Routing

Cisco Certifications

- Cisco is a multinational digital communications technology best known for its networking hardware and software.
- It develops, manufactures, and sells networking equipment, software, telecommunications equipment, and other high-technology services.
- Cisco certifications are crucial in the IT industry, particularly for networking professionals, as they demonstrate expertise and enhance career prospects.

- Cisco validate skills, boost job opportunities, and often lead to higher salaries and promotions.
- Cisco certifications also cover a wide range of IT domains, including networking, security, cloud, and collaboration, making them valuable for various IT roles.

Certification Level

- **Associate -** CCNA (Cisco Certified Network Associate) : Master the essentials needed to launch a rewarding career and expand your job possibilities with the latest technologies.
- **Professional - CCNP (Cisco Certified Network Professional) :** Select core technology track (Enterprise, Datacenter, Collaboration, Security & Service Provider) and a focused concentration exam to customize professional-level certification.
- **Expert - CCIE (Cisco Certified Internetwork Expert):** This certification is accepted worldwide as the most prestigious certification in the technology industry. Core technology based on Enterprise, Datacenter, Collaboration, Security, Service Provider etc.
- **Cisco Certified Architect (CCAr)** certification is for senior network infrastructure architects who produce technical specifications for the network to support business objectives.

Role and Functions of Network Components

Core Topics

- Routers
- Layer 2 and Layer 3 switches
- Next generation firewalls and IPS
- Access Points
- Controllers (Cisco DNA Center and WLC)
- Endpoints
- Servers
- PoE

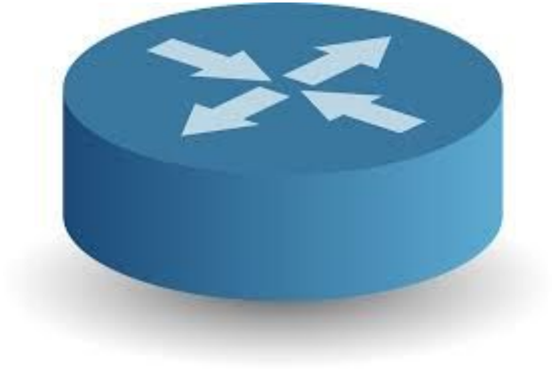
Router

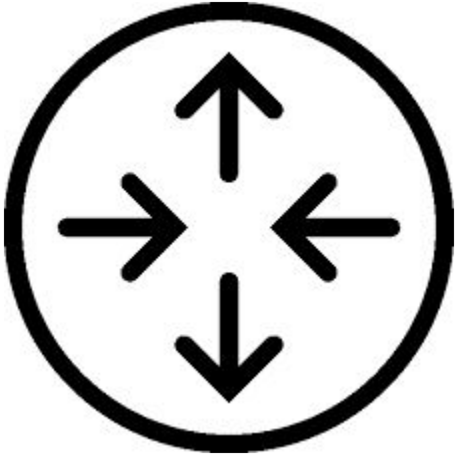
- A router is a Layer 3 network device that connects different networks together and directs data packets between them.
- It functions primarily to route data from one network to another based on their IP addresses.

Functions of a router

- A router's core function is to direct data packets between different networks, ensuring they reach their correct destination.
- It connects local networks (like a home or office network) to larger networks, such as the internet, by using routing tables and IP addresses.
- Routers manage traffic efficiently, often using protocols to choose the fastest path for data.

Network symbol of a router





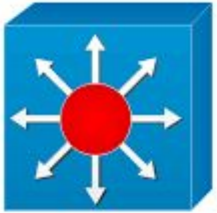
Layer 2 Switches

- A Layer 2 switch is a network device that operates at the data link layer (Layer 2) of the OSI model, using Media Access Control (MAC) addresses to forward data frames between devices within the same Local Area Network (LAN).
- A layer 2 device is a device that makes a forwarding decision based on a physical address (MAC Address)
- Layer 2 devices are Switch and Bridge.

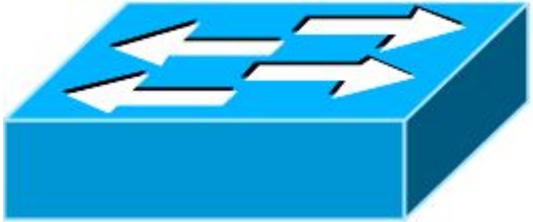
Layer 3 Switches

- A Layer 3 switch combines the functionality of a switch and a router.
- It acts as a switch to connect devices that are on the same subnet or virtual LAN.
- It can support routing protocols, inspect incoming packets, and may even make routing decisions supporting source and destination addresses.

