CSCI 5010 – Fundamentals of Data Communications

Lab 8
Wireless Lab

University of Colorado Boulder
Department of Computer Science

Professor Levi Perigo, Ph.D.

Objectives

- Learn how wireless (Wi-Fi) technology works.
- Learn how to simulate roaming in wireless network.
- Learn how to configure wireless networks.
- Learn about wireless security protocols.

Summary

Wireless LANs enable users to communicate without the need cables. Each WLAN needs a wireless Access Point (AP) to transmit and receive data. Unlike a wired network which operates at full-duplex (send and receive at the same time), a wireless network operates at half-duplex, so sometimes an AP is referred as a Wireless Hub.

This lab will provide a basic understanding of configuring wireless networks that comprise of AP's, a switch, and a router on Cisco Packet Tracer. IPv4 DHCP scopes will be created for the new users connecting to the wireless network. The lab expands on the "Router-on-a-Stick framework to include roaming scenarios in WLAN networks.

Objective 1: Creation of wireless topology in Cisco Packet Tracer (CPT)

1. Please create the following topology (Figure 1) in CPT:

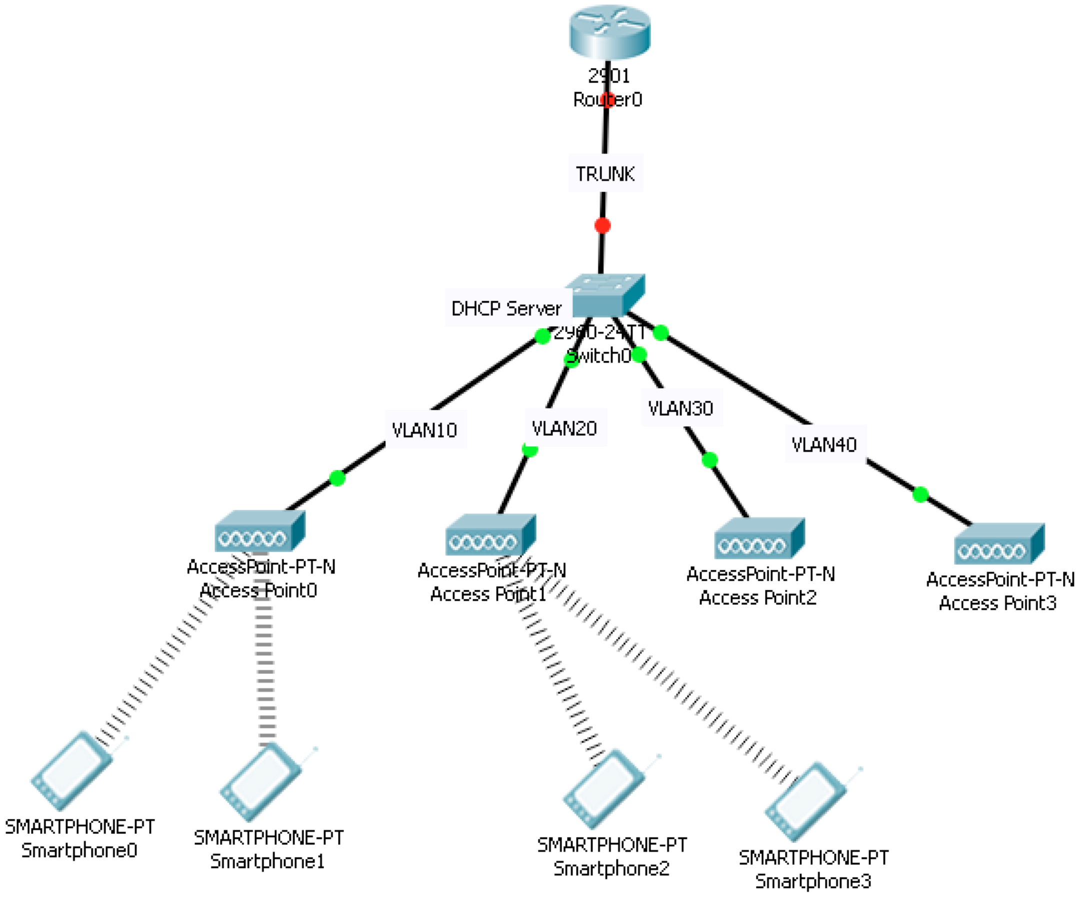
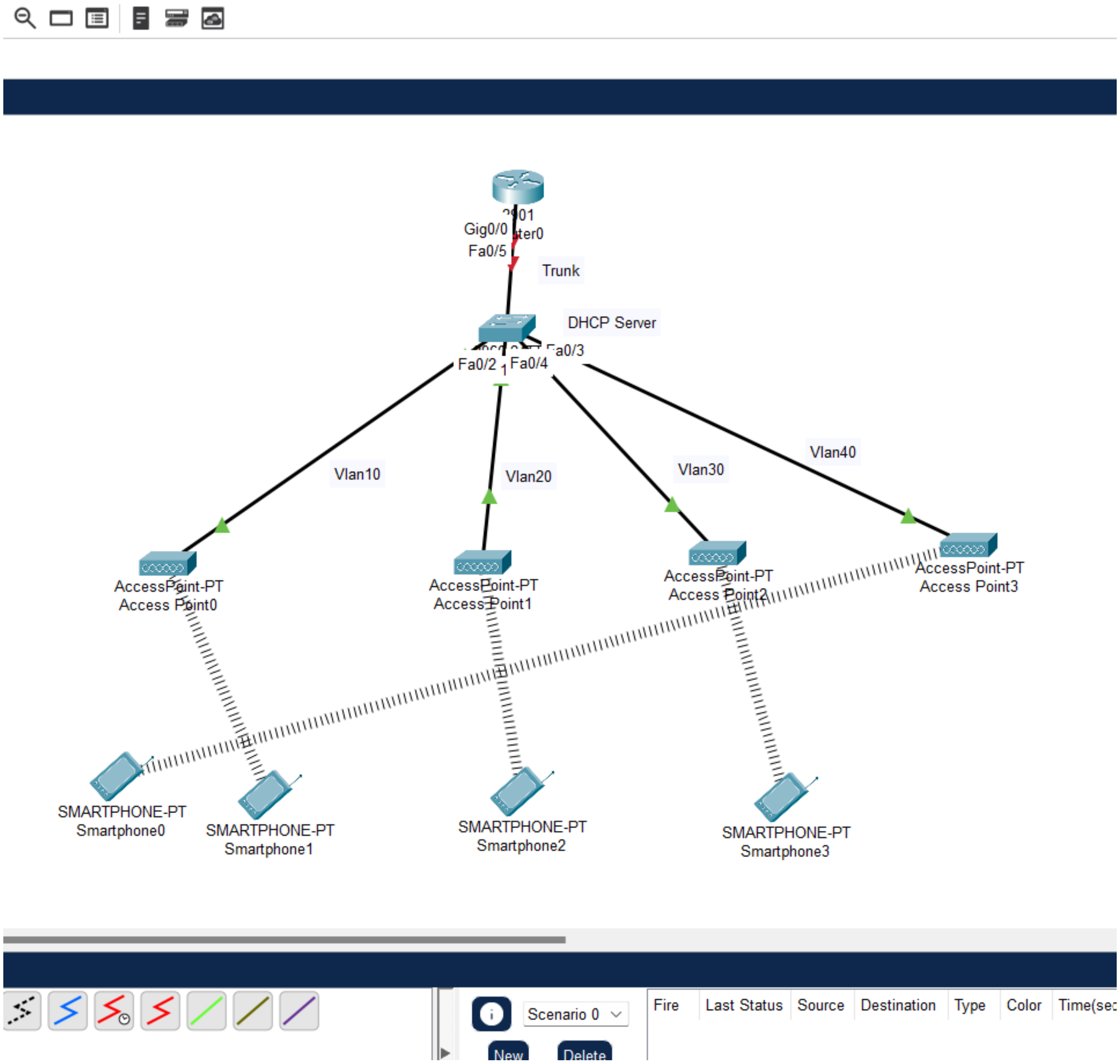


Figure 1: Wireless topology

2. The Access Points (AP’s) and wireless terminals (Smartphones) are located in the “Wireless Devices” section of CPT. Please drag and drop appropriately as indicated in Figure 1. The wireless terminals may connect randomly to AP’s. Please disregard it at this point. Paste the screenshot of the created topology from CPT **[20 points]**.

Ans: The wireless terminals may connect randomly to AP’s. Please disregard it at this point – YES! The wireless terminals were connecting randomly to AP’s

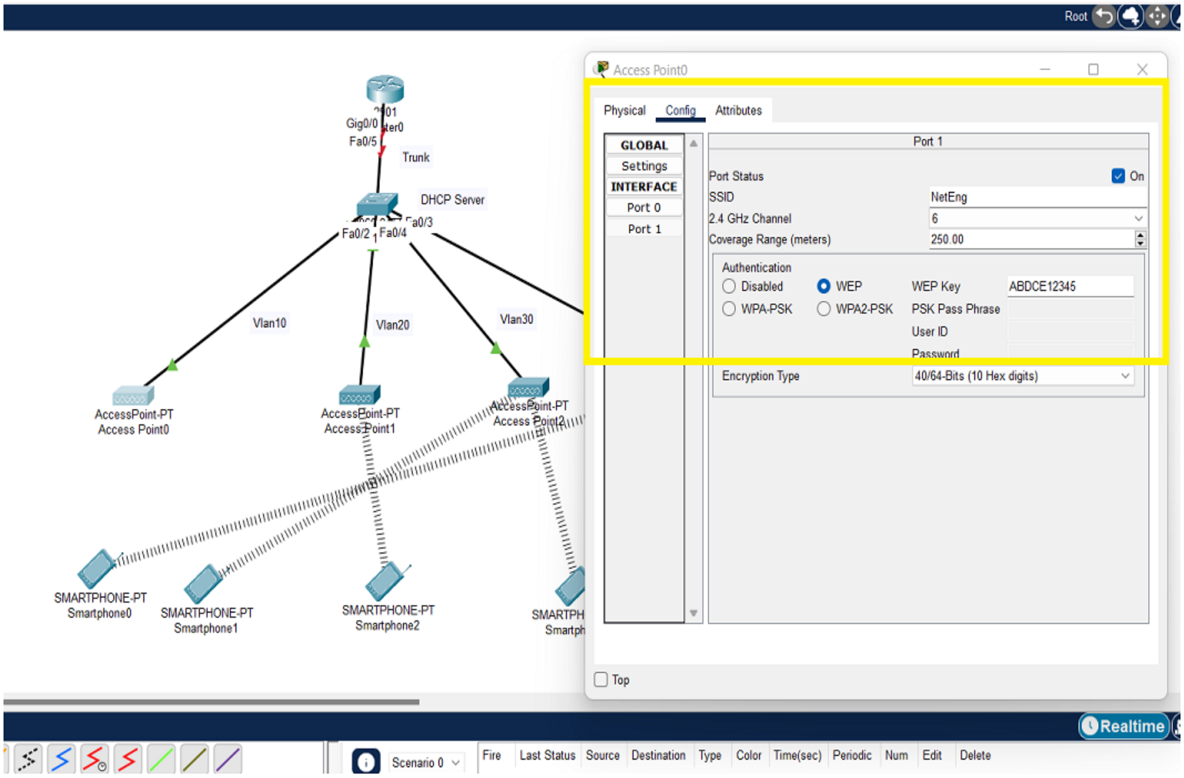


Objective 2: Wireless Network Configuration

1. Access Point and Smartphone configuration

   a. Configure AP0 in a way that its SSID is “NetEng,” and works on channel no. 6, coverage as “250 meters,” and WEP Authentication key as “ABDCE12345.” Similarly, Smartphones 0 and 1 should be configured to authenticate to “NetEng” with WEP key as “ABCDE12345.” Paste screenshot of configuration. **[10 points]**

