**1. Types of Networks: LAN, MAN, WAN**

**LAN (Local Area Network)**

* **Definition**: A network within a limited area like a building or campus.
* **Characteristics**: High-speed data transfer, privately owned, low latency, typically used for internal communications.
* **Examples**: Office networks, home Wi-Fi networks.

**MAN (Metropolitan Area Network)**

* **Definition**: Covers a city or large campus, connecting multiple LANs.
* **Characteristics**: Uses high-capacity backbone technologies like fiber optics to bridge the LANs over longer distances.
* **Examples**: City-wide public Wi-Fi networks.

**WAN (Wide Area Network)**

* **Definition**: A large-scale network that connects multiple LANs and MANs over vast distances.
* **Characteristics**: Typically slower speeds due to vast distances, uses leased lines or satellite connections.
* **Examples**: The Internet, international corporate networks.

**Acronym**: **L-M-W** – *Local, Metro, World*

**2. Circuit Route in PSTN for Medium-Distance Call**

**Steps to Establish a Circuit Route**:

1. **Local Exchange**: The user’s call is initially routed to the local telephone exchange.
2. **Tandem Switches**: If the call is outside the local area, the tandem switches act as intermediate devices to route the call over greater distances.
3. **Trunk Lines**: High-capacity trunk lines are used to carry the signal over medium or long distances.
4. **Destination Exchange**: Finally, the signal reaches the destination exchange for final routing to the recipient’s telephone.

**Acronym**: **L-T-T-R** – *Local, Tandem, Trunk, Receiver*

**3. IP Header Format & TTL Role in DoS Attacks**

**IP Header Fields**:

* **Version (4 bits)**: Identifies the version of IP (IPv4 or IPv6).
* **Header Length (4 bits)**: Specifies the length of the IP header.
* **Type of Service (ToS)**: Determines the priority of the packet.
* **Total Length**: Specifies the total size of the packet.
* **Identification, Flags, Fragment Offset**: Used for packet fragmentation and reassembly.
* **TTL (Time To Live)**: Prevents packets from circulating indefinitely in case of routing loops.
* **Protocol**: Defines the protocol used at the transport layer (TCP, UDP).
* **Source & Destination IP**: Identifies the origin and destination addresses.

**TTL in DoS Attacks**:

* **Role of TTL**: The TTL value is decremented by each router as the packet passes through. A small TTL value can prevent packets from reaching their destination and flood the network with traffic in DoS (Denial of Service) attacks.

**Acronym**: **VIP-TTL** – *Version, IPs, Protocol, TTL*

**4. Framing & Data Link Layer Role**

**Framing**:

* **Definition**: Framing is the process of encapsulating data into frames for transmission over the physical layer.

**Data Link Layer Functions**:

1. **Encapsulation**: It adds headers and trailers to the data received from the Network Layer.
2. **Transmission**: The frame is then transmitted over the physical medium.
3. **Decapsulation**: At the receiver’s end, the frame is stripped of its header and trailer to retrieve the data.

**Acronym**: **EDF** – *Encapsulate, Decapsulate, Frame*

**5. Importance of Domain Name & IP Address**

**Role of Domain Name**:

* **Easier Identification**: Domain names like [www.google.com](http://www.google.com/) are easier for humans to remember.
* **Translation**: DNS (Domain Name System) resolves the domain name to an IP address.

**Role of IP Address**:

* **Unique Identifier**: Every web server is assigned a unique IP address (e.g., 142.250.72.206) to ensure the correct delivery of data.

**Web Server Interaction**:

* A client types a domain name into the browser → DNS resolves it to an IP address → The server responds with the requested data.

**Acronym**: **DIP** – *Domain, IP, Process*

**6. CIDR: 64.32.16.8/27**

**CIDR Notation Calculation**:

* **Block Size**: 2^(32-27) = 32 addresses.
* **First Address**: 64.32.16.8
* **Last Address**: 64.32.16.39
* **Usable Addresses**: 64.32.16.9 to 64.32.16.38.

