Hotel System Network Design :

The following are part of the considerations during the design and implementation:

- There should be three routers connecting each floor
  (all placed in the server room in IT department).
- All routers should be connected to each other using serial DCE cable.
- The network between the routers should be 10.10.10.0/30,10.10.10.4/30 and 10.10.10.8/30.
- Each floor is expected to have one switch (placed in the respective floor).
- Each floor is expected to have WIFI networks connected to laptops and phones.
- Each department is expected to have a printer.
- Each department is expected to be in different VLAN with the following details;

1st Floor:
- Reception- VLAN 80, Network of 192.168.8.0/24
- Store- VLAN 70, Network of 192.168.7.0/24
- Logistics- VLAN 60, Network of 192.168.6.0/24

2nd Floor:
- Finance- VLAN 50, Network of 192.168.5.0/24
- HR- VLAN 40, Network of 192.168.4.0/24
- Sales- VLAN 30, Network of 192.168.3.0/24

3rd Floor:
- Admin- VLAN 20, Network of 192.168.2.0/24
- IT- VLAN 10, Network of 192.168.1.0/24

- Useing OSPF as the routing protocol to advertise routes.
- All devices in the network are expected to obtain IP address dynamically with their
  respective router configured as the DHCP server.
- All the devices in the network are expected to communicate with each other.
- Configuring SSH in all the routers for remote login.
- In IT department, add PC called Test-PC to port fa0/1 and use it to test remote login.
- Configuring port security to IT-dept switch to allow only Test-PC to access port fa0/1
  (use sticky method to obtain mac-address with violation mode of shutdown.)

Technologies Implemented:
-Creating a network topology using Cisco Packet Tracer.
-Hierarchical Network Design.
-Connecting Networking devices with Correct cabling.
-Creating VLANs and assigning ports VLAN numbers.
-Subnetting and IP Addressing.
-Configuring Inter-VLAN Routing (Router on a stick).
-Configuring DHCP Server (Router as the DHCP Server).
-Configuring SSH for secure Remote access.
-Configuring switchport security or Port-Security on the switches.
-Configuring WLAN or wireless network (Cisco Access Point).
-Host Device Configurations.
-Test and Verifying Network Communication.

F1_Router Configuration:

```
enable
configure terminal
interface se0/0/0
no shutdown
exit
interface se0/0/1
```

```
no shutdown
exit
interface gig0/0
no shutdown
exit
interface se0/0/1
clock rate 64000
exit
do wr
interface se0/0/1
ip address 10.10.10.5 255.255.255.252
exit
interface se0/0/0
ip address 10.10.10.9 255.255.255.252
exit
do wr
interface gig0/0.80
encapsulation dot1Q 80
ip address 192.168.8.1 255.255.255.0
exit
interface gig0/0.70
encapsulation dot1Q 70
ip address 192.168.7.1 255.255.255.0
exit
interface gig0/0.60
encapsulation dot1Q 60
ip address 192.168.6.1 255.255.255.0
exit
do wr
service dhcp
ip dhcp pool Reception
network 192.168.8.0 255.255.255.0
default-router 192.168.8.1
dns-server 192.168.8.1
exit
service dhcp
ip dhcp pool Store
network 192.168.7.0 255.255.255.0
default-router 192.168.7.1
dns-server 192.168.7.1
exit
service dhcp
ip dhcp pool Logistics
network 192.168.6.0 255.255.255.0
default-router 192.168.6.1
dns-server 192.168.6.1
exit
do wr
router ospf 10
network 10.10.10.4 255.255.255.252 area 0
network 10.10.10.8 255.255.255.252 area 0
network 192.168.8.0 255.255.255.0 area 0
network 192.168.7.0 255.255.255.0 area 0
network 192.168.6.0 255.255.255.0 area 0
do wr
```

exit
hostname F1-Router
ip domain-name cisco
username cisco password cisco
crypto key generate rsa
1024
line vty 0 15
login local
transport input ssh
do wr
exit

