Module -7: Network fundamentals

**(1)Which of the following messages in the DHCP**

process are broadcast? (Choose two)

A. Request C. Discover

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

B. permit tcp any any eq 80

**(3)Explain Network Topologies.**

A network topology is the physical or logical arrangement of devices (nodes) and how they are connected to each other in a network. It defines the layout pattern of connections between computers, switches, routers, and other devices.

**Types of Network Topologies**

1. Bus Topology
   * All devices are connected to a single central cable called the bus.
   * Data travels in both directions along the bus.
   * Pros: Easy to set up, uses less cable.
   * Cons: If the bus cable fails, the whole network goes down. Performance decreases as more devices are added.
2. Star Topology
   * All devices connect individually to a central device (like a switch or hub).
   * The central device manages all data transmission.
   * Pros: Easy to manage and troubleshoot, failure of one device doesn’t affect others.
   * Cons: If the central device fails, the whole network is down.
3. Ring Topology
   * Each device connects to exactly two other devices, forming a circular path.
   * Data travels in one direction (or sometimes both directions in a dual ring).
   * Pros: Can perform better than bus under heavy load.
   * Cons: Failure of one device or connection breaks the loop and can disrupt the network.
4. Mesh Topology
   * Every device connects directly to every other device.
   * Provides multiple paths for data to travel.
   * Pros: Highly reliable and fault-tolerant.
   * Cons: Very expensive and complex to set up due to many connections.
5. Tree Topology
   * A combination of star and bus topologies.
   * Groups of star-configured networks are connected to a linear bus backbone.
   * Pros: Scalable and easy to manage.
   * Cons: If the backbone fails, segments can become isolated.
6. Hybrid Topology
   * A combination of two or more different types of topologies.
   * Designed to suit the needs of a specific network.

**(4)Explain TCP/IP Networking Model**

The TCP/IP model is a conceptual framework used to understand and implement network protocols and communication over the internet and other networks. It defines how data should be transmitted between devices.

Layers of the TCP/IP Model

The TCP/IP model has 4 layers, each with specific functions:

|  |  |  |
| --- | --- | --- |
| Layer Name | Description | Key Protocols |
| 1. Network Interface Layer (also called Link Layer) | Handles the physical transmission of data over network hardware (like Ethernet, Wi-Fi). Deals with hardware addressing (MAC addresses). | Ethernet, Wi-Fi, ARP (Address Resolution Protocol) |
| 2. Internet Layer | Responsible for addressing, packaging, and routing the data packets to the destination across multiple networks. | IP (Internet Protocol), ICMP (Internet Control Message Protocol), IGMP |
| 3. Transport Layer | Provides communication services directly to the application processes. Ensures data delivery with error checking and flow control. | TCP (Transmission Control Protocol), UDP (User Datagram Protocol) |
| 4. Application Layer | Provides network services directly to user applications. Deals with high-level protocols that enable user interaction. | HTTP, FTP, SMTP, DNS, Telnet, SSH |

**(5)Explain LAN and WAN networks**

**1. LAN (Local Area Network)**

* Definition: A LAN is a network that connects computers and devices in a small, localized area such as a home, office, or building.
* Purpose: To share resources like files, printers, and internet connections within a close proximity.
* Characteristics:
  + Usually owned and managed by a single organization or individual.
  + High data transfer speeds (e.g., Ethernet can offer 1 Gbps or more).
  + Limited geographic area, typically within a single building or campus.
* Examples:
  + An office network connecting employee computers and printers.
  + A home Wi-Fi network connecting laptops, phones, and smart devices.

**2. WAN (Wide Area Network)**

* Definition: A WAN is a network that covers a large geographic area, often connecting multiple LANs together. It can span cities, countries, or even continents.
* Purpose: To enable communication and data sharing over long distances.
* Characteristics:
  + Typically uses leased telecommunication lines or internet connections.
  + Managed by multiple organizations or service providers.
  + Slower data speeds compared to LANs, due to distance and infrastructure differences.
* Examples:
  + The Internet itself is the largest WAN.
  + A company with offices in different cities connected via a WAN.

**(6)Explain the Operation of the Switch**

A network switch is a device that connects multiple devices (like computers, printers, servers) within a LAN and uses MAC addresses to forward data only to the intended recipient device.

