VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Computer Science & Engineering

CSE3501 – Information Security Analysis and Audit

LAB ASSIGNMENT 6

Submitted to **Prof. RAJA SP**

NAME: PUNIT MIDDHA
REG.NO: 19BCE2060

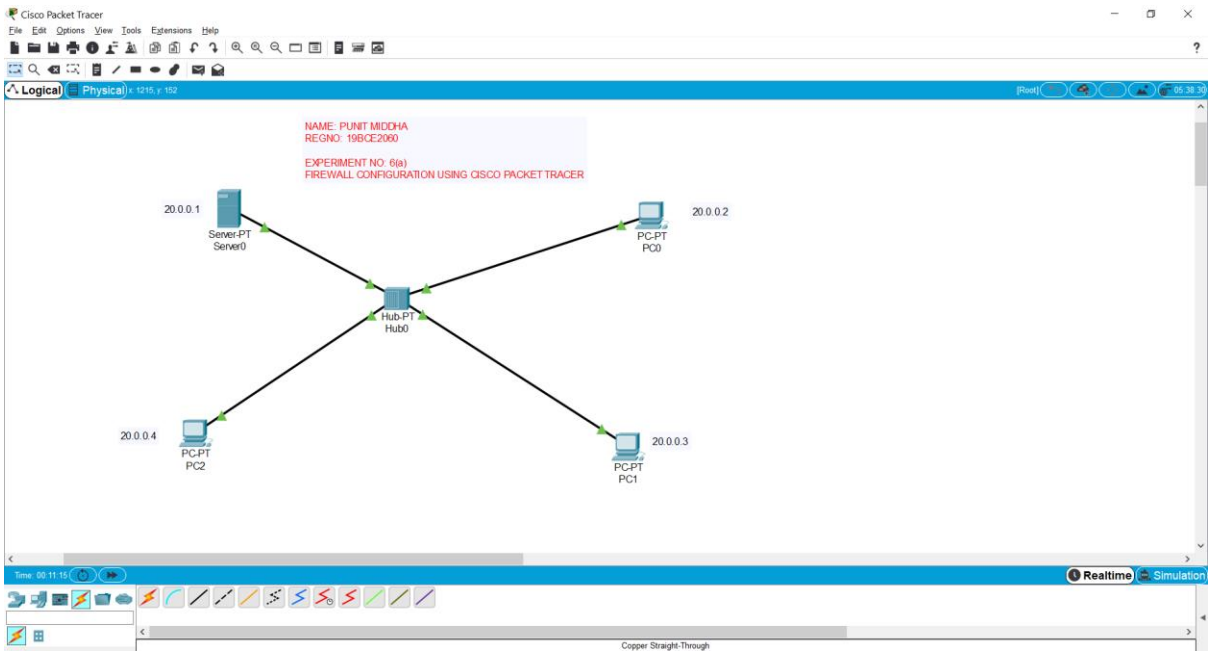
SLOT: L39+L40

DATE: 28/11/2021

6(a). Firewall Configuration Using Cisco Packet Tracer

Procedure:

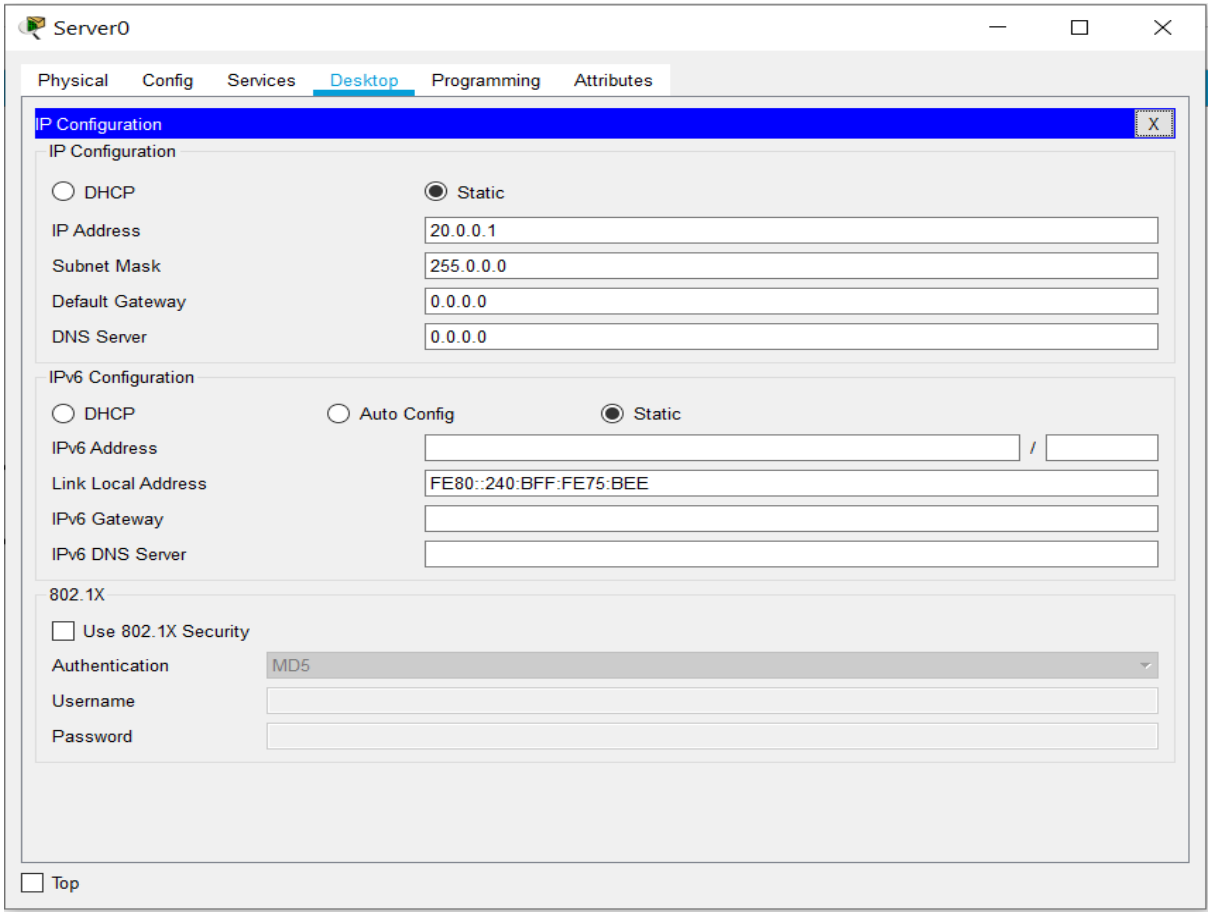
1. Go to end devices and place 1 hub, 1 server and 3 PC's.
2. Now, go to connections and choose Copper-Straight Through cable and connect as in screenshot given below.
   - Connect hub with 3 PC's and 1 Server i.e., Server0, PC0, PC1, PC2.

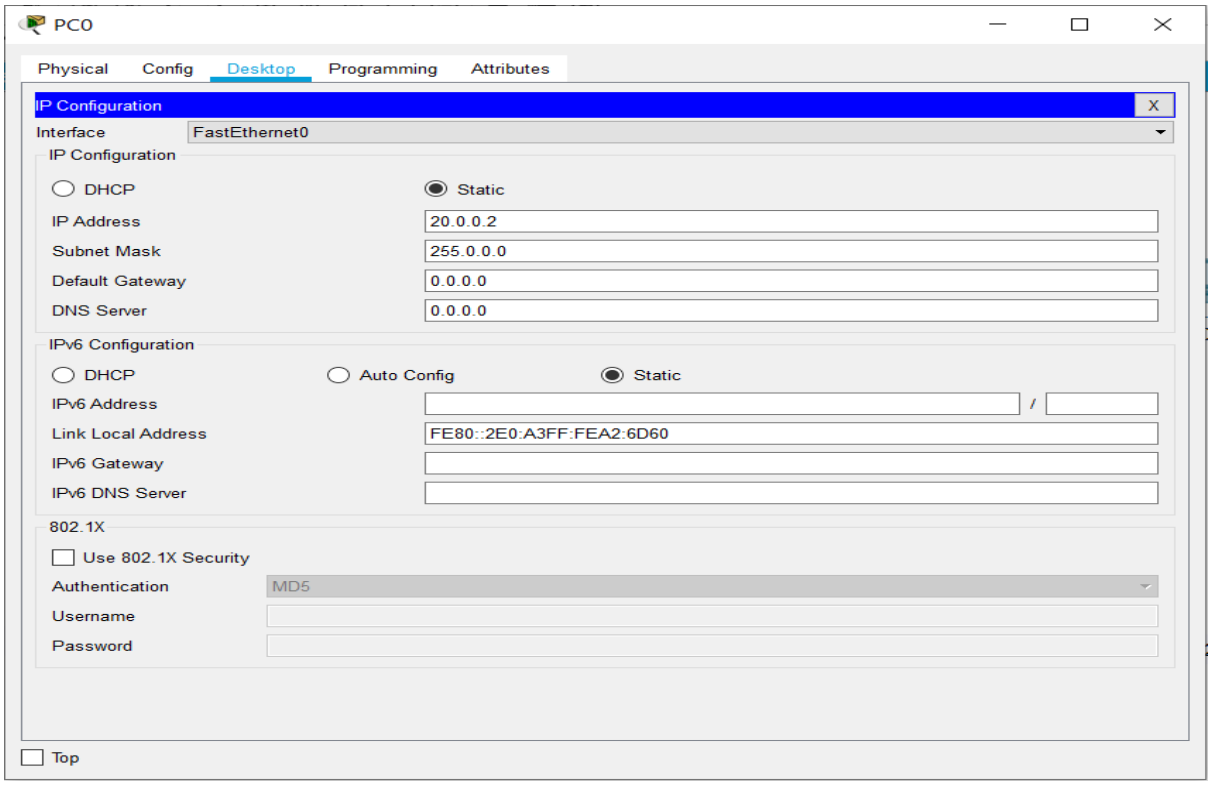


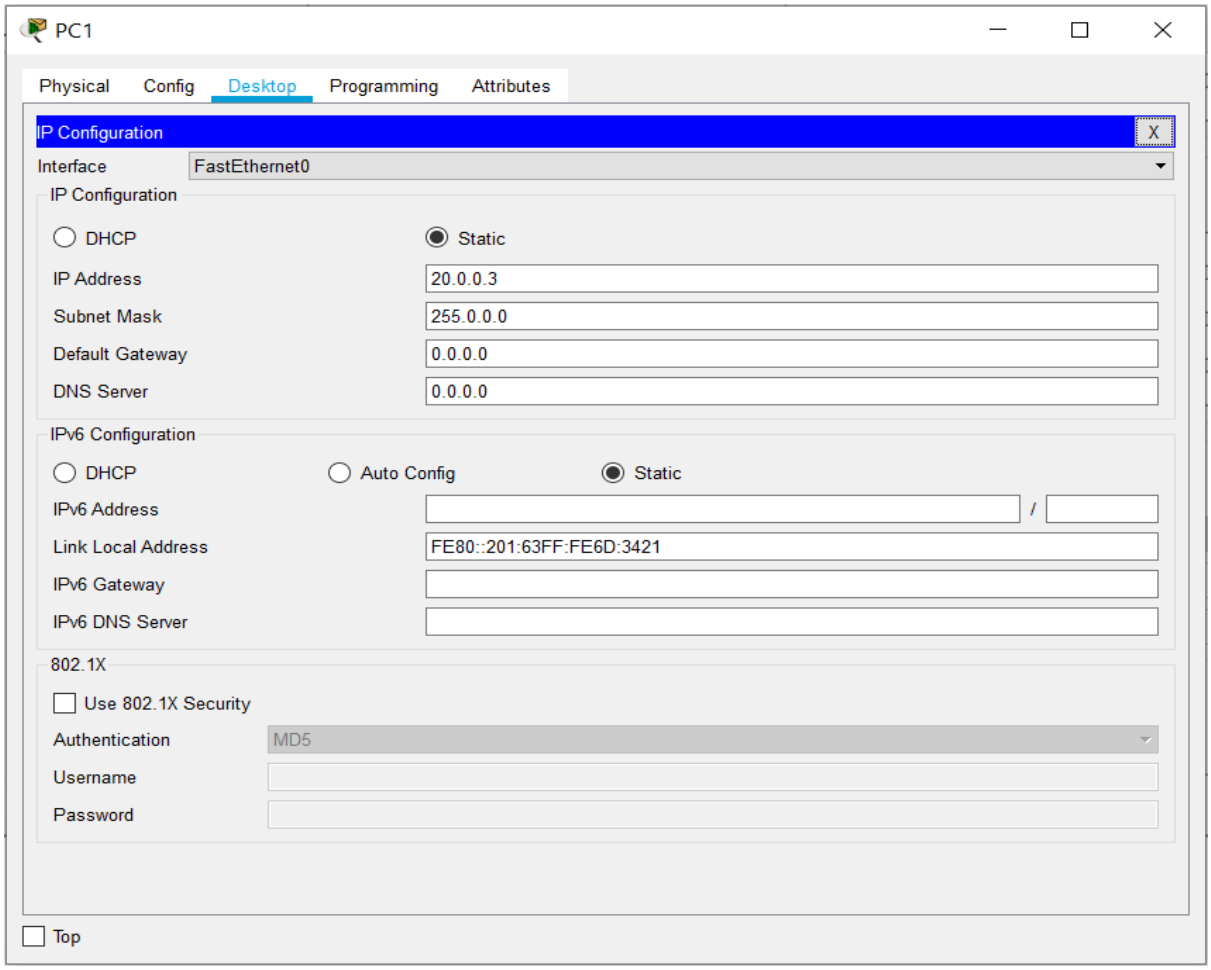
3. After completing the connection procedure, go to **Desktop → IP Configuration** and set the IP Addresses for each and every end device
   - **Server0:**
     IPv4 Address – 20.0.0.1
   - **PC0:**

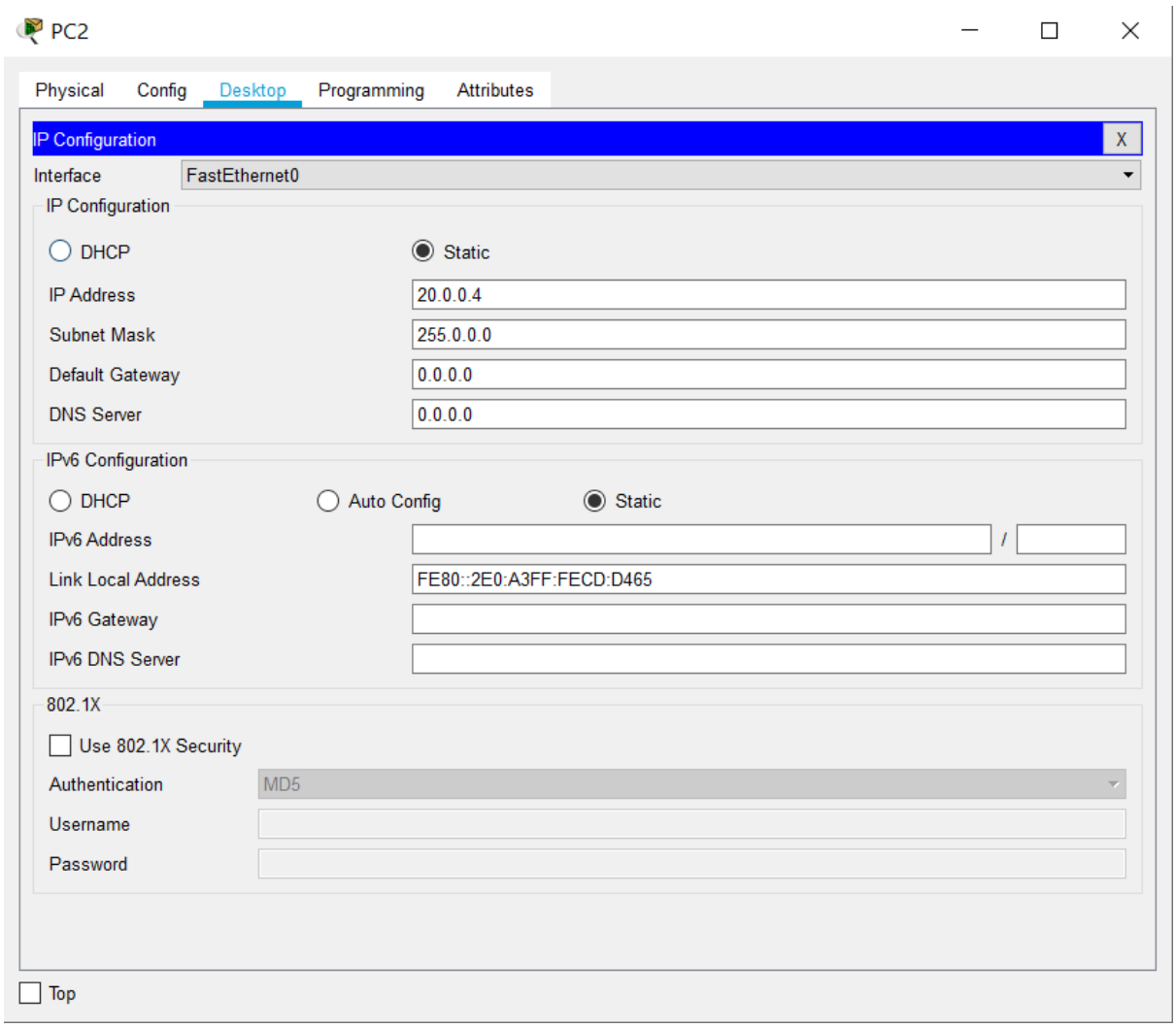
IPv4 Address - 20.0.0.2

- **PC1:**
  IPv4 Address - 20.0.0.3
- **PC2:**
  IPv4 Address - 20.0.0.4

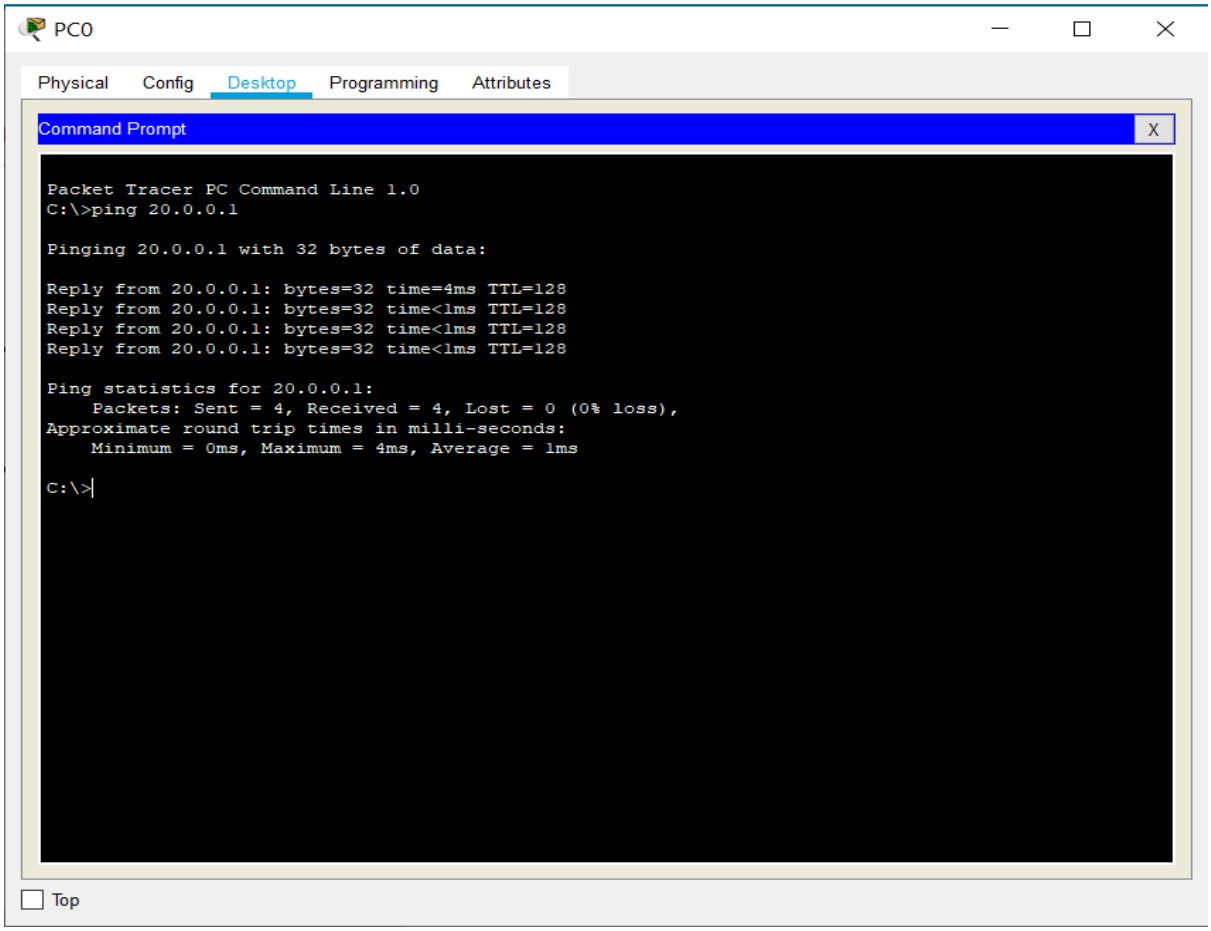


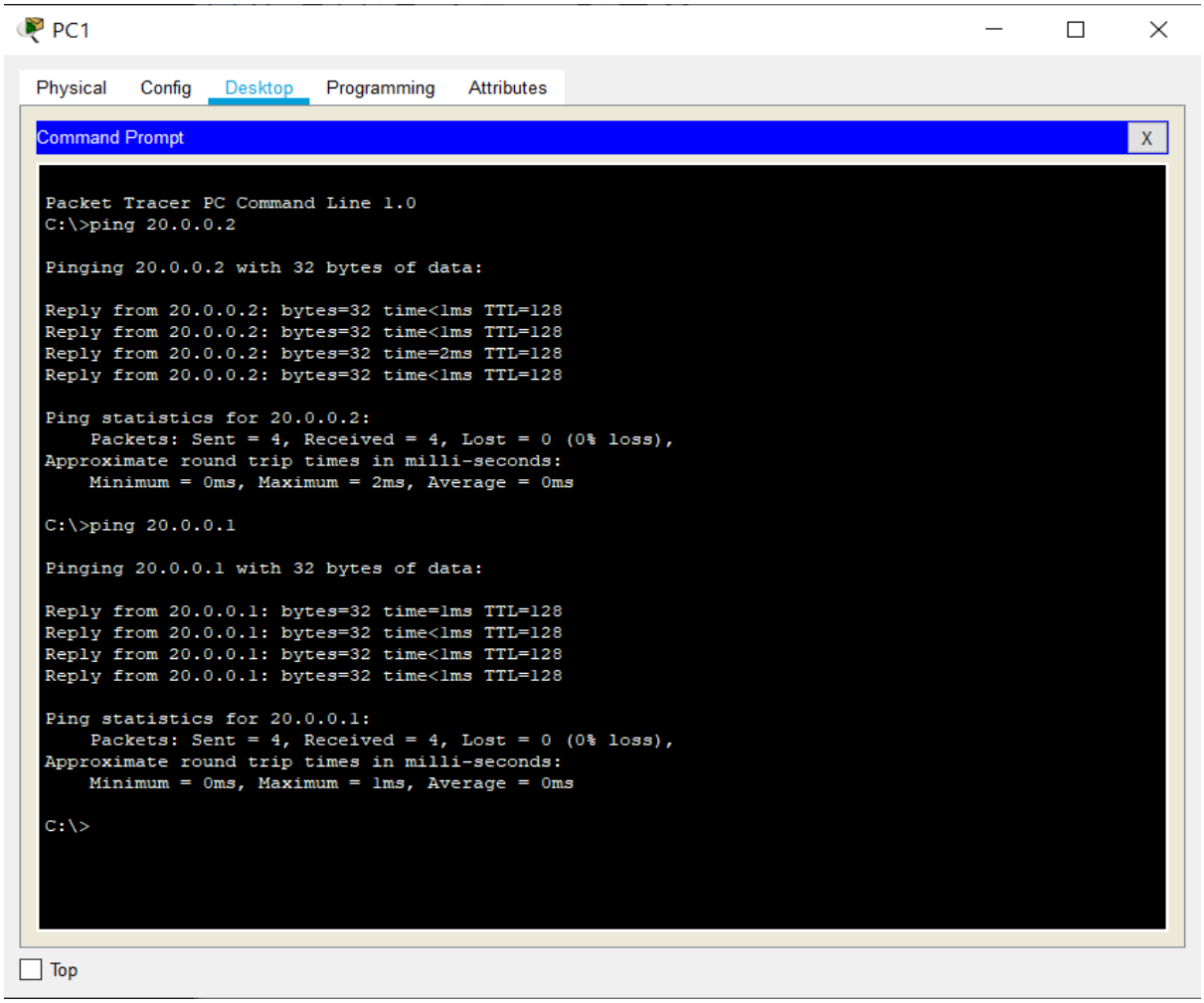



PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
20.0.0.3
Subnet Mask
255.0.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::201:63FF:FE6D:3421
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
20.0.0.4
Subnet Mask
255.0.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::2E0:A3FF:FECD:D465
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

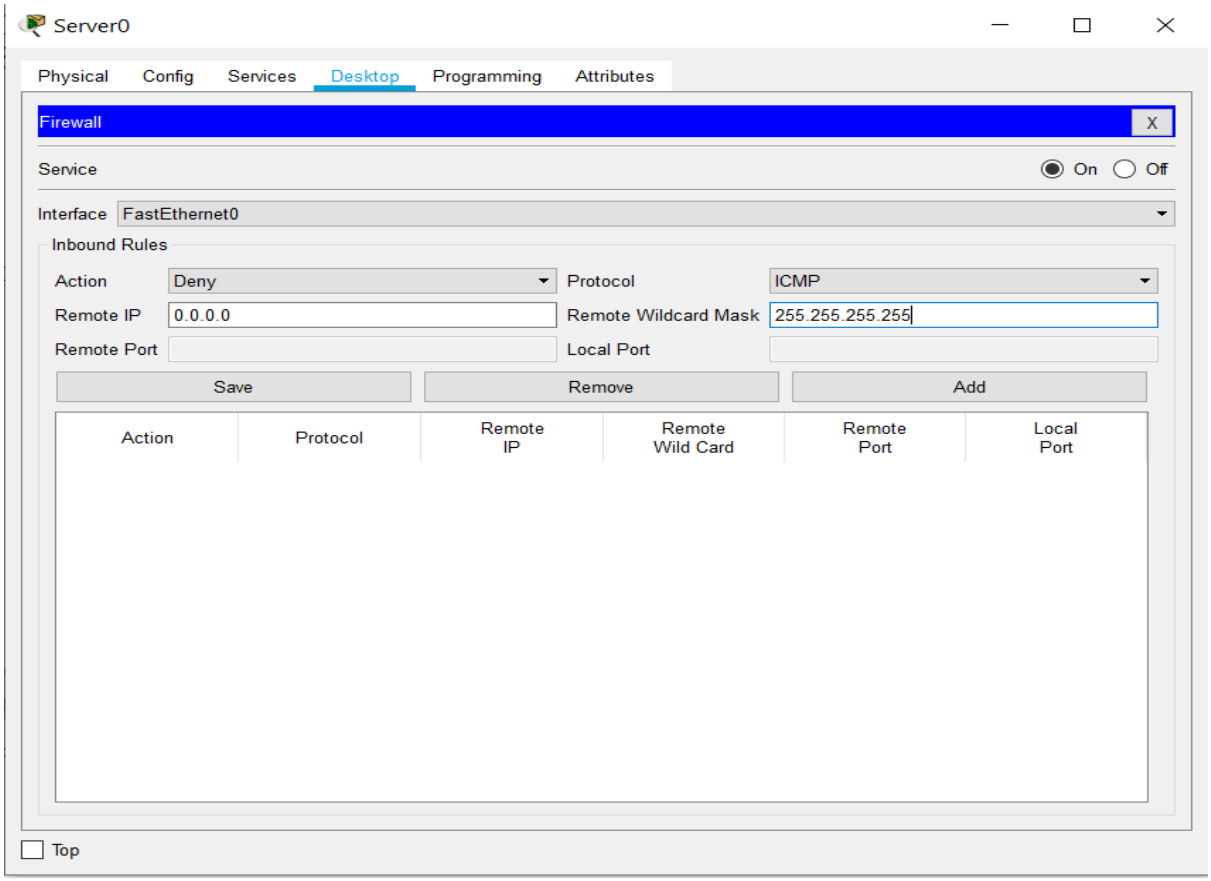
4. Now to check the connection **(Before Firewall Configuration)**, we have to use ping command from one end device to another end device as shown below in given screenshot.