Network symbols



Layer 3 (Multilayer Switch)



Layer 2 Switch

Next-generation firewalls

- A firewall is a network security system that acts as a barrier between a trusted internal network and untrusted external networks, such as the internet.
- It controls incoming and outgoing network traffic based on pre-defined security rules, allowing only authorized traffic while blocking unauthorized or malicious traffic.
- This helps protect the network from unauthorized access, malware, and other security threats.

- A Next-Generation Firewall (NGFW) is a network security appliance that goes beyond the capabilities of traditional firewalls to protect against a wider range of threats, including advanced cyber attacks and malware.
- NGFWS employ a combination of packet filtering, deep packet inspection, application control, and other advanced features to provide more robust security.

IPS - Intrusion Prevention System

An intrusion prevention system (IPS) is a network security tool (which can be a hardware device or software) that continuously monitors a network for malicious activity and takes action to prevent it, including reporting, blocking, or dropping it, when it does occur.

Types of IPS

- **Network-based IPS (NIPS):** Monitors traffic on the network as a whole, offering broad protection.
- **Host-based IPS (HIPS):** Monitors traffic on a specific device, providing more granular control.
- **Wireless IPS (WIPS):** Protects wireless networks by detecting and preventing unauthorized access.
- **Network Behavior Analysis (NBA):** Looks for anomalous traffic patterns and behaviors, helping to identify and prevent sophisticated attacks

Access Point

Access Point is a device that provides wireless network connectivity to devices like laptops, smartphones, and IoT devices.

It essentially acts as a bridge between wireless devices and a wired network, allowing them to connect and communicate without physical cables.

Controllers - Cisco DNA Center

- DNA Center is a comprehensive network management platform that provides automation, policy, and assurance across the entire network, including wired, wireless, and WAN solutions.
- Enables automation, configuration management, network visualization, and security features for both wired and wireless networks

Controllers - WLC (Wireless LAN Controller)

- Specifically manages wireless network access points (APs), allowing for centralized control of features like roaming, security, and policy enforcement.
- Enables features like Extended Service Set (ESS) for seamless roaming between APs, and centralized management of AP configurations, security policies, and radio frequency (RF) management.

Endpoints

- An endpoint is a device that connects to a network, providing a starting or ending point for data transfer.
- Endpoints allow users to access and utilize network resources, send and receive data, and interact with other devices and services on the network.
- **Examples:**

  Laptops, desktops, smartphones, tablets, servers, printers, IoT devices and even virtual machines.

Servers

- A server in a network is a powerful computer or device that provides services, resources, or data to other computers, known as clients, over the network. Servers are designed to manage, store, and share information, applications, or resources with multiple users or devices.
- Computer hardware, software, or even virtual machines with requisite software capabilities can act as a server.
- However, server functionalities go beyond a traditional computer.

- Servers handle complex server processes, from managing multiple user queries every second, hosting content-heavy websites, and setting up a shareable drive for network devices, to processing intensive workloads such as database transaction management that requires high computing power.

Power over Ethernet (PoE)

- Power over Ethernet (PoE) is a networking technology that allows devices to receive both power and data through a single Ethernet cable.
- This eliminates the need for separate power cords, simplifying installations and reducing clutter, especially in locations where traditional power outlets are inaccessible.

Applications of PoE

- **IP Cameras:** PoE is a standard for powering security cameras.
- **Wireless Access Points:** PoE is commonly used to power wireless access points, especially in remote locations.
- **VoIP Phones:** PoE is used to power and connect VoIP phones to the network.
- **IoT Devices:** PoE is increasingly used to power various IoT devices, including LED lighting and smart home devices.
- **Industrial Applications:** PoE is used in various industrial settings to power equipment.

Characteristics of network topology

Core Topics:

- Two-tier
- Three-tier
- Spine-leaf
- WAN
- Small office/home office (SOHO)
- On-premise and cloud

Network Topology Architecture

- Network architecture refers to the design and structure of a network, encompassing both the hardware and software components that define how a network is built, how devices are interconnected, and how data flows within the system.
- It is the blueprint for a network—defining the technologies, protocols, devices, and layout of connections that enable devices and systems to communicate effectively.

There are various types of network topology architectures.

