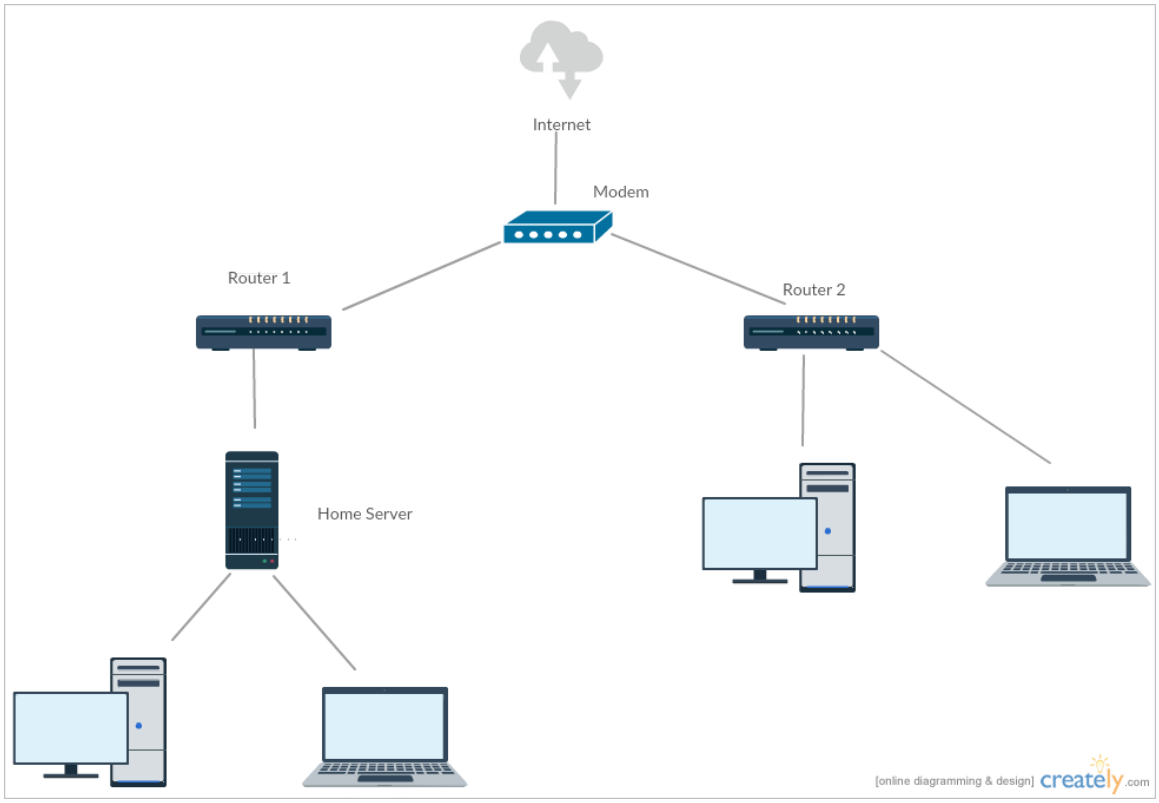
Day 04 – Computer Networking



Home Network Topology

A typical home network starts with an internet service line entering the house from the service provider. This line is connected to a modem, which converts the incoming signal into digital data that can be understood by networking devices.

The modem is connected to a router. The router plays a central role in the network by distributing the internet connection to multiple devices within the home.

Devices such as desktop computers, laptops, printers, mobile phones, tablets, and home servers connect to the router, usually through Wi-Fi.

The router allows all connected devices to access the internet simultaneously and also enables communication between devices within the same network.

This type of network topology is simple to manage, requires minimal wiring, and is suitable for daily activities such as browsing, printing, streaming, and file sharing.

IPv4 vs IPv6

IPv4 is the older version of the Internet Protocol and has been widely used since the early days of the internet.

It uses a 32-bit addressing system, written in dotted decimal format such as 192.168.1.1. Due to the limited number of available addresses, IPv4 addresses began to run out as internet usage increased.

To overcome address shortages, technologies such as Network Address Translation (NAT) are used, which add complexity to network management.

IPv6 is the newer version of the Internet Protocol, developed to address the limitations of IPv4.

It uses a 128-bit address written in hexadecimal format, allowing an extremely large number of unique IP addresses.

IPv6 removes the need for NAT and includes built-in security features, making communication more secure and efficient.

Subnetting Basics

Subnetting is the process of dividing a large network into smaller, more manageable logical networks called subnets.

By splitting a network into subnets, network traffic is reduced because devices communicate within their own subnet rather than across the entire network.

Subnetting improves security by allowing administrators to apply different access rules and policies to each subnet.

It also ensures efficient use of IP addresses by allocating addresses based on actual requirements.

For example, an office with 200 computers can be divided into two subnets of 100 devices each to improve performance and reduce congestion.

Network Address Translation (NAT)

Network Address Translation is a technique that allows multiple devices in a private network to share a single public IP address.

When data leaves the private network, the router replaces the private IP address with a public IP address.

NAT is widely used in home and office networks because public IP addresses are limited and expensive.

It also provides basic security by hiding the internal network structure from external users.

In a home network, devices such as laptops, mobile phones, and smart TVs rely on NAT for internet connectivity.

Wired Networks

Wired networks use physical cables such as Ethernet cables to connect devices.

They provide high-speed and stable connections with minimal interference.

Wired networks are generally more secure because data travels through physical cables.

These networks are commonly used in offices, schools, and computer laboratories.

Wireless Networks

Wireless networks connect devices using radio waves or Wi-Fi signals instead of cables.

They allow users to move freely within the network coverage area.

Wireless networks are easy to install and expand compared to wired networks.

They are widely used in homes, colleges, cafes, and public places.

Comparison of Wired and Wireless Networking

Wired networking uses physical cables, while wireless networking relies on Wi-Fi signals.

Wired connections are generally faster and more stable than wireless connections.

Wireless connections may experience speed variations due to distance and obstacles.

Wired networks are more secure, while wireless networks require additional security measures such as passwords.

Wireless networks provide greater mobility compared to wired networks.

Networking Technologies

Wi-Fi is a wireless networking technology that allows devices to connect to the internet without cables.

Ethernet is a wired networking technology that provides fast and reliable connectivity.

Powerline communication uses existing electrical wiring to transmit data signals.

Optical fiber communication uses light signals to transmit data at very high speeds over long distances.

Introduction to Network Security Challenges

Firewalls are security systems that monitor and control incoming and outgoing network traffic based on predefined rules.

They help prevent unauthorized access and protect internal networks from external threats.

Firewalls also support network monitoring and help detect suspicious activities.

Virtual Private Networks (VPNs) create secure, encrypted connections over the internet.

VPNs are commonly used for secure remote access and protecting sensitive data on public networks.