# 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:

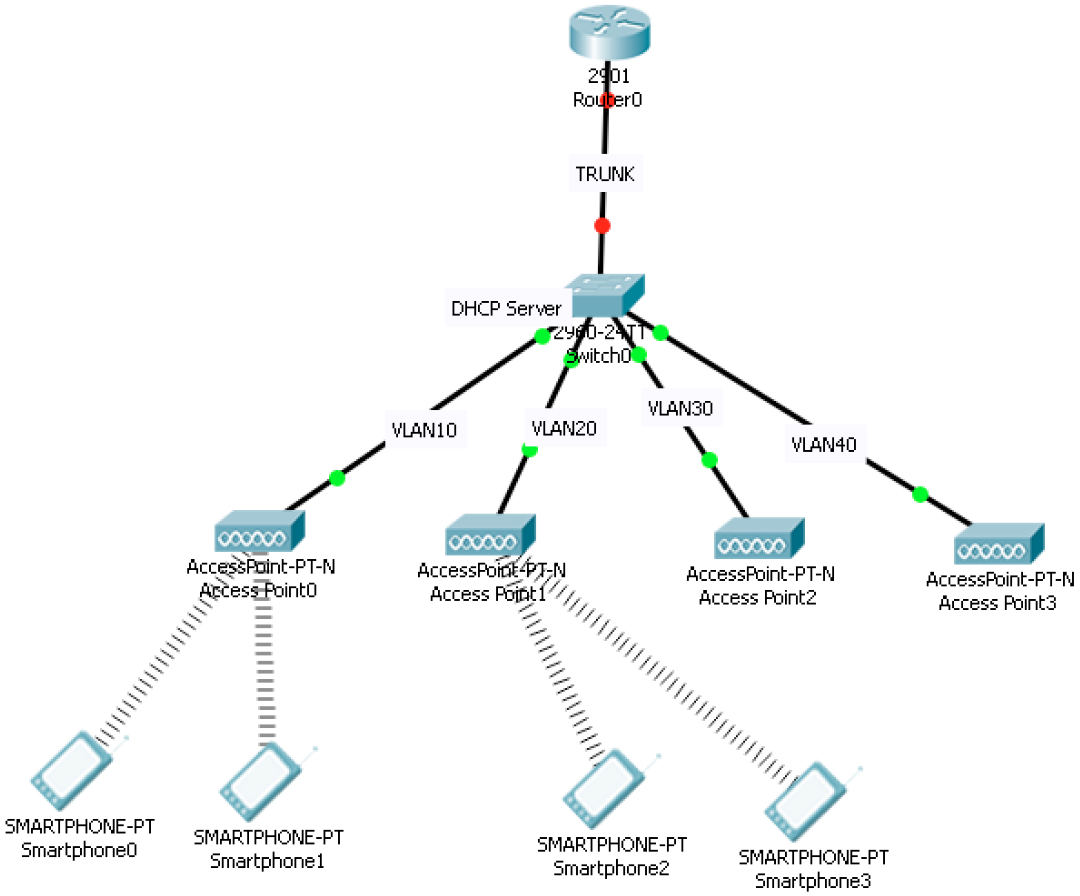
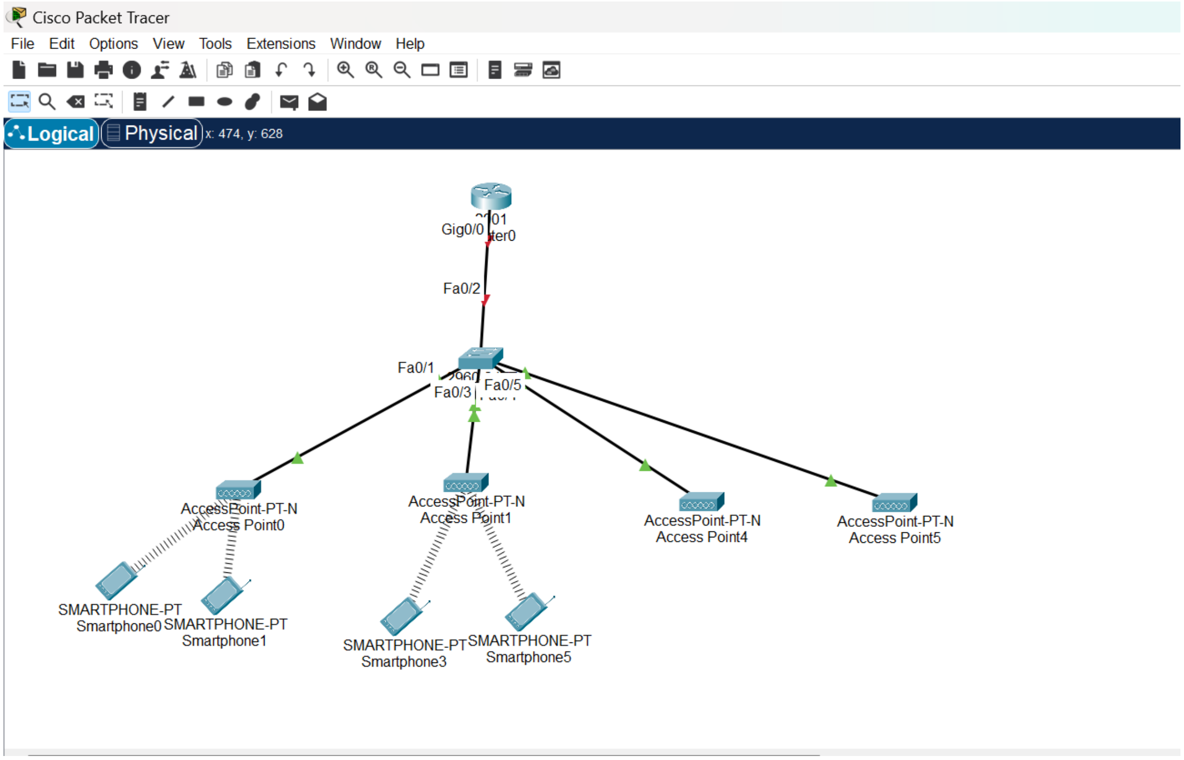


Figure 1: Wireless topology

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]**.