**Acronym**: **FBL** – *First, Block size, Last*

**7. DNS Hijacking**

**Definition**:

* DNS hijacking is a malicious attack that redirects DNS queries to unauthorized websites.

**Solutions**:

* Use **DNSSEC** to verify the authenticity of DNS responses.
* Employ **secure DNS resolvers** like DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT).
* Ensure routers and DNS servers are **updated regularly**.

**Example**:  
An attacker changes the DNS settings on a router, and users are redirected from legitimate sites like "[www.bank.com](http://www.bank.com/)" to phishing sites.

**Acronym**: **DRS** – *DNS, Redirect, Solution*

**8. SLAAC in DHCP**

**Definition**:

* **Stateless Address Autoconfiguration (SLAAC)** allows a device to automatically assign itself an IPv6 address without needing a DHCP server.

**How SLAAC Works**:

1. The host listens for **Router Advertisement (RA)** messages.
2. The router sends the network prefix to the host.
3. The host generates its full IPv6 address by combining the prefix with its interface ID.

**Acronym**: **SRI** – *Stateless, RA, Interface ID*

**9. VPN Operation**

**Functionality**:

* A **VPN** (Virtual Private Network) creates a secure, encrypted tunnel over the internet to allow private communication.

**Steps**:

1. The data is **encrypted** at the sender’s side.
2. A **secure tunnel** is established (e.g., using IPSec or SSL).
3. The encrypted data is **decrypted** at the receiver’s side.

**Example**:  
Employees working remotely can securely access corporate data without exposing sensitive information.

**Acronym**: **ETD** – *Encrypt, Tunnel, Decrypt*

**10. ISP Subnetting (190.100.0.0/16)**

**Subnet Allocation**:

* **Group 1**: 64 customers, each needing 256 addresses → 64 subnets of /24.
* **Group 2**: 128 customers, each needing 128 addresses → 128 subnets of /25.

**Slash Notation**:

* **Group 1**: /24
* **Group 2**: /25

**Acronym**: **GSN** – *Group, Subnet, Notation*

**11. Subnetting of 130.34.12.64/26**

**Subnet Breakdown**:

* Required: 4 subnets from the /26 network.
* Each subnet gets a new prefix:
  + **Subnet 1**: 130.34.12.64/28 → Addresses: 130.34.12.64 to 130.34.12.79
  + **Subnet 2**: 130.34.12.80/28 → Addresses: 130.34.12.80 to 130.34.12.95
  + **Subnet 3**: 130.34.12.96/28 → Addresses: 130.34.12.96 to 130.34.12.111
  + **Subnet 4**: 130.34.12.112/28 → Addresses: 130.34.12.112 to 130.34.12.127

**Acronym**: **SNR** – *Subnet, Notation, Range*

**12. Special Addresses in IPv4**

**Special IPv4 Addresses**:

1. **Loopback Address**: 127.0.0.1 (Used to test local networking stack).
2. **Broadcast Address**: 255.255.255.255 (Used to send packets to all devices in the network).
3. **Private Addresses**: Reserved for private networks (e.g., 10.0.0.0 to 10.255.255.255).
4. **APIPA Address**: 169.254.x.x (Assigned automatically if DHCP fails).

**Acronym**: **L-B-P-A** – *Loopback, Broadcast, Private, APIPA*

**13. Two-Tier vs Three-Tier Enterprise Network Architecture**

**Two-Tier Architecture**:

* **Structure**: Includes two layers: the access layer and the distribution layer.
* **Characteristics**: Simple design with fewer switches, often used in small to medium-sized enterprises.

**Three-Tier Architecture**:

* **Structure**: Includes three layers: access, distribution, and core.
* **Characteristics**: Scalable design, more robust for large enterprises with complex needs.

**Acronym**: **T-T-C** – *Two-Tier, Three-Tier, Core*

**14. Global Unicast Address in IPv6**

**Definition**:

* A **Global Unicast Address (GUA)** is a globally unique IP address that can be routed on the IPv6 internet.

**Characteristics**:

* Similar to public IPv4 addresses.
* Typically begins with "2" or "3" in the first hex digit.

