Computer Networks

PROJECT REPORT

Configure Wireless LAN Access

National University
of computer and emerging sciences

I21-0572 Kissa Zahra (AI-K)

I21-0603 Hamna Sadia Rizwan (AI-K)

I21-0345 Amna khan (AI-J)

Presented to: Dr. Abid Rauf

4th May, 2024

TABLE OF CONTENTS

Project Objective

This project's goal is to install a Linksys WRT300N wireless access point. It will cover tasks like configuring MAC filtering, allowing different security protocols including WEP and WPA2 PSK AES, and changing the SSID.

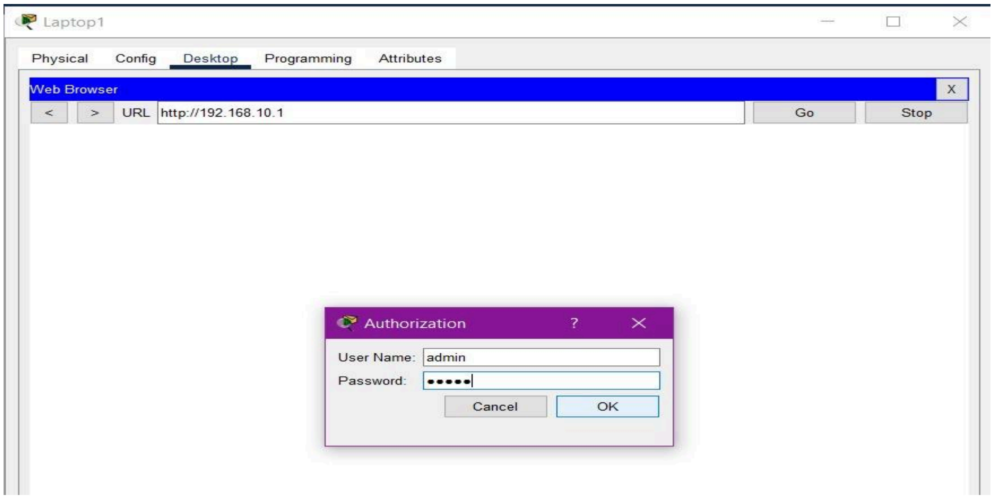
Equipment Used

- Linksys WRT300N Wireless Router
- Laptop1, Laptop2, Laptop 3
- Smartphone1, Smartphone2
- TabletPc-PT
- Server (IP: 10.0.0.2)

Task Summary

1. Connect wireless router WRT300N through a browser

Any device within range of the WRT300N router can establish a wireless connection. The desktop Web Browser program on Laptop 1 can be used for this. Enter 192.168.0.1, the address of the inner router's LAN interface, as the default gateway in the URL box. Enter admin for bot when asked for a username and password, then click OK.



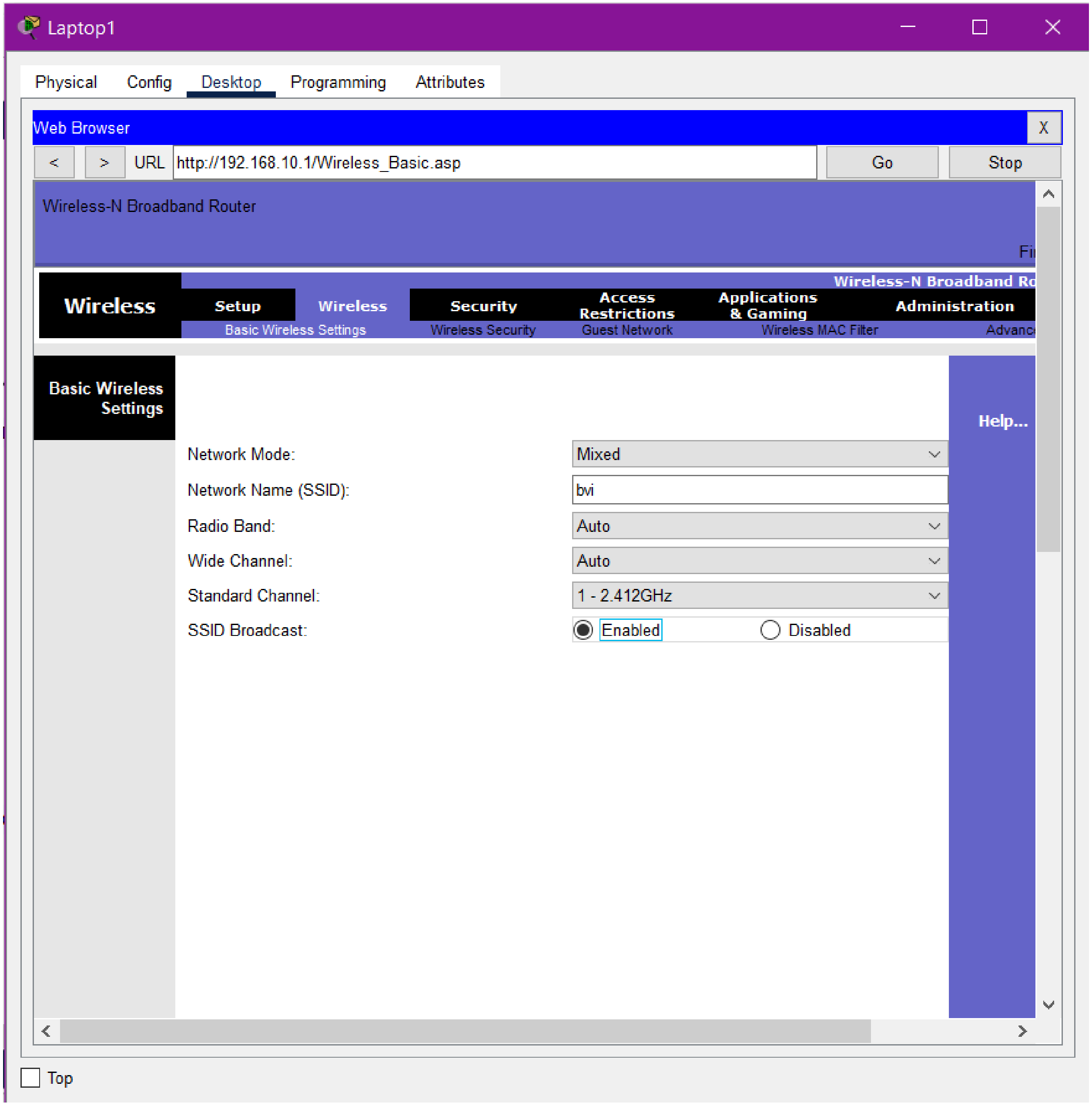
URL http://192.168.10.1

User Name: admin

Password: •••••

2. Change SSID name

Change the network name from Default to ‘bvi’ in the Network Name (SSID) box. On the Wireless tab, select the Save Settings option located at the bottom. Your connection to the default network is lost. Laptop 1 needs to rejoin the new SSID Warwick after switching SSIDs.After shutting down the browser, select Laptop1's Wireless. It opens the Linksys Wireless Network Monitor v1.0. Select the Connect tab. The wireless network name should show the ‘bvi’ network.

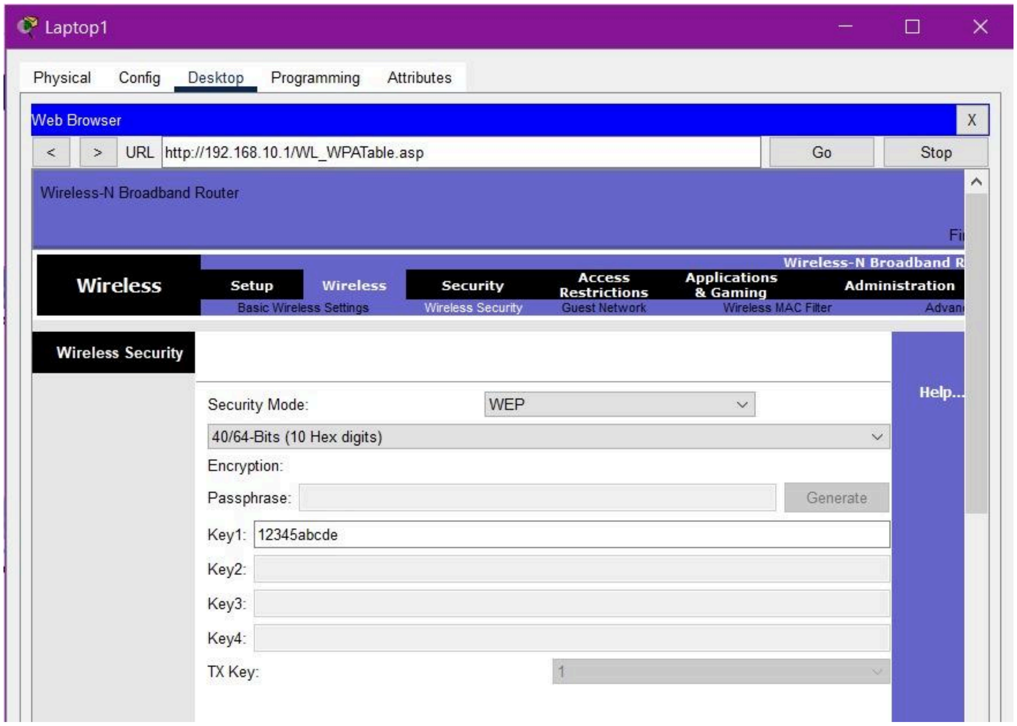


URL http://192.168.10.1/Wireless_Basic.asp

Network Mode:	Mixed
Network Name (SSID):	bvi
Radio Band:	Auto
Wide Channel:	Auto
Standard Channel:	1 - 2.412GHz
SSID Broadcast:	● Enabled ○ Disabled

3. Enable WEP wireless security

Click the Wireless tab in the web browser window.. Next, select the subtab for wireless security. Select WEP from the Security Mode drop-down menu. Enter 12345abcde in the Key 1 area while using the 40/64-Bit encryption setting by default. Select “Save Settings”.



