Q1. Network Interface Cards (NICs):

* NICs are hardware devices that allow computers to connect to a network.
* Types of NICs include Ethernet NICs, Wireless NICs, and Token Ring NICs.
* NICs work by transmitting and receiving data packets over a network, translating data between the network and the computer's internal bus structure.

Q2. Hub:

* A hub is a networking device that acts as a central connection point for devices in a network.
* Hubs work by receiving incoming data and then broadcast it to all connected devices, regardless of which device it was intended for.
* Hubs operate at the Physical layer (layer 1) of the OSI Model.

Q3. Switch:

* A switch is a networking device that forwards and filters data packets based on their destination MAC addresses.
* Unlike a hub, a switch only broadcasts data to the specific device for which it was intended, improving network efficiency and performance.
* Switches operate at the Data Link layer (layer 2) of the OSI Model.

Q4. Router:

* A router is a networking device that forwards data packets based on their destination IP addresses.
* Routers use routing tables and protocols to determine the best path for data to take.
* Routers operate at the Network layer (layer 3) of the OSI Model.

Q5. Bridge:

* A bridge is a networking device that connects multiple network segments together, allowing them to function as a single network.
* Bridges work by forwarding data only between the segments that need to communicate with each other.
* Bridges operate at the Data Link layer (layer 2) of the OSI Model.

Q6. Networking Wires and Connectors:

* Types of networking wires include twisted-pair, coaxial, and fiber optic cables.
* Common connector types include RJ45, BNC, and SC.
* Cable specifications include cable length, bandwidth, and maximum data transmission rate.

Q7. Wireless Access Points:

* Wireless Access Points (WAPs) are networking devices that allow wireless devices to connect to a wired network.
* WAPs work by receiving incoming wireless signals and converting them into wired signals for transmission over a network.
* WAPs may also provide a variety of other features such as security, traffic management, and user authentication.

Q8. Proxy Servers:

* Proxy servers are servers that act as intermediaries between clients and servers in a network.
* Proxy servers can be used for a variety of purposes, including content filtering, anonymity, and performance optimization.
* When a client device makes a request, the request is first sent to the proxy server, which then forwards it to the intended server and returns the response back to the client.

Q9. Firewall:

* A security system that controls incoming and outgoing network traffic based on predetermined security rules.
* Acts as a barrier between a private internal network and the public Internet to protect from unauthorized access and malicious attacks.
* Can be hardware, software, or a combination of both.
* Uses firewall policies to determine which traffic to allow or block.
* Can perform network address translation (NAT).

Working principle:

* Monitors and inspects all network traffic based on firewall policies.
* Analyses header information (such as source IP, destination IP, and port number) to determine if packet meets firewall criteria.
* Allows packet through or blocks it based on firewall policies.
* Enhances security with techniques like stateful packet inspection, application layer filtering, and intrusion detection/prevention.