**1.1 Explain the Role and Function of Network Components**

**1. Question**

What are the primary functions of a **router**, and how does it differ from a Layer 2 switch?

**Answer**

* **Router Functions**:
  1. **Packet Forwarding at Layer 3** using IP addresses.
  2. **Path Selection** using routing protocols (e.g., OSPF, EIGRP, BGP).
  3. **Network Segmentation** between different IP networks or subnets.
* **Difference from L2 Switch**: A Layer 2 switch forwards based on MAC addresses and operates at the data link layer. A router uses IP addresses at Layer 3 to decide how to forward packets outside a local subnet.
* **Real-World**: Routers connect multiple networks (e.g., connecting the internal LAN to the Internet).

**2. Question**

What is the main distinction between a **Layer 2 switch** and a **Layer 3 switch**, and why might you deploy a Layer 3 switch in an enterprise network?

**Answer**

* **L2 vs. L3**:
  + **Layer 2 Switch**: Forwards frames based on MAC addresses; typically used within the same VLAN or broadcast domain.
  + **Layer 3 Switch**: Can also forward traffic based on IP addresses (routing).
* **Why Use Layer 3**:
  + **Inter-VLAN Routing**: A Layer 3 switch can route between VLANs, eliminating the need for an external router.
  + **Scalability**: Simplifies large campus designs, reducing network hops and improving performance.
* **Real-World**: Most modern enterprise “distribution” or “core” switches are Layer 3 capable for faster internal routing.

**3. Question**

Explain the role of a **next-generation firewall (NGFW)** compared to traditional firewalls, and how an **Intrusion Prevention System (IPS)** complements it.

**Answer**

* **NGFW**:
  1. Performs deep packet inspection at Layer 7 (application level).
  2. Identifies and blocks advanced threats (malware, application-based attacks).
  3. Integrates features like URL filtering, application control, and sometimes IPS.
* **IPS**:
  1. Monitors traffic for known vulnerabilities or malicious behavior and can block or quarantine in real time.
* **Real-World**: While a NGFW can filter based on app/user identity, an IPS actively inspects traffic for intrusion signatures, giving layered security in critical environments (e.g., data centers).

**4. Question**

What are **access points (APs)**, and how do they typically connect to the rest of the network?

**Answer**

* **Function**: Provide wireless access (Wi-Fi) by bridging wireless clients onto a wired LAN.
* **Connection**: Usually connect via Ethernet to a switch port—often on a VLAN dedicated for wireless traffic or, in large deployments, a trunk for multiple WLANs (SSID-to-VLAN mapping).
* **Real-World**: Organizations place APs in strategic locations (ceilings, offices) to ensure coverage. They may be autonomous or lightweight (controller-based).

**5. Question**

How do **Cisco DNA Center** and a **Wireless LAN Controller (WLC)** differ in their roles as “controllers” in a network?

**Answer**

* **Cisco DNA Center**:
  1. A centralized management and automation platform for the entire enterprise network (campus, WAN, etc.).
  2. Provides policy-based automation, assurance, and analytics.
* **WLC**:
  1. Specifically manages **wireless access points**—handling configurations, roaming, and radio frequency (RF) management.
* **Real-World**: Large enterprises may use DNA Center for end-to-end automation (switches, routers, wireless) while the WLC is still the direct “brain” for APs.

**6. Question**

Define **endpoints** in a network, and provide examples of how they interact with network infrastructure.

**Answer**

* **Endpoints**: Devices at the edge of a network that directly use or generate data (e.g., PCs, smartphones, printers, IoT sensors).
* **Interaction**: Endpoints connect via wired or wireless interfaces to access network resources (servers, cloud services) and rely on switches/routers for connectivity.
* **Real-World**: An employee’s laptop is an endpoint that authenticates via an access switch, obtains IP settings from DHCP, and reaches corporate apps through routers.

**7. Question**

Why are **servers** a critical network component, and what role do they play in centralized services?

