# **Name: Abdurrahman Qureshi**

# **Roll No: 242466**

Practical No: 1

Date Of Performance: 08/01/2024

Aim: To Learn various devices used in networking

Lab Objectives:

To study and analyse the functionality of various networking devices (Hub, Switch, Router, NIC, Bridge, Gateway, and Firewall) and their roles in network communication.

Lab Outcomes:

Understand the working, configuration, and differences between key networking devices and their contribution to network performance and security.

Repeater:

THEORY:

Repeater is a device that receives a signal and retransmits it, use to extend the range of the signal or to overcome signal loss or use to increase the signal strength.

ADVANTAGES:

* Extends the range of a network by amplifying signals.
* Ensures data integrity over long distances by regenerating signals.
* Simple and cost-effective device for small networks.

DISADVANTAGES:

* Cannot filter traffic; broadcasts all signals.
* May amplify noise or distortions along with the signal.



Hub:

THEORY:

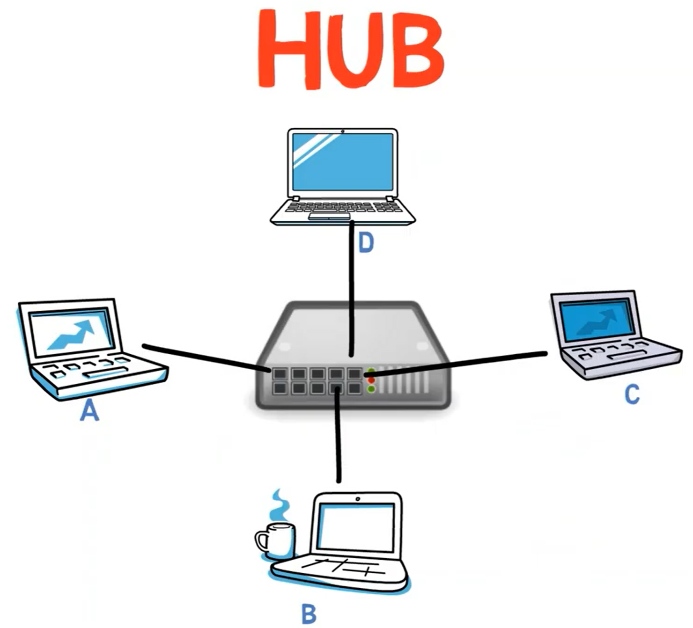
Hub is device that connects multiple devices to a network, such as a local area network (LAN). Hubs are also known as repeaters or concentrators. They act as a central point for data transmission, where each device on the network is connected directly to the hub.

ADVANTAGES:

* Simple to use and cost-effective for small networks.
* Allows multiple devices to connect in a star topology.
* Easy to expand a network by connecting multiple hubs.

DISADVANTAGES:

* Inefficient as it broadcasts data to all connected devices.
* Limited to a single collision domain, leading to network congestion.
* No data prioritization or traffic management.



Switch:

THEORY:

Switch is a device that connects multiple devices in a network, allowing them to communicate with each other. Switches manage the flow of data by transmitting packets to the intended devices.

ADVANTAGES:

* Filters and forwards data only to the intended recipient, improving efficiency.
* Operates in multiple collision domains, reducing traffic congestion.
* Supports full-duplex communication, enhancing speed and performance.

DISADVANTAGES:

* More expensive compared to hubs.
* Complex configuration in larger networks.



NIC (Network Interface Card):

THEORY:

NIC (Network Interface Card) acts as an interface between the physical layer and the data link layer of a network. It converts signals from cables or antennas into digital signals, which are then sent over the network.

ADVANTAGES:

* Enables devices to connect to a network, both wired and wireless.
* Supports high-speed data transfer rates.
* Can provide advanced features like VLAN tagging and wake-on-LAN.

DISADVANTAGES:

* Adds cost to devices without built-in network interfaces.
* Can fail and disrupt connectivity.
* Limited to the specifications of the card, requiring upgrades for higher speeds.



Router:

THEORY:

A router connects devices like computers, phones, and tablets to the internet, and can also connect multiple networks together.

ADVANTAGES:

* Connects different networks, enabling communication between them.
* Provides network security features like NAT and firewall capabilities.
* Supports multiple devices and dynamic routing protocols.

DISADVANTAGES:

* More expensive than basic networking devices.
* Configuration can be complex for inexperienced users.