Ans: SSID: NetEng, Channel No. 6 , Coverage: 250mts, WEP: ABDCE12345



Port 1

Port Status ☑ On

SSID: NetEng

2.4 GHz Channel: 6

Coverage Range (meters): 250.00

Authentication

○ Disabled ● WEP

○ WPA-PSK ○ WPA2-PSK

WEP Key: ABDCE12345

PSK Pass Phrase:

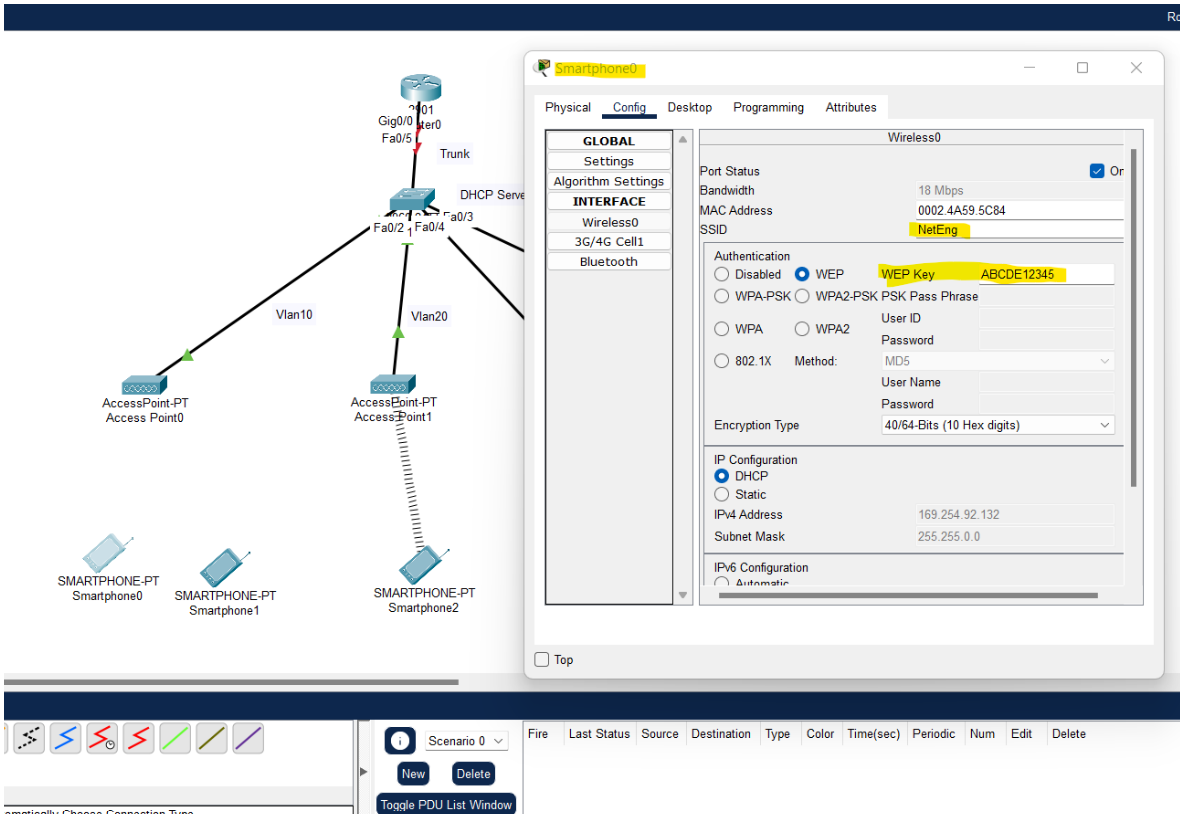
User ID:

Password:

Encryption Type: 40/64-Bits (10 Hex digits)

Similarly, Smartphones 0 and 1 should be configured to authenticate to “NetEng” with WEP key as “ABCDE12345.” Paste screenshot of configuration

Ans :: SmartPhone 0



Smartphone0

Physical | Config | Desktop | Programming | Attributes

GLOBAL
Settings
Algorithm Settings
INTERFACE
Wireless0
3G/4G Cell1
Bluetooth

Wireless0

Port Status ☑ On
Bandwidth 18 Mbps
MAC Address 0002.4A59.5C84
SSID NetEng

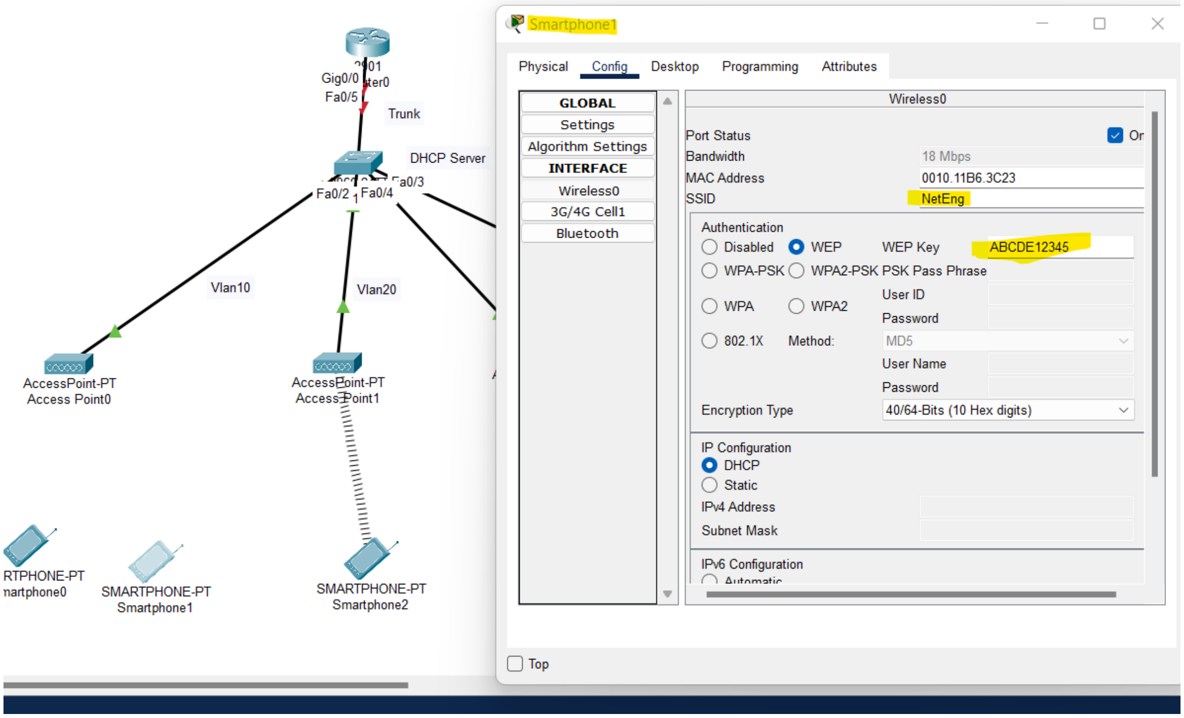
Authentication
○ Disabled ● WEP WEP Key ABCDE12345
○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase
○ WPA ○ WPA2 User ID
Password
○ 802.1X Method: MD5
User Name
Password
Encryption Type 40/64-Bits (10 Hex digits)

IP Configuration
● DHCP
○ Static
IPv4 Address 169.254.92.132
Subnet Mask 255.255.0.0

IPv6 Configuration
○ Automatic

□ Top

Ans : SmartPhone 1



Smartphone1

Physical | Config | Desktop | Programming | Attributes

GLOBAL
Settings
Algorithm Settings
INTERFACE
Wireless0
3G/4G Cell1
Bluetooth

Wireless0

Port Status ☑ On
Bandwidth 18 Mbps
MAC Address 0010.11B6.3C23
SSID NetEng

Authentication
○ Disabled ● WEP WEP Key ABCDE12345
○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase
○ WPA ○ WPA2 User ID
Password
○ 802.1X Method: MD5
User Name
Password
Encryption Type 40/64-Bits (10 Hex digits)

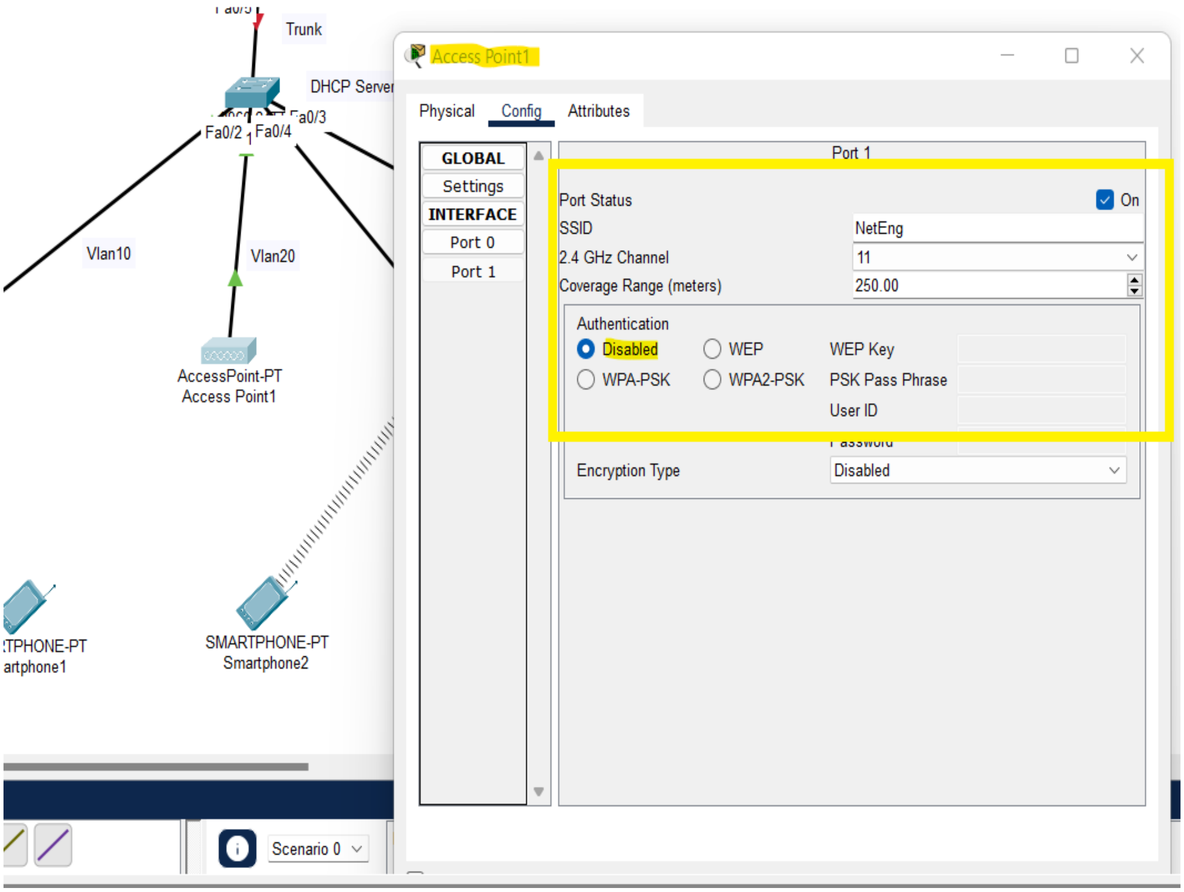
IP Configuration
● DHCP
○ Static
IPv4 Address
Subnet Mask