**Acronym**: **GUA** – *Global Unicast Address*

**15. Three Types of Inter-VLAN Routing**

1. **Router-on-a-Stick**: A single router interface configured with subinterfaces for each VLAN.
2. **Layer 3 Switch**:

A switch with routing capability, directly routing traffic between VLANs. 3. **External Router**: A separate physical router connects multiple VLANs.

**Acronym**: **S-L-R** – *Stick, Layer 3, Router*

Here are the detailed answers for **Questions 16 to 20**, formatted pointwise with **acronyms** at the end of each answer for easy recall:

**16. What is an EtherChannel? Explain its Types.**

**Definition:**

* EtherChannel is a port-linking technology that allows bundling multiple physical Ethernet links into a single logical link for increased bandwidth and redundancy.

**Key Features:**

1. **Load Balancing:** Traffic is distributed across all bundled links.
2. **Redundancy:** If one link fails, traffic continues through others.
3. **Single IP/MAC:** Logical channel appears as a single interface to STP and Layer 3.

**Types of EtherChannel Protocols:**

1. **PAgP (Port Aggregation Protocol):** Cisco proprietary; automatic negotiation.
2. **LACP (Link Aggregation Control Protocol):** IEEE 802.3ad standard; vendor-neutral.

**Acronym:** **BLP** – *Bundle, Load-balance, PAgP/LACP*

**17. Compare Layer 2 Protocols: CDP and LLDP**

| **Feature** | **CDP** | **LLDP** |
| --- | --- | --- |
| Full Form | Cisco Discovery Protocol | Link Layer Discovery Protocol |
| Standard | Cisco proprietary | IEEE 802.1AB |
| Device Compatibility | Only Cisco devices | Multi-vendor interoperability |
| Information Shared | Device ID, IP, platform, ports | Same as CDP + optional extensions |
| Usage | Network troubleshooting | Network inventory and management |

**Acronym:** **CSUDI** – *Cisco, Standard, Usage, Devices, Info*

**18. Explain the Following VLAN Terms**

1. **Default VLAN:**
   * VLAN 1 is the default in Cisco switches. All ports are members unless reassigned.
2. **Access Ports:**
   * Connect to end devices (PCs, printers); carry traffic for a single VLAN.
3. **Trunk Ports:**
   * Connect between switches; carry traffic for multiple VLANs using tagging (802.1Q).
4. **DTP (Dynamic Trunking Protocol):**
   * Cisco protocol that negotiates trunk links automatically between switches.
5. **VTP (VLAN Trunking Protocol):**
   * Distributes VLAN information across switches to maintain consistency.

**Acronym:** **DATDV** – *Default, Access, Trunk, DTP, VTP*

**19. Explain IEEE 802.11 in Detail**

**Definition:**

* IEEE 802.11 is the set of standards for wireless local area networking (Wi-Fi).

**Standards and Features:**

1. **802.11a:** 5 GHz, 54 Mbps
2. **802.11b:** 2.4 GHz, 11 Mbps
3. **802.11g:** 2.4 GHz, 54 Mbps
4. **802.11n:** 2.4/5 GHz, up to 600 Mbps (MIMO)
5. **802.11ac:** 5 GHz, gigabit speed, wider channels
6. **802.11ax (Wi-Fi 6):** High efficiency, more devices, lower latency

**Security:**

* WEP → WPA → WPA2 → WPA3

**Acronym:** **ABG-NAX** – *a, b, g, n, ac, ax*

**20. Describe Routing in a Network & Shortest Path Routing**

**Definition:**

* Routing is the process of forwarding data packets from source to destination using routers.

**Types of Routing:**

1. **Static Routing:** Manual configuration; less flexible.
2. **Dynamic Routing:** Uses protocols to learn/update routes.

**Shortest Path Routing:**

* Uses algorithms like **Dijkstra's Algorithm** to find the optimal path.

**Routing Protocols:**

* **OSPF:** Link-state, shortest path calculation.
* **RIP:** Distance-vector, max 15 hops.
* **EIGRP:** Hybrid protocol with DUAL algorithm.

