WAN using VSAT

35. List any four advantages of VSAT communication
36. Write down the functions of BUC in a VSAT network.
37. Write down the functions of LNB in a VSAT network.
38. List the functions of IDU of VSAT.
39. Draw the diagram of a VSAT terminal marking all important elements.
40. List any four services that can be provided using VSAT.
41. List the type of topologies supported by VSAT network.

V. SAN

42. What is SAN?
43. List three basic forms of Network storage
44. Draw the layered architecture of FC protocol
45. List any four SAN benefits.
46. List the three topologies supported by SAN
47. Describe RAID 5

VI. Security, AV, IDS, Firewall

48. Name the Three common types of Firewalls
49. List three aims to put firewalls
50. Define Intrusion
51. Name the three IDS implementation options.
52. List any four malicious effects of a virus infection
53.

Answers

1.
    a. Broadcast Address – 210.212.140.255
    b. IP Address of First possible host – 210.212.140.1
    c. IP Address of Last possible host – 210.212.140.254
    d. Subnet Mask- 255.255.255.0
2.
    a. Larger address space
    b. Better security
    c. Global reachability
    d. Efficient routing
    e. Multihoming
    f. Scalability
    g. Autoconfiguration

3.
    a. Static or manual
    b. Dynamic or automatic
4.
    a. Static or manual
    b. Dynamic or automatic (using DHCP server)
    c. Autoconfiguration (without DHCP server)
5.
    a. Distance to be covered
    b. Bandwidth
    c. Security
    d. No of nodes to be connected
    e. Cost
6. To dissipate the signal power going towards ends in terminating resistance ,hence avoiding reflection of signals from open ends & causing collisions.
7.
    a. Easy to develop & scale
    b. Easy fault diagnose
    c. Cutting of media at one point does not disrupt whole network
    d. High data rates
    e. cheaper
8.
    a. To ensure interoperability among networks
    b. To make networks independent of hardware & software platforms
    c. To discourage monopoly in hardware & software
9.
    a. Automatic congestion control in the internetworks
    b. To avoid infinite looping of packets
    c. To efficiently use valuable internet bandwidth
10.

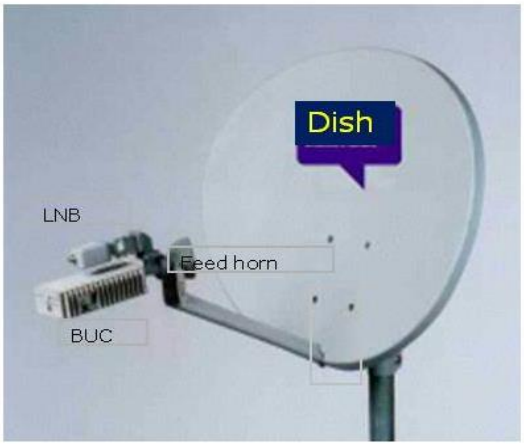
    RTT is round trip time. It is measure of average time taken by a network to forward traffic through it. It is used in network for flow controls eg sliding window.

11. Sensing & measuring information at distance & transmitting it for processing at some central location
12. UHF, Microwave, Satellite, PLCC, Telephony cable, OFC, Radio links
13. List the components of PLCC system
    a. ROBUSTNESS AGAINST ALL KINDS OF INTERFERENCE
    b. DIRECT INTERFACING TO POWER SYSTEM SERVICES e.g PROTECTION , TELECONTROL
    c. HIGH FLEXIBILITY OF NETWORKCONFIGURATION
    d. INETERFERENCE OFFERED TO OTHER EQUIPMENTS
14. Line trap, Coupling Capacitor, Line Matching Unit (LMU), PLC terminal
15. Large carrying capacity, Low power loss, immunity to inductive interference, Light weight & small dia, higher security, negligible cross talk, long life of cable
16. SM fiber is used as it is sending single wavelength over fiber, which does not have the problem of interference from other wavelengths as in case of MM fibers.
17. Limited carrier frequency, Noise, Radio Interference
18. IT for system operations (SCADA, DAS), IT for other business functions (Metering, billing, HR, office automation) & Communication systems used for coordination
19. Cyber Security is a common term used to describe a set of practices, measures and/or actions taken to protect personal information and computers etc from attacks.
20. Use licensed software, install O/S & software updates, use firewalls & antivirus, Protect & change passwords, use online & offline periodic backups
21. Malicious code or malware is software designed to infiltrate or damage a computer system without the owner's informed consent. Malicious code is hostile, intrusive, or annoying software or program code. Commonly known malware are virus, worms, Trojans, spyware, adware and Bots.
22. Phishing is an attack aimed at stealing the 'confidential data' like sensitive information, such as usernames, passwords and credit card details that can lead to committing online frauds.
23. DoS is an attempt to make a computer resource unavailable to its intended users. A distributed denial of service attack (DDoS) occurs when multiple compromised computer systems flood the communication link (called bandwidth or resources) of a targeted system
24. All the vulnerable areas like control centre area should be notified as restricted Area and only authorized persons should be allowed to enter the area. The Security should be manned by the armed personnel of Central Industrial Security Force (CISF) / other security agencies approved by GOI on round the clock basis equipped with metal detector system etc. For important locations e.g. entry gate, building door control room door etc; a video surveillance system should also been installed and all the move ments may be monitored from the Control Room.
25.
    a. Be sure to work with your technical support coordinator before implementing new cyber-safety measures.
    b. Talk with your technical support coordinator about what cyber-safety measures are in place in your department.
    c. Report to your supervisor any cyber-safety policy violations, security flaws/weaknesses you discover or any suspicious activity by unauthorized individuals in your work area.
    d. Physically secure your computer by using security cables and locking building/office doors and windows.

