

**Hardware Networking**

**Network Fundamental**

**SUBMITTED TO**

**KAMLESH SHUKLA SIR**

**SUBMITTED BY**

**MANAV BANDHANIA**

### 1. **Which of the following messages in the DHCP process are broadcasted? (Choose two)**

**Correct Answers:**

* C. Discover
* A. Request

**Explanation:**  
In the DHCP (Dynamic Host Configuration Protocol) process, certain messages are broadcasted to ensure proper communication between clients and servers:

* **DHCP Discover:**
  + **Purpose:** Initiated by a client to locate available DHCP servers.
  + **Broadcast Nature:** Since the client doesn't have an IP address yet, it sends the Discover message as a broadcast to the network, allowing all DHCP servers to receive it.
* **DHCP Request:**
  + **Purpose:** Sent by the client after receiving an offer, indicating its acceptance of the offered IP address.
  + **Broadcast Nature:** This message is broadcasted to inform all DHCP servers of the client's selection, ensuring that any other offers can be withdrawn.

Broadcasting these messages ensures that multiple DHCP servers on the network are aware of the client's actions, preventing IP address conflicts and ensuring efficient IP allocation.

### 2. **Which command would you use to ensure that an ACL does not block web-based TCP traffic?**

**Correct Answer:**

* B. permit tcp any any eq 80

**Explanation:**  
Access Control Lists (ACLs) are used to control network traffic and enforce security policies by permitting or denying packets based on specified criteria.

* **Command Breakdown:**
  + permit: Allows the specified traffic.
  + tcp: Specifies the protocol as TCP.
  + any: Indicates any source IP address.
  + any: Indicates any destination IP address.
  + eq 80: Specifies port 80, the default port for HTTP traffic.

### 3. **Explain Network Topologies**

**Explanation:**  
Network topology refers to the arrangement of various elements (links, nodes, etc.) in a computer network. It defines how different devices are connected and how data flows between them.

**Common Network Topologies:**

1. **Bus Topology:**
   * **Structure:** All devices are connected to a single central cable, known as the bus.
   * **Advantages:**
     + Easy to implement and extend.
     + Requires less cable length than some other topologies.
   * **Disadvantages:**
     + A failure in the central cable can bring down the entire network.
     + Performance degrades as more devices are added.
2. **Star Topology:**
   * **Structure:** All devices are connected to a central hub or switch.
   * **Advantages:**
     + Easy to install and manage.
     + Failure of one link doesn't affect others.
   * **Disadvantages:**
     + If the central hub fails, the entire network is inoperable.
     + Requires more cable than bus topology.
3. **Ring Topology:**
   * **Structure:** Each device is connected to two other devices, forming a circular data path.
   * **Advantages:**
     + Data flows in a single direction, reducing the chance of packet collisions.
   * **Disadvantages:**
     + A failure in any cable or device can disrupt the entire network.
     + Troubleshooting can be challenging.
4. **Mesh Topology:**
   * **Structure:** Every device is connected to every other device.
   * **Advantages:**
     + Provides high redundancy and reliability.
     + Failure of one link doesn't affect network connectivity.
   * **Disadvantages:**
     + Expensive and complex to install and manage.
     + Requires a large number of cables and ports.
5. **Tree Topology:**
   * **Structure:** A hybrid topology that combines characteristics of star and bus topologies, with groups of star-configured networks connected to a linear bus backbone.
   * **Advantages:**
     + Scalable and easy to manage.
     + Fault isolation is straightforward.
   * **Disadvantages:**
     + If the backbone line breaks, the entire segment goes down.
     + More complex than star or bus topologies.
6. **Hybrid Topology:**
   * **Structure:** A combination of two or more different topologies to form a resultant topology.
   * **Advantages:**
     + Flexible and scalable.
     + Can be designed to meet specific network requirements.
   * **Disadvantages:**
     + Complex design and implementation.
     + Can be expensive to maintain.

### 4. **Explain TCP/IP Networking Model** (continued)

1. **Application Layer (cont.):**
   * **Protocols:**
     + **HTTP (Hypertext Transfer Protocol):** Used for web browsing.
     + **SMTP (Simple Mail Transfer Protocol):** Email transfer.
     + **DNS (Domain Name System):** Resolves domain names to IP addresses.
2. **Transport Layer:**
   * **Function:** Provides end-to-end communication, data integrity, and flow control.
   * **Protocols:**
     + **TCP (Transmission Control Protocol):** Reliable, connection-oriented protocol that ensures data delivery.
     + **UDP (User Datagram Protocol):** Unreliable, connectionless protocol used for fast, low-latency applications like video streaming or DNS queries.
3. **Internet Layer:**
   * **Function:** Handles packet routing, addressing, and fragmentation for delivery across different networks.
   * **Protocols:**
     + **IP (Internet Protocol):** Routes packets across networks.
     + **ICMP (Internet Control Message Protocol):** Provides error messages and network diagnostics (e.g., ping).
     + **ARP (Address Resolution Protocol):** Resolves IP addresses to MAC addresses within a local network.
4. **Network Access Layer:**
   * **Function:** Manages hardware-level operations, including data transmission over physical media.
   * **Protocols:**
     + Ethernet, Wi-Fi, and other link-layer technologies.

