***Network Devices and Their Security Perspectives***

***Author: Vineeth M***

***Date: sep, 24***

## ***1.What is a Router***

*A* ***router*** *is a networking device that connects multiple networks and forwards data packets between them, operating at the* ***Network Layer (Layer 3) of the OSI model****. It ensures that information reaches the correct destination by examining the destination IP address of each packet. For example, when you type* [*www.google.com*](http://www.google.com/) ***in your browser, your computer sends a request divided into packets, which do not go directly to Google. Instead, they pass through a series of routers that determine the best path to the server. Routers have multiple interfaces to connect different networks and allow several devices to share an internet connection, making them one of the most common and essential devices in networking.***

***How Router Works***

*A* ***router works*** *by looking at the destination IP address on each data packet to figure out where it should go. To do this, it uses a* ***routing table****, which is like a map that shows all the possible paths to different networks. Routers connect to the internet through a modem (such as cable, fiber, or DSL) and usually have multiple ports so many devices can be connected at the same time. Most routing tables include a* ***default path*** *for sending packets, but this path may not always be the best route. There are two main types of routing tables:* ***static tables****, which are set up manually by network administrators, and* ***dynamic tables****, which update automatically based on network activity. This way, the router makes sure that data finds its way from your device to the right destination.*

***Functions of router***

* ***Forwarding:*** *Receives packets, checks their header, and sends them to the correct output port using the routing table.*
* ***Routing:*** *Determines the best path for packets to reach their destination using routing algorithms.*
* ***Network Address Translation (NAT):*** *Allows multiple devices in a private network to share a single public IP address for internet access.*
* ***Security:*** *Provides firewalls and other security features to block unauthorized access and threats.*
* ***Quality of Service (QoS):*** *Prioritizes important traffic (e.g., video calls, online games) over less critical traffic.*
* ***VPN Connectivity:*** *Enables secure remote access to the network through Virtual Private Networks.*
* ***Bandwidth Management:*** *Controls and allocates data flow to prevent congestion and ensure smooth performance.*
* ***Monitoring and Diagnostics:*** *Tracks network traffic and helps identify and fix network problems quickly.*

## ***Types of Router***

* **Wireless Routers:** Create a Wi-Fi signal for homes or offices.
* **Broadband Routers:** Connect computers and provide internet access.
* **Wired Routers:** Connect multiple devices via Ethernet cables; commonly used in schools and small offices.
* **Edge Routers:** Located at network edges, usually connect to ISPs, and manage traffic between networks.
* **Core Routers:** Operate within a network to handle large data transfers efficiently.
* **Virtual Routers:** Software-based routers running on virtual machines; flexible and scalable.
* **Portable Routers:** Provide private Wi-Fi and are designed for easy portability.

### *****Router Security Strengths*****

* *Can block unwanted traffic using* ***firewalls*** *and* ***access control lists (ACLs)****.*
* *Uses* ***NAT (Network Address Translation)*** *to hide internal devices from the internet.*
* *Supports* ***VPNs*** *for secure remote access.*
* *Can* ***segment networks****, reducing exposure to external threats.*
* *Often includes* ***traffic monitoring*** *to detect suspicious activity.*

### *****Router Security Weaknesses*****

* ***Firmware vulnerabilities*** *can be exploited if not updated regularly.*
* ***Default admin credentials*** *(like “admin/admin”) are often weak and easily guessed.*
* *Can be targeted in* ***DDoS attacks*** *that overload the router and shut down the network.*
* ***Misconfiguration*** *(wrong settings) can open security holes.*
* *Home or low-end routers may have* ***limited security features*** *compared to enterprise routers.*

***2.What is Network Hub***

*A* ***hub*** *is a simple networking device that connects multiple devices in a network, usually within a LAN. It works at the* ***Physical Layer (Layer 1)*** *of the OSI model. A hub has* ***multiple ports****, and when it receives data from one device, it* ***broadcasts the data to all connected devices*** *instead of sending it only to the intended device.*

*In simple terms, a hub acts like a* ***multi-port repeater****. It does not have a routing table, cannot filter or identify the destination of data, and all devices connected to it share the same* ***collision domain****, which can lead to network slowdowns if many devices send data at the same time. Hubs are mostly replaced by* ***switches*** *today because they are less efficient and less secure.*