**Answer**

* **Servers**: High-performance computers hosting services, applications, databases, or storage accessible by endpoints.
* **Centralized Services**: Email (Exchange), file storage, web hosting, authentication (Active Directory), etc.
* **Real-World**: In a typical corporate environment, servers might reside in a data center. Endpoints request services from these servers across routed or switched networks.

**8. Question**

What is **Power over Ethernet (PoE)**, and how does it simplify network deployments of certain devices?

**Answer**

* **PoE**: Supplies electrical power over standard Ethernet cables.
* **Benefits**:
  1. Eliminates separate power cabling for devices like IP phones, APs, and cameras.
  2. Centralized UPS backup at the switch ensures continuous power during outages.
* **Real-World**: PoE drastically simplifies installation for VoIP phones in large offices, as you only need a single Ethernet drop for both data and power.

**1.2 Describe Characteristics of Network Topology Architectures**

**9. Question**

How does a **two-tier** (collapsed core) architecture differ from a **three-tier** architecture in a campus network design?

**Answer**

* **Two-Tier** (Collapsed Core):
  1. **Access Layer** connects endpoints.
  2. **Distribution/Core** layers are combined into a single layer for simplicity and cost savings.
* **Three-Tier**:
  1. **Access**
  2. **Distribution**
  3. **Core** (high-speed backbone)
* **Real-World**: Smaller campuses often use two-tier for fewer switches, while larger ones need a dedicated core for high capacity and redundancy.

**10. Question**

What are the primary layers in a **three-tier** architecture, and what is the general role of each?

**Answer**

1. **Access Layer**: Directly connects users and endpoint devices (PCs, phones).
2. **Distribution Layer**: Aggregates access layer switches, often handles inter-VLAN routing and policy enforcement.
3. **Core Layer**: High-speed backbone linking distribution layers; optimizes fast switching and high availability.

* **Real-World**: A large university might place distribution switches in each building or floor and tie them into a robust, redundant core for campus-wide services.

**11. Question**

What is **spine-leaf** topology, and in which type of network is it commonly deployed?

**Answer**

* **Definition**: A data center architecture where every **leaf switch** connects to every **spine switch**.
* **Common Deployment**: Modern data centers. It minimizes latency and ensures consistent bandwidth between any two leaves.
* **Real-World**: Cloud service providers use spine-leaf to scale out horizontally, supporting large east-west traffic in virtualized or containerized environments.

**12. Question**

Describe how **WAN (Wide Area Network)** topologies differ from LAN topologies, and give an example of a common WAN technology.

**Answer**

* **WAN Topology**: Connects geographically dispersed sites over longer distances (leased lines, MPLS, broadband, etc.). Often uses provider-based infrastructure.
* **Common WAN Technology**:
  + **MPLS**: Multi-Protocol Label Switching used by enterprises for predictable performance.
  + **SD-WAN**: Software-defined WAN leveraging multiple connection types (Internet, LTE, MPLS) with centralized management.
* **Real-World**: A business with offices in multiple cities uses a WAN to interconnect each branch to the headquarters.

**13. Question**

What considerations come into play for a **SOHO (Small Office/Home Office)** network design compared to a larger enterprise environment?

**Answer**

* **SOHO Considerations**:
  1. **Equipment Simplicity**: Often a single router/firewall combo for Internet, NAT, Wi-Fi, and basic switch ports.
  2. **Cost Sensitivity**: Fewer, cheaper devices due to smaller scale.
  3. **Minimal Redundancy**: Usually no budget for dedicated backup links or core switches.
* **Real-World**: Home offices typically rely on ISP-provided modems/routers with integrated Wi-Fi.

**14. Question**

How do **on-premise** data centers differ from **cloud** deployments, and why might an organization choose a hybrid approach?