IPv6 Configuration
○ Automatic

□ Top

b. Configure AP1 in a way that its SSID is “NetEng,” works on channel no. 11, coverage as “250 meters,” and Authentication as “Disabled.” Similarly, Smartphones 2 and 3 should be configured to connect with “NetEng” with no Authentication. Paste screenshot of configuration. **[10 points]**

Ans: SSID – NetEng, Channel – 11, Auth - Disabled



Access Point1

Physical | Config | Attributes

GLOBAL
Settings
INTERFACE
Port 0
Port 1

Port 1

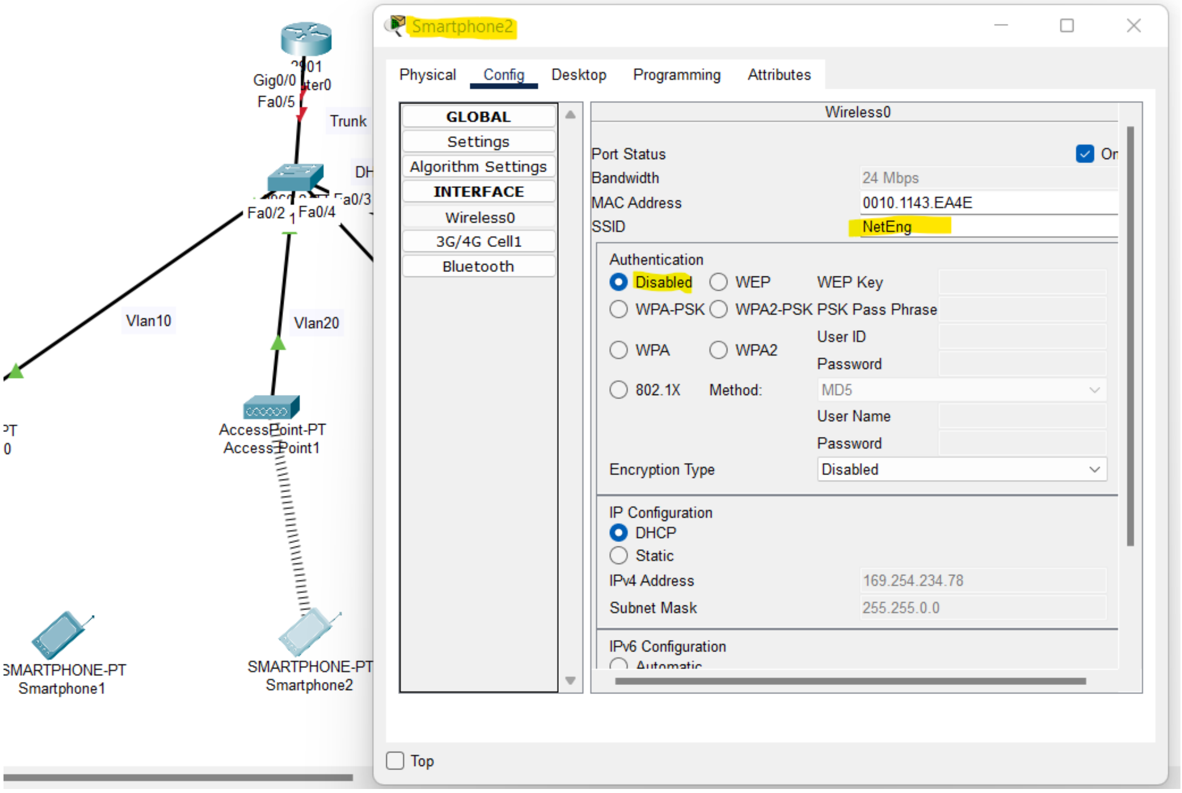
Port Status ☑ On
SSID: NetEng
2.4 GHz Channel: 11
Coverage Range (meters): 250.00

Authentication
● Disabled ○ WEP WEP Key
○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase
User ID
Password

Encryption Type: Disabled

Similarly, Smartphones 2 and 3 should be configured to connect with “NetEng” with no Authentication. Paste screenshot of configuration

Smartphone -2



Smartphone2

Wireless0

Port Status ☑ On

Bandwidth 24 Mbps

MAC Address 0010.1143.EA4E

SSID NetEng

Authentication

● Disabled ○ WEP WEP Key

○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase

○ WPA ○ WPA2 User ID

Password

○ 802.1X Method: MD5

User Name

Password

Encryption Type Disabled

IP Configuration

● DHCP

○ Static

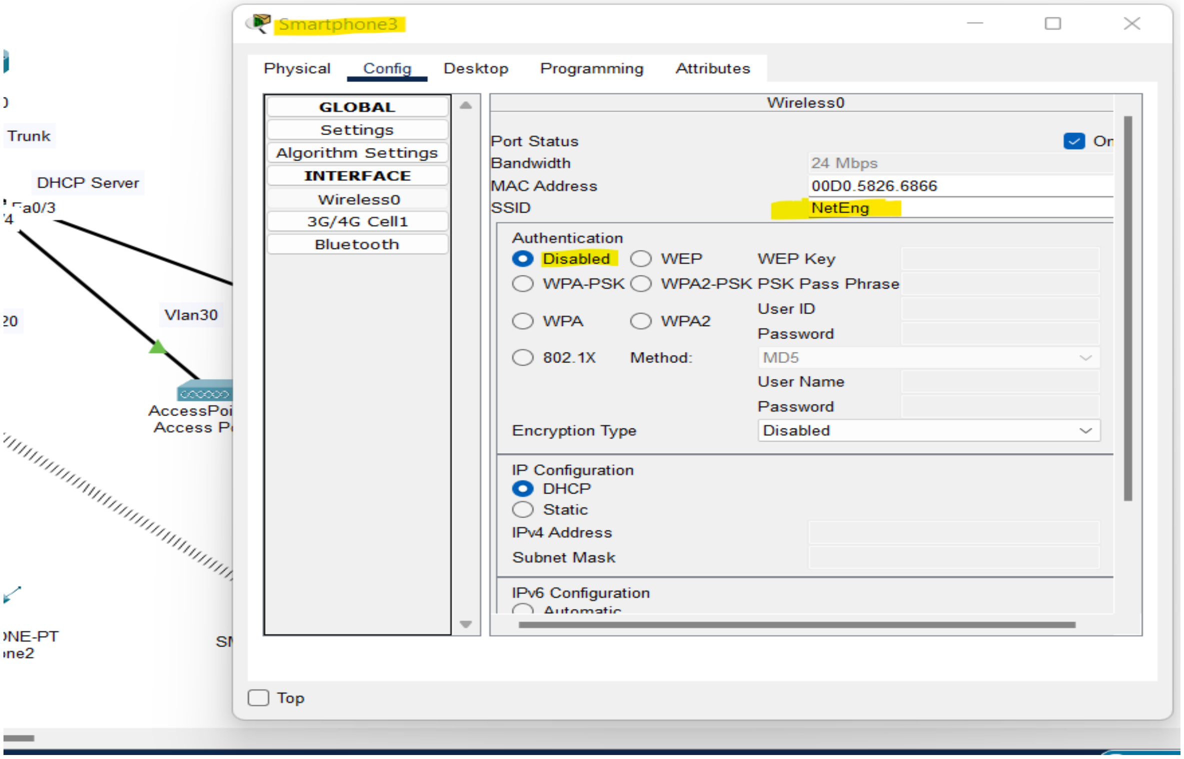
IPv4 Address 169.254.234.78

Subnet Mask 255.255.0.0

IPv6 Configuration

○ Automatic

SmartPhone 3:



Smartphone3

Wireless0

Port Status ☑ On

Bandwidth 24 Mbps

MAC Address 00D0.5826.6866

SSID NetEng

Authentication

● Disabled ○ WEP WEP Key

○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase

○ WPA ○ WPA2 User ID

Password

○ 802.1X Method: MD5

User Name

Password

Encryption Type Disabled

IP Configuration

● DHCP

○ Static

IPv4 Address

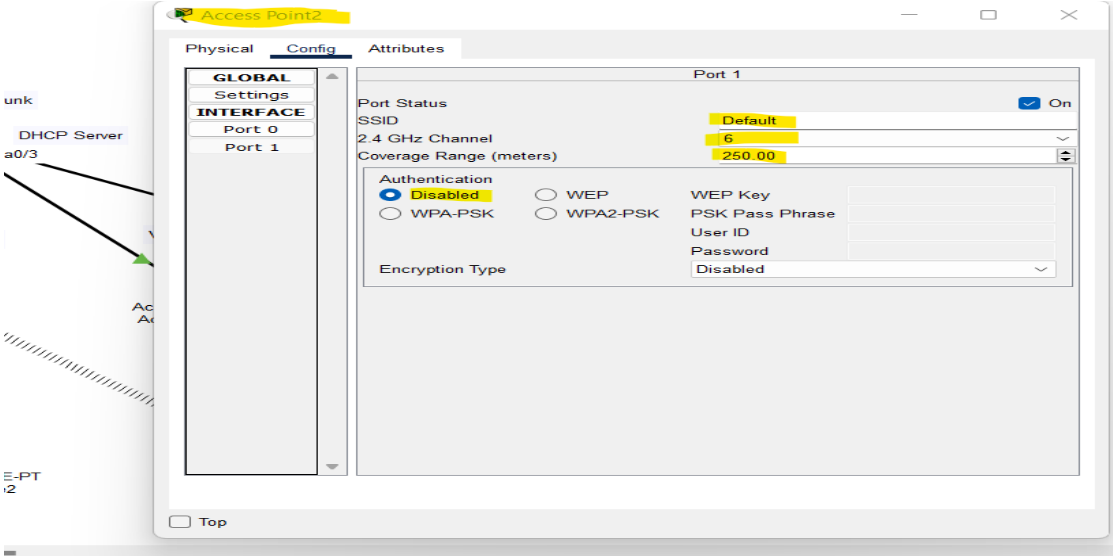
Subnet Mask

IPv6 Configuration

○ Automatic

c. Configure AP2 in a way that its SSID is “Default,” works on channel no. 6, coverage as “250 meters,” and Authentication as “Disabled.” Paste screenshot of configuration. **[10 points]**