F2_Router Configuration:

enable
configure terminal
interface se0/0/0
no shutdown
exit
interface se0/0/1
no shutdown
exit
interface gig0/0
no shutdown
exit
interface se0/0/1
clock rate 64000
exit
do wr
interface se0/0/1
ip address 10.10.10.10 255.255.255.252
exit
interface se0/0/0
ip address 10.10.10.1 255.255.255.252
exit
do wr
interface gig0/0.30
encapsulation dot1Q 30
ip address 192.168.3.1 255.255.255.0
exit
interface gig0/0.40
encapsulation dot1Q 40
ip address 192.168.4.1 255.255.255.0
exit
interface gig0/0.50
encapsulation dot1Q 50
ip address 192.168.5.1 255.255.255.0
exit
do wr
service dhcp
ip dhcp pool Sales/Marketing
network 192.168.3.0 255.255.255.0
default-router 192.168.3.1
dns-server 192.168.3.1

exit
service dhcp
ip dhcp pool HR
network 192.168.4.0 255.255.255.0
default-router 192.168.4.1
dns-server 192.168.4.1
exit
service dhcp
ip dhcp pool Finance
network 192.168.5.0 255.255.255.0
default-router 192.168.5.1
dns-server 192.168.5.1
exit
do wr
router ospf 10
network 10.10.10.0 255.255.255.252 area 0
network 10.10.10.8 255.255.255.252 area 0
network 192.168.3.0 255.255.255.0 area 0
network 192.168.4.0 255.255.255.0 area 0
network 192.168.5.0 255.255.255.0 area 0
do wr
exit
hostname F2-Router
ip domain-name cisco
username cisco password cisco
crypto key generate rsa
1024
line vty 0 15
login local
transport input ssh
do wr
exit

F3_Router Configuration:

enable
configure terminal
interface se0/0/0
no shutdown
exit
interface se0/0/1
no shutdown
exit
interface gig0/0
no shutdown
exit
interface se0/0/0
clock rate 64000
exit
do wr
interface se0/0/0
ip address 10.10.10.1 255.255.255.252
exit
interface se0/0/1

ip address 10.10.10.6 255.255.255.252
exit
do wr
interface gig0/0.10
encapsulation dot1Q 10
ip address 192.168.1.1 255.255.255.0
exit
interface gig0/0.20
encapsulation dot1Q 20
ip address 192.168.2.1 255.255.255.0
exit
do wr
service dhcp
ip dhcp pool IT
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 192.168.1.1
exit
ip dhcp pool Admin
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
dns-server 192.168.2.1
exit
do wr
router ospf 10
network 10.10.10.0 255.255.255.252 area 0
network 10.10.10.4 255.255.255.252 area 0
network 192.168.1.0 255.255.255.0 area 0
network 192.168.2.0 255.255.255.0 area 0
do wr
exit
hostname F3-Router
ip domain-name cisco
username cisco password cisco
crypto key generate rsa
1024
line vty 0 15
login local
transport input ssh
do wr
exit

F1_Switch Configuration:
enable
configure terminal
interface range fa0/2-3
switchport mode access
switchport access vlan 80
exit
interface range fa0/4-5
switchport mode access
switchport access vlan 70
exit
interface range fa0/6-8

```
switchport mode access
switchport access vlan 60
exit
interface range fa0/1
switchport mode trunk
do wr
```

F2_Switch Configuration:

```
enable
configure terminal
interface range fa0/2-3
switchport mode access
switchport access vlan 40
exit
interface range fa0/4-5
switchport mode access
switchport access vlan 50
exit
interface range fa0/6-8
switchport mode access
switchport access vlan 30
exit
interface range fa0/1
switchport mode trunk
do wr
```

F3_Switch Configuration:

```
enable
configure terminal
interface range fa0/2-3
switchport mode access
switchport access vlan 10
exit
interface range fa0/4-6
switchport mode access
switchport access vlan 20
exit
interface range fa0/1
switchport mode trunk
do wr
interface fa0/2
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation shutdown
do wr
```

SSH Remote login test on Test-Pc command:

```
ssh -l cisco 10.10.10.1
```

password : cisco

WAP configuration:
Floor1 WAP:
 SSID : floor1
 Password : WPA2-PSK
 PSK pass phrase: floor1@123
 Channel : 1

Floor2 WAP:
 SSID : floor2
 Password : WPA2-PSK
 PSK pass phrase: floor2@123
 Channel : 6
Floor3 WAP:
 SSID : floor3
 Password : WPA2-PSK
 PSK pass phrase: floor3@123
 Channel : 11