**Answer**

* **On-Premise**:
  + Organization owns and manages the physical servers, networking, security.
  + Greater control, but higher upfront costs and ongoing maintenance.
* **Cloud**:
  + Resources hosted by a provider (AWS, Azure) with on-demand scaling.
  + Reduced hardware overhead, but less direct control.
* **Hybrid**:
  + Mix on-prem servers for sensitive data while leveraging cloud for elasticity and cost savings.
* **Real-World**: A retail company may keep payment processing on-prem for compliance yet use cloud for customer-facing websites.

**1.3 Compare Physical Interface and Cabling Types**

**15. Question**

What is the difference between **single-mode fiber (SMF)** and **multimode fiber (MMF)** in terms of distance and use cases?

**Answer**

* **Single-Mode Fiber**:
  1. Uses a smaller core (typically 9 µm).
  2. Supports longer distances (tens of kilometers).
  3. Typically used in MAN/WAN or large campus backbones.
* **Multimode Fiber**:
  1. Larger core (50/62.5 µm).
  2. Shorter distances (up to a few hundred meters).
  3. Used within a building or small campus runs (server rooms).
* **Real-World**: Enterprises use MMF for switch-to-switch links in the same building, SMF for connecting distant buildings or data centers.

**16. Question**

What are some advantages and disadvantages of **copper (twisted-pair) cabling** compared to fiber?

**Answer**

* **Advantages (Copper)**:
  1. **Lower Cost**: Generally cheaper than fiber for short runs.
  2. **Ease of Installation**: Tools and connectors more common.
* **Disadvantages**:
  1. **Distance Limitations**: Typically max 100 meters for Ethernet.
  2. **EMI Susceptibility**: Prone to electromagnetic interference.
  3. **Lower Bandwidth Potential** at long distances.
* **Real-World**: Copper is standard for office desktops (Cat5e/Cat6). Fiber is used for backbone or high-speed/long-distance links.

**17. Question**

Explain the difference between **Ethernet shared media** (hub-based) and **point-to-point** (switch-based) connections.

**Answer**

* **Shared Media**:
  + Older technology with hubs where all devices share the same collision domain.
  + Only one device can transmit at a time, leading to collisions.
* **Point-to-Point**:
  + Each switch port connects directly to a single device.
  + Full-duplex possible, no collisions.
* **Real-World**: Modern networks use switches in point-to-point configurations, virtually eliminating collisions.

**18. Question**

Why do large data centers often prefer **fiber** over copper cables for switch-to-switch connections?

**Answer**

1. **Higher Bandwidth**: 10 Gbps, 25 Gbps, 40 Gbps, and beyond are more feasible on fiber.
2. **Longer Distance**: Data center rows can be hundreds of meters long. Fiber supports these lengths at high speeds.
3. **Reduced Interference**: Fiber is immune to electromagnetic interference from large machinery or power supplies.

* **Real-World**: Spine-leaf architectures heavily rely on fiber for top-of-rack to spine connections at 10/25/40/100 Gbps.

**1.4 Identify Interface and Cable Issues**

**19. Question**

What are some common indicators of a **cable mismatch** or **physical media problem** on an Ethernet interface?

**Answer**

* **Indicators**:
  1. **CRC Errors** or input errors in show interfaces output.
  2. **Late Collisions** or runts/giants.
  3. **Interface Flapping** (going up/down frequently).
* **Real-World**: A poorly crimped RJ-45 or using a Cat5 cable for a 10G connection can cause errors and slow performance.

**20. Question**

How does a **speed or duplex mismatch** manifest on a switch port, and how do you typically resolve it?

**Answer**

* **Symptoms**:
  1. Excessive collisions, CRC errors.
  2. Link up but very poor throughput.
* **Resolution**:
  1. Ensure both ends are set to **auto-negotiate** or manually configured to the **same speed/duplex**.
  2. Check the show interface status for mismatch clues.
* **Real-World**: A classic cause of “slow network” calls—particularly if one end is forced Full duplex and the other is Auto (which falls back to Half).

**21. Question**

What is a **collision** in Ethernet, and why are they rare in modern **full-duplex** switched networks?