Access Point 2



Port 1

Port Status ☑ On

SSID: Default

2.4 GHz Channel: 6

Coverage Range (meters): 250.00

Authentication

● Disabled ○ WEP ○ WPA-PSK ○ WPA2-PSK

WEP Key

PSK Pass Phrase

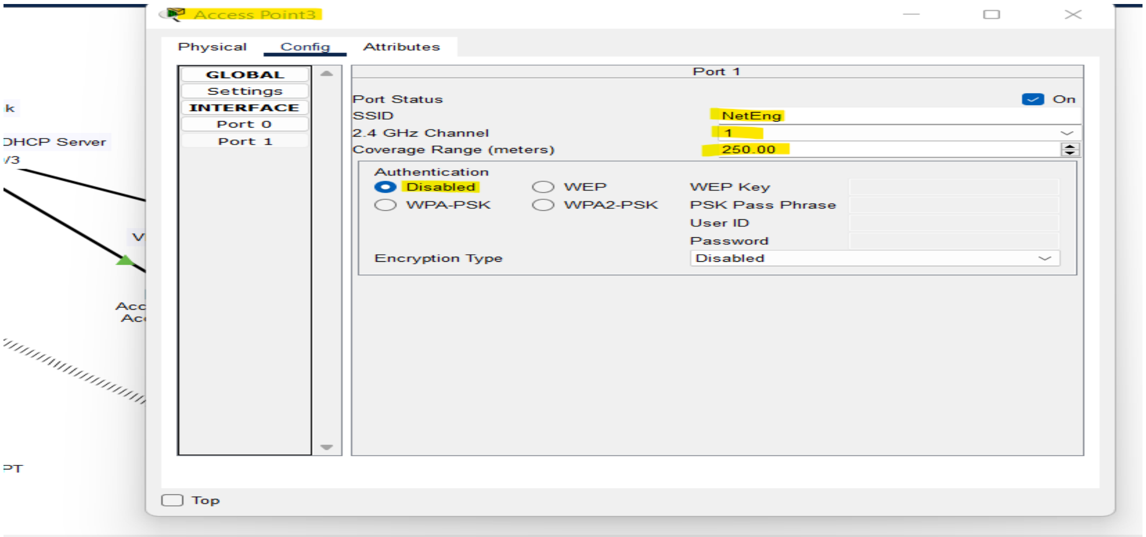
User ID

Password

Encryption Type: Disabled

d. Configure AP3 in a way that its SSID is “NetEng,” works on channel no. 1, coverage as “250 meters,” and Authentication as “Disabled.” Paste screenshot of configuration. **[10 points]**

Access Point 3



Port 1

Port Status ☑ On

SSID: NetEng

2.4 GHz Channel: 1

Coverage Range (meters): 250.00

Authentication

● Disabled ○ WEP ○ WPA-PSK ○ WPA2-PSK

WEP Key

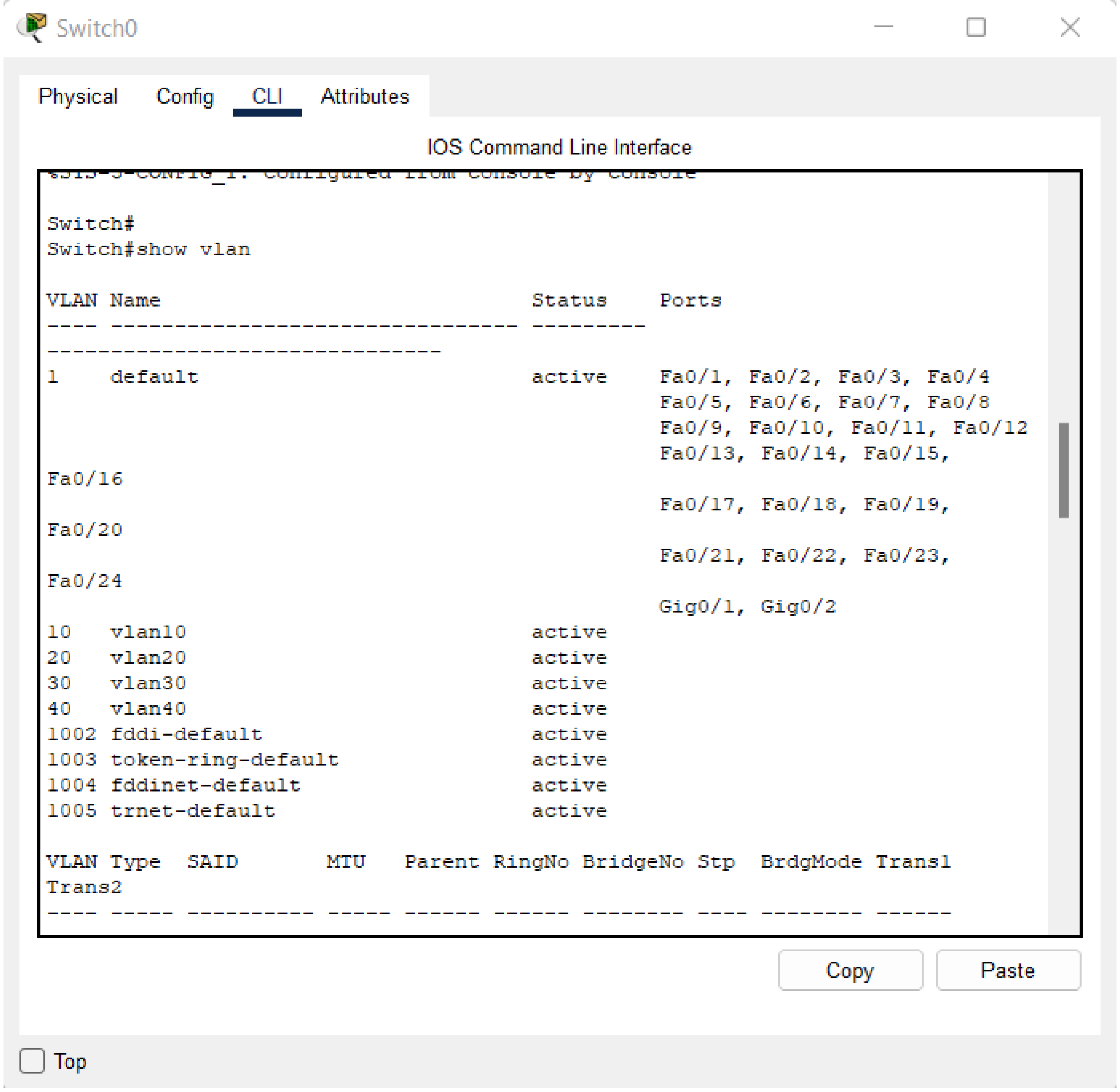
PSK Pass Phrase

User ID

Password

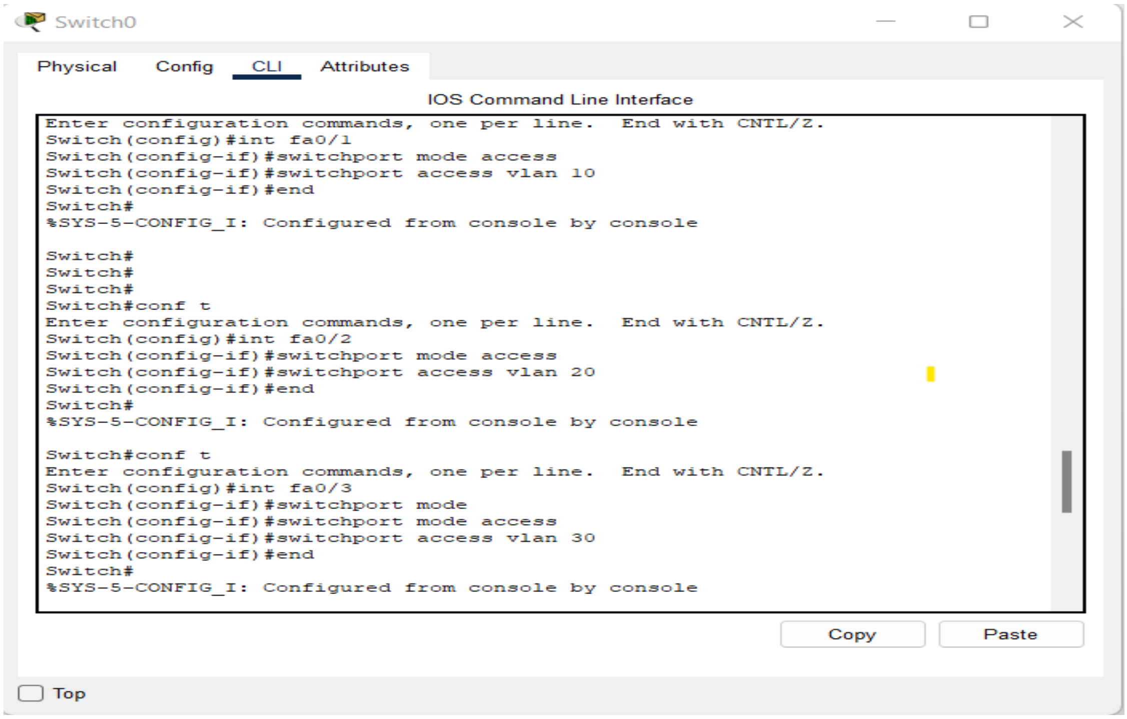
Encryption Type: Disabled

2. Configure Cisco switch 0 in a fashion that each of its four switch ports are in separate VLAN’s as shown in Figure 1 and the port connected to the router 0 as “TRUNK” port. Additionally, configure the switch as DHCP server having four different pools for it to assign IP addresses for the connecting wireless devices/terminals. Paste the screenshot of configuration window of all Smartphones highlighting received DHCP address. **[20 points]**



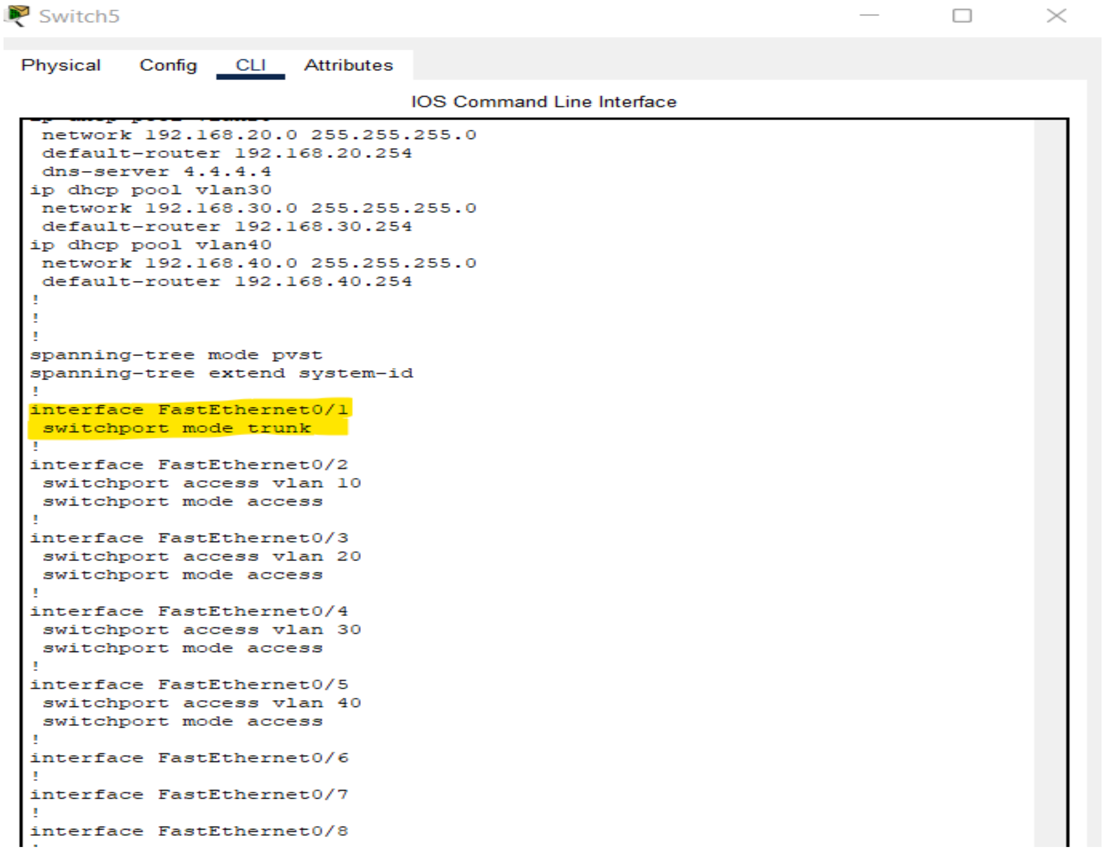
```
%SYS-5-CONFIG_I: Configured from console by console

Switch#
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15,
Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19,
Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23,
Fa0/24
                                                Gig0/1, Gig0/2
10   vlan10                           active
20   vlan20                           active
30   vlan30                           active
40   vlan40                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1
Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------
```

