PM Networking

CISCO

CCNA

Exam (200-301) v1.1 Study Companion

+91-85118 26341

www.pmnetworking.in

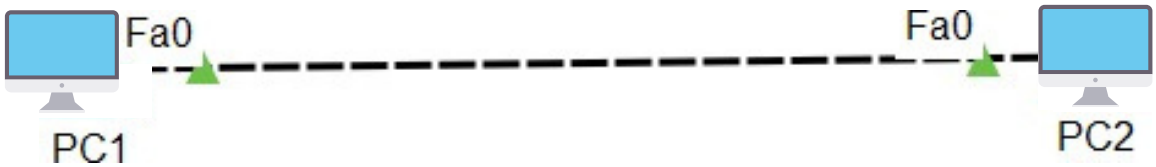
Day - 1

What is a Network?

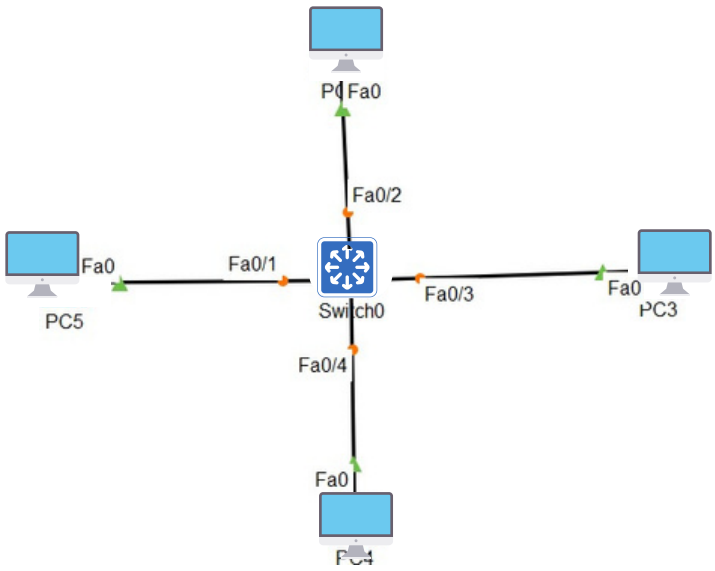
A network refers to interconnected devices or computers that can communicate and share resources.

Example - There are multiple computers in an office. Each computers are connected to a Central server either through cables or wireless. This is called Network. These devices communicate to exchange network resources, such as files and printers, and network services.

When two computers are interconnected with each other this is also called Network.



We know in one PC there is only one NIC Card so we can connect only one PC if we want to connect more than two devices in a Network in this case we need networking devices like HUB, Switches, or Routers. And all of the devices on the network can communicate with each other. We will discuss this in more detail about all Networking devices later.



As an End-user, what do you think about the Network?

As an End-User we want Networks that provide Confidentiality, Integrity, and Availability.

CONFIDENTIALITY

Confidentiality ensures that data is only accessible to authorized individuals or entities. This means that unauthorized users should not be able to access sensitive data.

There are mainly Two types of DATA.

1) **Static Data -** The data that is present inside the database or any other storage system is called Static Data and if you want to access this you must need access or permission.
2) **Floating Data -** Data that we are sending over the Network or Internet is called Floating Data. E.g. – WhatsApp message

INTEGRITY

Integrity means keeping our data accurate, complete, and unchanged. It makes sure that no one can modify or tamper with our data without permission. The main goal is to make our data trustworthy and reliable. As users, we want our data to stay safe and not be tampered with online, which is our right.

AVAILABILITY

Availability means we can access the internet and our data on the server at any time. It means the system should always be working and ready 24/7. There are many ways that companies make sure we always have access.

For example, Amazon is a popular shopping website that gets a lot of visitors, especially during holiday sales. To keep the website running smoothly and avoid overloading the server, Amazon uses a technique called load balancing. This means that the traffic is spread across many servers so that no single server gets too much load, preventing any disruptions during busy times.

