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:

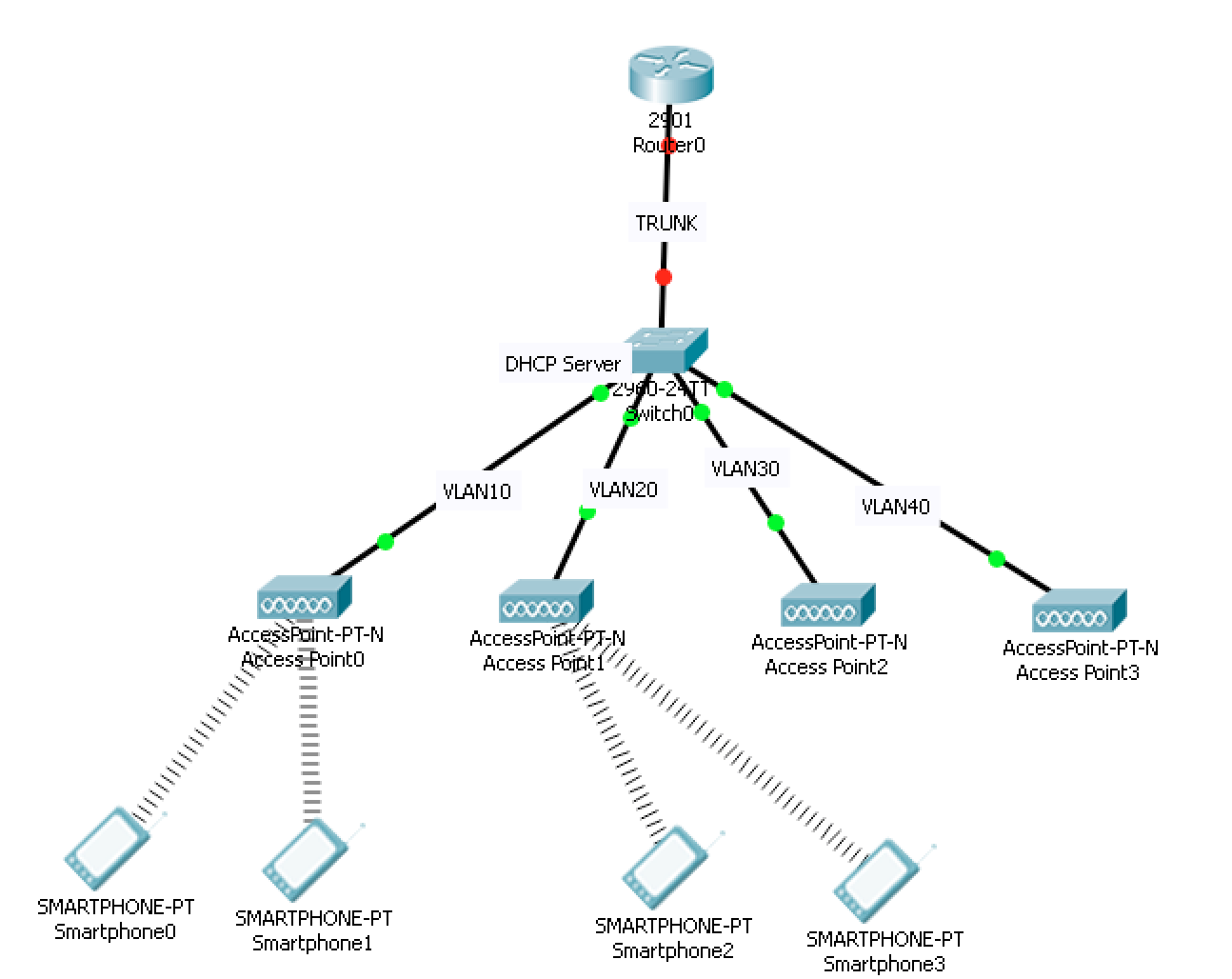
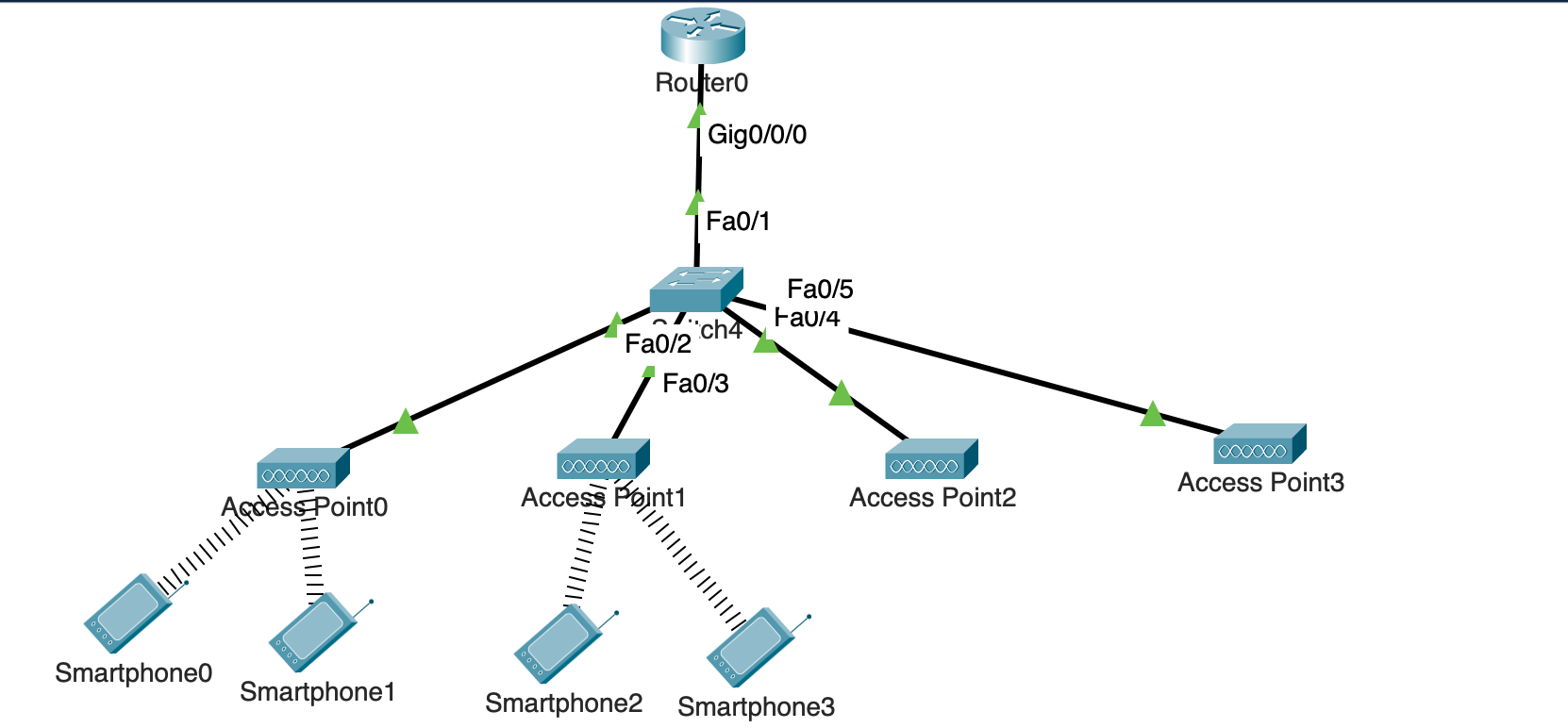


