Q8) Use Linux to view the MAC address table of a switch (if using a Linux-based network switch). Use the bridge or ip link commands to inspect the MAC table and demonstrate a basic switch's operation:

Observations & Explanations for Viewing the MAC Address Table on a Linux-Based Switch:

Observation	Explanation
MAC Table Entries Appear Per Interface	Running `bridge fdb show` lists MAC addresses with associated interfaces. Each MAC belongs to a connected device, and `dev ethX` shows which port learned it. The "master br0" confirms it's part of a bridge (switch).
MAC Addresses Update Dynamically	Using `watch -n 2 bridge fdb show`, MAC addresses appear/disappear in real-time. The switch learns new MAC addresses from active traffic, and inactive devices are removed after a timeout (~5 min).
Clearing the MAC Table Forces Relearning	Running `bridge fdb flush` empties the MAC table. When traffic resumes (`ping` or other activity), the switch **relearns** MACs dynamically. This confirms the switch builds its table based on actual communication.
Checking Packet Statistics	Running `ip -s link show eth0` shows RX (received) and TX (transmitted) packets. If RX is high but TX is low/zero, packets might be dropped. This helps diagnose network issues.
Verifying Forwarding with Packet Capture	Using `tcpdump -i eth0`, network frames can be captured to confirm MAC-level communication. This ensures the switch is forwarding frames correctly.

The MAC table updates dynamically as traffic flows.
Flushing the MAC table forces the switch to relearn addresses.
Packet statistics (**ip -s link show**) help identify traffic flow issues.
Using **tcpdump** confirms if Ethernet frames are correctly forwarded.