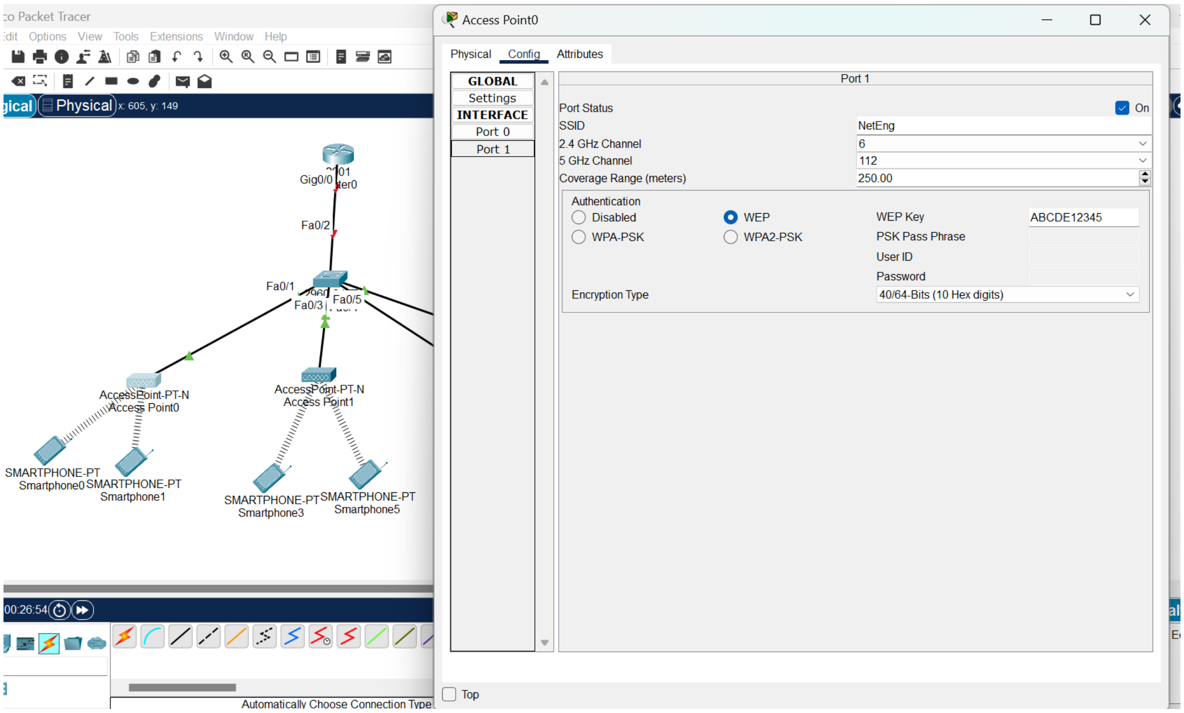


## Objective 2: Wireless Network Configuration

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]**

## AP0-



Port 1

Port Status ☑ On

SSID: NetEng

2.4 GHz Channel: 6

5 GHz Channel: 112

Coverage Range (meters): 250.00

Authentication

○ Disabled ● WEP

○ WPA-PSK ○ WPA2-PSK

WEP Key: ABCDE12345

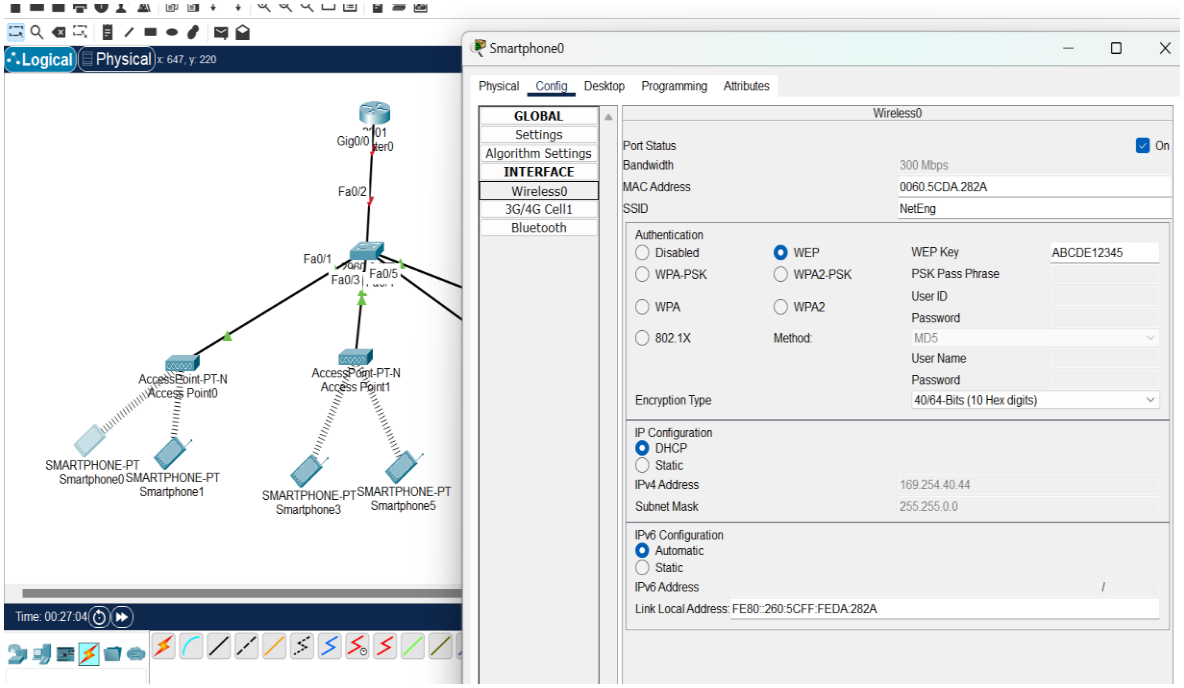
PSK Pass Phrase

User ID

Password

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

## Smartphone0-



Wireless0

Port Status ☑ On

Bandwidth: 300 Mbps

MAC Address: 0060.5CDA.282A

SSID: NetEng

Authentication

○ Disabled ● WEP

○ WPA-PSK ○ WPA2-PSK

○ WPA ○ WPA2

○ 802.1X Method: MD5

WEP Key: ABCDE12345

PSK Pass Phrase

User ID

Password

User Name

Password

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

IP Configuration

● DHCP