### ***How a Network Hub Works***

*A* ***hub*** *is a device with multiple ports that connects several devices in a network. When one device sends data to the hub, the hub* ***broadcasts the data to all ports*** *because it cannot tell which device is the intended recipient.*

*For example, if a hub has ports A, B, C, D, and E, and device A sends data, the hub will forward that data to B, C, D, and E. If another device, like B, sends data at the same time, the data from A and B can* ***collide****, causing data loss. When a collision happens, all devices are notified, and the senders wait for a short time before trying again.*

### ***Security of a Hub***

*A hub is a very simple networking device, which means it doesn’t have many complex features that can be attacked. This is its only minor* ***strength****—hackers have fewer software features to exploit. However, the* ***weaknesses*** *of a hub make it very insecure. Hubs* ***broadcast all data to every connected device****, so anyone on the network can easily capture or sniff the traffic. They also have* ***no built-in security features*** *like firewalls, filtering, or access control, making it easy for attacks to spread. Additionally, all devices share the same collision domain, which can lead to data loss and network problems. Because of these weaknesses, hubs are considered* ***not secure*** *and are rarely used in modern networks, with switches and routers being preferred for safer communication.*

# ***3.What is a Network Switch***

*A* ***network switch*** *is a device used to divide a network into smaller segments called subnets or LAN segments. It operates at the* ***Data Link Layer (Layer 2)*** *of the OSI model and is responsible for* ***filtering and forwarding data*** *to the correct device using its MAC address. Switches have many ports, and when data arrives, the switch checks the destination address, performs some error checking, and then sends the data only to the intended device. Switches support different types of communication:* ***unicast*** *(one-to-one),* ***multicast*** *(one-to-many), and* ***broadcast*** *(one-to-all). They work in* ***full-duplex mode****, allowing devices to send and receive data simultaneously, and allocate bandwidth efficiently to each connected segment. Packet-switching techniques ensure data moves quickly and accurately from the source to the destination.*

*Switches are essential for modern networks because they improve network speed and efficiency. They provide reliable wired connections to devices like computers, printers, IoT devices, and wireless access points. Full-duplex communication helps make the best use of bandwidth, while IoT devices rely on switches to transmit data that can be used in smart systems powered by AI. Switches are also important in telecommunications, as they can handle large amounts of network traffic efficiently.*

### *****How a Network Switch Works*****

*When a device wants to send data to another device, the data first goes to the* ***switch****. The switch reads the* ***header*** *of the data packet to find the* ***MAC address*** *of the destination device and sends the data only through the port that leads to that specific device. For* ***local communication*** *within the network, the switch establishes a* ***temporary connection*** *between the sender and receiver and provides* ***full bandwidth*** *to reduce collisions. When the data needs to go to the* ***internet****, the switch forwards the data to the* ***router****. The router then reads the* ***IP address*** *and determines the best path for the data to travel outside the local network. In this way, switches manage* ***local traffic efficiently****, while routers handle* ***traffic to and from the internet****.*

***MAC Address Table***

*A MAC address table is like a short-term memory inside a network switch. It stores which device (by its MAC address) is connected to which port. When a device sends data, the switch remembers its MAC address and the port it came from. This helps the switch send data only to the right device instead of broadcasting it to everyone, which makes the network faster and safer. But since the table has limited space, if an attacker floods it with fake MAC addresses, the switch can get confused and start sending all data to every device, allowing the attacker to see the network traffic.*

***Attacks Related to Switches***

***MAC Address Flooding (CAM Table Overflow)***

***A switch normally remembers which device (MAC) is on each port using a table (the CAM* (Content Addressable Memory) *or MAC table). When it sees a frame from a device it stores the device’s MAC and the port. An attacker sends lots of frames with fake, random source MAC addresses so the table fills. When the table is full the switch can’t match destinations to ports, so it behaves like a hub and floods frames out all ports. The attacker’s machine then receives copies of other hosts’ traffic and can sniff sensitive data.***

***MAC Spoofing***

***MAC spoofing is when someone changes the hardware MAC address on their device to pretend to be another device on the same network. Attackers do this to bypass MAC-based access controls, hide their real identity, or make the switch send traffic meant for the legitimate device to the attacker’s port.***