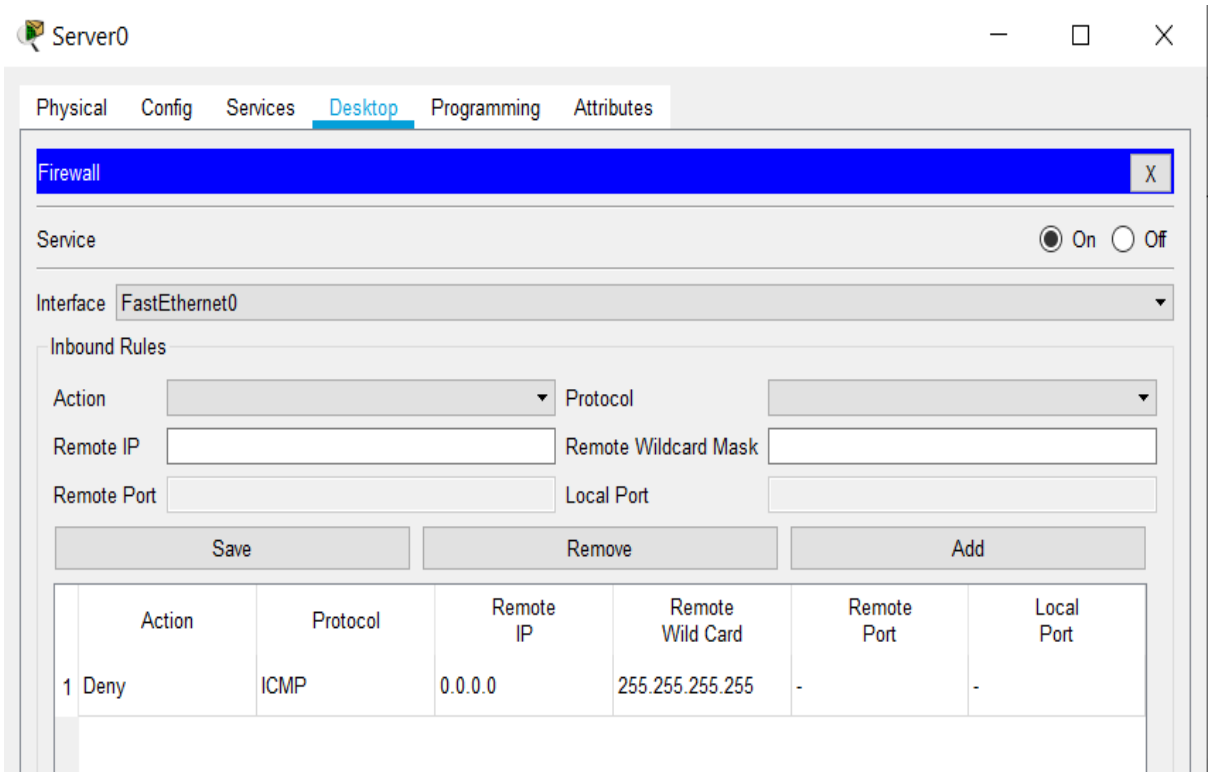




5. We can see that we are able to successfully ping from one device to another device. Now to configure firewall, go to **Server0 → Desktop → Firewall**.
   Select the following settings:
   Interface → FastEthernet0
   Action → Deny
   Protocol → ICMP
   Remote IP → 0.0.0.0
   Remote Wildcard Mask → 255.255.255.255

Now, 'ON' the services, click on 'Add' and 'Save' the settings.

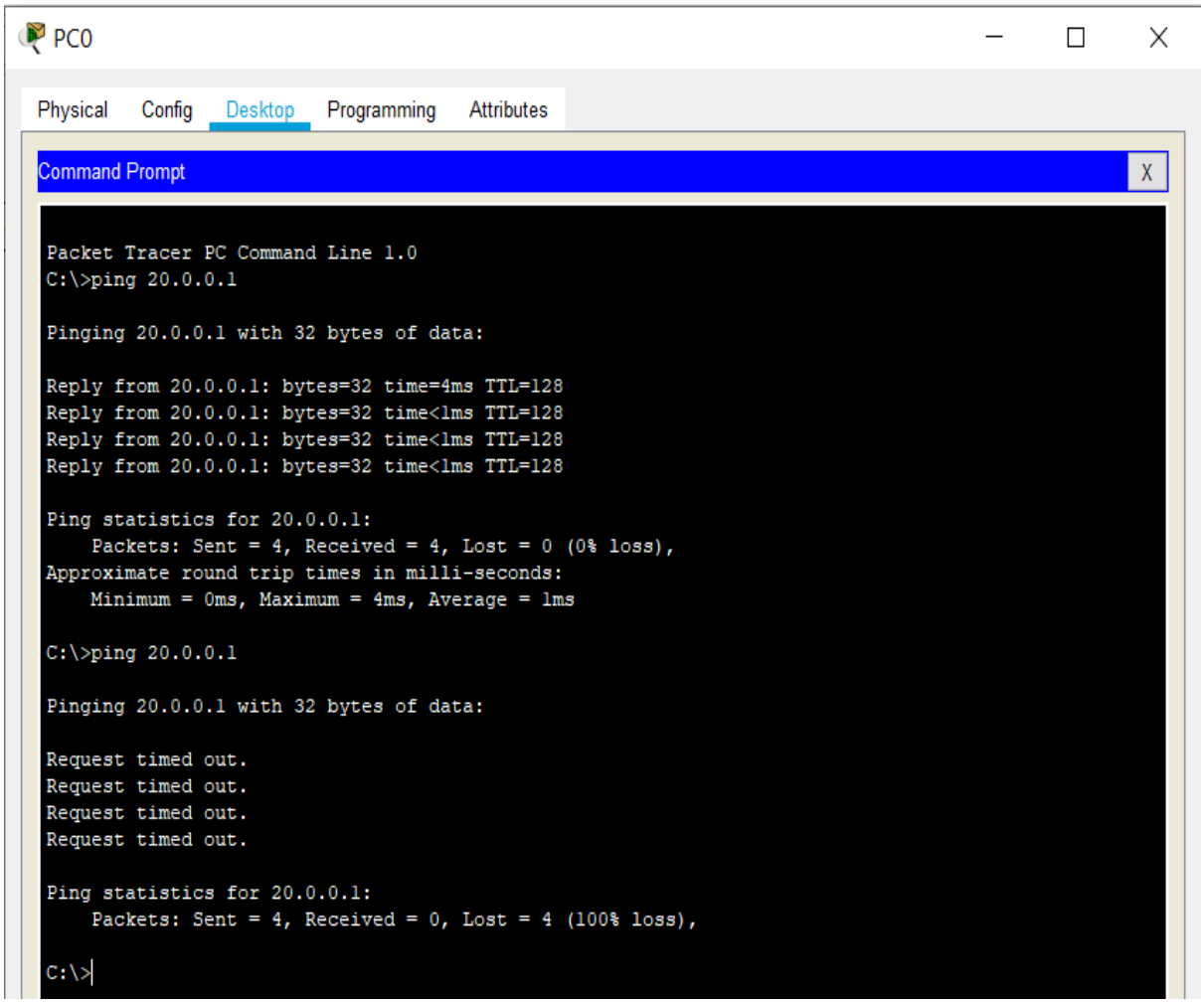


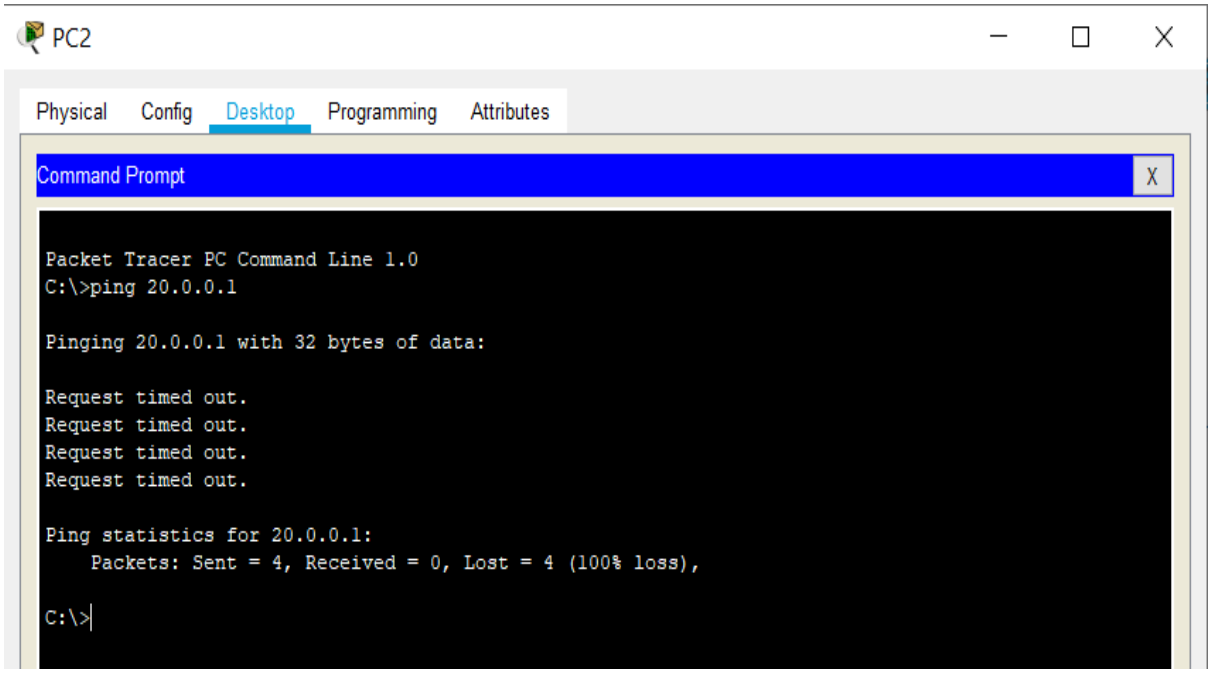


6. After configuring Firewall, we will try to ping from one device to another. Go to **PC0 → Desktop → Command Prompt.** Now, try to ping from PC0 to Server0 using **ping 20.0.0.1** command.

Output:

We can see that after configuration of firewall, we are not able to get any reply from one device to another. It is showing 'Request timed out' for all the packets. Hence, we can say that Firewall Configuration is working properly.



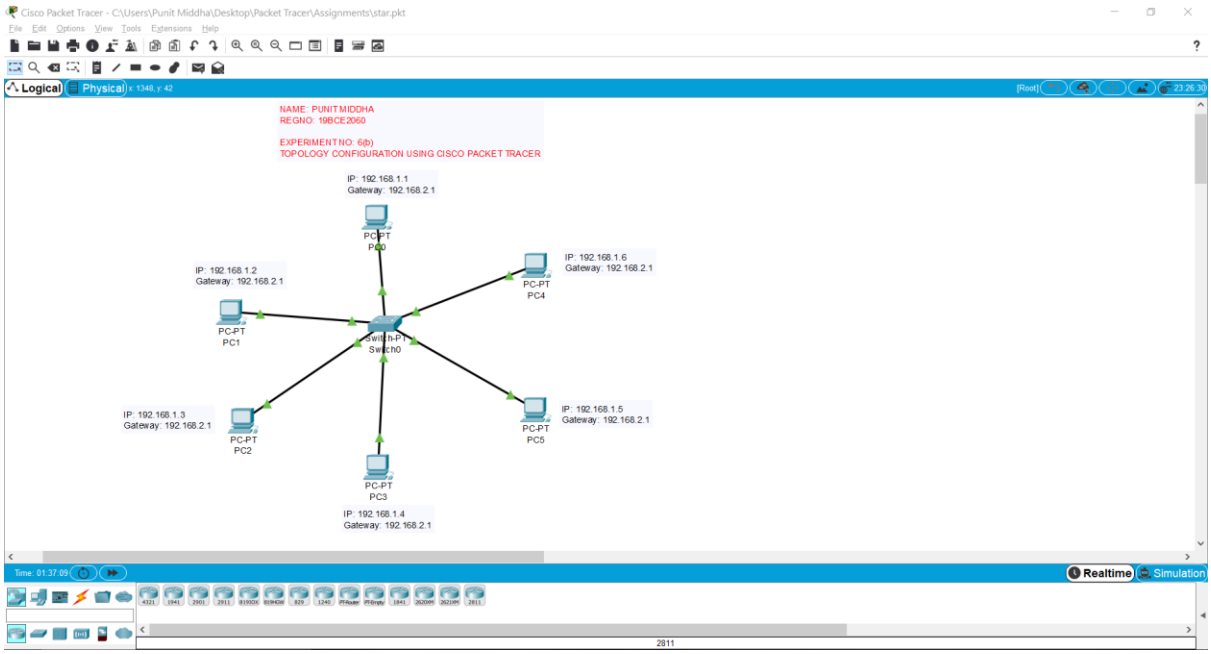


6(b). Topology Configuration Using Cisco Packet Tracer

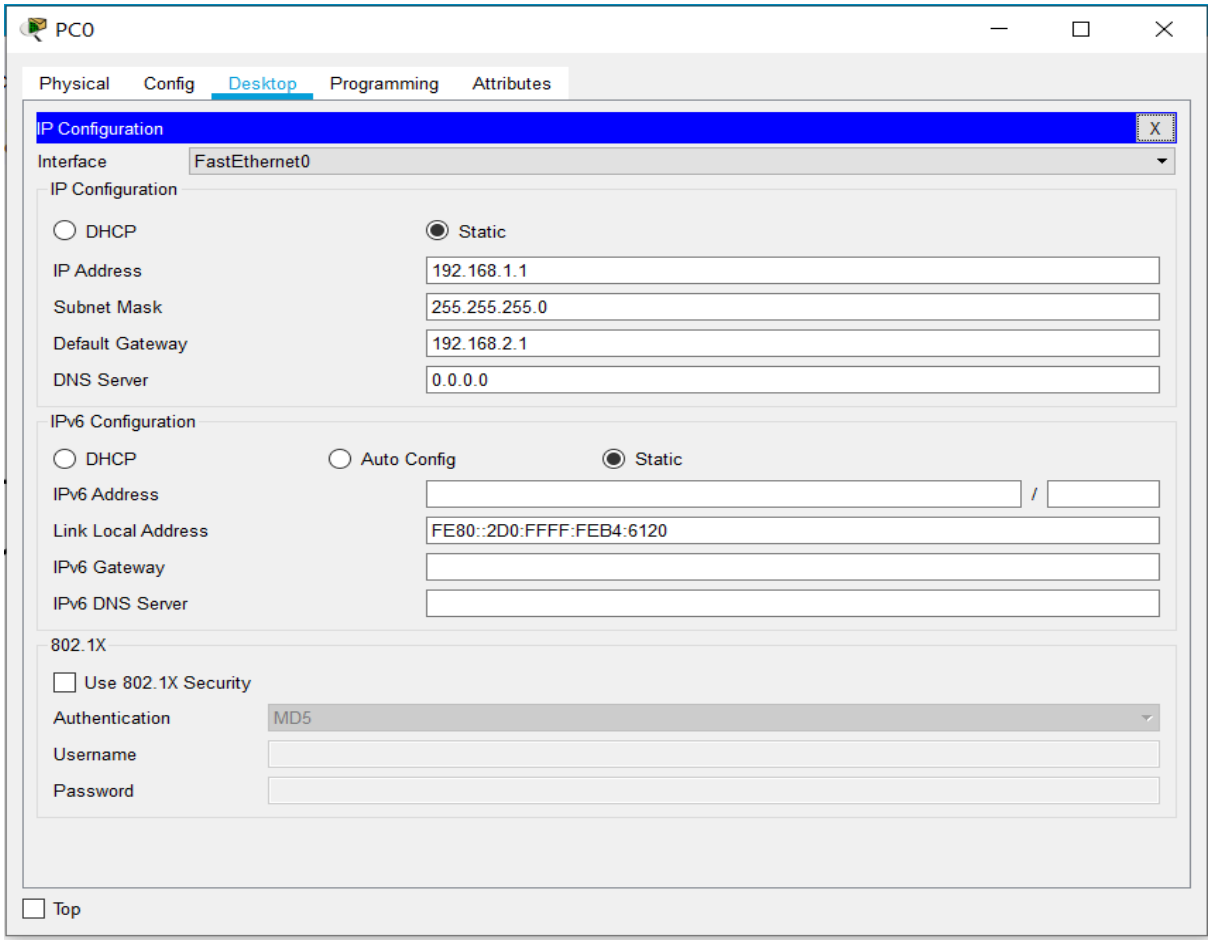
I. Star Topology:

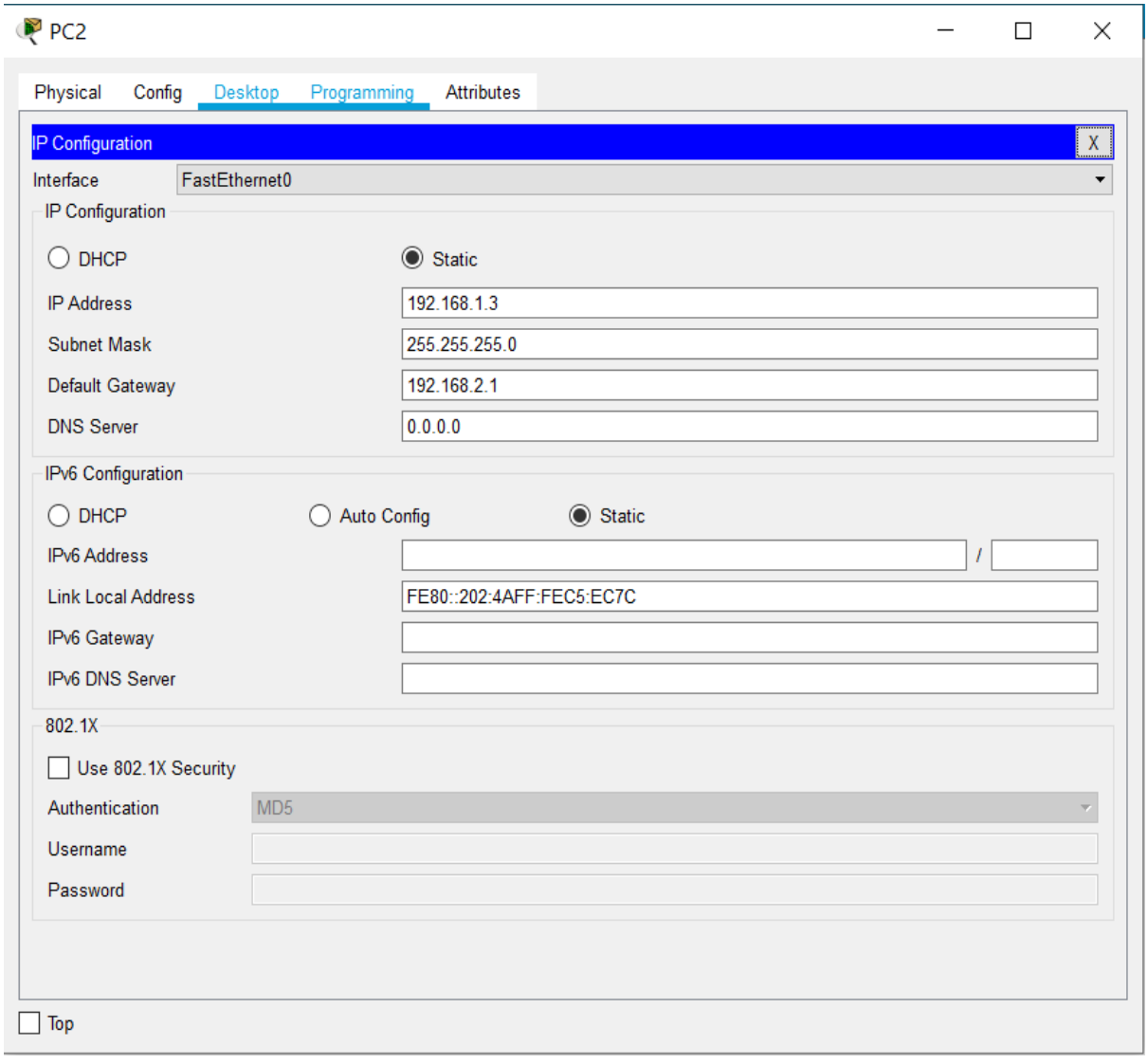
Procedure:

1. Go to end devices and place 1 switch and 6 PC's.
2. Now, go to connections and choose Copper-Straight Through cable and connect as in screenshot given below.
   - Connect Switch0 with 6 PC's i.e., PC0, PC1, PC2, PC3, PC4, PC5.



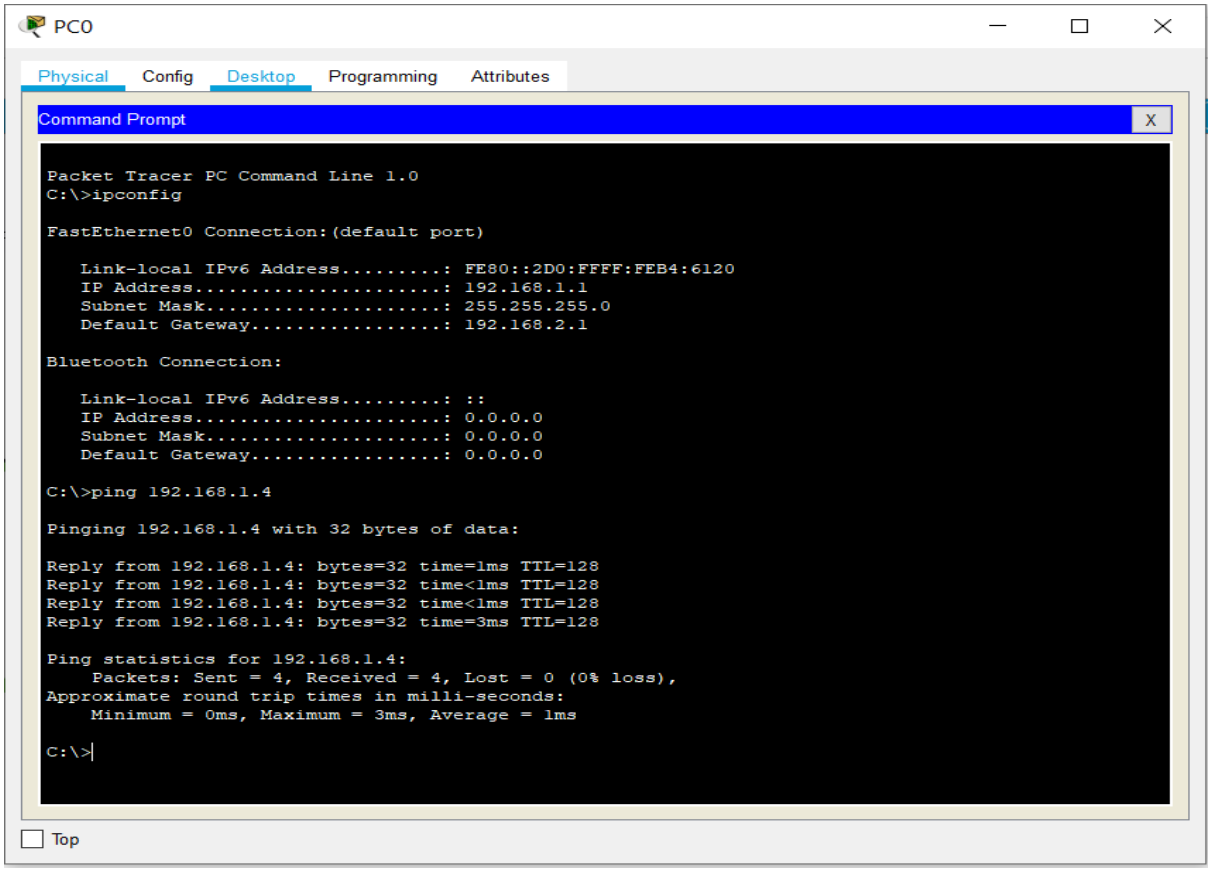
3. After completing the connection procedure, go to **Desktop → IP Configuration** and set the IP Addresses for each and every end device
   - **PC0:**
     IPv4 Address – 192.168.1.1
     Default Gateway - 192.168.2.1
   - **PC1:**
     IPv4 Address – 192.168.1.2
     Default Gateway - 192.168.2.1
   - **PC2:**
     IPv4 Address – 192.168.1.3
     Default Gateway - 192.168.2.1
   - **PC3:**
     IPv4 Address – 192.168.1.4
     Default Gateway - 192.168.2.1
   - **PC4:**
     IPv4 Address – 192.168.1.6
     Default Gateway - 192.168.2.1
   - **PC5:**
     IPv4 Address – 192.168.1.5
     Default Gateway - 192.168.2.1

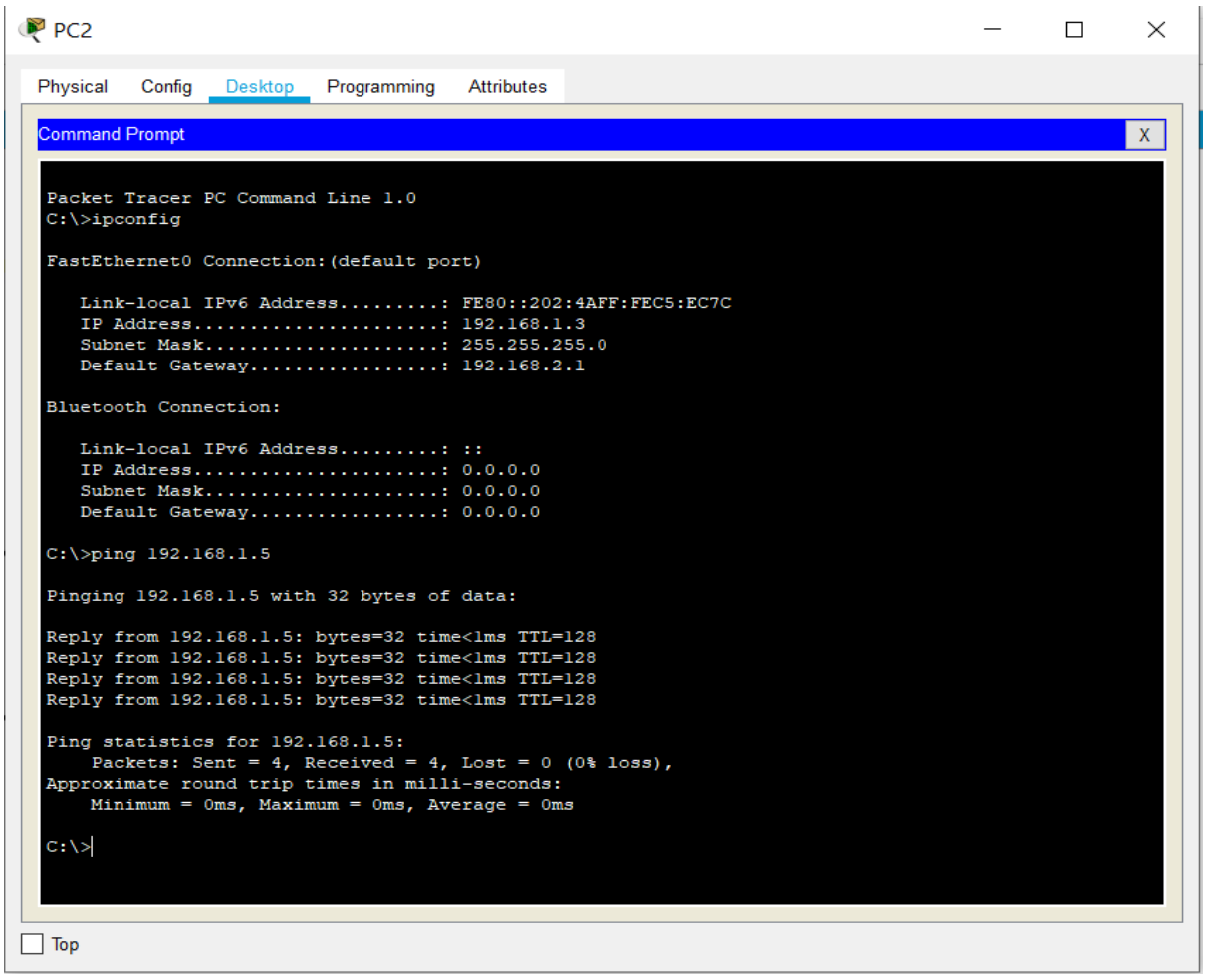

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.1.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::2D0:FFFF:FEB4:6120
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::202:4AFF:FEC5:EC7C
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

Output:

To check the connection, go to **PC → Desktop → Command Prompt** use **ipconfig and ping command** as shown in screenshot below. We can see that ping command **(ping 192.168.1.4, ping 192.168.1.5)** is executing successfully hence, implementation of mesh topology using cisco packet tracer is correct.