**Answer**

* **Collision**: When two devices transmit simultaneously on the same shared medium, corrupting frames.
* **Modern Full-Duplex**: Each port has a dedicated channel for send/receive with no shared medium. Hence, collisions don’t occur.
* **Real-World**: Collisions were common with hubs or half-duplex setups. Today, seeing collisions is a sign of misconfiguration or outdated equipment.

**1.5 Compare TCP to UDP**

**22. Question**

How does **TCP** provide reliable data delivery, and in what scenarios is it preferred?

**Answer**

* **Reliability Mechanisms**:
  1. **Three-Way Handshake** to establish a connection.
  2. **Sequence/Acknowledgments** to ensure every segment arrives.
  3. **Retransmissions** if packets are lost.
* **Preferred Scenarios**: File transfers (FTP), web browsing (HTTP), email (SMTP) where data integrity is critical.
* **Real-World**: A user downloading a software update relies on TCP to ensure the file is correctly received without corruption.

**23. Question**

What are the key differences between **TCP** and **UDP** in terms of overhead and use cases?

**Answer**

* **TCP**: Connection-oriented, reliable, more overhead (handshakes, acknowledgments).
* **UDP**: Connectionless, best-effort delivery, minimal overhead.
* **Use Cases (UDP)**: Real-time streaming, voice/video calls, DNS queries—where speed matters more than guaranteed packet delivery.
* **Real-World**: VoIP uses UDP because even small delays from re-transmission degrade call quality.

**24. Question**

Give a real-world example where **UDP** is favored over **TCP** due to performance considerations.

**Answer**

* **Example**: Live video streaming platforms (e.g., Zoom, YouTube Live).
* **Reason**: Missing a frame is less harmful than delaying the stream. UDP avoids the overhead of TCP’s retransmissions, reducing latency.
* **Real-World**: Time-sensitive data (like voice or video) benefits from fast delivery over guaranteed delivery.

**1.6 Configure and Verify IPv4 Addressing and Subnetting**

**25. Question**

Explain the concept of an **IPv4 subnet mask**, and how does it help a router determine the network portion of an address?

**Answer**

* **Subnet Mask**: A binary pattern where consecutive 1 bits mark the network portion; 0 bits mark the host portion.
* **Function**: Allows devices/routers to separate an IP address into **network** and **host** segments, guiding routing decisions.
* **Real-World**: 255.255.255.0 (/24) means the first 24 bits are network, so an IP like 192.168.1.10 belongs to network 192.168.1.0.

**26. Question**

What is the primary purpose of **subnetting**, and how can it enhance network efficiency?

**Answer**

* **Primary Purpose**: Break a large IP network into smaller, more manageable sub-networks, each with its own broadcast domain.
* **Enhancement**:
  1. **Reduced Broadcast Traffic** within each subnet.
  2. **Better IP Address Utilization**: Allows right-sizing subnets for departments.
* **Real-World**: A company with 200 users can create a /27 for specific teams or VLANs, avoiding wasted addresses.

**27. Question**

If you have the subnet **192.168.10.0/26**, how many usable host IP addresses are available, and what is the broadcast address?

**Answer**

* **/26**: Subnet mask is 255.255.255.192 → 64 addresses per subnet.
* **Usable Hosts**: 64 total addresses − 2 (network + broadcast) = 62 usable.
* **Broadcast Address**: For **192.168.10.0/26**, the range is 192.168.10.0–192.168.10.63, so broadcast is **192.168.10.63**.
* **Real-World**: This subnet is commonly used for a small LAN segment with up to 62 devices.

**28. Question**

How would you verify an interface’s **IPv4 address** and **subnet mask** on a Cisco router or switch?

**Answer**

* **Commands**:
  1. show ip interface brief – Shows assigned addresses and status but not the mask in detail.
  2. show running-config – Lists configured IP/mask on interfaces.
  3. show ip interface <interface> – Displays detailed interface info, including IP, mask, encapsulation.
* **Real-World**: If a device is unreachable, checking IP configuration is a first step to confirm correct address/mask assignment.

