NATIONAL UNIVERSITY OF COMPUTER AND EMERGING SCIENCES

DEPARTMENT OF COMPUTER SCIENCE

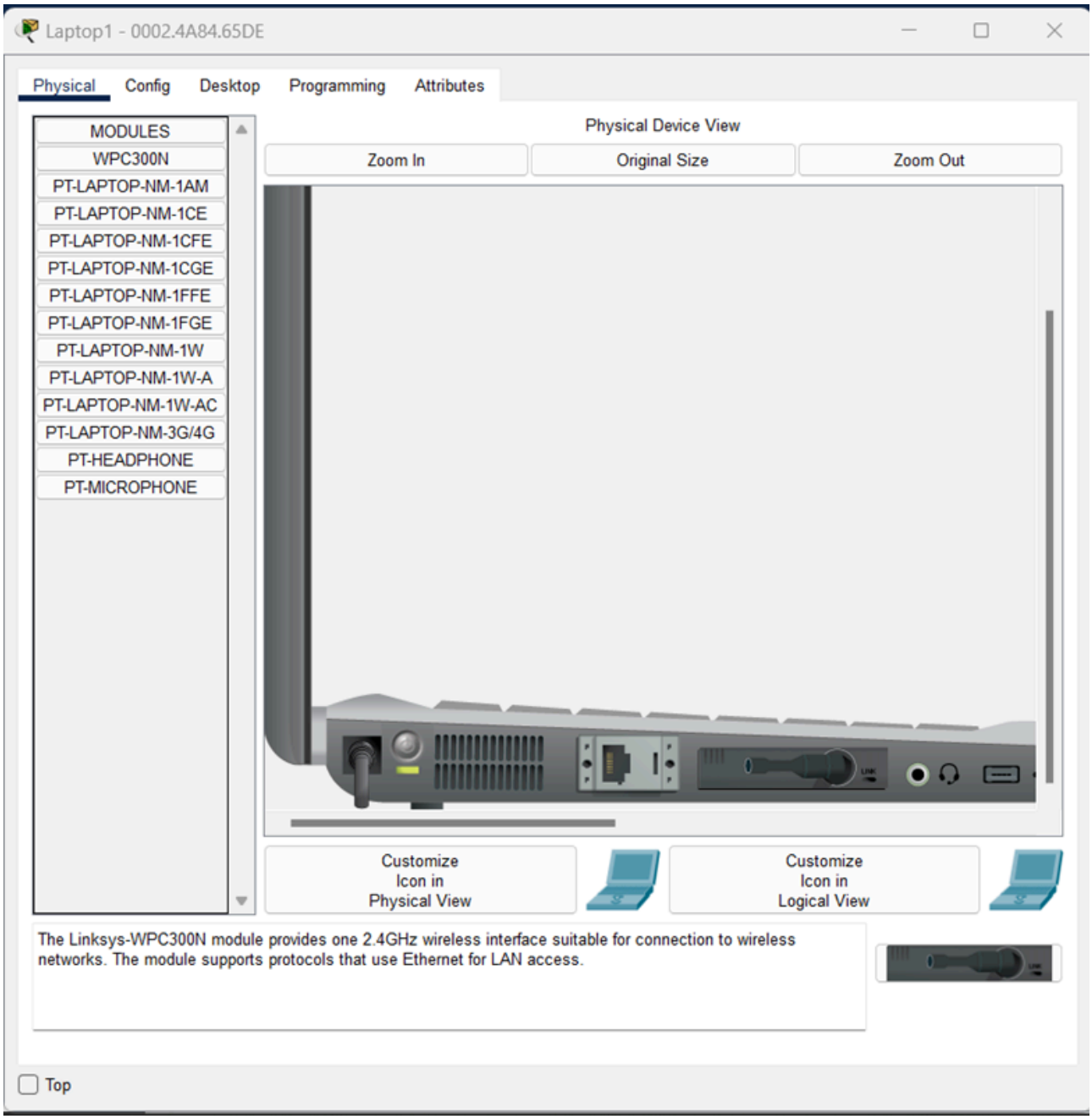
CONFIGURATION OF THE LINKSYS WRT300N WIRELESS ACCESS POINT: A REPORT

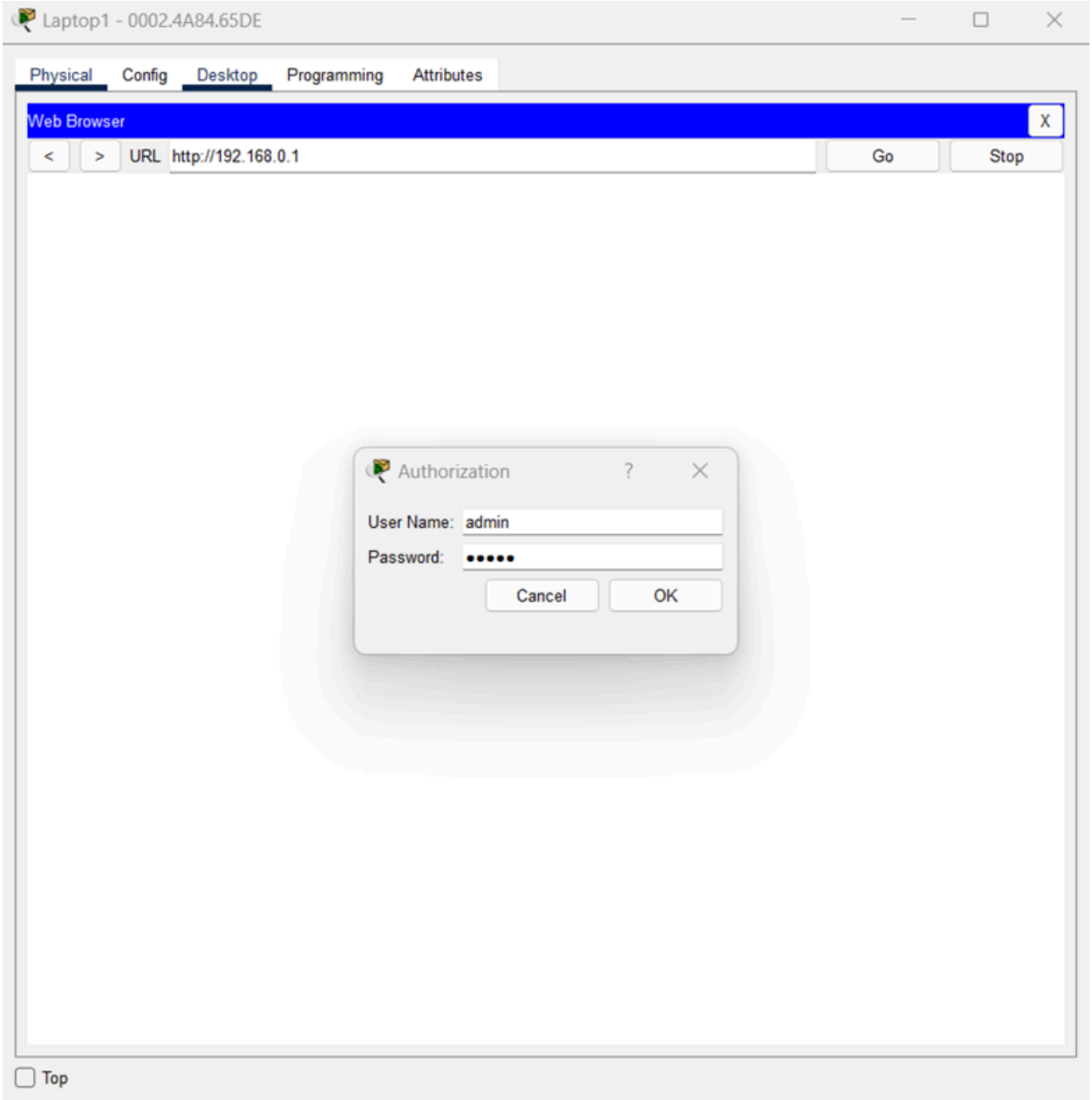
Group Members: Muhammad Yahya, 21i-2592
Muhammad Omer Nasir, 21i-2476
Mohammad Abdullah Omer, 21i-2569

Submitted on: Thursday, May 02, 2024

Task 1: Connect to Wireless Router WRT300N

- **Device Used**: Laptop1
- **Procedure**: Accessed the router's admin interface through a web browser using the URL `192.168.1.1` and logged in with the credentials `admin/admin`.
- **Screenshot(s)**:

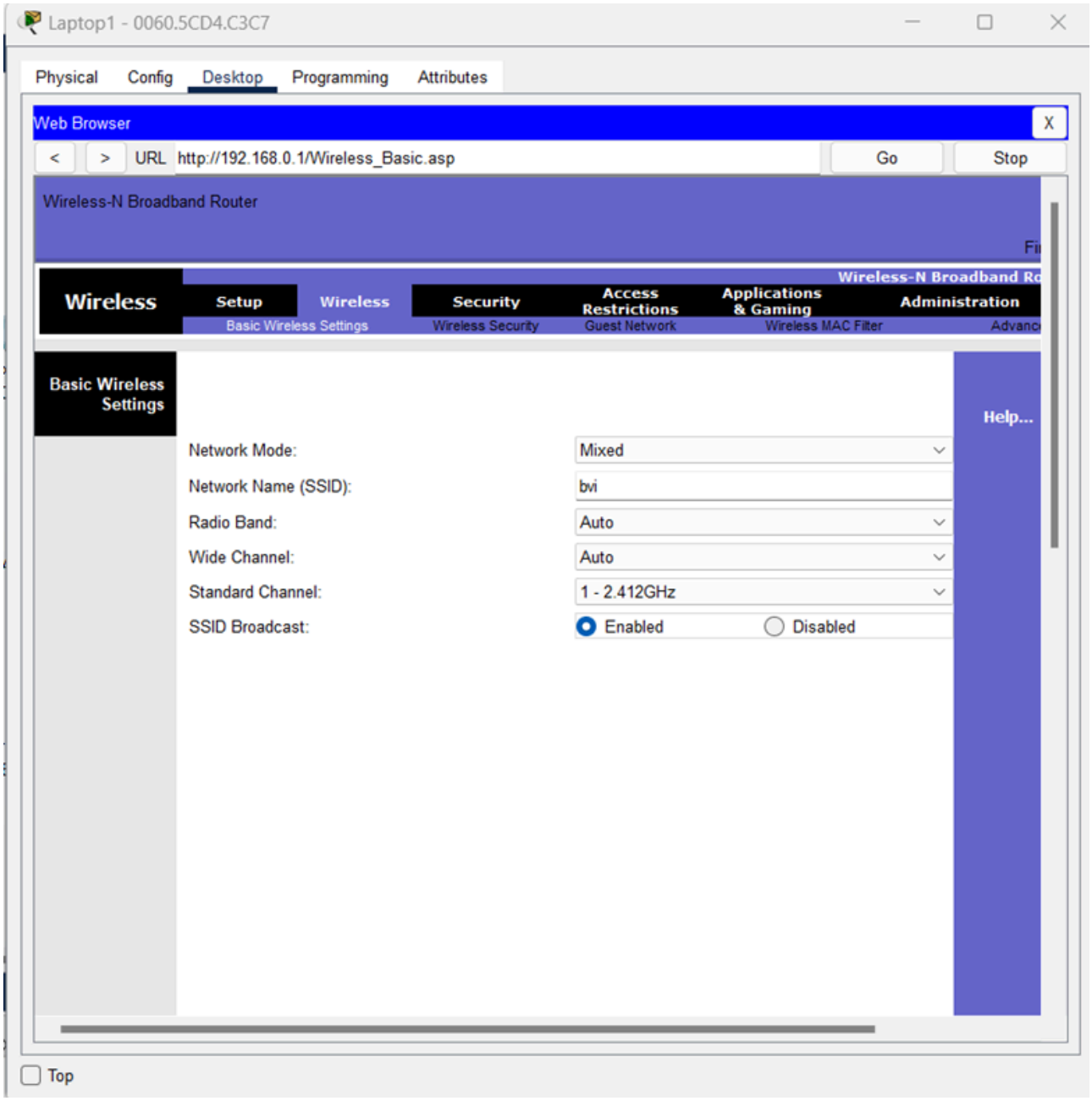


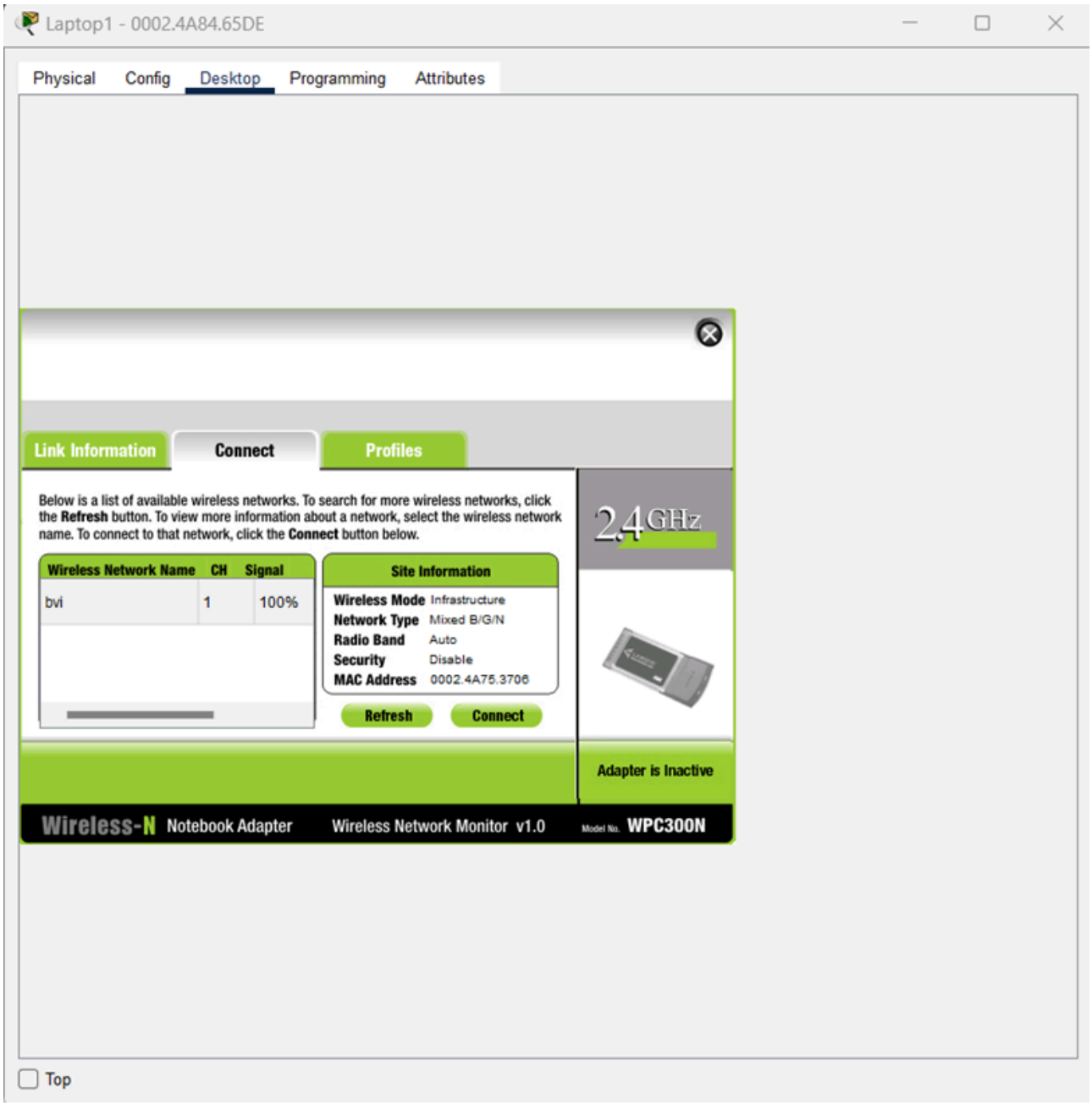


Task 2: Change SSID Name

- **New SSID**: “bvi”
- **Procedure**: Navigated to the wireless settings section and updated the SSID name from the default to “bvi”. Saved the settings and rebooted the router to apply changes.

- **Screenshot(s)**:

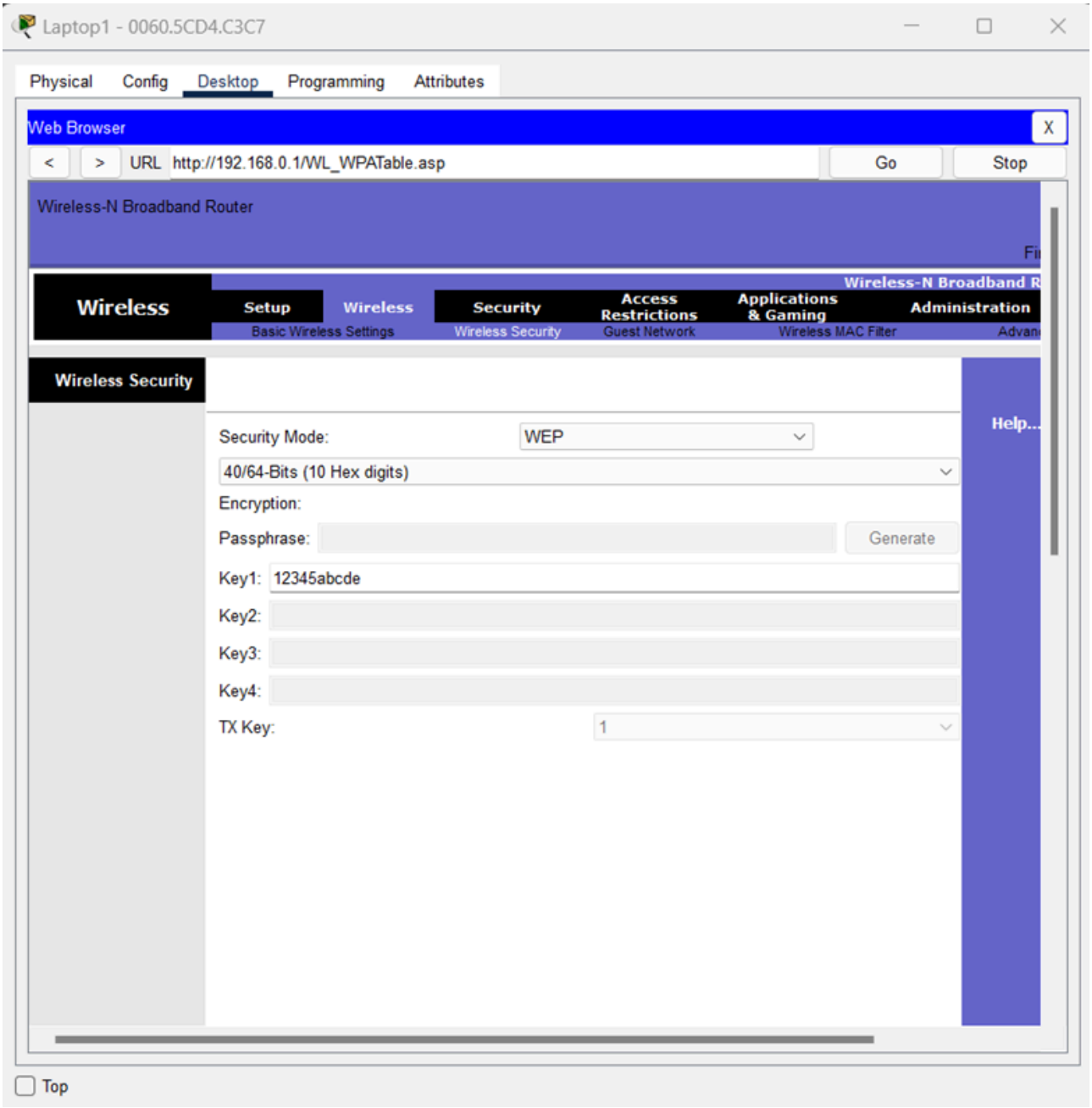




Task 3: Enable WEP Wireless Security

- **WEP Key**: “12345abcde”
- **Procedure**: Under the wireless security settings, selected WEP encryption and entered the 10 hexadecimal digits as the key. Applied and saved the settings.

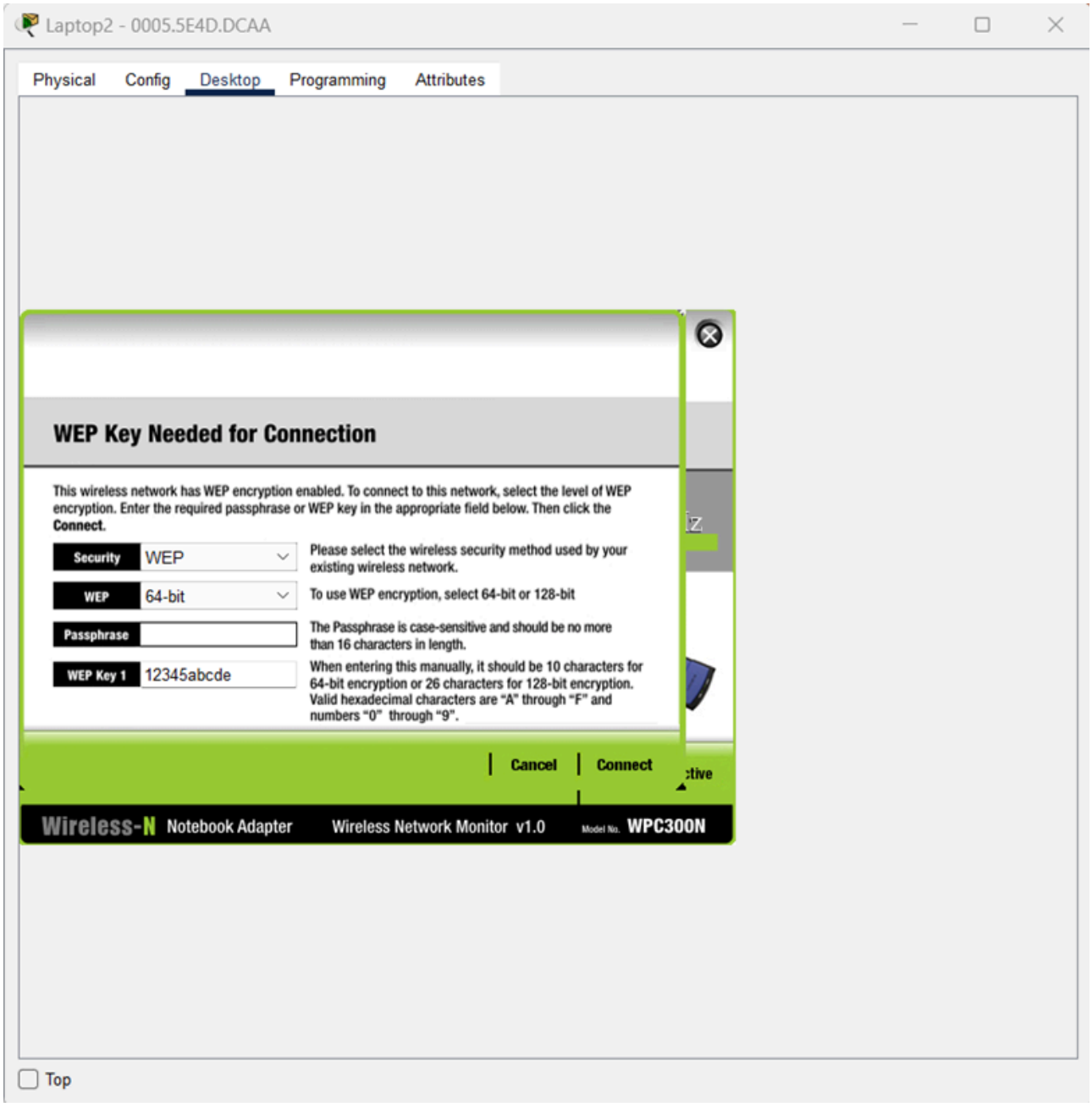
- **Screenshot(s)**:

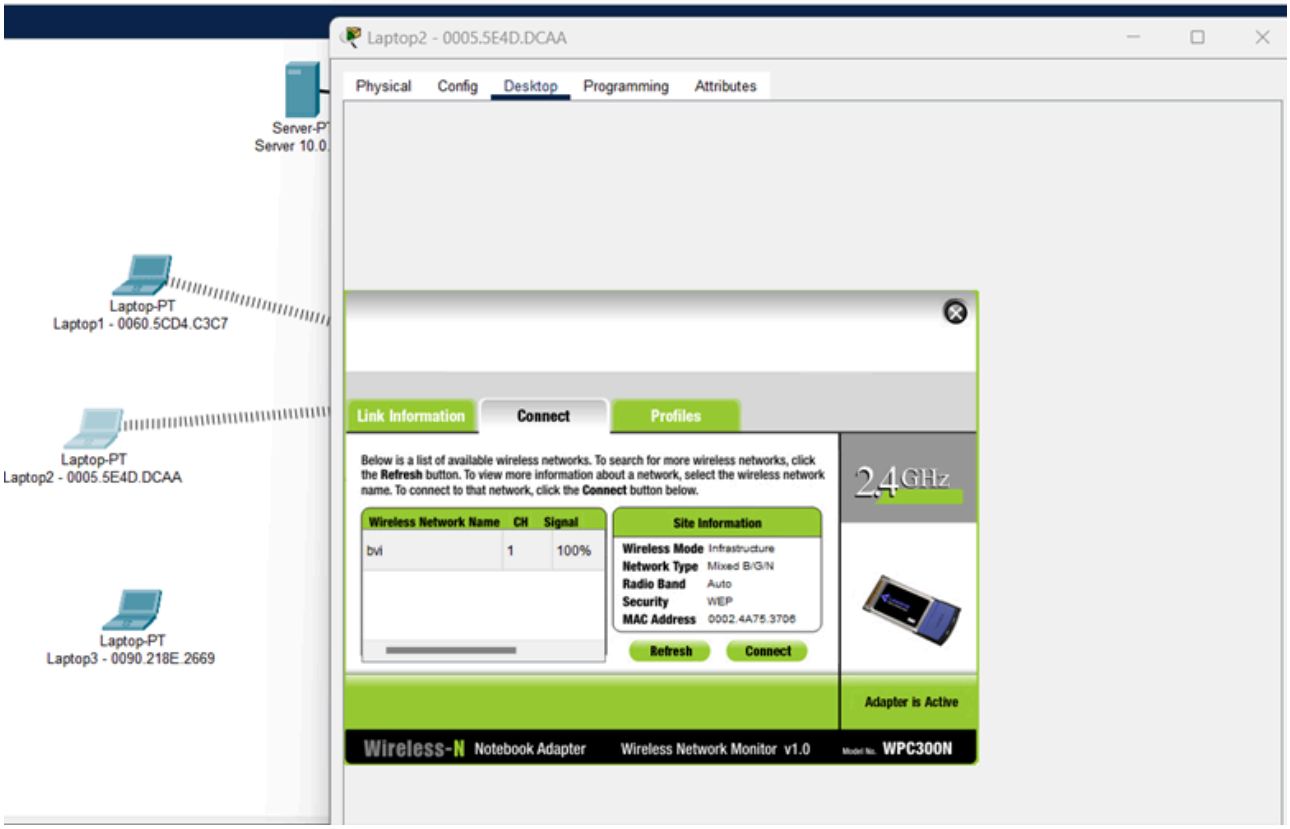


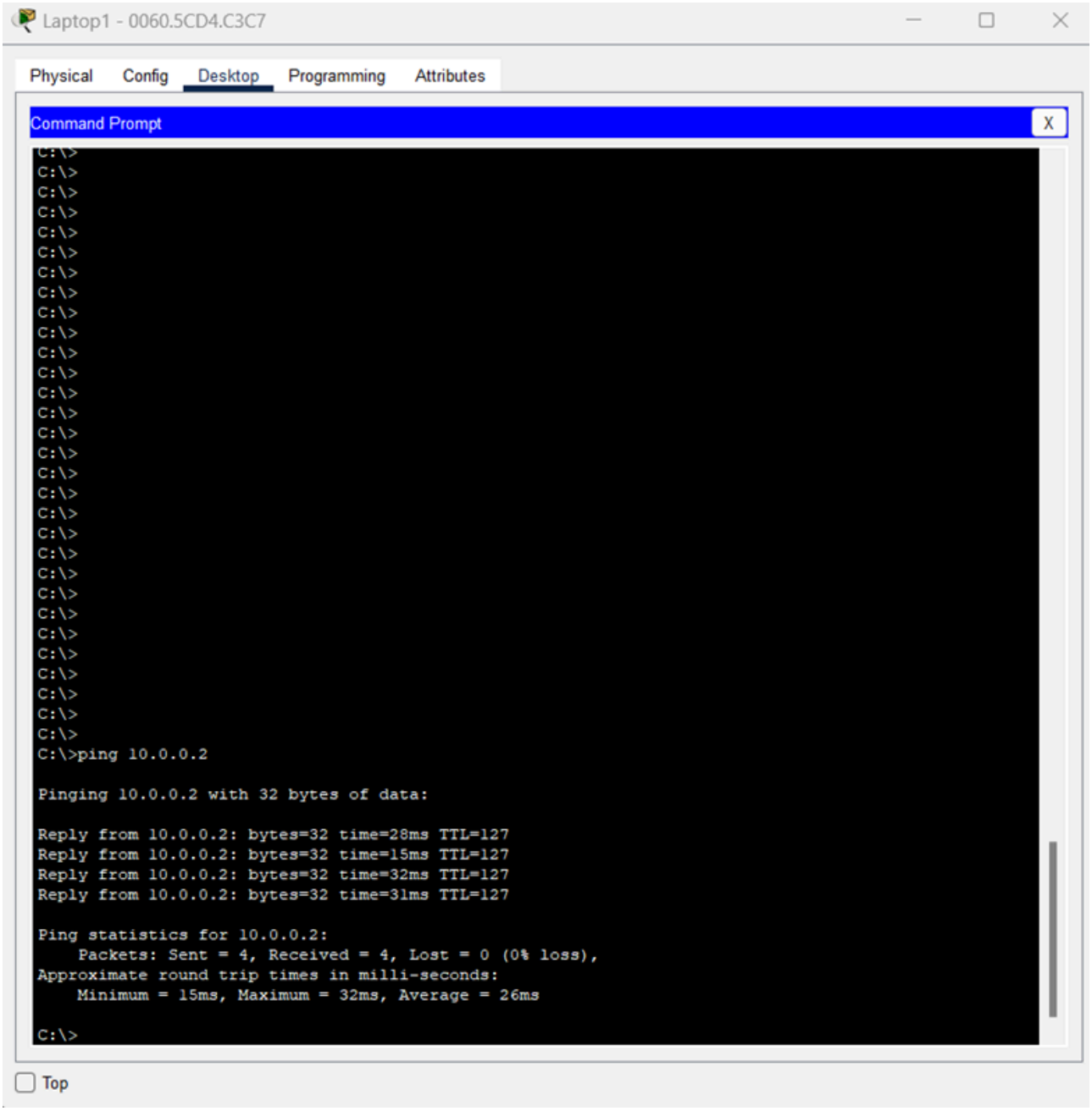
Task 4: Connect Devices to Network “bvi” using WEP Key

- **Devices**: Laptop1 and Laptop2
- **Procedure**: Configured both laptops to connect to the SSID “bvi” using the WEP key “12345abcde”. Both devices were connected successfully. Performed a ping test to the server at `10.0.0.2` which returned successful replies.

- **Screenshot(s)**:



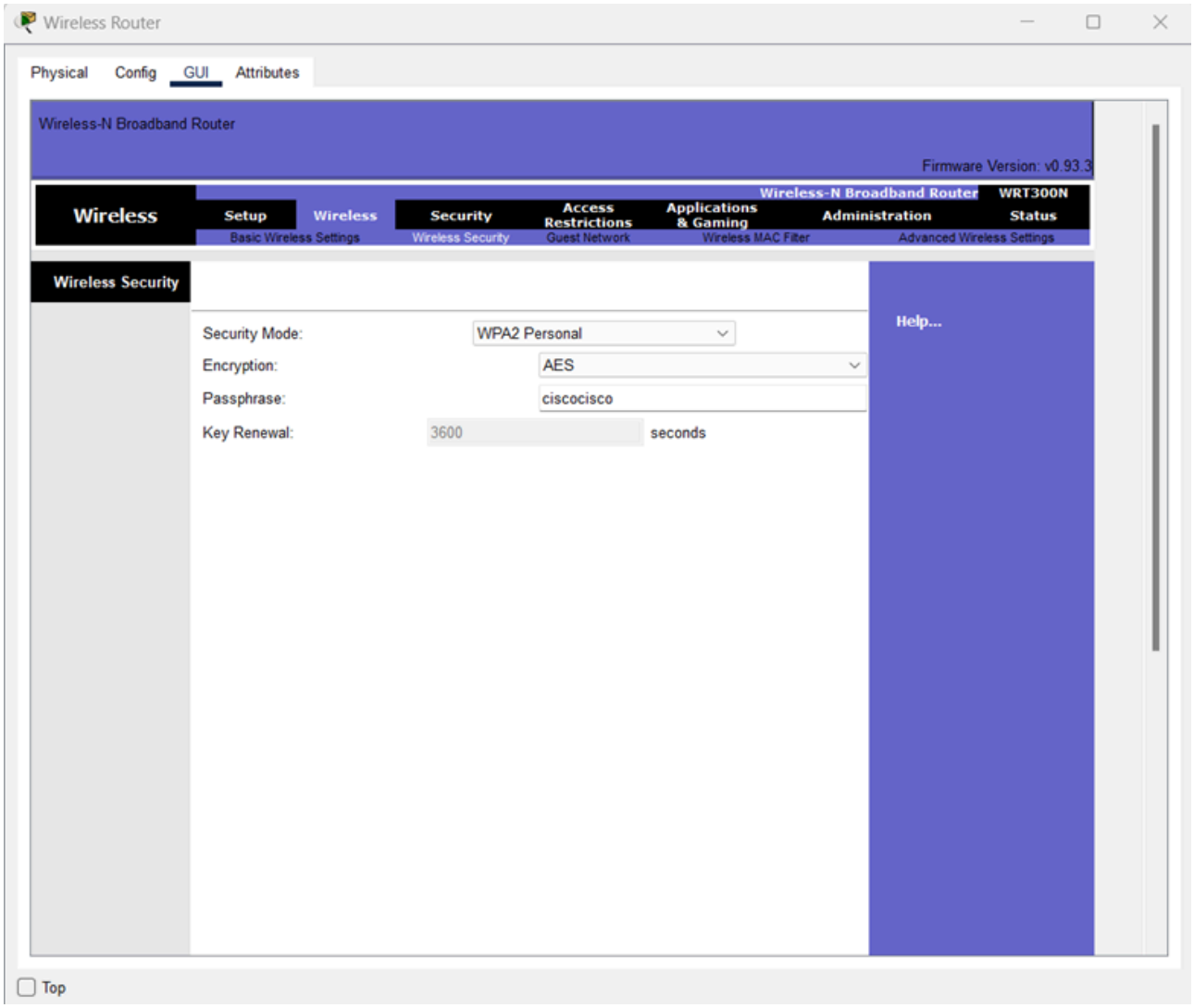

Laptop2 - 0005.5E4D.DCAA
Physical
Config
Desktop
Programming
Attributes
Server-PT
Server 10.0.
Laptop-PT
Laptop1 - 0060.5CD4.C3C7
Laptop-PT
Laptop2 - 0005.5E4D.DCAA
Laptop-PT
Laptop3 - 0090.218E.2669
Link Information
Connect
Profiles
Below is a list of available wireless networks. To search for more wireless networks, click the Refresh button. To view more information about a network, select the wireless network name. To connect to that network, click the Connect button below.
2.4GHz
Wireless Network Name
CH
Signal
bvi
1
100%
Site Information
Wireless Mode Infrastructure
Network Type Mixed B/G/N
Radio Band Auto
Security WEP
MAC Address 0002.4A75.3706
Refresh
Connect
Adapter is Active
Wireless-N Notebook Adapter
Wireless Network Monitor v1.0
WPC300N



Task 5: Change Wireless Security to WPA2 PSK AES

- **Passphrase**: “ciscocisco”
- **Procedure**: Updated the router’s wireless security settings from WEP to WPA2 PSK with AES encryption. Set the passphrase to “ciscocisco”. Saved and applied the changes.