Based on how our devices are connected Geographically, there are different types of networks:

Local Area Network (LAN) – LANs are used in small to medium places like offices or buildings with limited space.
Personal Area Network (PAN) – PANs cover a short distance, usually about 10 meters. Bluetooth is a good example of a PAN.
Metropolitan Area Network (MAN) – MANs connect networks in a single city or town.
Wide Area Network (WAN) – WANs cover large areas like states or even countries.
Wireless Local Area Network (WLAN) – WLANs are used for wireless networks, allowing both wired and wireless devices to connect.

Types of Communications:

Unicast: Unicast communication involves sending data packets from one sender to one specific receiver. It is a one-to-one communication method.

Multicast: Multicast communication involves sending data packets from one sender to multiple specific receivers. It is a one-to-many communication method.

Broadcast: Broadcast communication involves sending data packets from one sender to all devices within the network. It is a one-to-all communication method.

Modes of Communications:

Simplex Communication:

- In simplex communication, data travels in only one direction, from the sender to the receiver.
- The receiver cannot send data back to the sender in a simplex mode.
- This mode is often used for situations where one-way communication is sufficient or where the sender and receiver have distinct roles.
- Television and radio broadcasting are classic examples of simplex communication. The TV station broadcasts content to viewers, but viewers cannot send feedback through the same channel.

Half Duplex Communication:

- In half-duplex communication, data can travel in both directions, but not simultaneously.
- It alternates between sending and receiving.
- Only one party can send data at a time, and the other party must wait to receive or respond.
- Walkie-talkies often use half-duplex communication. Users press a button to speak (send) and release it to listen (receive).

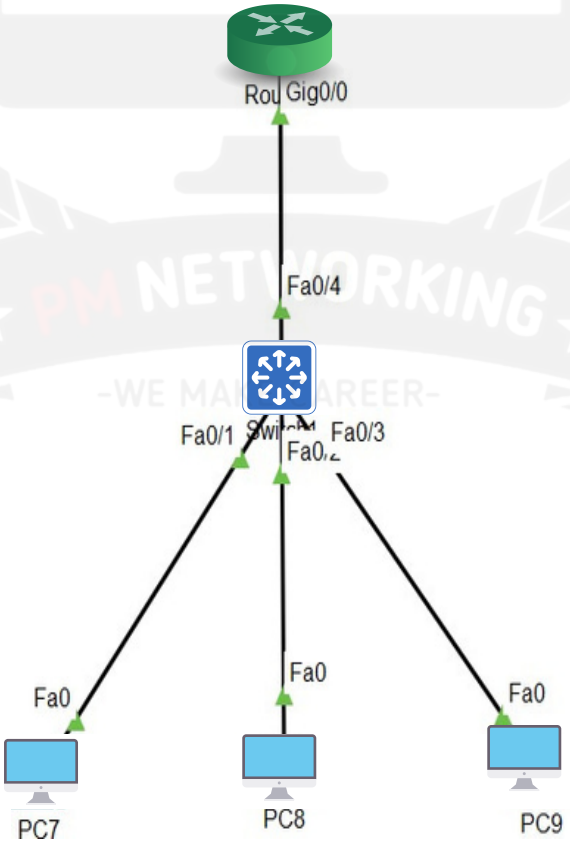
Full Duplex Communication:

- Full duplex communication allows data to travel in both directions simultaneously.
- Both parties can send and receive data independently without waiting for the other.
- Traditional telephone conversations and most internet connections. In a phone call,
- both parties can speak and listen at the same time.

NETWORKING DEVICE

Router

- It is a Layer 3 device according to the OSI Model
- It is used to forward the data from Network to Another.
- It forwards the data based on a logical address called an IP Address.
- The router maintains a Routing table to take the forwarding decision.
- Every interface of the router will be in a different Network.
- It has fewer network interfaces compared to Switch.
- It provides connectivity between LANs.
- Generally, Routers handle unicast traffic in a Network.
- The router will multicast data when you configure a routing protocol that uses multicast like OSPF or EIGRP.
- Routers do not forward broadcast traffic between different network segments. They typically block broadcast packets from passing beyond their local network.
- Routers don’t generate broadcast messages to other networks, but they generate broadcast messages within their Local network. For example, A router generates an ARP Request Message (Which is Broadcast)to find a device's MAC address on the same network.