○ Static

IPv4 Address: 169.254.40.44

Subnet Mask: 255.255.0.0

IPv6 Configuration

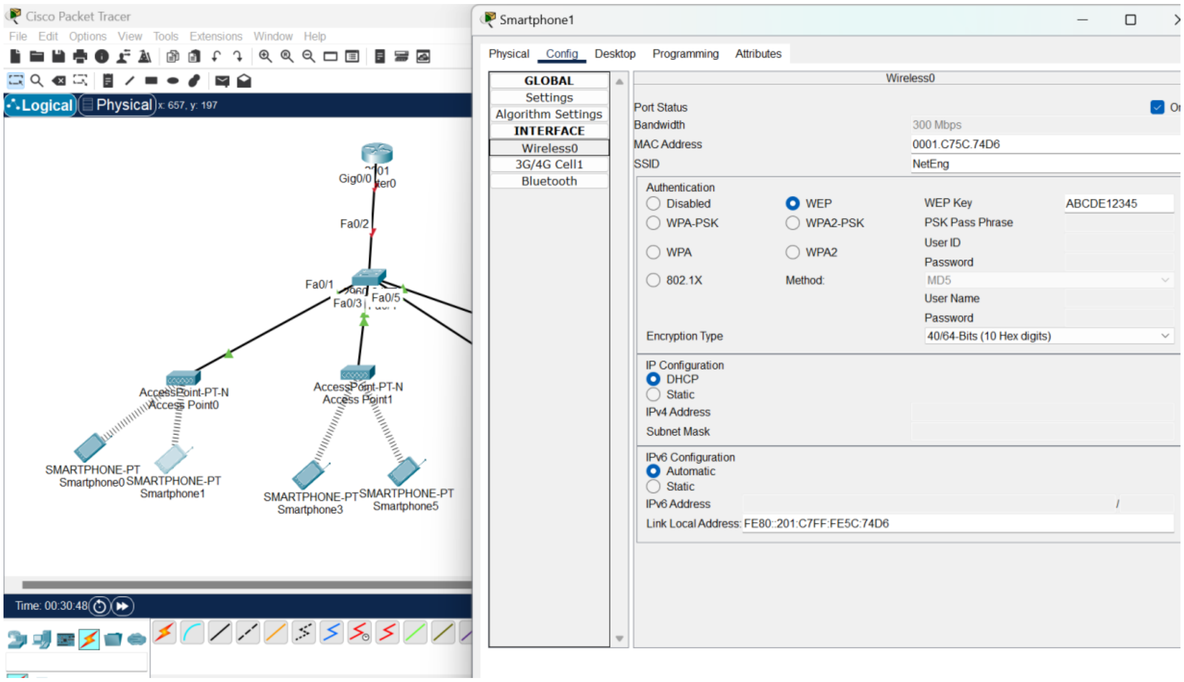
● Automatic

○ Static

IPv6 Address: /

Link Local Address: FE80::260:5CFF:FEDA:282A

## Smartphone1:-



Wireless0

Port Status ☑ O

Bandwidth 300 Mbps

MAC Address 0001.C75C.74D6

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

Subnet Mask

IPv6 Configuration

● Automatic

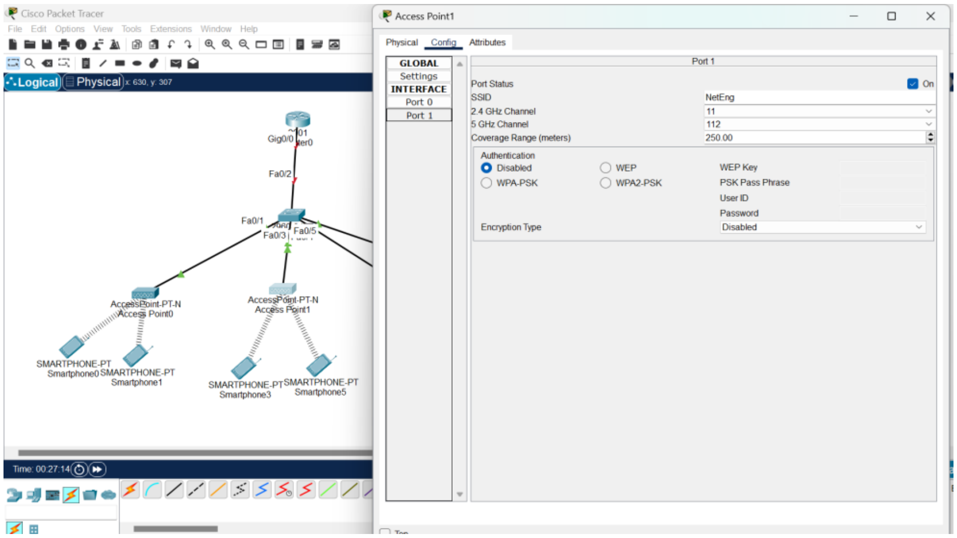
○ Static

IPv6 Address /

Link Local Address: FE80::201:C7FF:FE5C:74D6

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]**

**AP1-**



Port 1

Port Status ☑ On

SSID NetEng

2.4 GHz Channel 11

5 GHz Channel 112

Coverage Range (meters) 250.00

Authentication

● Disabled ○ WEP WEP Key

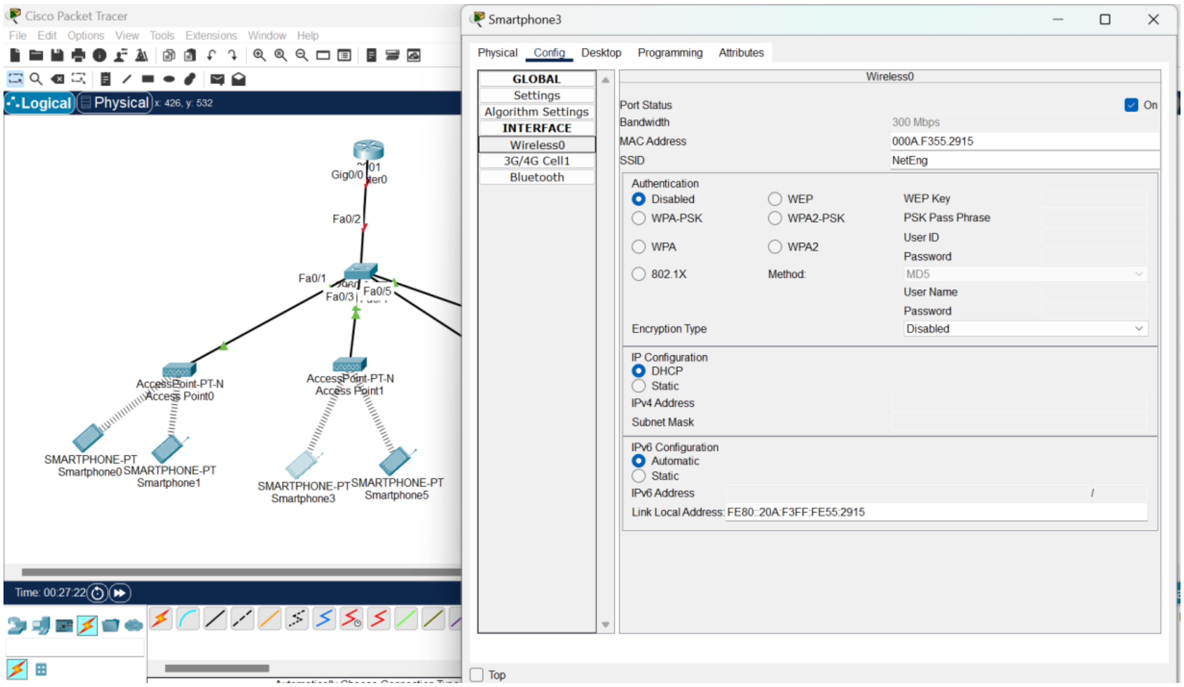
○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase

