Q1. What is the Dhcp Process for Client Machine?

Ans The Dynamic Host Configuration Protocol (DHCP) process for a client machine involves four steps:

1. DHCP DISCOVER
- The client sends a DHCP DISCOVER packet to discover a DHCP server.

2. DHCP OFFER
- The DHCP server responds with a DHCP OFFER packet, offering an IP address to the client

3. DHCP REQUEST
- The client responds with a PHCPREQUEST packet to accept the offer and request the IP address.

4. DHCPACK
- The DHCP server responds with a DHCPACK packet to confirm the IP address lease.

- This entire process is also known as DORA, which stands for discovery, offer, request and acknowledgement.

Q2. List some benefits of using DHCP?

Ans The use of DHCP on a network offers the following advantages:

1. It sets free the network administrator from the duties of setting up the configuration

information, such as the IP address, the subnet mask and the routing tables, manually.

- The DHCP simplifies network administration by doing these tasks automatically.

2. Avoids this and ~~the~~ sometimes the same IP address is assigned to ~~def~~ two different hosts.
- The DHCP avoids this and the consequent malfunctioning of both the hosts from happening.

3. If the DHCP was not used, then the movement of computers from one network to another requires must be reconfigured.
- With DHCP, you can move the computers from one network to ~~another~~ ~~are~~ different subnets or networks without the need to reconfigure them.

Q3. What is a mac address

Ans. A MAC address (short for medium access control address) is a unique identifier assigned to a network interface controller (NIC) for use as a network address ~~is~~ in communications within a network segment.
- This use is common on most IEEE 802 networking technologies, including Ethernet, Wi-fi and Bluetooth.
- Within the Open Systems Interconnection (OSI) network model, MAC addresses are used in the medium access control protocol sublayer of the data link layer.
- As typically represented, MAC addresses are recognizable as six groups of two hexadecimal

digits, separated by hyphens, colons, or without a separator.

Q4. what is ~~DH~~ Dhcp Spoofing?

Ans.
- DHCP Spoofing is a layer 2 security technology incorporated into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable.
- DHCP spoofing prevents unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients.
- DHCP snooping offers a number of benefits, such as increased security, reduced network downtime, and lower bandwidth consumption
- It protects the network from a variety of attacks by validating DHCP messages and filtering out potentially malicious offers.
- This creates a more secure environment where only legitimate devices can communicate, thus protecting sensitive data and preventing unauthorized access.
- DHCP snooping helps reduce network downtime due to unauthorized server activity.