SWITCH

- Switch is a Layer 2 Device according to OSI Mode.
- A switch operates based on a Physical address called a MAC Address.
- Switch Maintain MAC-Address table and take forwarding decision based on this. Switch map the MAC-Address and port in the MAC-Address Table.
- A switch is used to connect multiple end-users in a LAN Network.
- The switch has many ports compared to the Router.
- The switch is used in our LAN Network. It does not provide the connectivity between the LAN Network.
- Switch can Unicast / Multicast and Broadcast the Packets.
- It operates at Full Duplex mode so it means hosts can both send and receive data at the same time.

When choosing a switch, you need to decide between a managed or an unmanaged switch. The main difference is how much control you have over the switch settings.

Unmanaged Switches: These are very simple. You just plug them in, and they work without needing any setup. They are good for small networks with basic needs.

Managed Switches: These are more advanced. You can customize and adjust many settings to fit your needs. They also give you detailed information about network performance. Managed switches are better for larger networks or for important tasks that need extra control and monitoring.

Difference Between Managed Switchand Un-Managed Switch

Feature	Un Managed Switch	Managed Switch
Setup	Plug and play; no setup needed	Requires setup and configuration
Control	Limited control; basic operation	Full control; customizable settings
Monitoring	No performance monitoring	Provides detailed performance and traffic info
Network Management	No network management options	Offers advanced features like VLANs and QoS
Cost	Generally cheaper	More expensive due to advanced features

Based on operations we can divide the Switch into Layer 2 & Layer 3.

Layer-2 Switch: This switch operates at the Data Link layer (Layer 2) of the OSI Model. It forwards data based on MAC (Media Access Control) addresses.

Layer-3 switch: This Switch operates at the Network layer (Layer 3) of the OSI Model. It performs routing functions in addition to switching, using IP addresses to route data between different networks or VLANs.

What are the differences Between Layer2 Switch and Layer3 Switch?

Feature	Layer-2 Switch	Layer-3 Switch
Layer	Operates at Layer 2 (Data Link)	Operates at Layer 3 (Network)
Function	Switches data based on MAC addresses	Routes data based on IP addresses
Routing Capability	Does not perform routing	Can perform routing between VLANs
Network Segmentation	Segments network into VLANs only	Segments network and routes between VLANs
Forwarding Table	Uses MAC address table	Uses routing table and MAC address table
Inter-VLAN Routing	Cannot route between VLANs	Can route between VLANs
Cost	Generally cheaper	More expensive due to routing capabilities
Performance	Generally faster for switching	May have slightly higher latency due to routing

CiscoCatalyst2960

CiscoCatalyst9300

FIREWALL

There are two types of Firewalls-Traditional Firewalls and Next Generation Firewalls.

Traditional Firewalls

- A traditional firewall provides stateful inspection of network traffic. Stateful Inspection means it Keeps track of active connections and ensures that packets are part of a valid ongoing connection.
- It allows or blocks traffic based on state, port, and protocol, and filters traffic based on administrator-defined rules.
- It Hides internal IP addresses from the outside world.
- It is Good for basic traffic control and network protection based on static rules.

CISCOASA5500

Next-Generation Firewall (NGFW)

This firewall also includes traditional (first-generation) firewall functionalities such as stateful port/protocol inspection, Network Address Translation (NAT), and Virtual Private Network (VPN).

A part from the Traditional Firewall feature It Provides advanced security features. So It uses more advanced techniques to control and inspect network traffic:

Application Identification and Filtering:

- This key feature of NGFWs can identify and control specific applications.
- Instead of just blocking or allowing traffic based on port numbers, NGFWs understand which applications are running and can block or allow them based on their identity.
- This helps stop harmful apps that might try to sneak through by using unusual ports.