**1.7 Describe Private IPv4 Addressing**

**29. Question**

What are the **private IPv4 address ranges**, and why are they commonly used in LAN environments?

**Answer**

* **Ranges**:
  1. 10.0.0.0 – 10.255.255.255 (10/8)
  2. 172.16.0.0 – 172.31.255.255 (172.16/12)
  3. 192.168.0.0 – 192.168.255.255 (192.168/16)
* **Common Usage**:
  1. **Non-routable on the public internet**, used internally with NAT at the perimeter for Internet access.
  2. Avoids IP address depletion of public space.
* **Real-World**: Most home routers default to 192.168.x.x subnets for local networks.

**30. Question**

Explain how **NAT** (Network Address Translation) allows devices with private IPs to access the internet.

**Answer**

* **NAT**: Translates private source IP addresses to a public IP on the router/firewall’s external interface.
* **Process**: Outbound packets appear from the router’s public IP, inbound responses get translated back.
* **Real-World**: This is how most home/office networks share a single ISP-assigned IP with multiple private devices.

**1.8 Configure and Verify IPv6 Addressing and Prefix**

**31. Question**

What is the structure of a typical **IPv6 address**, and how is the prefix length represented?

**Answer**

* **Structure**: 128-bit address often written in eight 16-bit hextets (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
* **Prefix Length**: Uses CIDR notation like /64 to indicate the network portion.
* **Real-World**: IPv6 eliminates the exhaustion problem of IPv4, providing a vastly larger address space.

**32. Question**

How do you **manually configure** an IPv6 address on a Cisco router interface?

**Answer**

plaintext

Copy

Router(config)# interface GigabitEthernet0/0

Router(config-if)# ipv6 address 2001:db8:1:100::1/64

Router(config-if)# no shutdown

* **Verification**: show ipv6 interface brief displays assigned IPv6 addresses and interface status.
* **Real-World**: Important for labs or environments not using auto-configuration (SLAAC/DHCPv6).

**33. Question**

What steps do you use to verify your IPv6 settings on a Windows client, and how do you confirm connectivity?

**Answer**

1. **Check IP**: Open command prompt and run ipconfig /all to see the assigned IPv6 address, prefix, gateway.
2. **Ping**: Use ping -6 <IPv6 address> to test connectivity to a local or remote IPv6 host.
3. **Traceroute**: On Windows, tracert -6 <IPv6 address> for route verification.

* **Real-World**: If a Windows PC can’t reach an IPv6 resource, verifying the assigned address and default gateway is the first troubleshooting step.

**1.9 Describe IPv6 Address Types**

**34. Question**

What are **global unicast** addresses, and how do they compare to private IPv4 addresses?

**Answer**

* **Global Unicast**: Publicly routable IPv6 addresses akin to public IPv4 addresses. Typically start with **2000::/3**.
* **Comparison**: No direct analog to private IPv4 subnets because IPv6 has unique local addresses, but global unicast addresses are meant for internet or large-scale usage.
* **Real-World**: An ISP assigns a /48 or /56 global prefix to an organization for their IPv6-enabled network.

**35. Question**

Define **unique local** and **link-local** IPv6 addresses and their scope of usage.

**Answer**

* **Unique Local** (fc00::/7):
  + Non-routable on the internet, used similarly to private IPv4 inside an organization.
  + Provide local addressing but unique across multiple sites (if carefully assigned).
* **Link-Local** (fe80::/10):
  + Valid only on a single link; typically auto-configured.
  + Used for neighbor discovery and within the local broadcast domain.
* **Real-World**: Routers rely on link-local addresses for routing protocols (like OSPFv3), while unique local addresses are for internal global uniqueness without going public.

**36. Question**

What is an **anycast** IPv6 address, and how might it be used in a distributed service architecture?