Figure 1: Wireless topology

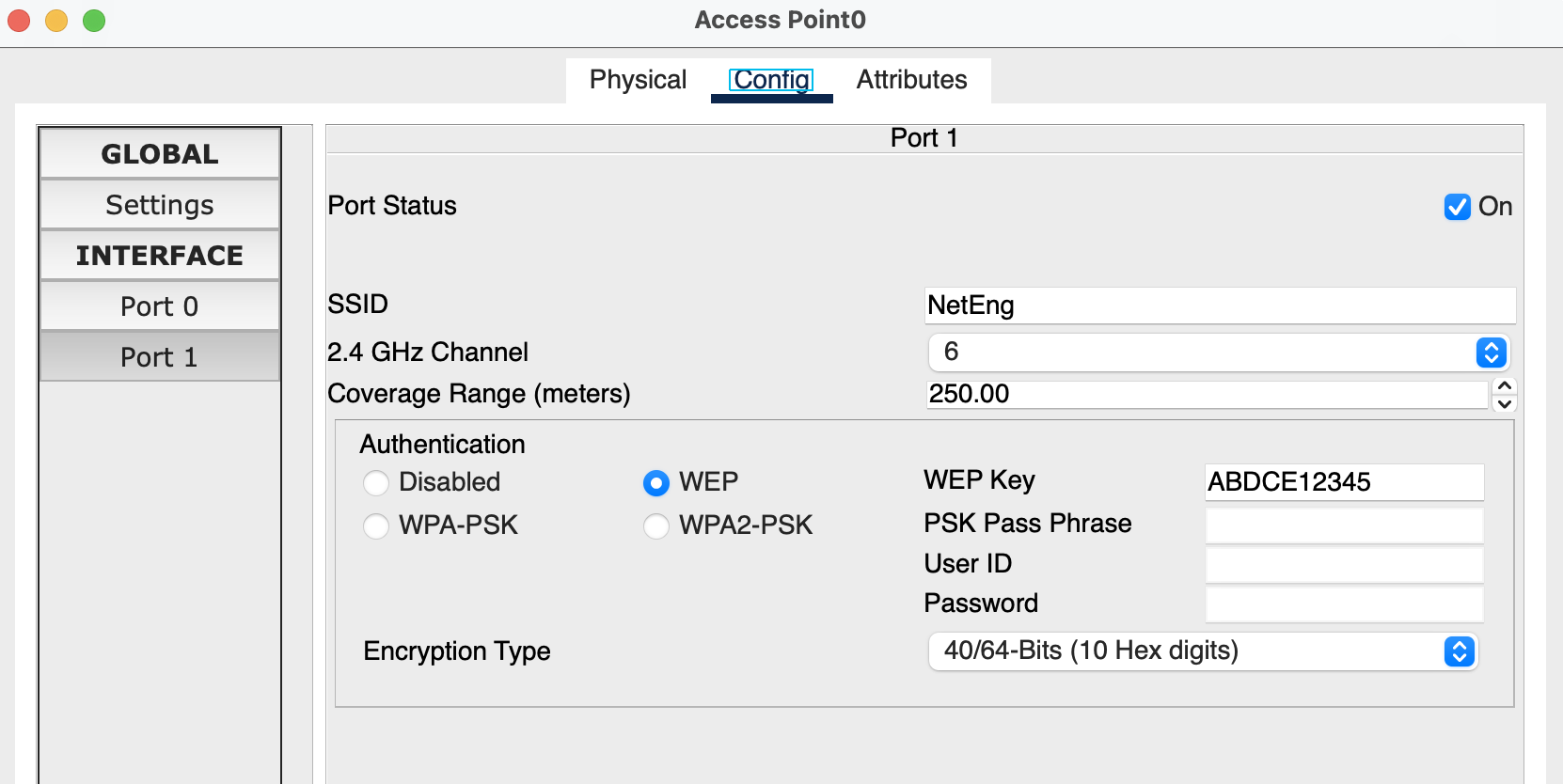
1. The Access Points (AP’s) and wireless terminals (Smartphones) are located in the “Wireless Devices” section of CPT. Please drag and drop appropriately as indicated in Figure 1. The wireless terminals may connect randomly to AP’s. Please disregard it at this point. Paste the screenshot of the created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

****

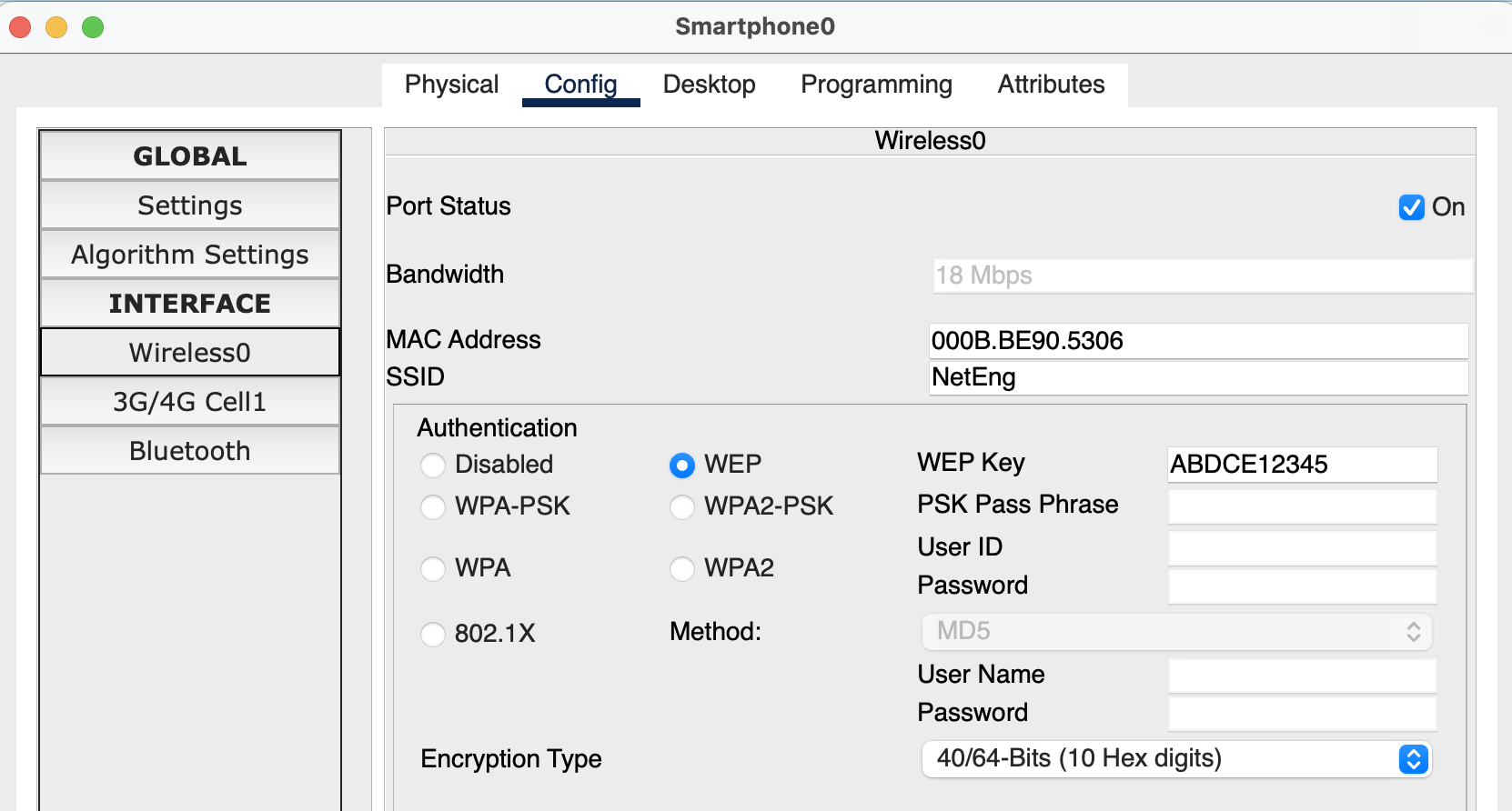
# Objective 2: Wireless Network Configuration