SSL and SSH Inspection:

- NGFWs can look into encrypted traffic that uses SSL or SSH.
- They first decrypt the data, check if it follows the rules and if the applications are allowed, and then re-encrypt it.
- This helps protect against harmful apps that try to hide by using encryption.

Intrusion Prevention:

- NGFWs have advanced features that deeply inspect network traffic to find and stop threats.
- Some NGFWs include built-in intrusion prevention, so you might not need a separate IPS device.

CISCO FIREPOWER4100

Palo Alto

What is an IPS?

An **Intrusion Prevention System (IPS)** is a network security tool that helps protect systems and networks from malicious activities. It monitors network traffic or system behavior to detect and prevent harmful actions before they can cause damage.

Major Functionsof IPS:

- IPS continuously scans network traffic or system actions to spot anything suspicious or harmful. It looks for patterns, signatures, or behaviors that match known threats.
- When the IPS detects potential threats, it gathers detailed information about these activities. This data helps in understanding what is happening and why it is considered a threat.
- The system notifies network administrators or security teams when it finds something dangerous. This alert allows the security team to take immediate action if needed.
- IPS can take action to prevent the detected threats from causing harm. This might involve blocking malicious traffic, stopping harmful processes, or isolating affected systems.

CISCO IPS

ACCESS POINT

- A Wireless Access Point (WAP) is a device that allows wireless devices, like smartphones, laptops, and tablets, to connect to a wired network using Wi-Fi.
- It acts as a bridge between your wired network (like your router) and your wireless devices.

What are the benefits of WAP?

Mobility: Wireless Access Points let users move around freely while staying connected to the network. There's no need to stay close to a cable.

Easy Connectivity: Multiple devices can connect to the network without needing physical cables.

Scalability: You can easily add more WAPs to expand your network's coverage area as your needs grow.

Flexibility: Wireless networks can be set up in places where running cables is difficult or impossible.

How Does It Work?

WAPs use radio waves to send and receive data between devices and the network. This allows communication without physical cables.

Wireless LAN Controller (WLC)

- A Wireless LAN Controller (WLC) is a device used to manage multiple Wireless Access Points (WAPs) in a network.
- Instead of configuring each WAP separately, you can use a WLC to control them all from one place.
- The WLC makes managing many access points easier.
- It provides a central place to manage settings, security, and other features for all the WAPs in your network.
- With a WLC, you can update settings for all your WAPs at once. For example, if you need to change the Wi-Fi password, you do it in the WLC, and it updates all the WAPs automatically.
- The WLC ensures that all the WAPs follow the same security rules. This means you can easily manage who has access to your network and protect your data.

- When you have a WLC, users can move around the building without losing their Wi-Fi connection. The WLC ensures that their connection is passed smoothly from one WAP to another.

- The WLC helps distribute the data load evenly across all WAPs, preventing any single WAP from becoming overloaded and ensuring a smooth experience for all users.

- As your network grows, you can add more WAPs, and the WLC will manage them all. This makes it easy to expand your Wi-Fi coverage without complicating the management.

- By centralizing the management of WAPs, the WLC saves time and reduces the effort needed to maintain the wireless network.

ENDPOINTS

- An endpoint is any device that connects to a network. Common examples include computers, smartphones, tablets, and printers.

- Endpoints are the devices that people use to access and interact with the network. They are the starting and ending points for data in a network.

- When you use an endpoint, like a laptop, to access the internet or a network, it sends and receives data. This data travels through the network to reach other devices or services.

SERVER

- A server is a powerful computer that provides services, data, or resources to other computers, known as clients, over a network.

- Servers store, manage, and share data with other computers. They also run applications and programs that other devices on the network can use.

- When a client (like your computer) needs something, it sends a request to the server. The server processes the request and sends back the data or service needed.

- Servers make it possible for multiple users to access the same resources, like files, websites, or applications, without needing individual copies on each device.

Types of Servers:

File Servers: Store and share files with other computers.