**Answer**

* **Anycast**: Assigning the same IPv6 address to multiple interfaces (often on different servers/nodes).
* **Usage**: The network routes a client’s request to the **nearest** (by routing metric) instance.
* **Real-World**: CDN providers or DNS root servers use anycast to direct users to geographically closer servers, reducing latency.

**1.9.d Modified EUI-64**

**37. Question**

How does **Modified EUI-64** generate an IPv6 interface identifier, and why might you disable it in favor of privacy extensions?

**Answer**

* **EUI-64**: Takes a 48-bit MAC address, inserts FFFE in the middle, and flips the 7th bit to create a 64-bit interface ID.
* **Reasons to Disable**:
  1. **Privacy**: The device’s MAC can be inferred from the IPv6 address, allowing potential tracking.
  2. **Privacy Extensions**: Create randomized interface IDs, improving anonymity.
* **Real-World**: Modern OSes often default to privacy addresses to prevent tracking across networks.

**1.10 Verify IP Parameters for Client OS (Windows, Mac OS, Linux)**

**38. Question**

Which commands or tools would you use on a **Windows** machine to verify and troubleshoot IP settings?

**Answer**

1. **ipconfig** – Displays IP, subnet, default gateway.
2. **ping**, **tracert** – Tests connectivity.
3. **nslookup** – DNS resolution checks.
4. **route print** – Shows local routing table.

* **Real-World**: Common first step in helpdesk calls: “Open cmd, type ipconfig /all,” verifying if the client has the correct address.

**39. Question**

On a **Linux** system, how would you view and manage network interfaces and IP configurations?

**Answer**

* **Commands**:
  1. ip addr show or ifconfig (older) to list interfaces and IPs.
  2. ip route show to view the routing table.
  3. Configuration files vary by distro (e.g., /etc/netplan on Ubuntu or /etc/sysconfig/network-scripts on CentOS).
* **Real-World**: System administrators commonly script changes to network configs for server deployments, using ip commands or editing config files directly.

**1.11 Describe Wireless Principles**

**40. Question**

Why are **nonoverlapping Wi-Fi channels** important in the 2.4 GHz band, and which channels in the U.S. are typically used to avoid overlap?

**Answer**

* **Importance**: Minimizes co-channel interference; multiple APs on overlapping channels degrade performance.
* **2.4 GHz Nonoverlapping**: Channels **1, 6, and 11** in North America.
* **Real-World**: Small offices often use a single AP on channel 1, but larger ones must plan channel usage carefully to prevent coverage overlap and interference.

**41. Question**

What is an **SSID**, and how can multiple SSIDs be mapped to different VLANs in an enterprise deployment?

**Answer**

* **SSID (Service Set Identifier)**: The Wi-Fi network name broadcast by an AP.
* **Mapping**:
  + Each SSID can associate with a specific VLAN ID on the WLC or AP.
  + E.g., “Corporate” → VLAN 10, “Guest” → VLAN 20.
* **Real-World**: Allows separation of guest traffic from internal corporate traffic while still sharing physical AP hardware.

**42. Question**

Explain what **RF (Radio Frequency)** is in the context of Wi-Fi, and how environmental factors can impact signal quality.

**Answer**

* **RF**: Electromagnetic waves used by wireless devices (2.4 GHz, 5 GHz, 6 GHz) for data communication.
* **Environmental Factors**:
  1. Physical obstacles (walls, metal).
  2. Interference (microwaves, Bluetooth, neighboring networks).
  3. Signal attenuation over distance.
* **Real-World**: A dense office with thick concrete walls requires careful AP placement or additional APs to maintain adequate RF coverage.

**43. Question**

How do **encryption protocols** like WPA2 and WPA3 protect wireless networks, and why is open (unencrypted) Wi-Fi discouraged?

**Answer**

* **WPA2/WPA3**: Uses AES-based encryption (WPA2-PSK or 802.1X) to secure data in transit, preventing eavesdropping. WPA3 adds stronger key management and forward secrecy.
* **Open Wi-Fi**: Traffic is unencrypted; attackers can sniff sensitive data or perform man-in-the-middle attacks.
* **Real-World**: Corporate and public hotspots should use at least WPA2 encryption to protect users from basic sniffing or hijacking.

