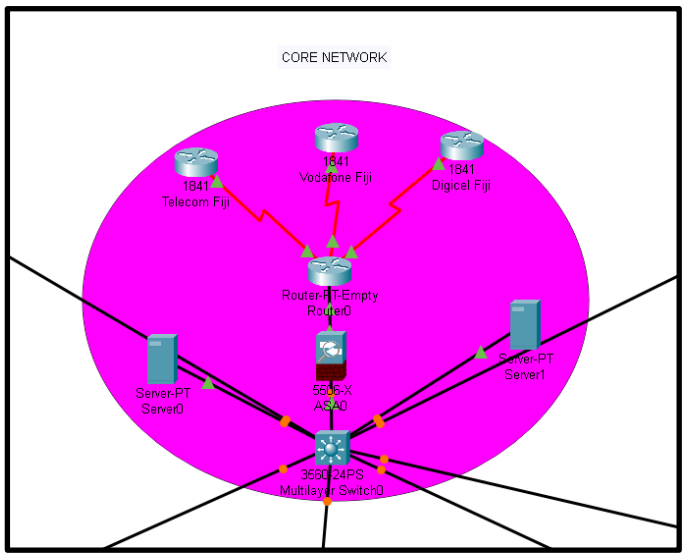
Name: Shainesh Nand ID :S11208989

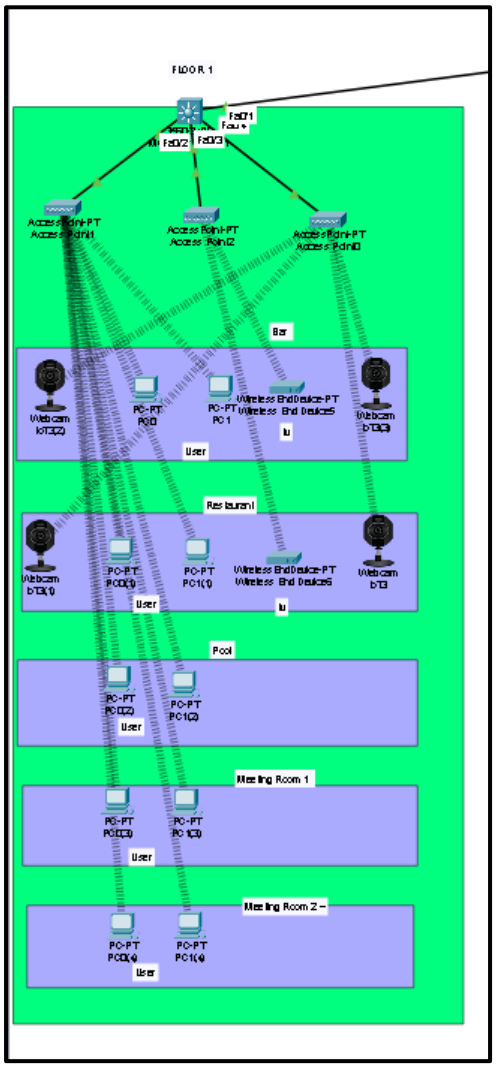
Network Design and Addressing

Network design

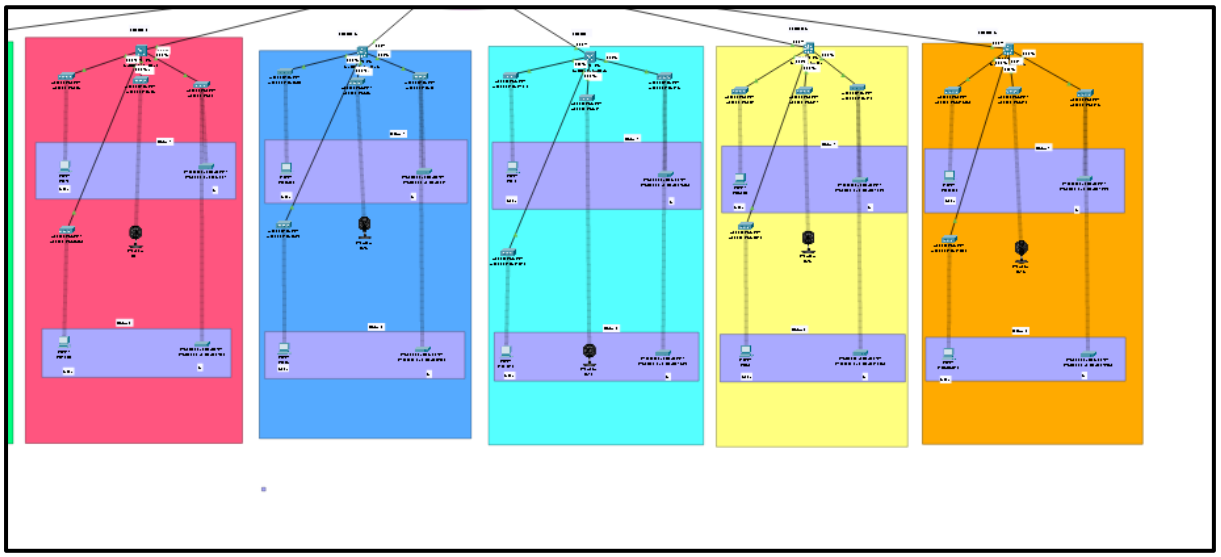
Core network



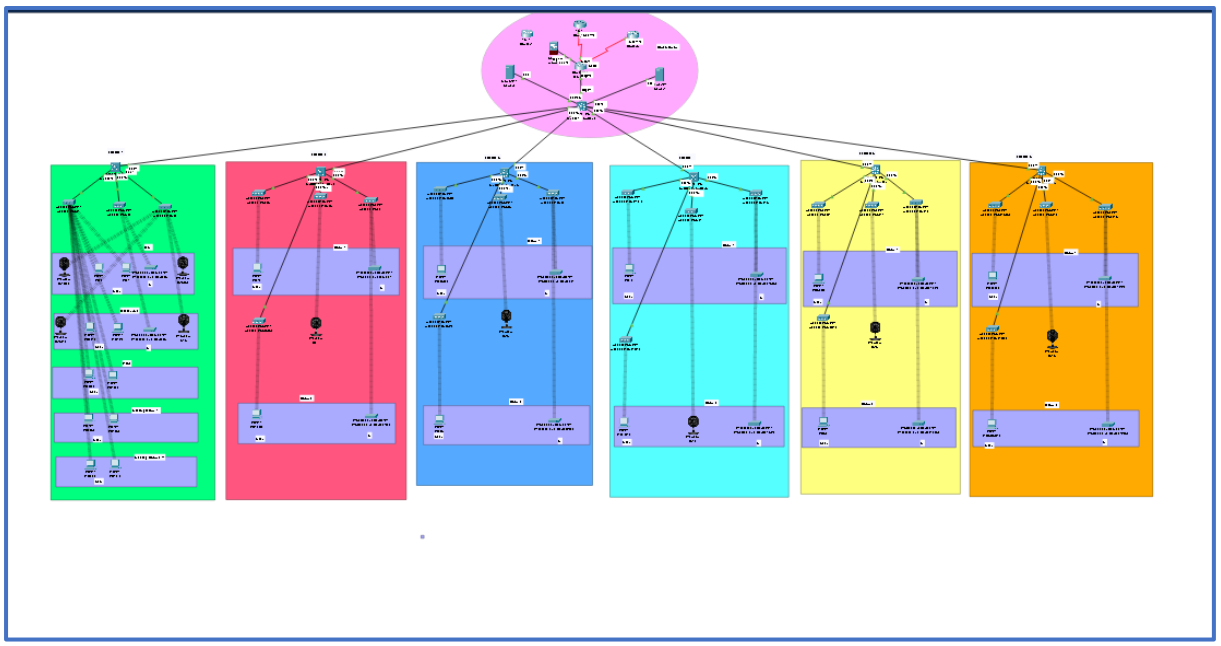
Floor 1



Floor 2-6



Overall topology of the network.



Selection of Devices

Purpose: Provide high-speed, reliable Wi-Fi coverage.

Reason: Supports Wi-Fi 5/6/6E for high-density guest usage and streaming.

Purpose: is the centralized management of access point.

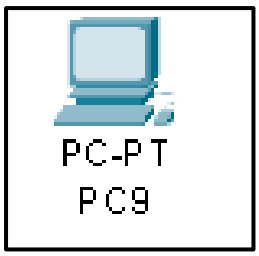
Reason: makes the management of access point easier and for troubleshooting.

Purpose: Security and surveillance in each floor

Reason: provides security and form of evidence

Purpose: for entertainment view purpose in each rooms.

Reason: Delivers digital streaming services over the hotel's IP network.



Purpose: represents the users as guest.

Reason: good connection , reliable and has high bandwidth.

Purpose: simply manages the Dhcp and dns

Reason: it was selected to fulfill the request made by network resources.

Purpose: Provides connectivity for wired devices to communicate Reason: it was used as due to its stability in handling many devices..

Purpose: Manages inter-VLAN routing and Layer 3 operations.

Reason: Supports high-performance routing between VLANs for network efficiency

Purpose: provides security by filtering the network traffic.