1. **Learning MAC Addresses**
   * When a switch receives a frame (a data packet at the Data Link Layer), it looks at the source MAC address of the frame.
   * It records this MAC address and the port it came from in its MAC address table.
   * This way, the switch “learns” which devices are connected to which ports.
2. **Forwarding Frames**
   * When the switch receives a frame, it checks the destination MAC address.
   * It looks up this address in its MAC address table.
     + If the address is found, the switch forwards the frame only to the specific port associated with that MAC address.
     + If the address is not found, the switch floods the frame to all ports except the one it came from to find the device.
3. **Filtering**
   * By forwarding frames only to the correct port, the switch reduces unnecessary traffic on other ports, improving network efficiency compared to hubs.
4. **Loop Prevention**
   * Switches often use protocols like Spanning Tree Protocol to prevent loops in the network, which can cause broadcast storms.

**(7)Describe the purpose and functions of various network devices**

**1. Router**

* Purpose: Connects different networks together (e.g., a LAN to the Internet).
* Functions:
  + Routes data packets between networks based on IP addresses.
  + Determines the best path for data to travel.
  + Can provide NAT (Network Address Translation), DHCP services, and firewall protection.
  + Works mainly at the Network layer of the OSI model.

**2. Switch**

* Purpose: Connects devices within the same network .
* Functions:
  + Forwards data frames between devices based on MAC addresses.
  + Reduces collisions by creating separate collision domains for each port.
  + Operates primarily at the Data Link layer , some switches have Layer 3 capabilities.

**3. Hub**

* Purpose: Connects multiple Ethernet devices in a network segment.
* Functions:
  + Broadcasts incoming data packets to all ports (no filtering).
  + Operates at the Physical layer.
  + Less efficient and largely replaced by switches.

**4. Access Point (AP)**

* Purpose: Provides wireless connectivity to wired networks.
* Functions:
  + Allows wireless devices to connect to a wired LAN via Wi-Fi.
  + Manages wireless client connections, authentication, and security.

**5. Modem**

* Purpose: Converts digital data from a computer to analog signals for transmission over telephone lines .
* Functions:
  + Enables Internet access by connecting to ISP over DSL or cable.
  + Modulates and demodulates signals.

**6. Firewall**

* Purpose: Protects networks by controlling incoming and outgoing traffic.
* Functions:
  + Filters traffic based on predefined security rules.
  + Can block unauthorized access while allowing legitimate communication.
  + Can be hardware-based or software-based.

**7. Gateway**

* Purpose: Acts as a translator between different network protocols or architectures.
* Functions:
  + Connects networks that use different protocols .
  + Operates at various layers depending on function.

**8. Repeater**

* Purpose: Extends the range of a network by regenerating signals.
* Functions:
  + Amplifies and retransmits signals to overcome distance limitations in network cables.
  + Operates at the Physical layer.

**(7)Make list of the appropriate media, cables, ports, and connectors**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Media Type | Cable Type | Port Type | Connector Type | Typical Use |
| Copper (Twisted Pair) | Cat5e, Cat6, Cat6a | RJ-45 Ethernet port | RJ-45 connector | LAN connections (Ethernet) |
| Fiber Optic | Single-mode, Multi-mode | Fiber optic port (SFP, LC) | LC, SC, ST connectors | High-speed long-distance links |
| Coaxial Cable | RG-6, RG-58 | BNC port | BNC connector | Older networks, cable TV |
| Wireless (Wi-Fi) | N/A | Antenna port | N/A | Wireless connectivity |
| Serial | RS-232 cable | DB-9 port | DB-9 connector | Console management, legacy devices |
| USB | USB Cable (Type A/B) | USB port | USB connector | Device connection, console access |

**(8)connect switches to other**

* **Using Straight-Through Ethernet Cable:**  
  Modern switches have **Auto-MDIX** capability, so you can use a standard straight-through cable to connect the **uplink ports** or any ports between switches.
* **Using Crossover Cable:**  
  Older switches without Auto-MDIX require a **crossover cable** to connect switch ports directly.
* **Using Uplink Ports:**  
  Some switches have a dedicated **uplink port** for easy connection to other switches or routers.
* **Using Fiber Optic Links:**  
  For longer distances, switches can be connected using **fiber optic cables** through SFP (Small Form-factor Pluggable) ports.

**(9)Define Network devices and hosts**

**1. Network Devices:**  
These are hardware components that facilitate communication and connectivity within a network. They manage data traffic, routing, switching, and access control. Examples include:

* Routers
* Switches
* Hubs
* Access Points
* Firewalls
* Modems

**2. Hosts:**  
Hosts are end devices on a network that use the network to send or receive data. They usually have IP addresses and are the source or destination of network communication. Examples include:

* Computers (desktops, laptops)
* Smartphones and tablets
* Servers
* Printers
* IoT devices (smart sensors, cameras)