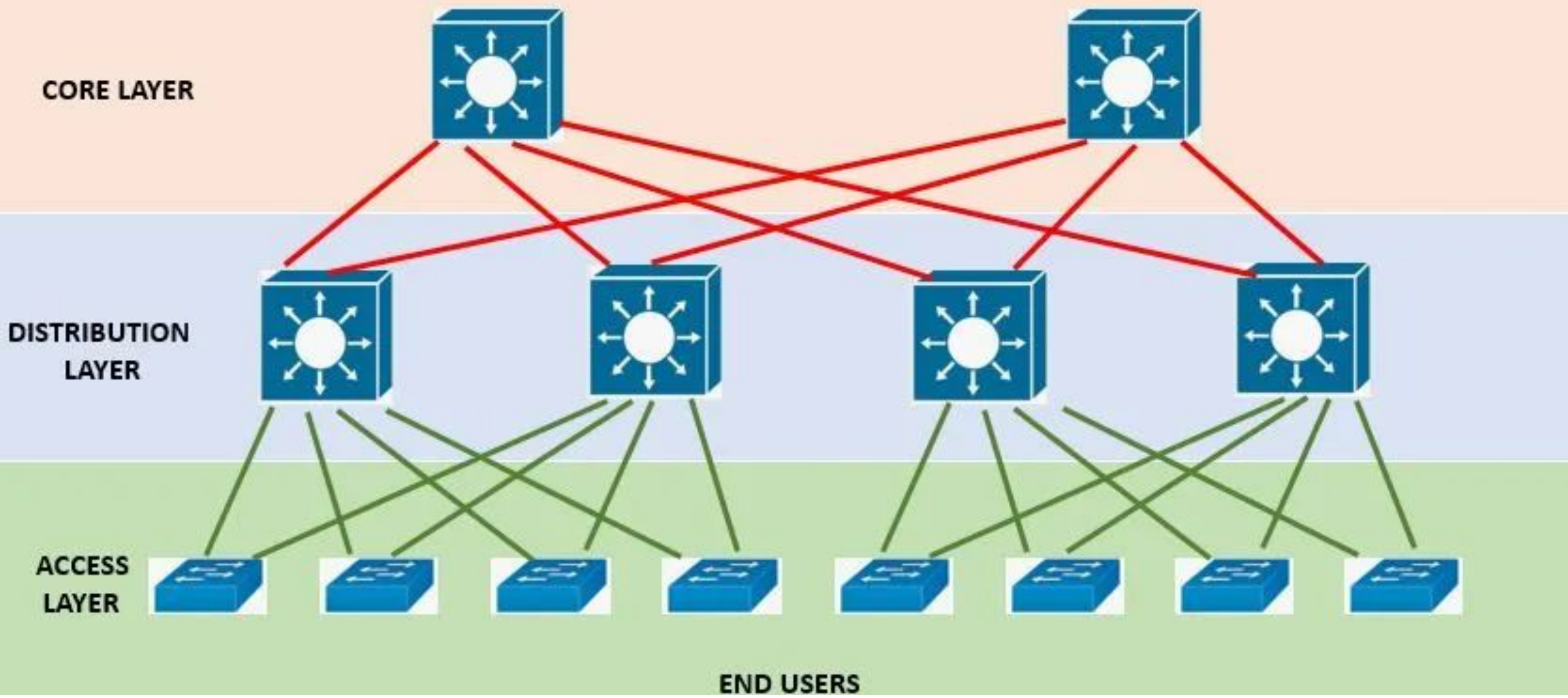
- Three-Tier Architecture
- Two-Tier Architecture
- Spine Leaf Architecture
- WAN Architecture
- SOHO Architecture
- On-Premise/Cloud Architecture

Three-Tier Architecture

The three-tier architecture consists of the following 3 layers:

- Access Layer (bottom layer)
- Distribution Layer (middle layer)
- Core Layer (Topmost layer)

THREE TIER ARCHITECTURE



Access Layer:

- The access layer is the lowest layer in the 3-tier architecture.
- It is also called as workstation layer.
- It is the closest layer to the end users.
- It consists of access switches.
- These switches connect users to the network.

Distribution Layer:

- It is the middle layer in the three-tier architecture.
- The distribution layer is also referred to as the aggregation layer.
- It performs quality of service and security work.
- It consists of multilayer switches.
- It moves the traffic from the access layer to the core layer.
- It aggregates LAN and WAN links.