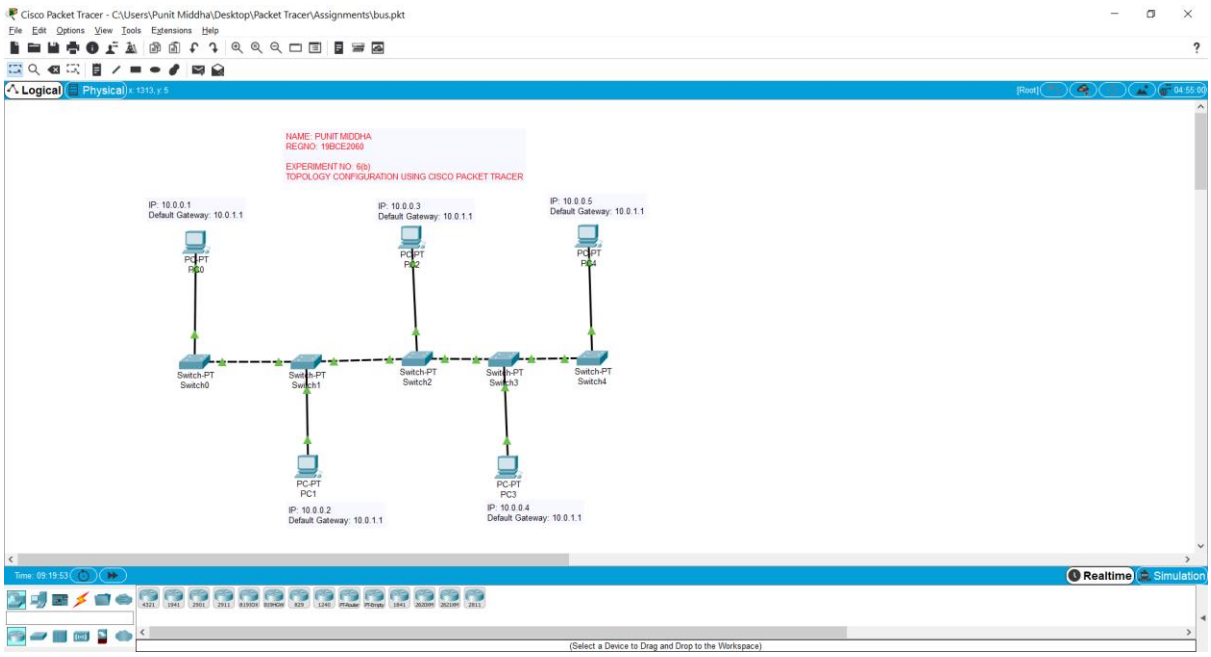




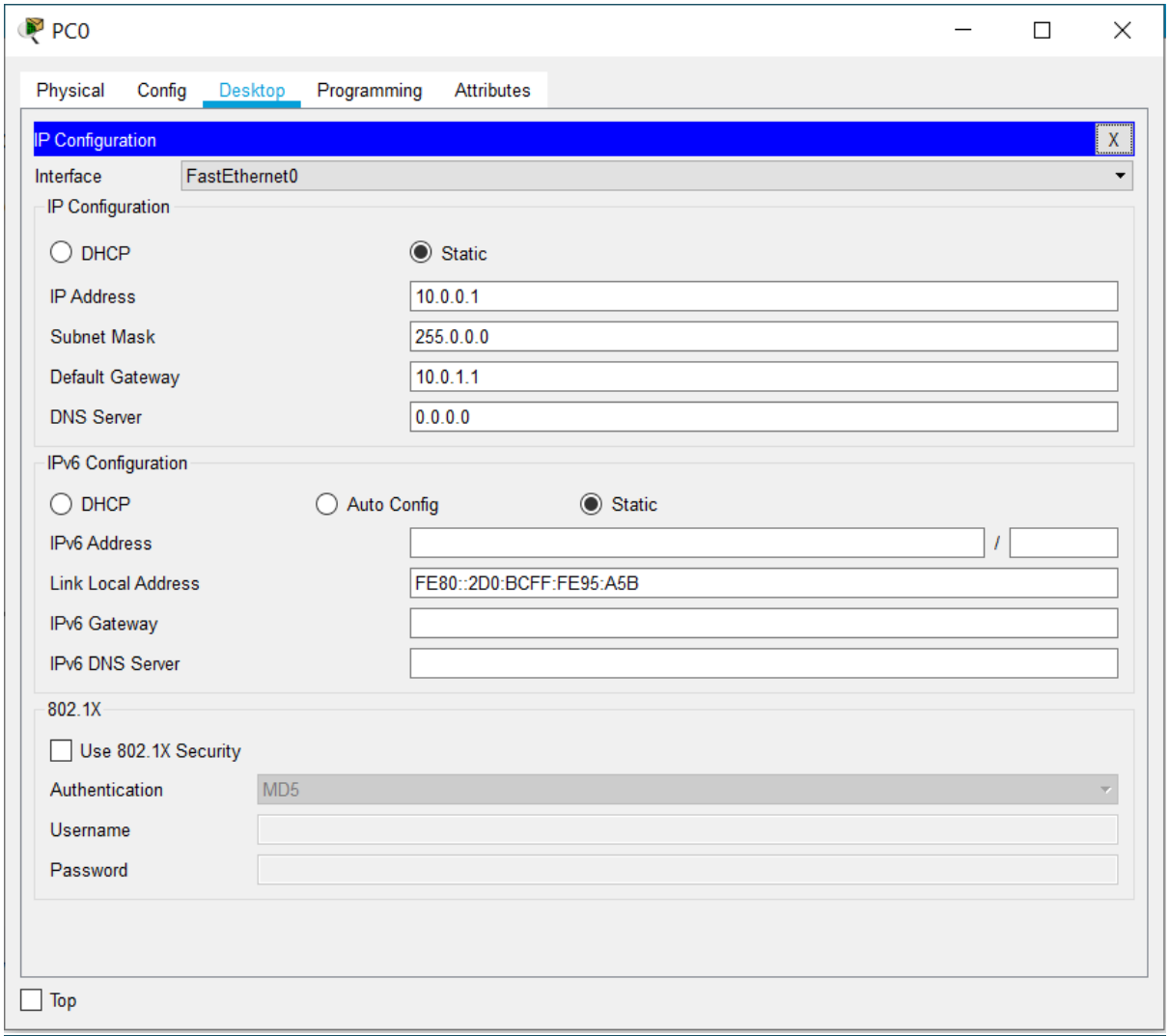
II. Bus Topology:

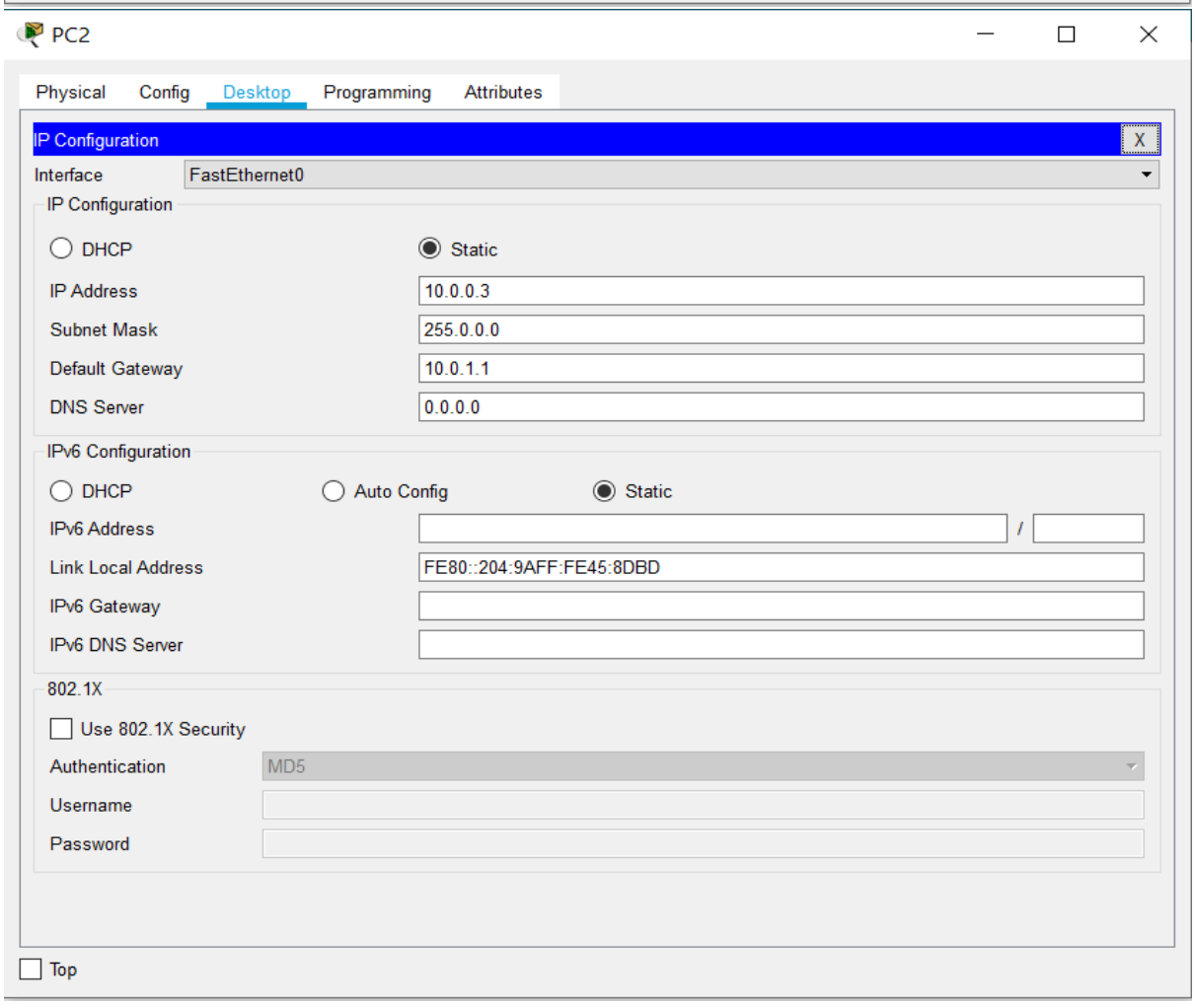
Procedure:

1. Go to end devices and place 5 switch and 5 PC's.
2. Now, go to connections and choose Copper-Straight Through cable and connect as in screenshot given below.
   - Connect one PC with each Switch.



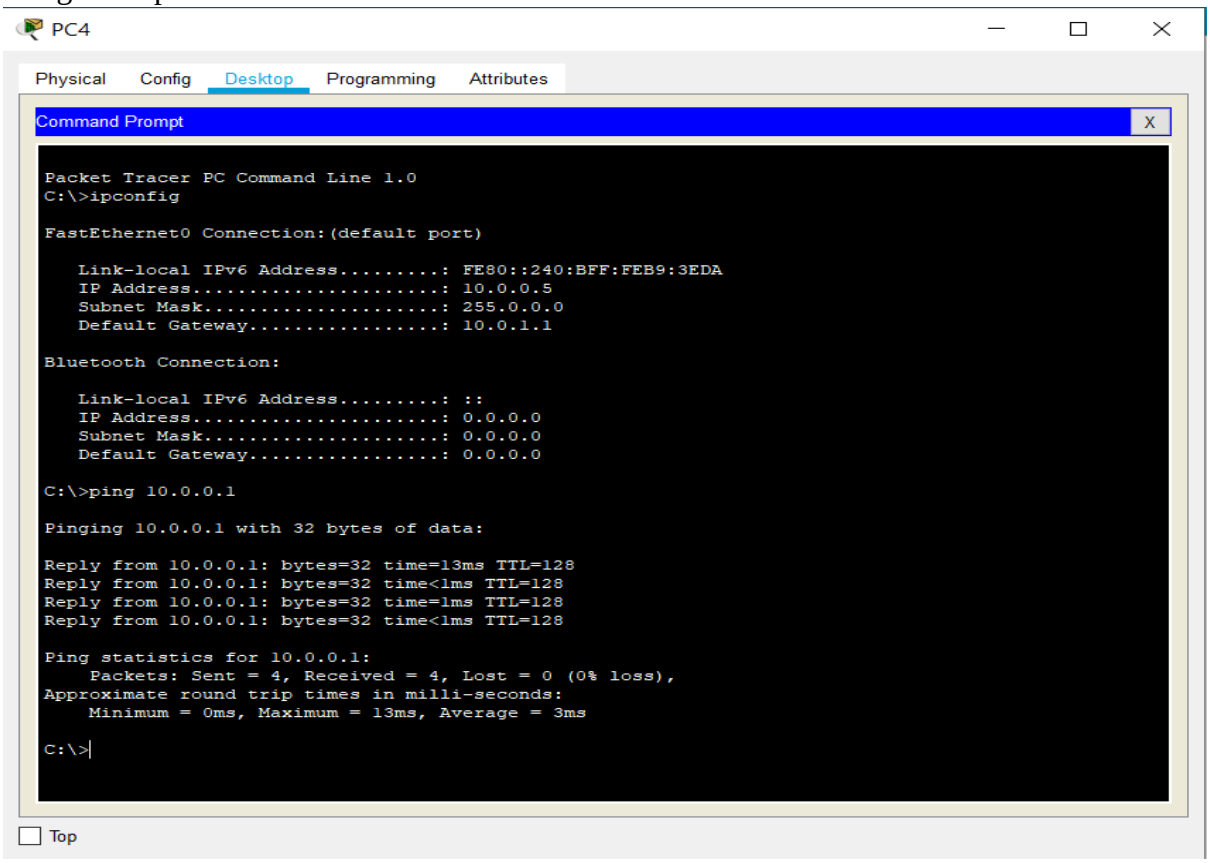
3. After completing the connection procedure, go to **Desktop → IP Configuration** and set the IP Addresses for each and every end device
   - **PC0:**
     IPv4 Address – 10.0.0.1
     Default Gateway – 10.0.1.1
   - **PC1:**
     IPv4 Address – 10.0.0.2
     Default Gateway – 10.0.1.1
   - **PC2:**
     IPv4 Address – 10.0.0.3
     Default Gateway – 10.0.1.1
   - **PC3:**
     IPv4 Address – 10.0.0.4
     Default Gateway – 10.0.1.1
   - **PC4:**
     IPv4 Address – 10.0.0.5
     Default Gateway – 10.0.1.1

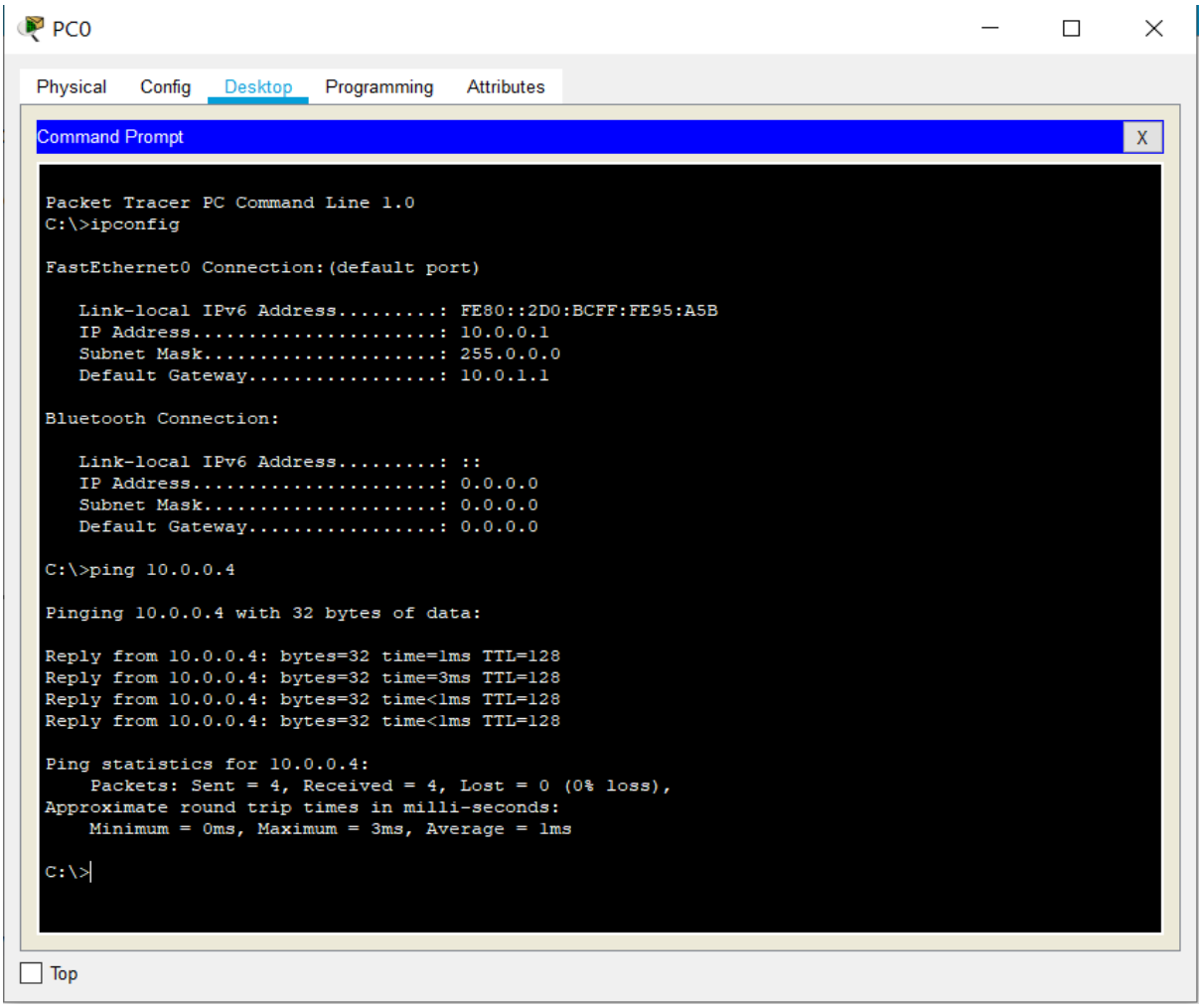

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
10.0.0.1
Subnet Mask
255.0.0.0
Default Gateway
10.0.1.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::2D0:BCFF:FE95:A5B
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
10.0.0.3
Subnet Mask
255.0.0.0
Default Gateway
10.0.1.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::204:9AFF:FE45:8DBD
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

Output:

To check the connection, go to **PC → Desktop → Command Prompt** use **ipconfig and ping command** as shown in screenshot below. We can see that ping command **(ping 10.0.0.1, ping 10.0.0.4)** is executing successfully hence, implementation of bus topology using cisco packet tracer is correct.

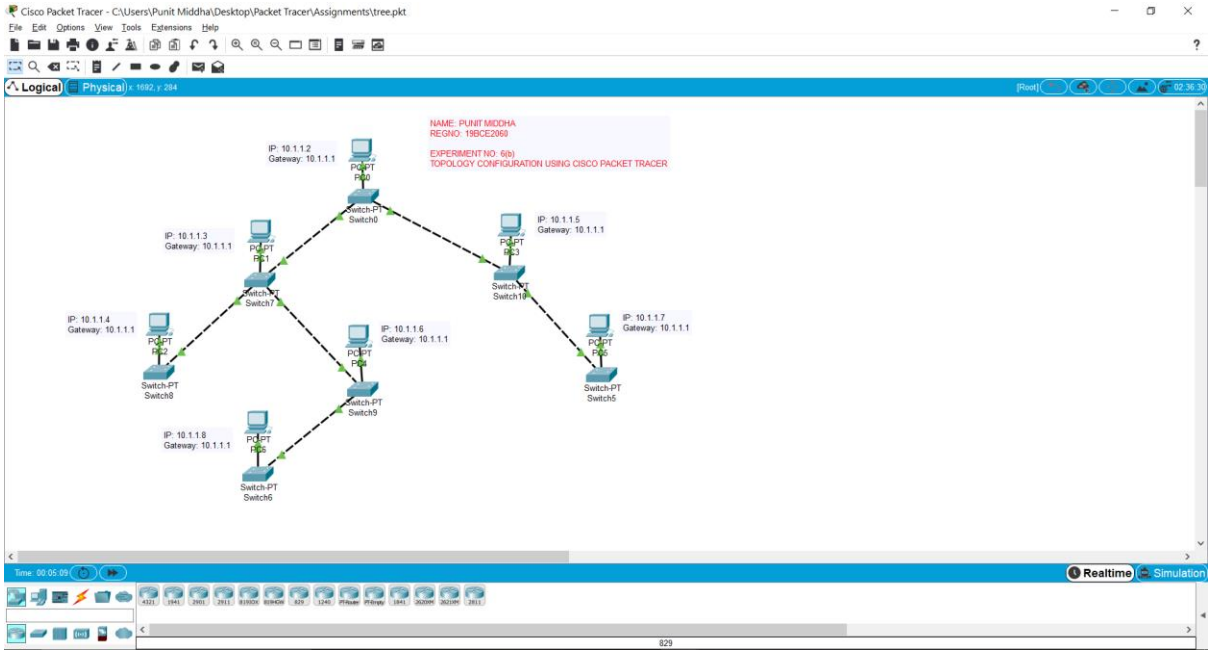




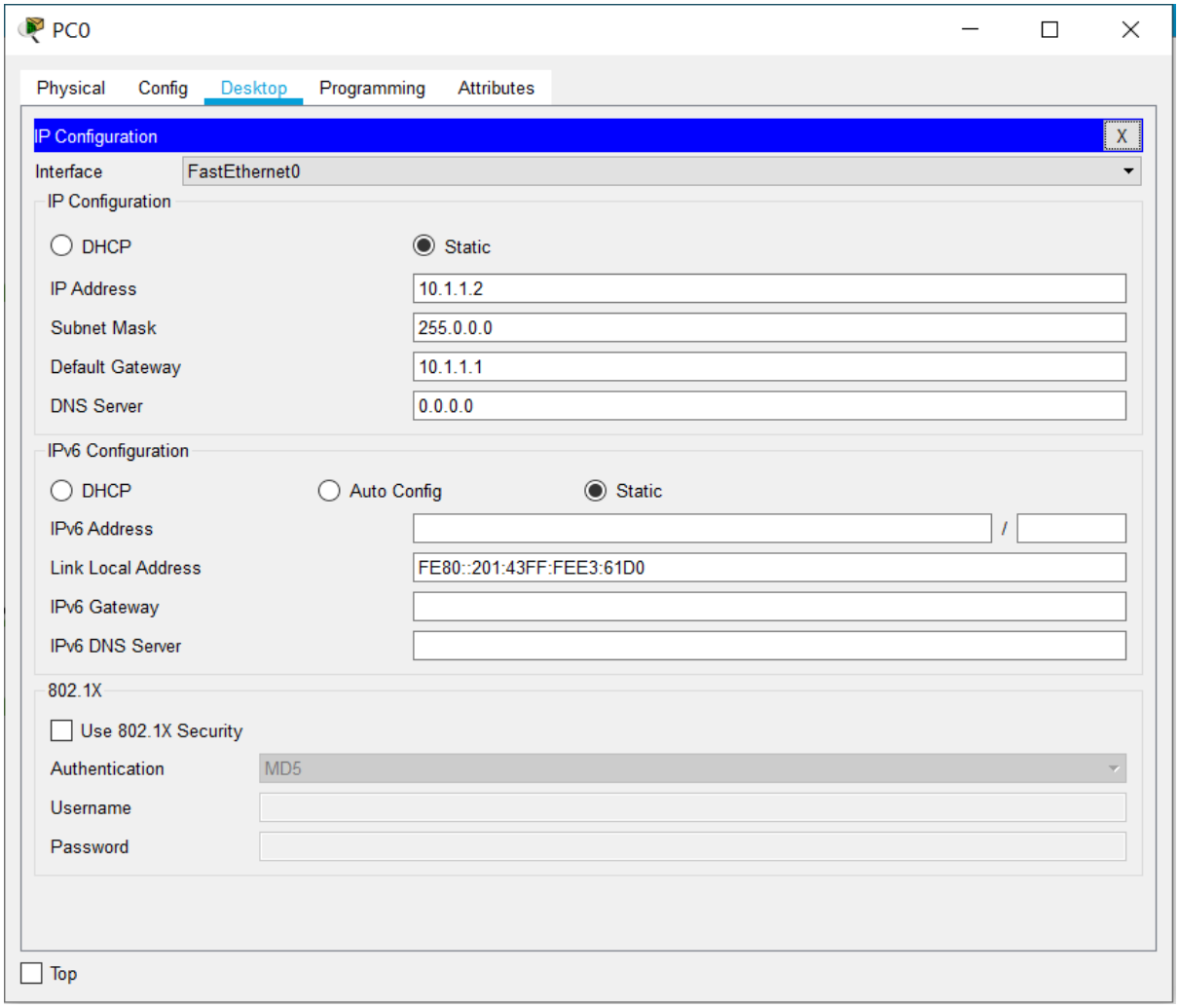
III. Tree Topology:

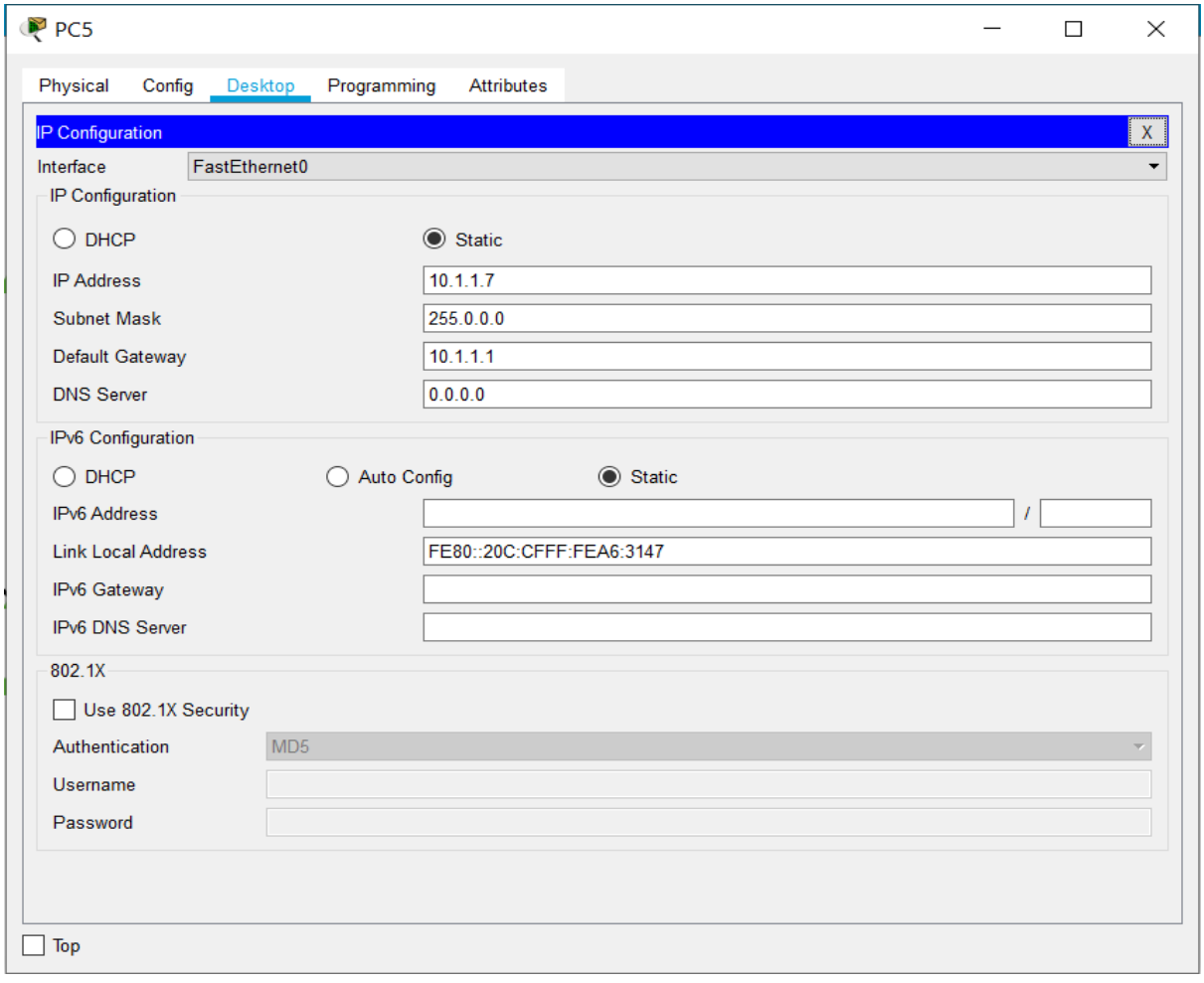
Procedure:

1. Go to end devices and place 7 switch and 7 PC's.
2. Now, go to connections and choose Copper-Straight Through cable and connect as in screenshot given below.
   - Connect one PC with each Switch.



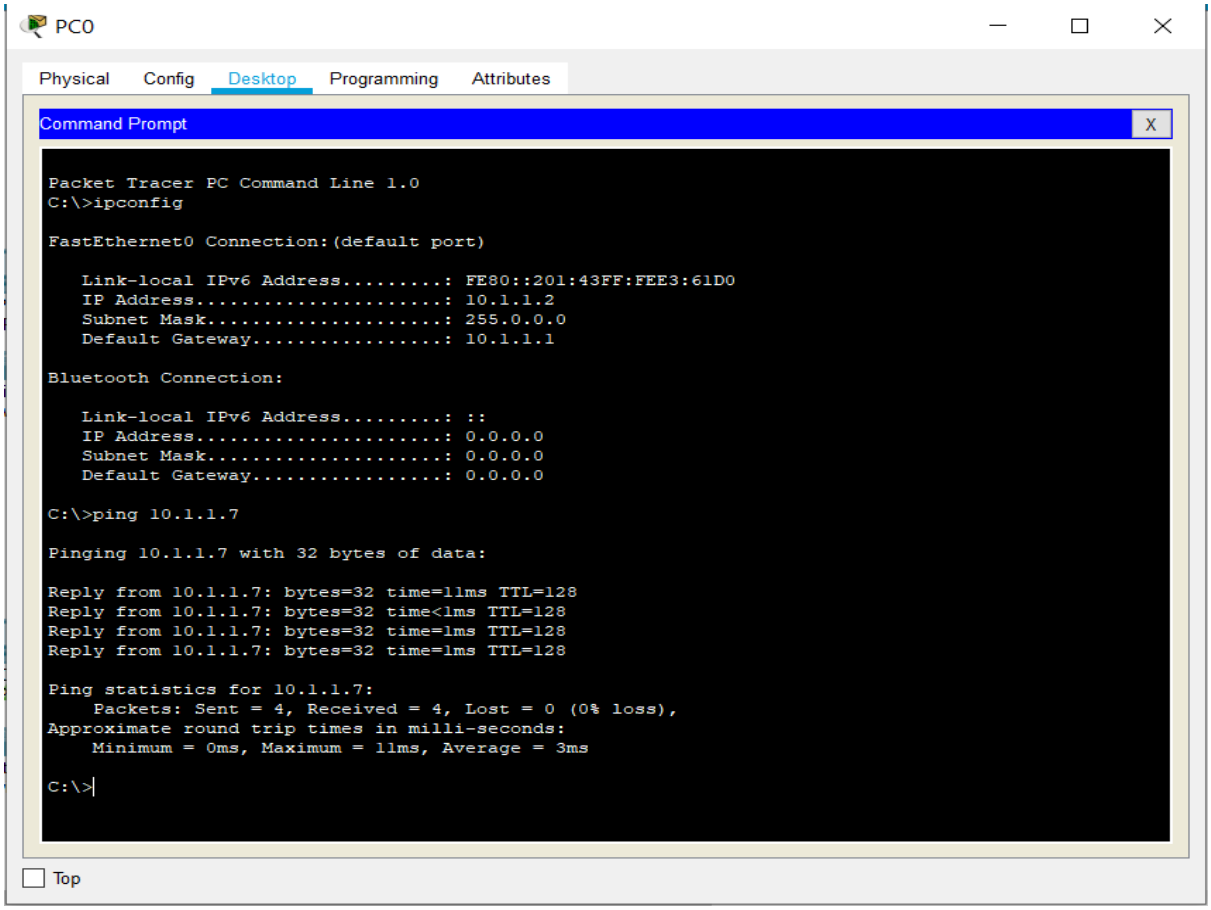
3. After completing the connection procedure, go to **Desktop → IP Configuration** and set the IP Addresses for each and every end device
   - **PC0:**
     IPv4 Address – 10.1.1.2
     Default Gateway – 10.1.1.1
   - **PC1:**
     IPv4 Address – 10.1.1.3
     Default Gateway – 10.1.1.1
   - **PC2:**
     IPv4 Address – 10.1.1.4
     Default Gateway – 10.1.1.1
   - **PC3:**
     IPv4 Address – 10.1.1.5
     Default Gateway – 10.1.1.1
   - **PC4:**
     IPv4 Address – 10.1.1.6
     Default Gateway – 10.1.1.1
   - **PC5:**
     IPv4 Address – 10.1.1.7
     Default Gateway – 10.1.1.1
   - **PC6:**
     IPv4 Address – 10.1.1.8
     Default Gateway – 10.1.1.1

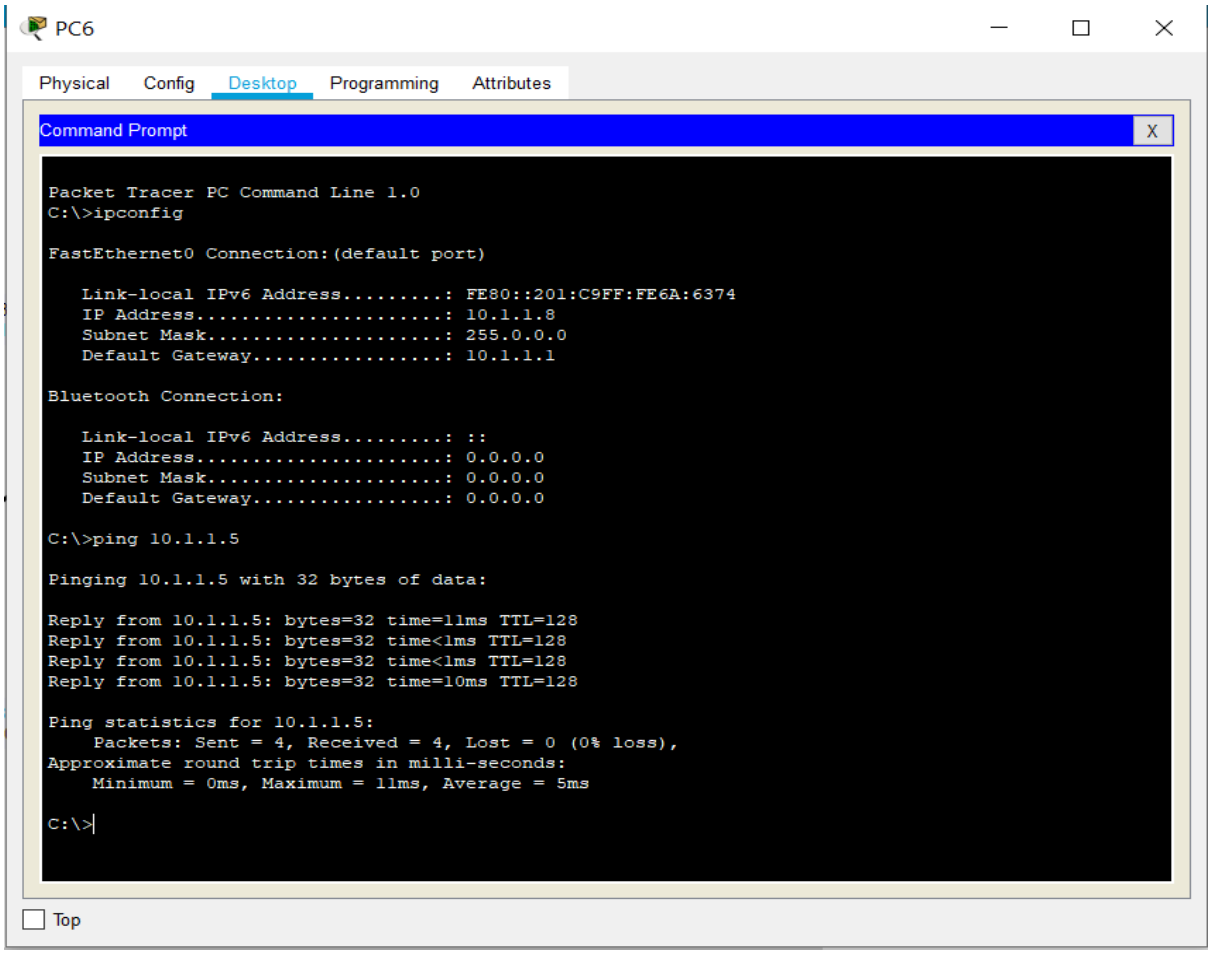

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
10.1.1.2
Subnet Mask
255.0.0.0
Default Gateway
10.1.1.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::201:43FF:FEE3:61D0
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC5
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
10.1.1.7
Subnet Mask
255.0.0.0
Default Gateway
10.1.1.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::20C:CFFF:FEA6:3147
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

Output:

To check the connection, go to **PC → Desktop → Command Prompt** use **ipconfig and ping command** as shown in screenshot below. We can see that ping command **(ping 10.1.1.7, ping 10.1.1.5)** is executing successfully hence, implementation of tree topology using cisco packet tracer is correct.

