1.

a. Network connects a collection of devices that can provide computing power.

2.

a.Network protocol is a set of rules which is needed to create communication.
FTP-> files
SMTP->mails
HTTP->texts

b.TCP stands for transmission protocol. UDP stands for user datagram protocol.
TCP is a connection-oriented protocol and UDP is a connectionless protocol.
TCP is slower than UDP. TCP can resend lost data but UDP can't.

3.

a.LAN stands for local area network.
That means LAN is a collection of devices connected in one physical location.
WAN stands for wide area network.
That means WAN is a network that exists over a large-scale geographical area.
LANs allow users to transfer data faster.
WANs have a comparatively slower data transfer rate.
LAN has a higher speed, whereas WAN has a slower speed.

b.LAN used for private IoT networks, bot networks, and small business networks.

4.

a. The router is a device that capable of sharing data packets to different connections.
b. Switches connect devices to a singular LAN to transmit data from one device to another.
Hubs group Ethernet devices on a LAN, broadcasting all data to another.

5.

a. Firewall is a security device or application.
It can disable unauthorized networks
b.A VPN connection establishes a secure connection between you and the internet.
Via the VPN, all the data traffic is routed through an encrypted virtual tunnel.

6.

a.IP address is the unique identifying number assigned to every device connected to the internet. It is used to identify the place where the device is located
b.DNS converts IP Addresses to human-readable text.

7.

a.A gateway connects two networks with different transmission protocols together.

b. Bandwidth refers to the volume of data sent.

And latency refers to the speed at which it's transmitted.

8.

a.In networking, a packet is a unit of data.

b.TCP is more reliable but it transfers data more slowly.

UDP is more reliable but it transfers data more quickly.

9.

a.DHCP is used to dynamically assign an IP address to any device, or node, on a network so it can communicate using IP.

b.MAC address is used to identify the physical address of a device on the same local network.

10.

a.IPv6 is the current standard for assigning public IP addresses to internet-connected devices. IPv6 offers More efficient routing without fragmenting packets.

b.Better security**:**

IPv6 includes security in the underlying protocol.

Consideration of real-time**:**

To implement better support for real-time traffic IPv6

includes a flow label mechanism so routers can more easily recognize where to send information.

Plug and play:

IPv6 includes plug-and-play, which makes it easier for novice users to connect their machines to the network. Essentially, the configuration will happen automatically.

11.

a.A proxy server is a system or router that provides a gateway between users and the internet.

b. ISP provides access to the internet.

Part 2:

1. Client-server architecture, architecture of a computer network in which many clients request and receive responses from a centralized server.

2. Socket programming shows how to use socket APIs to establish communication links between remote and local processes. The processes that use a socket can reside on the same

system or different systems on different networks. A socket is a communication endpoint in a computer network**.** Sockets allow you to exchange information between processes on the same machine or across a network, distribute work to the most efficient machine, and easily allow access to centralized data.

3.

Advantages of socket programming

Platform Independence

One of the biggest advantages of Java Sockets is that they are platform-independent. This means that the same Java code can be run on multiple operating systems and devices without the need for modification. This allows for easy deployment of network-based applications across different systems and ensures that the application can be run on different devices without the need for platform-specific code.

Easy to Use

Java Sockets are also relatively easy to use, even for developers who are new to network programming. The Java API provides a simple, consistent interface for creating and managing sockets, which makes it easy to implement network-based applications without needing to understand the underlying network protocols.

Scalability

Java Sockets are highly scalable, making them suitable for large-scale network-based applications. They can easily handle thousands of simultaneous connections and can be used to create distributed systems that can handle high levels of traffic.

Security

Java Sockets provide built-in support for secure communication, including SSL and TLS encryption. This makes it easy to create secure network-based applications and ensures that sensitive data is protected while in transit.

Multithreading

Java Sockets support multithreading, which means that multiple threads can be used to handle multiple connections simultaneously. This improves the performance of network-based applications and allows them to handle a large number of requests without becoming overloaded.

Disadvantages of socket programming

Increased complexity cost and high-security restrictions.
Socket-based communications allow only to send packets of raw data between applications.
Communication can be established with the machine requested not with another machine.
Both ends should have the ability to intercept the data.