User ID

Password

Encryption Type Disabled

## Smartphone2:-



Smartphone3

Wireless0

Port Status ☑ On

Bandwidth 300 Mbps

MAC Address 000A.F355.2915

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

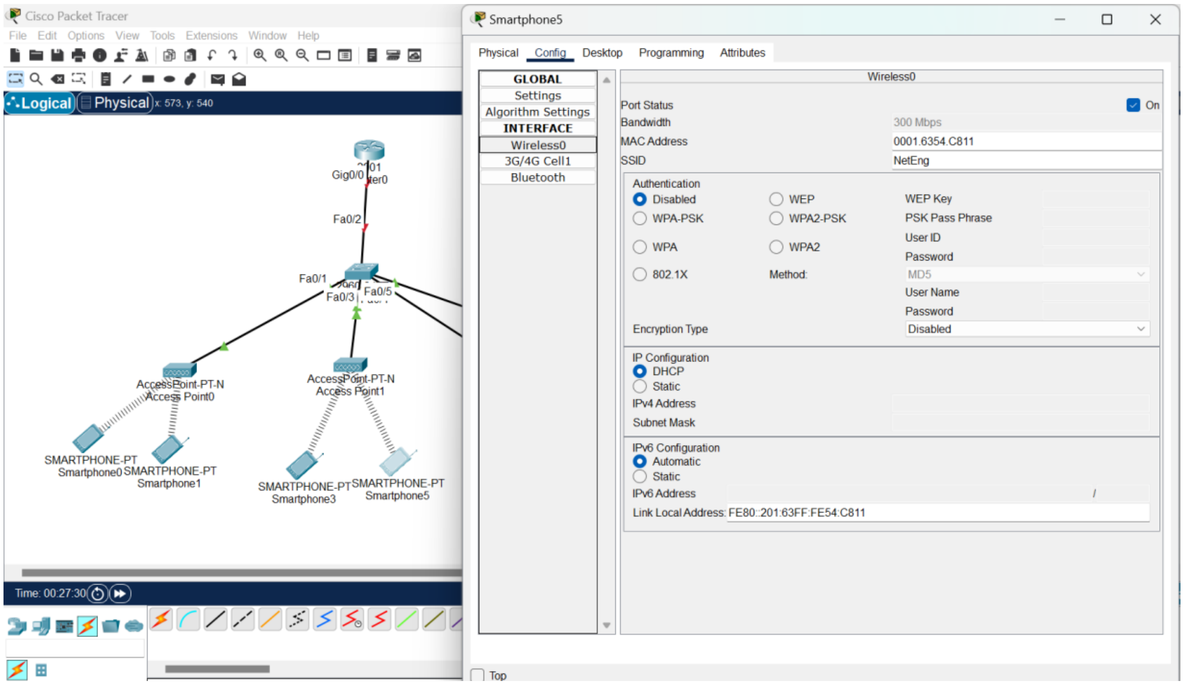
○ Static

IPv6 Address /

Link Local Address: FE80::20A:F3FF:FE55:2915

□ Top

## Smartphone3:-



Smartphone5

Wireless0

Port Status ☑ On

Bandwidth 300 Mbps

MAC Address 0001.6354.C811

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

○ Static

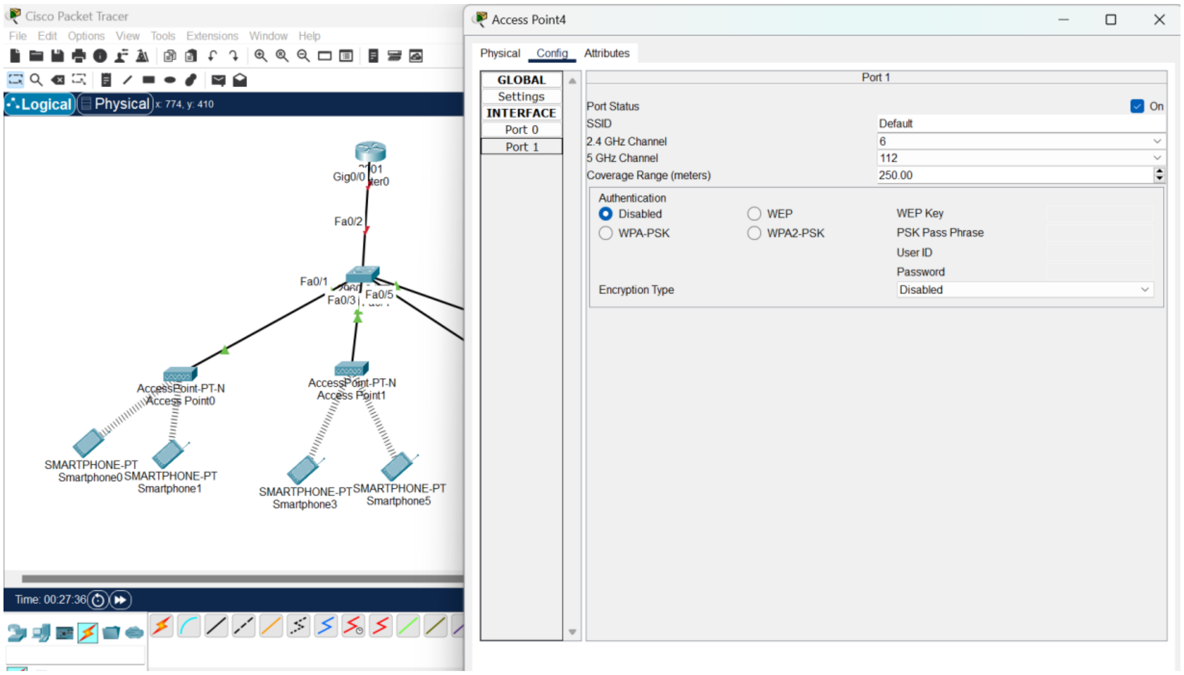
IPv6 Address /

Link Local Address: FE80::201:63FF:FE54:C811

□ Top

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]**