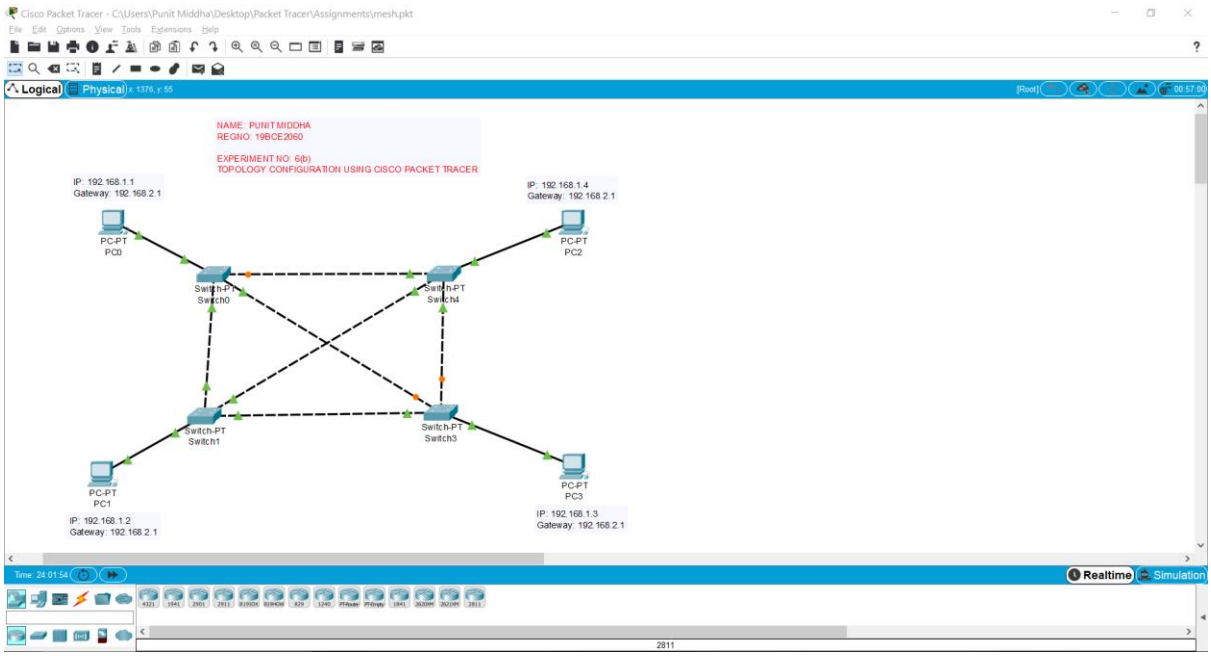




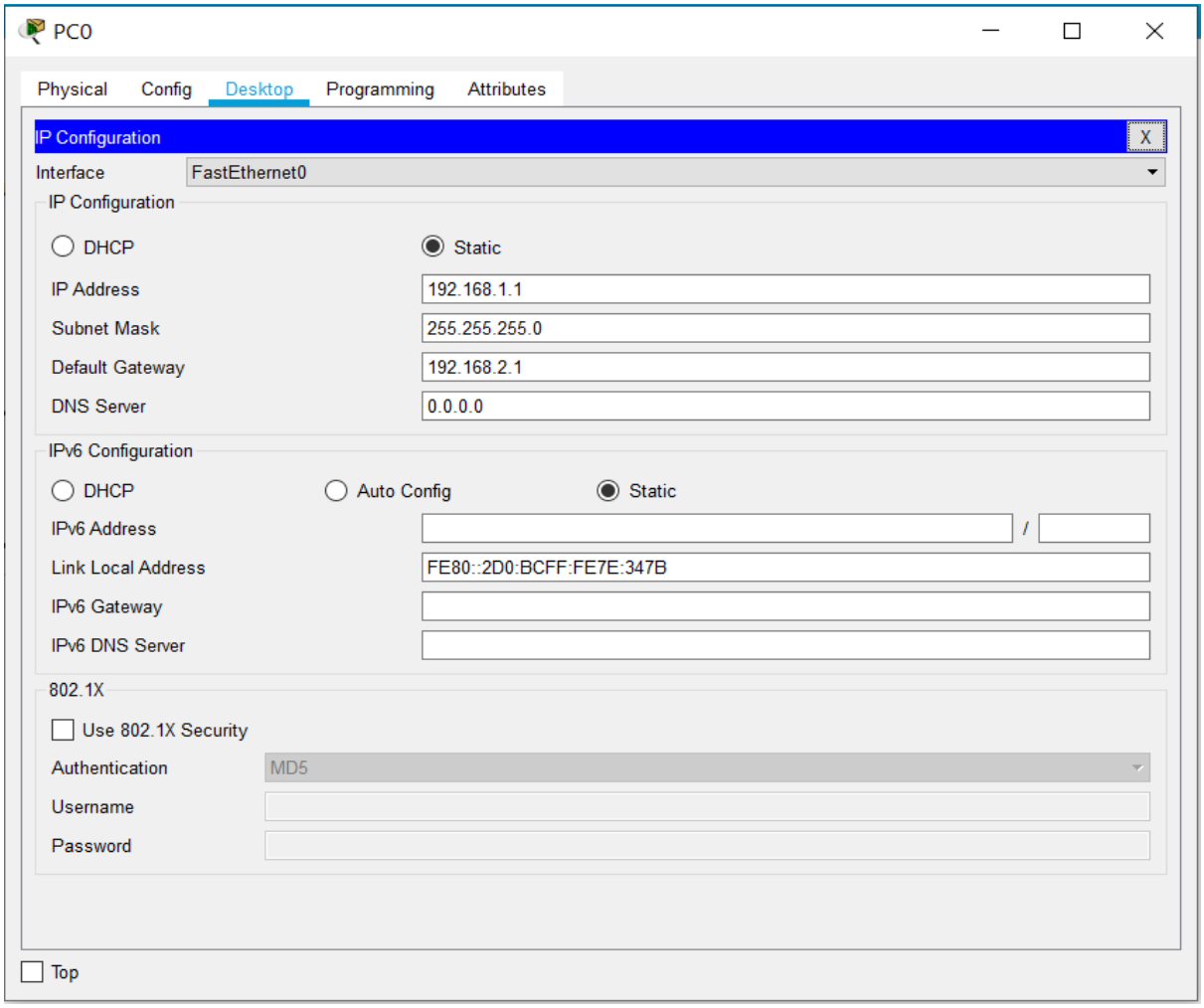
IV. Mess Topology

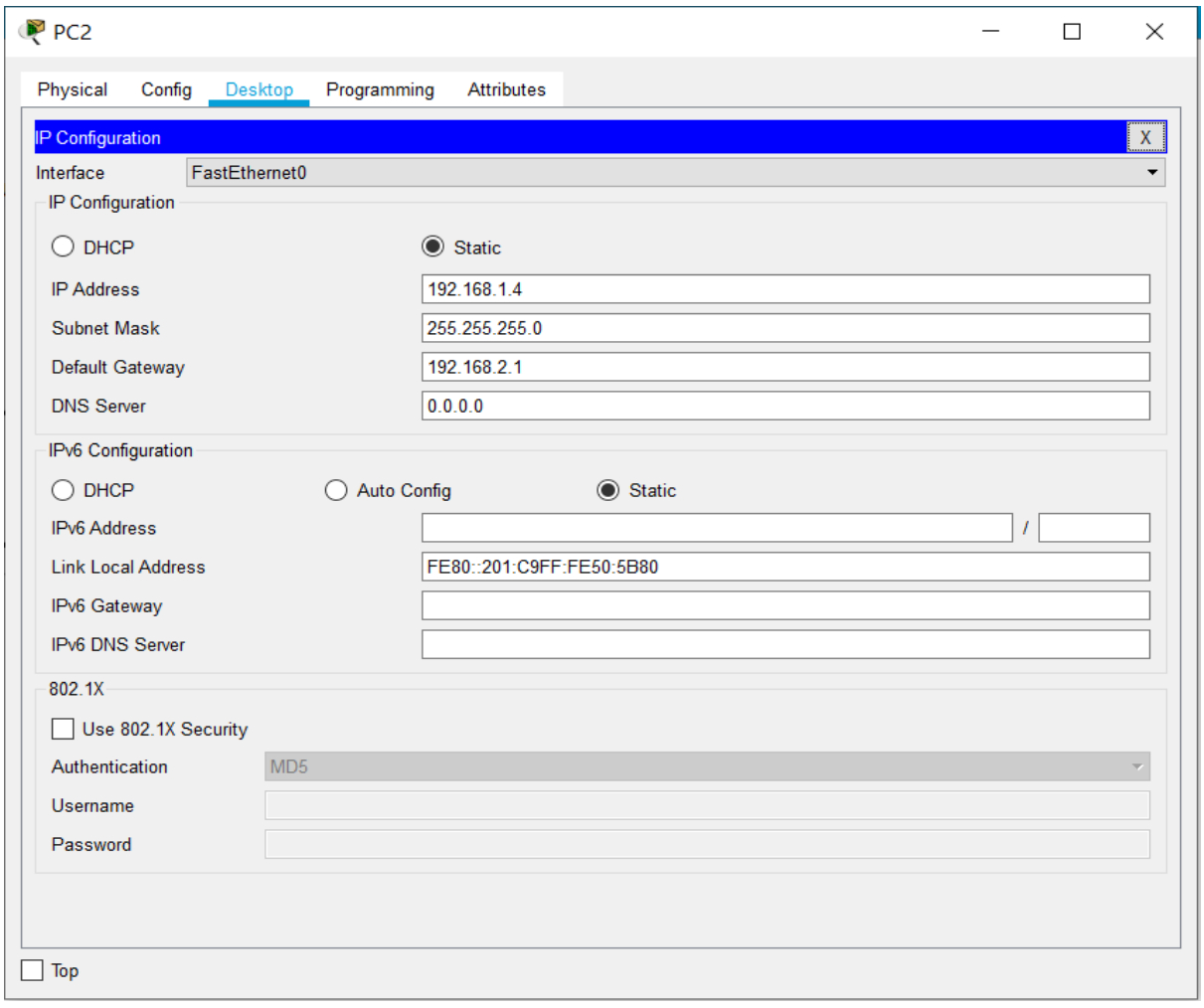
Procedure:

1. Go to end devices and place 4 switch and 4 PC's.
2. Now, go to connections and choose Copper-Straight Through cable and connect as in screenshot given below.
   - Connect one PC with each Switch and all Switches must be connected with each other.



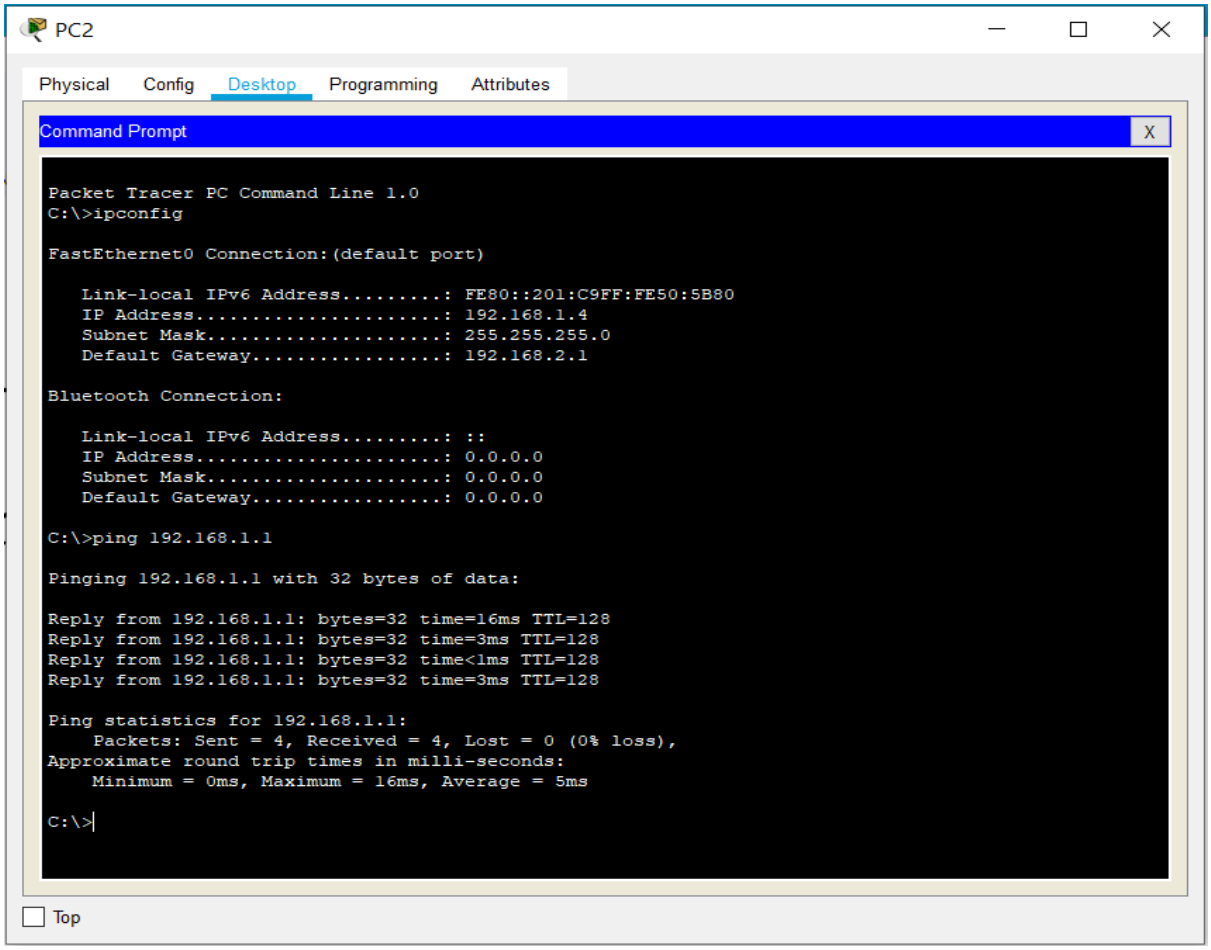
3. After completing the connection procedure, go to **Desktop → IP Configuration** and set the IP Addresses for each and every end device
   - **PC0:**
     IPv4 Address – 192.168.1.1
     Default Gateway – 192.168.2.1
   - **PC1:**
     IPv4 Address – 192.168.1.2
     Default Gateway – 192.168.2.1
   - **PC2:**
     IPv4 Address – 192.168.1.4
     Default Gateway – 192.168.2.1
   - **PC3:**
     IPv4 Address – 192.168.1.3
     Default Gateway – 192.168.2.1

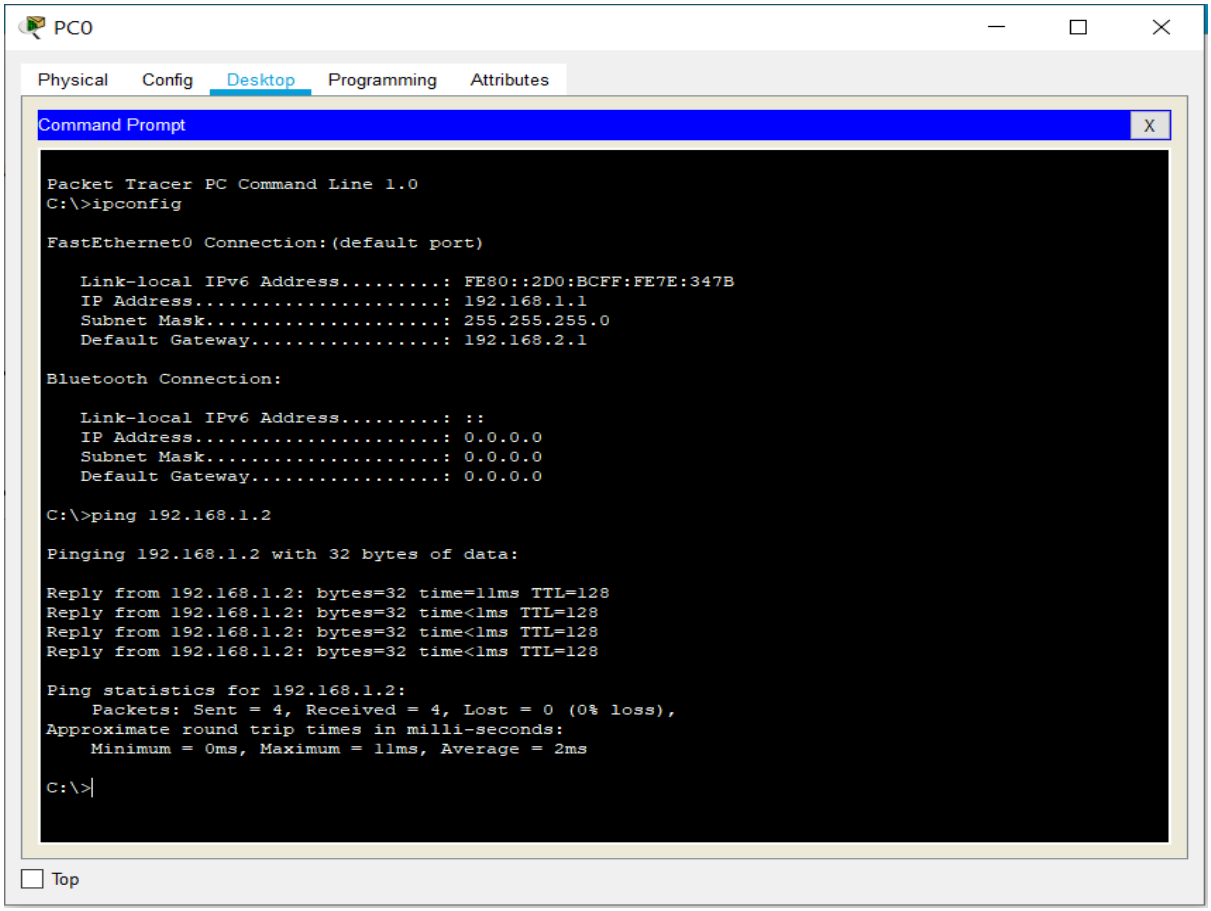

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.1.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::2D0:BCFF:FE7E:347B
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.1.4
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::201:C9FF:FE50:5B80
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

Output:

To check the connection, go to **PC → Desktop → Command Prompt** use **ipconfig and ping command** as shown in screenshot below. We can see that ping command **(ping 192.168.1.1, ping 192.168.1.2)** is executing successfully hence, implementation of mess topology using cisco packet tracer is correct.

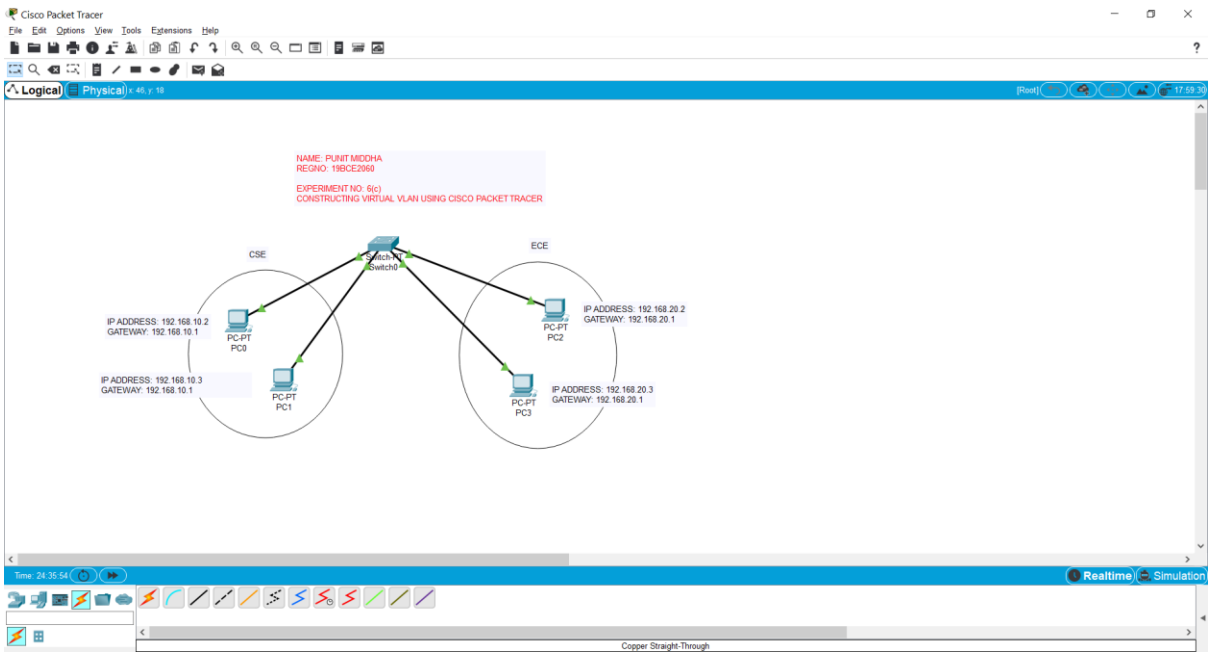




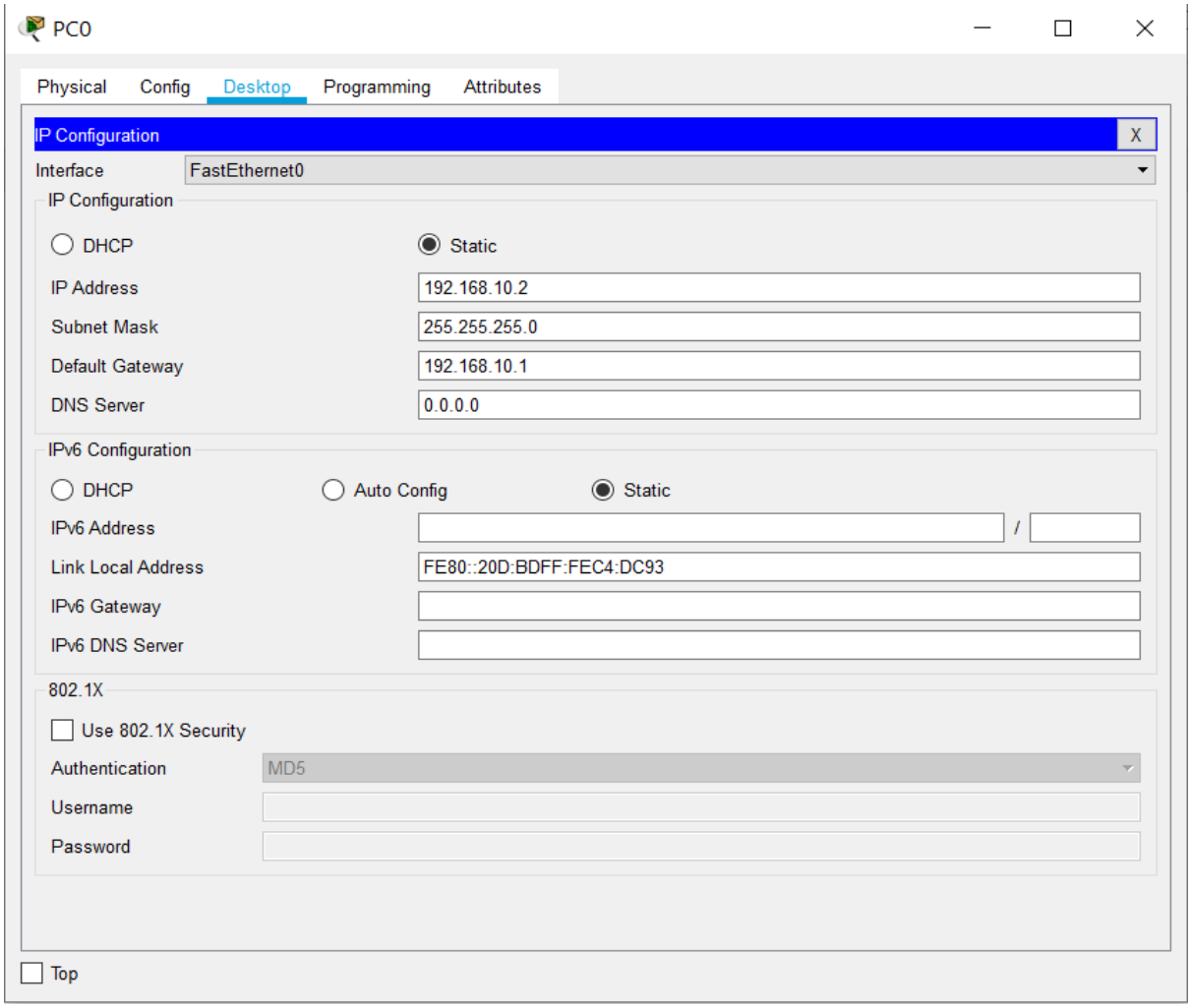
6(c). Virtual VLAN Using Cisco Packet Tracer