URL http://192.168.10.1/WL_WPATable.asp

Security Mode: WEP

40/64-Bits (10 Hex digits)

Encryption:

Passphrase:

Key1: 12345abcde

Key2:

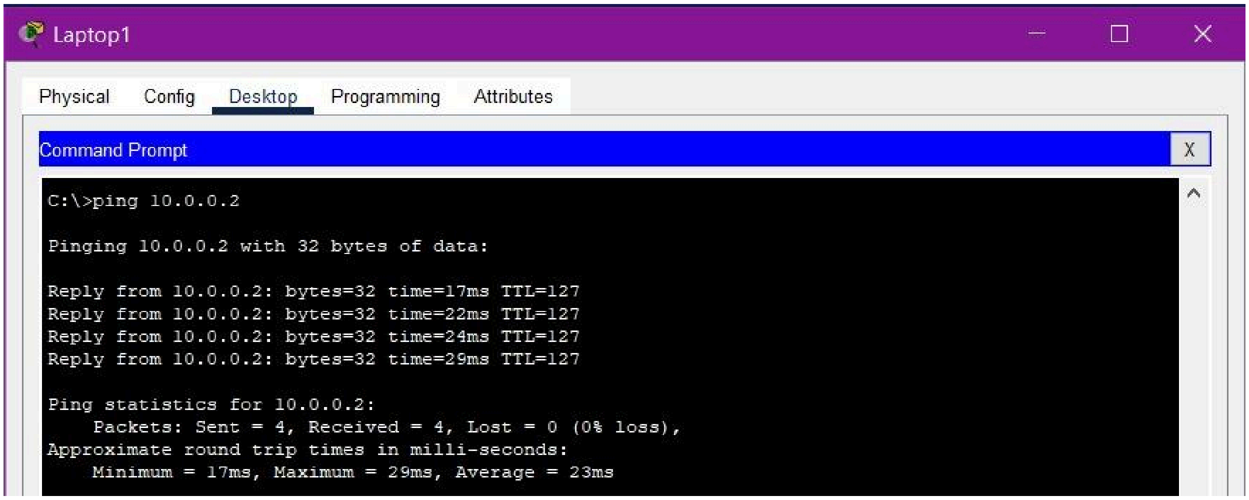
Key3:

Key4:

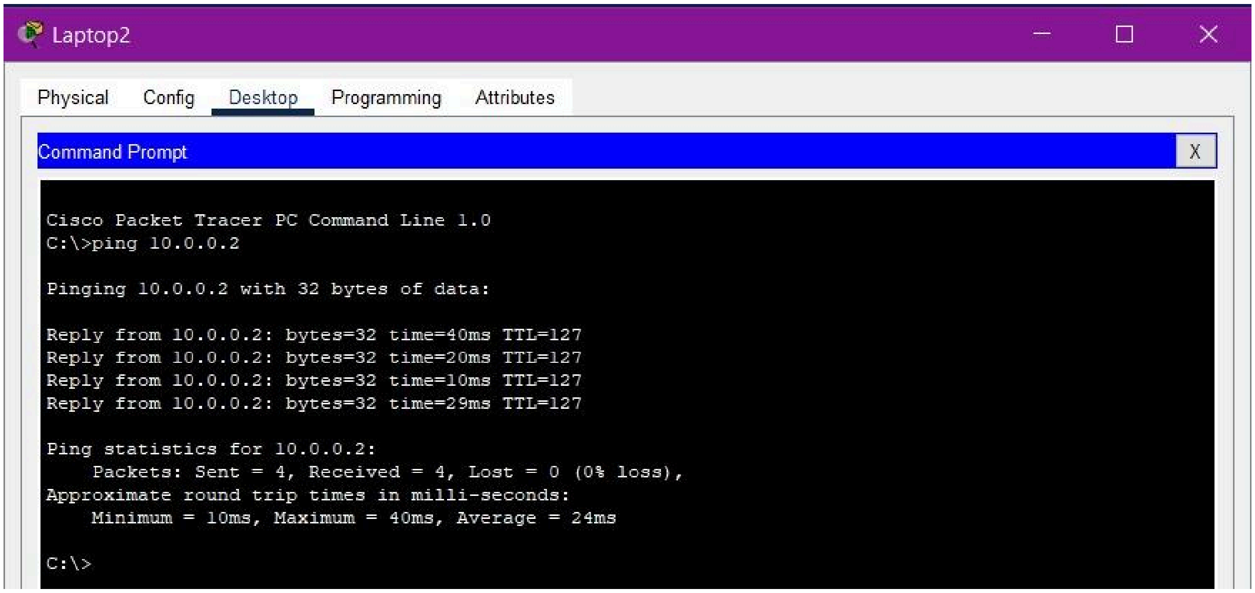
TX Key: 1

4. Connect Laptop1 and Laptop2 to the wireless network "bvi" using WEP key. Ping server 10.0.0.2

Click the PC Wireless on Laptops 1 and 2. Close the web browser. Select the Connect tab. Under Wireless Network Name, the bvi network should appear. After selecting this entry, select Connect. After entering “12345abcde” which is the WEP Passkey, select Connect.



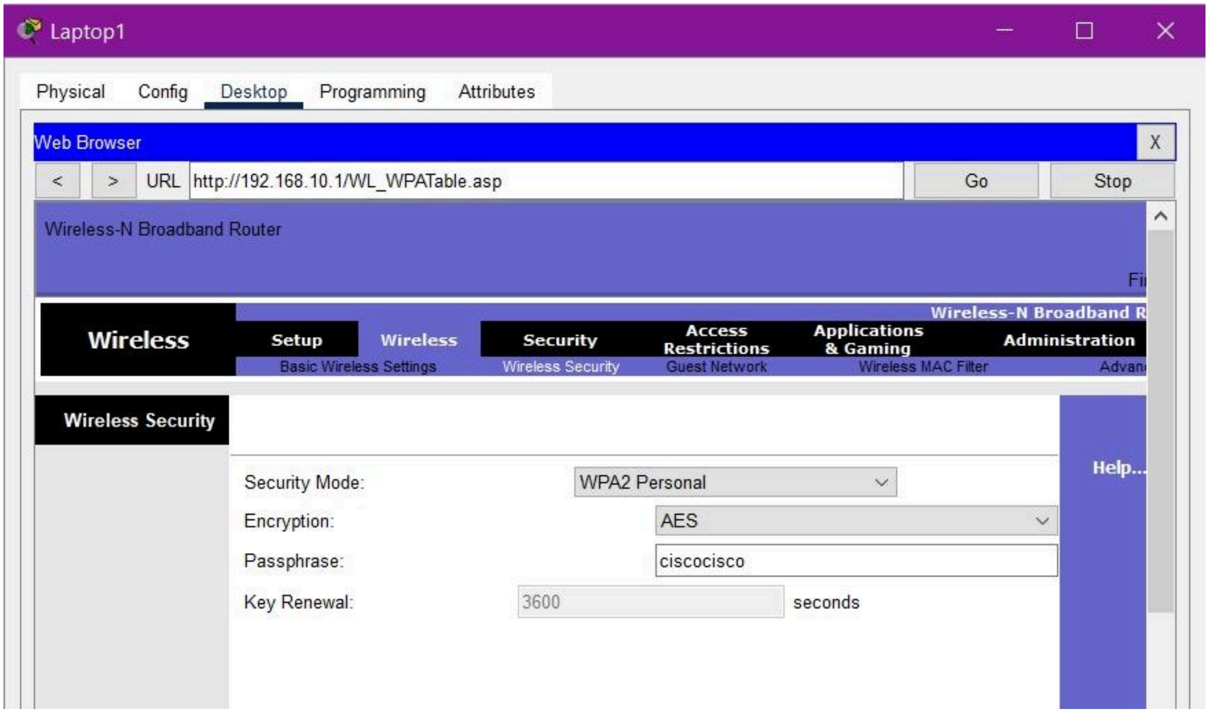
```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=17ms TTL=127
Reply from 10.0.0.2: bytes=32 time=22ms TTL=127
Reply from 10.0.0.2: bytes=32 time=24ms TTL=127
Reply from 10.0.0.2: bytes=32 time=29ms TTL=127

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 29ms, Average = 23ms
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=40ms TTL=127
Reply from 10.0.0.2: bytes=32 time=20ms TTL=127
Reply from 10.0.0.2: bytes=32 time=10ms TTL=127
Reply from 10.0.0.2: bytes=32 time=29ms TTL=127

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 40ms, Average = 24ms

C:\>
```

5. Change wireless security to WPA2 PSK AES

Click the Wireless tab in the web browser window. Next, select the subtab for wireless security. Select WPA2 Personal from the Security Mode drop-down list. In the Passphrase field, type “ciscocisco”, using the AES default encryption setting. Select “Save Settings”.