Reason: prevents unauthorized access and cyber threats, trying to breach the system.

Subnetting

The objective of the assignment is to design a network design for Pullman Group hotel, considering all the floors and rooms in the hotel. Subnets and hots in each floor have been assigned with the given network address10.9.0.0/15

Bellow is the host calculation for each floor considering all the devices.

Floor 1 Host:

- Pool Area: 100 Wi-Fi Users
- Bar: 100 Wi-Fi Users, 2 IPTV, 5 Cameras
- Restaurant: 100 Wi-Fi Users, 2 IPTV, 5 Cameras
- Meeting Room 1: 200 Wi-Fi Users
- Meeting Room 2: 200 Wi-Fi Users

Floors 2 to 6 Host Requirements (Each Floor):

- Rooms: 10 Rooms
    - Each Room: 5 Wi-Fi Users + 1 IPTV
- Corridor: 3 Cameras

Subnetting Process:

Lets start the subnetting with the highest host number which is floor one and then later move top floor 2 to 6.

Floor 1

Network address	Subnet mask	Usable Ip	Broadcast address
10.9.0.0	255.255.252.0	10.9.0.1-10.9.4.2	10.9.4.3

IPTV

Network address	Subnet mask	Usable Ip	Broadcast address
10.9.4.4	255.255.255.192	10.9.0.5-10.9.4.66	10.9.4.67

Camera

Network address	Subnet mask	Usable Ip	Broadcast address
10.9.4.68	255.255.255.224	10.9.0.69-10.9.4.98	10.9.4.99

Floor 2

Room	Network address	Subnet mask	Usable Ip	Broadcast address
1	10.9.4.100	255.255.255.224	10.9.4.101-10.9.4.106	10.9.4.107
2	10.9.4.108	255.255.255.224	10.9.4.109-10.9.4.114	10.9.4.115
3	10.9.4.116	255.255.255.224	10.9.4.117-10.9.4.122	10.9.4.123
4	10.9.4.124	255.255.255.224	10.9.4.125-10.9.4.130	10.9.4.131
5	10.9.4.132	255.255.255.224	10.9.4.133-10.9.4.138	10.9.4.139
6	10.9.4.140	255.255.255.224	10.9.4.141-10.9.4.146	10.9.4.147
7	10.9.4.148	255.255.255.224	10.9.4.149-10.9.4.154	10.9.4.155
8	10.9.4.156	255.255.255.224	10.9.4.157-10.9.4.162	10.9.4.163
9	10.9.4.164	255.255.255.224	10.9.4.165-10.9.4.170	10.9.4.171
10	10.9.4.172	255.255.255.224	10.9.4.173-10.9.4.178	10.9.4.179

Floor 3

Room	Network address	Subnet mask	Usable Ip	Broadcast address
1	10.9.4.180	255.255.255.224	10.9.4.181-10.9.4.186	10.9.4.187
2	10.9.4.188	255.255.255.224	10.9.4.189-10.9.4.194	10.9.4.195
3	10.9.4.196	255.255.255.224	10.9.4.197-10.9.4.202	10.9.4.203
4	10.9.4.204	255.255.255.224	10.9.4.205-10.9.4.210	10.9.4.211
5	10.9.4.212	255.255.255.224	10.9.4.213-10.9.4.219	10.9.4.219
6	10.9.4.220	255.255.255.224	10.9.4.221-10.9.4.226	10.9.4.227
7	10.9.4.228	255.255.255.224	10.9.4.229-10.9.4.234	10.9.4.235
8	10.9.4.236	255.255.255.224	10.9.4.237-10.9.4.222	10.9.4.223

9	10.9.4.224	255.255.255.224	10.9.4.225-10.9.4.250	10.9.4.251
10	10.9.4.252	255.255.255.224	10.9.4.253-10.9.5.3	10.9.5.4

Floor 4

Room	Network address	Subnet mask	Usable Ip	Broadcast address
1	10.9.5.5	255.255.255.224	10.9.5.6-10.9.5.11	10.9.5.12
2	10.9.5.13	255.255.255.224	10.9.5.14-10.9.5.19	10.9.5.20
3	10.9.5.21	255.255.255.224	10.9.5.22-10.9.5.27	10.9.5.28
4	10.9.5.29	255.255.255.224	10.9.5.30-10.9.5.35	10.9.5.36
5	10.9.5.37	255.255.255.224	10.9.5.38-10.9.5.43	10.9.5.44
6	10.9.5.45	255.255.255.224	10.9.5.46-10.9.5.51	10.9.5.52
7	10.9.5.53	255.255.255.224	10.9.5.54-10.9.5.59	10.9.5.60
8	10.9.5.61	255.255.255.224	10.9.5.62-10.9.5.67	10.9.5.68
9	10.9.5.69	255.255.255.224	10.9.5.70-10.9.5.75	10.9.5.76
10	10.9.5.77	255.255.255.224	10.9.5.78-10.9.5.83	10.9.5.84