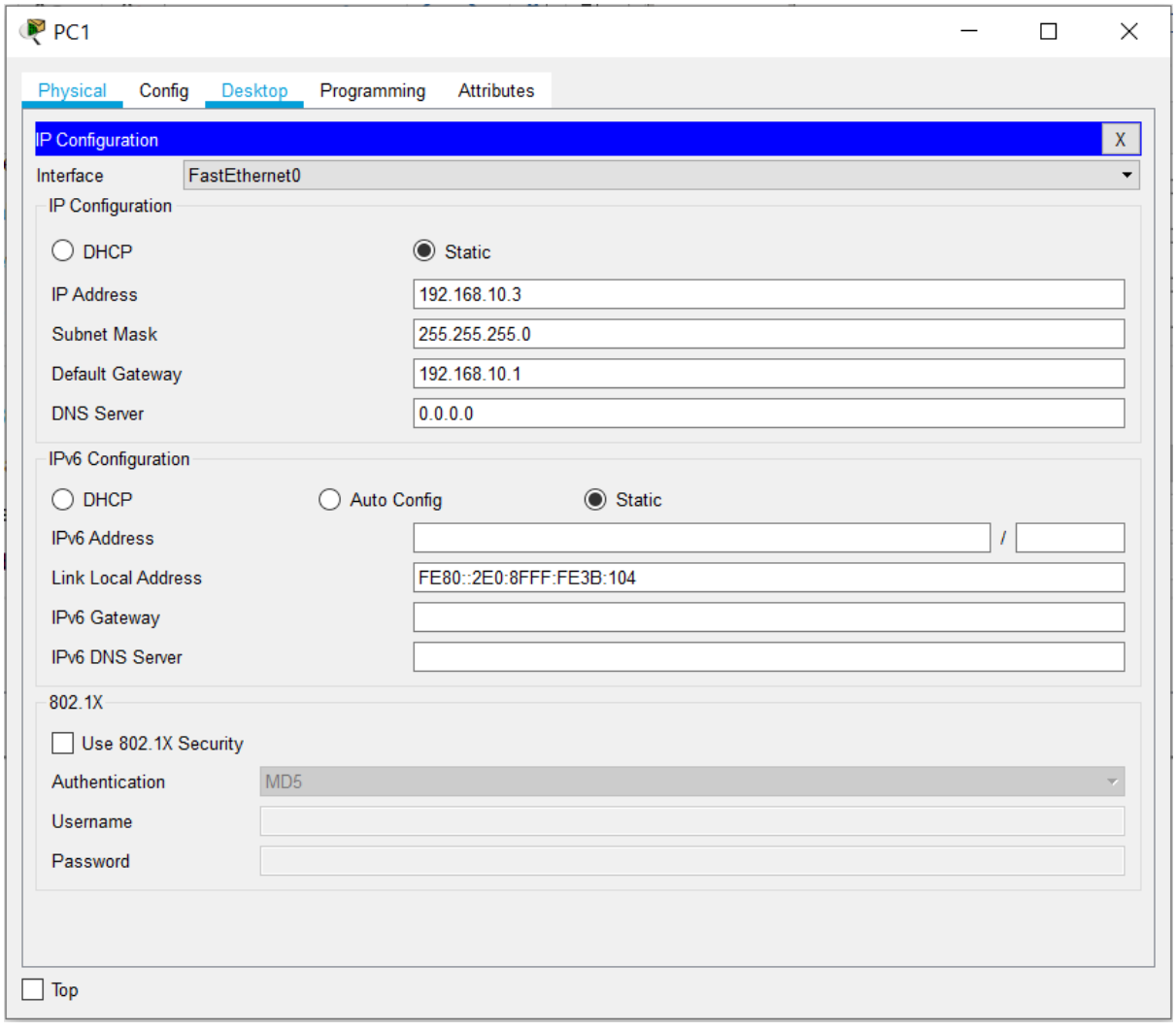
Procedure:

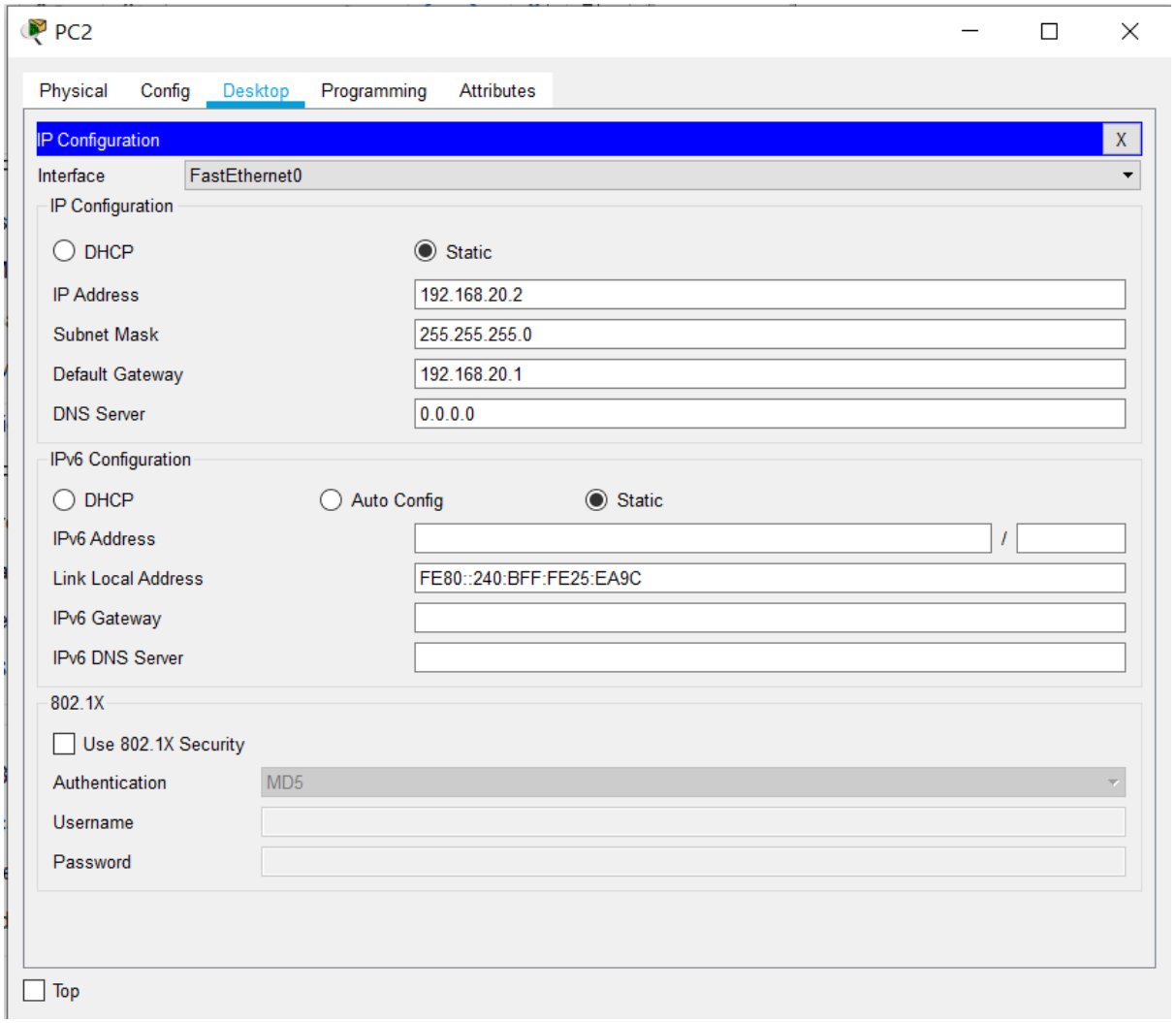
1. Go to end devices and place 1 switch and 4 PC's.
2. Now, go to connections and choose Copper-Straight Through cable and connect as in screenshot given below.
   - Connect 2 PC's i.e., PC0, PC1 in the right side (ECE) with Switch0 and 2 PC's i.e., PC2, PC3 in the left side (CSE).

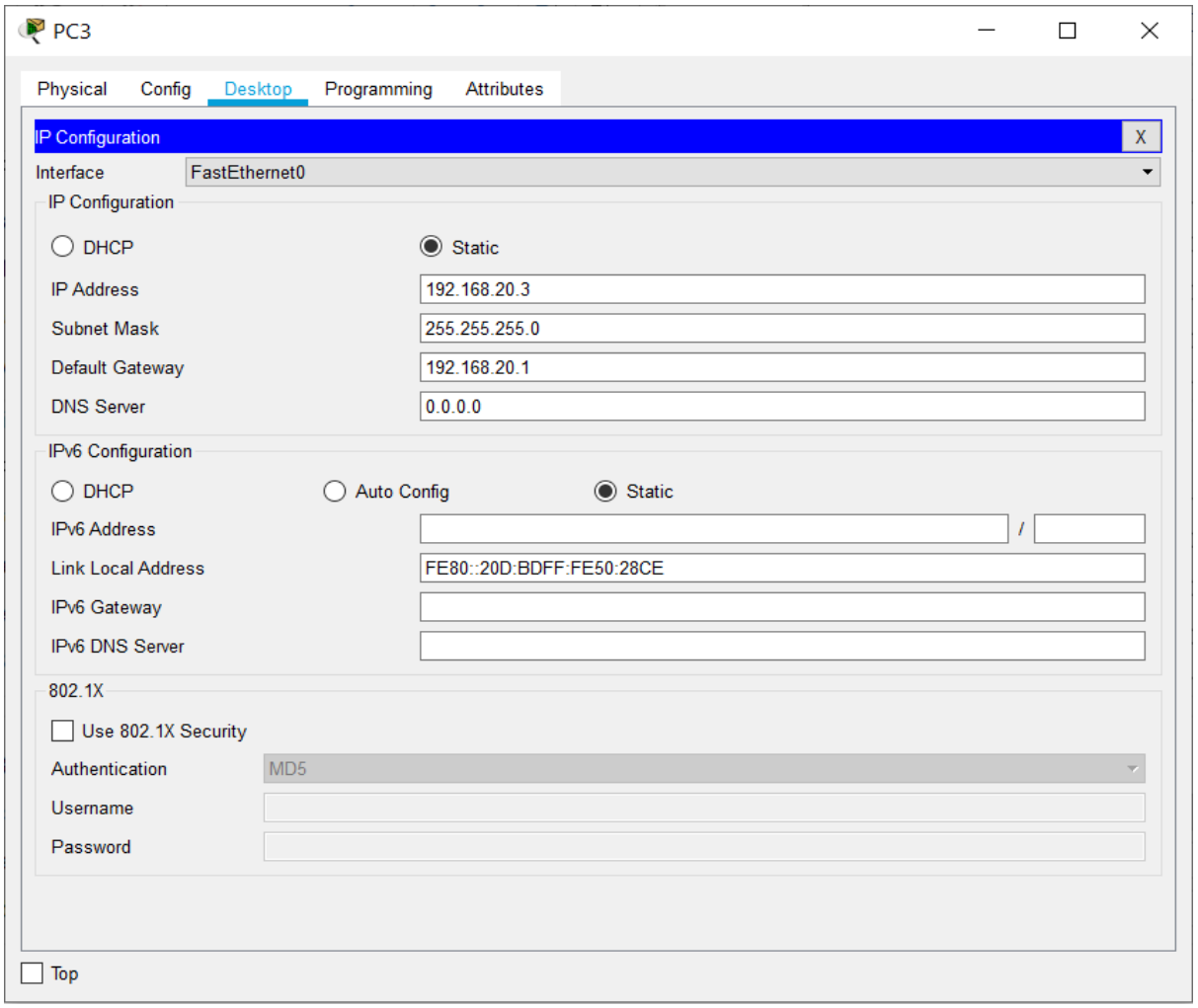


3. After completing the connection procedure, go to **Desktop → IP Configuration** and set the IP Addresses for each and every end device
   - **PC0:**
     IPv4 Address – 192.168.10.2
     Default Gateway - 192.168.10.1
   - **PC1:**
     IPv4 Address - 192.168.10.3
     Default Gateway - 192.168.10.1
   - **PC2:**
     IPv4 Address - 192.168.20.2
     Default Gateway - 192.168.20.1
   - **PC3:**
     IPv4 Address - 192.168.20.3
     Default Gateway - 192.168.20.1

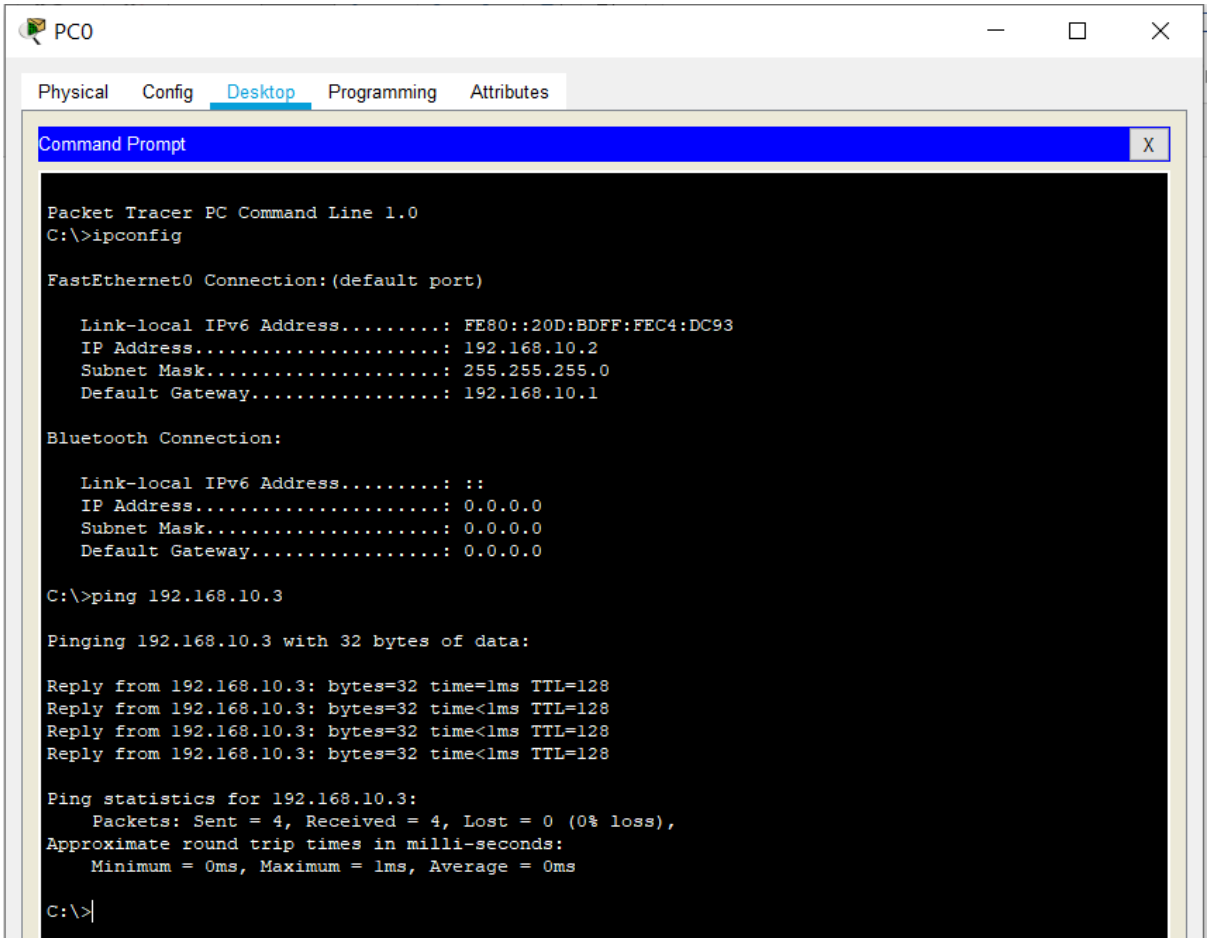

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.10.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.10.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::20D:BDFF:FEC4:DC93
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

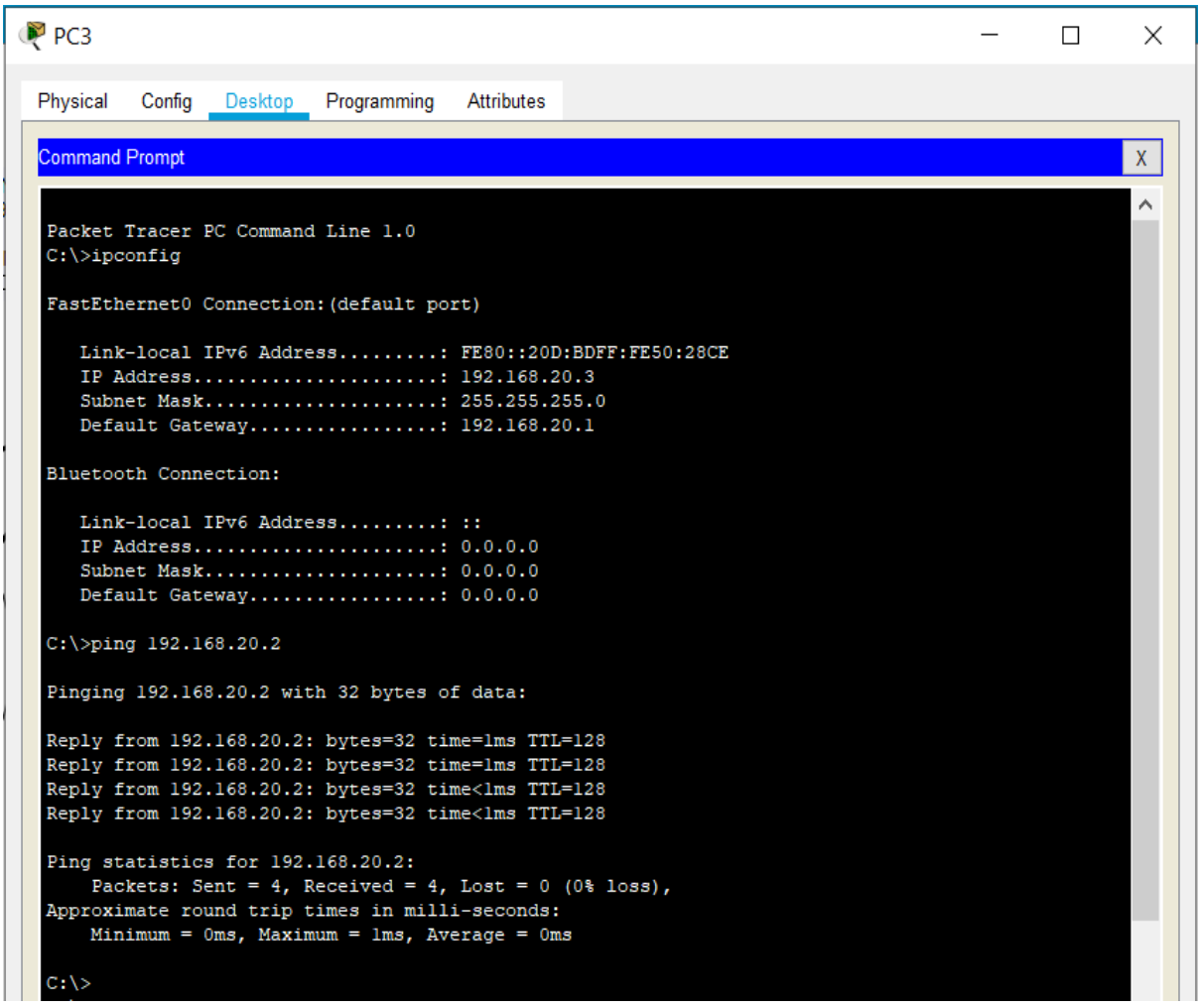

PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.10.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.10.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::2E0:8FFF:FE3B:104
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.20.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.20.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::240:BFF:FE25:EA9C
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.20.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.20.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::20D:BDFF:FE50:28CE
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

4. To check the connections, we will use **ipconfig and ping** command from one PC to another. After that we will proceed to configure the Virtual VLAN.





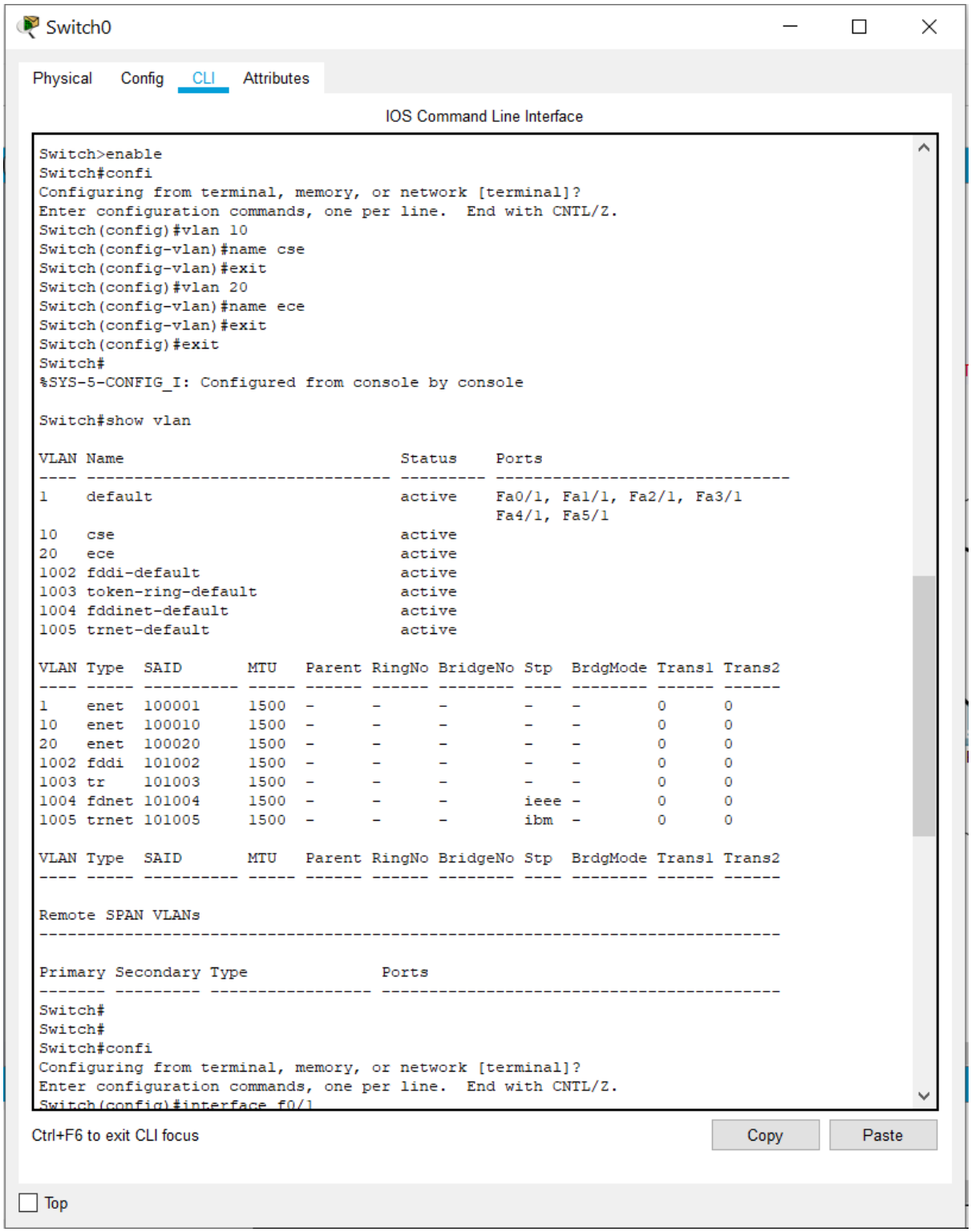
5. Now, to configure the two vlan's go to **Switch0 → CLI**. Follow the steps given below:

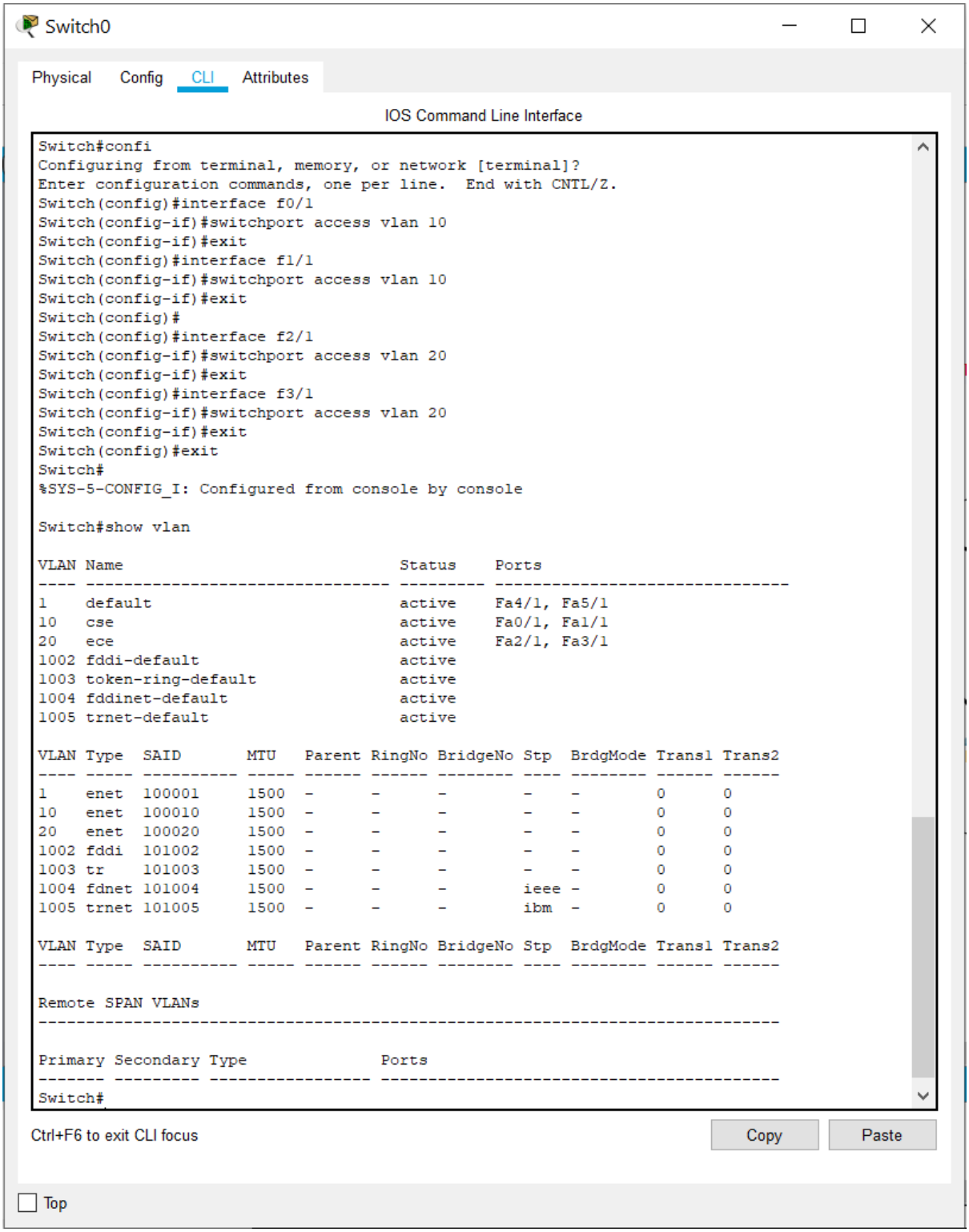
i. Use **vlan 10** to enter into vlan.
ii. Use **name cse** command for the naming of vlan repeat the steps for vlan 20
iii. After exiting, use **show vlan** command to view the available name of vlan i.e., cse, ece
iv. Now we have to assign ports according to the vlan. Use **interface f0/1 command to open interface and then use switchport access vlan 10 command to assign port for vlan 10**.
For example: Switch(config) #interface f0/1
Switch(config-if) #switchport access vlan 10
v. Exit and close the Switch0 window

```
Switch#confi
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name cse
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name ece
Switch(config-vlan)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa1/1, Fa2/1, Fa3/1
                                                Fa4/1, Fa5/1
10   cse                              active
20   ece                              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
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

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

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

```
Switch#
Switch#
Switch#confi
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface f0/1
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface f1/1
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#
Switch(config)#interface f2/1
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#interface f3/1
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa4/1, Fa5/1
10   cse                              active    Fa0/1, Fa1/1
20   ece                              active    Fa2/1, Fa3/1
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
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