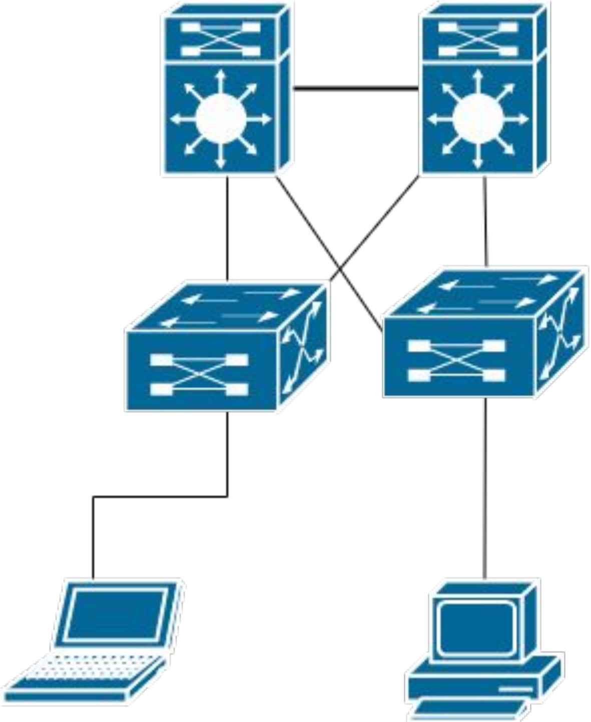
Core Layer:

- It is the topmost layer in the three-tier architecture.
- The Core layer also has another name which is the backbone layer.
- It connects distribution layer devices.
- It performs high-speed transport of traffic.
- It is reliable and fault-tolerant.

Two-Tier Architecture

- It has a **collapsed core**. It is called so because it has a blended or collapsed distribution layer and core layer.
- Therefore, the two-tier architecture consists of only 2 layers:
  1. Access Layer
  2. Collapsed Core Layer
- It is therefore simpler.

Two-Tier Architecture



Core and Distribution

Access

Spine Leaf Architecture

- It is mostly used in data centers.
- It has low latency.
- It consists of two layers:
  1. Spine Layer
  2. Leaf Layer

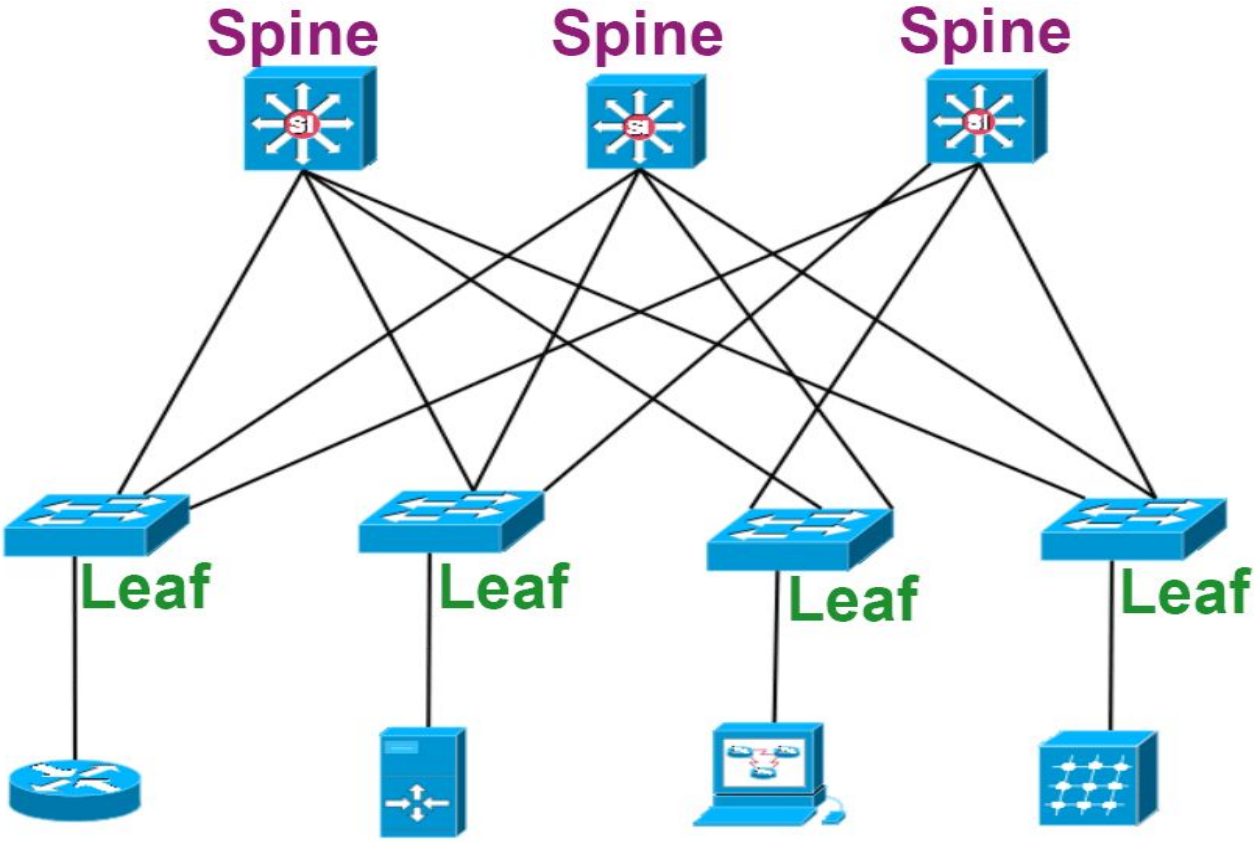
Spine Layer:

- The spine layer is the top layer.
- The Spine layer consists of very intelligent devices such as Cisco Nexus 9000 devices.
- These devices have ACI (Application Centric Infrastructure) Controller intelligence inside them.

Leaf Layer:

- It is the bottom layer in the spine leaf architecture.
- It consists of access switches.
- Each leaf is connected to every spine device.

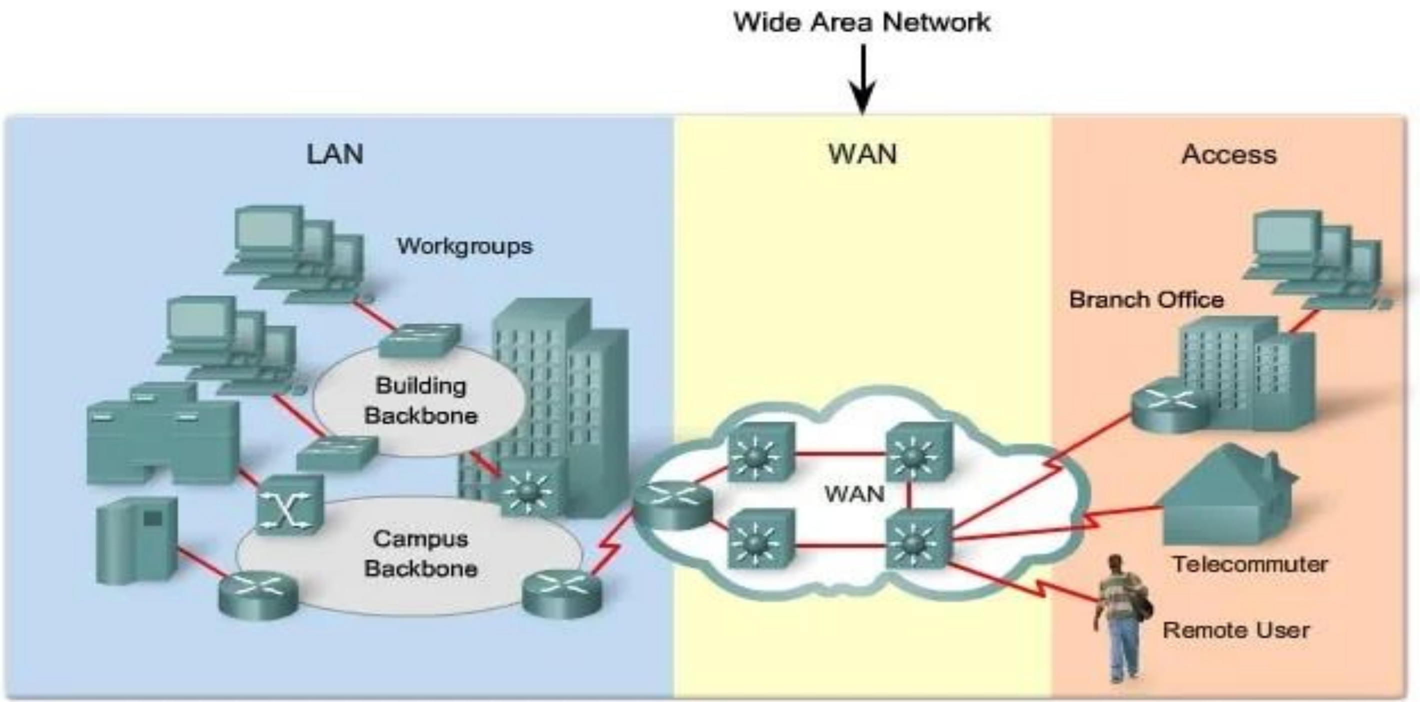
Spine-Leaf Architecture



WAN (Wide Area Network) Architecture

- WAN (Wide Area Network) architecture refers to the design, structure, and interconnection of a network that spans a large geographic area, typically across cities, countries, or even continents.
- WANs are essential for businesses, organizations, and individuals who need to access resources, share data, or communicate between geographically dispersed locations.

