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

**II. Telemetry**

1. Define Telemetry
2. Name any three options available for Power Utility Communication
3. List any four required features ofPower Utility Communication
4. Name the components of PLCC.
5. List any four advantages of Optical Fiber Communication
6. Optical Fiber Communication, for long distance transmission, which of SM or MM fibers is used & why?
7. List three limitations of PLCC

**III. Cyber security in power sector**

1. List three areas of power sector which are vulnerable for cyber attacks
2. Define Cyber Security
3. List any for actions required for cyber security
4. Explain Malicious code attacks
5. What is phishing attack
6. Explain DoS Attack
7. What do we mean by Physical security in reference to cyber security
8. List any four cyber security measures at work
9. What are the consequences if organisation/employees are not aware of cyber threats

**IV. Proxy & DHCP**

1. Leased IP provided by a DHCP server depends on which factors?
2. Write down the commands in proper order for renewing an IP address provided by DHCP manually using command prompt.
3. Name the four packets used for communication during the IP assignment by DHCP server to a host.
4. Which IP addresses should be excluded from the range of DHCP server in a Network?
5. What are the general guidelines for setting lease duration parameter during a DHCP server configuration?
6. Why a Proxy server is used in LANs?
7. What are the reasons to do Caching in the networks?
8. How proxy provides control and discipline in a LAN?

**IV. WAN using VSAT**

1. List any four advantages of VSAT communication
2. Write down the functions of BUC in a VSAT network.
3. Write down the functions of LNB in a VSAT network.
4. List the functions of IDU of VSAT.
5. Draw the diagram of a VSAT terminal marking all important elements.
6. List any four services that can be provided using VSAT.
7. List the type of topologies supported by VSAT network.

**V. SAN**

1. What is SAN?
2. List three basic forms of Network storage
3. Draw the layered architecture of FC protocol
4. List any four SAN benefits.
5. List the three topologies supported by SAN
6. Describe RAID 5

**VI. Security, AV, IDS, Firewall**

1. Name the Three common types of Firewalls
2. List three aims to put firewalls
3. Define Intrusion
4. Name the three IDS implementation options.
5. List any four malicious effects of a virus infection

Answers

* 1. Broadcast Address – 210.212.140.255
	2. IP Address of First possible host – 210.212.140.1
	3. IP Address of Last possible host – 210.212.140.254
	4. Subnet Mask- 255.255.255.0
	5. Larger address space
	6. Better security
	7. Global reachability
	8. Efficient routing
	9. Multihoming
	10. Scalability
	11. Autoconfiguration
	12. Static or manual
	13. Dynamic or automatic
	14. Static or manual
	15. Dynamic or automatic (using DHCP server)
	16. Autoconfiguration (without DHCP server)
	17. Distance to be covered
	18. Bandwidth
	19. Security
	20. No of nodes to be connected
	21. Cost
1. To dissipate the signal power going towards ends in terminating resistance ,hence avoiding reflection of signals from open ends & causing collisions.
2. Easy to develop & scale
3. Easy fault diagnose
4. Cutting of media at one point does not disrupt whole network
5. High data rates
6. cheaper
7. To ensure interoperability among networks
8. To make networks independent of hardware & software platforms
9. To discourage monopoly in hardware & software
10. Automatic congestion control in the internetworks
11. To avoid infinite looping of packets
12. To efficiently use valuable internet bandwidth

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.

1. Sensing & measuring information at distance & transmitting it for processing at some central location
2. UHF, Microwave, Satellite, PLCC, Telephony cable, OFC, Radio links
3. 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