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

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
Switch#
Switch#
```

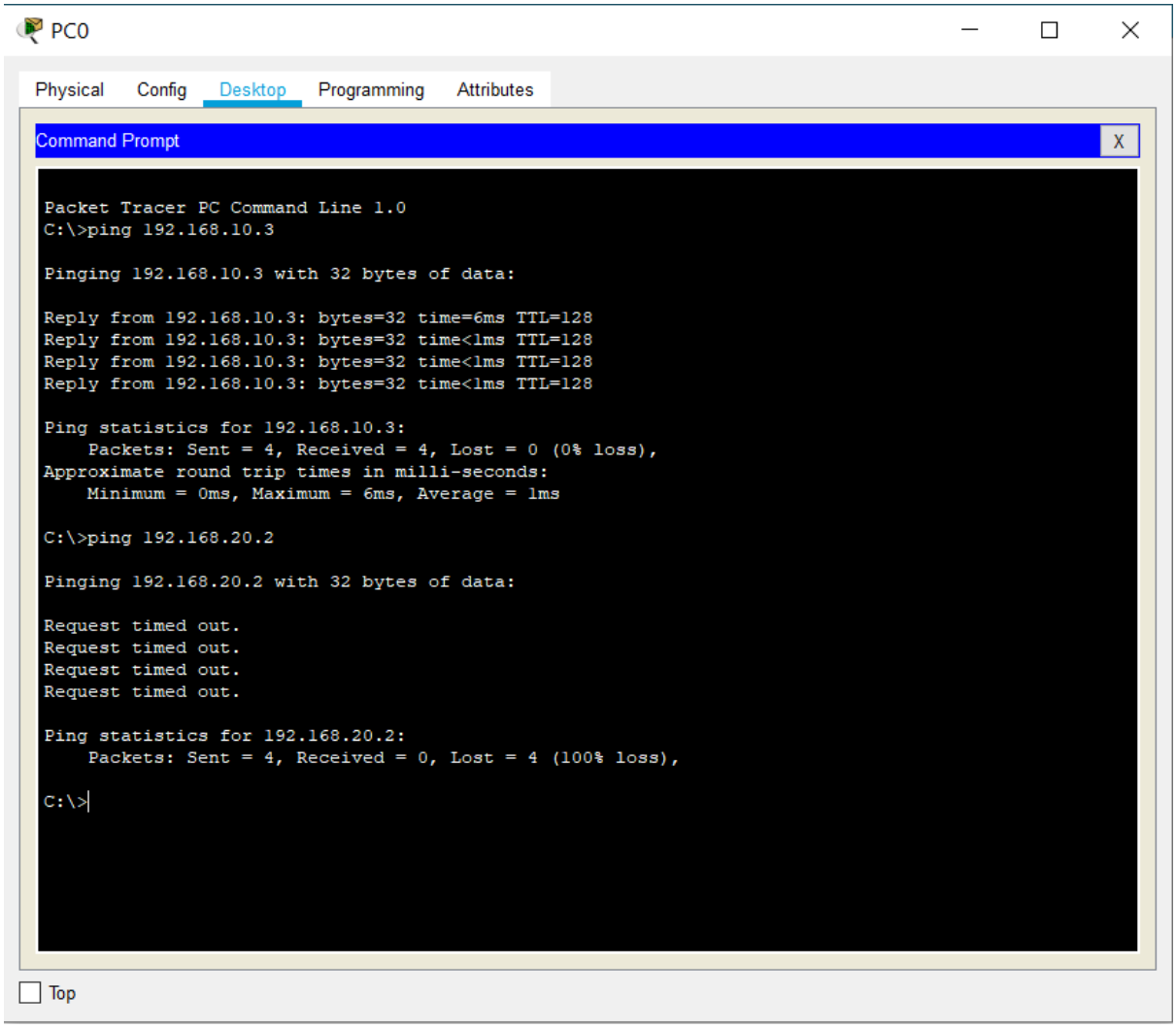
These screenshots related to CLI programming to set names and ports for specific VLAN's.

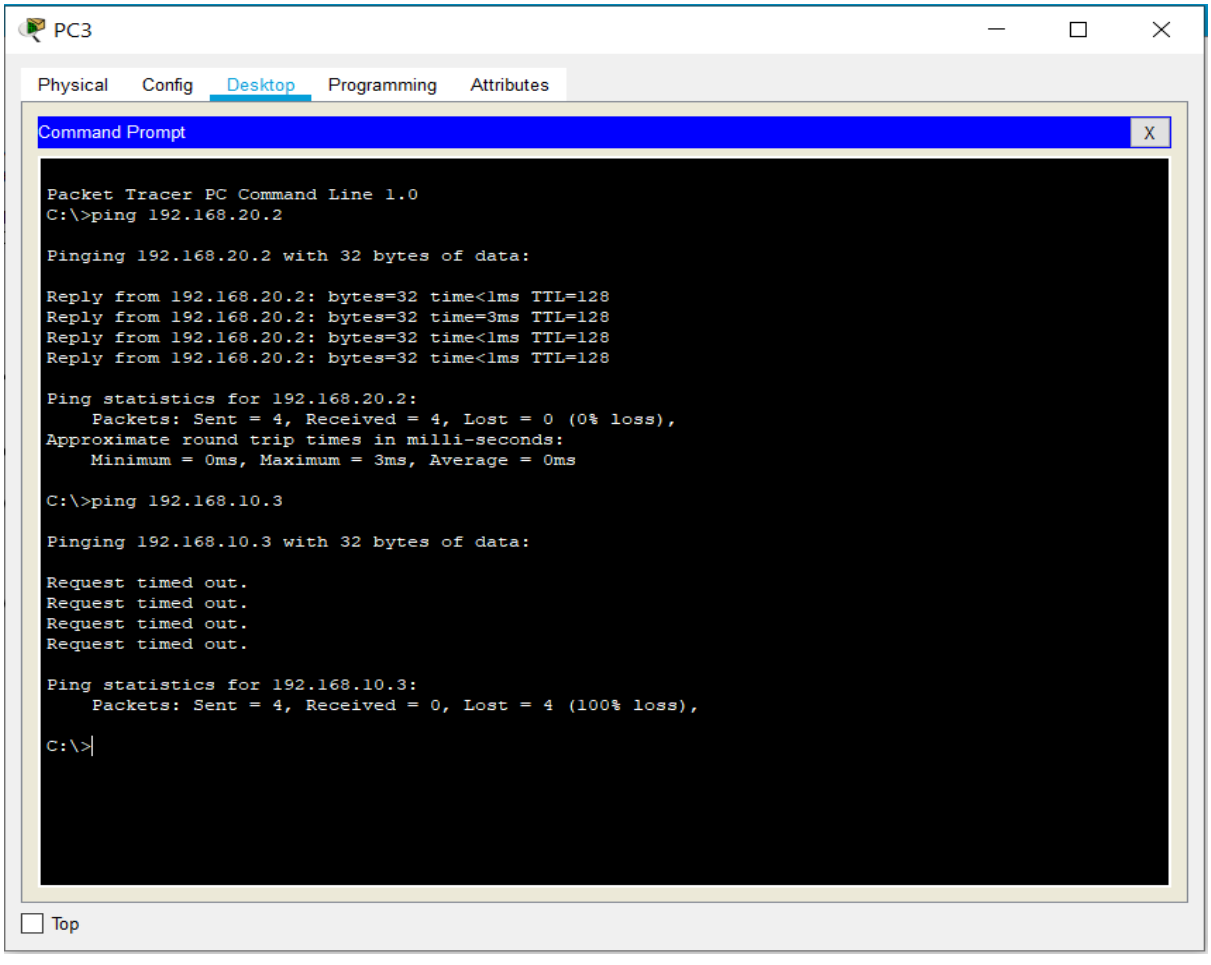




Output:

We can see that before configuring the Virtual VLAN ping command was working successfully but after configuring the Virtual VLAN, we are not able to ping from one device to another device as shown below.

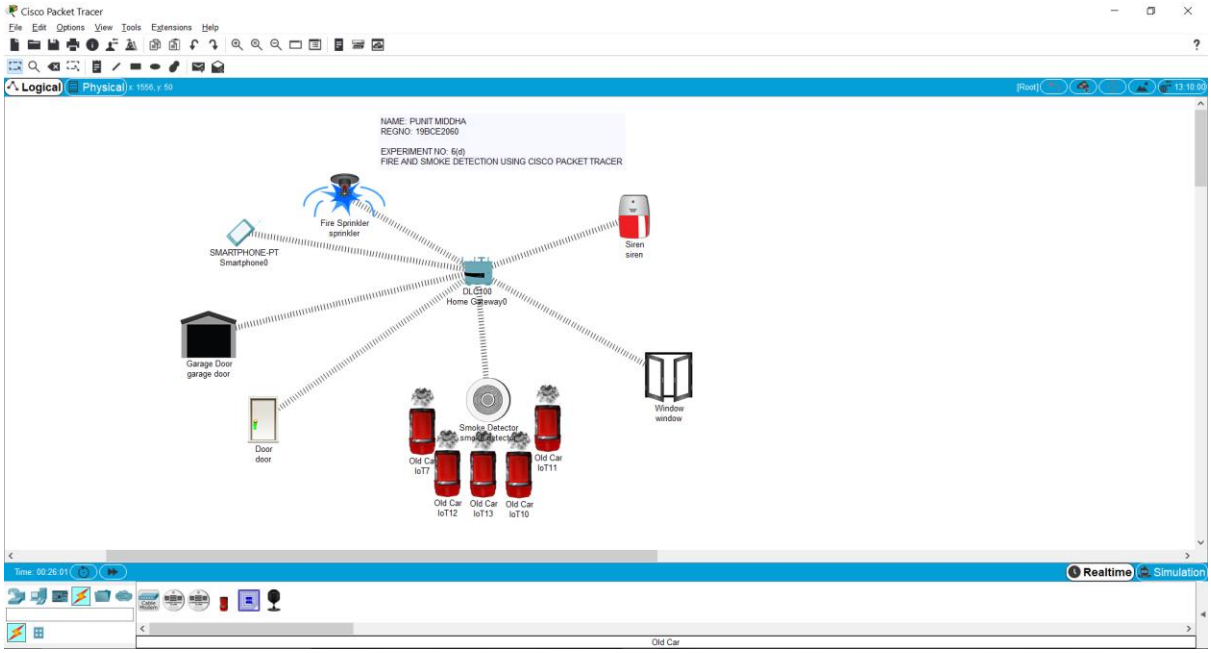

PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.3
Pinging 192.168.10.3 with 32 bytes of data:
Reply from 192.168.10.3: bytes=32 time=6ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.10.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 6ms, Average = 1ms
C:\>ping 192.168.20.2
Pinging 192.168.20.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.20.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top


PC3
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.2
Pinging 192.168.20.2 with 32 bytes of data:
Reply from 192.168.20.2: bytes=32 time<1ms TTL=128
Reply from 192.168.20.2: bytes=32 time=3ms TTL=128
Reply from 192.168.20.2: bytes=32 time<1ms TTL=128
Reply from 192.168.20.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.20.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 3ms, Average = 0ms
C:\>ping 192.168.10.3
Pinging 192.168.10.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.10.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top

6(d). Fire and Smoke Detection Using Cisco Packet Tracer

Procedure:

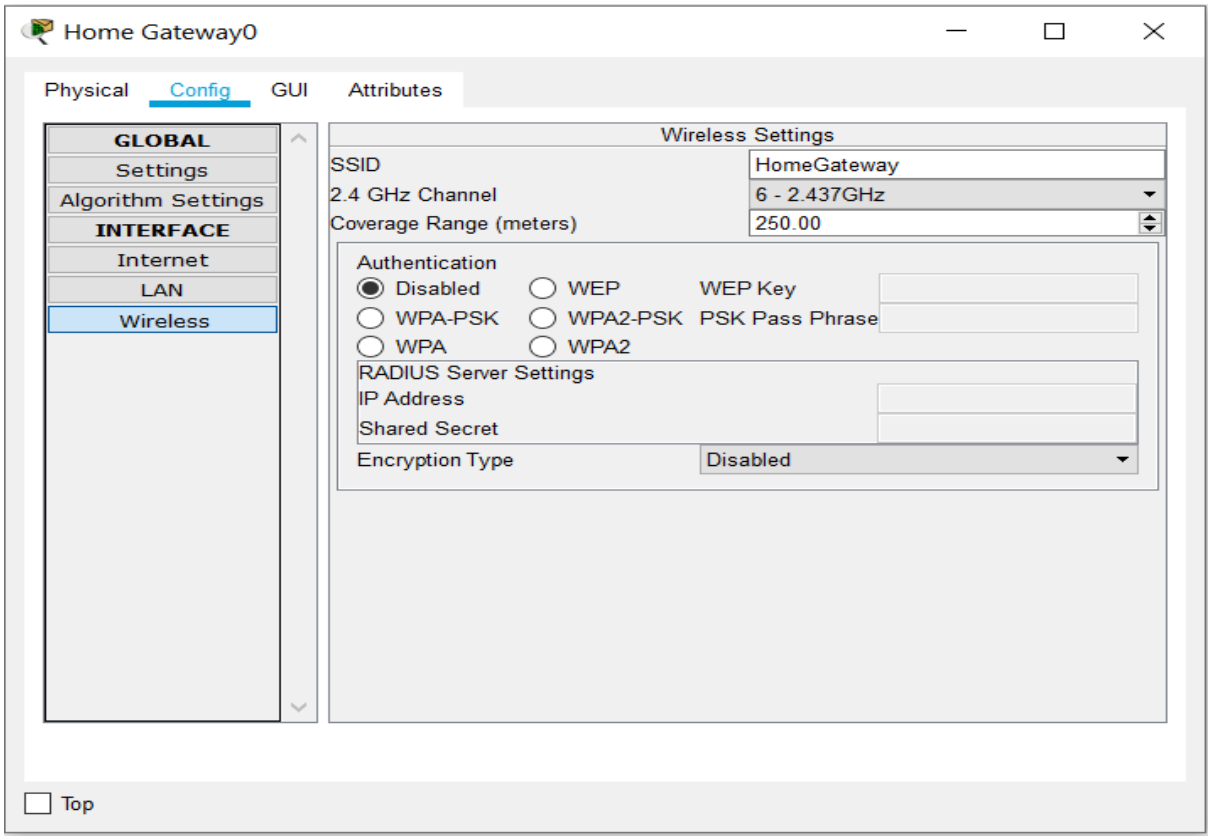
1. Go to end devices and place 1 Home Gateway, 1 Smartphone, 1 Siren, 1 Smoke Detector, 1 Fire Sprinkler, 1 Door, 1 Window, 1 Garage Door and 5 Old Cars as in screenshot given below.
2. Since, we are going to connect all the devices wirelessly with Home Gateway.



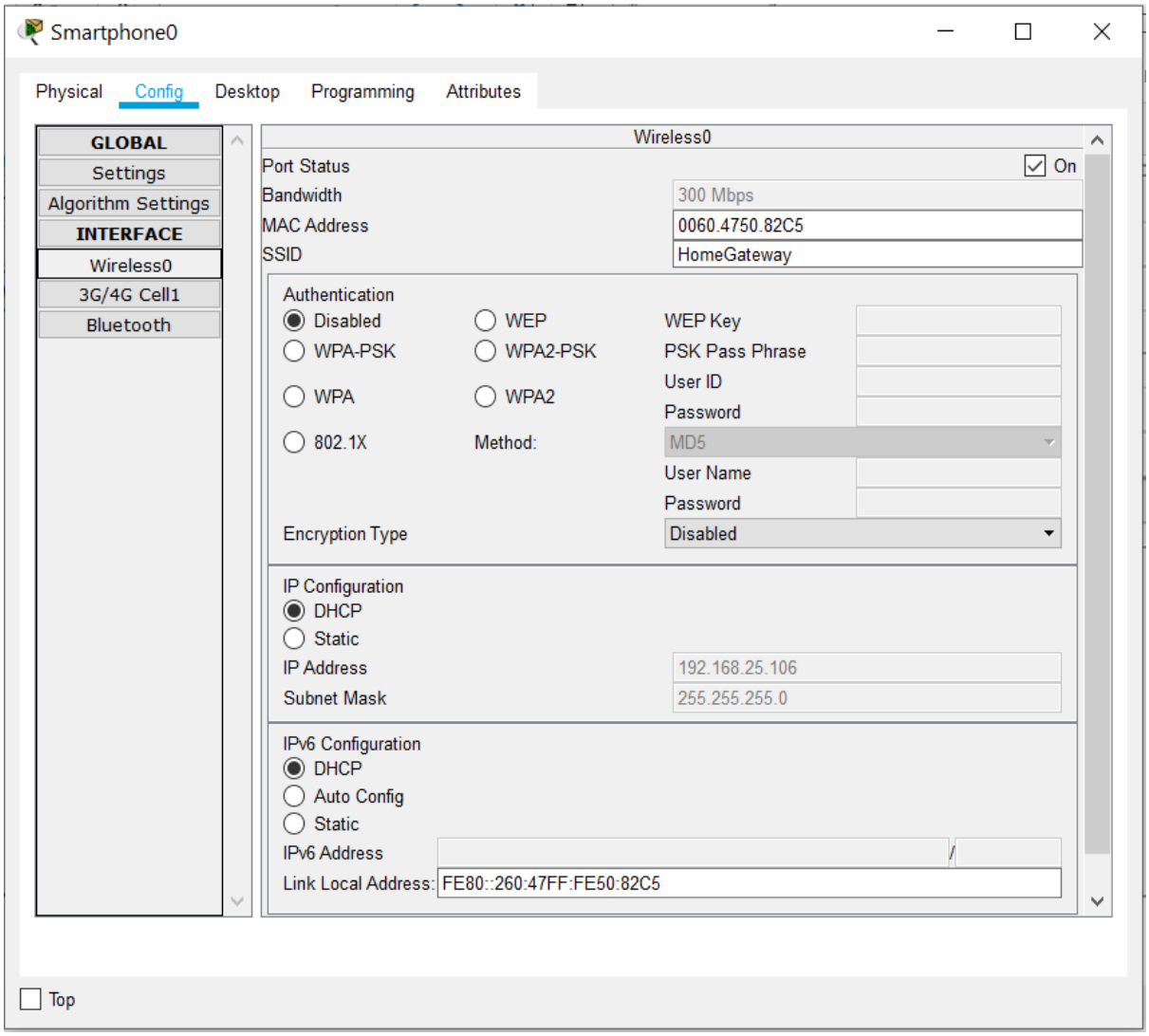
3. For the connection, go to **Home Gateway0 → Config → Wireless**. Select the following:

   SSID → HomeGateway

   Authentication → Disabled

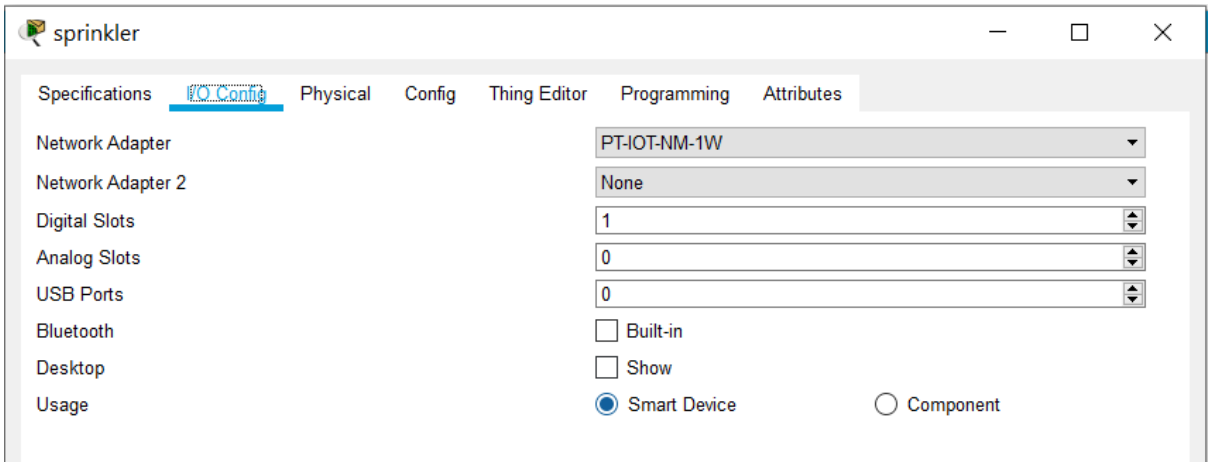


4. To connect Smartphone0 with Home Gateway0, go to **Smartphone0 → Config → Wireless0**. Set the **port status to be 'ON'** with same SSID → HomeGateway, Authentication → Disabled, IP Configuration → DHCP, IPv6 Configuration → DHCP. Now, the connection will be successfully established.

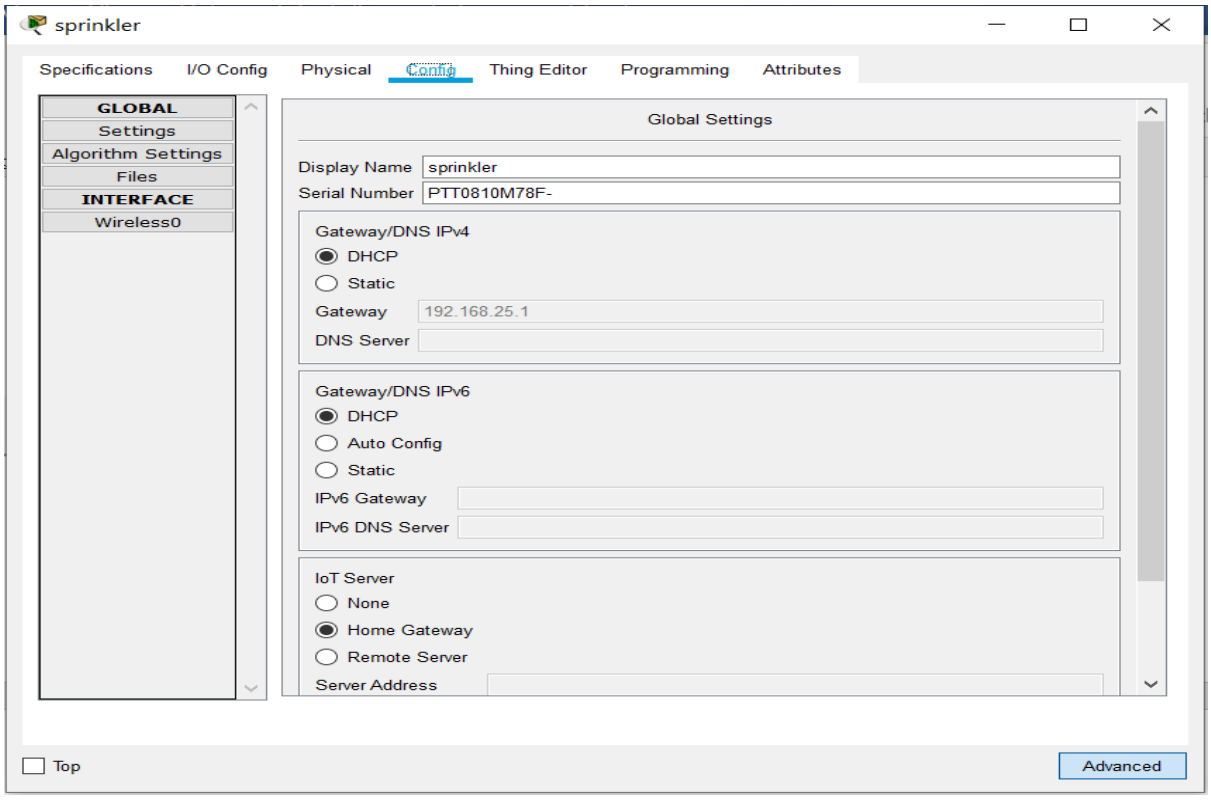


5. In next step we have to connect end devices wirelessly i.e., Sprinkler, Smoke Detector, Siren, Door, Window, Garage Door. I have shown this process for two devices (sprinkler, smoke detector).

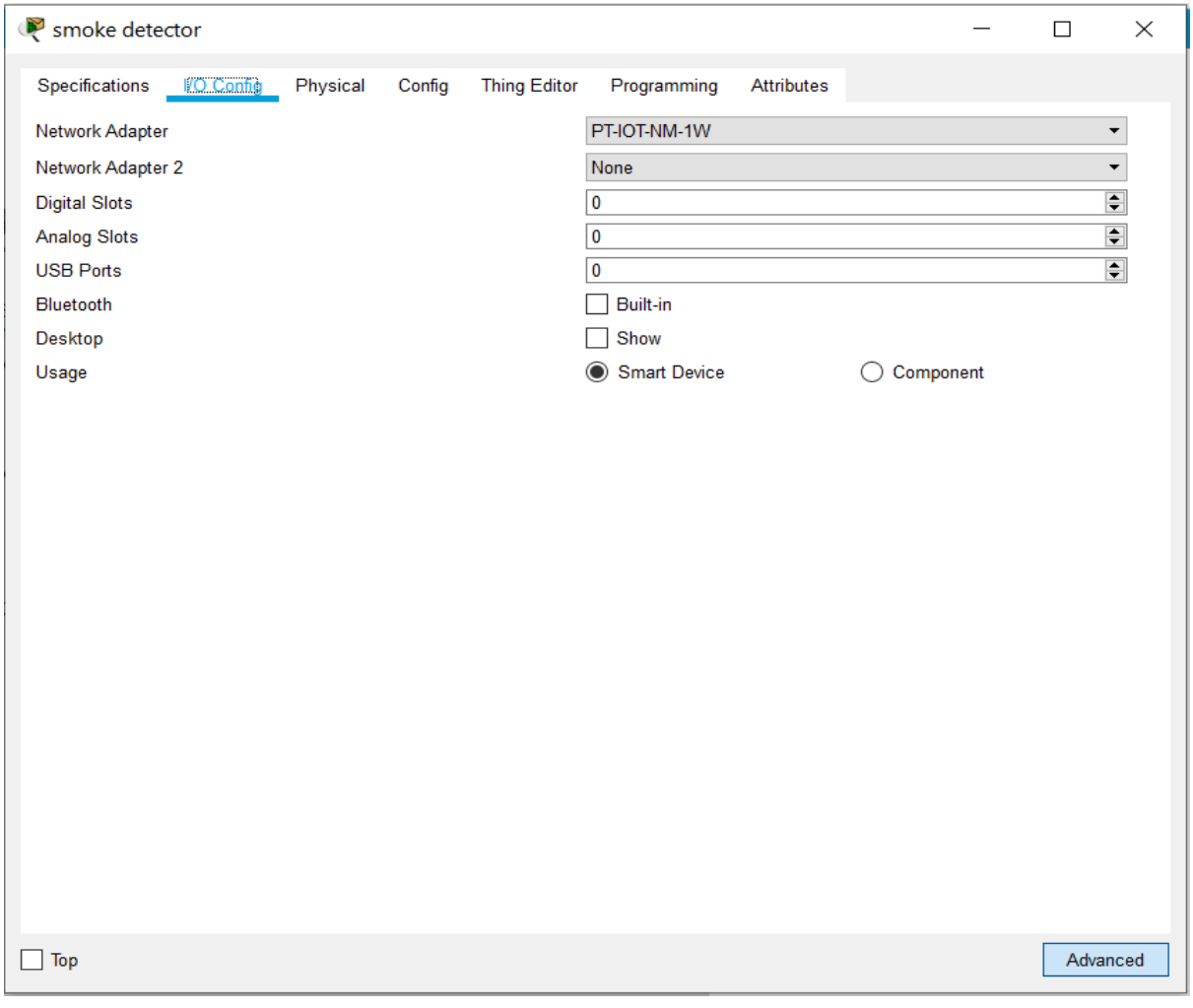