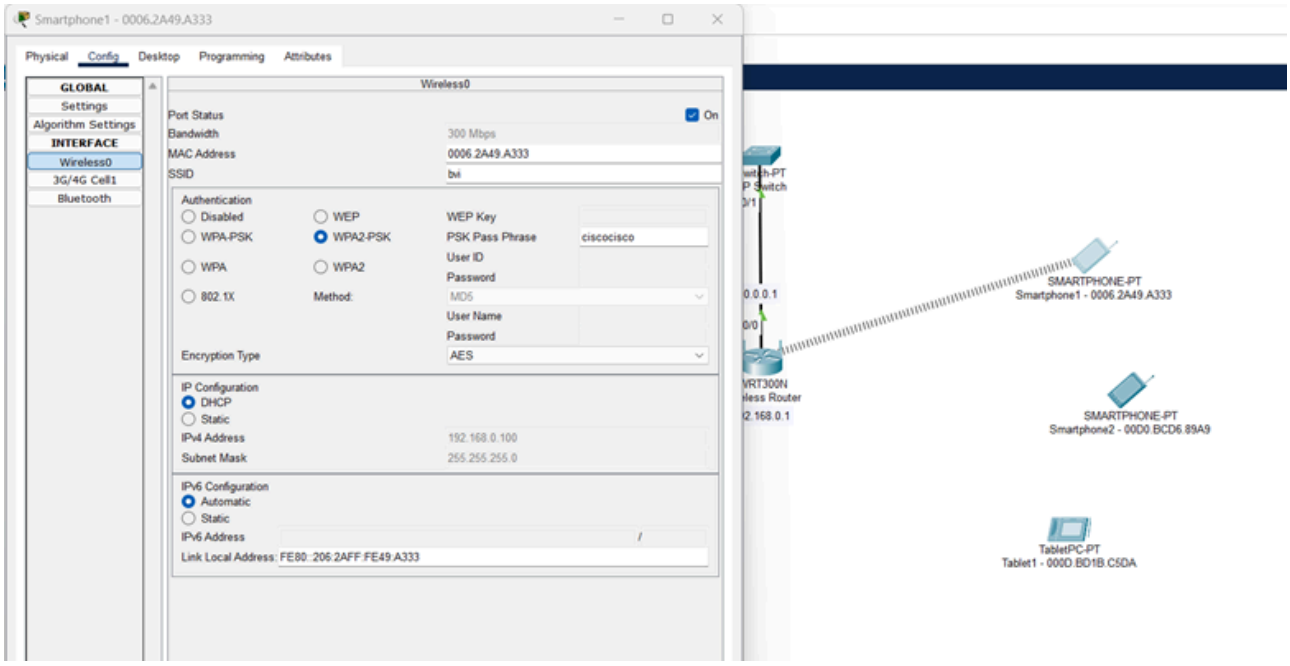
- **Screenshot(s)**:

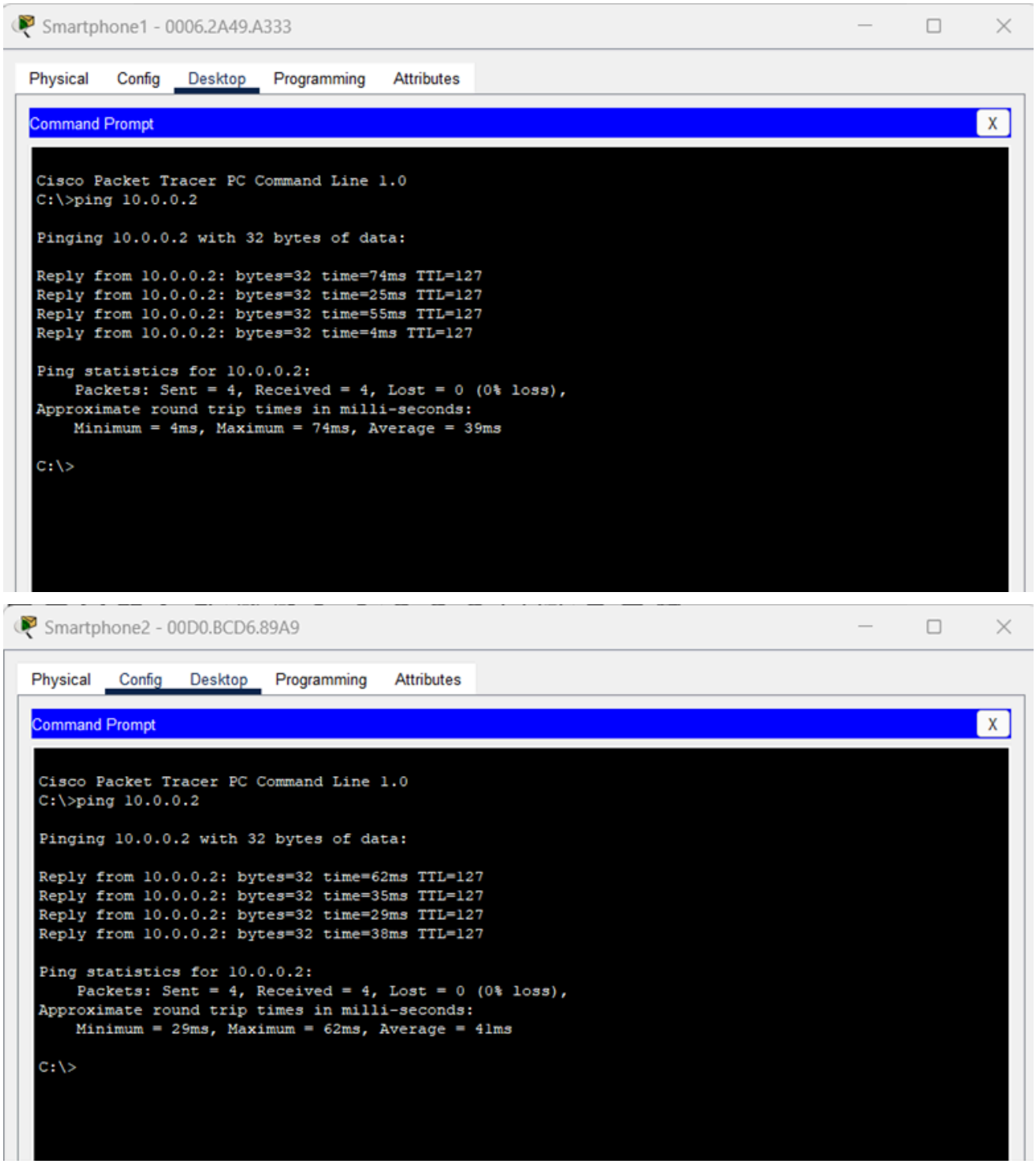


Task 6: Connect Smartphones to Network “bvi” using WPA2 PSK

- **Devices**: Smartphone1 and Smartphone2
- **Procedure**: Configured both smartphones to connect to “bvi” using the new WPA2 PSK AES passphrase “ciscocisco”. Both smartphones connected successfully and were able to ping the server at `10.0.0.2`.

- **Screenshot(s)**:

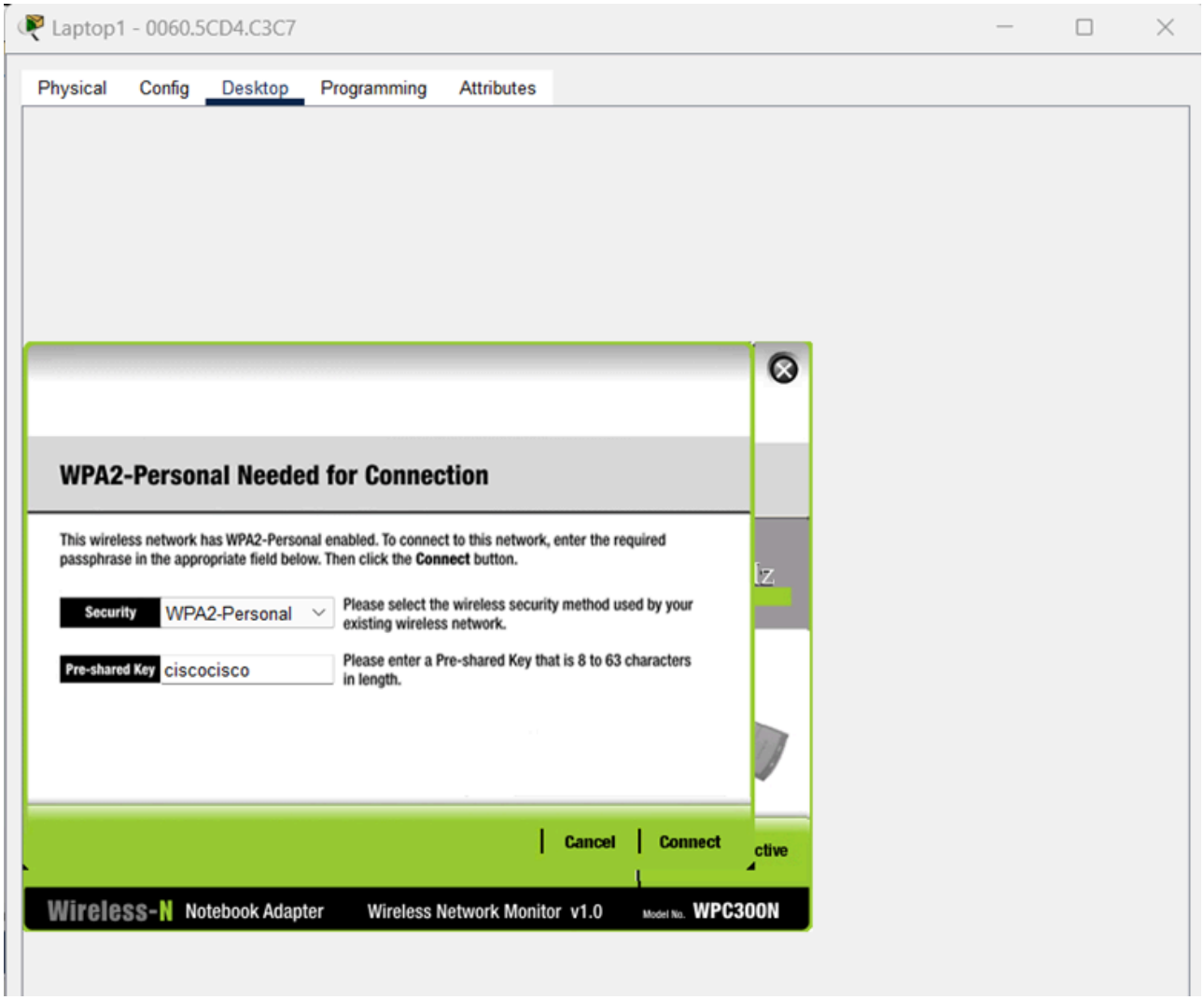


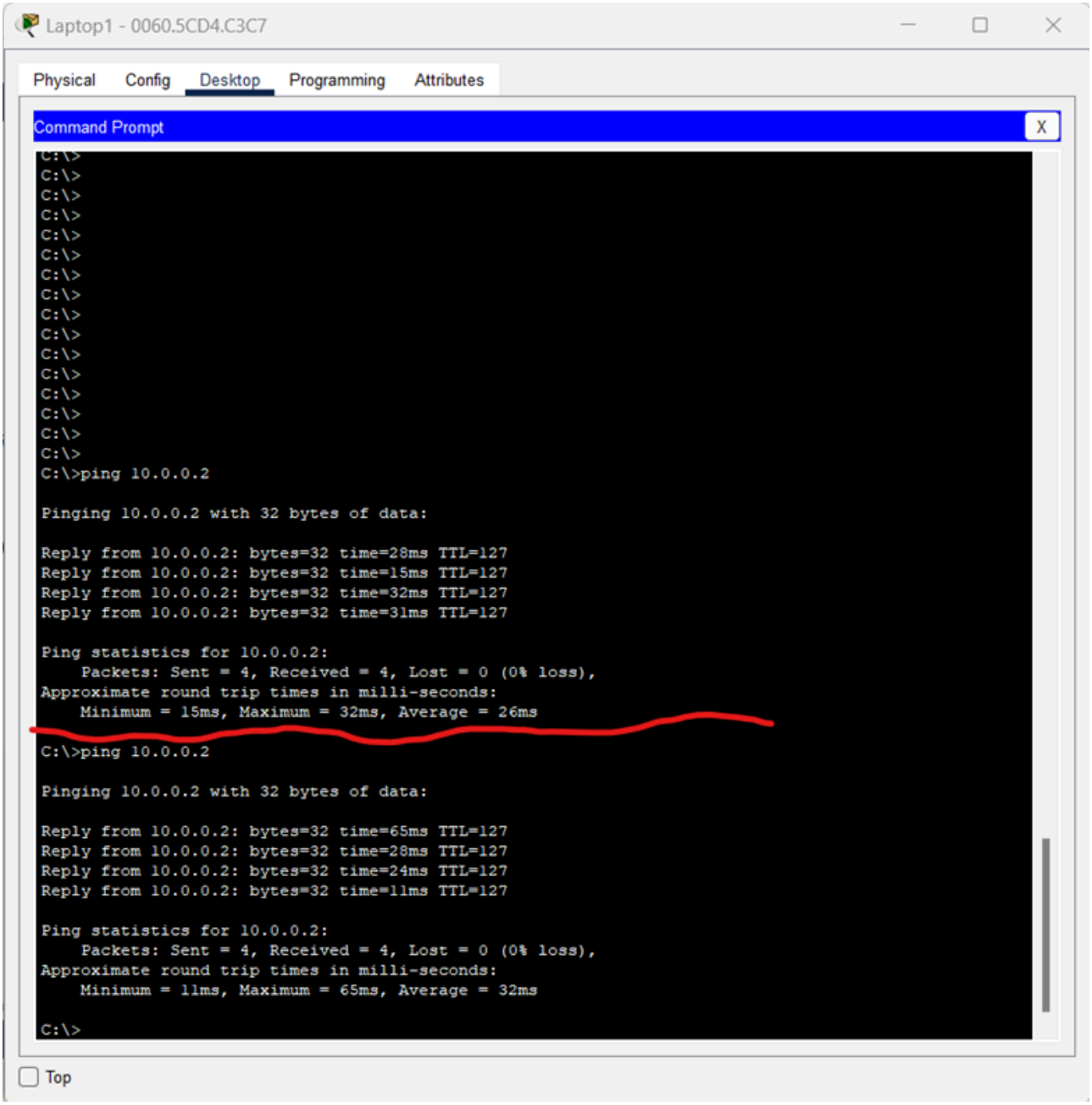


Task 7: Reconnect Laptops to Network “bvi” using WPA2 PSK

- **Devices**: Laptop1 and Laptop2
- **Procedure**: Reconfigured both laptops to connect to the “bvi” network using the updated WPA2 PSK AES settings. After successful connection, conducted a ping test to `10.0.0.2`, which was successful.

- **Screenshot(s)**:

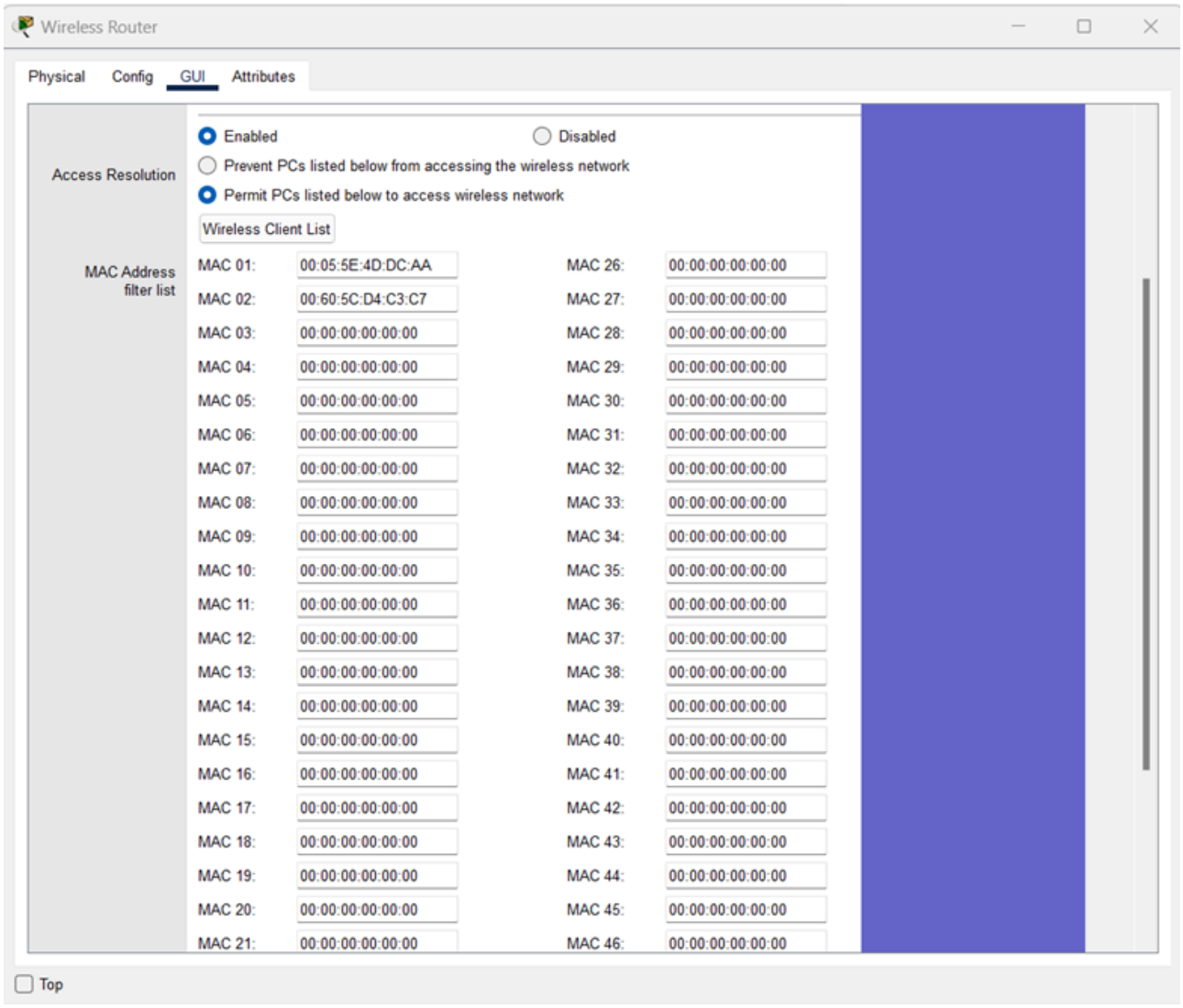


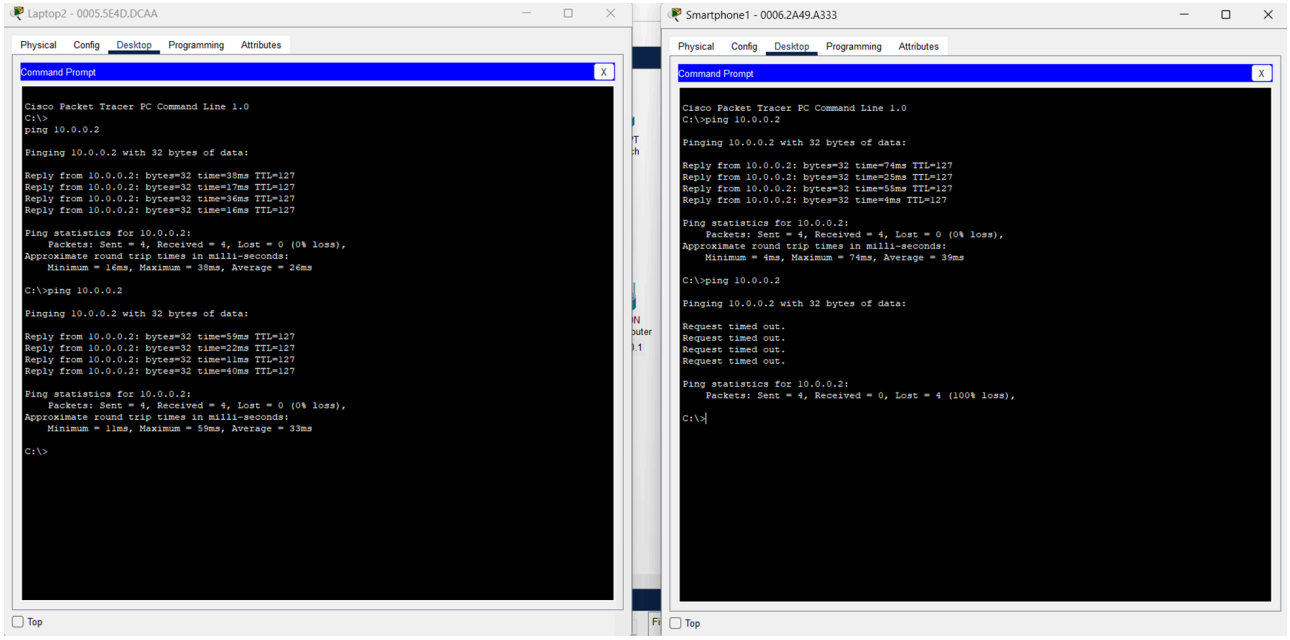


Task 8: Enable Wireless MAC Filter

- **Allowed Devices**: Laptop1 and Laptop2
- **Procedure**: Enabled MAC filtering on the router and added the MAC addresses of Laptop1 and Laptop2 to the allow list. Tested connectivity by pinging `10.0.0.2` from both laptops. Both pings were successful. Pings from Smartphone1 and Smartphone2 failed, indicating they were blocked.

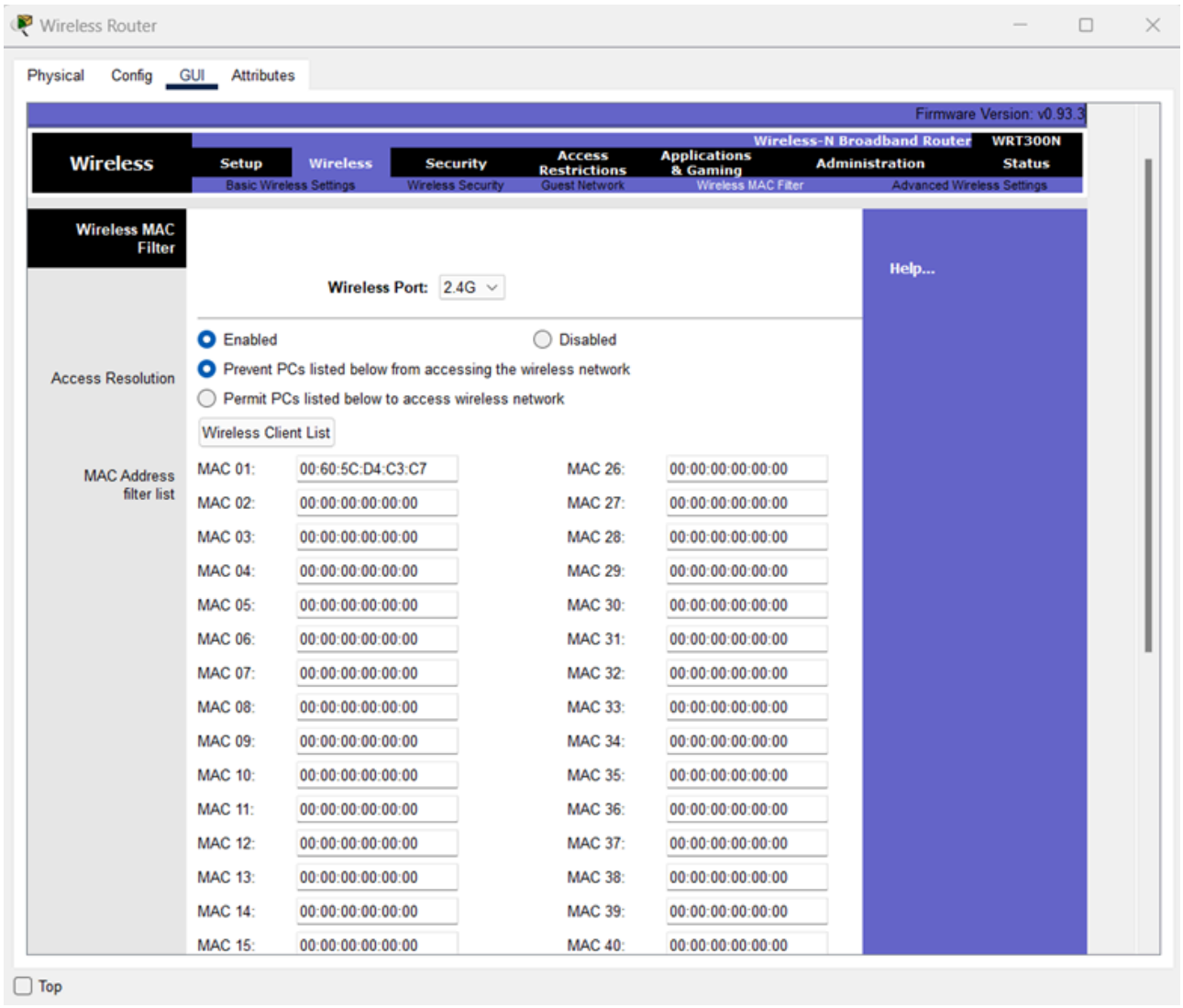
- **Screenshot(s)**:

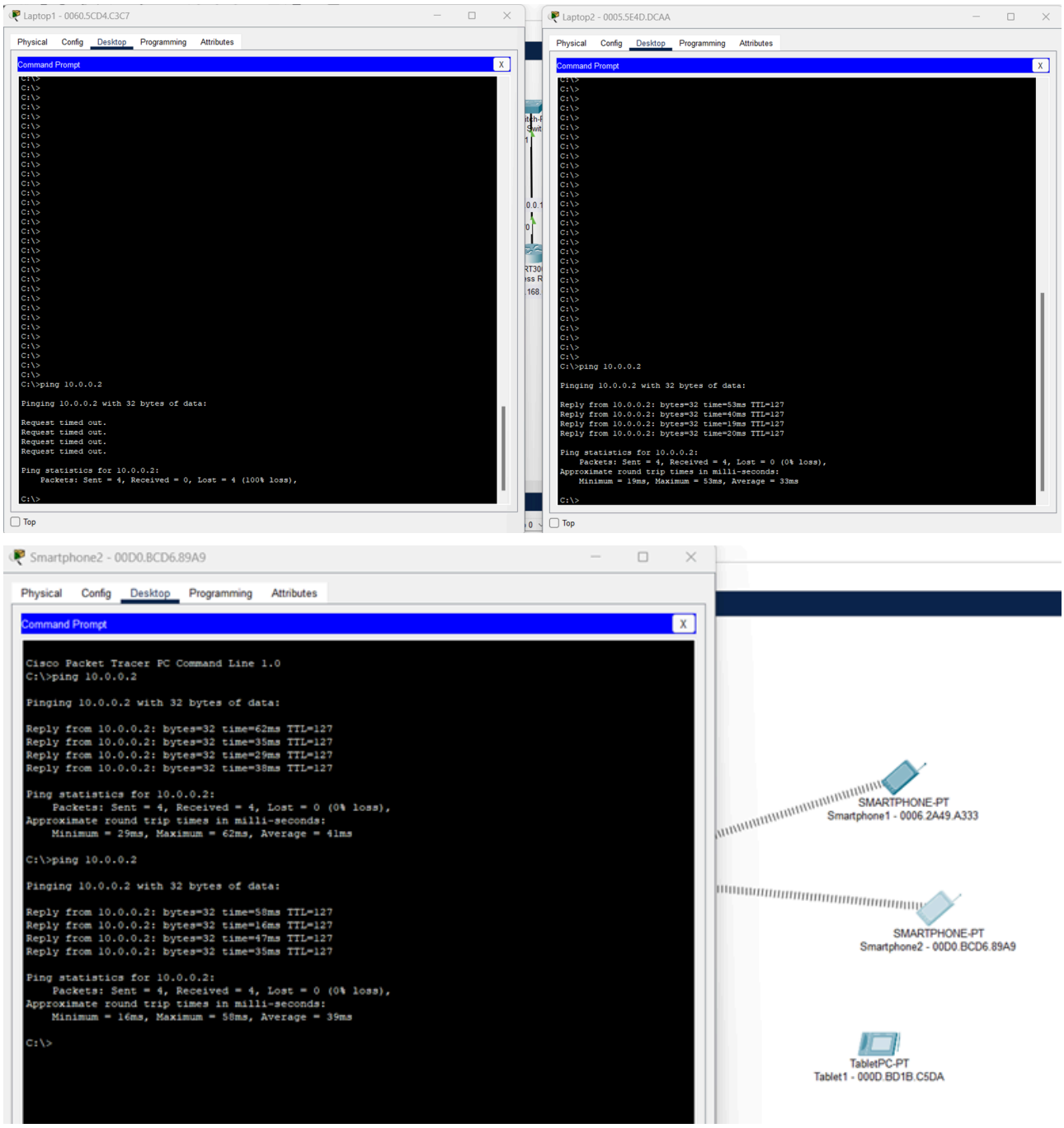




Task 9: Modify MAC Filter to Block Laptop1

- **Blocked Device**: Laptop1
- **Procedure**: Modified the MAC filter settings to block Laptop1 while allowing all other devices. Ping tests were conducted from Laptop1, which failed, and from Laptop2 and Smartphone1, which succeeded, indicating that the filter was working as expected.
- **Screenshot(s)**:

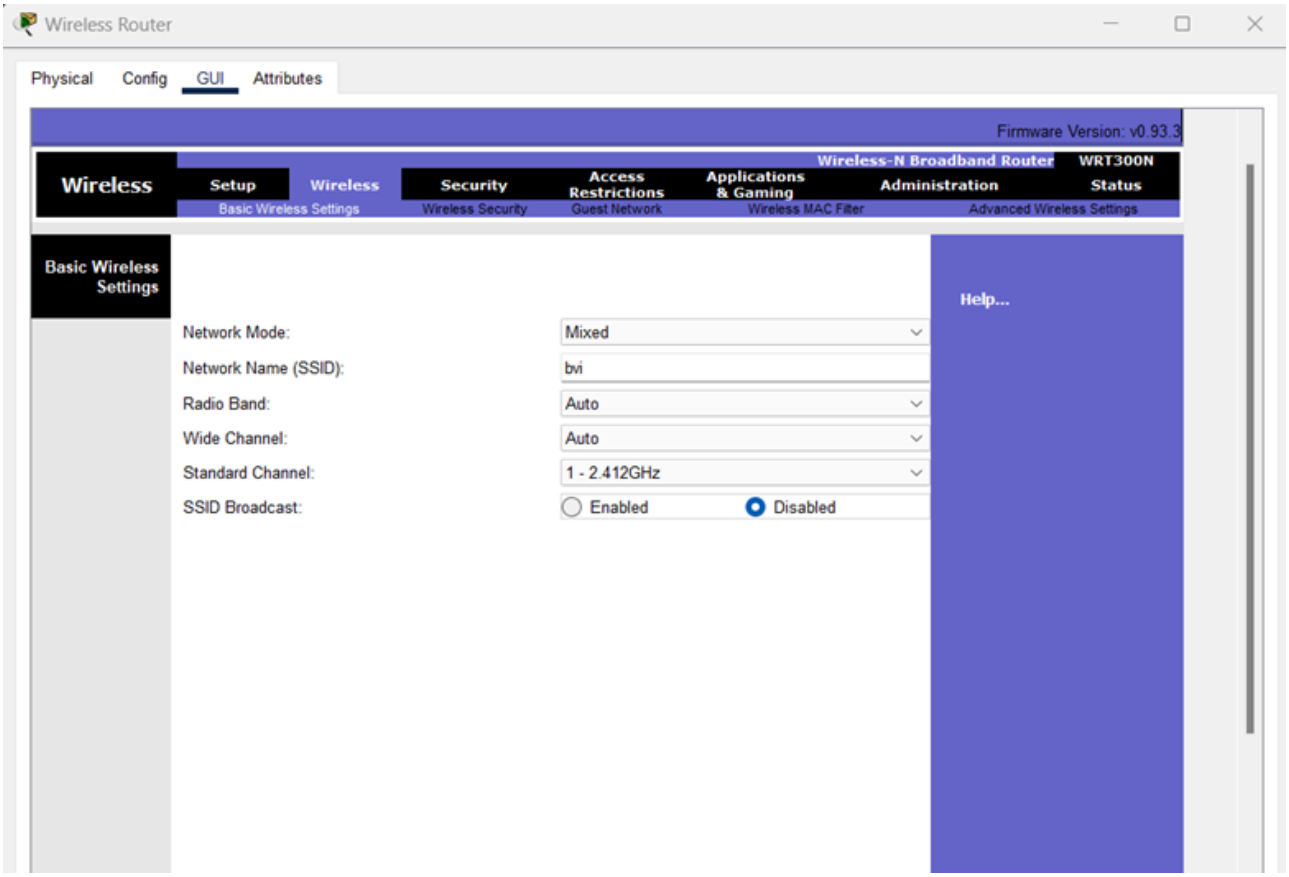


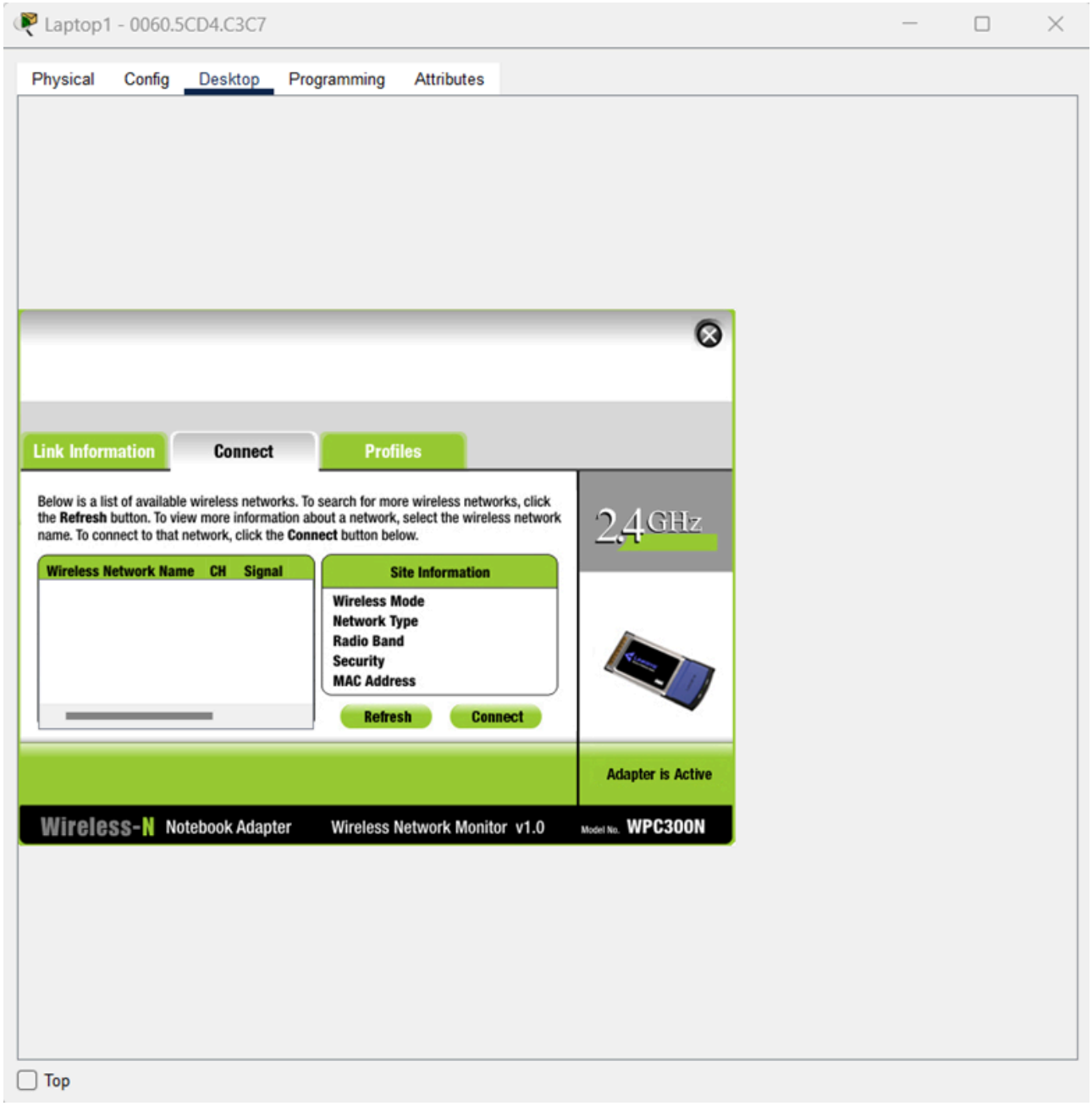


Task 10: Disable SSID Broadcast

- **Procedure**: Disabled the SSID broadcast feature on the router. Checked the visibility from Laptop1, which was configured to connect to “bvi” even when the SSID was not broadcasting. The network “bvi” was no longer visible to new devices scanning for networks but remained accessible to previously connected devices.

- **Screenshot(s)**:





Notes

This report provides a comprehensive view of each task, supplemented with screenshots that illustrate key steps and confirmations of the configurations applied.