URL http://192.168.10.1/WL_WPATable.asp

Security Mode: WPA2 Personal

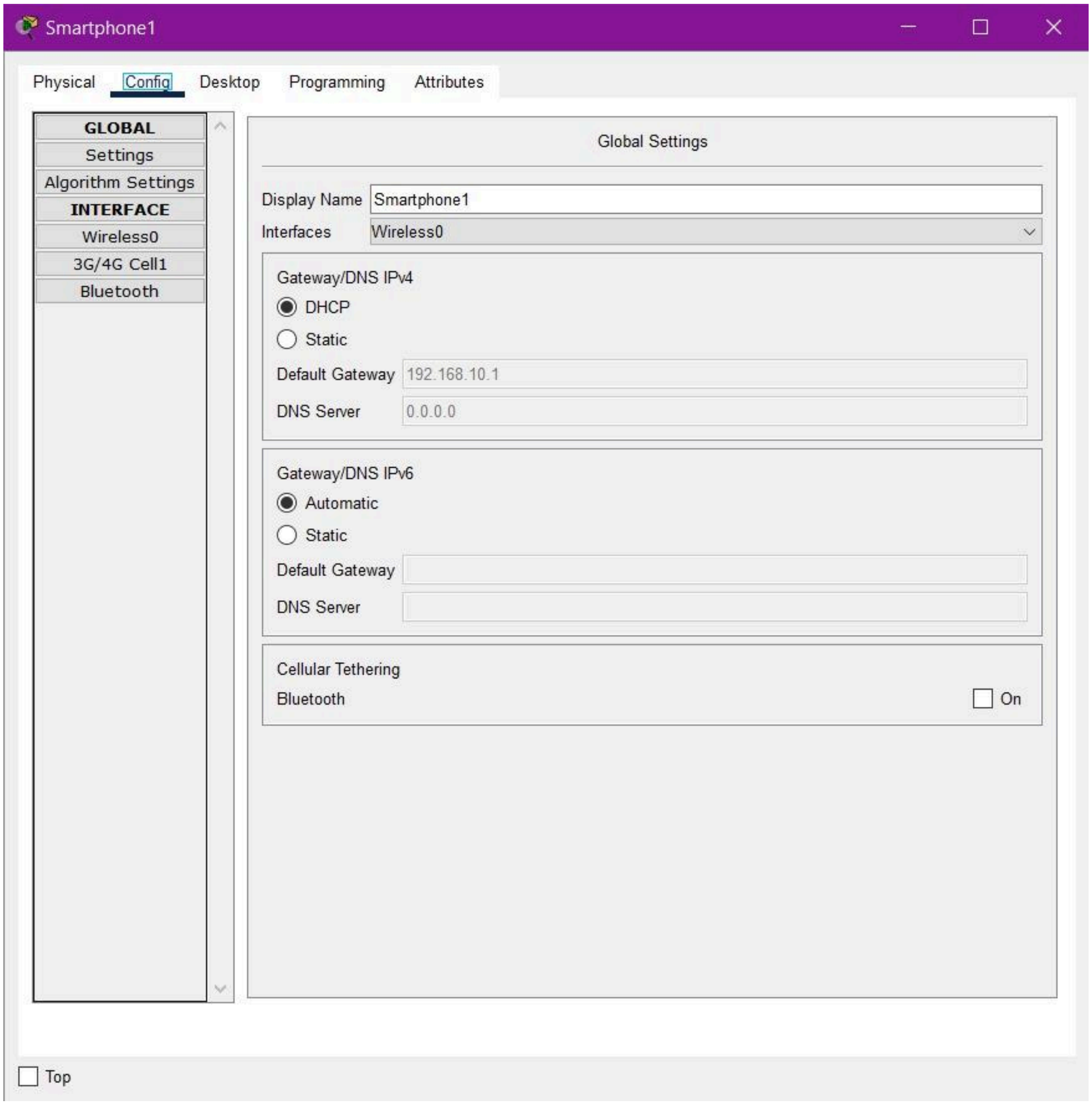
Encryption: AES

Passphrase: ciscocisco

Key Renewal: 3600 seconds

6. Connect Smartphone1 and Smartphone2 to wireless network "bvi" using WPA2 PSK passphrase. Ping server 10.0.0.2

Link smartphones 1 and 2 to the "bvi" wireless network. When prompted, enter passphrase ("ciscocisco") to test connectivity with Ping server (10.0.0.2).