1. Line trap, Coupling Capacitor, Line Matching Unit (LMU), PLC terminal
2. Large carrying capacity, Low power loss, immunity to inductive interference, Light weight & small dia, higher security, negligible cross talk, long life of cable
3. 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.
4. Limited carrier frequency, Noise, Radio Interference
5. IT for system operations (SCADA, DAS), IT for other business functions (Metering, billing, HR, office automation) & Communication systems used for coordination
6. 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.
7. Use licensed software, install O/S & software updates, use firewalls & antivirus, Protect & change passwords, use online & offline periodic backups
8. 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.
9. 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.
10. 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
11. 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 movements may be monitored from the Control Room.
	1. Be sure to work with your technical support coordinator before implementing new cyber-safety measures.
	2. Talk with your technical support coordinator about what cyber-safety measures are in place in your department.
	3. 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.
	4. Physically secure your computer by using security cables and locking building/office doors and windows.
	5. Do not install unnecessary programs on your work computer.
	6. Loss of access to the campus computing network
	7. Loss of confidentiality, integrity and/or availability of valuable university information, re
	8. Lawsuits, loss of public trust and/or grant opportunities, prosecution, internal disciplinary action or termination of employment
12. Duration, Computer ID
13. i. ipconfig/ release ii. ipconfig/ renew
14. four packets:
	1. DHCPDISCOVER
	2. DHCPOFFER
	3. DHCPREQUEST
	4. DHCPACK
15. Addresses for 1. Servers 2. Routerinterfaces
	1. Shorter leases for mobile devices such as laptops
	2. Longer leases for permanent devices such as desktops
16. Proxy server
	1. Used when clients do not access the web directly
	2. Used for security, logging, accounting and
	 performance
17. Caching
	1. Shorter response time
	2. Reduced bandwidth requirement
	3. Reduced load on servers
	4. Access control and logging
18. By logging & monitoring each packet, it can restrict packets based on IP address, Contents of packets.
19. VSAT
	1. Full or partial independence from terrestrial infrastructure
	2. Cost savings over terrestrial lines
	3. Nationwide reach, distance-independent
	4. Network management from a single point
	5. Quick deployment, network flexibility
	6. Consistent and rapid response time
	7. Increased network availability and reliability
	8. Inherent broadcast / multicast platform
20. BUC

Block up-converter converts incoming I.F. (from IDU) to R.F. transmitting frequency, amplifies it and passes it to feed.

1. LNB

LNB amplifies incoming R.F.(Radio Frequency) from feed using low noise amplifier, converts it to I.F. and passes it to IDU

1. IDU
	1. On receive side-IDU converts I.F. (Intermediate Frequency) from ODU to base band signals which may be data, video or voice.
	2. On transmit side-IDU converts base band signals to I.F. and passes them to ODU**.**
2. **VSAT Equipment is mainly consist of-**
	1. **ODU ( Outdoor Unit )**
	2. **IDU ( Indoor Unit )**

****

1. VSAT services
	1. LEASED LINES Through VSAT on IP PLATFORM: 4KbpS Onwards
	2. High speed Broadband Internet
	3. VPN Networking
	4. VOIP Telephony
	5. Facsimile
	6. Telemedicine
	7. E-learning
	8. IP multicasting, video conferencing, Video streaming
	9. DSPT (Digital Satellite Phone Terminal)
2. One way, two way star, two way star-double hop, two way mesh
3. 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
4. Network storage forms
	1. Direct access storage (DAS)
	2. Network attached storage (NAS)
	3. Storage area network (SAN)



1. San benefits
	1. Storage consolidation
	2. Data sharing
	3. Non-disruptive scalability for growth
	4. Improved backup and recovery
	5. Tape pooling
	6. LAN-free and server-free data movement
	7. High performance
	8. High availability server clustering
	9. Data integrity
	10. Disaster tolerance
	11. Ease of data migration
	12. Cost-effectives (total cost of ownership)
2. Point to point, Arbitrated Loop, Switched fabric
3. RAID 5
	1. Data protection with ECC, but parity is spread on the array
	2. Good redundancy
	3. Same speed reads, slower writes
	4. One disk per array of added cost
4. Firewall types
	1. Packet-filtering routers
	2. Application-level gateways
	3. Circuit-level gateways
5. Aims to put a firewall
	1. Establish a controlled link
	2. Protect the premises network from Internet-based attacks
	3. Provide a single choke point
6. Intrusion
	1. A set of actions aimed to compromise the security goals, namely Integrity, confidentiality, or availability, of a computing and networking resource
7. IDS implementation options
	1. Network-based IDS
	2. Host-base IDS
	3. Hybrid implementations
8. Virus can
	1. Carry out a denial of service attack
	2. Crash the machine
	3. Randomly destroy data
	4. Install a trojan horse program
	5. Perform password cracking