That's quite an extensive list! Let's go through each question one by one:

1. What do you mean by socket?

- A socket is an endpoint for communication between two machines over a network. It enables processes to communicate with each other, either on the same machine or across a network, by sending and receiving data.

2. Explain socket header files.

- Socket programming in C typically involves including the `<sys/socket.h>` header file, which provides functions and structures for working with sockets, and `<netinet/in.h>` header file for handling Internet addresses.

3. Explain functions used in socket programming.

- Some common socket programming functions include `socket()` for creating a socket, `bind()` for associating a socket with a specific address and port, `listen()` for placing the socket in a passive listening state, `accept()` for accepting incoming connections, `connect()` for connecting to a remote socket, `send()` and `recv()` for sending and receiving data, and `close()` for closing the socket.

4. Differentiate between TCP socket and UDP socket.

- TCP sockets provide reliable, connection-oriented communication with error checking and data sequencing. UDP sockets provide unreliable, connectionless communication without error checking or sequencing. TCP ensures that data sent is received in the same order it was sent, while UDP does not guarantee ordering or delivery.

5. How communication between client and server done in TCP socket programming?

- In TCP socket programming, the server creates a socket and binds it to a specific port. It then listens for incoming connections using the `listen()` function. The client creates a socket and connects to the server using the `connect()` function. Once the connection is established, both client and server can send and receive data using the `send()` and `recv()` functions.

6. List features of packet tracer.

- Packet Tracer is a network simulation tool developed by Cisco. It allows users to create, configure, and simulate networks composed of Cisco devices. Some features include device configuration, network topology creation, packet simulation, and real-time network monitoring.

7. How to design a network in Packet Tracer?

- To design a network in Packet Tracer, you can:
  - Drag and drop devices from the device palette onto the workspace.
  - Connect devices using appropriate cables (Ethernet, serial, etc.).
  - Configure device settings such as IP addresses, routing protocols, and security settings.
  - Test the network by simulating traffic and monitoring device behavior.

8. Explain different types of cables supported in Packet Tracer software.

- Packet Tracer supports various types of cables including Ethernet cables (straight-through and crossover), serial cables, console cables, and fiber optic cables.

9. Write commands for router configuration.

- Router configuration commands in Packet Tracer include:
  - `enable`: Enters privileged EXEC mode.
  - `configure terminal`: Enters global configuration mode.
  - `interface [interface_name]`: Enters interface configuration mode.
  - `ip address [ip_address] [subnet_mask]`: Assigns an IP address to an interface.
  - `router ospf [process_id]`: Enters OSPF configuration mode.
  - `network [network_address] [wildcard_mask] area [area_id]`: Configures OSPF network statements.

10. What is the default gateway?

- The default gateway is the IP address of the router interface that a device uses to send packets to destinations outside of its own subnet.

11. Differentiate between router and switches.

- Routers operate at the network layer (Layer 3) of the OSI model and make forwarding decisions based on IP addresses. They connect multiple networks together. Switches operate at the data link layer (Layer 2) and forward frames based on MAC addresses. They connect devices within the same network segment.

12. What is DHCP? How to configure it?

- DHCP (Dynamic Host Configuration Protocol) is a network protocol used to dynamically assign IP addresses and other network configuration parameters to devices on a network. In Packet Tracer, DHCP can be configured on a router or a dedicated DHCP server using the `ip dhcp pool` and related commands.

13. Differentiate between OSPF and EIGRP.

- OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol) are both routing protocols used to determine the best path for routing packets. OSPF is an open standard protocol based on link-state routing, while EIGRP is a Cisco proprietary protocol based on distance-vector routing.

14. How dynamic routing is performed in EIGRP.

- In EIGRP, routers exchange routing information using hello packets. When a change occurs in the network, routers update their routing tables accordingly. EIGRP uses the Diffusing Update Algorithm (DUAL) to calculate the best path to a destination based on factors such as bandwidth, delay, reliability, and load.

15. How to configure a wireless router.

- To configure a wireless router in Packet Tracer:
  - Enter global configuration mode (`configure terminal`).
  - Configure the router's interface with an IP address (`interface [interface_name]` followed by `ip address [ip_address] [subnet_mask]`).
  - Enable the wireless LAN interface (`interface wlan 0`).
  - Configure the SSID and security settings (`ssid [SSID]`, `encryption mode [mode]`, etc.).

16. Write network administration commands.

- Network administration commands in Packet Tracer include:
  - `show running-config`: Displays the current configuration of the device.
  - `show ip route`: Displays the routing table.
  - `ping [ip_address]`: Tests connectivity to a specific IP address.
  - `traceroute [ip_address]`: Traces the route packets take to reach a destination.

17. How to configure an FTP server?

- To configure an FTP server in Packet Tracer, you can use the `ftp-server enable` command on a router to enable FTP services. You can then configure user accounts and access permissions using the `username` and `ip ftp username` commands.

18. Explain RSA algorithm in detail.

- RSA (Rivest-Shamir-Adleman) is a public-key cryptosystem widely used for secure data transmission. It involves generating a public and private key pair, where the public key is

used for encryption and the private key is used for decryption. The security of RSA relies on the difficulty of factoring large prime numbers.