Global Settings

Display Name Smartphone1

Interfaces Wireless0

Gateway/DNS IPv4

● DHCP

○ Static

Default Gateway 192.168.10.1

DNS Server 0.0.0.0

Gateway/DNS IPv6

● Automatic

○ Static

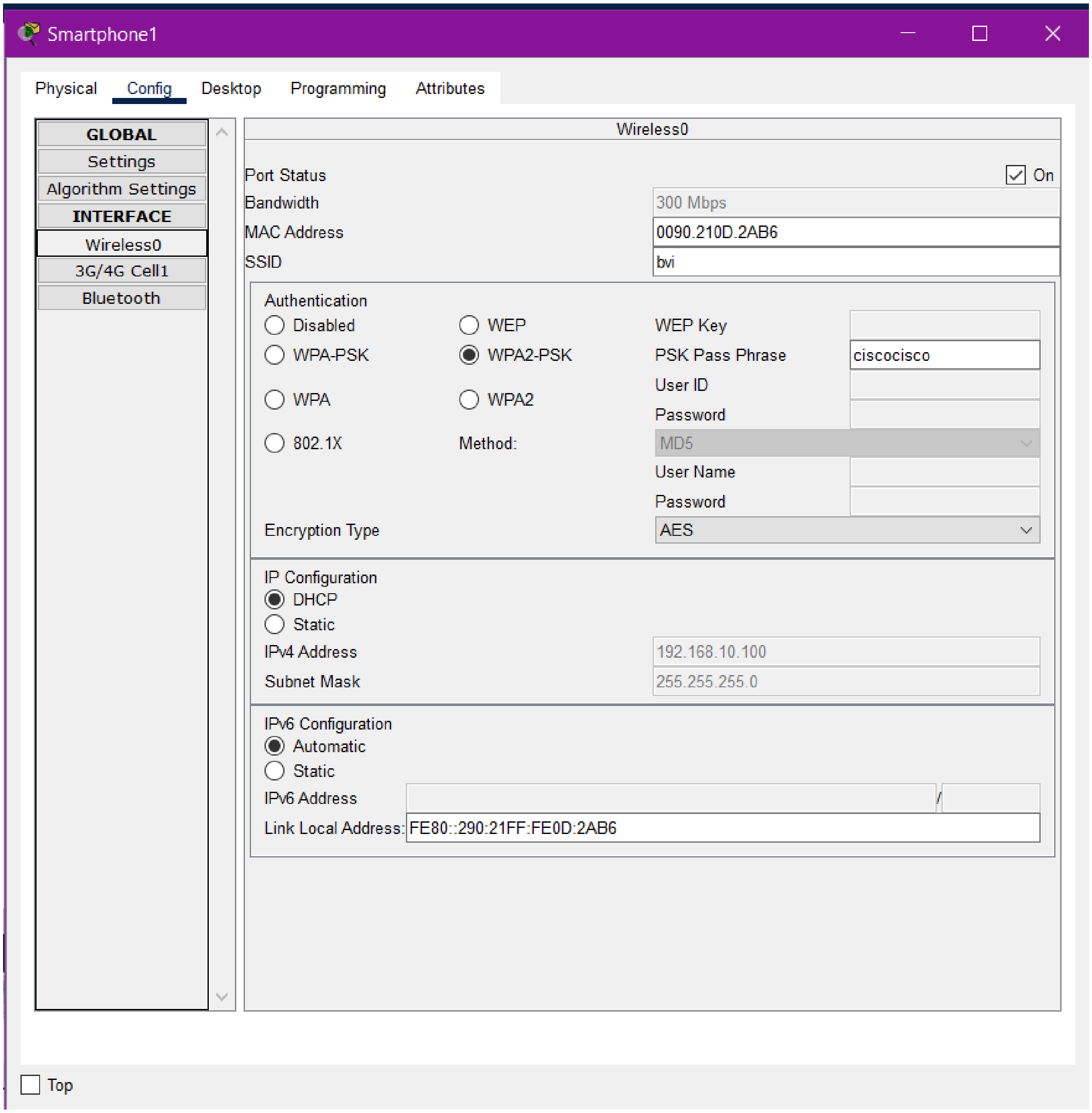
Default Gateway

DNS Server

Cellular Tethering

Bluetooth □ On

□ Top



Wireless0

Port Status ☑ On

Bandwidth 300 Mbps

MAC Address 0090.210D.2AB6

SSID bvi

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase ciscocisco

User ID

○ WPA ○ WPA2 Password

○ 802.1X Method: MD5

User Name

Password

Encryption Type AES

IP Configuration

● DHCP

○ Static

IPv4 Address 192.168.10.100

Subnet Mask 255.255.255.0

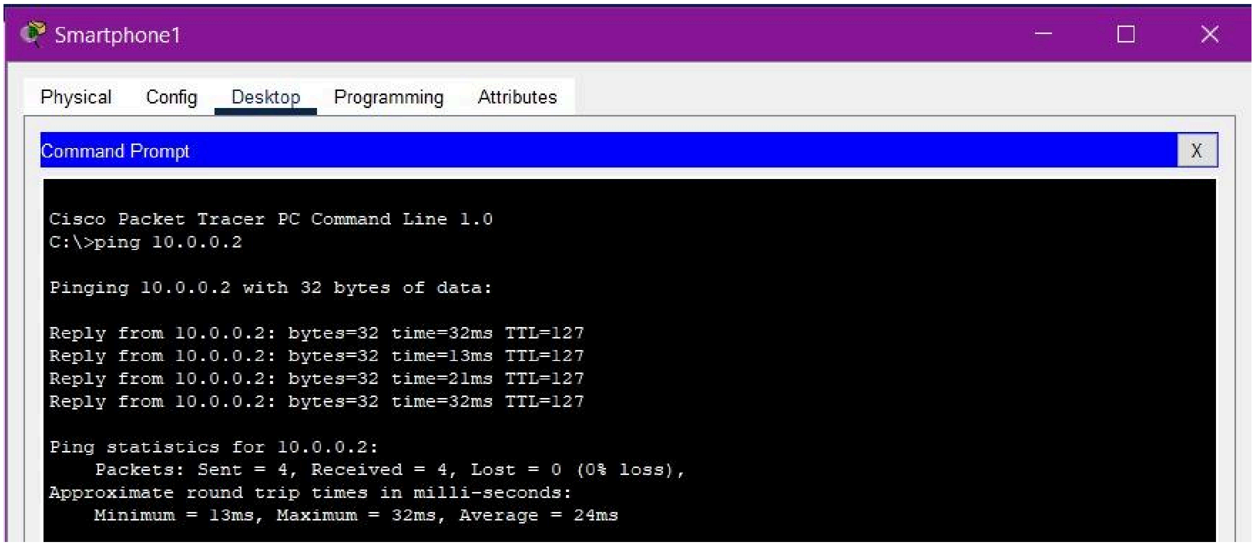
IPv6 Configuration

● Automatic

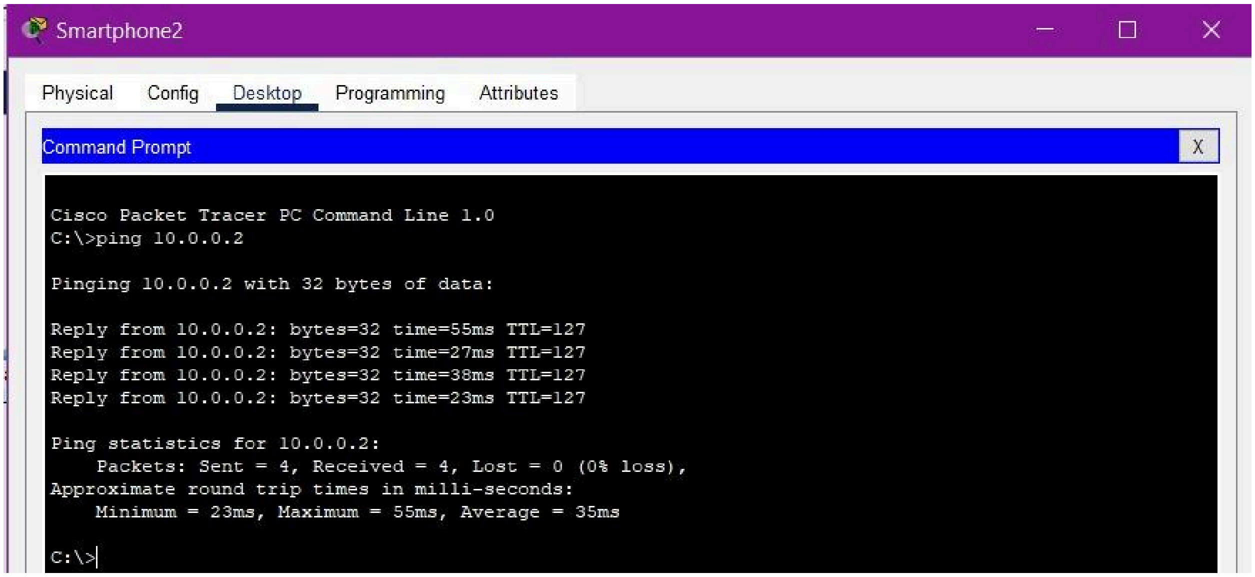
○ Static

IPv6 Address /

Link Local Address: FE80::290:21FF:FE0D:2AB6



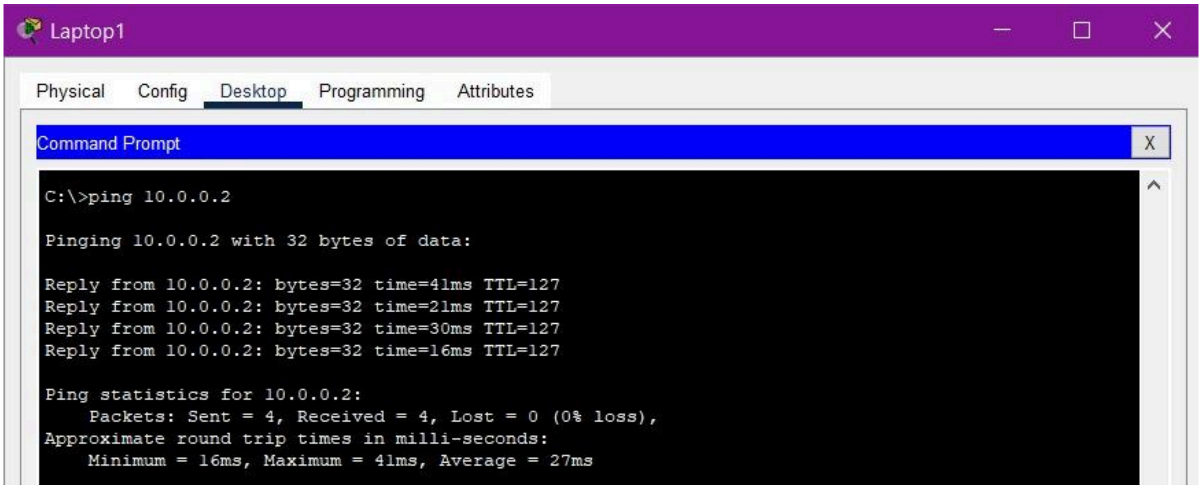
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=32ms TTL=127
Reply from 10.0.0.2: bytes=32 time=13ms TTL=127
Reply from 10.0.0.2: bytes=32 time=21ms TTL=127
Reply from 10.0.0.2: bytes=32 time=32ms TTL=127

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 32ms, Average = 24ms
```



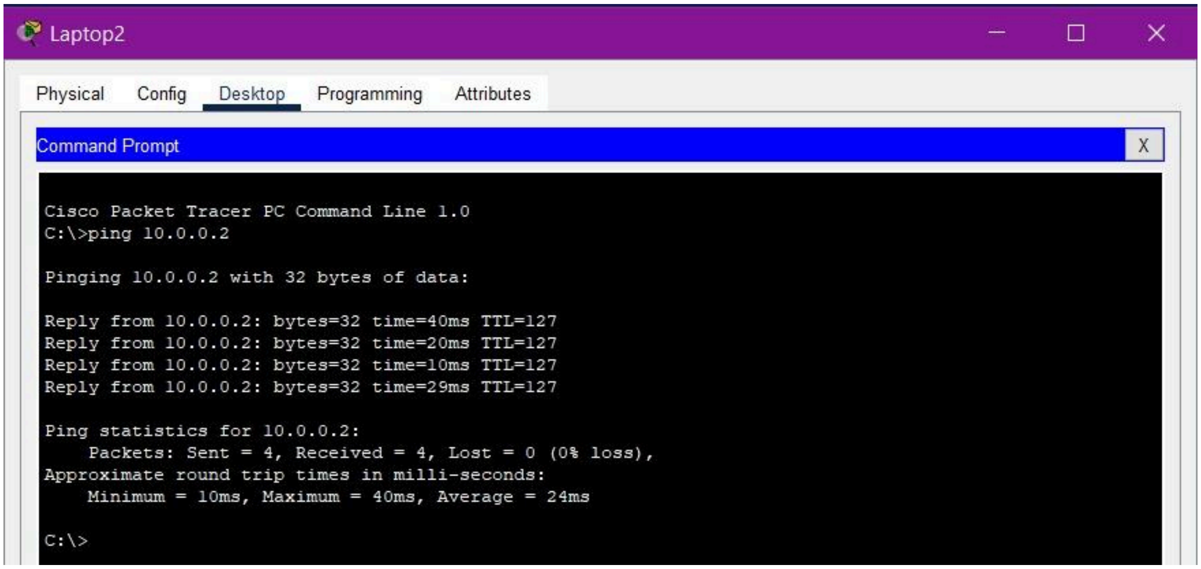
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=55ms TTL=127
Reply from 10.0.0.2: bytes=32 time=27ms TTL=127
Reply from 10.0.0.2: bytes=32 time=38ms TTL=127
Reply from 10.0.0.2: bytes=32 time=23ms TTL=127

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 55ms, Average = 35ms

C:\>
```

7. Connect Laptop1 and Laptop2 to wireless network "bvi" .Ping server 10.0.0.2

To link Laptops 1 and 2 to the bvi network with WPA2 security, the same steps as in Task 4 must be followed to set the WPA2 PSK passphrase.