WAN (Wide Area Network) Architecture



What is a WAN?

Small Office/Home Office (SOHO) Architecture

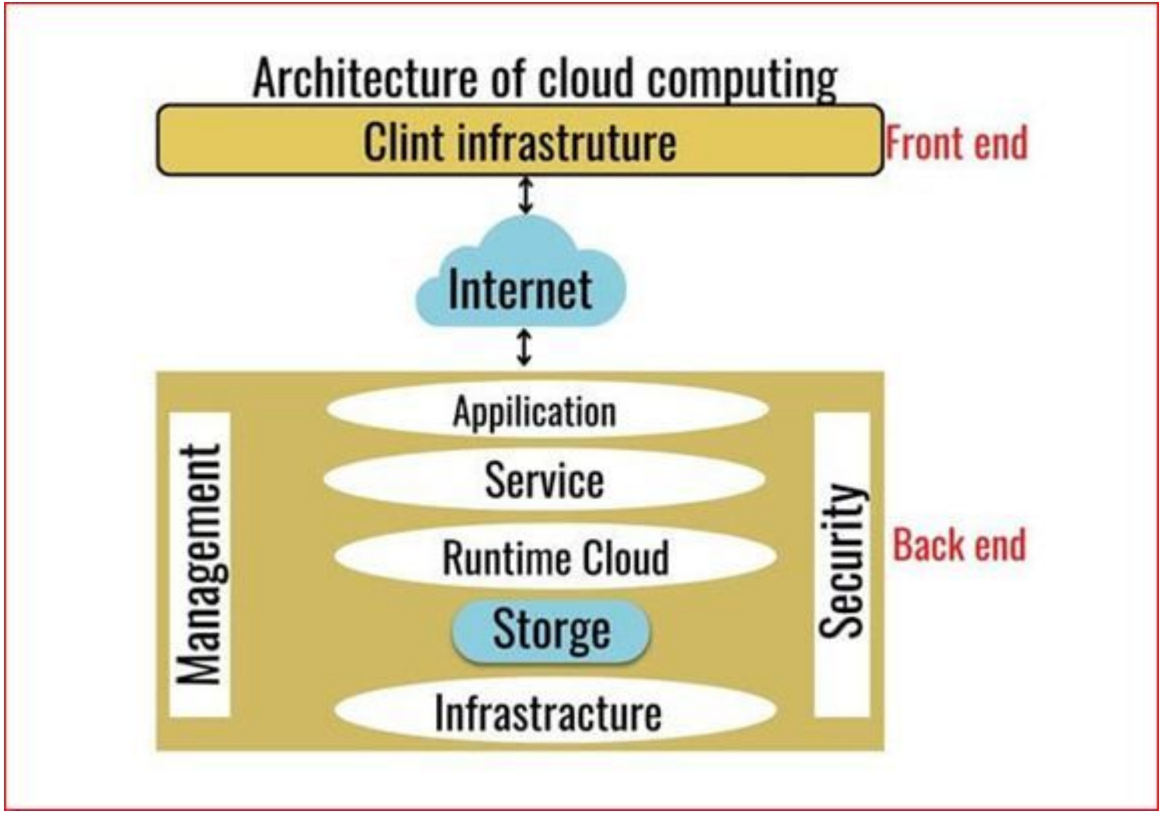
The SOHO architecture consists of the simplest architecture.

- As the name suggests, it is mostly used in homes and/or small enterprises.
- This type of architecture consists of three components:
  1. A small switch
  2. A router
  3. Connected access devices such as printers, PCs, etc.
- Usually, a single device is used that acts as both a switch and router.
- The devices are hardwired into this router.

On-Premises and Cloud Architecture

- Data centers traditionally hosted centralized enterprise infrastructure.
- It is referred to as on-premises infrastructure, which implies that companies have full control over the network, compute, storage, and software components.