### 5. **Explain LAN and WAN Networks**

#### **LAN (Local Area Network):**

* **Scope:** Covers small areas such as homes, offices, or schools.
* **Characteristics:**
  + High-speed communication (typically 1 Gbps or more).
  + Devices are connected via Ethernet cables, switches, or wireless access points.
  + Easier to set up and maintain compared to WANs.

#### **WAN (Wide Area Network):**

* **Scope:** Covers large geographical areas like cities, countries, or continents.
* **Characteristics:**
  + Uses technologies like leased lines, MPLS, or satellite links.
  + Typically slower than LANs due to distance and infrastructure limitations.
  + Often relies on Internet Service Providers (ISPs) for connectivity.

#### **Key Differences:**

| **Feature** | **LAN** | **WAN** |
| --- | --- | --- |
| Coverage Area | Small (e.g., a room) | Large (e.g., global) |
| Speed | High (1+ Gbps) | Moderate to low |
| Cost | Low | High |
| Ownership | Private | Shared with ISPs |

### 6. **Explain Operation of Switch**

A network **switch** is a device used to connect multiple devices in a LAN and operates primarily at **Layer 2** of the OSI model.

#### **How It Works:**

1. **Address Learning:**
   * The switch learns the MAC addresses of connected devices by analyzing incoming frames.
   * It stores this information in a **MAC address table**.
2. **Forward/Filter Decision:**
   * For each incoming frame, the switch checks the destination MAC address.
   * If the MAC address is in its table, the frame is sent to the specific port (unicast). If not, the switch broadcasts it.
3. **Loop Avoidance:**
   * Redundant paths in a network can cause loops.
   * The switch uses protocols like **Spanning Tree Protocol (STP)** to prevent loops.
4. **Port Security:**
   * A switch can be configured to restrict the number of MAC addresses on a port, preventing unauthorized devices from connecting.
5. **Full Duplex Operation:**
   * Switches can operate in full-duplex mode, allowing simultaneous sending and receiving of data without collisions.

### 7. **Describe the Purpose and Functions of Various Network Devices**

#### **Network Devices Overview:**

1. **Router:**
   * **Function:** Routes packets between different networks using IP addresses.
   * **Purpose:** Enables communication between LANs and WANs.
2. **Switch:**
   * **Function:** Connects devices within a LAN and forwards frames based on MAC addresses.
   * **Purpose:** Reduces collisions and increases network efficiency.
3. **Firewall:**
   * **Function:** Filters incoming and outgoing traffic based on security rules.
   * **Purpose:** Protects the network from unauthorized access and attacks.
4. **Access Point (AP):**
   * **Function:** Provides wireless connectivity.
   * **Purpose:** Extends LANs wirelessly.
5. **Modem:**
   * **Function:** Converts digital data to analog signals for transmission over telephone lines or cables.
   * **Purpose:** Connects the LAN to the internet.
6. **Network Interface Card (NIC):**
   * **Function:** Enables a device to connect to a network.
   * **Purpose:** Acts as the hardware interface between the computer and the network.

### 8. **List Appropriate Media, Cables, Ports, and Connectors to Connect Switches**

#### **Media Types:**

1. **Twisted Pair Cables:**
   * **Categories:** Cat5e, Cat6, Cat6a (supports Gigabit Ethernet).
   * **Usage:** Commonly used in LAN environments.
2. **Fiber Optic Cables:**
   * **Types:** Single-mode (long-distance) and multi-mode (short-distance).
   * **Usage:** High-speed backbone connections between switches.

#### **Connectors and Ports:**

1. **RJ45 Connectors:**
   * Used with twisted pair cables for Ethernet connections.
2. **LC/SC Connectors:**
   * Used with fiber optic cables for high-speed links.
3. **Switch Ports:**
   * **Ethernet Ports:** For copper-based twisted-pair connections.
   * **SFP/SFP+ Ports:** For modular fiber connections.

#### **Special Cables:**

* **Straight-Through Cable:** Connects devices like a PC to a switch.
* **Crossover Cable:** Connects two switches directly.
* **Fiber Cables:** Connect switches over long distances.

### 9. **Define Network Devices and Hosts**

#### **Network Devices:**

* Hardware used to manage, direct, or facilitate communication within a network.
* Examples: Routers, switches, firewalls, modems, and access points.

#### **Hosts:**

* Devices that communicate over the network, either consuming or providing resources.
* Examples: Computers, servers, smartphones, IoT devices.