1. Access Point and Smartphone configuration
   1. 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]**

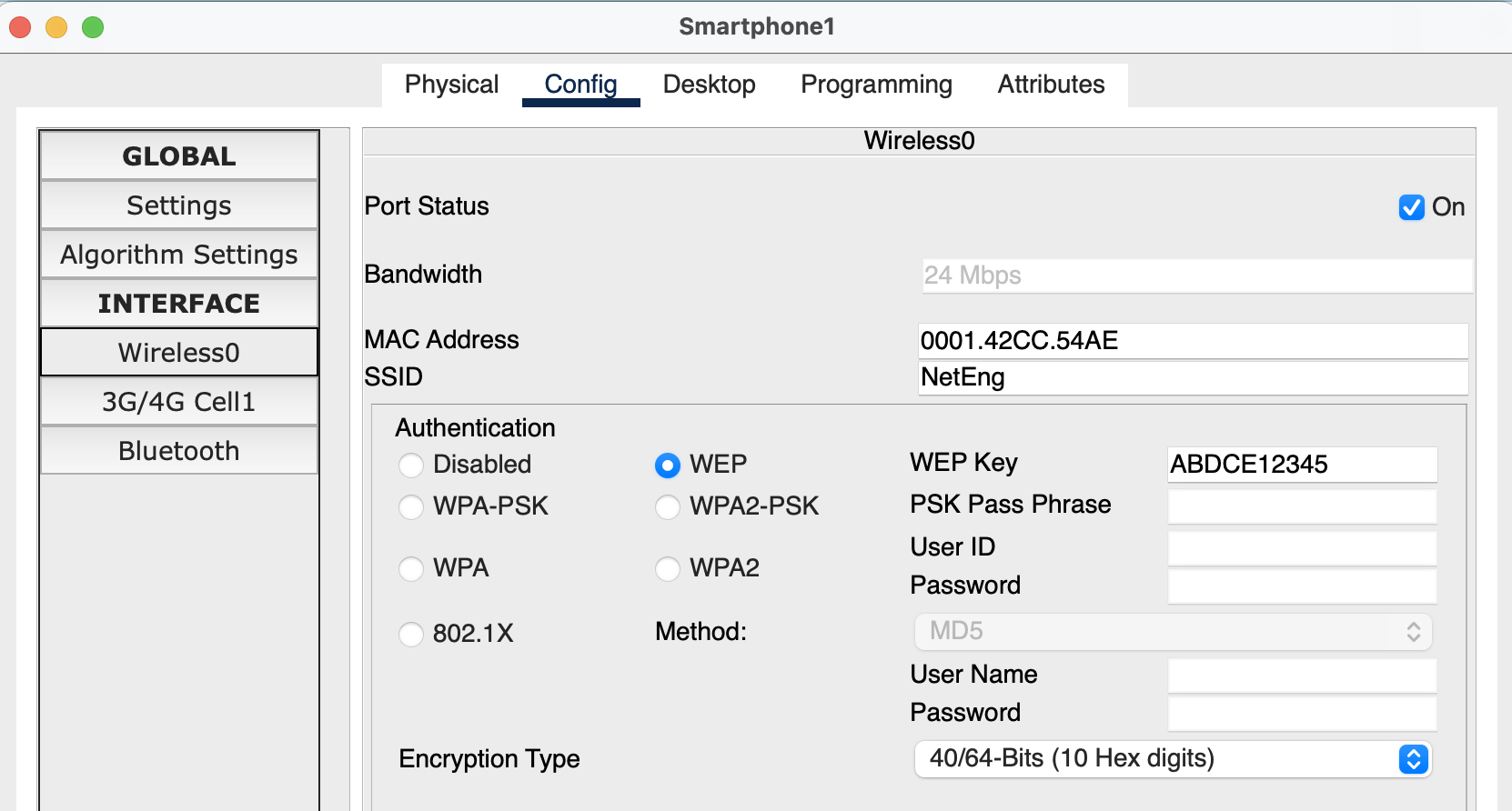
**Access Point 0 config:**

****

**Smartphone0 config:**

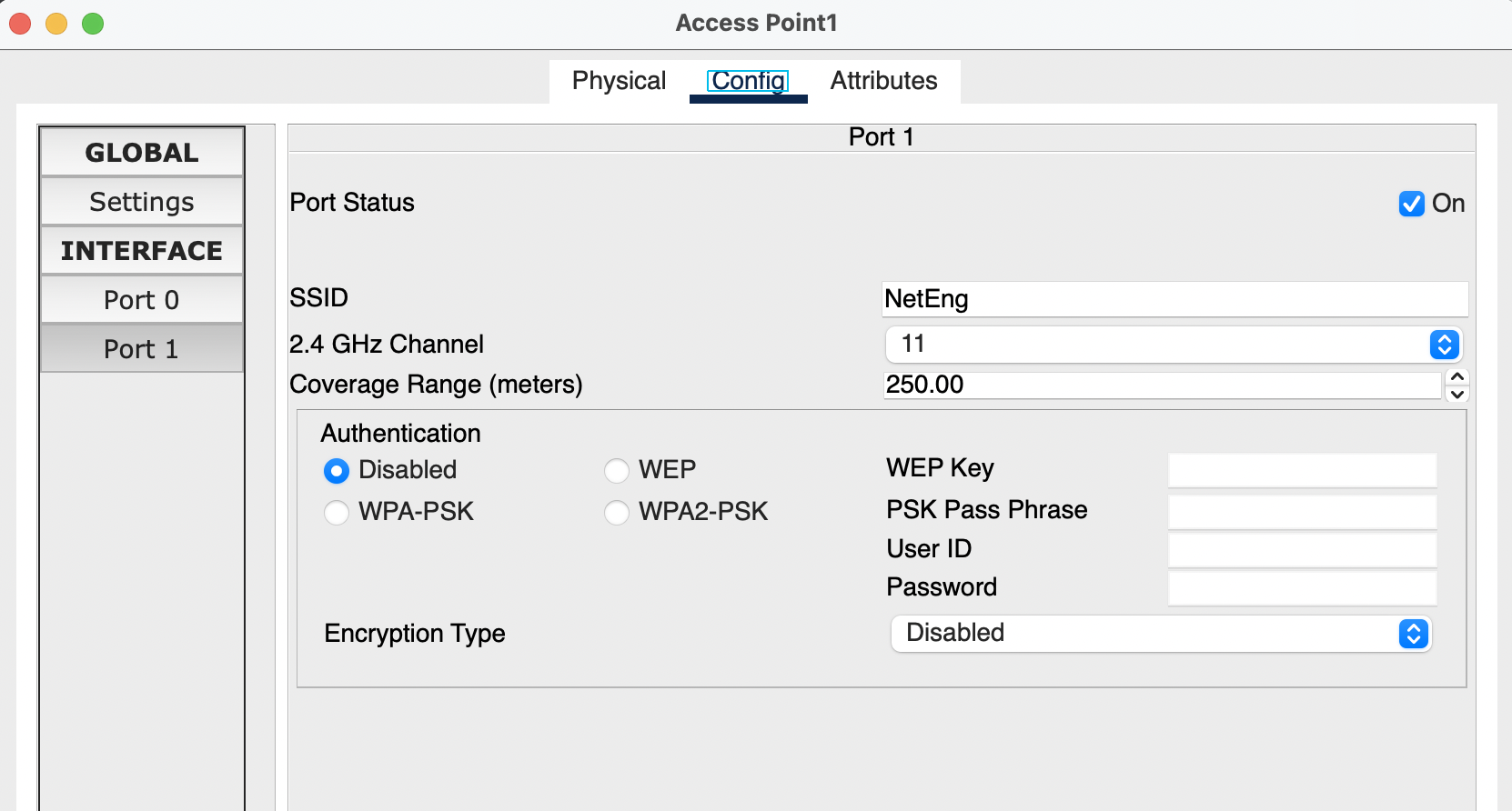
****

**Smartphone1 config:**

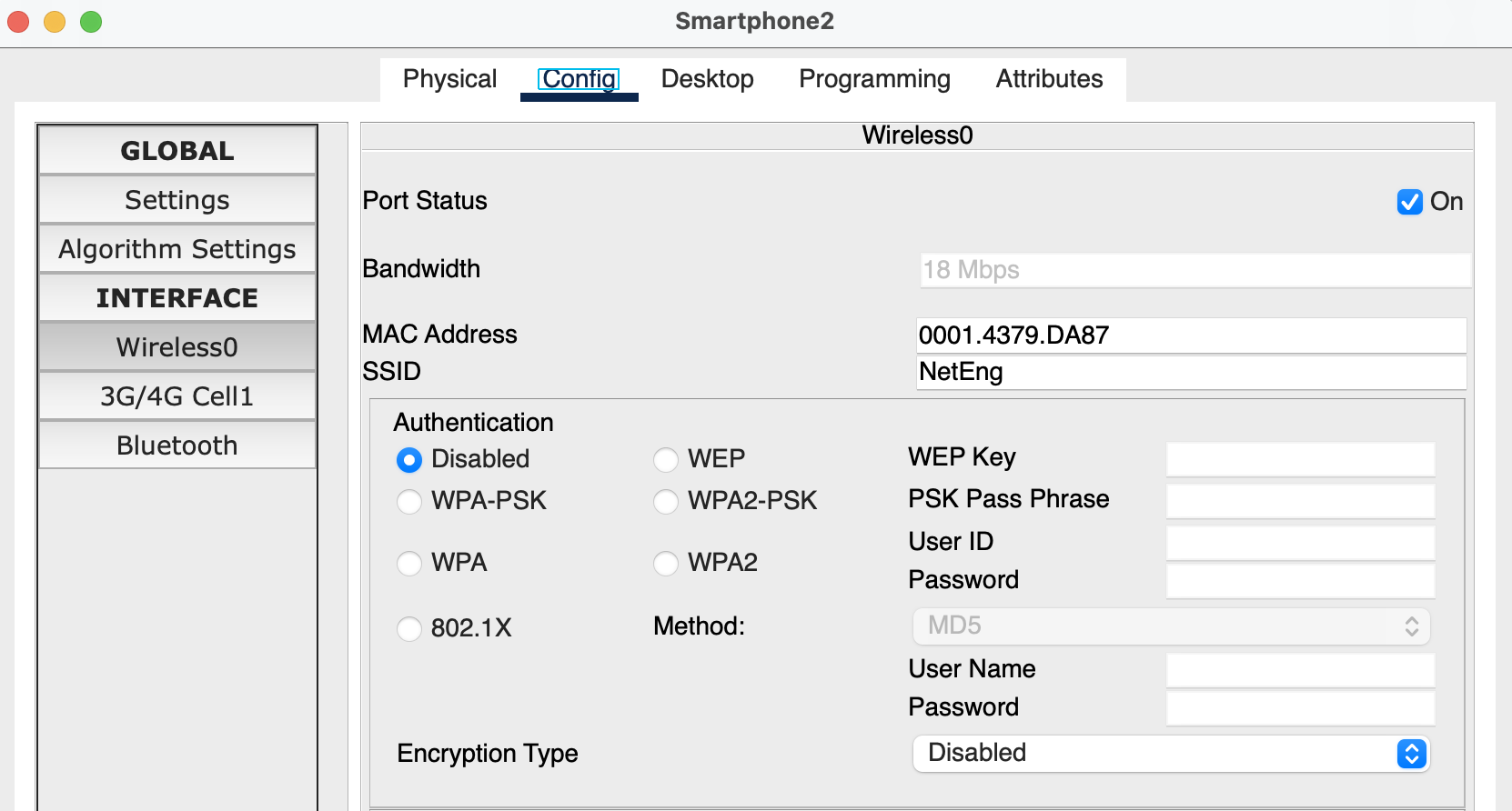