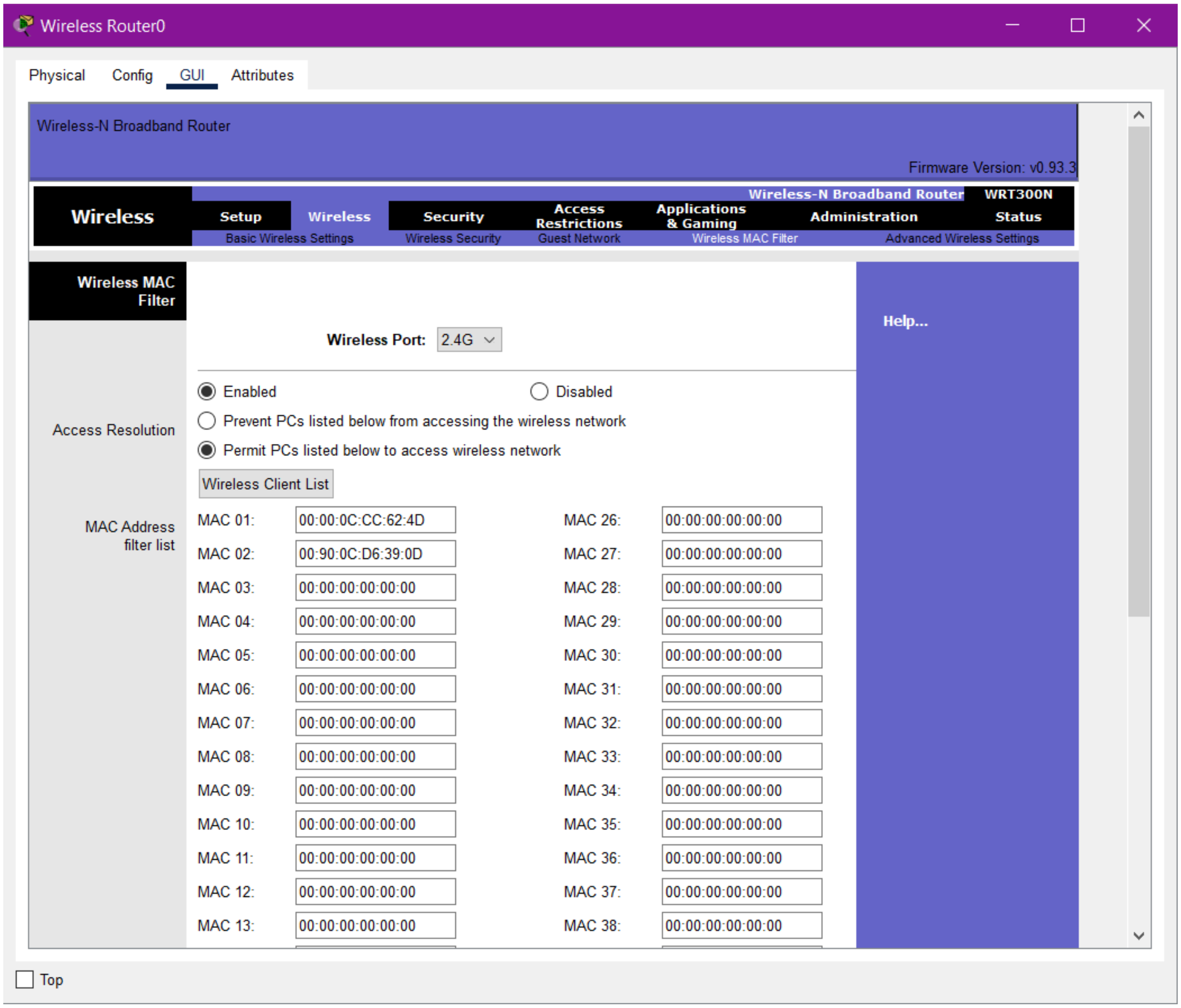
```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=41ms TTL=127
Reply from 10.0.0.2: bytes=32 time=21ms TTL=127
Reply from 10.0.0.2: bytes=32 time=30ms TTL=127
Reply from 10.0.0.2: bytes=32 time=16ms TTL=127

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 41ms, Average = 27ms
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=40ms TTL=127
Reply from 10.0.0.2: bytes=32 time=20ms TTL=127
Reply from 10.0.0.2: bytes=32 time=10ms TTL=127
Reply from 10.0.0.2: bytes=32 time=29ms TTL=127

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 40ms, Average = 24ms

C:\>
```

8. Enable Wireless MAC filter

Select the Wireless MAC Filter subtab and the Wireless tab. Make sure the Wireless MAC Filter is turned onEnter the MAC addresses for Laptop1 and Laptop2 in the MAC01 and MAC02 fields. From Laptop1, Laptop2, Smartphone1, and Smartphone2, ping the server 10.0.0.2.



Wireless MAC Filter

Wireless Port: 2.4G

● Enabled ○ Disabled

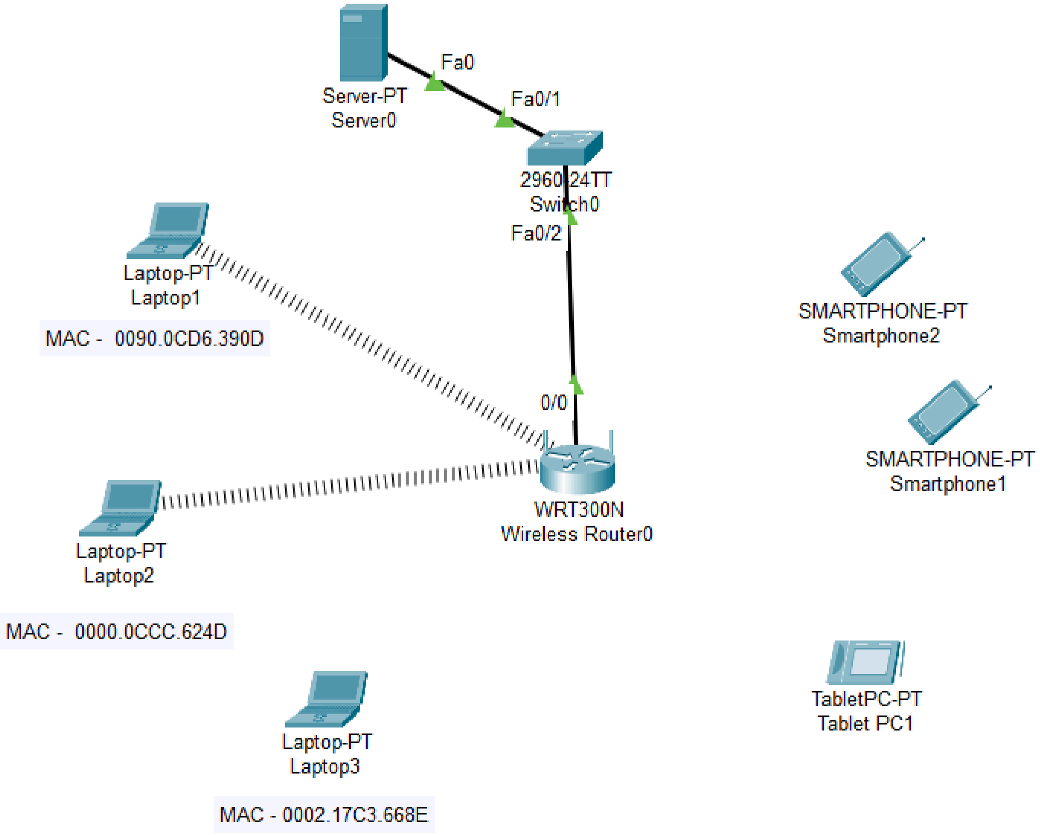
Access Resolution

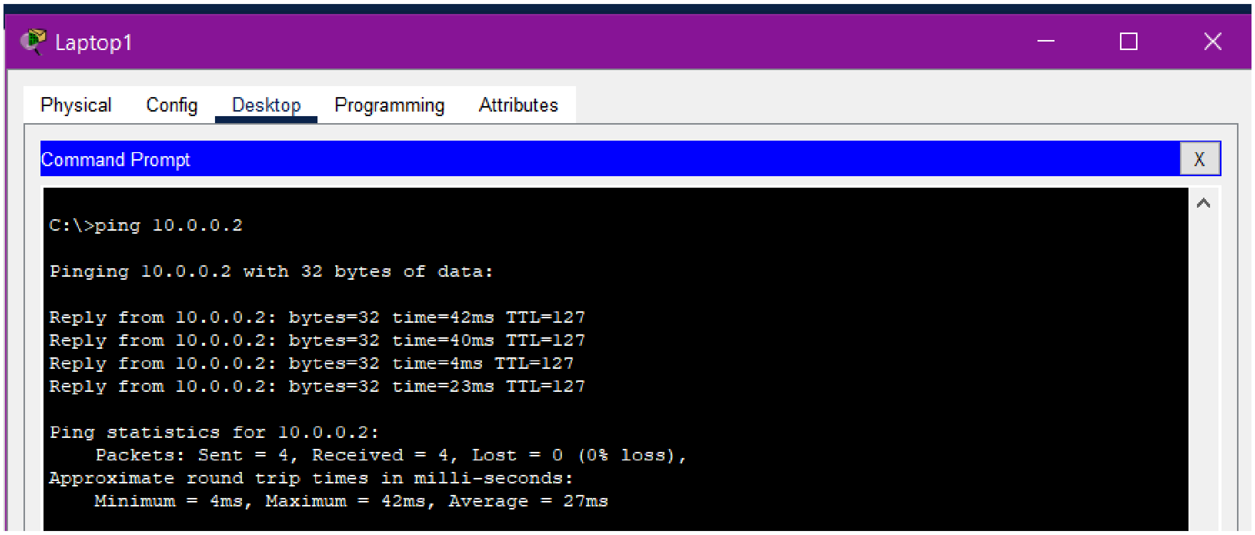
○ Prevent PCs listed below from accessing the wireless network