**Acronym:** **SDS-OER** – *Static, Dynamic, Shortest path, OSPF, EIGRP, RIP*

**21. Importance of Firewall and Its Types**

**Importance:**

* **Network Security:** Prevents unauthorized access and cyber threats.
* **Traffic Control:** Monitors incoming/outgoing data.
* **Policy Enforcement:** Enforces network usage rules.
* **Threat Mitigation:** Detects and blocks malware, DDoS, etc.

**Types of Firewalls:**

1. **Packet-Filtering Firewall:** Filters based on IP, ports, protocols.
2. **Stateful Inspection Firewall:** Tracks state of active connections.
3. **Proxy Firewall:** Intercepts and inspects traffic at application level.
4. **Next-Gen Firewall (NGFW):** Integrates antivirus, IDS/IPS, DPI, etc.

**Diagram:** (You can include a simple network diagram showing firewall between internal LAN and Internet)

**Acronym:** **NTP-S** – *Network, Traffic, Policy, Security*

**22. WAN Technology Options**

**Definition:**

* WAN connects devices across large geographical areas.

**Options:**

1. **Leased Line:** Dedicated, expensive, high-speed.
2. **DSL (Digital Subscriber Line):** Uses telephone lines.
3. **MPLS (Multiprotocol Label Switching):** Fast routing using labels.
4. **Frame Relay:** Packet-switching, older tech.
5. **Satellite & Cellular (4G/5G):** Wireless communication over long distances.

**Example:** Company HQ in Delhi connected to branch in Mumbai via MPLS.

**Acronym:** **LDM-FC** – *Leased, DSL, MPLS, Frame, Cellular*

**23. Network Topology & Types (LAN)**

**Definition:**

* Physical/logical arrangement of devices in a network.

**Topologies:**

1. **Bus:** All nodes connected to a single backbone.
2. **Star:** Central switch connects all nodes.
3. **Ring:** Nodes connected in a loop.
4. **Mesh:** Every node connects to every other.
5. **Tree:** Hierarchical combination of star and bus.

**Diagram:** Include visual representation of each.

**Acronym:** **B-S-R-M-T** – *Bus, Star, Ring, Mesh, Tree*

**24. Advantages & Disadvantages of Topologies**

| **Topology** | **Advantages** | **Disadvantages** |
| --- | --- | --- |
| Bus | Easy to implement, less cable | Difficult troubleshooting |
| Star | Easy to manage, isolate faults | Central hub failure = network down |
| Ring | Equal access, orderly communication | A break disables entire network |
| Mesh | High redundancy, reliable | Costly and complex wiring |
| Tree | Scalable, structured | Dependent on main backbone |

**Acronym:** **BED-RC** – *Bus, Easy, Down; Ring, Complex*

**25. Compare Star, Bus, and Ring**

| **Feature** | **Star** | **Bus** | **Ring** |
| --- | --- | --- | --- |
| Reliability | High | Low | Medium |
| Cost | Moderate | Low | Medium |
| Performance | High | Low if traffic high | Fair (token passing) |
| Scalability | Easy | Limited | Difficult |

**Acronym:** **SRC-P** – *Star, Ring, Cost, Performance*

**26. Short Questions (Assumed sub-parts are in 27-30)**  
(Handled in following questions)

**27. Router Modes & Commands**

**Modes:**

1. **User Mode:** Basic commands, monitoring.
2. **Privileged Mode:** Access to all router commands.
3. **Global Configuration Mode:** Router-wide configuration.

**Commands:**

* show ip interface brief, enable, configure terminal, exit

**Acronym:** **UPG-C** – *User, Privileged, Global – Commands*

**28. Router Memory Types**

1. **ROM:** Bootstrap instructions.
2. **RAM:** Running configuration, routing tables.
3. **NVRAM:** Stores startup configuration.
4. **Flash:** Contains IOS image.

**Acronym:** **R-RNF** – *ROM, RAM, NVRAM, Flash*

**29. Verification Commands**

1. **Ping:** Tests connectivity using ICMP.
2. **Traceroute:** Shows path a packet takes.
3. **Telnet:** Remote login and testing TCP connectivity.