Floor 5

Room	Network address	Subnet mask	Usable Ip	Broadcast address
1	10.9.5.85	255.255.255.224	10.9.5.86-10.9.5.91	10.9.5.92
2	10.9.5.93	255.255.255.224	10.9.5.94-10.9.5.99	10.9.5.100
3	10.9.5.101	255.255.255.224	10.9.5.102-10.9.5.107	10.9.5.108
4	10.9.5.109	255.255.255.224	10.9.5.108-10.9.5.115	10.9.5.116
5	10.9.5.117	255.255.255.224	10.9.5.118-10.9.5.125	10.9.5.124
6	10.9.5.125	255.255.255.224	10.9.5.126-10.9.5.131	10.9.5.132

7	10.9.5.133	255.255.255.224	10.9.5.134-10.9.5.139	10.9.5.140
8	10.9.5.141	255.255.255.224	10.9.5.142-10.9.5.147	10.9.5.148
9	10.9.5.149	255.255.255.224	10.9.5.150-10.9.5.155	10.9.5.156
10	10.9.5.157	255.255.255.224	10.9.5.158-10.9.5.163	10.9.5.164

Floor 6

Room	Network address	Subnet mask	Usable Ip	Broadcast address
1	10.9.5.165	255.255.255.224	10.9.5.166-10.9.5.171	10.9.5.172
2	10.9.5.173	255.255.255.224	10.9.5.174-10.9.5.179	10.9.5.180
3	10.9.5.181	255.255.255.224	10.9.5.182-10.9.5.187	10.9.5.188
4	10.9.5.189	255.255.255.224	10.9.5.190-10.9.5.195	10.9.5.196
5	10.9.5.197	255.255.255.224	10.9.5.198-10.9.5.203	10.9.5.204
6	10.9.5.205	255.255.255.224	10.9.5.206-10.9.5.211	10.9.5.212
7	10.9.5.213	255.255.255.224	10.9.5.214-10.9.5.219	10.9.5.220
8	10.9.5.221	255.255.255.224	10.9.5.222-10.9.5.227	10.9.5.228
9	10.9.5.229	255.255.255.224	10.9.5.230-10.9.5.235	10.9.5.236
10	10.9.5.237	255.255.255.224	10.9.5.238-10.9.5.243	10.9.5.244

Access Point Management

10	10.9.5.25	255.255.255.248	10.9.5.215-10.9.5.31	10.9.5. 32
8	10.9.5.33			

VLAN Configuration for Network Topology

The network topology is broken into multiple segments to cater for traffic and security purpose thus multiple vlan is created for this assignment which includes guest wifi, cameras, IpTv and network management.

Lets look at the main vlan design :

1. VLAN 10 – Guest Wi-Fi:
    - Purpose: This VLAN is dedicated to guest Wi-Fi access. Devices connecting to the "Pullman Guest" SSID will be assigned to this VLAN.
    - Devices: Laptops, tablets, and mobile devices connecting to the Wi-Fi.
    - Ports: Access ports for guest access points are configured for VLAN 10.
    - Security: ACLs are configured to restrict access to other VLANs, especially IPTV (VLAN 20) and Camera (VLAN 30).
2. VLAN 20 – IPTV:
    - Purpose: This VLAN is reserved for the IPTV system. Each floor has its own access point for IPTV .
    - Devices: smart TVs.
    - Ports: Access points for IPTV are connected to ports assigned to VLAN 20.
    - QoS: Quality of Service (QoS) settings are applied to ensure IPTV traffic has priority over general network traffic.
3. VLAN 30 – Cameras:
    - Purpose: This VLAN is dedicated to the camera systems throughout the hotel. Each floor has access points that connects over wifi with the camras, and the "Pullman Camera" SSID is utilize for this Vlan.
    - Devices: IP cameras.
    - Ports: Camera access points are connected to switch ports configured for VLAN 30.
    - QoS: Qos is configure to provide high quality of camera services like recording .

. other vlan are done in the packet tracer

VLAN Trunking and Inter-VLAN Communication

To ensure that VLANs are carried across the network infrastructure, VLAN trunking is implemented between the switches:

1. VLAN Trunk Links:

- Trunk links are configured between the core switch in the data center (Level 1) and the floor distribution switches.
- Each trunk link is set to carry traffic from VLAN 10, 20, 30, can communicate across different floors.