***ARP Spoofing***

**ARP spoofing (also called ARP poisoning) happens when an attacker sends fake ARP messages on a local network. These messages falsely tell other devices that the attacker’s computer has the same IP address as another trusted device (like the router). As a result, the victim devices start sending their data to the attacker instead of the real device, allowing the attacker to intercept or modify the traffic.**

**The OS keeps using the destination IP address, but when sending on the local network it wraps the IP packet in a link-layer frame and uses the MAC address from its ARP cache. The network card looks only at the frame’s destination MAC — so if the ARP cache has been poisoned to the attacker’s MAC, the attacker receives the frame, examines the IP packet inside, and can forward it to the real router, modify it, or drop it.**

***VLAN Hopping***

***VLAN hopping is a network attack where someone on one VLAN tricks the switches to send or accept traffic for a different VLAN, letting them reach devices they shouldn’t. In simple terms: VLANs are like separate rooms in a building, and VLAN hopping is when an attacker finds a way to slip through the walls so they can listen to or send traffic in another room. Common methods are pretending to be a trunk (switch spoofing) or adding two VLAN tags to a packet (double tagging). Proper switch configuration (disable automatic trunking on user ports, tag all VLANs, use port security) prevents it.***

*****Switch spoofing*****

***A hacker can make their computer act like a switch so the real switch treats their port as a trunk port. This lets the hacker send and receive traffic from many VLANs, allowing them to see or change data they shouldn’t have access to.***

*****Double tagging*****

***Double tagging is a network attack trick where an attacker sends a packet with two VLAN tags. The first tag is removed by the first switch, and the second tag is then forwarded to a target VLAN that the attacker normally shouldn’t access. This allows the attacker to inject packets into another VLAN, potentially reaching devices or data that are supposed to be isolated.***

*****DHCP spoofing / DHCP starvation*****

*****DHCP spoofing*****

***DHCP spoofing is when an attacker sets up a fake DHCP server on the network. When clients request an IP address, they might get a response from the attacker’s server instead of the real one. This lets the attacker assign IPs, gateways, or DNS servers under their control, which can redirect traffic through the attacker’s system for sniffing, MITM, or manipulation.***

***DHCP starvation***

***DHCP starvation is when an attacker floods the real DHCP server with fake IP requests, consuming all available IP addresses. Legitimate clients then cannot get an IP, causing a denial-of-service, or they may fall back to a rogue DHCP server controlled by the attacker.***

**STP manipulation / BPDU attacks**

### **1. **Purpose of STP****

STP is used in **Ethernet networks with switches** to prevent **loops**. Loops happen when multiple paths exist between switches, and without control, frames could circulate endlessly, causing network congestion or failure.

***Functions of Switches***

* ***Filtering:*** *Checks incoming frames and decides whether to forward or drop them based on* ***MAC addresses****.*
* ***Forwarding: Sends data only to the device with the correct MAC address using the switching table.***
* ***Segmentation:*** *Divides the network into smaller parts called* ***VLANs (Virtual LANs)*** *to reduce traffic and collisions.*
* ***Full-Duplex Communication:*** *Allows devices to* ***send and receive data at the same time*** *over Ethernet.*
* ***Traffic Management:*** *Uses* ***Quality of Service (QoS)*** *to prioritize important data and share bandwidth fairly.*
* ***Communication Types:*** *Supports* ***unicast*** *(one-to-one),* ***multicast*** *(one-to-many), and* ***broadcast*** *(one-to-all) traffic.*
* ***Error Checking:*** *Uses* ***frame check sequence (FCS)*** *or other error detection methods to verify data.*
* ***Monitoring and Diagnostics:*** *Supports* ***SNMP (Simple Network Management Protocol)*** *and port monitoring to detect and fix network issues.*

### ***Security of a Network Switch***

*Network switches are more secure than hubs because they* ***send data only to the intended device*** *instead of broadcasting it to all devices. This is their main* ***strength****, as it reduces the risk of data being intercepted. Switches can also support* ***port security****,* ***VLANs*** *(to segment the network), and* ***802.1X authentication*** *to control which devices can connect. They often allow* ***traffic monitoring*** *to detect suspicious activity.*

*However, switches also have some* ***weaknesses****. They can be vulnerable to* ***MAC address spoofing****,* ***VLAN hopping****, and other attacks if not configured properly. Low-end or unmanaged switches may* ***lack advanced security features****, making them easier to exploit. Misconfigurations can also create security gaps, allowing attackers to access sensitive network data.*