● Permit PCs listed below to access wireless network

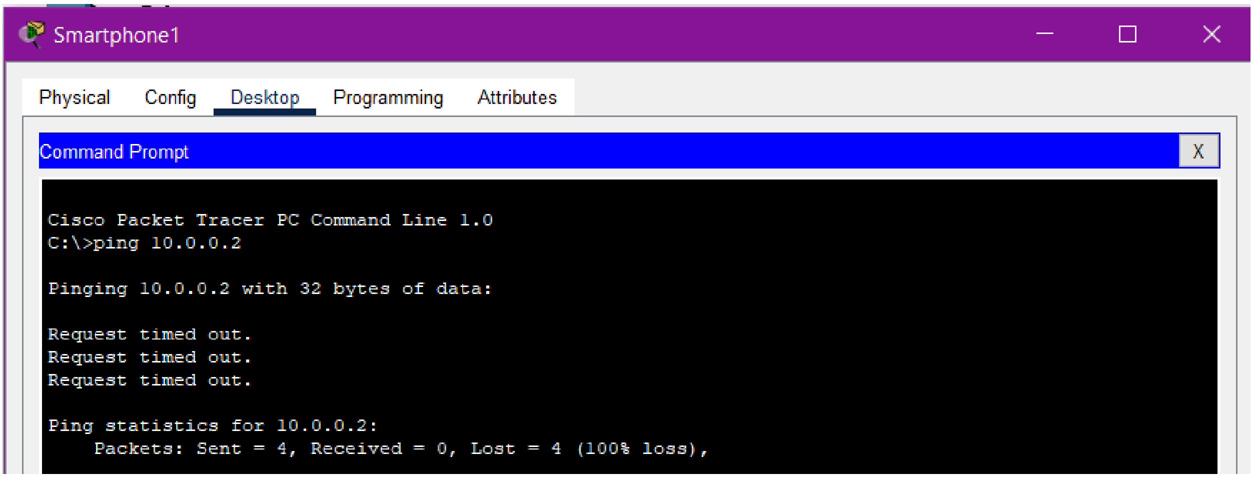
MAC Address filter list

MAC 01:	00:00:0C:CC:62:4D	MAC 26:	00:00:00:00:00:00
MAC 02:	00:90:0C:D6:39:0D	MAC 27:	00:00:00:00:00:00
MAC 03:	00:00:00:00:00:00	MAC 28:	00:00:00:00:00:00
MAC 04:	00:00:00:00:00:00	MAC 29:	00:00:00:00:00:00
MAC 05:	00:00:00:00:00:00	MAC 30:	00:00:00:00:00:00
MAC 06:	00:00:00:00:00:00	MAC 31:	00:00:00:00:00:00
MAC 07:	00:00:00:00:00:00	MAC 32:	00:00:00:00:00:00
MAC 08:	00:00:00:00:00:00	MAC 33:	00:00:00:00:00:00
MAC 09:	00:00:00:00:00:00	MAC 34:	00:00:00:00:00:00
MAC 10:	00:00:00:00:00:00	MAC 35:	00:00:00:00:00:00
MAC 11:	00:00:00:00:00:00	MAC 36:	00:00:00:00:00:00
MAC 12:	00:00:00:00:00:00	MAC 37:	00:00:00:00:00:00
MAC 13:	00:00:00:00:00:00	MAC 38:	00:00:00:00:00:00





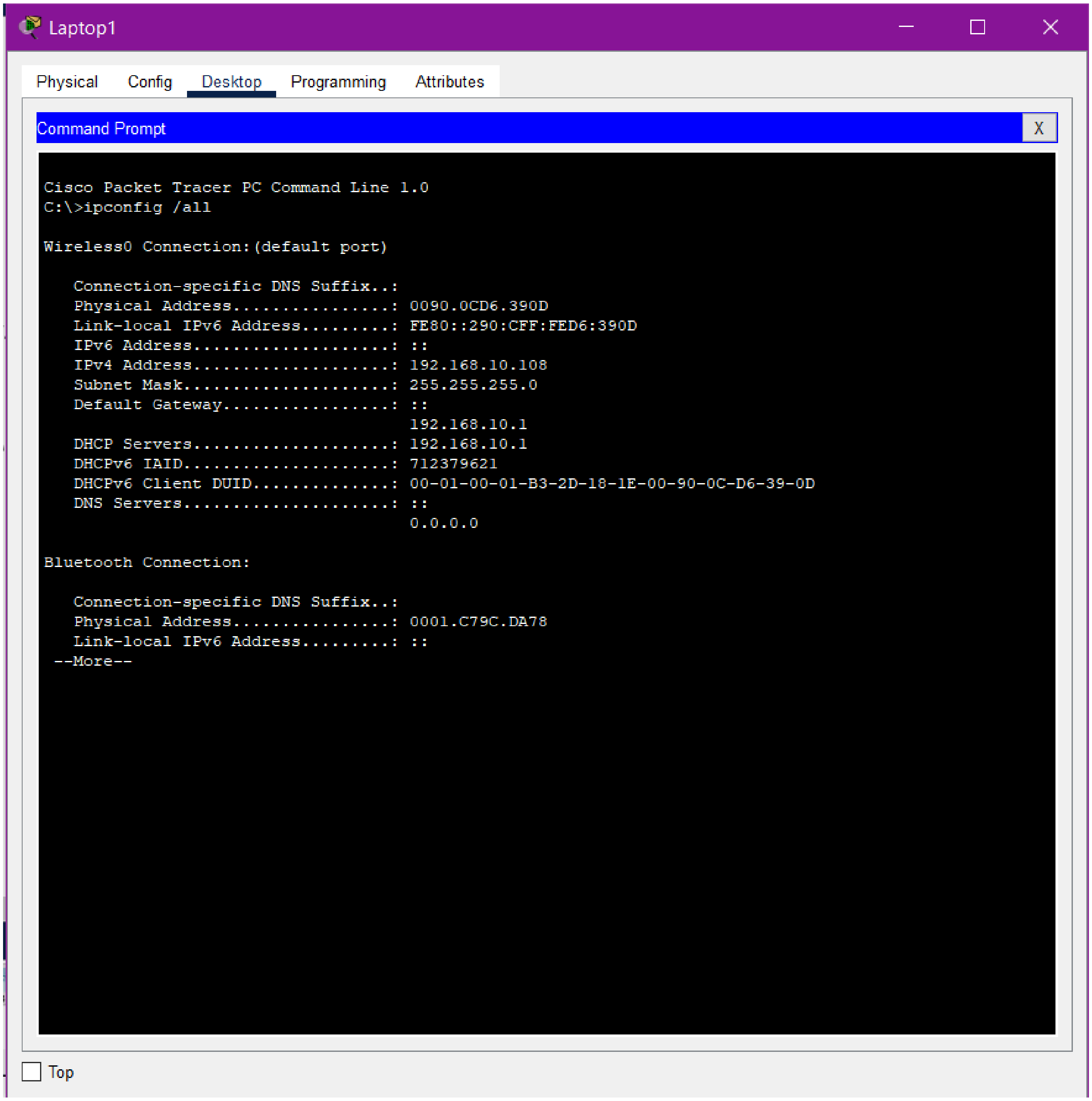
```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=42ms TTL=127
Reply from 10.0.0.2: bytes=32 time=40ms TTL=127
Reply from 10.0.0.2: bytes=32 time=4ms TTL=127
Reply from 10.0.0.2: bytes=32 time=23ms TTL=127

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 42ms, Average = 27ms
```