**AP2:-**



Port 1

Port Status ☑ On

SSID: Default

2.4 GHz Channel: 6

5 GHz Channel: 112

Coverage Range (meters): 250.00

Authentication

● Disabled ○ WEP

○ WPA-PSK ○ WPA2-PSK

WEP Key

PSK Pass Phrase

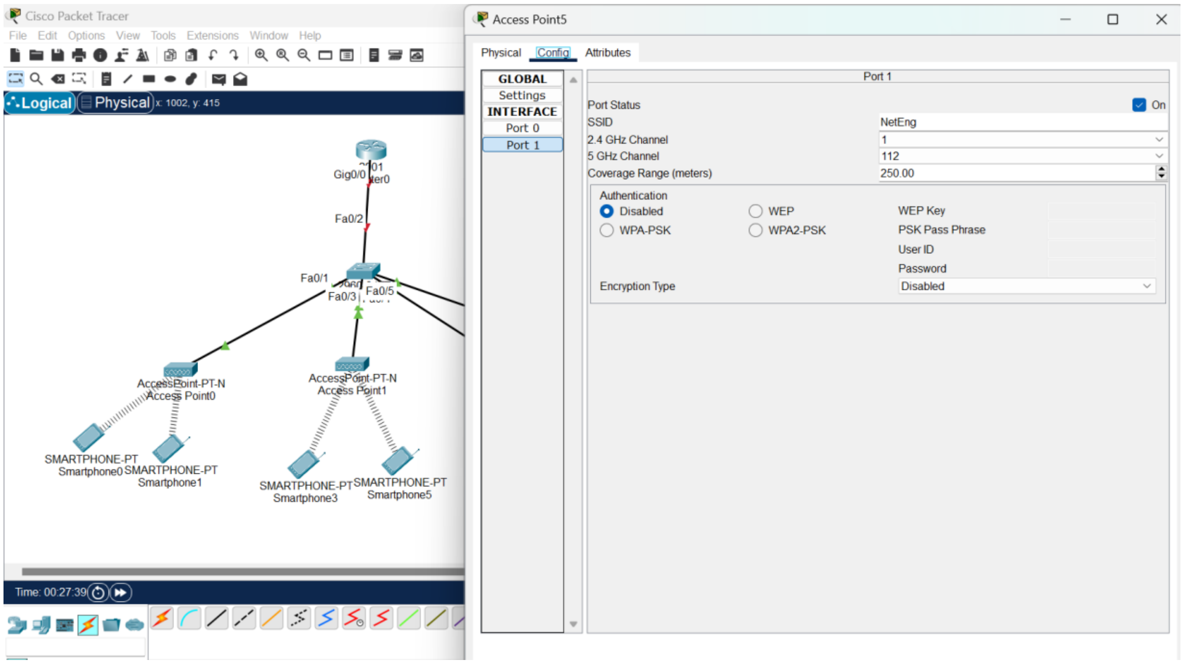
User ID

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]**

AP3:-



Access Point5

Port 1

Port Status ☑ On

SSID NetEng

2.4 GHz Channel 1

5 GHz Channel 112

Coverage Range (meters) 250.00

Authentication

● Disabled ○ WEP ○ WPA-PSK ○ WPA2-PSK

WEP Key

PSK Pass Phrase

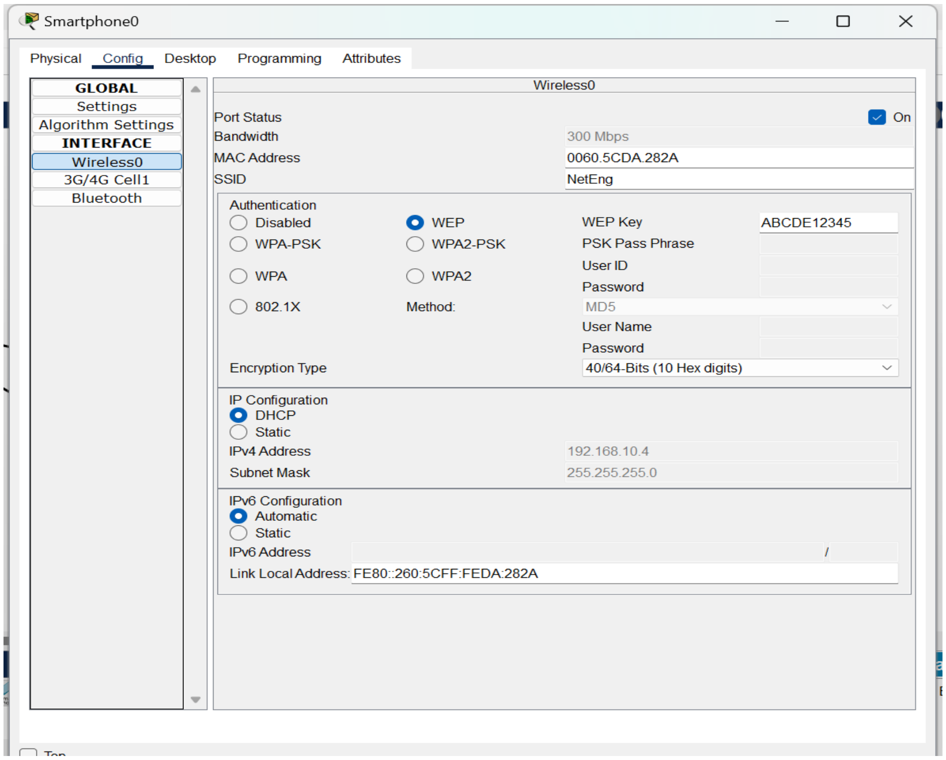
User ID

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]**