19. Explain Diffie-Hellman algorithm in detail.

- Diffie-Hellman is a key exchange algorithm used to securely establish a shared secret key between two parties over an insecure channel. It allows the parties to agree on a secret key without explicitly transmitting it. The security of Diffie-Hellman relies on the difficulty of the discrete logarithm problem.

20. What do you mean by primitive root, coprime numbers?

- A primitive root modulo n is an integer g such that every integer coprime to n is congruent to a power of g modulo n. Coprime numbers are integers that have no common divisor other than 1.

21. How are keys generated in RSA?

- In RSA, keys are generated by selecting two large prime numbers, p and q. The product of these primes, n = p * q, is used as the modulus for both the public and private keys. The public key consists of the modulus n and an exponent e, while

the private key consists of the modulus n and an exponent d, which is the modular multiplicative inverse of e modulo φ(n), where φ is Euler's totient function.

22. Explain the logic of digital signature RSA cryptosystem implementation.

- In RSA, digital signatures are created by hashing the message to produce a fixed-length digest, which is then encrypted using the sender's private key. The recipient can verify the signature by decrypting it using the sender's public key and comparing the resulting digest with a newly computed hash of the message.

23. What do you mean by digital signature?

- A digital signature is a cryptographic technique used to authenticate the sender of a message and ensure its integrity. It involves creating a unique digital fingerprint of the message using a cryptographic hash function and then encrypting this fingerprint with the sender's private key. The recipient can verify the signature using the sender's public key.

24. What is Snort?

- Snort is an open-source network intrusion detection system (NIDS) and intrusion prevention system (IPS) that monitors network traffic for suspicious activity and alerts administrators to potential security threats.

25. Where is the snort.conf file located?

- The snort.conf file is typically located in the `/etc/snort/` directory on Unix-based systems or in the installation directory on Windows.

26. Explain different cybersecurity attacks.

- Cybersecurity attacks include various malicious activities aimed at exploiting vulnerabilities in computer systems or networks. Some common types of attacks include malware (viruses, worms, ransomware), phishing, DDoS (Distributed Denial of Service), man-in-the-middle attacks, SQL injection, and social engineering.

27. What is a DDoS attack?

- A DDoS (Distributed Denial of Service) attack is a malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of traffic from multiple sources.

28. What is cybersecurity?

- Cybersecurity is the practice of protecting computer systems, networks, and data from unauthorized access, cyberattacks, and other security breaches.

29. Differentiate between stream cipher and block cipher.

- A stream cipher encrypts data one bit or byte at a time, while a block cipher encrypts data in fixed-size blocks, typically 64 or 128 bits at a time.

30. Differentiate between symmetric and asymmetric cipher.

- In symmetric encryption, the same key is used for both encryption and decryption, while in asymmetric encryption (or public-key cryptography), different keys are used for encryption and decryption.

31. Explain the working of DES.

- DES (Data Encryption Standard) is a symmetric-key block cipher that encrypts data in 64-bit blocks using a 56-bit key. It involves multiple rounds of substitution, permutation, and bitwise operations to transform the plaintext into ciphertext.

32. Draw a block diagram of DES.

```
[Plaintext] -> Initial Permutation -> [16 Rounds of Feistel Function] -> Final Permutation -> [Ciphertext]
```

33. Numerical on RSA, Diffie-Hellman.

- Numerical problems involving RSA and Diffie-Hellman typically involve generating keys, performing modular exponentiation, and computing shared secret keys.

34. Linux network commands.

- Linux network commands include `ifconfig` for configuring network interfaces, `ping` for testing network connectivity, `traceroute` for tracing the route to a destination, `netstat` for displaying network statistics, and `iptables` for configuring firewall rules.

35. Class A, B, C, D, E IP addresses.

- Class A: 1.0.0.0 to 126.0.0.0
- Class B: 128.0.0.0 to 191.255.0.0
- Class C: 192.0.0.0 to 223.255.255.0
- Class D: 224.0.0.0 to 239.255.255.255 (Multicast)
- Class E: 240.0.0.0 to 255.255.255.255 (Reserved)

36. Comment on Private and public IPs.

- Private IPs are reserved for use within private networks and cannot be routed on the public internet. Public IPs are globally routable and can be accessed from anywhere on the internet.

37. How to configure Access Control List and MAC filtering.

- Access Control Lists (ACLs) can be configured on routers and switches to control traffic flow based on various criteria such as source/destination IP address, port number, protocol, etc. MAC filtering involves restricting network access based on the MAC addresses of devices.

38. What do you mean by NAT? Use of NAT.

- NAT (Network Address Translation) is a technique used to map private IP addresses to public IP addresses to enable communication between devices on a private network and the public internet. It allows multiple devices on a private network to share a single public IP address.

39. What do you mean by static NAT and Dynamic NAT.

- Static NAT involves mapping a specific private IP address to a specific public IP address on a one-to-one basis. Dynamic NAT involves mapping multiple private IP addresses to a pool of public IP addresses on a many-to-many basis.

40. Command to set static NAT.

- In Packet Tracer, the command to configure static NAT is:

```
ip nat inside source static [inside_local_ip] [outside_global_ip]
```