**Use:**

* Helpful for diagnosing network issues and verifying routes.

**Acronym:** **PTT** – *Ping, Traceroute, Telnet*

**30. VLAN and Its Benefits**

**Definition:**

* Virtual LAN is a logical grouping of devices in the same broadcast domain, regardless of physical location.

**Benefits:**

1. **Segmentation:** Isolates traffic.
2. **Security:** Reduces broadcast storms and unauthorized access.
3. **Efficiency:** Reduces congestion.
4. **Flexibility:** Devices can move without reconfiguring network.

**Acronym:** **SSEF** – *Segmentation, Security, Efficiency, Flexibility*

**MCQ**

**1. Version 6 of IP address has how many bits?**  
a. 64 bits  
**b. 128 bits**  
c. 32 bits  
d. 256 bits

**2. Given an IP address 172.16.28.252 with a subnet mask of 255.255.240.0, what is the correct network address?**  
a. 172.16.16.0  
b. 172.16.0.0  
**c. 172.16.24.0**  
d. 172.16.28.0

**3. Which IPv6 address is the equivalent of the IPv4 interface loopback address 127.0.0.1?**  
**a. ::1**  
b. ::  
c. 2000::/3  
d. 0::/10

**4. Which command enables IPv6 forwarding on a Cisco router?**  
a. ipv6 local  
a. ipv6 host  
**c. ipv6 unicast-routing**  
d. ipv6 neighbor

**5. What is known as "one-to-nearest" addressing in IPv6?**  
a. global unicast  
**b. anycast**  
c. multicast  
d. unspecified address

**6. What is the network mask for n=13?**  
a. 255.247.0.0  
b. 255.246.0.0  
**c. 255.248.0.0**  
d. 255.249.0

**7. Which of the following statement is incorrect?**  
a. The role of prefix is defining the network to which the host belongs  
**b. In subnetting, the value of prefix is always less than the value of the prefix of the original network**  
c. In CIDR, the prefix is always added to the address separated by a slash  
d. In the network mask, the rightmost 32-n bits are set to 0's

**8. Which of these addresses cannot be used as a source address?**  
**a. 0.0.0.0**  
b. 255.255.255.255  
c. 192.168.1.7  
d. 172.16.0.1

**9. You are the new IT admin, and you need to find the network configuration. What should you use?**  
**a. ipconfig**  
b. cmd  
c. netchange  
d. newnet

**10. To get the most detailed network configuration, use this command.**  
**a. ipconfig /all**  
b. ipconfig  
c. ipconfig /renew  
d. ipconfig /most

**11. This command sends a request out and expects a response, indicating that both hosts are communicating.**  
**a. ping**  
b. tracert  
c. ipconfig /renew  
d. nslookup

**12. If you wanted to ping a host but also follow the path at which it pings, what would you use?**  
**a. tracert**  
b. ping  
c. tracert /ping  
d. ipconfig /most

**13. The IP network 192.168.50.0 is to be divided into 10 equal sized subnets. Which of the following subnet masks can be used for the above requirement?**  
a. 255.243.240  
b. 255.255.0.0  
**c. 255.255.255.0**  
d. 255.255.255.255

**14. Which of the following is correct IPv4 address?**  
a. 124.201.3.1.52  
b. 300.142.210.64  
c. 10110011.32.16.8  
**d. 128.64.0.0**

**15. What IP address class allocates 8 bits for the host identification part?**  
**a. Class A**  
b. Class B  
c. Class C  
d. Class D

**16. Default Administrative Distance Value of RIP routing Protocol is:**  
a. 0  
b. 1  
c. 100  
**d. 120**

**17. MPLS in WAN Technologies expands to:**  
**a. Multiprotocol Label Switching**  
b. Mono-protocol Label Switching  
c. Multiple Protocol Layer Switching  
d. Monotonous Protocol Layer Subnetting

**18. Which of the following is TRUE for etherchannel protocols?**  
**a. PAgP is a Cisco proprietary protocol for Ether Channel.**  
b. LACP is a Cisco proprietary protocol for Ether Channel.  
c. LACP is an open-source IEEE 802.1ad standard.  
d. PAgP is an open-source IEEE 802.1ad standard.