   Go to **sprinkler → advanced (button at right bottom) → I/O Config.** For the wireless connection, we have to change the **Network Adapter to PT-IOT-NM-1W**.

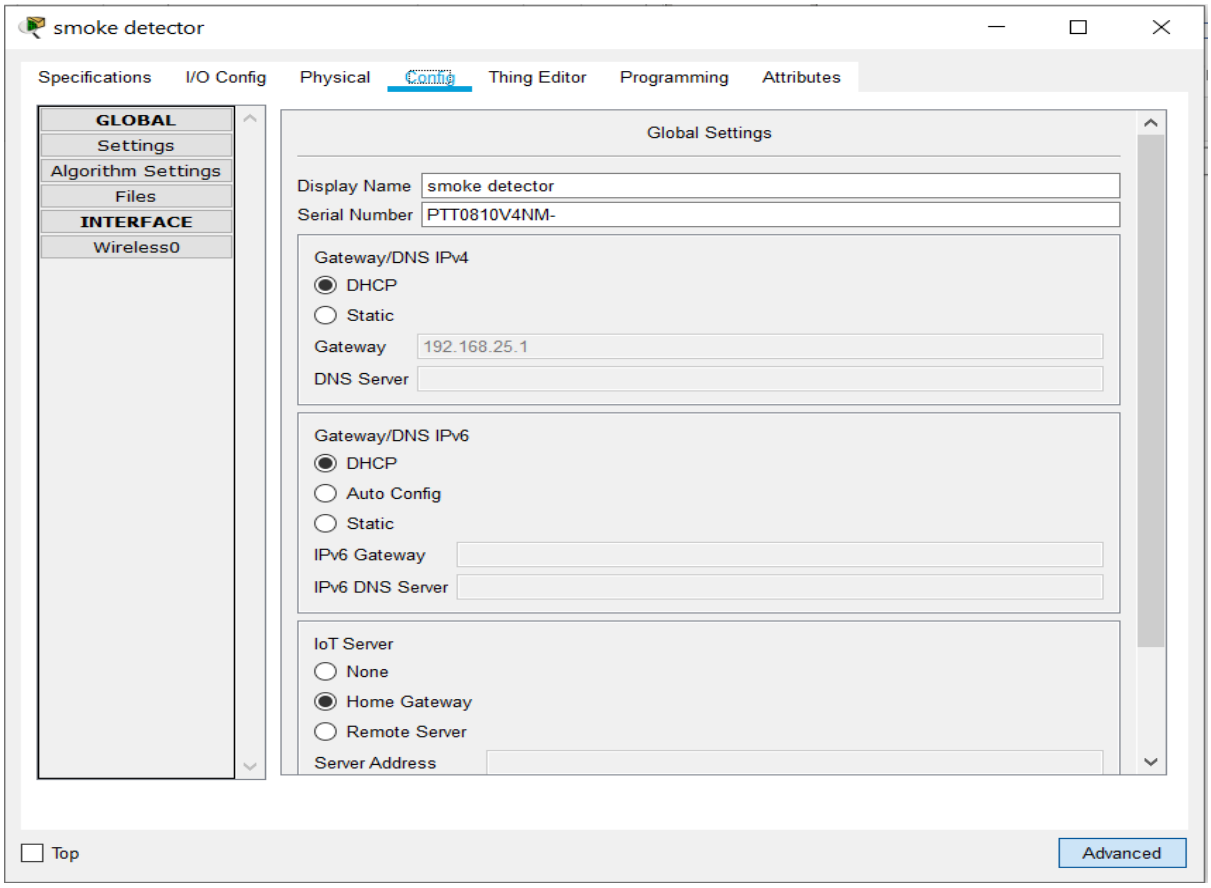


6. We have to connect all devices with Home Gateway. Go to **Sprinkler → Config**, change the Display Name, Gateway/DNS IPv4 and Gateway/DNS IPv6 to be DHCP and the IoT server to be Home Gateway. Click on '**Connect**'.

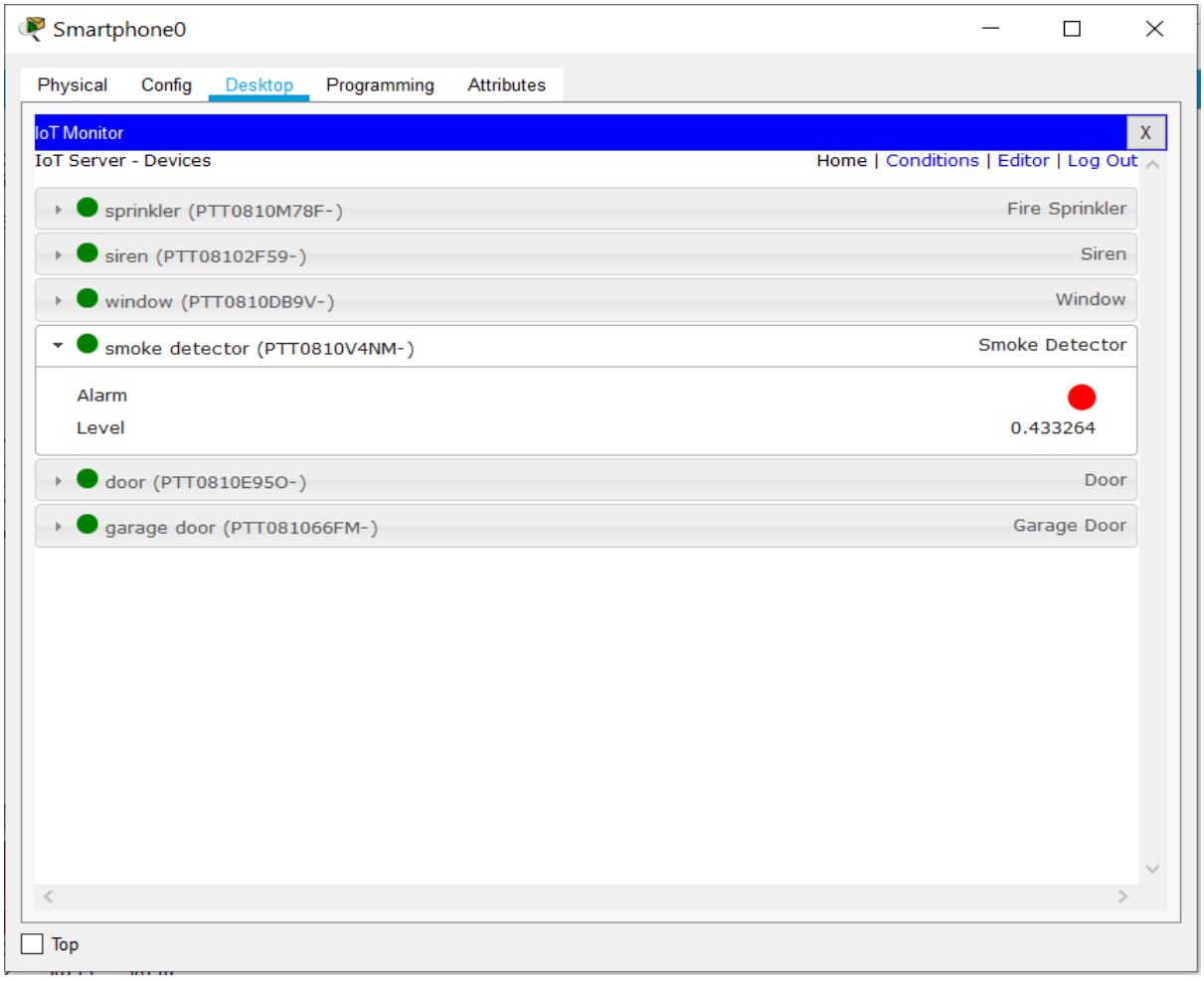


7. Repeat the step 4 and 5 for Smoke Detector and all the respective devices.





8. We have to give some conditions on which our Fire and Smoke Detector model works. For the same go to **Smartphone0 → Desktop → IoT Monitor**, in IoT Monitor go to Conditions given in top Right of given window.



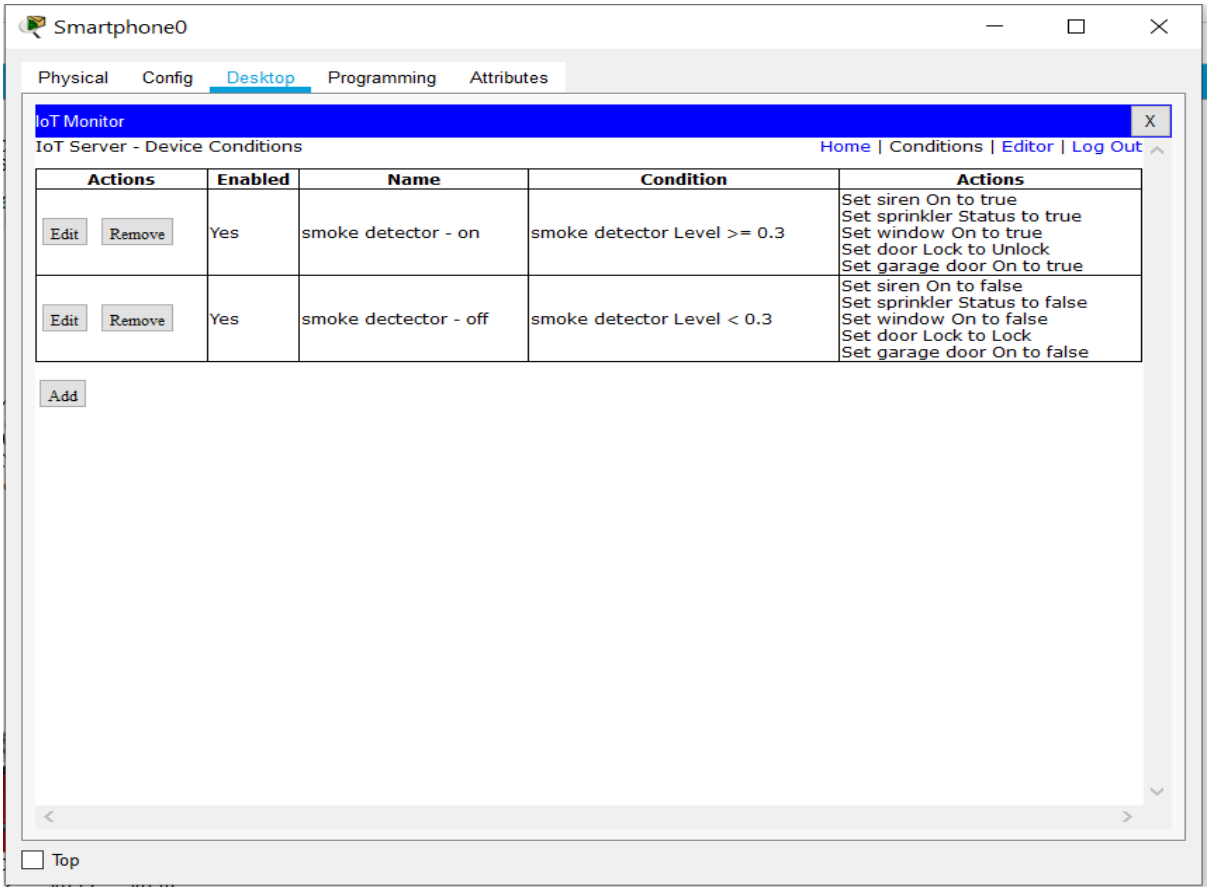
9. Now, click on ‘Add’ to add some conditions. Give the name (**smoke detector - on**) for your **condition1**, in ’if’ block select Smoke Detector and level to be greater than or equals to 0.3 (**smoke detector Level >= 0.3**) then set the actions for another devices as follow:
    - Set siren On to true
    - Set sprinkler Status to true
    - Set window On to true
    - Set door Lock to Unlock
    - Set garage door On to true

Click “OK” to save Condition.

Give the name (**smoke detector - off**) for your **condition2**, in ’if’ block select Smoke Detector and level to be less than 0.3 (**smoke detector Level < 0.3**) then set the actions for another devices as follow:

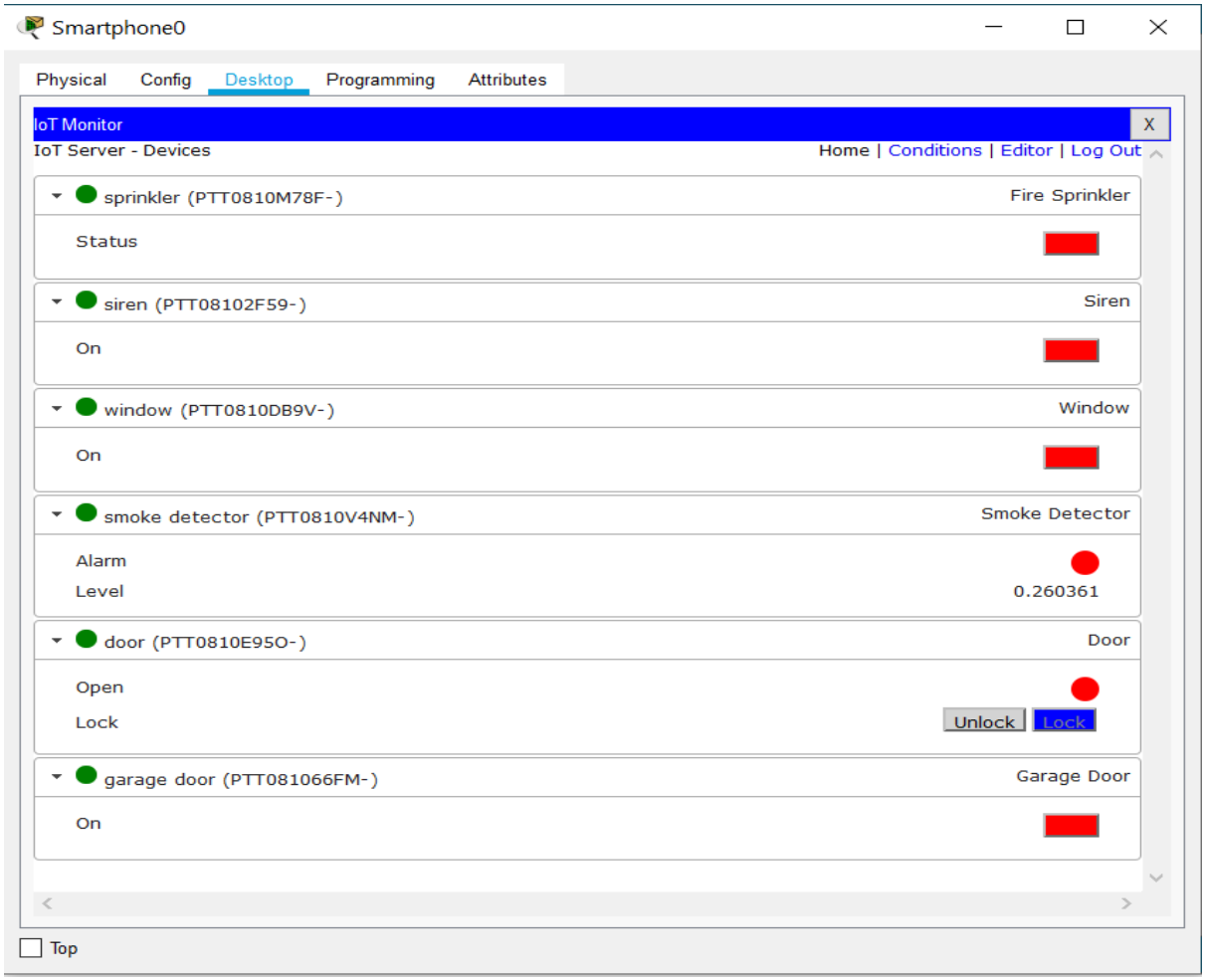
- Set siren On to false
- Set sprinkler Status to false
- Set window On to false
- Set door Lock to Lock
- Set garage door On to false

Click “OK” to save Condition.

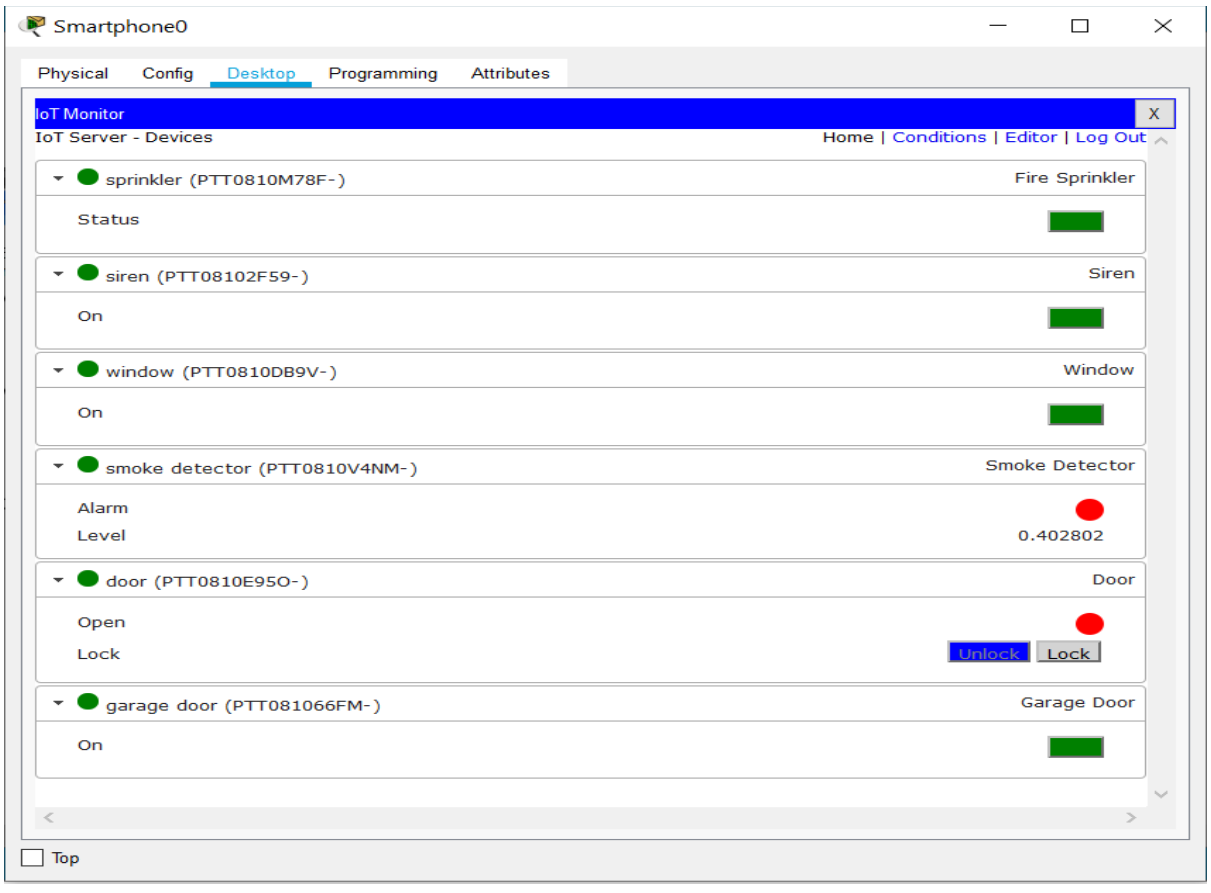


Output:

In output screenshot 1, We can see that whenever the level of Smoke Detector level is less than 0.3 (**smoke detector Level < 0.3**) then condition2 came to an action i.e., siren on to false, sprinkler Status to false, window on to false, door Lock to Lock, garage door on to false



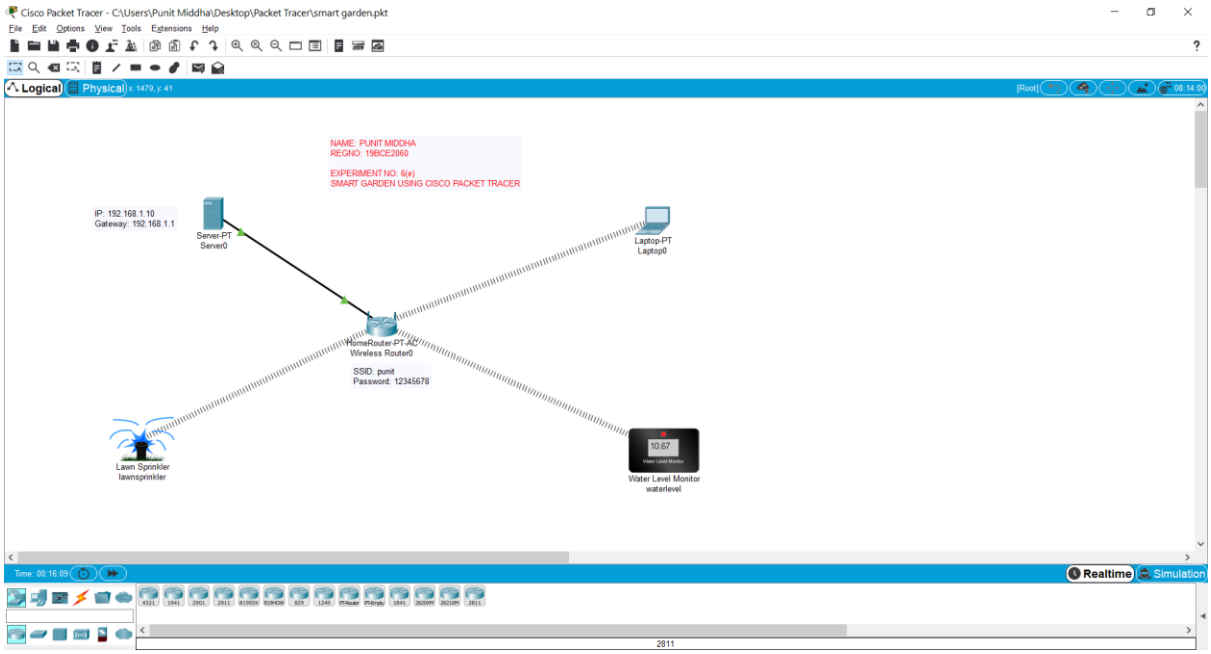
In output screenshot 2, We can see that whenever the level of Smoke Detector level is greater than or equals to 0.3 (**smoke detector Level >= 0.3**) then condition1 came to an action i.e., siren on to true, sprinkler Status to true, window on to true, door Lock to Unlock, garage door on to true.



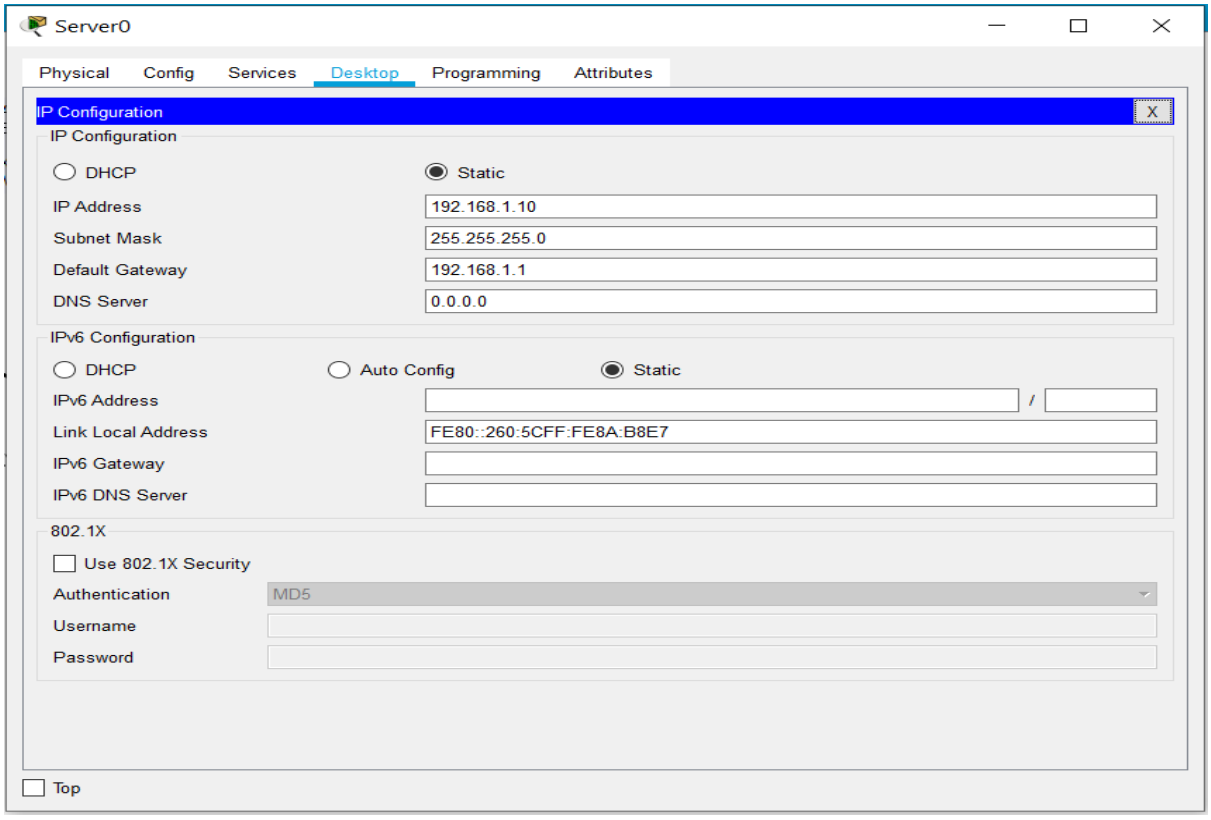
6(e). Smart Garden Using Cisco Packet Tracer

Procedure:

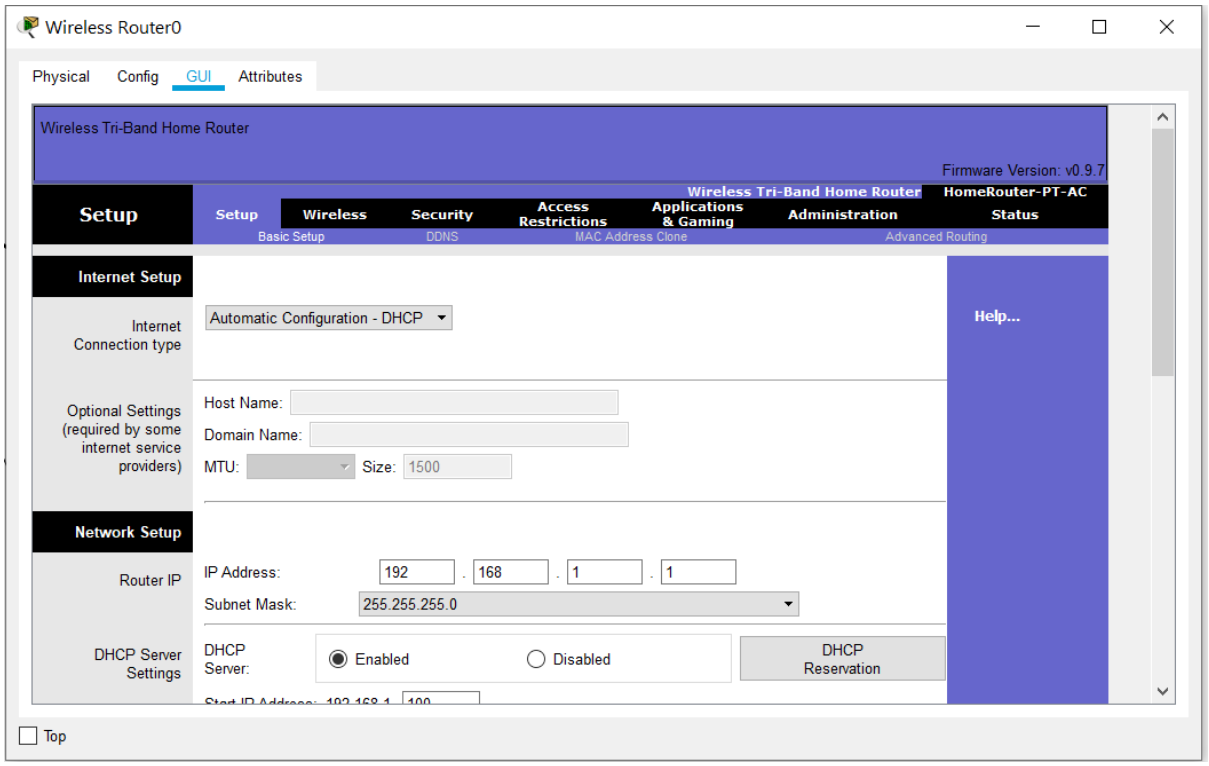
1. Go to end devices and place 1 Wireless Router, 1 server, 1 Water Level Monitor, 1 Lawn Sprinkler and 1 Laptop.
2. Now, go to connections and choose Copper-Straight Through cable and connect as in screenshot given below.
   - Connect Server0 with Wireless Router.