2. Inter-VLAN Routing:
    - A Layer 3 core switch or router is configured to route traffic between VLANs. However, ACLs will be applied to limit inter-VLAN communication, allowing only necessary management traffic and preventing guests from accessing the IPTV and Camera VLANs.

Quality of Service (QoS) Configuration

QoS is implemented across the network like IPTV and Camera to ensure high quality of services being provided over the guest wifi.

- IPTV (VLAN 20): ensuring high quality and smooth video streaming for guests.
- Cameras (VLAN 30): real-time video streams with high quality and clear video recordings for security purposes.
- Guest Wi-Fi (VLAN 10): low configuration as guest should not have more priority over others.

Security and ACLs

To implement extra layer of security ACL are utilized to prevent access.

- Guests (VLAN 10): placing restriction to access the IPTV and Cameras in the hotel, as users should not have that priority. They should only have internet access.

Configuration for VLANs

Switch Configuration

```
en
config  terminal
```

Creating the VLANs

```
vlan 10
 name Pullman_Guest
vlan 20
 name Pullman_IPTV
vlan 30
name Pullman_Camera
```

Assigning ports to VLANs to each of the switch in the hotel

```
interface fa0/1
 switchport mode access
 switchport access vlan 10   # Guest Wi-Fi VLAN

interface range fa0/11
 switchport mode access
 switchport access vlan 20   # to IPTV VLAN

interface range fa0/16
 switchport mode access
 switchport access vlan 30   # Cameras VLAN
```

Configuring trunk to connect to core switch

```
interface range fa2/1-fa7/1
```

```
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30
```

3. Router Configuration

```
en
config t

# Create sub-interfaces for each VLAN
interface gig0/0.10
 encapsulation dot1Q 10
 ip address 10.9.1.1 255.255.255.0   # Gateway for Guest Wi-Fi

interface gig0/0.20
 encapsulation dot1Q 20
 ip address 10.9.2.1 255.255.255.0   # Gateway for IPTV

interface gig0/0.30
 encapsulation dot1Q 30
 ip address 10.9.3.1 255.255.255.0   # Gateway for Cameras

# Enable routing between VLANs
ip routing
```

Applying QoS for IPTV and Cameras

```
en
config t

# For IPTV VLAN
class-map match-any IPTV_Class
```

```
 match access-group 20

policy-map IPTV_Policy
 class IPTV_Class
  priority 2000  # Sets priority for IPTV traffic

# For Cameras VLAN
class-map match-any Camera_Class
 match access-group 30

policy-map Camera_Policy
 class Camera_Class
  priority 1500
service-policy output IPTV_Policy
 service-policy output Camera_Policy
```

Configuring ACLs to Restrict Guest Access

```
access-list 101 deny icmp 10.9.0.1 0.0.3.255 10.9.4.68 0.0.0.31
access-list 101 deny icmp 10.9.0.1 0.0.3.255 10.9.4.4 0.0.0.63
access-list 101 permit ip any any
int g9/0
ip access-group 101 in

access-list 101 deny icmp 10.9.4.100 0.0.0.7 10.9.4.68 0.0.0.31
access-list 101 permit icmp 10.9.4.100 0.0.0.7 10.9.4.4 0.0.0.63
access-list 101 permit ip any any
int g9/0.10
ip access-group 101 in
```

access-list 101 deny icmp 10.9.4.124 0.0.0.7 10.9.4.68 0.0.0.31

access-list 101 permit icmp 10.9.4.124 0.0.0.7 10.9.4.4 0.0.0.63

access-list 101 permit ip any any

int g9/0.10

ip access-group 101 in

access-list 101 deny icmp 10.9.4.196 0.0.0.7 10.9.4.68 0.0.0.31

access-list 101 permit icmp 10.9.4.196 0.0.0.7 10.9.4.4 0.0.0.63

access-list 101 permit ip any any

int g9/0.10

ip access-group 101 in

access-list 101 deny icmp 10.9.4.204 0.0.0.7 10.9.4.68 0.0.0.31

access-list 101 permit icmp 10.9.4.204 0.0.0.7 10.9.4.4 0.0.0.63

access-list 101 permit ip any any

int g9/0.10

ip access-group 101 in

Conclusion

This VLAN configuration ensures efficient traffic management and security within the Pullman Group hotel network. By segmenting the network into specific VLANs for guest access, IPTV, camera systems, and network management, the design meets the key operational requirements while providing security and service prioritization through QoS. Static IP addressing guarantees that all devices have consistent and predictable IP configurations, simplifying network management.