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| | **Feature** |  |  | | --- | --- | --- | | **Router** | **Switch** |
| |  |  |  | | --- | --- | --- | | Purpose |  |  | | Connects multiple networks and directs data packets between them. | Connects devices within the same network and forwards data. |
| |  |  |  | | --- | --- | --- | | Layer |  |  | | Operates at the Network Layer (Layer 3) of the OSI model. | Operates at the Data Link Layer (Layer 2) or sometimes Layer 3. |
| |  |  |  | | --- | --- | --- | | Data Forwarding |  |  | | Routes data based on IP addresses. | Forwards data based on MAC addresses. |
| |  |  |  | | --- | --- | --- | | Functionality |  |  | | Provides communication between different networks (e.g., LAN to WAN). | Ensures communication between devices in the same network (e.g., LAN). |
| |  |  |  | | --- | --- | --- | | Traffic Management |  |  | | Can perform Network Address Translation (NAT) and manage IP routing. | Creates separate collision domains to reduce traffic but does not manage routing. |
| |  |  |  | | --- | --- | --- | | Security |  |  | | Offers features like firewalls and VPN support for added security. | Limited security; focuses on efficient data forwarding. |
| |  |  |  | | --- | --- | --- | | Speed |  |  | | Generally slower due to processing of complex routing decisions. | Faster within a local network as it doesn’t handle routing. |
| |  |  |  | | --- | --- | --- | | Use Case |  |  | | Used in larger networks to connect multiple subnets or provide internet access. | Used in LANs to connect computers, printers, and other devices. |
| |  |  |  | | --- | --- | --- | | Cost |  |  | | More expensive than switches due to advanced functionality. | More affordable for basic network setups. |

Bridge:

THEORY:

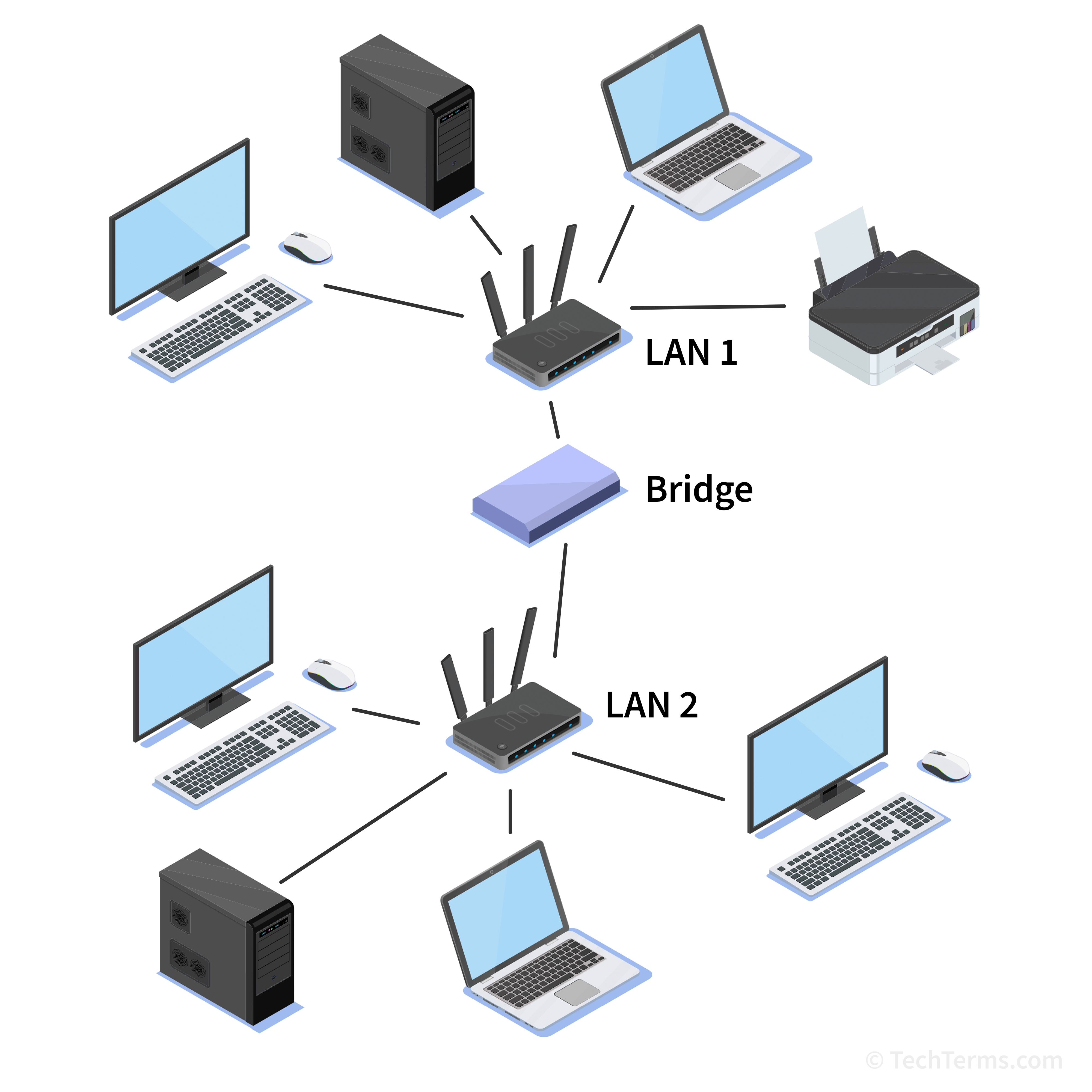
A network bridge is a device or software that connects multiple networks or network segments to create a single network. This process is called network bridging.