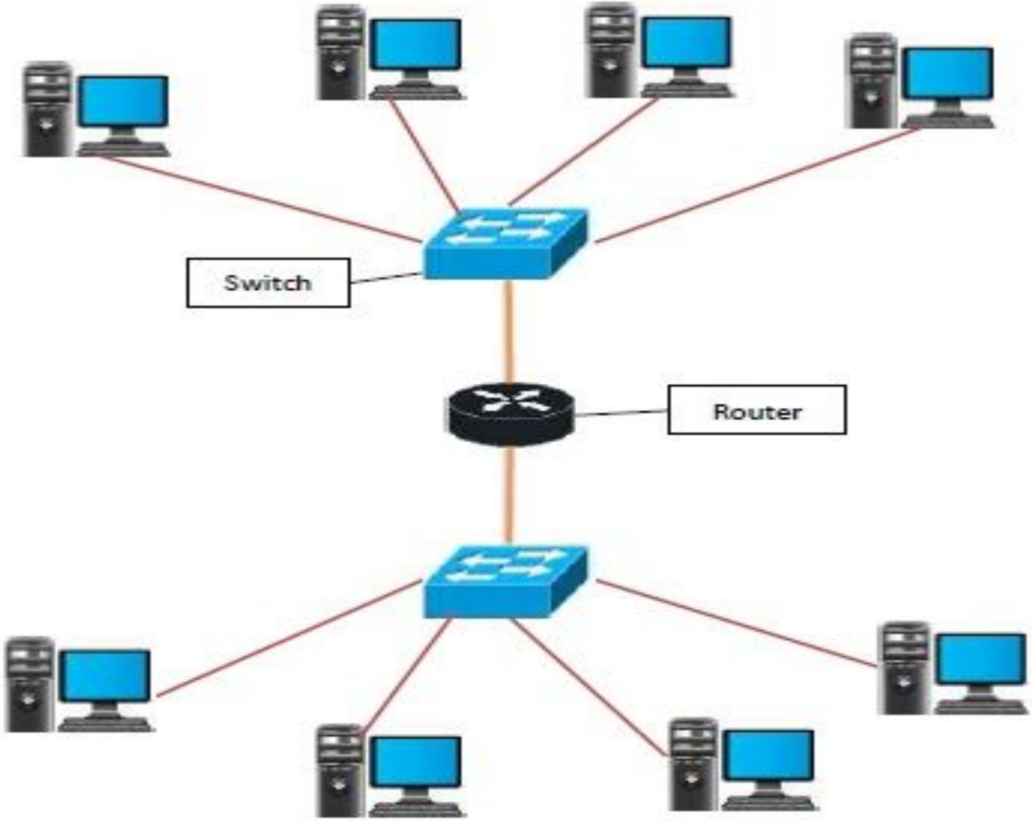
- Cloud-based networks leverage remote servers and infrastructure hosted by third-party providers (e.g., Amazon Web Services, Google Cloud).
- These resources are accessed over the internet. Compared to on-premises data centers, public clouds offer very good scalability and rapid deployment with a consumption-based billing model.
- **Example**: Cloud storage services like **Google Drive** or **Dropbox**, where users can store and access data from anywhere with an internet connection.



Architecture of cloud computing

Router

- Routers are networking devices operating at layer 3 or a network layer of the OSI model.
- They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks.
- When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.



Router Connecting Two Networks

Types of Routers

Fixed and Modular Routers

Fixed Routers:

A fixed router has a set number of ports and a pre-defined configuration, meaning its functionality and capacity are fixed at the time of manufacture.

Fixed routers has:

- Limited expansion or customization options.
- Typically more cost-effective for smaller networks.
- May be suitable for basic networking needs where future expansion is not expected.

Modular Routers

A modular router allows for customization and expansion through the addition of modules, such as interface cards or other hardware components.

A modular router has:

- Highly customizable and scalable to meet changing network requirements.
- Can accommodate various interface types (Ethernet, serial, etc.) and speeds.
- More expensive than fixed routers but offer greater flexibility.

Cisco Router types

Branch Routers:

Targeted for branch offices, these routers offer more advanced features like VPN, WAN optimization, and support for voice and video.

Router Series and models

800 series - 810, 860, 880
1900 series - 1905, 1921, 1941
2600 series - 2610, 2611, 2620
2800 series - 2811, 2851
2900 series - 2901, 2911, 2921

Edge Routers / Aggregation Routers:
As their name indicates, edge routers are placed at the edge or boundary of networks, and typically connect to Internet service providers (ISPs) or other organizations’ networks.

Router Series and models
1000 series - 1001, 1002, 1004
5000 series - 5001, 5002

Service Provider Routers: Designed for Internet service providers (ISPs) and telecommunications companies, these routers provide high availability, scalability, and carrier-grade NAT.