**19. Which of the following is TRUE for Router-on-stick inter VLAN routing?**  
a. Each VLAN is connected to a different physical router interface.  
b. Large networks with a large number of VLANs require many router interfaces.  
**c. Logical subinterfaces are created, one sub-interface per VLAN.**  
d. IP routing needs to be enabled.

**20. \_\_\_\_\_\_\_\_\_ is one way to set up a direct point-to-point connection across a network, for the purpose of simplifying connections between separate networks.**  
a. CDP  
b. PgDP  
c. LACP  
**d. GRE**

**21. If one needs to pass traffic over an incompatible network, a \_\_\_\_\_\_ should be implemented.**  
**a. VPN**  
b. GRE Tunnel  
c. VLAN  
d. PAN

**22. The above set of commands are part of:**  
a. Legacy inter VLAN routing  
**b. Router-on-a-stick inter VLAN routing**  
c. Multilayer switch inter VLAN routing  
d. Difficult VLAN routing

**23. Administrative distance is used to rate routing protocol’s:**  
a. Time management  
**b. Trustworthiness**  
c. Path selection criteria  
d. Ip address management

**24. A default administrative distance value 0 denotes:**  
**a. Static route out an interface**  
b. Static route to a next-hop  
c. Connected interface  
d. IGRP

**25. Which of the following is NOT a part of WAN optimization?**  
a. Compression  
b. Protocol optimization  
c. Traffic shaping  
**d. No caching**

**26. An \_\_\_\_\_\_\_\_ is a data communications technique in which software is used to create virtual networks on top of another network, typically a hardware and cabling infrastructure.**  
**a. Overlay network**  
b. Partial Network  
c. Relay Network  
d. Underlay Network

**27. PoS in WAN technologies expands to:**  
**a. Packet over SONET**  
b. Process of SDWAN  
c. Packet of Successful delivery  
d. Process of Synchronization

**28. The correct order of Configuring PAP Authentication on WAN interface is:**  
a. Step 1 is ‘creating the account’  
Step 2 is ‘assigning the credentials’  
Step 3 is enabling PAP  
**b. Step 1 is enabling PAP  
Step 2 is ‘assigning the credentials’  
Step 3 is ‘creating the account’**  
c. Step 1 is ‘assigning the credentials’  
Step 2 is enabling PAP  
Step 3 is ‘creating the account’  
d. Step 1 is enabling PAP  
Step 2 is ‘creating the account’  
Step 3 is ‘assigning the credentials’

**29. In Point-to-Point Protocols, which authentication protocol is encrypted one:**  
a. PAP  
**b. CHAP**  
c. PaGP  
d. LACP

**30. In Dynamic Trunking Protocol, which of the following settings on the two connecting switches will not result in a TRUNK port?**  
a. S1: Dynamic desirable, S2: Dynamic desirable  
b. S1: Dynamic Auto, S2: Access  
c. S1: Dynamic Auto, S2: Trunk  
**d. S1: Dynamic Auto, S2: Dynamic desirable**

Here are the answers for questions 31 to 48:

**31. The device router, bridge, Gateway are used in which of the following layers of OSI reference model:**  
a) Layer -2, Layer-1 and Layer-5  
b) Layer-3, Layer-2, Layer-7  
**c) Layer-1, Layer-3, Layer-5**  
d) Layer-7, Layer-2, Layer-3

**32. To deliver a message to the correct application program running on a host, the \_\_\_\_\_\_\_ address must be consulted.**  
**a. port**  
b. IP  
c. physical  
d. None of the above

**33. Transmission media lie below the \_\_\_\_\_\_\_ layer.**  
**a. physical**  
b. network  
c. transport  
d. application

**34. One of the responsibilities of the transport layer protocol is to create a \_\_\_\_\_\_ communication.**  
**a. host-to-host**  
b. process-to-process  
c. node-to-node  
d. none of the above