## Smartphone0:-



Smartphone0

Physical | Config | Desktop | Programming | Attributes

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

Wireless0

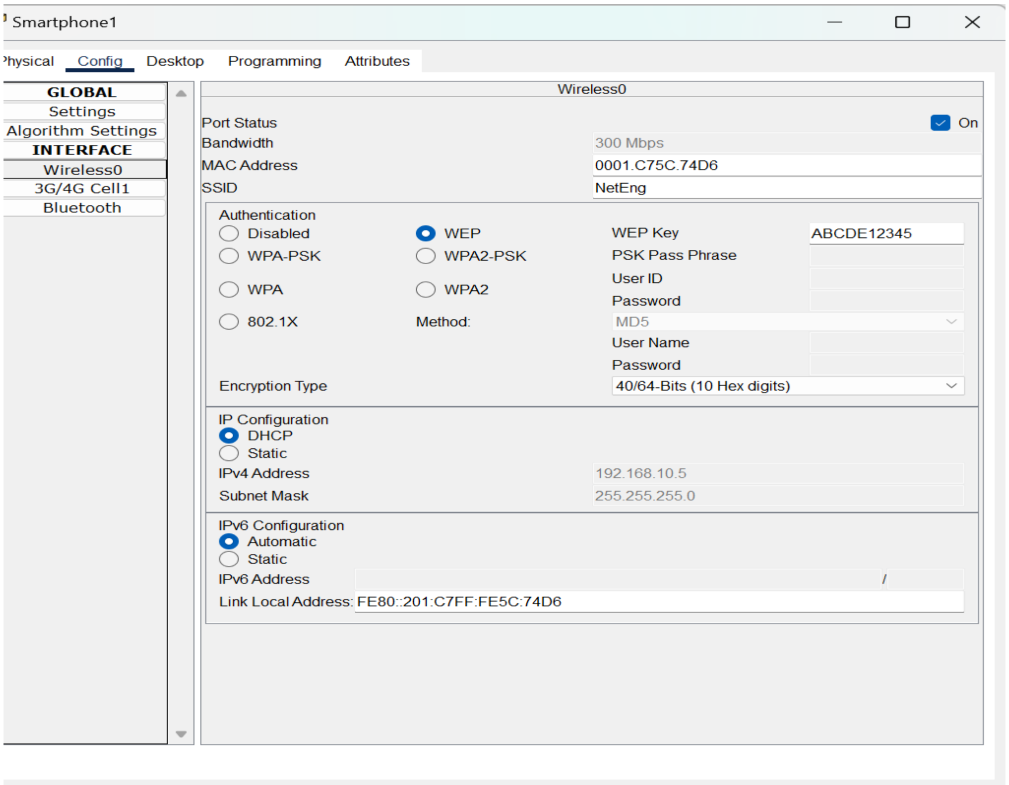
Port Status ☑ On
Bandwidth 300 Mbps
MAC Address 0060.5CDA.282A
SSID NetEng

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
○ Static
IPv6 Address /
Link Local Address: FE80::260:5CFF:FEDA:282A

## Smartphone1:-



Smartphone1

Physical | Config | Desktop | Programming | Attributes

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

Wireless0

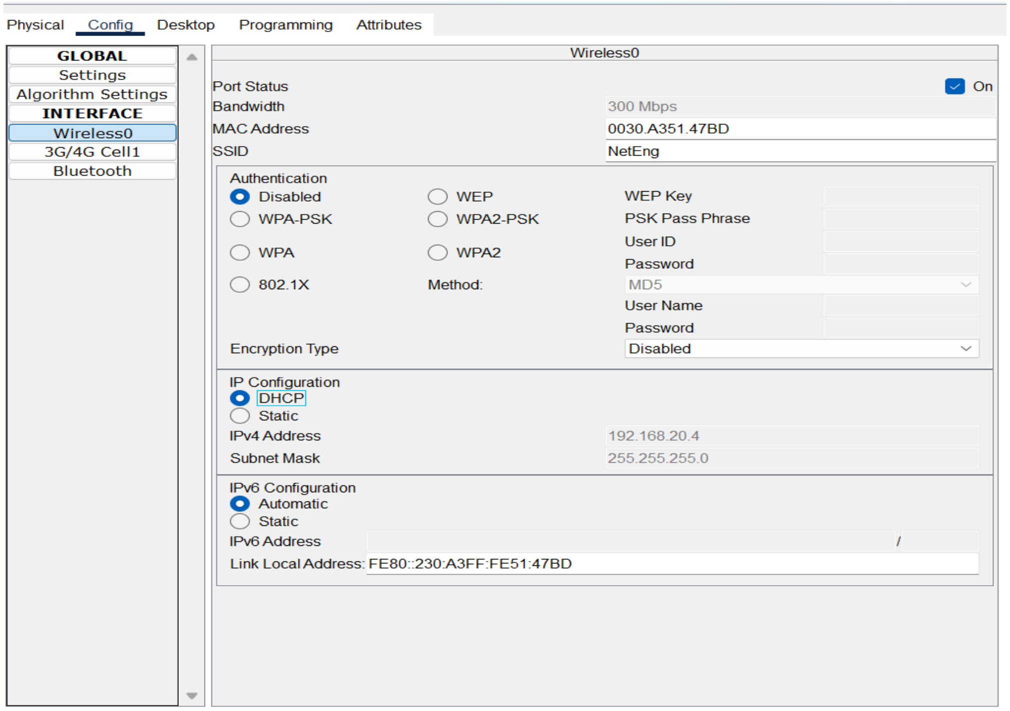
Port Status ☑ On
Bandwidth 300 Mbps
MAC Address 0001.C75C.74D6
SSID NetEng