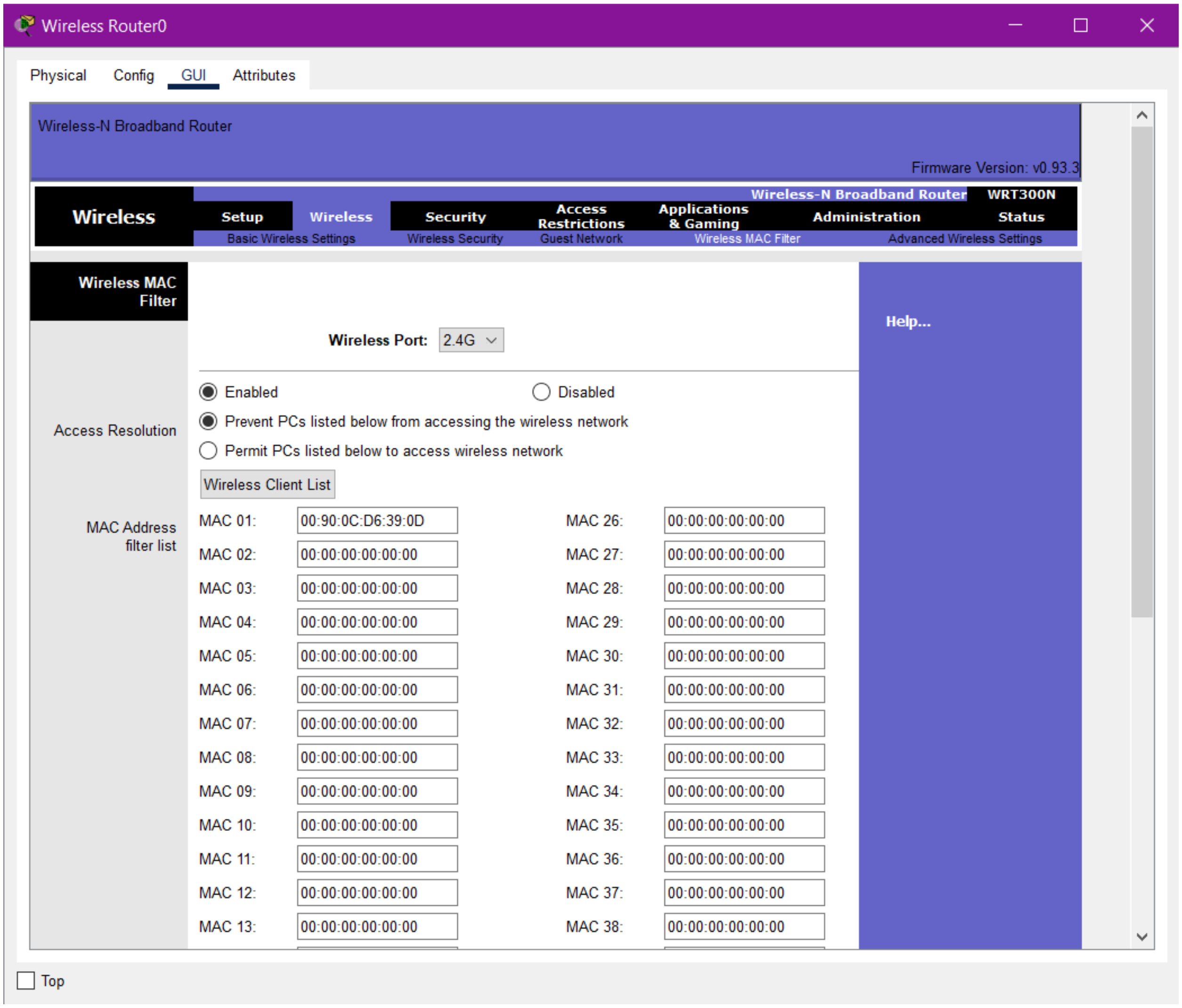
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

9. Change MAC filter to allow all devices except Laptop1

Select the Wireless MAC Filter subtab and the Wireless tab. Make sure the Wireless MAC Filter is turned on. Enter the Laptop1 MAC address in fields MAC01 and MAC02. From Laptop1, Laptop2, Smartphone1, and Smartphone2, ping the server 10.0.0.2.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