**35. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a method of implementing a telecommunication network in which two network nodes establish a dedicated communication channel before the nodes communicate with each other**  
a. Packet switching  
b. Message switching  
**c. Circuit Switching**  
d. End-to-end transmission

**36. What is the size of MAC Address?**  
a) 16-bits  
b) 32-bits  
**c) 48-bits**  
d) 64-bits

**37. The 8-bit field in IPv4 header which controls the maximum number of routers visited by the datagram during its lifetime**  
a) VER  
b) Header length  
c) Payload  
**d) Time to live (TTL)**

**38. Which of the following is a wireless LAN standards?**  
**a) IEEE 802.11**  
b) IEEE 609.12  
c) IEEE 803.14  
d) IEEE 809.10

**39. Which of the following is a wireless WAN standard?**  
a) IEEE 802.11  
b) IEEE 609.12  
c) IEEE 803.14  
**d) IEEE 802.16**

**40. Authentication mechanisms use \_\_\_\_\_\_\_\_\_\_ qualities to confirm a user's identity**

1. Something the user knows.
2. Something the user has
3. Something the user is  
   **4. All of the above**

**41. During computer communication in a network the following two key words are transmitted: 1 1 0 1 0 1 1 0 and 0 0 0 0 1 1 0 0. After Mod 2 operation what is the final key word received is \_\_\_\_\_\_\_\_\_\_\_\_\_**

(As this is a bitwise operation question, you would perform XOR on the two given sets. This answer would depend on the XOR of these bit sequences.)

**42. Bit stuff the following payload:**  
100000111111111110000010101010101111111111000111111111111111000

(Bit stuffing adds a 0 bit after five consecutive 1 bits, to ensure data integrity in the transmission. A detailed operation of the stuffing will result in a longer sequence.)

**43. A class A network on the internet has a subnet mask of 255.255.224.0. What is the maximum number of subnets connected**  
a) 4  
b) 6  
**c) 8**  
d) 10

**44. In the label header of MPLS the no.of bits allocated for TTL are:**  
**a) 8**  
b) 6  
c) 16  
d) 32

**45. VPN stands for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  
**a. Virtual Private Network**

**46. DNS uses port no. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ during internet operations**  
a) 50  
b) 25  
c) 80  
**d) 53**

**47. DHCPv4 assigns IPv4 addresses and other network configuration information \_\_\_\_\_\_\_\_\_\_\_**  
**a) Dynamically**  
b) Static  
c) both static & dynamic  
d) None of the above

**48. DHCPv4 server sends the binding \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_message to the requesting client as a unicast.**  
a) DHCPDISCOVER  
b) DHCPREQUEST  
**c) DHCPOFFER**  
d) DHCPACK