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 192.168.10.5
Subnet Mask 255.255.255.0

IPv6 Configuration
● Automatic
○ Static
IPv6 Address /
Link Local Address: FE80::201:C7FF:FE5C:74D6

## Smartphone2:-



Wireless0

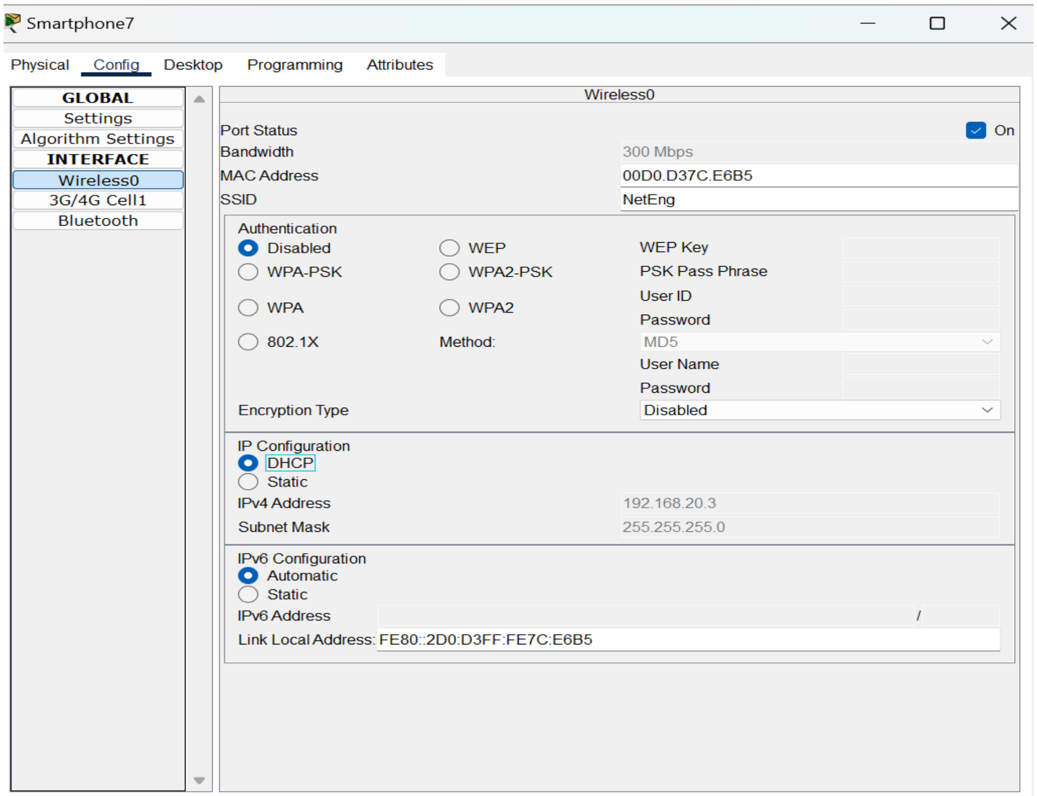
Port Status ☑ On
Bandwidth 300 Mbps
MAC Address 0030.A351.47BD
SSID NetEng

Authentication
● Disabled ○ WEP
○ WPA-PSK ○ WPA2-PSK
○ WPA ○ WPA2
○ 802.1X
Method:
WEP Key
PSK Pass Phrase
User ID
Password
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
○ Static
IPv6 Address /
Link Local Address: FE80::230:A3FF:FE51:47BD

## Smartphone3:-



Wireless0

Port Status ☑ On
Bandwidth 300 Mbps
MAC Address 00D0.D37C.E6B5
SSID NetEng

Authentication
● Disabled ○ WEP
○ WPA-PSK ○ WPA2-PSK
○ WPA ○ WPA2
○ 802.1X
Method:
WEP Key
PSK Pass Phrase
User ID
Password
MD5
User Name
Password
Encryption Type Disabled

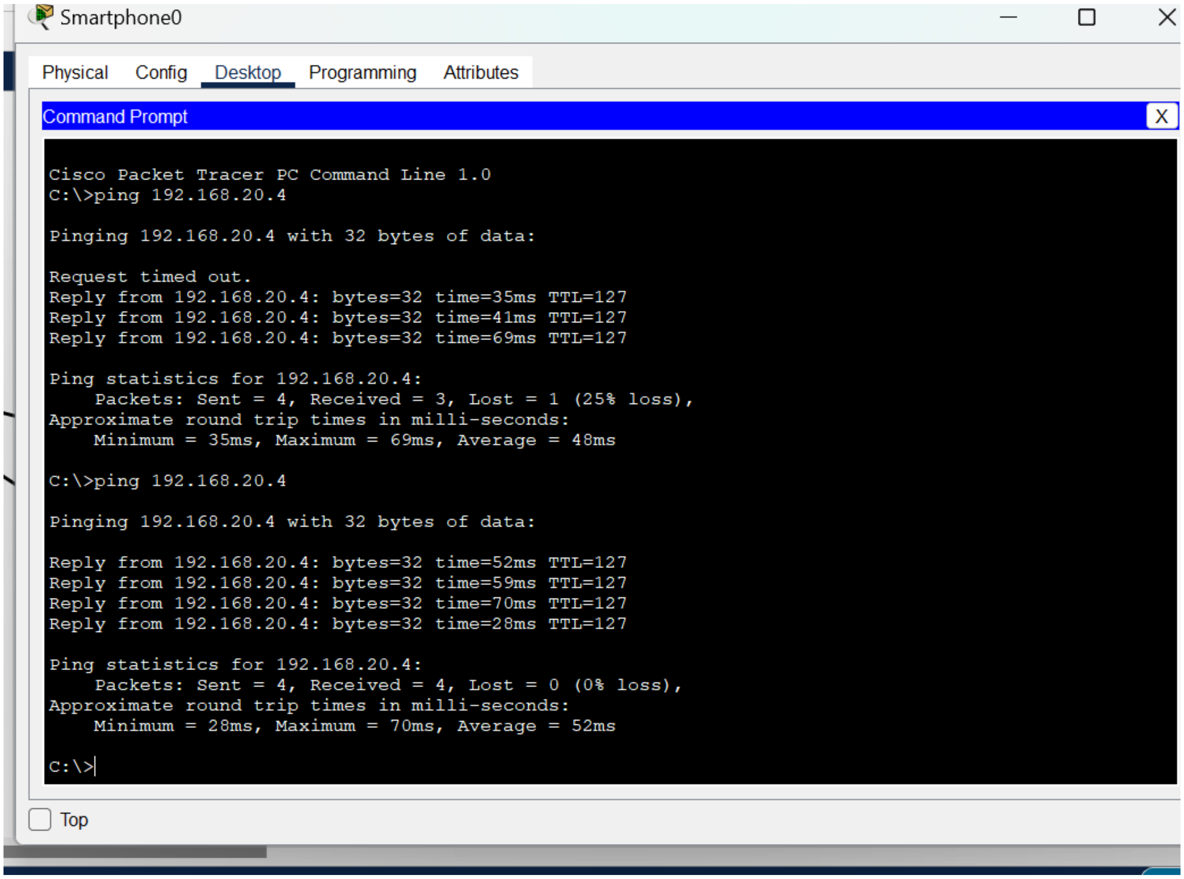
IP Configuration
● DHCP
○ Static
IPv4 Address 192.168.20.3
Subnet Mask 255.255.255.0