****

* 1. 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]**

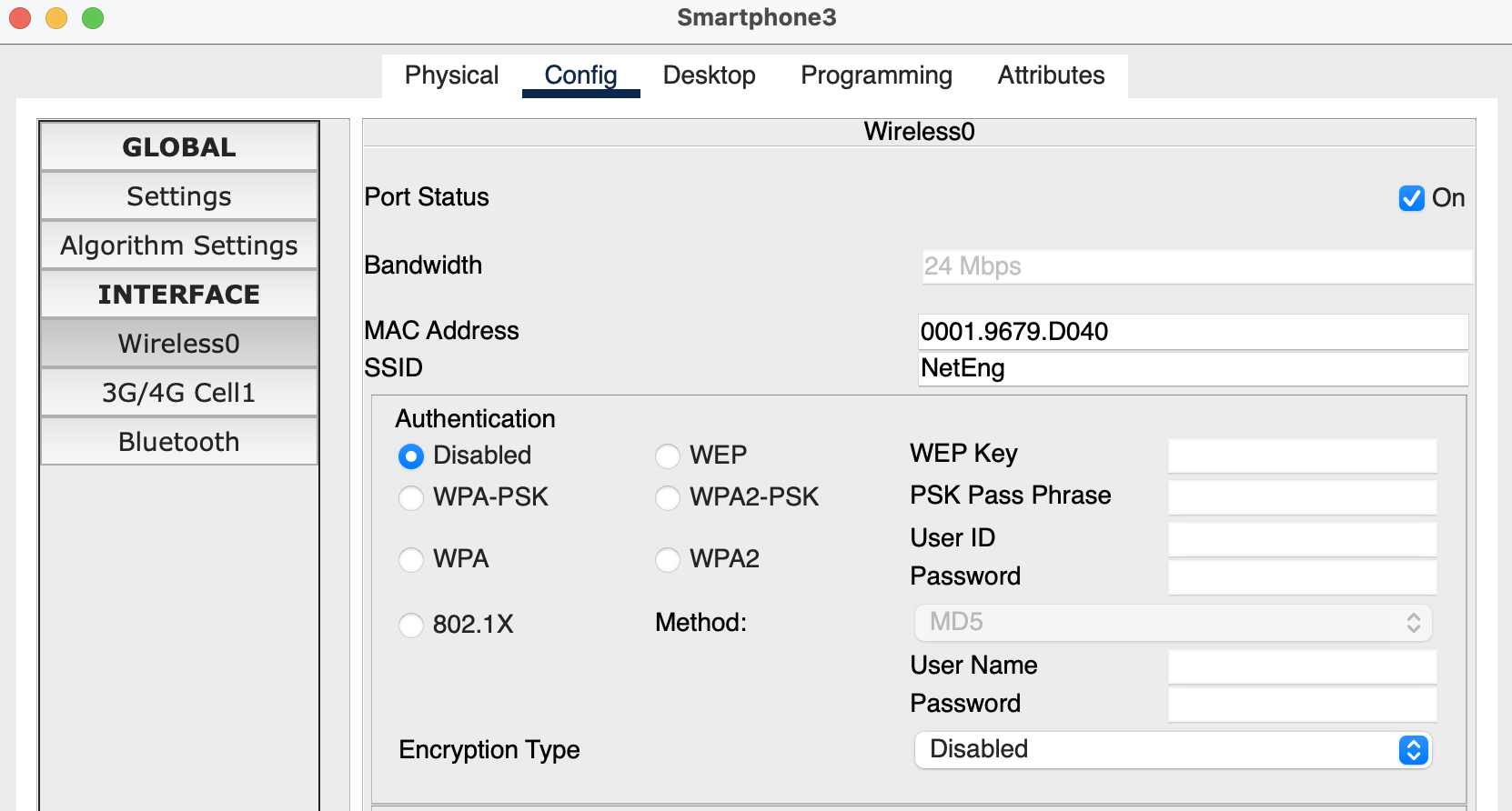
**Access Point 1 config:**

****

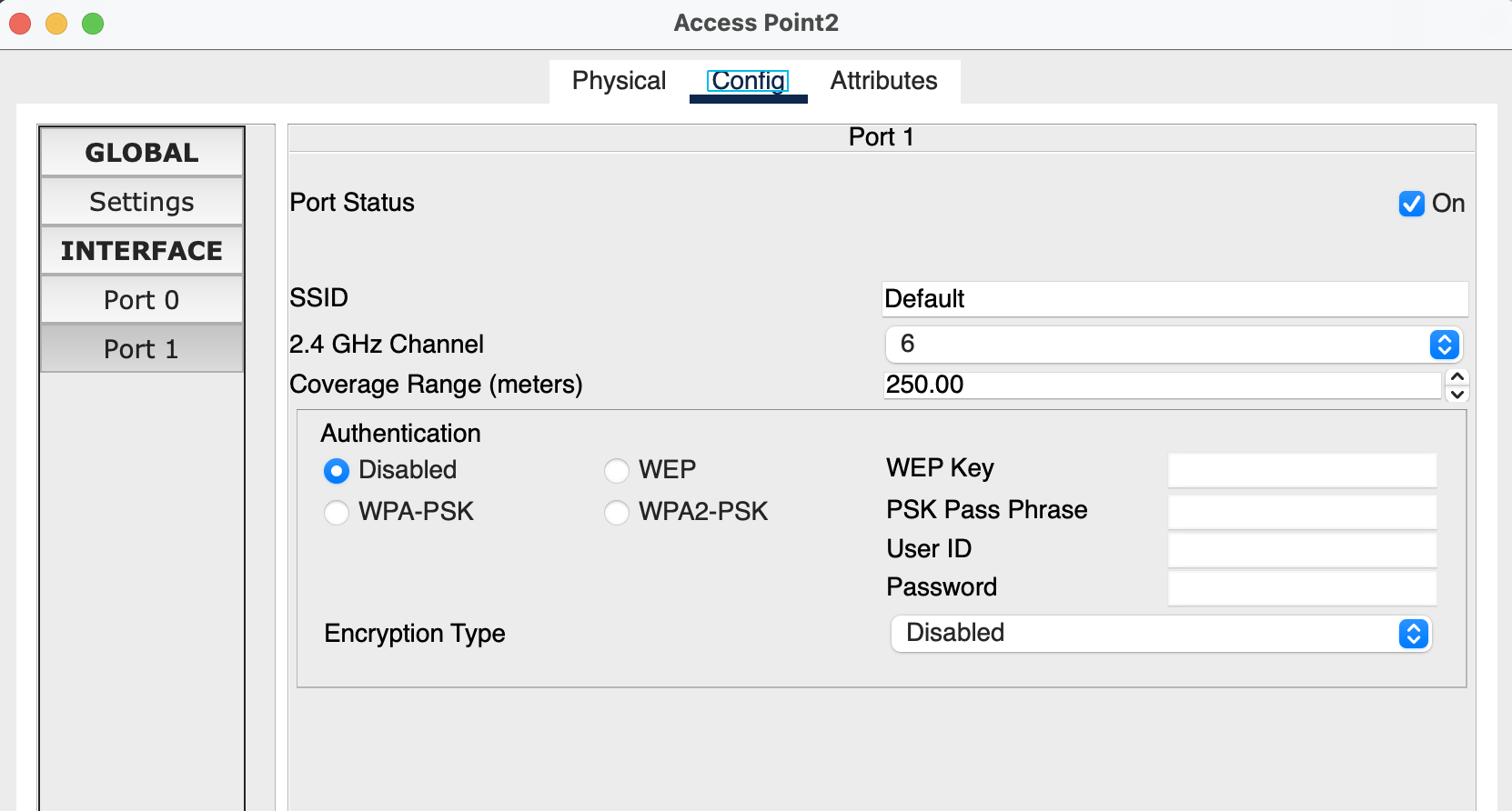
**Smartphone2 config:**

****

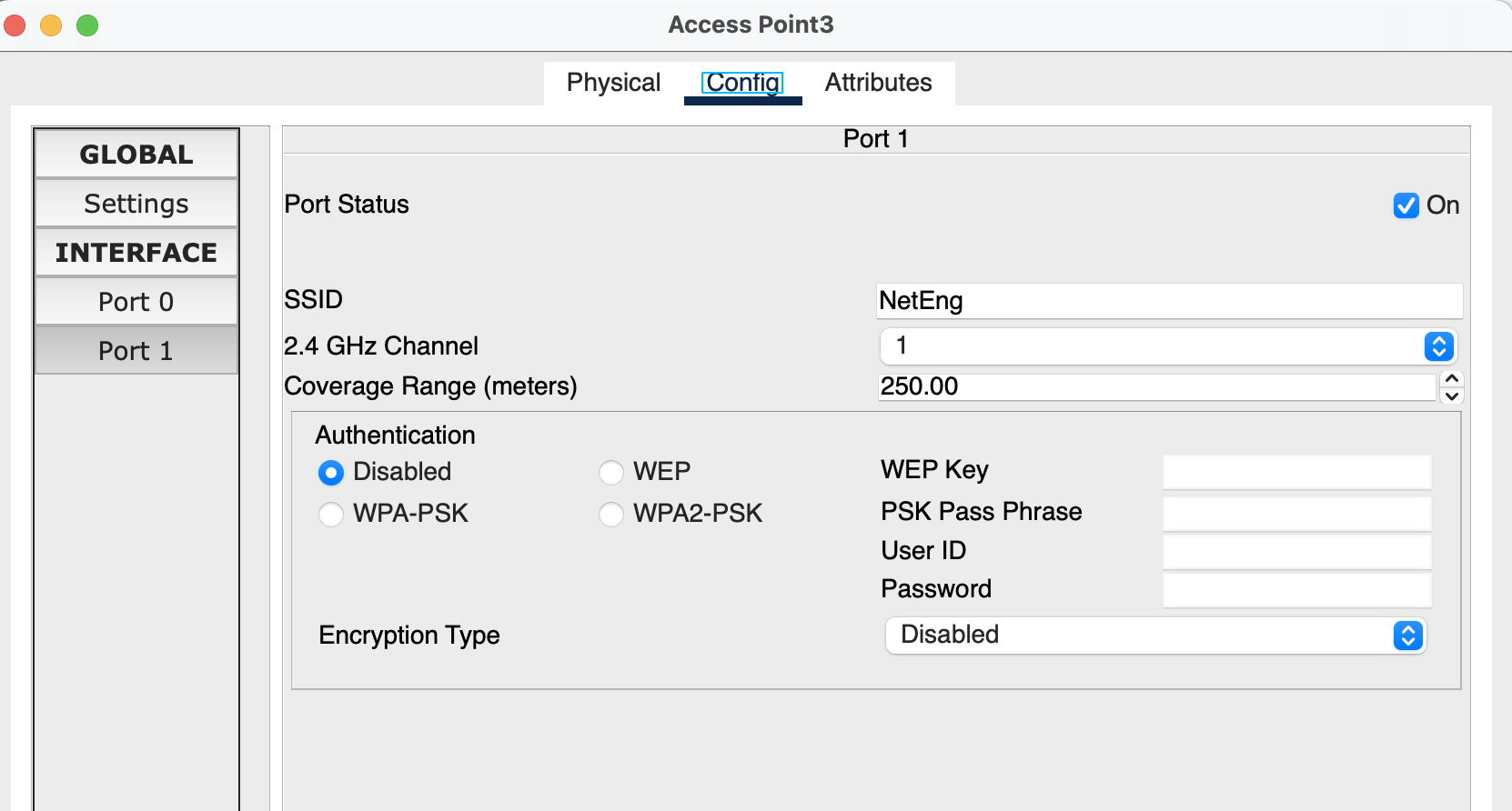
**Smartphone3 config:**

****

* 1. 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]**