Creating separate VLAN’s on interfaces using access port



```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/3
Switch(config-if)#switchport mode
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

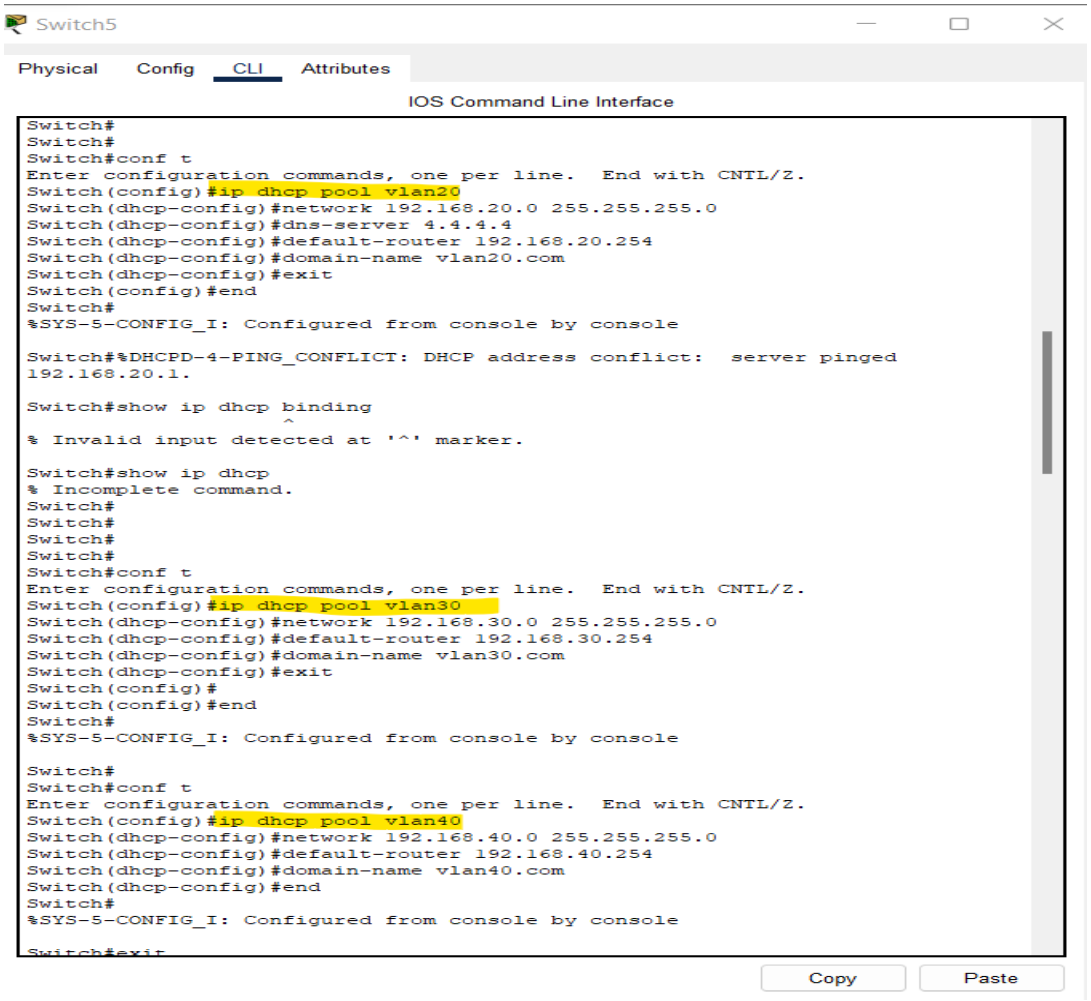
and the port connected to the router 0 as “TRUNK” port



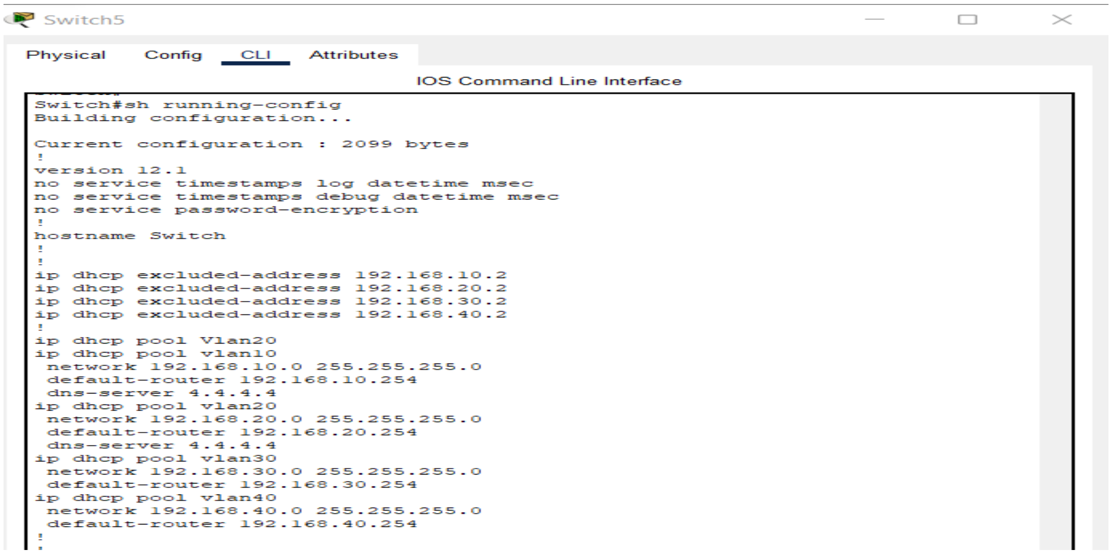
```
ip dhcp pool vlan20
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.254
 dns-server 4.4.4.4
ip dhcp pool vlan30
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.254
ip dhcp pool vlan40
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.254
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
```

Additionally, configure the switch as DHCP server having four different pools for it

to assign IP addresses for the connecting wireless devices/terminals

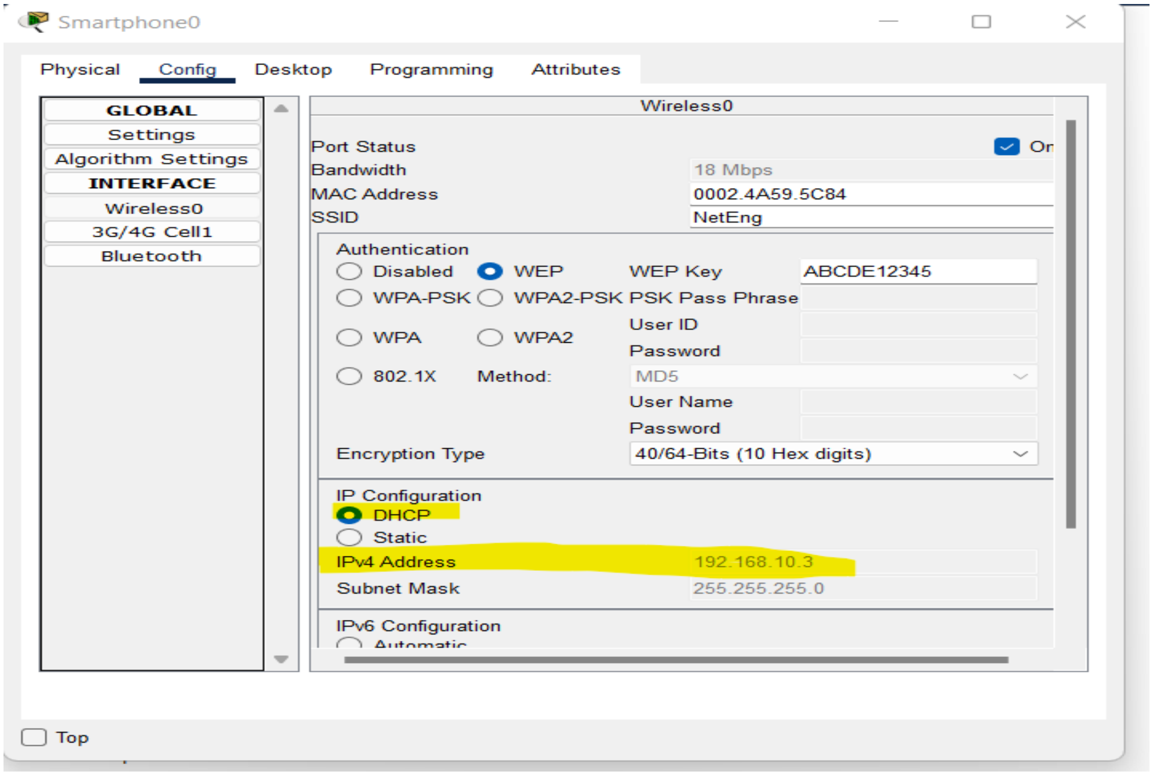


```
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp pool vlan20
Switch(dhcp-config)#network 192.168.20.0 255.255.255.0
Switch(dhcp-config)#dns-server 4.4.4.4
Switch(dhcp-config)#default-router 192.168.20.254
Switch(dhcp-config)#domain-name vlan20.com
Switch(dhcp-config)#exit
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged
192.168.20.1.

Switch#show ip dhcp binding
                    ^
% Invalid input detected at '^' marker.

Switch#show ip dhcp
% Incomplete command.
Switch#
Switch#
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp pool vlan30
Switch(dhcp-config)#network 192.168.30.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.30.254
Switch(dhcp-config)#domain-name vlan30.com
Switch(dhcp-config)#exit
Switch(config)#
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp pool vlan40
Switch(dhcp-config)#network 192.168.40.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.40.254
Switch(dhcp-config)#domain-name vlan40.com
Switch(dhcp-config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#exit
```



```
Switch#sh running-config
Building configuration...