Wireless0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0090.0CD6.390D
   Link-local IPv6 Address.........: FE80::290:CFF:FED6:390D
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.10.108
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.10.1
   DHCP Servers....................: 192.168.10.1
   DHCPv6 IAID.....................: 712379621
   DHCPv6 Client DUID..............: 00-01-00-01-B3-2D-18-1E-00-90-0C-D6-39-0D
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 0001.C79C.DA78
   Link-local IPv6 Address.........: ::
 --More--
```



Wireless Port: 2.4G

Access Resolution

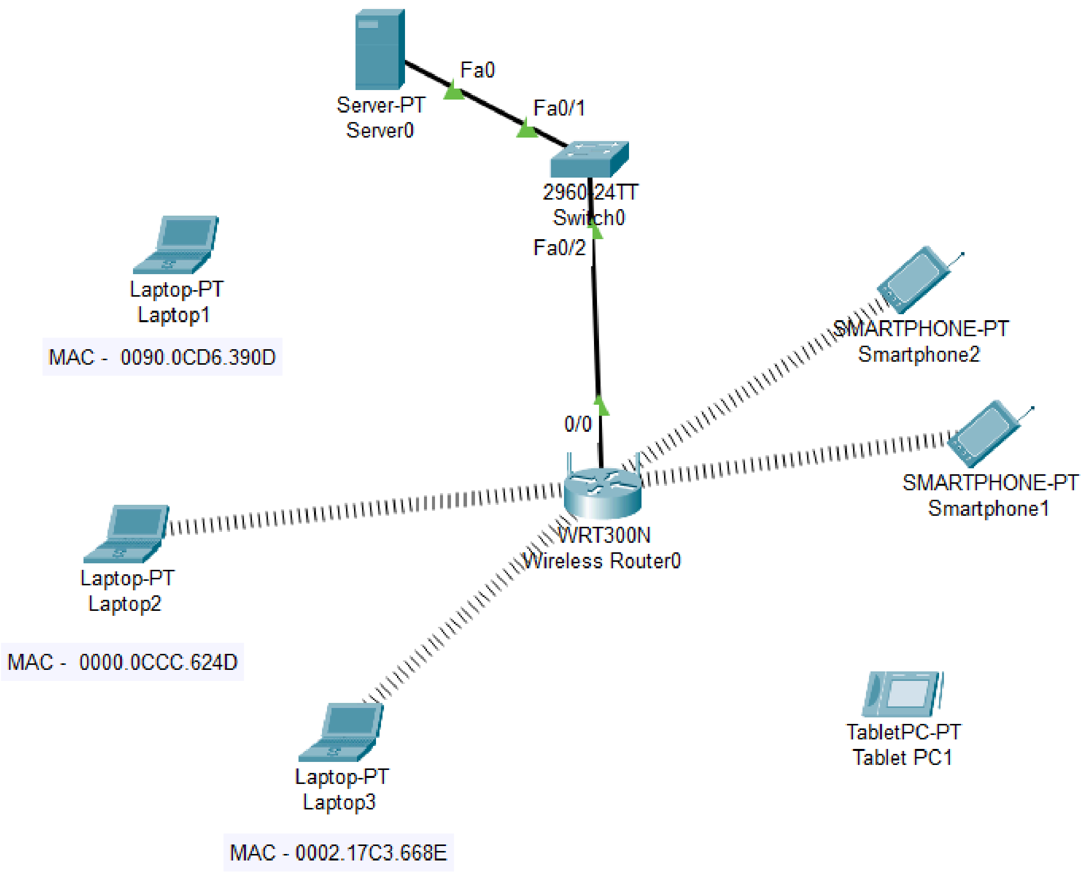
● Enabled ○ Disabled

● Prevent PCs listed below from accessing the wireless network

○ Permit PCs listed below to access wireless network

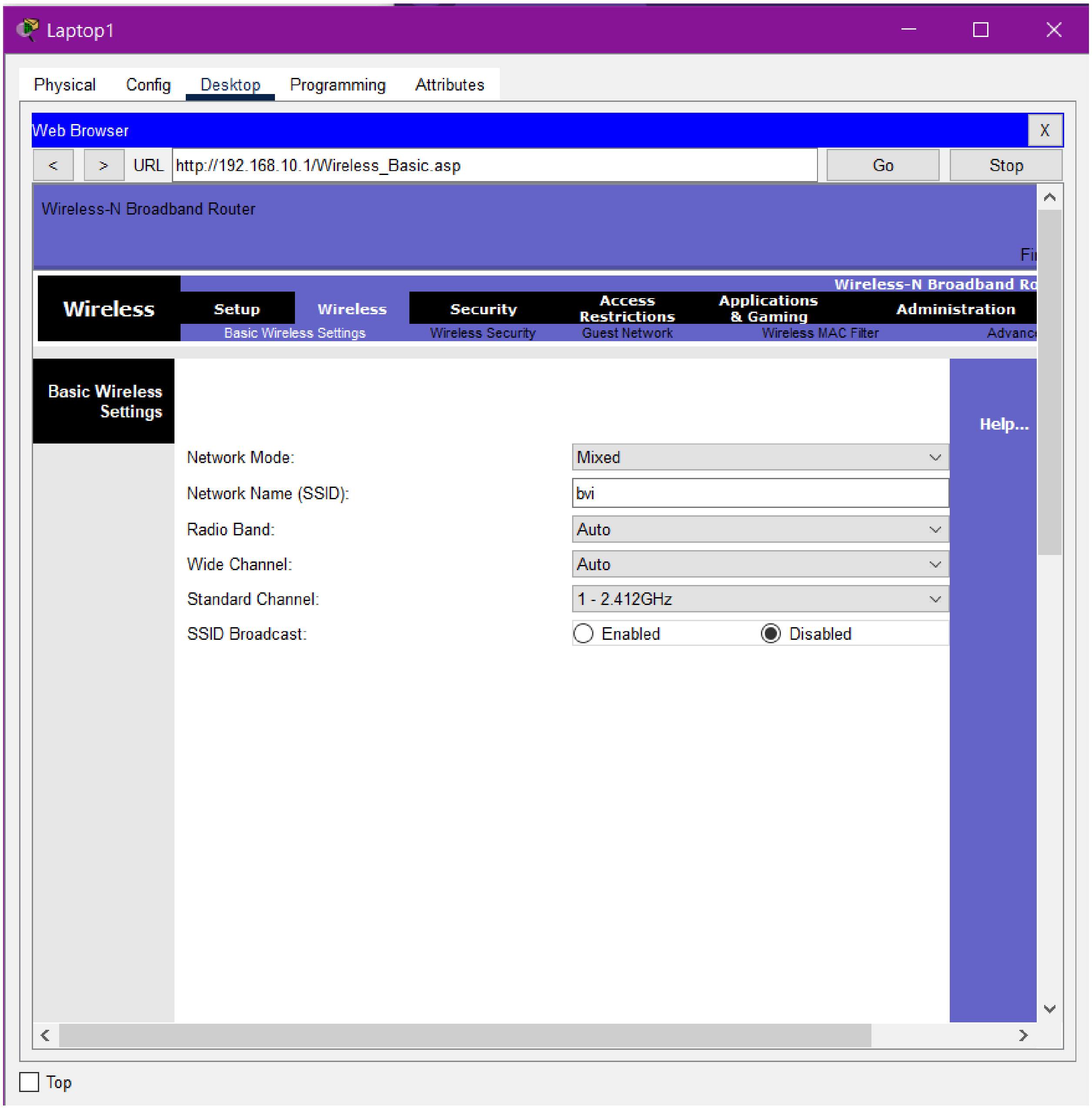
MAC Address filter list

MAC 01:	00:90:0C:D6:39:0D	MAC 26:	00:00:00:00:00:00
MAC 02:	00:00:00:00:00:00	MAC 27:	00:00:00:00:00:00
MAC 03:	00:00:00:00:00:00	MAC 28:	00:00:00:00:00:00
MAC 04:	00:00:00:00:00:00	MAC 29:	00:00:00:00:00:00
MAC 05:	00:00:00:00:00:00	MAC 30:	00:00:00:00:00:00
MAC 06:	00:00:00:00:00:00	MAC 31:	00:00:00:00:00:00
MAC 07:	00:00:00:00:00:00	MAC 32:	00:00:00:00:00:00
MAC 08:	00:00:00:00:00:00	MAC 33:	00:00:00:00:00:00
MAC 09:	00:00:00:00:00:00	MAC 34:	00:00:00:00:00:00
MAC 10:	00:00:00:00:00:00	MAC 35:	00:00:00:00:00:00
MAC 11:	00:00:00:00:00:00	MAC 36:	00:00:00:00:00:00
MAC 12:	00:00:00:00:00:00	MAC 37:	00:00:00:00:00:00
MAC 13:	00:00:00:00:00:00	MAC 38:	00:00:00:00:00:00



10. Disable SSID broadcast and check visibility from Laptop1

Select the Basic Wireless Settings subtab and then the Wireless tab. Gain the disabled status for the SSID Broadcast. Examine the “bvi” network's visibility from Laptop1.



URL: http://192.168.10.1/Wireless_Basic.asp

Basic Wireless Settings

Network Mode: Mixed

Network Name (SSID): bvi

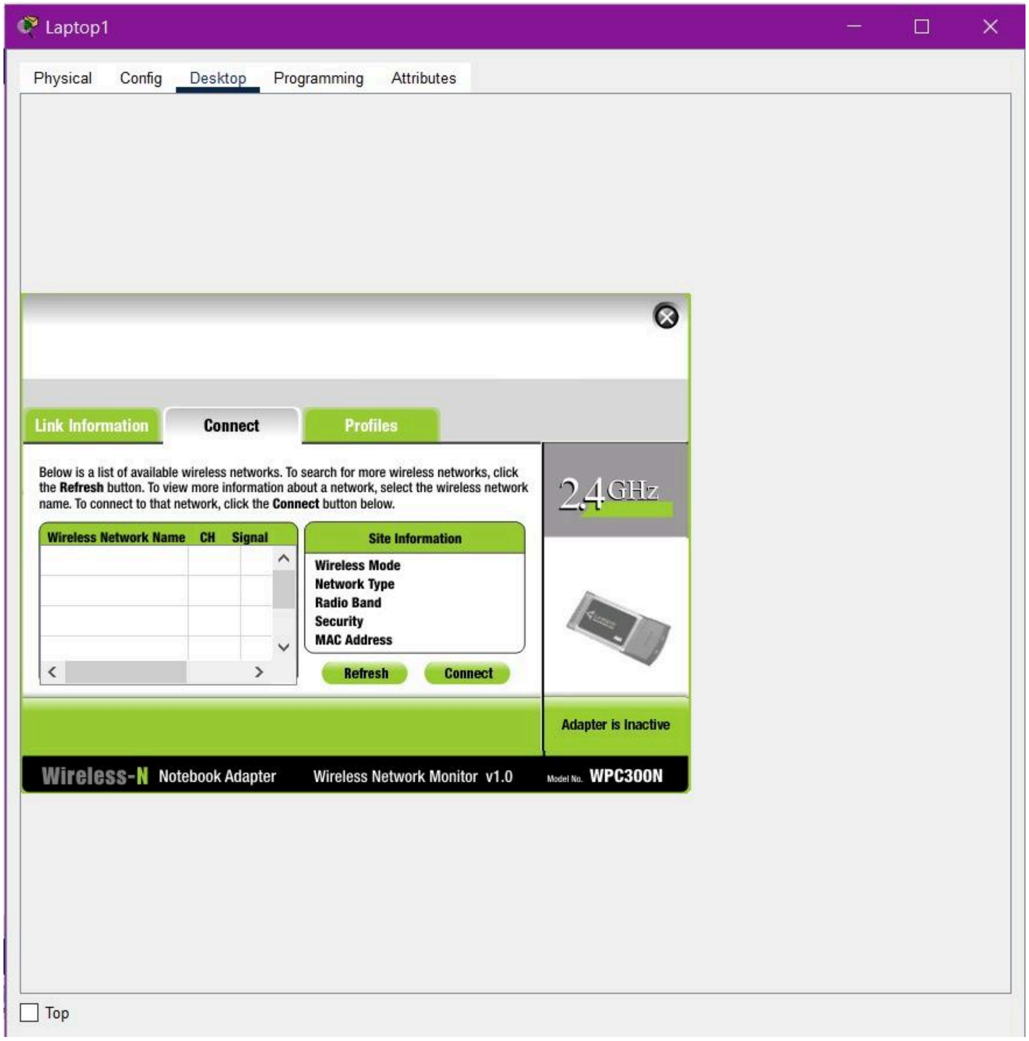
Radio Band: Auto

Wide Channel: Auto

Standard Channel: 1 - 2.412GHz

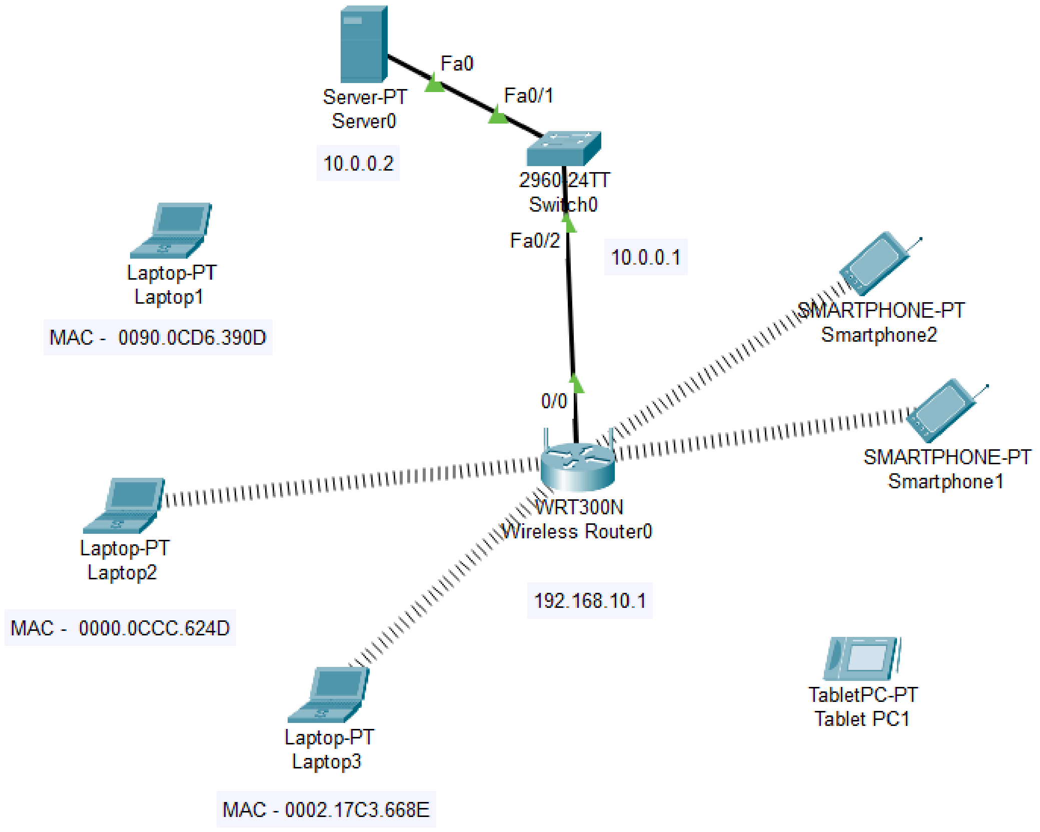
SSID Broadcast: ○ Enabled ● Disabled

□ Top



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.

Output



Conclusion

This project enabled multiple security protocols, including WEP, WPA2 PSK AES, and MAC filtering on WRT300N wireless access point. To improve network security,SSID was changed to “bvi” and SSID broadcast was turned off. Every device was linked to the network and its communication with the server is tested