

Small Business Network

Project No. 8

Team members:

1- Ahmed Shaban Abo-Elfaddle

2- Ahmed Ashraf Mokhtar

3- Hana Ashraf Badea

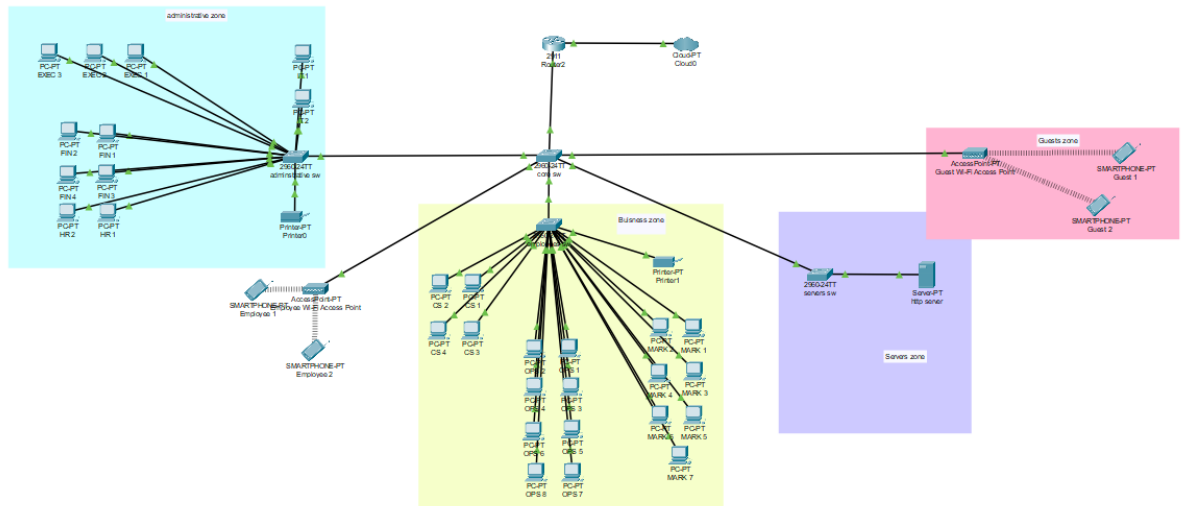
4- Hassan Hesham Eldein Hassan

5- Yoliana Adel Isaac

6- Malak Emad Amin

1. Network Topology & IP Addressing

- **Network Diagram:**



- **Segmentation & IP Addressing Scheme:**

VLAN ID	VLAN Name	IP Range	Devices
10	Management	192.168.10.0/24	Executive (3), IT Support (2)
20	Finance & HR	192.168.20.0/24	Finance & Accounting (4), Human Resources (2)
30	Sales & Marketing	192.168.30.0/24	Sales & Marketing (7)
40	Operations	192.168.40.0/24	Operations / Production (8)
50	Customer Service	192.168.50.0/24	Customer Service (4)
60	Servers	192.168.60.0/24	File Server, Print Server, etc.
70	Printers	192.168.70.0/24	Network Printers
100	Guest	192.168.100.0/24	Guest Wi-Fi & Employees Wi-Fi

- **Device Types:**

- **Routers:** 1 router (2911 model)
- **Switches:** 4 switches (2960-24TT model)
- **APS:** 2 APS (AccessPoint-PT model)

2. Security Measures

- **ACL Rules:** used an extended ACL to allow DHCP IP assignment from the router and to block the access of the external network to the internal network with the allowance to access the business's website
- **Network Segmentation:** segmented the network in a way to close facilitate the communication of the employees of the same or close departments with the allowance of different departments communication through layer 3

- **VPN Setup:** only allowed to the IT employees on the routers and switches for remote troubleshooting on the network

3. Device Configuration & Implementation

- **Router & Switch Configuration:** Have you documented the configuration steps for the routers, switches, and wireless access points?
- **Routing Protocols:** used static routing to route the packets through the specified sub-interface for each vlan

```
interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
 ip access-group END in
 ip access-group END out
!
interface GigabitEthernet0/1.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 ip access-group END in
 ip access-group END out
!
interface GigabitEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip access-group END in
 ip access-group END out
!
interface GigabitEthernet0/1.40
 encapsulation dot1Q 40
 ip address 192.168.40.1 255.255.255.0
 ip access-group END in
 ip access-group END out
!
interface GigabitEthernet0/1.50
 encapsulation dot1Q 50
 ip address 192.168.50.1 255.255.255.0
 ip access-group END in
 ip access-group END out
!
interface GigabitEthernet0/1.60
 encapsulation dot1Q 60
 ip address 192.168.60.1 255.255.255.0
 ip access-group END in
 ip access-group END out
```

```

interface GigabitEthernet0/1.70
  encapsulation dot1Q 70
  ip address 192.168.70.1 255.255.255.0
  ip access-group END in
  ip access-group END out
!
interface GigabitEthernet0/1.100
  encapsulation dot1Q 100
  ip address 192.168.100.1 255.255.255.0
  ip access-group END in
  ip access-group END out

```

- **ACL Configurations:**

```

ip access-list extended END
  permit udp any eq bootpc any eq bootps
  permit udp any eq bootps any eq bootpc
  permit ip 192.168.60.0 0.0.0.255 any
  permit ip any 192.168.60.0 0.0.0.255
  deny ip 192.168.0.0 0.0.255.255 192.168.100.0 0.0.0.255
  deny ip 192.168.100.0 0.0.0.255 192.168.0.0 0.0.255.255
  permit ip any any
  deny ip any any

```

4. Security Hardening:

- setup a password to access any of level 2&3 network device

```

Switch#confi
Switch#configure
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#lin
Switch(config)#line cos
Switch(config)#line con
Switch(config)#line console 0
Switch(config-line)#pas
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#ena
Switch(config)#enable se
Switch(config)#enable secret pas
Switch(config)#enable secret class
Switch(config)#lin
Switch(config)#line vty
Switch(config)#line vty 0 15
Switch(config-line)#pas
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#ser
Switch(config)#service pas
Switch(config)#service password-encryption
Switch(config)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#cop
Switch#copy ru
Switch#copy running-config st
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#reloa
Switch#reload

```

- and isolating the internal network by not making it accessible without a physical access except the server to allow external users to access the website of the business
- All unused ports are off