1. **Which of the following is not a characteristic of a VPN?**  
   A. It is a secure network  
   B. It is deployed over a shared infrastructure  
   C. It may use tunneling techniques  
   **D. It does not provide any cost savings to alternate connectivity options**
2. **What would be a good characterization of a VPN tunnel established between a telecommuter's PC using a VPN client software and a VPN Concentrator at the HQ location?**  
   **A. Remote access VPN**  
   B. Site to site VPN  
   C. Extranet VPN  
   D. LAN to LAN VPN
3. **Which of the following may be used as a terminating point for a site to site VPN tunnel?**  
   A. Router  
   B. Firewall  
   C. Concentrator  
   **D. All of the above**
4. **Which of the following is not a Layer 2 tunneling protocol?**  
   A. PPTP  
   B. IPSEC  
   C. L2TP  
   D. L2F
5. **Which of the following security techniques provide confidentiality (data privacy) service?**  
   A. Key exchange  
   **B. Encryption**  
   C. All of the above  
   D. Hashing
6. **DES, 3DES, and AES are examples of encryption algorithms that use the same key for encryption and decryption. Such encryption algorithms are categorized as:**  
   A. Asymmetrical encryption  
   **B. Symmetrical encryption**  
   C. Secure Hash Function  
   D. Public Key Infrastructure
7. **Which of the following is not true about DES, 3DES and AES?**  
   A. DES has the least cryptographic strength  
   B. 3DES is strong but has high CPU overhead  
   **C. AES offers a good balance of cryptographic strength and CPU overhead**  
   D. AES has export restrictions associated with it
8. **What do you call a cryptographic function that has the following features: - Takes a variable-sized message as input and produces a fixed-length output - The output will be identical for an identical input - A one-way function that is difficult to reverse (invert)?**  
   A. Encryption  
   B. Key Exchange  
   **C. Hashing**  
   D. Scrambling
9. **Hashing functions like MD5 and SHA are used in IPSEC to provide which of the following services:**  
   A. Data confidentiality (privacy from eavesdropping)  
   **B. Data Integrity (data protected from being changed during transit)**  
   C. Securely negotiating a key over a unsecure media  
   D. Anti replay protection
10. **Which of the following processes is used in IPSEC to negotiate symmetric keys securely between endpoints over an unsecured intermediate media?**  
    **A. Diffie-Hellman Key Exchange**  
    B. Advanced Encryption Standard (AES)  
    C. Secure Hashing Algorithm (SHA)  
    D. None of the above
11. **Which of the following services is not provided by an IPSEC tunnel?**  
    A. Data Confidentiality  
    B. Origin Authentication  
    C. Data Integrity  
    **D. Protection from Spyware**
12. **Which of the following services is not provided by AH?**  
    **A. Data Confidentiality (encryption)**  
    B. Origin Authentication  
    C. Data Integrity  
    D. Protection against Anti Replay attacks
13. **Which protocol number is associated with ESP?**  
    A. 51  
    B. 53  
    **C. 50**  
    D. 500
14. **Which of the following is not performed during Phase 1 of ISAKMP?**  
    A. Negotiate ISAKMP SAs  
    B. Negotiate IPSEC SAs  
    C. Perform peer authentication  
    **D. Perform initial Diffie-Hellman Key Exchange**
15. **The end result of Phase 1 of ISAKMP is an interim secure channel over which Phase II of ISAKMP is performed. What does Phase II do?**  
    A. Negotiate ISAKMP SAs  
    **B. Negotiate IPSEC SAs**  
    C. Perform peer authentication  
    D. Perform initial Diffie-Hellman Key Exchange
16. **What is the end result of Phase II of ISAKMP?**  
    **A. The IPSEC tunnel is established**  
    B. Phase III of ISAKMP commences  
    C. The IPSEC tunnel is torn down and renegotiated  
    D. An interim secure channel is established
17. **Which of the following is NOT a value add of the companion protocol ISAKMP for IPSEC?**  
    A. It automates the IPSEC tunnel establishment process  
    B. It allows symmetric keys used by encryption and hashing algorithms to be negotiated dynamically  
    C. It gives a lifetime to the tunnel, after which the tunnel expires and is reestablished  
    **D. It reduces the overheads associated with IPSEC tunnel establishment**
18. **Where does ISAKMP reside in the TCP/IP protocol stack?**  
    A. Directly above IP with protocol number 50  
    **B. Above UDP with port number 500**  
    C. Above TCP with port number 500  
    D. Over AH/ESP with port number 500
19. **Which of the following approaches may be used to do peer authentication during Phase 1 of ISAKMP?**  
    A. Pre-Shared Keys  
    B. Digital Certificates  
    **C. All the above**  
    D. Peer authentication is not performed during Phase 1 of ISAKMP
20. **Which of the following is a proprietary extension to IPSEC that is not defined in the RFC specifications for IPSEC?**  
    A. Peer Authentication using digital certificates during Phase 1 of ISAKMP  
    B. Per User Authentication when connecting from VPN client to VPN concentrator  
    C. AES encryption for confidentiality  
    **D. An IPSEC tunnel operating in transport mode**
21. **Which of the following describes the capability for a VPN terminating interface to simultaneously send IPsec protected traffic and regular unprotected traffic?**  
    **A. Split tunneling**  
    B. Load Balancing  
    C. Firewalling  
    D. Dual Stack tunneling