Web Servers: Host websites and deliver web pages to your browser.

Mail Servers: Manage and deliver emails.

Database Servers: Store and manage large amounts of data.

Application Servers: Run specific applications that other devices can access.

Example Google Server - Google has all types of servers for their users.

Web Servers: When you type a search query into Google, web servers handle your request and show search results.

File Servers: Google Drive stores your documents, photos, and other files and lets you access them from any device.

Database Servers: Google's database servers manage data related to search queries and user accounts.

Application Servers: Google Maps servers handle requests for map data and provide directions to users.

Power over Ethernet (PoE)

PoE is a technology that lets you send electrical power through an Ethernet cable along with data.

How Does It Work?

- PoE sends both power and data through the same Ethernet cable.
- At the source (like a PoE Switch), power is added to the Ethernet cable using a device called an injector.

- At the other end of the cable, if the device supports PoE, it will use the power and data from the same cable without any extra setup.

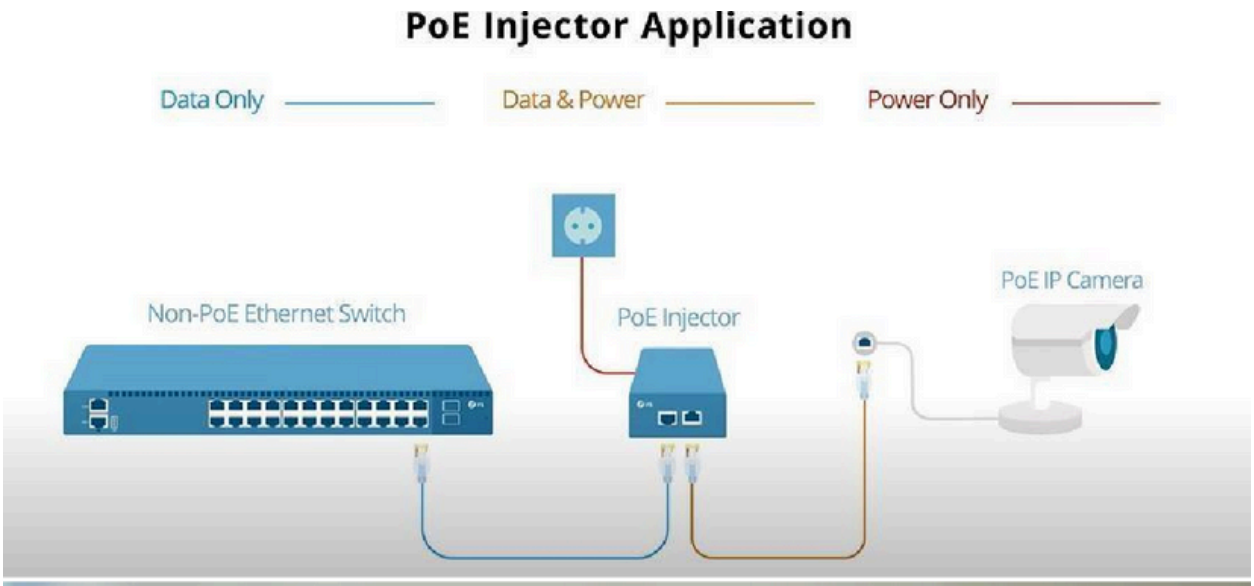
- If the device doesn't support PoE, a special adapter called a splitter is needed. This device separates the power from the data and sends the power to a regular power plug.

- The power and data stay separate inside the cable, so they don't mix up or cause problems with each other.

- It is useful because It reduces the need for extra power cables and outlets. This makes setup simpler and cleaner.

What are those devices that use POE Technology?

IP Cameras: To send video and receive power without extra cables.
Wireless Access Points: To provide Wi-Fi to devices and receive power through the Ethernet cable.
VoIP Phones: To make calls and receive power through the same cable.



Thank you

PM Networking

Click icons Follow Our Social media

www.pmnetworking.in

+91-85118 26341