Current configuration : 2099 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
ip dhcp excluded-address 192.168.10.2
ip dhcp excluded-address 192.168.20.2
ip dhcp excluded-address 192.168.30.2
ip dhcp excluded-address 192.168.40.2
!
ip dhcp pool Vlan20
ip dhcp pool vlan10
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.254
 dns-server 4.4.4.4
ip dhcp pool vlan20
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.254
 dns-server 4.4.4.4
ip dhcp pool vlan30
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.254
ip dhcp pool vlan40
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.254
!
!
```

Paste the screenshot of configuration window of all Smartphones highlighting received DHCP address.



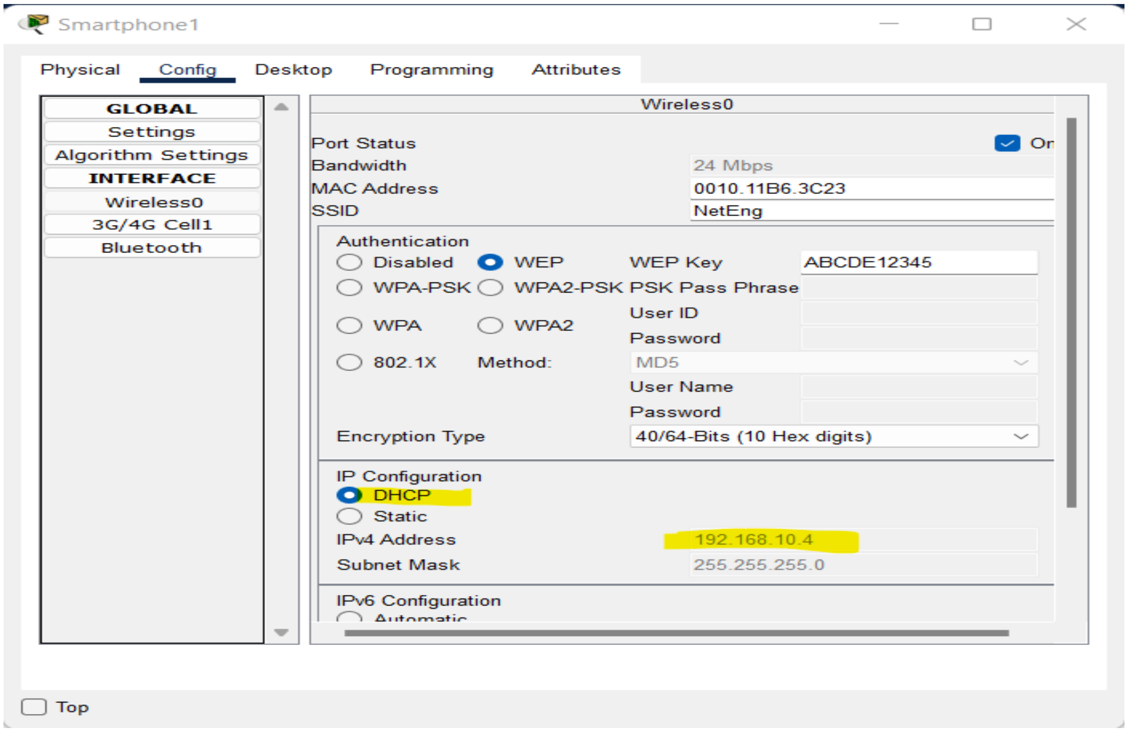
Wireless0

Port Status ☑ On
Bandwidth 18 Mbps
MAC Address 0002.4A59.5C84
SSID NetEng

Authentication
○ Disabled ● WEP WEP Key ABCDE12345
○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase
User ID
○ WPA ○ WPA2
Password
○ 802.1X Method: MD5
User Name
Password
Encryption Type 40/64-Bits (10 Hex digits)

IP Configuration
● DHCP
○ Static
IPv4 Address 192.168.10.3
Subnet Mask 255.255.255.0

IPv6 Configuration
○ Automatic



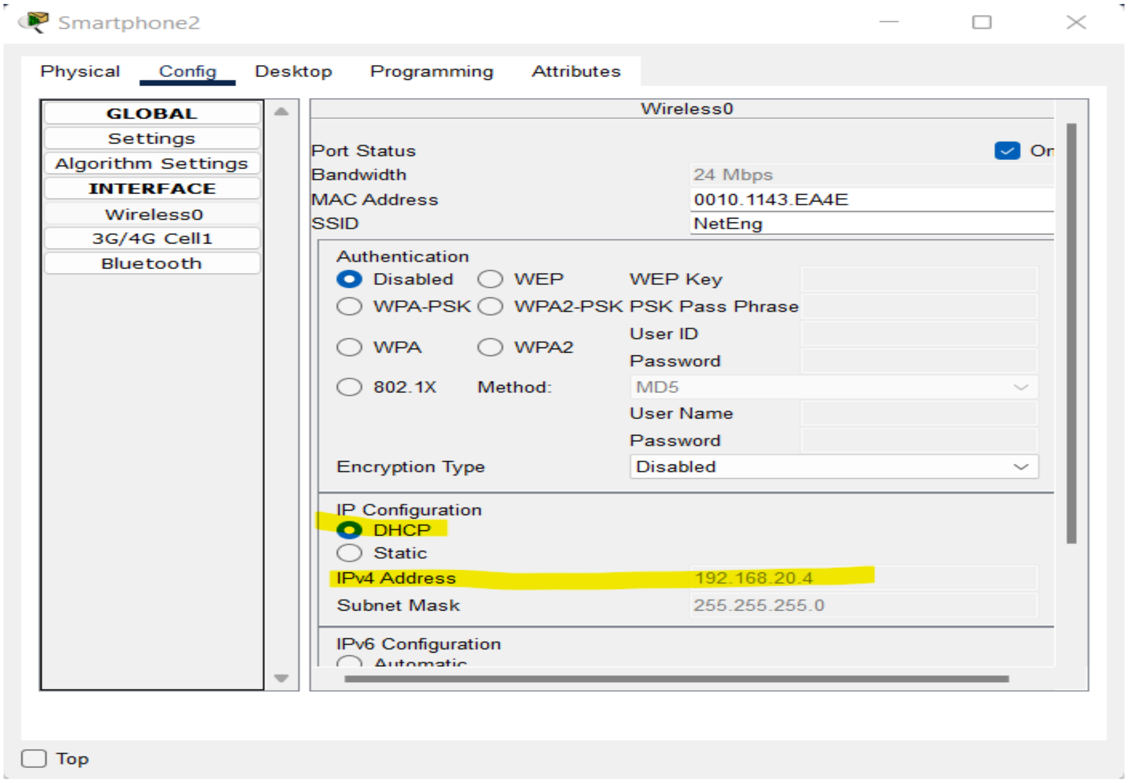
Wireless0

Port Status ☑ On
Bandwidth 24 Mbps
MAC Address 0010.11B6.3C23
SSID NetEng

Authentication
○ Disabled ● WEP WEP Key ABCDE12345
○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase
User ID
○ WPA ○ WPA2
Password
○ 802.1X Method: MD5
User Name
Password
Encryption Type 40/64-Bits (10 Hex digits)

IP Configuration
● DHCP
○ Static
IPv4 Address 192.168.10.4
Subnet Mask 255.255.255.0

IPv6 Configuration
○ Automatic



Smartphone2

Wireless0

Port Status ☑ On

Bandwidth 24 Mbps

MAC Address 0010.1143.EA4E

SSID NetEng

Authentication

● Disabled ○ WEP WEP Key

○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase

○ WPA ○ WPA2 User ID

Password

○ 802.1X Method: MD5

User Name

Password

Encryption Type Disabled

IP Configuration

● DHCP

○ Static

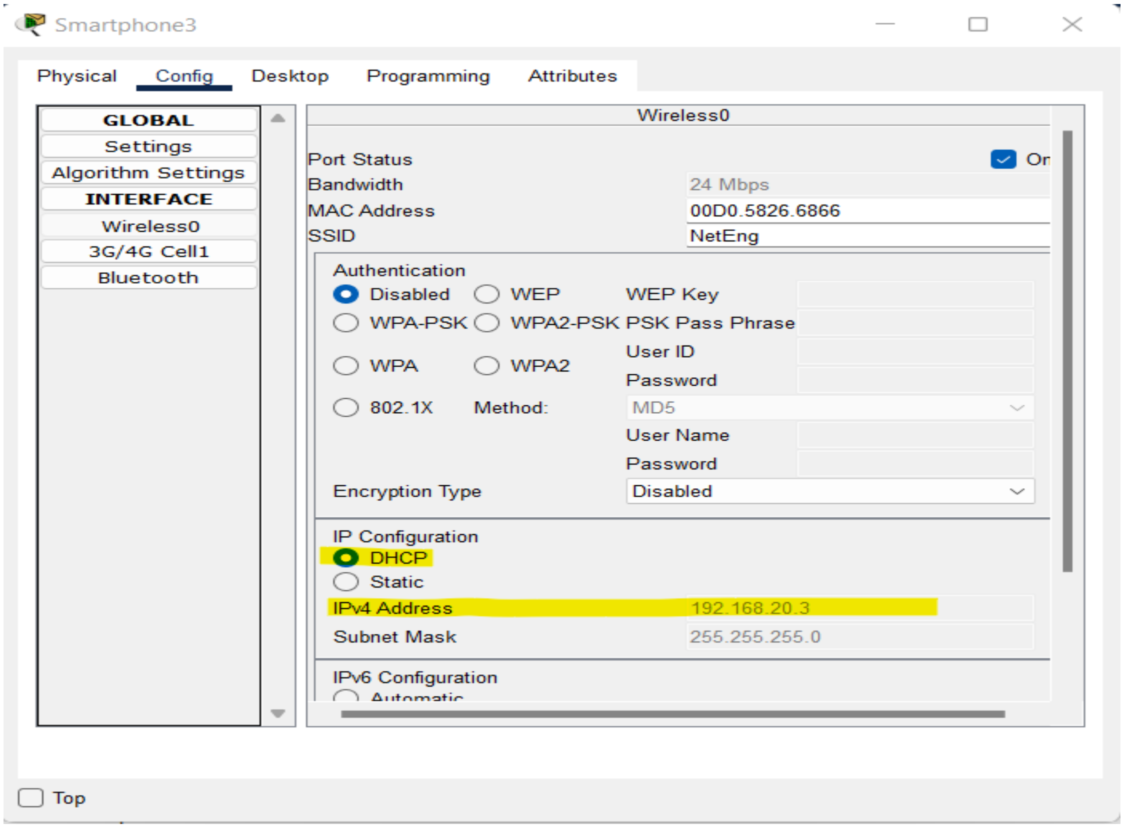
IPv4 Address 192.168.20.4

Subnet Mask 255.255.255.0

IPv6 Configuration

○ Automatic

□ Top



Smartphone3

Wireless0

Port Status ☑ On

Bandwidth 24 Mbps

MAC Address 00D0.5826.6866

SSID NetEng

Authentication

● Disabled ○ WEP WEP Key

○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase

○ WPA ○ WPA2 User ID

Password

○ 802.1X Method: MD5

User Name

Password

Encryption Type Disabled

IP Configuration

● DHCP

○ Static

IPv4 Address 192.168.20.3

Subnet Mask 255.255.255.0

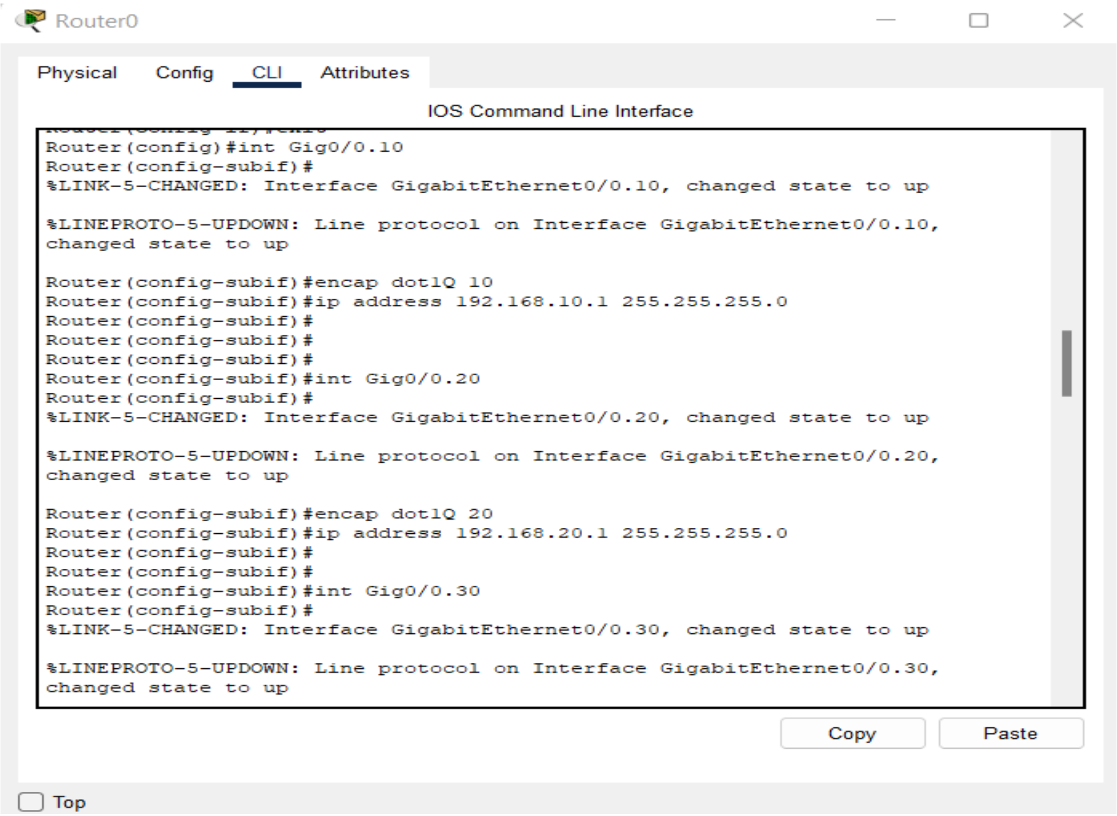
IPv6 Configuration

○ Automatic

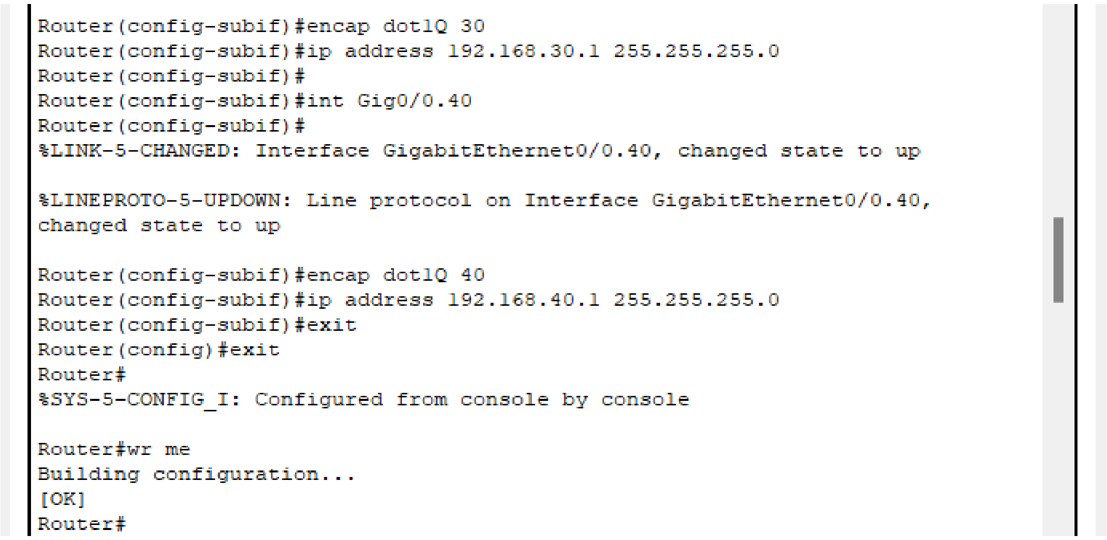
□ Top

3. In order to bring connectivity between different wireless devices, configure sub-interfaces on Router 0. *Hint: Router on a Stick configuration*

Router-On-Stick Config:



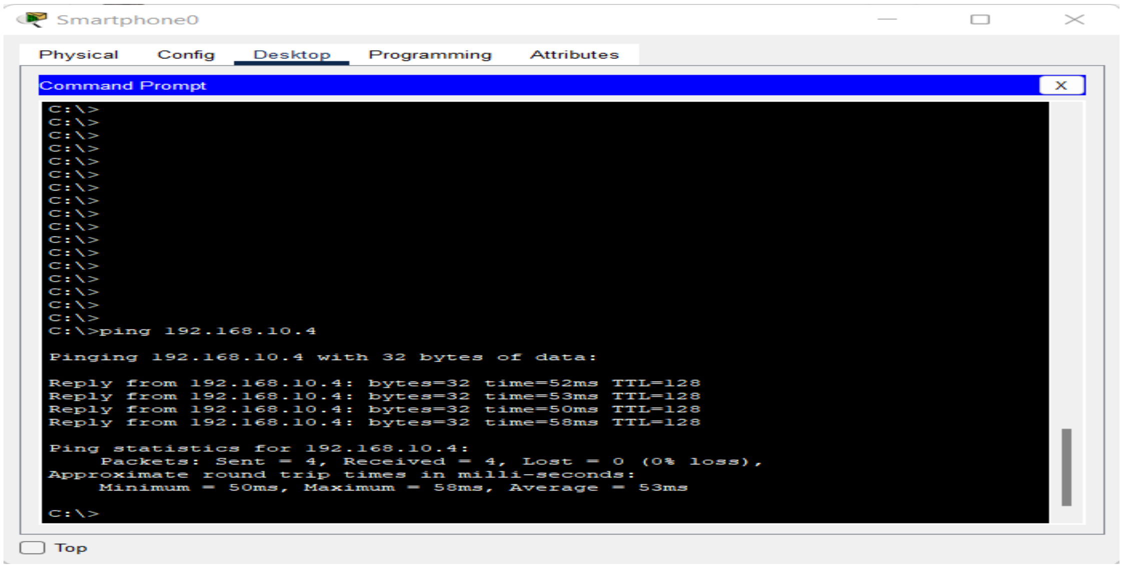
```
Router(config)#int Gig0/0.10
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10,
changed state to up