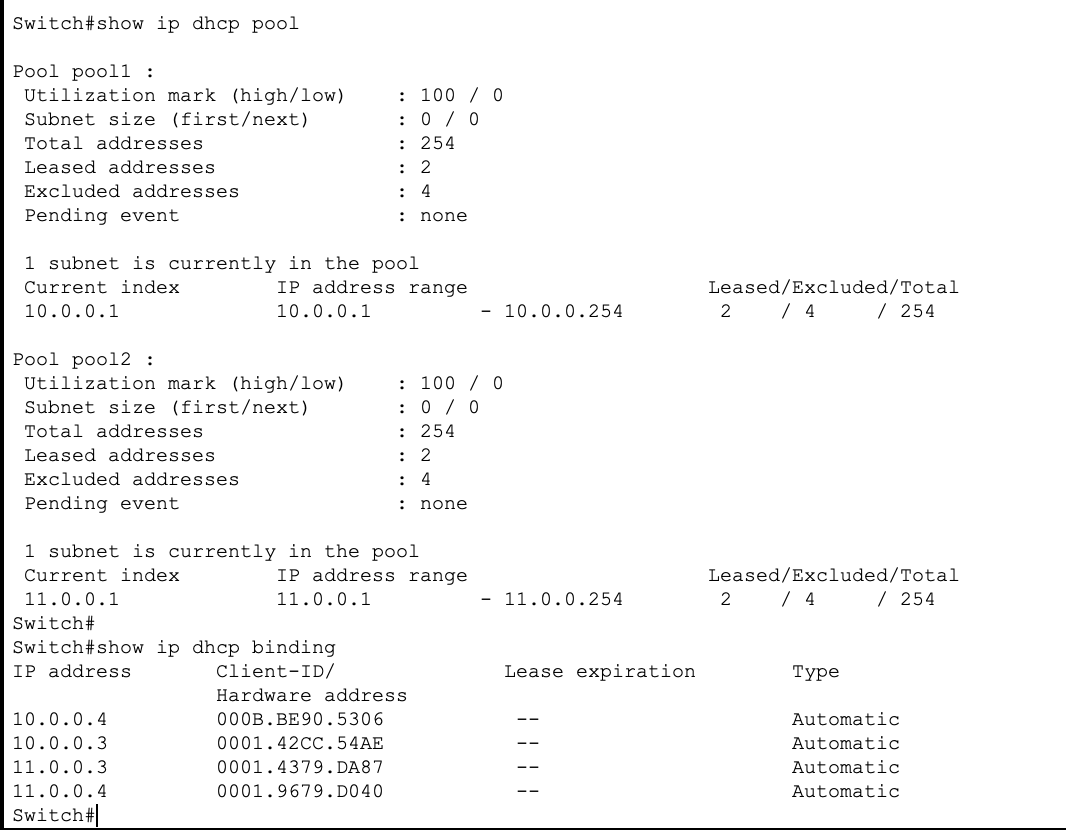
****

* 1. 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]**

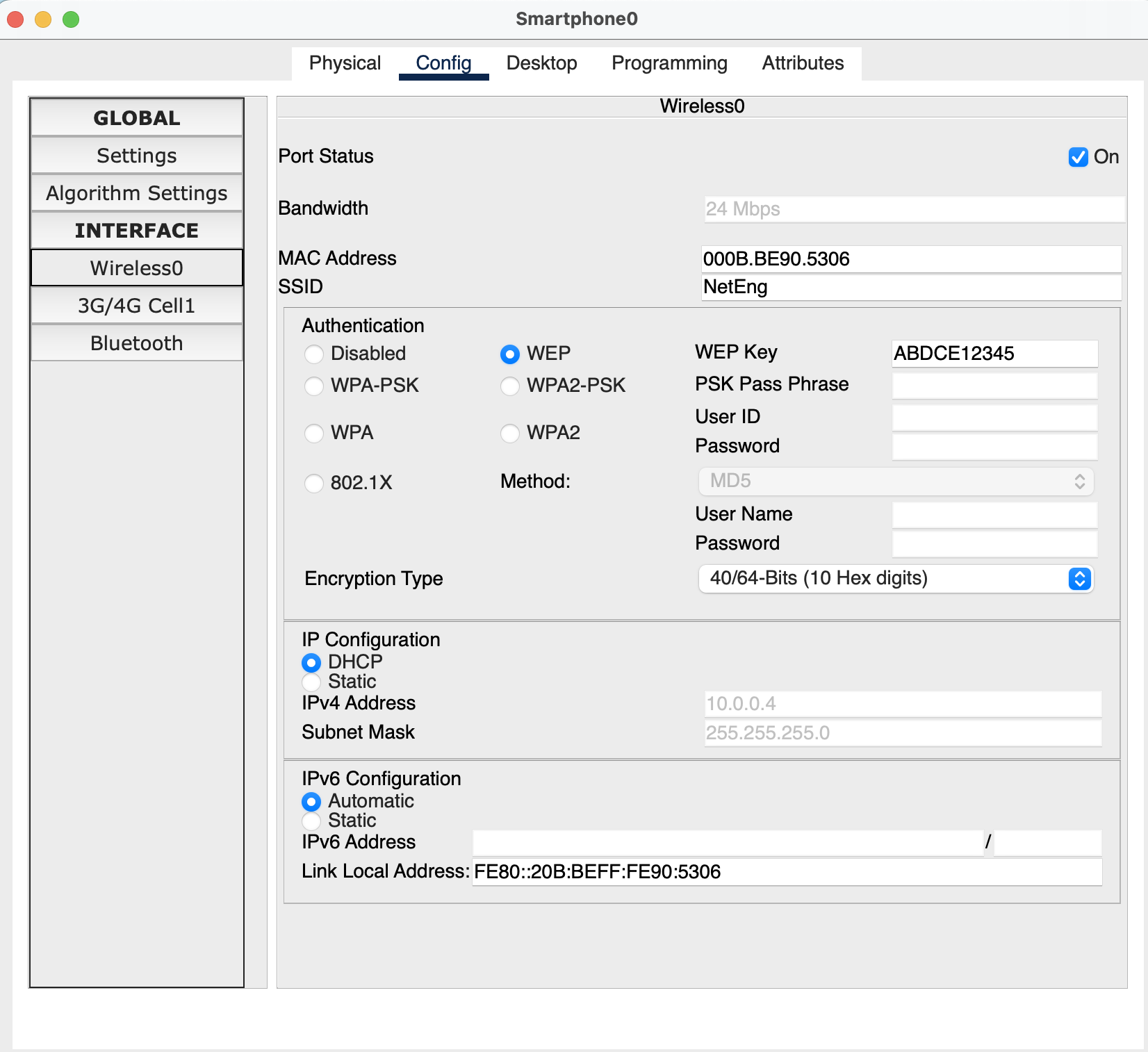
****

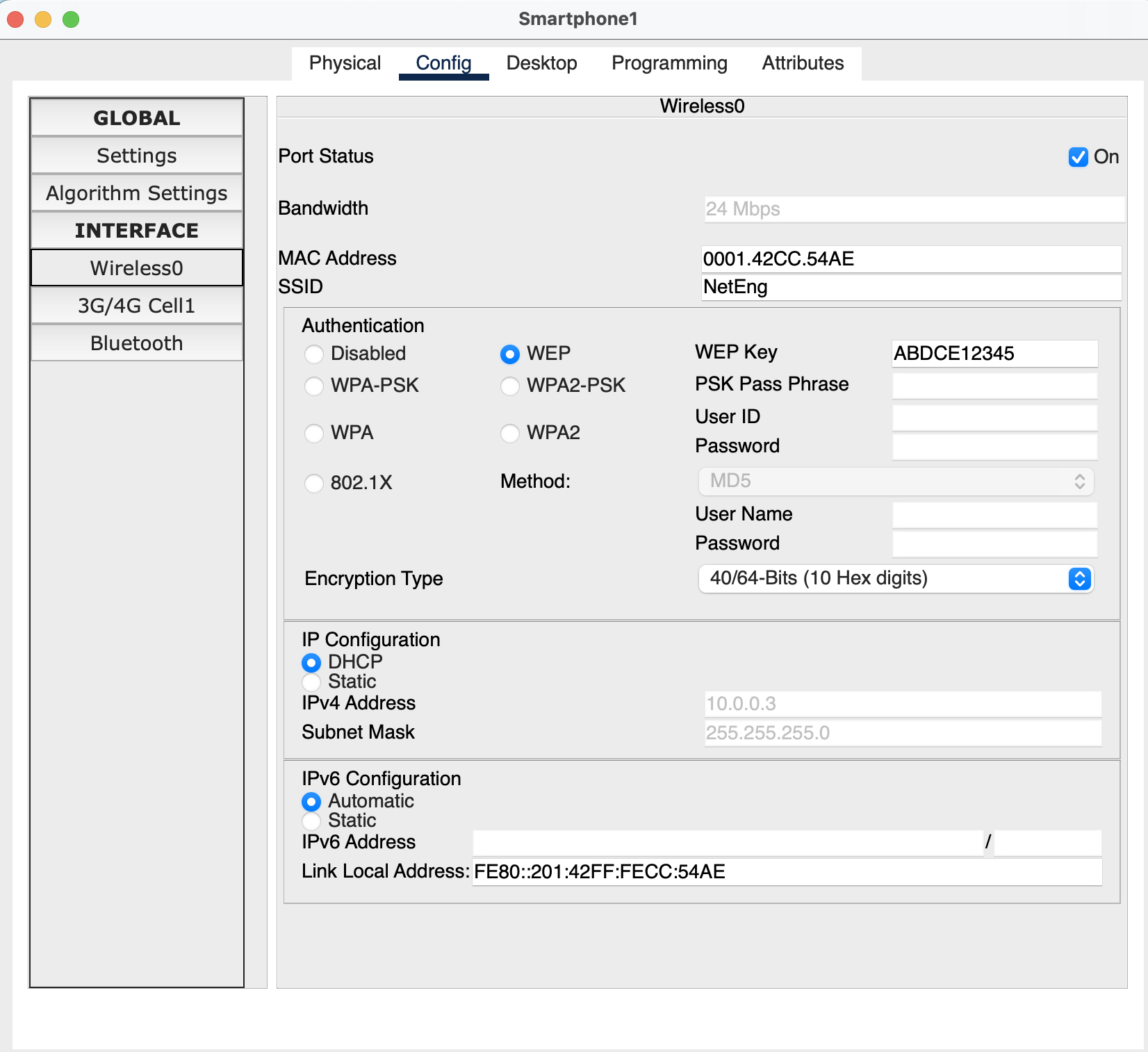
1. Configure Cisco switch 0 in a fashion that each of its four switch ports are in separate VLAN’s as shown in Figure 1 and the port