**1.12 Explain Virtualization Fundamentals (Server Virtualization, Containers, and VRFs)**

**44. Question**

What is **server virtualization**, and how has it transformed data center operations?

**Answer**

* **Definition**: Abstracting physical hardware into multiple virtual machines (VMs) running on a hypervisor (e.g., VMware, Hyper-V).
* **Transformation**:
  1. **Increased Hardware Utilization**: Multiple VMs share a single server.
  2. **Flexibility**: Easier to provision, migrate, or scale VMs.
  3. **Cost Savings**: Fewer physical servers needed.
* **Real-World**: Enterprises commonly run hundreds of VMs on fewer physical servers, reducing power/cooling costs.

**45. Question**

How do **containers** differ from virtual machines, and in what situations might an organization prefer containers?

**Answer**

* **Containers**: Package an application and its dependencies in a lightweight unit sharing the host OS kernel. (e.g., Docker)
* **Differences**:
  + **Less overhead** than VMs, faster spin-up.
  + **Share the OS kernel** rather than running separate OS instances.
* **Use Cases**: Microservices architectures, dev/test environments, continuous integration/continuous deployment (CI/CD).
* **Real-World**: Cloud-native apps at scale often use container orchestration (Kubernetes) for agile deployment.

**46. Question**

What are **VRFs (Virtual Routing and Forwarding)** on network devices, and how do they relate to virtualization at Layer 3?

**Answer**

* **VRF**: A logical instance of a routing table on a single physical router, keeping traffic separated as if on different routers.
* **Layer 3 Virtualization**: Multiple customers or departments can share one router with isolated routing domains.
* **Real-World**: Service providers use VRFs to host multiple customer networks on one physical router. Enterprises may use VRFs for segregating internal business units.

**1.13 Describe Switching Concepts**

**47. Question**

What is **MAC learning**, and why do switches need to keep a **MAC address table**?

**Answer**

* **MAC Learning**: A switch listens to source MAC addresses in incoming frames on each port to build a table of **which MAC is reachable on which port**.
* **MAC Address Table**: Maps MAC addresses to switch ports/VLANs, enabling the switch to forward frames only to the correct port (unicast).
* **Real-World**: This process reduces broadcast traffic and prevents collisions, essential for efficient Layer 2 operations.

**48. Question**

How does **frame switching** occur on a switch after it learns the MAC addresses?

**Answer**

1. **Receive Frame** on a port, read the destination MAC.
2. Look up the **MAC address table** to see which port is associated with that MAC.
3. **Forward** the frame out that specific port (if found).
4. If not in the table, **flood** the frame out all ports in the VLAN except the incoming port.

* **Real-World**: Speeds up local traffic by only sending frames where needed, not flooding the entire network.

**49. Question**

What is **frame flooding**, and under which conditions does a switch flood a frame?

**Answer**

* **Frame Flooding**: When the switch sends an incoming frame out all ports (in the same VLAN) except the port it arrived on.
* **Conditions**:
  1. **Unknown Unicast**: Destination MAC not in the table.
  2. **Broadcast**: MAC address of FF:FF:FF:FF:FF:FF.
  3. **Multicast** (depending on switch IGMP/MLD config).
* **Real-World**: Flooding ensures that if the destination is unknown, the frame still reaches it. Once the destination replies, the switch learns the MAC port.

**50. Question**

What causes **MAC address table aging**, and why is it beneficial in a dynamic network?

**Answer**

* **Cause**: After a configured timeout (e.g., 300 seconds), if no frames are seen from a MAC, the switch removes that entry from its table.
* **Benefit**: Frees up table space and adapts to changes (devices moving ports, going offline).
* **Real-World**: Without aging, the table could fill up with stale entries, leading to incorrect forwarding or table overflow.