Router Series

- 9000 series - **9006, 9010, 9904, 9910, 9922**

External Components of Router

External Components of router include the external ports of the router. These ports are divided into three categories i.e., LAN ports, WAN ports and Admin Ports.

WAN Port - Serial port

This is the port wired to the Wide Area Network or to an external network, which is typically the Internet.

Serial port available in 60 pin female connector or smart serial 25 pin female connector.

LAN Port - RJ 45 port

This is the port (RJ-45) connected to the Local Area Network or the port which will be connected to your switch.

The speed of the RJ-45 ports can be

- 10 Mbps Ethernet
- 10/100 Mbps Fast Ethernet
- 10/100/1000 Mbps Gigabit Ethernet

Admin Port (Console and Aux port)

They are used for the administration or configuration of the router with the help of HyperTerminal applications or terminal emulation softwares.

Console port

The console port on a router is primarily used by nearby users (administrators or technicians) to configure initial settings and perform direct, out-of-band management.

Aux port

The Auxiliary (Aux) port on a router is another type of physical port, similar in appearance to a console port . However, its primary function is for remote, out-of-band management via a modem connection.

HWIC - High-Speed WAN Interface Card

A HWIC card stands for High-Speed WAN Interface Card. It's a type of modular interface card used in certain Cisco’s modular routers to provide flexible and customizable connectivity options.

They can offer a diverse range of interfaces and services, including:

- **WAN Interfaces:** T1/E1, Serial (for Frame Relay, PPP, HDLC), ATM, DSL (ADSL, G.SHDSL).
- **Ethernet Interfaces:** Fast Ethernet or Gigabit Ethernet ports
- **Voice/TDM:** For connecting to traditional telephony systems (e.g., T1/E1 voice interfaces).
- Wireless: Support for cellular (3G, 4G LTE) or Wi-Fi connectivity.

Internal components of a Router

CPU: The CPU in the router executes the commands and processes the commands in the operating system. The flow of data on the interface is controlled by the CPU.

RAM: Random Access Memory in the router contains the executable file and running file of the configuration file and the contents are lost when the router’s power is turned off.

ROM: Read Only Memory in the router mainly works when the router boots up or is powered up. It stores the bootstrap program needed when the router is turned on.

Mini-IOS: Mini-IOS refers to a small, stripped-down version of the full Cisco IOS software stored in ROM.The Mini-IOS, also known as ROMMON or bootstrap image, provides a minimal set of commands and functions to support basic operations.

Bootstrap Loader (BSL): This is a small program stored in the router's ROM (Read-Only Memory). The BSL is responsible for initializing the router's hardware components, including the CPU, memory, and other peripherals.

Flash Memory: It contains the operating system (IOS - Internetwork Operating System). The data of the flash memory remain unchanged when the router is rebooted or powered off. So, whenever the router is powered on the OS is loaded into RAM from flash memory.

NVRAM: It stands for Nonvolatile RAM. It is a backup copy of the running configuration file. Its functioning basically helps when the router loses power and the router needs to establish the configuration and load it again. The content of NVRAM is changeable. When the router is powered on it searches the startup-config file in NVRAM only.

POST (Power-On Self test): It's a hardware diagnostic process that runs when the router is powered on, verifying the functionality of various components like memory, CPU, and network interfaces. The POST is stored in and executed from the ROM chip.

Booting Process

The booting process of a router involves several steps, starting with a power-on self test (POST) to check hardware, then loading the operating system (IOS) image from flash or other sources, and finally loading the configuration file (startup-config). The router then becomes operational, ready to route network traffic.

Booting Process steps

1. Power-On Self Test (POST):
When the router is powered on, it first performs a POST to check the hardware components, including memory and interfaces.

2. Loading the Bootloader:
The bootstrap program (similar to the BIOS on a computer) is loaded and executed, responsible for determining where to locate the IOS image.

3. Locating the IOS Image:

The bootstrap reads the configuration register value, which dictates where to load the IOS. It typically checks the startup-config for "boot system" commands first, then looks in Flash memory, and if not found, it may try TFTP or ROM.

4. Loading the IOS Image:

Once the IOS image is found, it's loaded into RAM.

5. Loading the Configuration File:

The IOS then attempts to load the startup-config from NVRAM (Non-Volatile RAM).

6. Configuration:

If the startup-config is not found in NVRAM, the IOS may try to load a configuration from TFTP. If no TFTP server responds, the router enters Setup Mode (initial configuration mode).

7. Router Operational:

Once the configuration is loaded, the router is ready to function and route network traffic.