Network Connectivity Layout

Cummins College of Engineering for Women

Basic Architecture

The College Area Network which have the IP address as 192.168.0.0 consist of 4 Building and VLAN is assigned to each building to have security over the WLAN as follows :-

Sr.no	Building Name	VLAN	IP Address
1.	Main Building	101	192.168.1.0
2.	Mechanical Building	102	192.168.2.0
3.	MBA Building	103	192.168.3.0
4.	Server Room	104	192.168.4.0
5.	IT Building	105	192.168.5.0

Department in Building

Campus Area Network includes Multiple types of Department as follows:-

Main Building
Instu Department-Ground Floor
Purchase Department-Ground Floor
ADMIN Department-1st Floor
E&TC Department-2nd & 4th Floor
Comp Department-3rd & 5th Floor
Library-3rd Floor

KB Joshi Building
T&P Department-Ground Floor
Sport Department-Ground Floor
IT Department - 2nd & 3rd Floor

MBA Building
MBA Department-All Floor

Mechanical Building
Workshop-Ground Floor
Mech Department -All Floor
Aligned Department - 3rd Floor

Server Room
Server Center

End Device

End Devices used in Network are as follows :-

- **PC**
- **Laptop**
- **IP Phone**
- **Server**
- **Printer**
- **Smartphone**

Security of End Device :-

Endpoint security are highly varied depending on the risk . The following are some of the most common endpoint security components

- **Device Protection**
- **Networks Control**
- **Application Control**
- **Browser Protection**

Wireless Access Point (WAP)

An **access point** is a device that creates a wireless local area **network**, or WLAN, usually in an office or large building.Instead, the **access point** functions as a hub that links all stations together. It serves as the focal **point** for communications, increasing the communication range of wireless users.

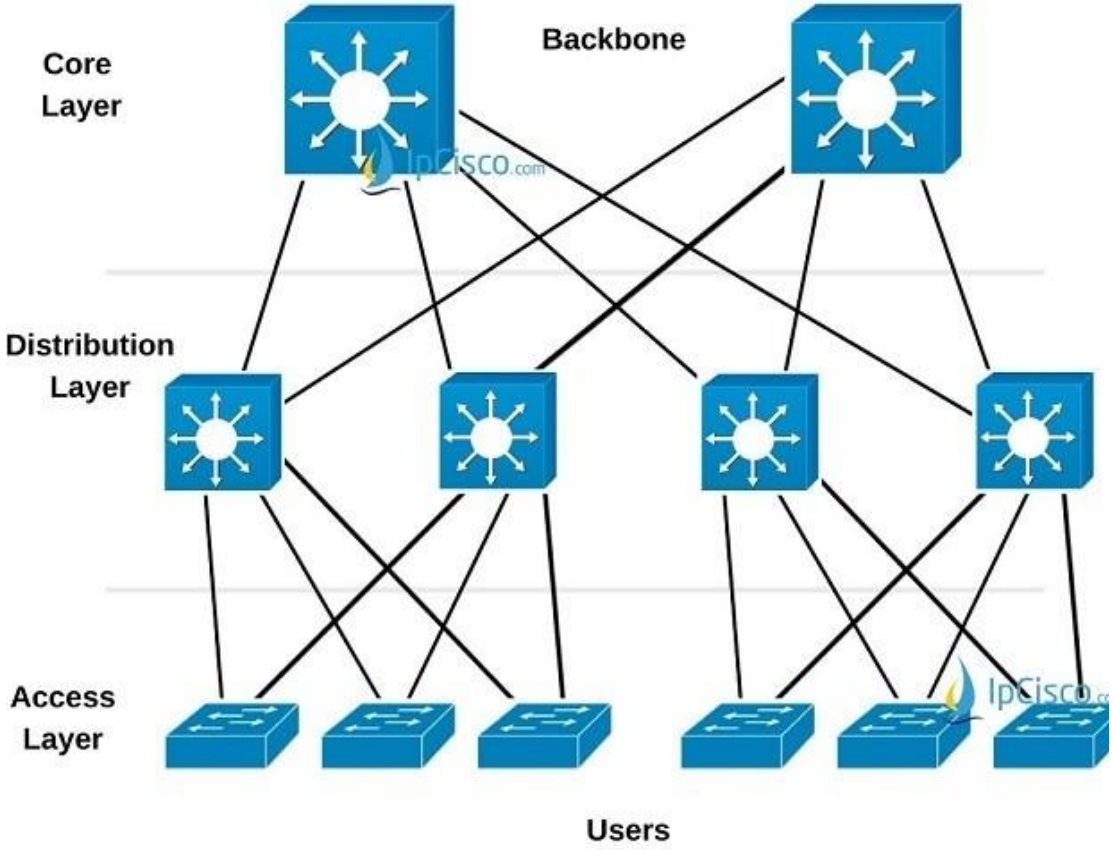
Security of Access Points :-

The most common solution is **wireless traffic encryption** . Modern access points come with built-in encryption such as **WEP,WPA,WPA2,WPA3**

WPA3 - **It is the most secured among all but packet tracer doesn't provides this so I have used WPA2**

Through WPA2 we can provide a password and encrypt it using AES or TKIP .Where TKIP is actually an older encryption protocol which is no longer consider as secure.AES is a more secure encryption protocol introduced with WPA2

Design using Three Tier Layer Modal



Three-tier layer model

This design model can be used in large campus networks where multiple distribution layer and buildings need to be interconnected

It consists of Basic Three Layer -

1.Access Layer - Access layer includes acces switches which are connected to the end devices

2.Distribution Layer - The purpose of this layer is to provide boundary definition by implementing access lists and other filters

3.Core Layer - Core Layer is considered as the backbone of networks

Switch

Three Type of Switch are used in Network as follows:-

- **Access Layer Switch** :-It is usually a **Layer** 2 **switch** and facilitates the connection of end node devices to the network .
  - Name of the switch used as ASW(Access Layer Switch)- 2960 IOS 15.
- **Distributed Layer Switch** :-It acts as a bridge between core **layer switch** and access **layer switch .**
  - Name of the switch used as DSW(Distributed Layer Switch)- 3650 24 PS
- **Crore Layer Switch**:- **Core switch** occupies in the topside **layer** of the enterprise networking (**core layer**), which functions as backbone **switch** for LAN access and centralizes multiple aggregation to the **core .**
  - Name of the switch used as CSW(Core Layer Switch)- 3650 24 PS

Secure of Switch

- Adding Console password with encryption
- To connect ASW(Access Layer) to DSW(Distributed Layer) we will require Multi Mode Fiber and to Connect from DSW to CSW(Core Layer)we will require Single Mode Fiber with the help of **Fiber patch ie LUI** so we will add **SPF** patch in the DSW Switch .
    - **Single-Mode Fiber** -Larger Distance greater than 500 meter
    - **Multi-Mode Fiber** -Small Distance less than 500 meter
- Adding SSH or Telnet . Telnet can cause a DDos so SSH is preferred
- Shutdown all unwanted ports of switch .
- **Attacks like Mac table Attacks,Vlan Attacks,DHCP Attack,ARP Attacks,ARP Attacks,STP Attacks to overcome this we can have port security , DHCP Snooping ,Dynamic ARP Inspection and IP secure Guard**

Server Room

- There are 2 ISP one for the backup .
- The ISP are Connected to the **firewall** for protection of network .
- In server room we can have different type of server , storage system and backup server.
- We can also have the workstation where all IP Phone ,IP Camera can be access .

Thank you