IPv6 Configuration
● Automatic
○ Static
IPv6 Address /
Link Local Address: FE80::2D0:D3FF:FE7C:E6B5

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

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]**

   *Hint: You can access command line terminal in a smartphone by navigating to "Desktop" tab after double-clicking on the device.*



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.4

Pinging 192.168.20.4 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.4: bytes=32 time=35ms TTL=127
Reply from 192.168.20.4: bytes=32 time=41ms TTL=127
Reply from 192.168.20.4: bytes=32 time=69ms TTL=127

Ping statistics for 192.168.20.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 35ms, Maximum = 69ms, Average = 48ms

C:\>ping 192.168.20.4

Pinging 192.168.20.4 with 32 bytes of data:

Reply from 192.168.20.4: bytes=32 time=52ms TTL=127
Reply from 192.168.20.4: bytes=32 time=59ms TTL=127
Reply from 192.168.20.4: bytes=32 time=70ms TTL=127
Reply from 192.168.20.4: bytes=32 time=28ms TTL=127

Ping statistics for 192.168.20.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 28ms, Maximum = 70ms, Average = 52ms

C:\>
```

The ping was successful. This means that inter-VLAN routing is working. The smartphones are in different VLANs, so for them to communicate the router must have inter-VLAN routing configured.

## 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]**

   When the coverage area of AP1 is reduced to 10 meters, smartphones that were connected to AP1 and are now outside this range will lose connectivity with AP1. As a result, they may attempt to reconnect to the nearest available access point with sufficient signal strength. As soon as I change the coverage on AP1 to 10 meters the packet tracer, the smartphones moved from AP1 to other access points to seek connectivity.

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

   The smartphones switched to an alternative AP due to signal loss from the reduced coverage of AP1. In a real-world scenario, this is like when we are connected to the Wi-Fi router, when we try to move away from the router, as soon as the distance increases, the signal strength decreases eventually leading to disconnection. When this happens, the device will attempt to connect to another available network with the same SSID or a different network if it has no remaining connections.

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

   Smartphones typically connect to the AP with the strongest signal within range.

   Factors affecting this choice include:

Signal Strength: Smartphones will prefer an AP with a higher signal-to-noise ratio.

Channel and Interference: If multiple Aps broadcast on the same channel, devices might connect to the AP with less interference.

Channel Availability: Smartphones avoid Aps with high interference, preferring those on less crowded channels.

Load Balancing-Some APs distribute connections across multiple APs to balance network load.

SSID and authentication: In environments with multiple Aps using the same SSID, the device will connect to the nearest AP with proper authentication.

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

The common WLAN modes include:

Infrastructure Mode: Devices connect to a central AP that manages the network. This is the most common setup in home and enterprise networks.

Ad-Hoc Mode: Devices connect directly to each other without an AP forming a peer-to-peer network.

Mesh Mode: Multiple Aps create a network that allows devices to hop between them seamlessly, often used in large areas for extended coverage.

The topology resembles infrastructure mode as all smartphones are connecting to central access points.

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

To overcome interference:

Channel planning: set each AP to operate on a different and non-overlapping channel.

Lowering Transit Power: Reducing The transmission power of APs can prevent overlap in coverage areas.

Use of 5 Ghz Band: The 5 Ghz band has more channels compared to 2.4 Ghz and is less prone to interference.

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

WEP (Wired Equivalent Privacy) – The key size is typically 64-bit and 128-bit, although the key structure and initialization vector make it vulnerable.

Security level: Low, WEP has several vulnerabilities because the key length is short, making it crackable.

Usage: Rarely used today due to security flaws; not recommended for modern networks.

WPA (Wi-Fi protected Access)- It adds a message integrity check to prevent packet forgery and provides dynamic key exchange.

Security level: Moderate, WPA significantly improves security over WEP, but still has vulnerabilities, especially when using a weak passphrase.

Usage: Still found on some older devices but largely phased out in favor pf WPA2.

WPA2 (Wi-Fi protected Access II)- WPA2 uses robust key management protocols and offers both PSK(pre-Shared Key) mode for home networks and enterprise mode for corporate networks with RADIUS authentication.

Security level: High; WPA2 is considered highly secure and widely used today. Its AES encryption provides strong security against most attacks.

WPA3 (Wi-Fi protected Access III)- WPA3 introduces simultaneous authentication of equals (SAE) instead of PSK, which provides more secure key exchange even if the password is weak.

Security level: Very High, WPA3 is resistant to most know attacks, and its SAE protocol enhances protection against dictionary attacks.

Usage: Adoption is still growing, as it requires compatible hardware. Many new devices support WPA3, but it may not be available on older devices.

WEP was used in this lab.

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

The two unlicensed spectrum bands commonly used for WI-FI are:

2.4Ghz Band

5Ghz Band

**Total Score = ____________________/157**