connected to the router 0 as “TRUNK” port. Additionally, configure the switch as DHCP server having four different pools for it to assign IP addresses for the connecting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

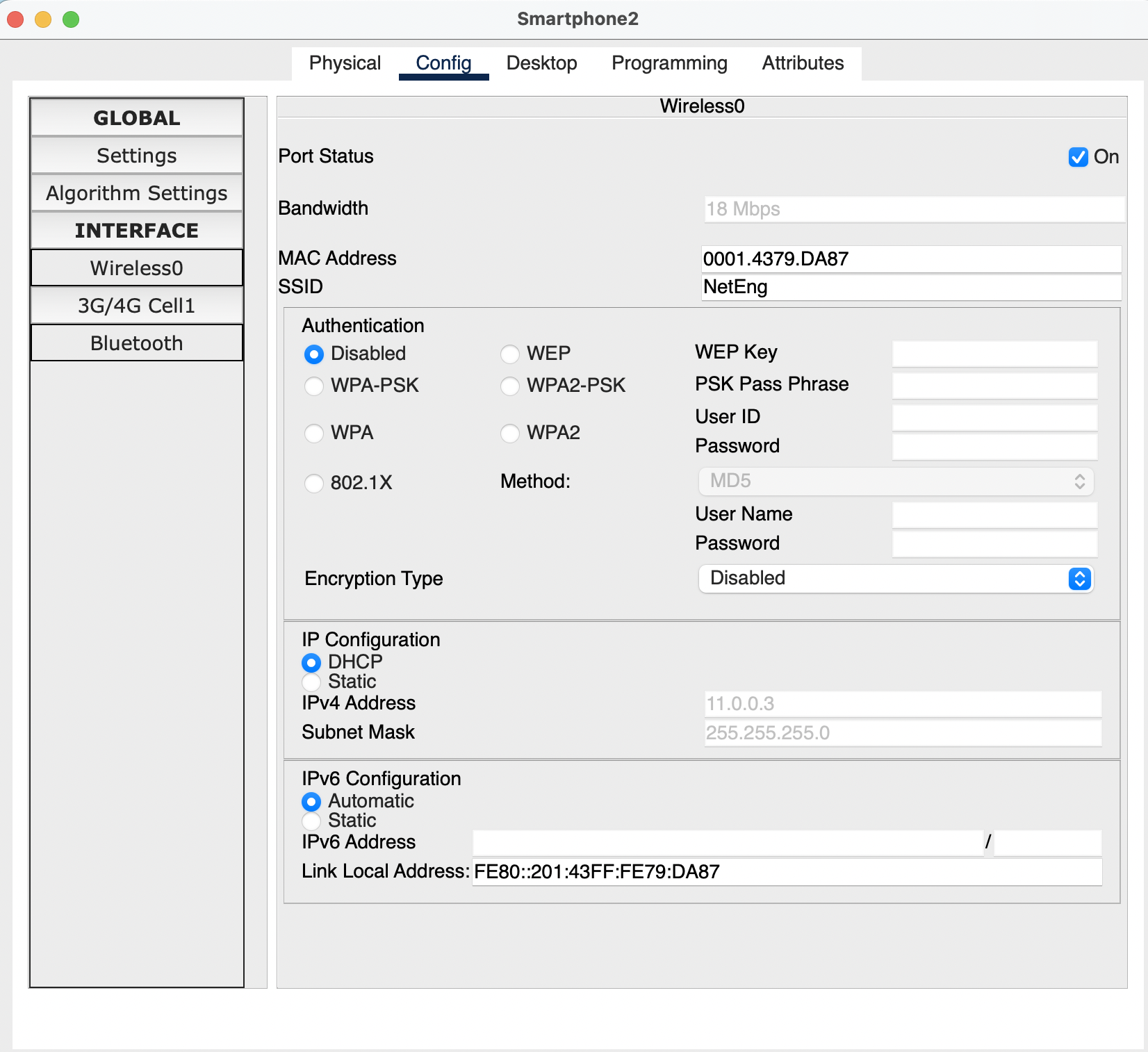
I have two subnets: 10.0.0.0/24 and 11.0.0.0/24. Here’s the pool config:

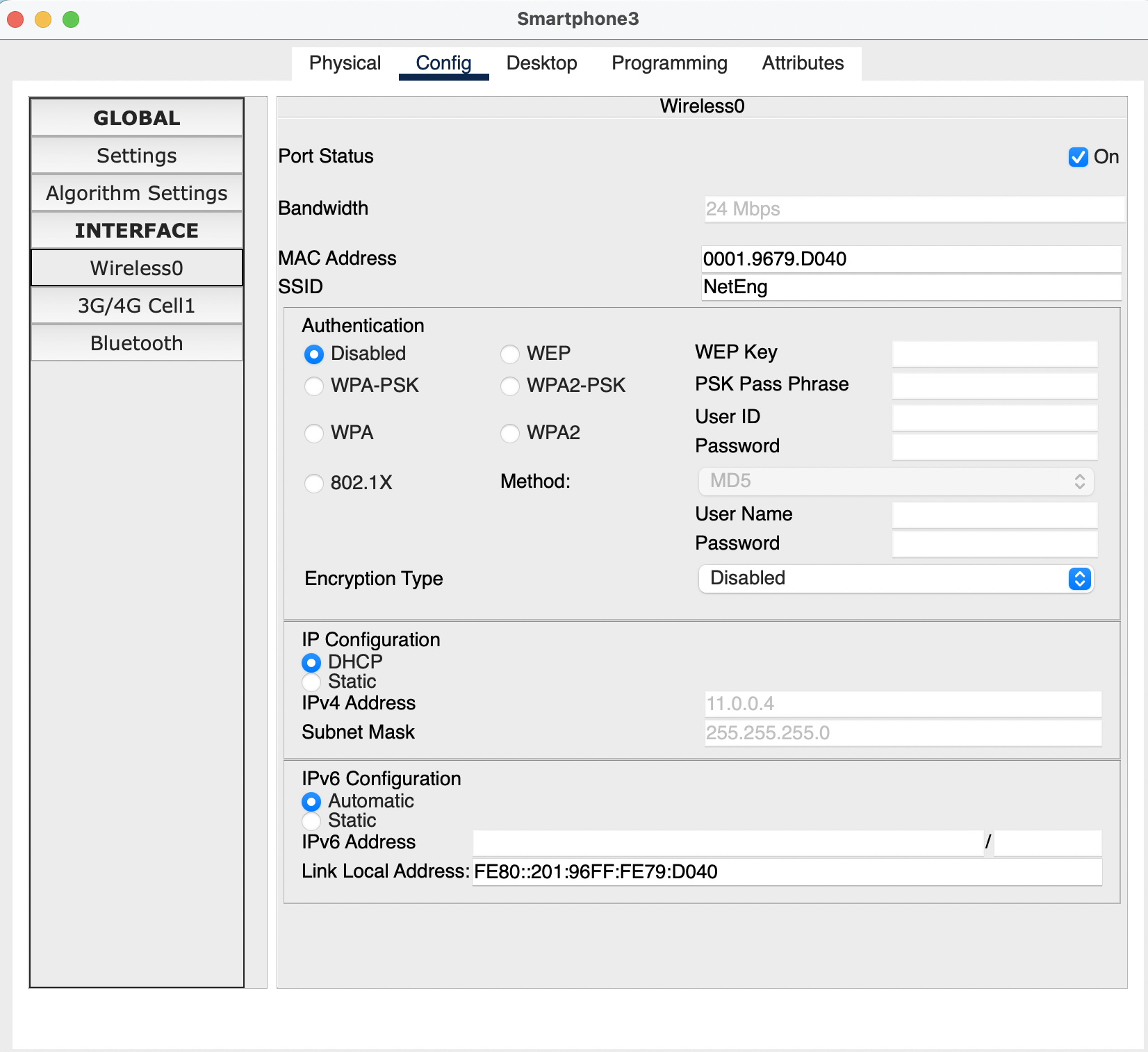
****

**Smartphones’ IP addresses:**

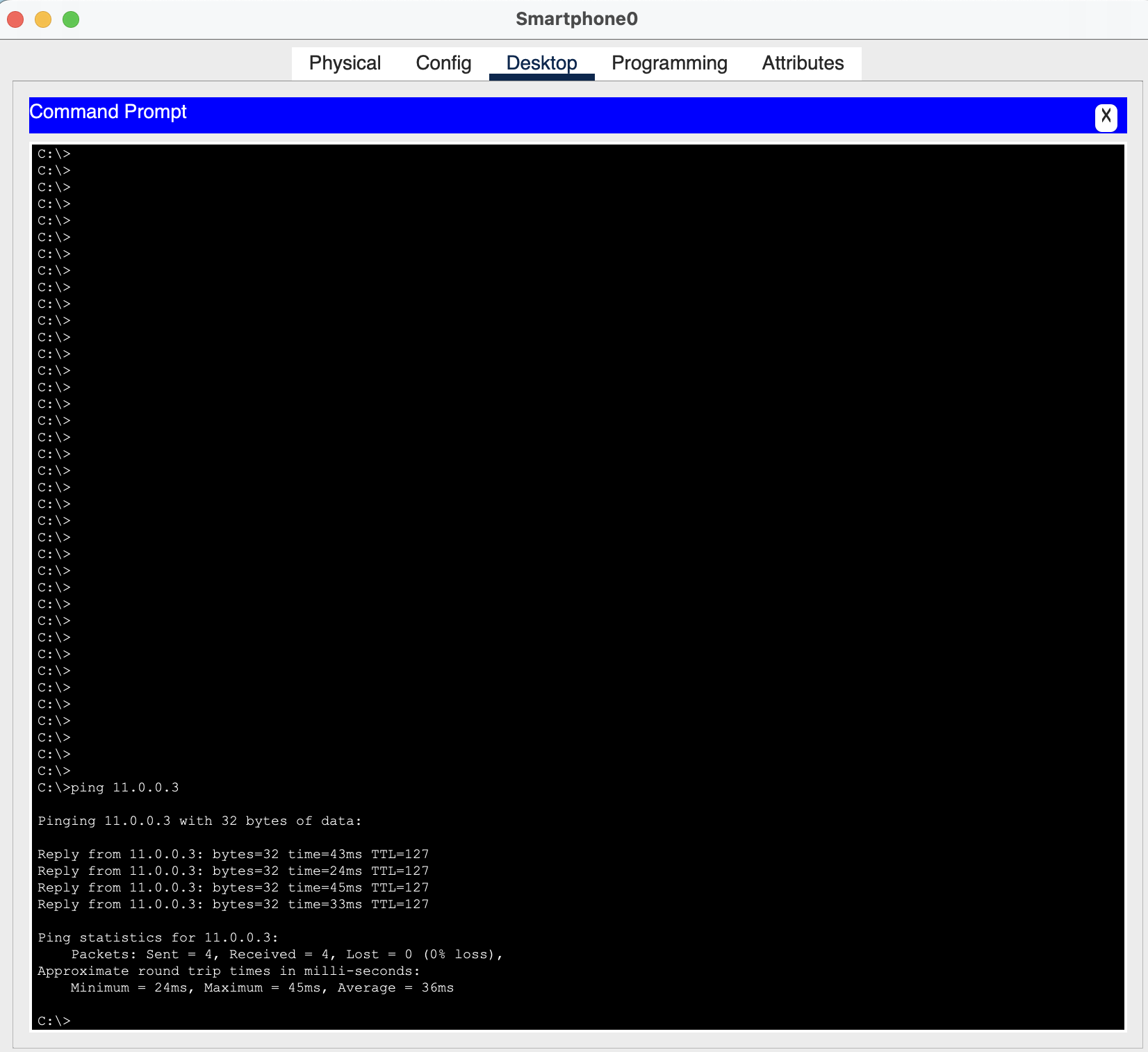
****

****

****

****

1. In order to bring connectivity between different wireless devices, configure sub-interfaces on Router 0. *Hint: Router on a Stick configuration*
2. 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.*

Yes, the ping from Smartphone 0 to Smartphone 2 was successful. This success can be attributed to the implementation of a Router-on-a-Stick configuration. Smartphone 0 has been assigned the IP address 10.0.0.4/24, while Smartphone 2 has the IP address 11.0.0.3/24. Since these devices reside on distinct subnets, a layer 3 device is necessary for communication. In this scenario, a router serves this purpose.