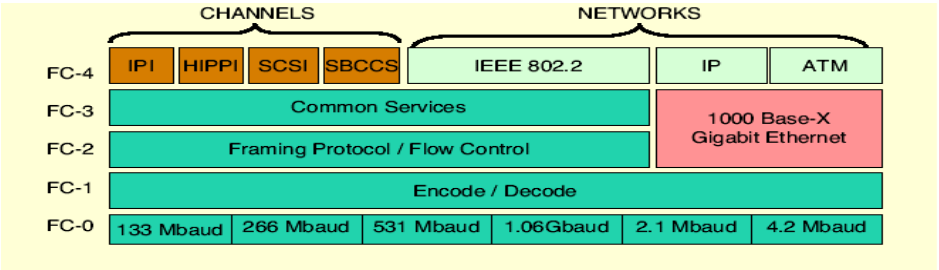
e. Do not install unnecessary programs on your work computer.

26.
   a. Loss of access to the campus computing network
   b. Loss of confidentiality, integrity and/or availability of valuable university information, re
   c. Lawsuits, loss of public trust and/or grant opportunities, prosecution, internal disciplinary action or termination of employment
27. Duration, Computer ID
28. i. ipconfig/ release ii. ipconfig/ renew
29. four packets:
   a. DHCPDISCOVER
   b. DHCPOFFER
   c. DHCPREQUEST
   d. DHCPACK
30. Addresses for 1. Servers 2. Routerinterfaces
31.
   a. Shorter leases for mobile devices such as laptops
   b. Longer leases for permanent devices such as desktops
32. Proxy server
   a. Used when clients do not access the web directly
   b. Used for security, logging, accounting and performance
33. Caching
   a. Shorter response time
   b. Reduced bandwidth requirement
   c. Reduced load on servers
   d. Access control and logging
34. By logging & monitoring each packet, it can restrict packets based on IP address, Contents of packets.
35. VSAT
   a. Full or partial independence from terrestrial infrastructure
   b. Cost savings over terrestrial lines
   c. Nationwide reach, distance-independent
   d. Network management from a single point
   e. Quick deployment, network flexibility
   f. Consistent and rapid response time
   g. Increased network availability and reliability
   h. Inherent broadcast / multicast platform
36. BUC
   Block up-converter converts incoming I.F. (from IDU) to R.F. transmitting frequency, amplifies it and passes it to feed.
37. LNB
   LNB amplifies incoming R.F.(Radio Frequency) from feed using low noise amplifier, converts it to I.F. and passes it to IDU
38. IDU
   a. On receive side-IDU converts I.F. (Intermediate Frequency) from ODU to base band signals which may be data, video or voice.
   b. On transmit side-IDU converts base band signals to I.F. and passes them to ODU.

39. **VSAT Equipment is mainly consist of-**
    a. **ODU (Outdoor Unit)**
    b. **IDU (Indoor Unit)**



40. VSAT services
    a. LEASED LINES Through VSAT on IP PLATFORM: 4KbpS Onwards
    b. High speed Broadband Internet
    c. VPN Networking
    d. VOIP Telephony
    e. Facsimile
    f. Telemedicine
    g. E-learning
    h. IP multicasting, video conferencing, Video streaming
    i. DSPT (Digital Satellite Phone Terminal)
41. One way, two way star, two way star-double hop, two way mesh
42. A SAN (Storage Area Network) is a network designed to transfer data from servers to targets, and it is alternative to a directly attached target architecture, or to a DAS architecture, where the storage is connected to the servers on general purpose networks
43. Network storage forms
    a. Direct access storage (DAS)
    b. Network attached storage (NAS)
    c. Storage area network (SAN)
44.



45. San benefits
    a. Storage consolidation
    b. Data sharing
    c. Non-disruptive scalability for growth
    d. Improved backup and recovery

e. Tape pooling
f. LAN-free and server-free data movement
g. High performance
h. High availability server clustering
i. Data integrity
j. Disaster tolerance
k. Ease of data migration
l. Cost-effectives (total cost of ownership)

46. Point to point, Arbitrated Loop, Switched fabric
47. RAID 5
    a. Data protection with ECC, but parity is spread on the array
    b. Good redundancy
    c. Same speed reads, slower writes
    d. One disk per array of added cost
48. Firewall types
    a. Packet-filtering routers
    b. Application-level gateways
    c. Circuit-level gateways
49. Aims to put a firewall
    a. Establish a controlled link
    b. Protect the premises network from Internet-based attacks
    c. Provide a single choke point
50. Intrusion

a. A set of actions aimed to compromise the security goals, namely Integrity, confidentiality, or availability, of a computing and networking resource

51. IDS implementation options
    a. Network-based IDS
    b. Host-base IDS
    c. Hybrid implementations
52. Virus can
    a. Carry out a denial of service attack
    b. Crash the machine
    c. Randomly destroy data
    d. Install a trojan horse program
    e. Perform password cracking
53.