Router(config-subif)#encap dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#int Gig0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20,
changed state to up

Router(config-subif)#encap dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#int Gig0/0.30
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30,
changed state to up
```



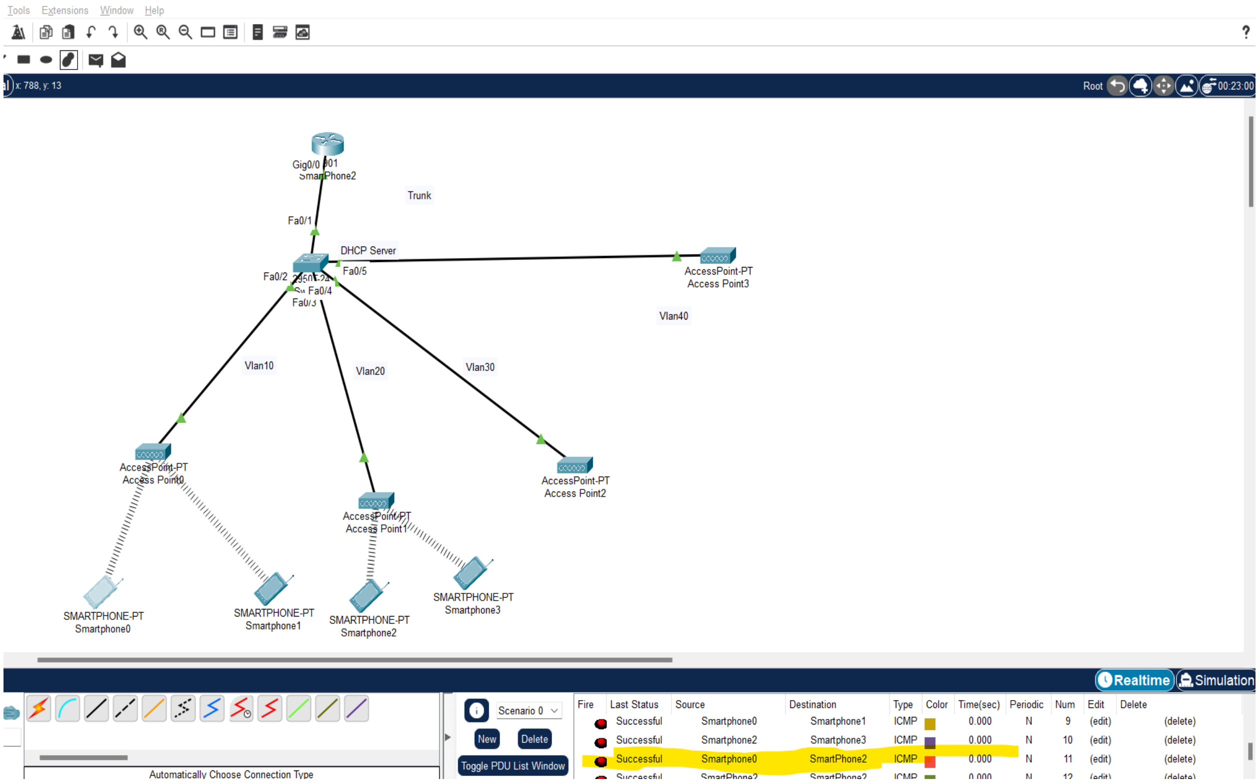
```
Router(config-subif)#encap dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#int Gig0/0.40
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.40,
changed state to up

Router(config-subif)#encap dot1Q 40
Router(config-subif)#ip address 192.168.40.1 255.255.255.0
Router(config-subif)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr me
Building configuration...
[OK]
Router#
```

4. Try to ping Smartphone 0 from Smartphone 2. Did it ping? If so why? Paste the screenshot of the output of the ping command. **[20 points]**

Yes. The ping is successful because the AP's are configured with same channel, same SSID, and same Coverage distance on the Vlan network configured with Router-on-Stick



```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.10.4

Pinging 192.168.10.4 with 32 bytes of data:

Reply from 192.168.10.4: bytes=32 time=52ms TTL=128
Reply from 192.168.10.4: bytes=32 time=53ms TTL=128
Reply from 192.168.10.4: bytes=32 time=50ms TTL=128
Reply from 192.168.10.4: bytes=32 time=58ms TTL=128

Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 50ms, Maximum = 58ms, Average = 53ms