ADVANTAGES:

* Connects and filters traffic between two network segments.
* Reduces network congestion by dividing collision domains.
* Enhances performance by forwarding data only when necessary.

DISADVANTAGES:

* Limited scalability for large networks.
* Slower than switches for complex networks.
* Does not support routing between different network protocols.



Gateway:

THEORY:

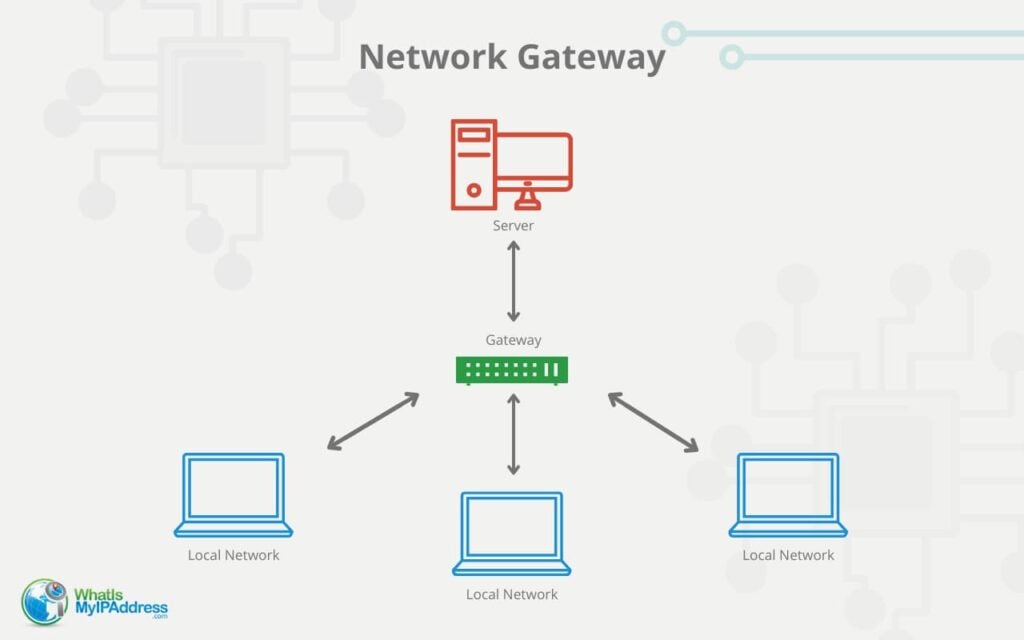
A network gateway is a device or piece of software that connects different networks by translating communication between them. Gateways are a vital part of corporate network architecture and are often located at the edge of a network.

ADVANTAGES:

* Connects networks with different protocols, enabling seamless communication.
* Translates data formats and handles protocol conversion.
* Essential for integrating disparate systems and cloud services.

Disadvantages:

* High cost and complexity of configuration.
* Potential performance bottleneck if overused.
* Dependence on gateway for communication can lead to single point of failure.



Firewall:

THEORY:

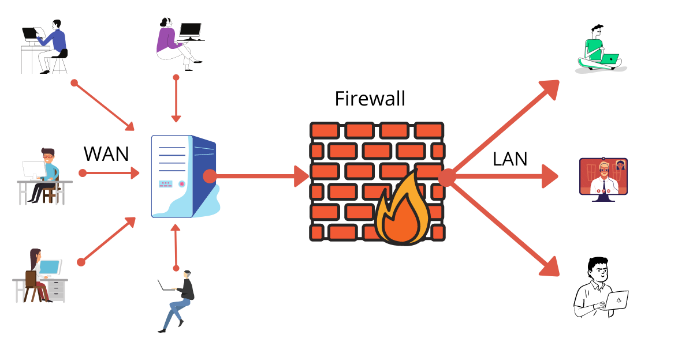
A firewall is a network security system that monitors and controls incoming and outgoing network traffic. Firewalls create a barrier between trusted and untrusted networks, such as the internet or different VLANs.

ADVANTAGES:

* Protects networks from unauthorized access and cyber threats.
* Can monitor and control incoming and outgoing traffic.
* Provides VPN support for secure remote access.

Disadvantages:

* Can be expensive, especially for advanced firewalls.
* Improper configuration can lead to security vulnerabilities.



Conclusion:

Choosing the right networking devices is key to building efficient and secure networks. The decision should match the network's size, traffic, and security needs to ensure smooth and reliable performance.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Performance  (7M) | Journal  (3M) | Lab Ethics  (2M) | Attendance  (3M) | Total  (15M) | Faculty Signature |
|  |  |  |  |  |  |