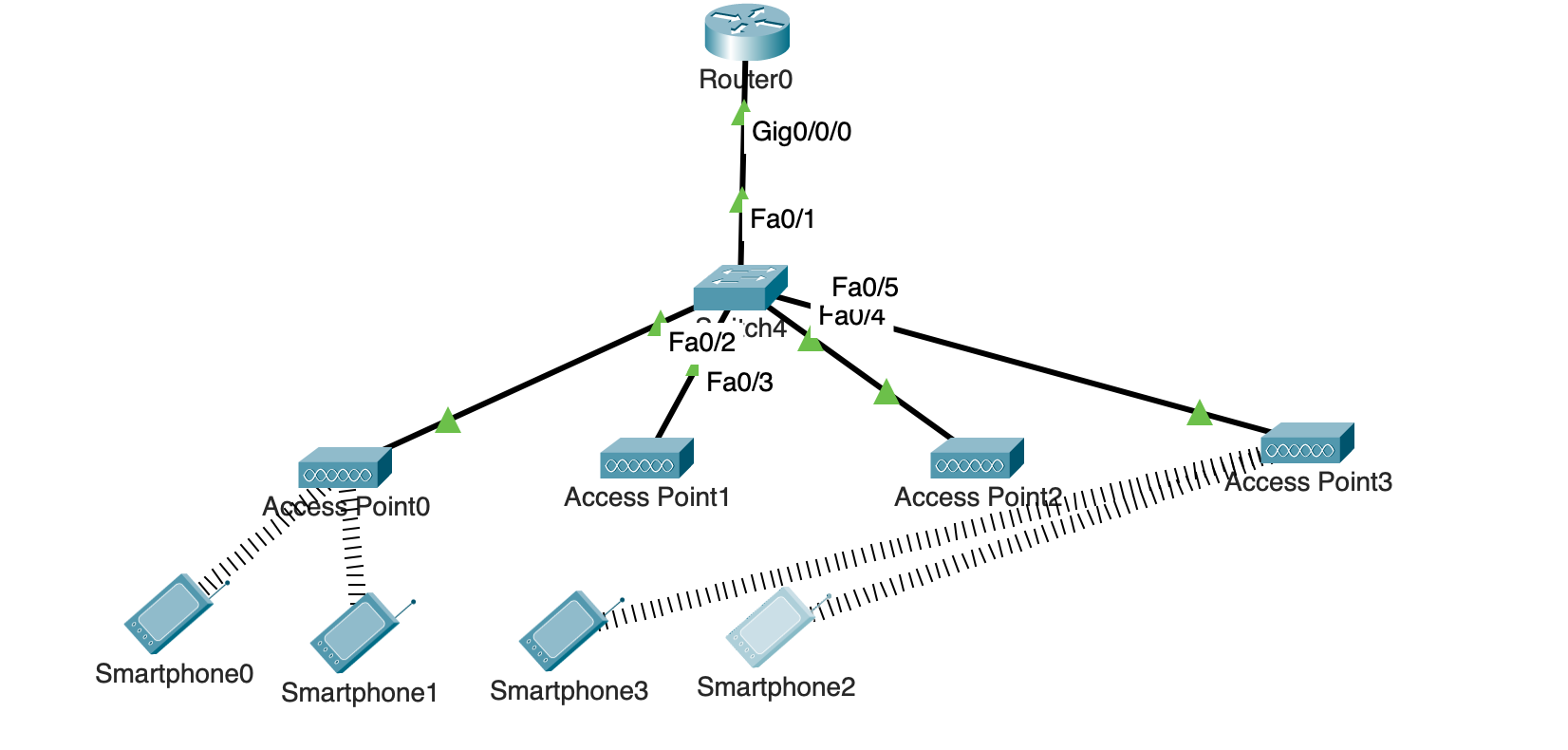
The router is configured with two sub-interfaces (Gi0/0/0.10 and Gi0/0/0.20), each assigned an IP address corresponding to the respective subnets. Specifically, Gi0/0/0.10 is configured with 10.0.0.1/24, and Gi0/0/0.20 is configured with 11.0.0.1/24. DHCP pools are established to assign default gateways to the smartphones. Smartphone 0 and Smartphone 1 are assigned 10.0.0.1/24 as their default gateway, while Smartphone 2 and Smartphone 3 have 11.0.0.1/24 as their default gateway.

When Smartphone 0 needs to communicate with the 11.0.0.0/24 subnet, it sends its traffic to its default gateway, 10.0.0.1. The router, with its connected routes for both 10.0.0.0/24 and 11.0.0.0/24 subnets, facilitates the routing process. This configuration enables the successful establishment of a ping connection.

# 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, both smartphone2 and smartphone3 got disconnected from Access Point1 and connected to Access Point3.



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

The reason for this change in behavior is due to the fact that AP1's reduced coverage of "10 meters" made it less accessible to Smartphones 2 and 3, which were now beyond the effective range. As a result, these smartphones sought an alternative access point with better signal strength, leading them to connect to AP3.

In a real-world scenario, consider a shopping mall where multiple access points are deployed to provide Wi-Fi coverage. Initially, a customer with a smartphone enters the mall and connects to AP1. However, as they move to an area that is closer to AP3, which has a stronger signal due to its extended coverage of 250 meters, the smartphone may automatically switch its connection to AP3 for a more reliable and faster connection. This behavior ensures that users maintain a seamless and optimal wireless experience as they move within the covered area.

1. 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]**

Let's examine the reasons why the smartphones opted not to connect to each of the access points (APs):

**AP0**: Despite AP0 broadcasting the "NetEng" SSID, it utilizes WEP encryption, a configuration not supported by the smartphones. As a result, the smartphones are unable to establish a connection with AP0.

**AP1**: While AP1 initially met all the connectivity requirements, the reduction in coverage from 250 meters to 10 meters placed it outside the reachable range for the smartphones. Consequently, the smartphones did not establish a connection with AP1.

**AP2**: AP2 is broadcasting the "Default" SSID, which differs from the configured "NetEng" SSID on the smartphones. This disparity in SSID configurations prevents the smartphones from connecting to AP2.

**AP3**: AP3, broadcasting the "NetEng" SSID with encryption disabled, aligns perfectly with the smartphone configurations. Consequently, the smartphones successfully connected to AP3.

In summary, the smartphones selectively connected to AP3 due to its adherence to the "NetEng" SSID with the appropriate encryption settings. The other APs presented barriers, including incompatible encryption methods, reduced coverage, and mismatched SSID configurations, leading to the smartphones not establishing connections with them.

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

**Infrastructure mode resembles the topology in this assignment.**

**Infrastructure Mode**: In this mode, wireless devices communicate through an access point (AP). The AP acts as a central hub, connecting wireless clients within its coverage range. This mode is similar to the traditional wired network infrastructure with a central connecting point.

**Ad-hoc Mode**: Also known as peer-to-peer mode, ad-hoc mode enables wireless devices to communicate directly with each other without the need for an access point. Devices in ad-hoc mode form a temporary network, suitable for scenarios where a centralized access point is unavailable or not needed.

**Mesh Mode**: In mesh mode, devices can communicate with each other directly or through intermediate devices (mesh nodes) to extend network coverage. Mesh networks are self-configuring and provide increased flexibility and redundancy.

**Repeater Mode**: A wireless repeater extends the range of an existing wireless network by receiving and retransmitting signals. It helps in bridging gaps in coverage and enhancing network reach.

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

1. Perform a site survey to analyze the RF environment and identify potential sources of interference. Adjust access point placements and configurations based on survey results.

2. Assign non-overlapping channels to neighboring access points. In the 2.4 GHz band, channels 1, 6, and 11 are non-overlapping.

3. Adjust the transmit power levels of the access points to control their coverage areas. Lowering the power level can reduce interference between neighboring access points.

4. Ensure that access points are strategically placed to provide sufficient coverage without creating excessive overlap. Overlapping cells can lead to interference.

5. Promote the use of the 5 GHz band over the 2.4 GHz band. The 5 GHz band generally has more available channels and is less congested.

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

**In this lab, we used WEP Encryption type.**

**WEP (Wired Equivalent Privacy):**

Encryption Type: WEP uses a simple encryption algorithm to secure wireless communication.

Security Level: Considered weak and vulnerable to various attacks.

**WPA (Wi-Fi Protected Access):**

Improvement over WEP: Introduced as a more secure replacement for WEP.

Encryption Types:

WPA: Uses TKIP (Temporal Key Integrity Protocol).

WPA2: Improved version using AES (Advanced Encryption Standard).

Security Level: WPA2 is considered secure for most purposes.

**WPA3 (Wi-Fi Protected Access 3):**

Enhancements over WPA2: Provides stronger security features.

Encryption Types: Utilizes WPA3-Personal and WPA3-Enterprise modes.

Security Level: Currently the most advanced and recommended standard for Wi-Fi security.

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

2.4 GHz band & 5 GHz band

These bands are available for use without the need for a specific license, making them widely utilized for various wireless technologies, including Wi-Fi networks.

# Total Score = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/157