C:\>
```



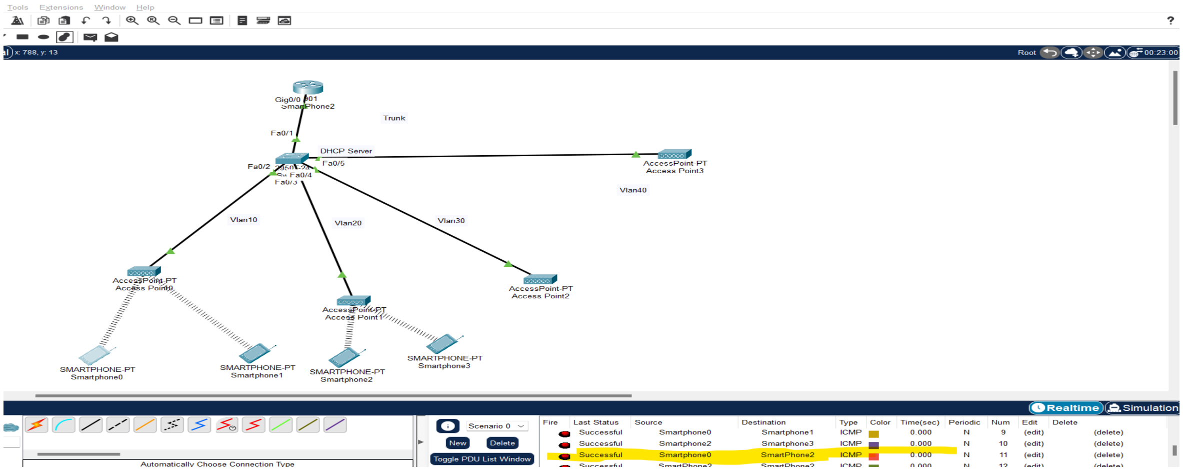
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	Smartphone0	Smartphone1	ICMP	🟨	0.000	N	9	(edit)	(delete)
●	Successful	Smartphone2	Smartphone3	ICMP	🟪	0.000	N	10	(edit)	(delete)
●	Successful	Smartphone0	SmartPhone2	ICMP	🟥	0.000	N	11	(edit)	(delete)
●	Successful	SmartPhone2	SmartPhone2	ICMP	🟩	0.000	N	12	(edit)	(delete)

Objective 3: Roaming Scenario Simulation

1. Change the coverage on AP1 to be “10 meters.” Did you notice any change in topology? If so, what behavior did you notice? Paste the screenshot of the changed topology. **[10 points]**

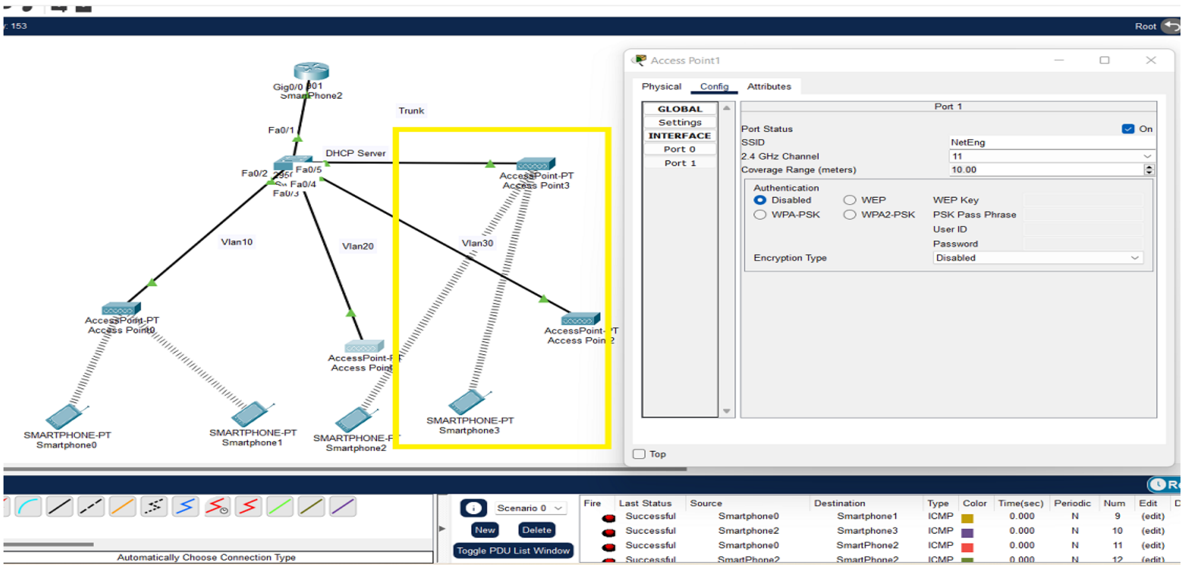
Yes. After changing the Coverage, the SmartPhones randomly connected to AP4.

Before Changing: Smartphone2, 3 were connected to AP2



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	Smartphone0	Smartphone1	ICMP	🟨	0.000	N	9	(edit)	(delete)
●	Successful	Smartphone2	Smartphone3	ICMP	🟪	0.000	N	10	(edit)	(delete)
●	Successful	Smartphone0	SmartPhone2	ICMP	🟥	0.000	N	11	(edit)	(delete)
●	Successful	SmartPhone2	SmartPhone2	ICMP	🟩	0.000	N	12	(edit)	(delete)

After Change ::



Port 1

Port Status ☑ On

SSID NetEng

2.4 GHz Channel 11

Coverage Range (meters) 10.00

Authentication

● Disabled ○ WEP WEP Key

○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase

User ID

Password

Encryption Type Disabled

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
●	Successful	Smartphone0	Smartphone1	ICMP	🟨	0.000	N	9	(edit)
●	Successful	Smartphone2	Smartphone3	ICMP	🟪	0.000	N	10	(edit)
●	Successful	Smartphone0	SmartPhone2	ICMP	🟥	0.000	N	11	(edit)
●	Successful	SmartPhone2	SmartPhone2	ICMP	🟩	0.000	N	12	(edit)

2. What is the reason that caused the wireless smartphones to switch to an alternative AP? Explain using a real-world scenario. **[10 points]**

In a congested Network it doesn't matter if the access point is stronger than the neighbors. From Levis lecture, If the AP can receive other APs, then it will share the air time with them by taking turns. All APs on the same channel will give other APs equal access to the spectrum. And because the coverage is within 10 meters coverage, the signal attenuation and the frequency will be higher if the device connects to a AP within lesser distance than that's at a farthest distance

Real world example : The switching to alternative Access point, called as "Handover" The most complex kind of hand-off is a real-time conversation… Imagine Skype or Facetime. I haven't used Skype in a long while, but I do know that Facetime occasionally loses its connection, and has to re-establish it. This will necessarily pause the conversation, and the "Hand Off" problem is limited to a few very specific instances, which mostly involve 2-way human interaction. For example : instance in a mobile phone type situation, you can have a multiple AP (base station) . Only a single base station is sending out data to be received by a phone, but all the base stations may be able to hear the phone….this is a little more difficult for WiFi, and can't really be done between systems (different SSID advertising systems).

Why do you think the smartphones switched to a particular AP as opposed toother nearby AP's? Explain the process considering wireless configuration present on all AP's. **[20 points]**

Unlike a wired network which operates at full-duplex (send and receive at the same time), a wireless network operates at half-duplex, so sometimes an AP is referred as a Wireless Hub. As per the WAL configuration topology used, **the Access point2 is configured with "Disabled authentication" and the same with AP4. Hence as the coverage distance is reduced, the end devices connected on AP1 on channel 11 has switched to non-overlapping channel 11 on AP4 with Same SSID "NetEng" configured with same "Disabled" authentication.**

Most can use the same SSID, encryption mode, pass phrase and channel. Some allow different values for one or more of these settings. And there can also be several reasons for the switch between AP1 and AP4,

1. If the SSIDs are the same, then sometimes a device will connect to one source (the router) and at other times it will connect to the other source (the repeater), if both are within range.
2. As the two transmissions are not continuous, a device may not see one source for a while and may switch to the other source. This can cause a short break in connectivity while it negotiates its connection with the new source.
3. A device may not connect to the stronger signal if it is in range of both.

However, switching to AP within smaller distance could absolutely work this way… the outward facing interface have the same MAC address and handling incoming packets from all APs (suppressing duplicates as needed) and sending traffic in the other direction from the single AP that most recently heard from the client device with the best signal strength

3. What are the different WLAN modes? Which mode resembles the topology presented in this lab? **[5 points]**

The two WLAN Modes defined in the IEE802.11 standard is **Adhoc** mode and **Infrastructure**.

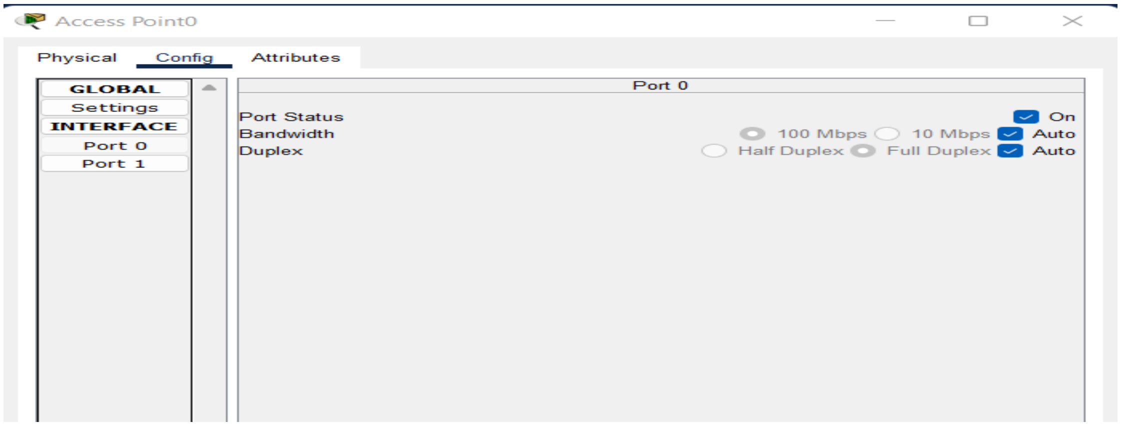
In **Adhoc mode**, the WLAN (wireless LAN) network is composed of only stations without Access Points.

In **infrastructure mode**, wlan network is hybrid comprised of stations as well as one or more access points(APs). The device Access Point is like base station used in cellular system. All the communications between stations will go through AP.

The topology we used in this lab is "Infrastructure mode" because used AP's.

4. How do we overcome interference caused by multiple AP's in a network having same SSID? **[5 points]**

One way to do it, as taught by Levi in class, is to leave them broadcasting if they are both the exact same SSID, or you can disable the broadcast on the second because computers will find the network anyway. Also, channels 1, 6, 11 are the non-overlapping channels, and by setting the configuration of AP to "AUTO" as opposed to manually configuring the AP's can discard interference.



Port 0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

And some other ways is to :

1. By optimizing the signal-to-ratio one can reduce the interference
2. Determine interfence by doing the Wi-fi spectrum survey or spectrum analysis
3. Or Use the beamforming technique

Differentiate between WLAN Security Standard briefly. Which one did we use in this lab? **[5 points]**

We used WEP (Wired Equivalent Privacy) for this lab

Different types of wireless security standards are WEP, WPA, and WPA2, serving the same purpose but being different at the same time.

WEP – Wired Equivalent Privacy. WEP encrypts traffic using a 64- or 128-bit key in hexadecimal. This is a static key, which means all traffic, regardless of device, is encrypted using a single key. A WEP key allows computers on a network to exchange encoded messages while hiding the messages' contents from intruders.

WPA – Wi-Fi protected Access, WPA uses the temporal key integrity protocol (TKIP), which dynamically changes the key that systems use. The TKIP encryption standard was later superseded by the Advanced Encryption Standard (AES).

WPA2 - . WPA2 is based on the robust security network (RSN) mechanism and operates on two modes: **Personal mode or Pre-shared Key (WPA2-PSK)** – which relies on a shared passcode for access and is usually used in home environments. **Enterprise mode (WPA2-EAP)** – as the name suggests, this is more suited to organizational or business use

5. Name the two unlicensed spectrum bands? **[2 points]**

   The three Unlicensed frequency bands used in the U.S. are the **900 MHz, 2.4 GHz and 5.8 GHz**

Total Score = ________________/157