3. After completing the connection procedure, go to **Desktop → IP Configuration** and set the IP Addresses for each and every end device
   - **Server0:**
     IPv4 Address – 192.168.1.10
     Default Gateway – 192.168.1.1



4. Now, we have to configure the Wireless Router0. Go to **Wireless Router0 → GUI → Setup → Network Setup**, in IP Router set the IP Address same as **Default Gateway (192.168.1.1)** of Server0 and save the settings.

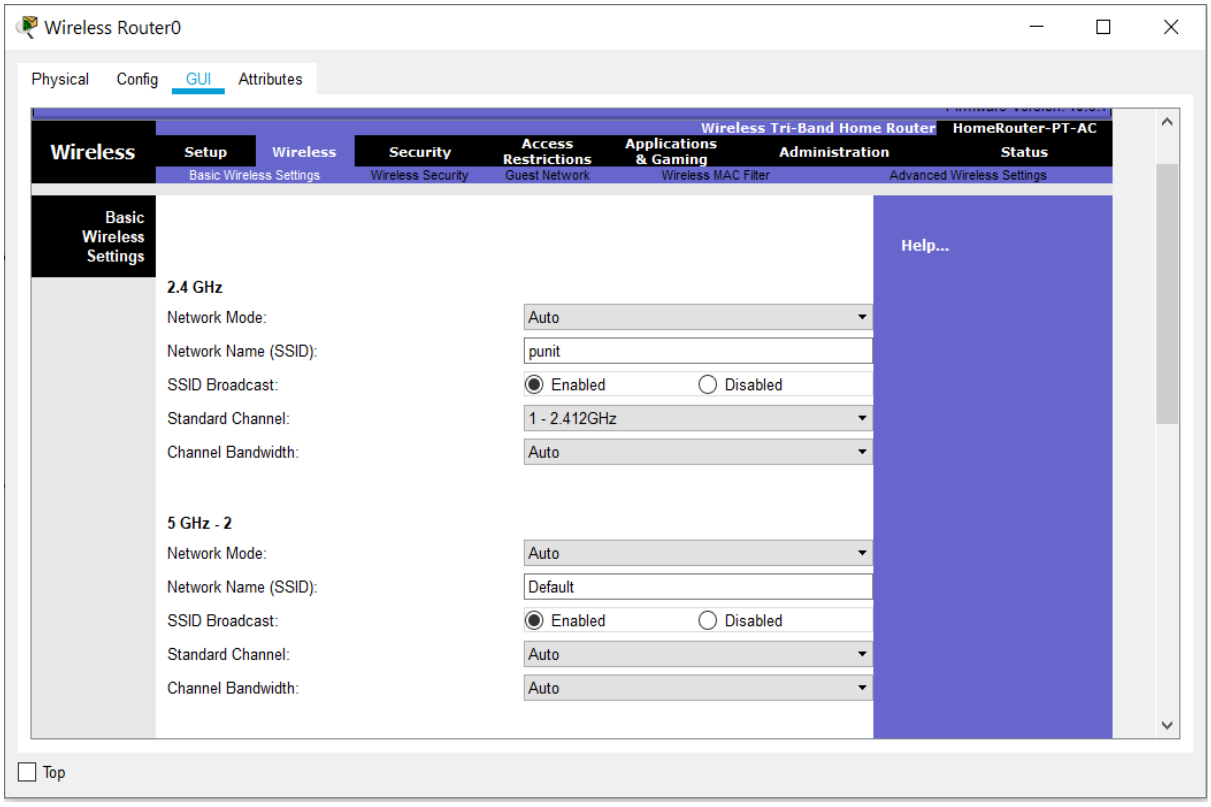


5. Go to **Wireless Router0 → GUI → Wireless → Basic Wireless Settings**, set the following:

   Network Name (SSID) → punit

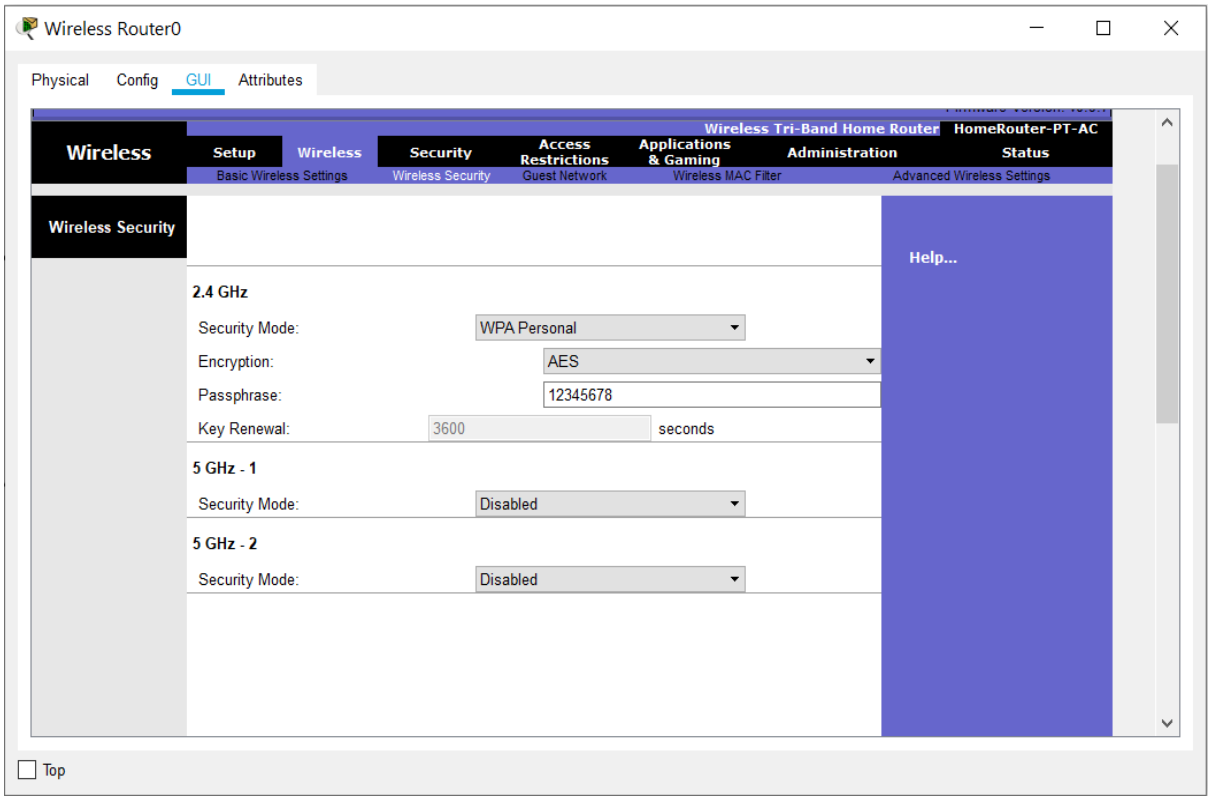
   SSID Broadcast → Enabled

   Save the Settings.

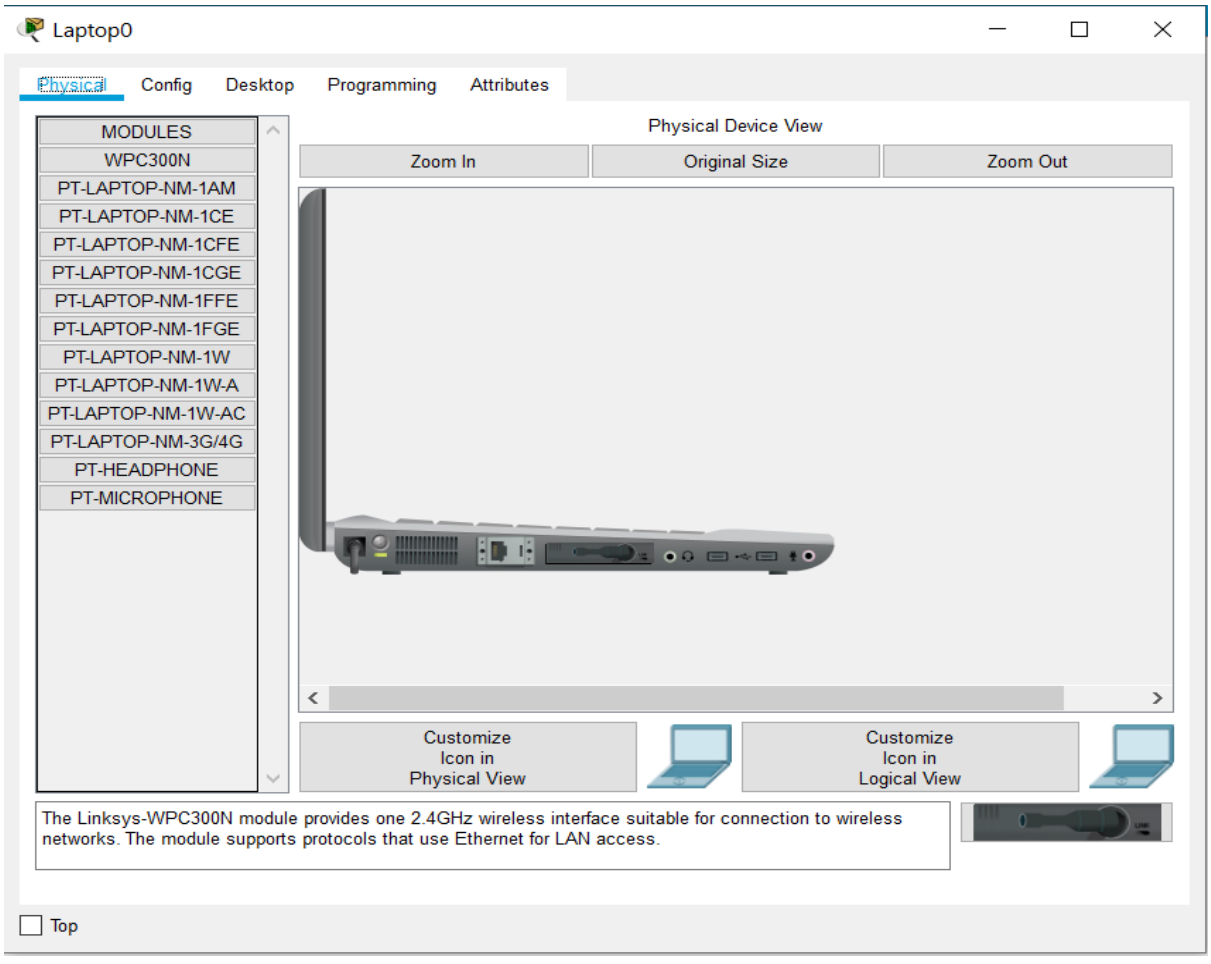


6. Go to **Wireless Router0 → GUI → Wireless → Wireless Security**, set the following:

Security Mode → WPA Personal, Encryption → AES, Passphrase → 12345678



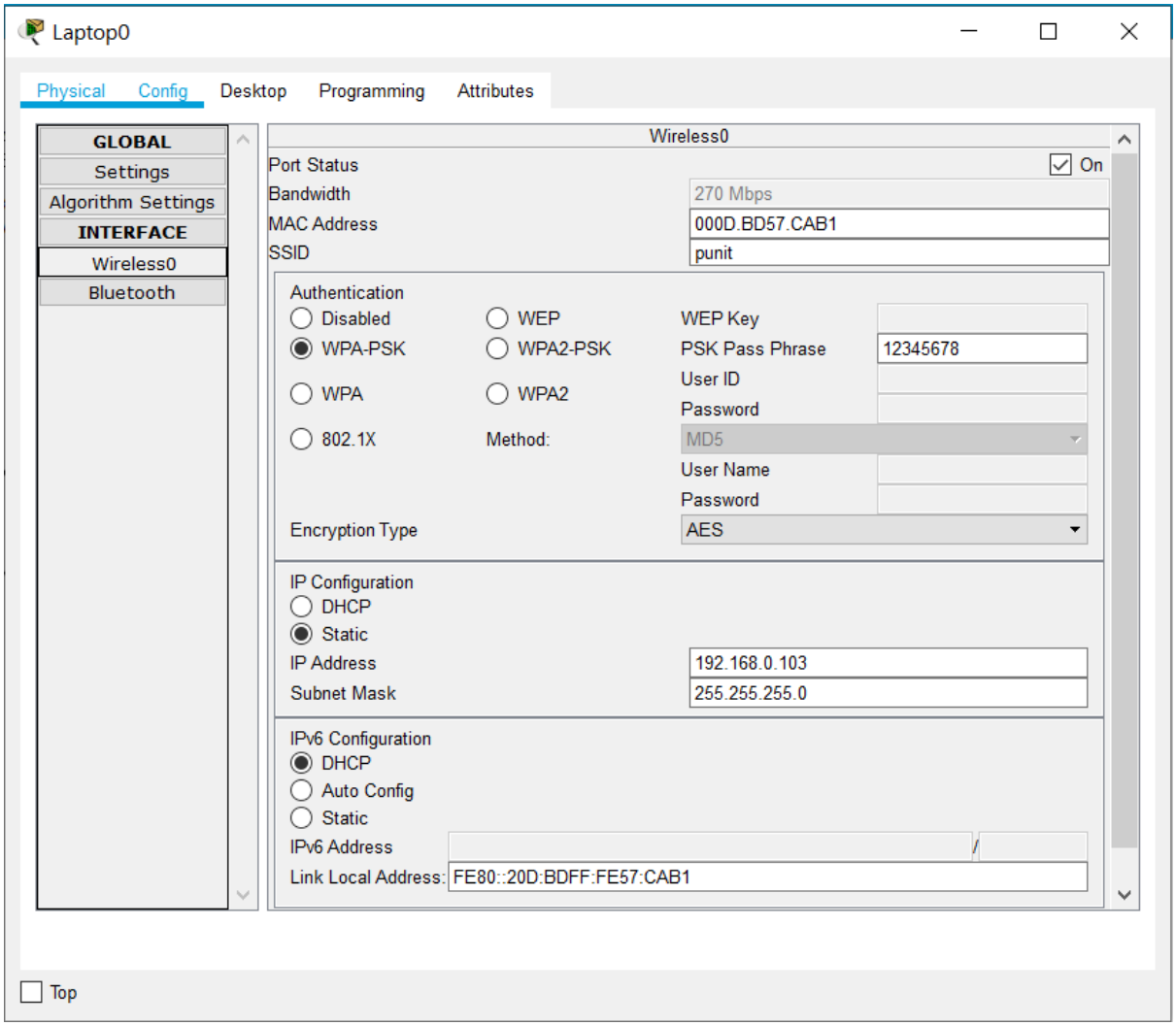
7. After the configuration of Wireless Router1, we have to connect Laptop0 wirelessly. For the same go to **Laptop0 → Physical**, turn off the Laptop0 and drag drop the Ethernet port and put the wireless port. Turn On the Laptop0 again.



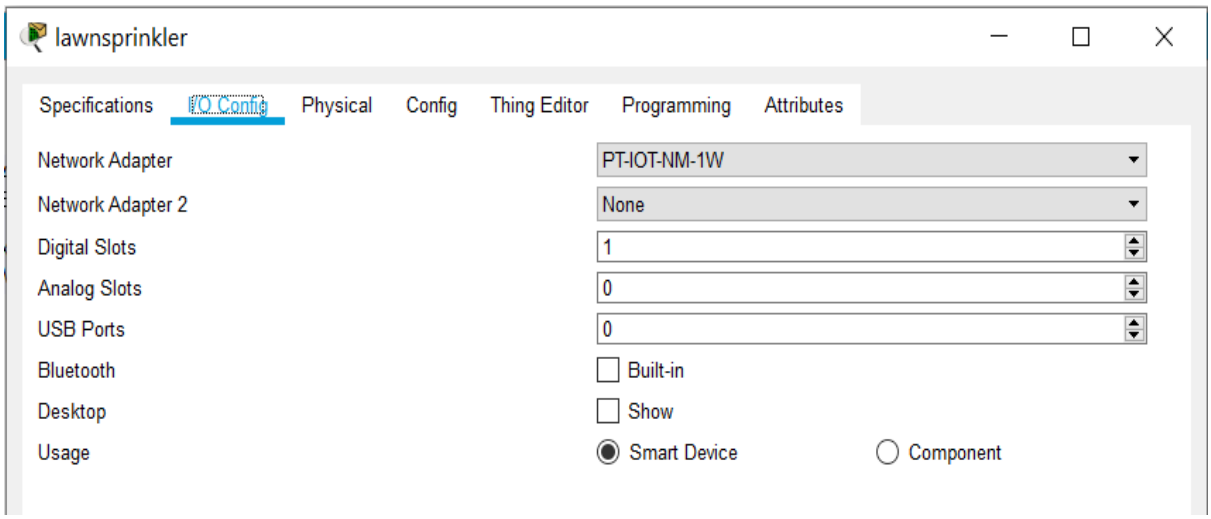
8. After successfully connecting the wireless port, go to **Laptop0 → Config → Interface → Wireless0**. Set the following settings given in **STEP 5, 6**:

   Port Status → 'ON', SSID → punit, Authentication → WPA-PSK,
   PSK Pass Phrase → 12345678, Encryption Type → AES

Laptop0 will now successfully connected

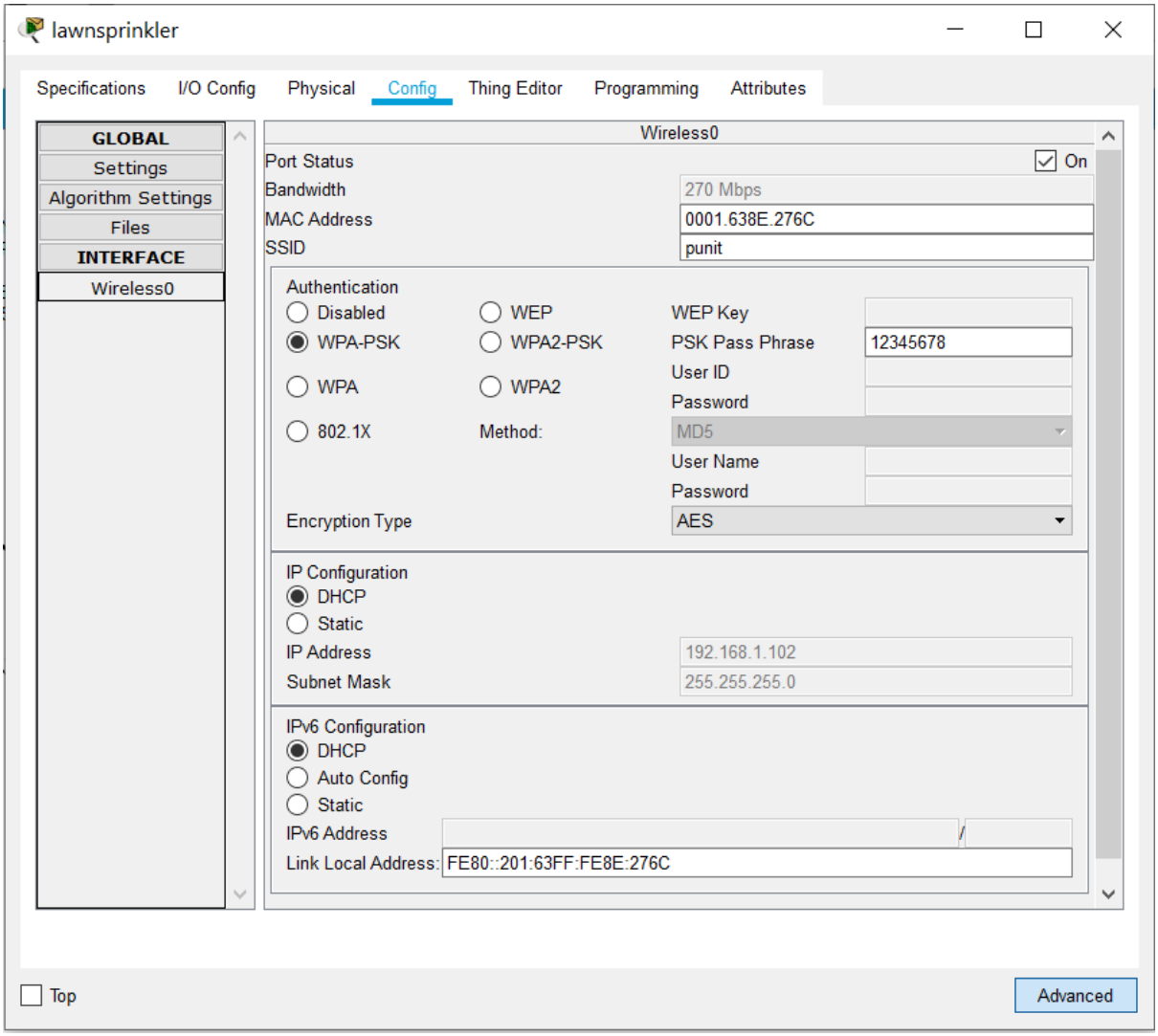


9. Go to **Lawnsprinkler → Advanced → I/O Config**, Select the **Network Adapter as PT-IOT-NM-1W**

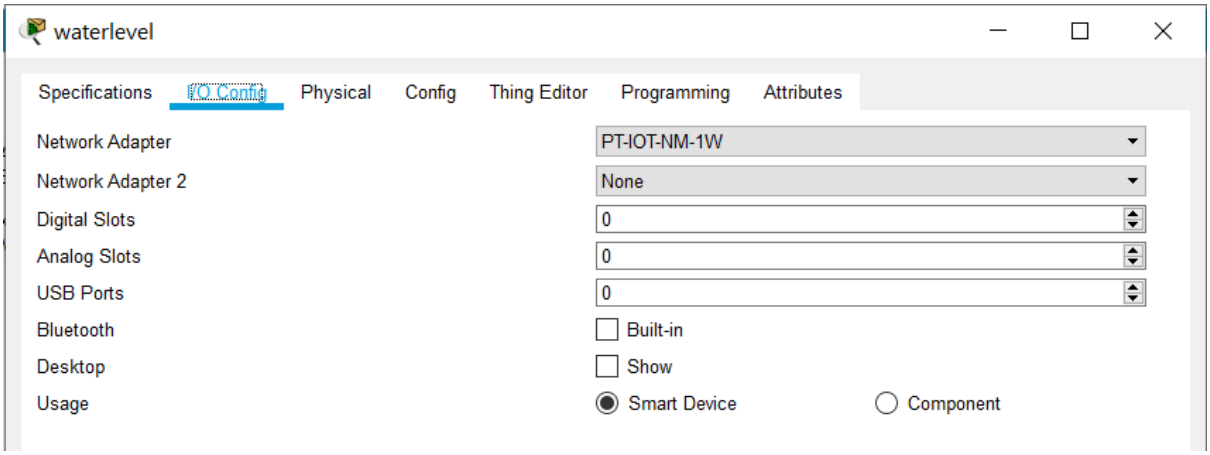


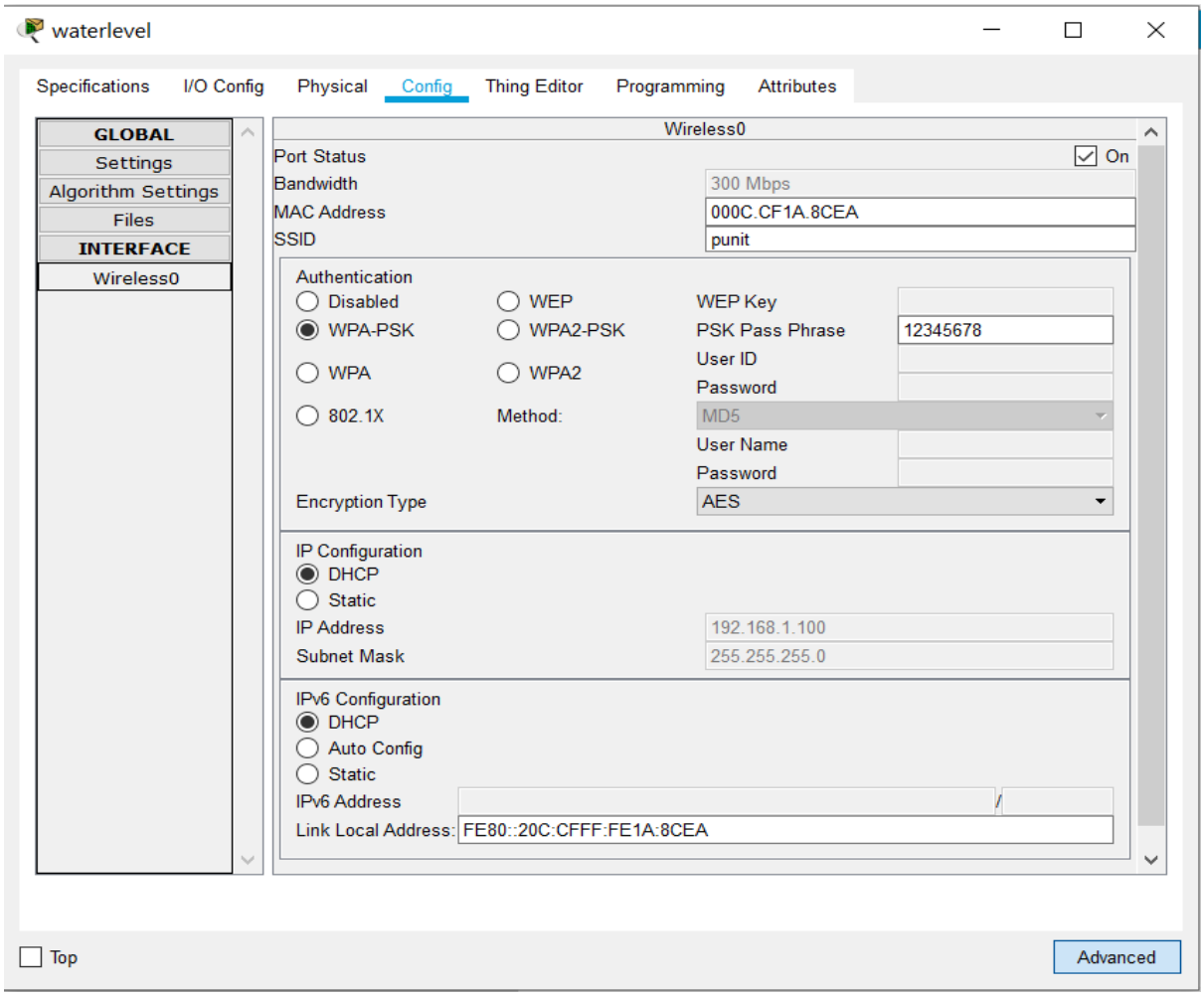
10. Again, to connect Lawnsprinkler wirelessly go to **Lawnsprinkler → Config → Interface → Wireless0**. Set the following settings given in **STEP 5, 6**:
Port Status → 'ON', SSID → punit, Authentication → WPA-PSK,
PSK Pass Phrase → 12345678, Encryption Type → AES

Lawnsprinkler will now successfully connected

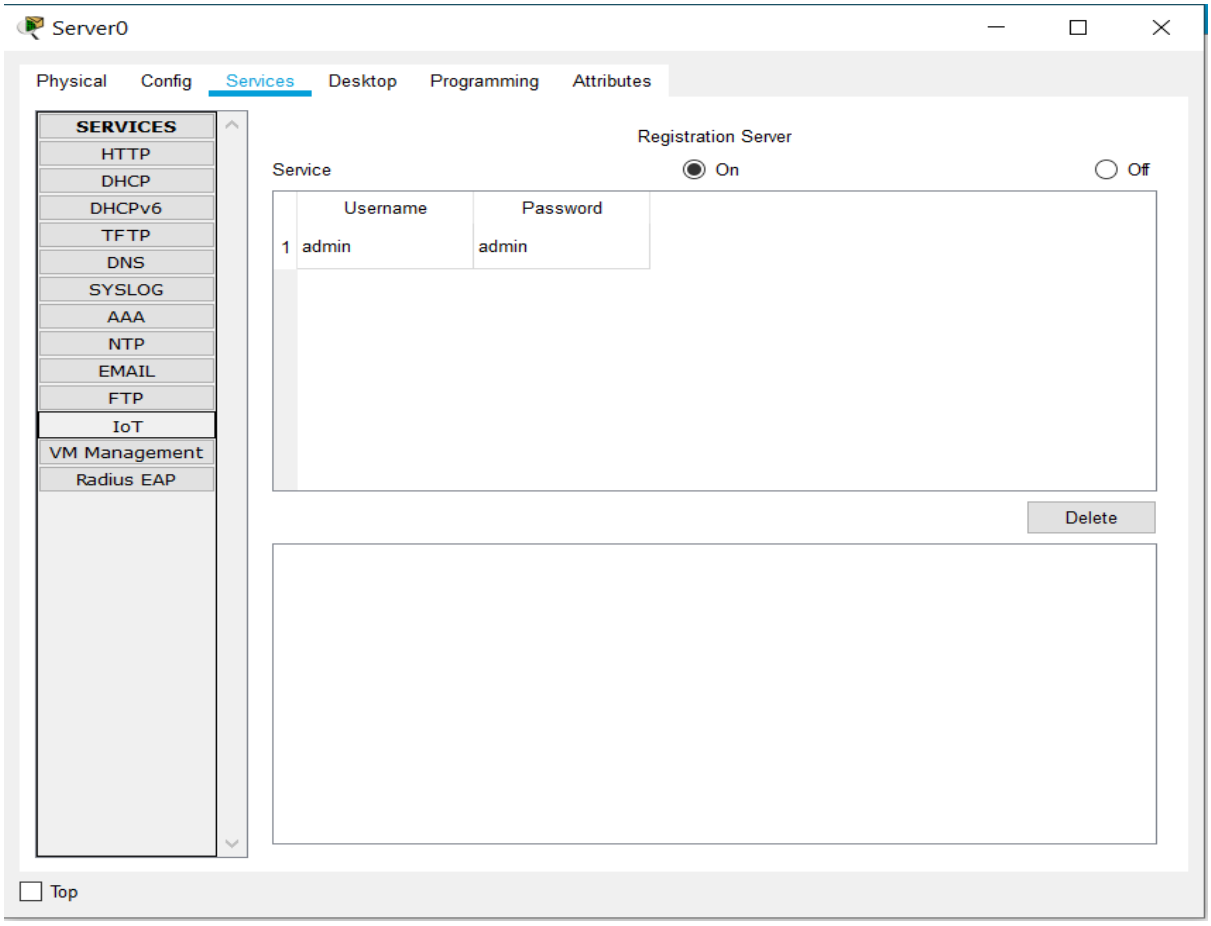


11. Repeat **STEP 9 & 10** to connect the Water Level Monitor (Waterlevel) wirelessly.



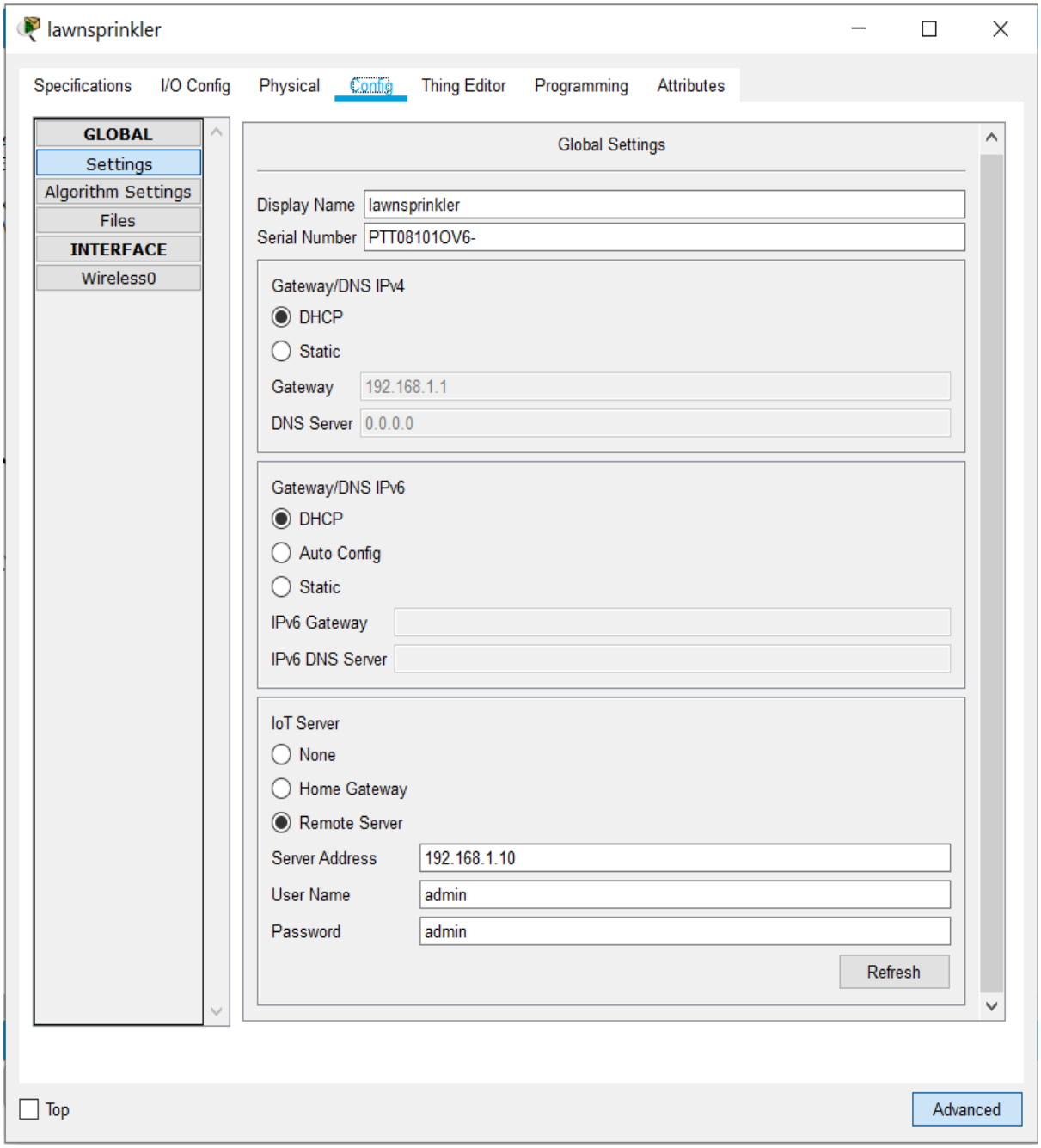


12. Now, we have enable the IoT servives in Server0, go to **Server0 → Services → IoT** and click '**on**' button to start the services.

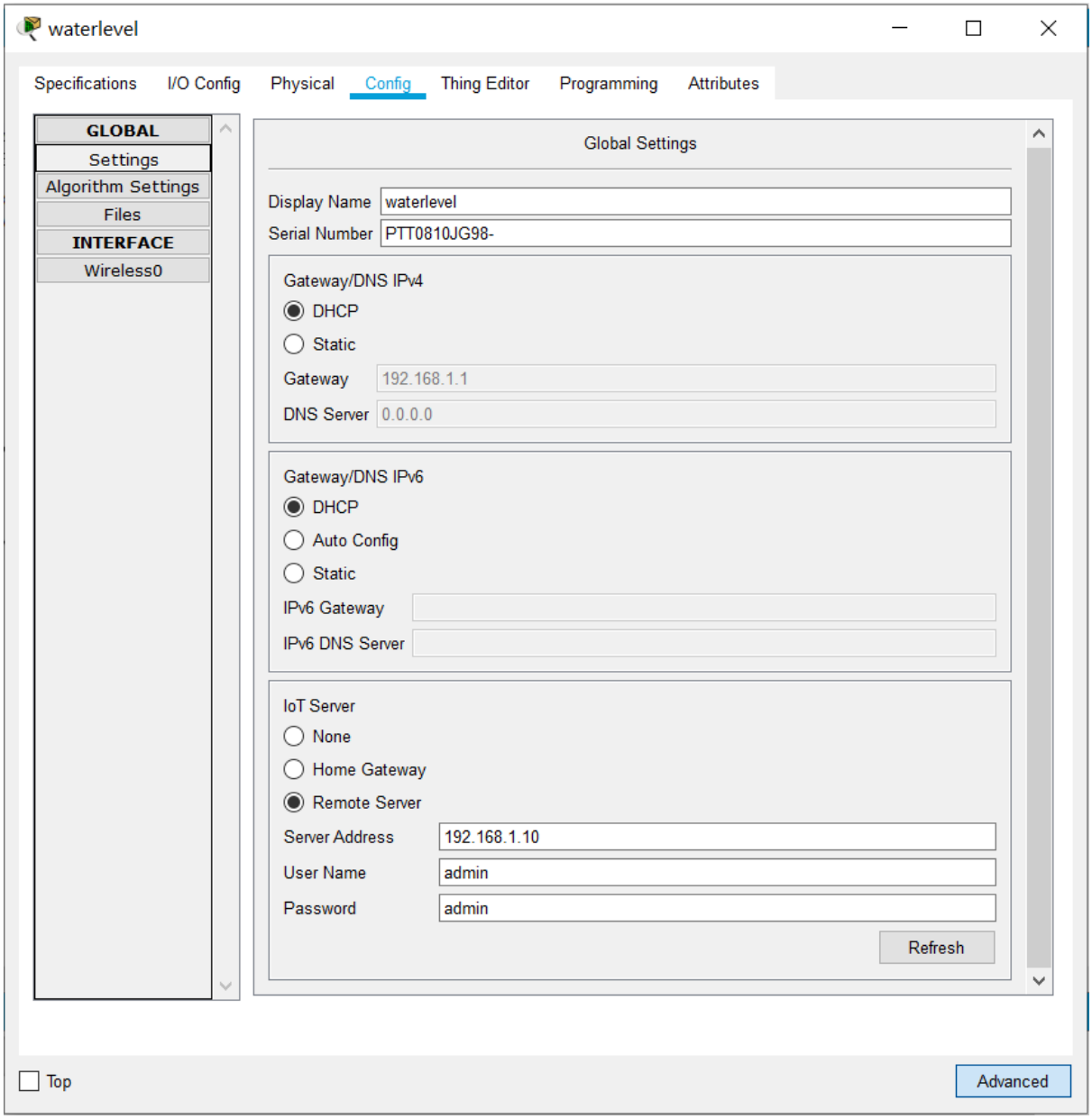


13. We have to set Username and Password for the IoT services, go to **Server0 → Desktop → IoT Monitor**. There fill the **IoT Server Address as IP Address of Server0 (192.168.1.10),** Username and Password. It will ask you to first Signup, click on Signup button and fill the Username and Password. In my case, **Username is 'admin'** and **Password is also 'admin'** as shown in above screenshot.

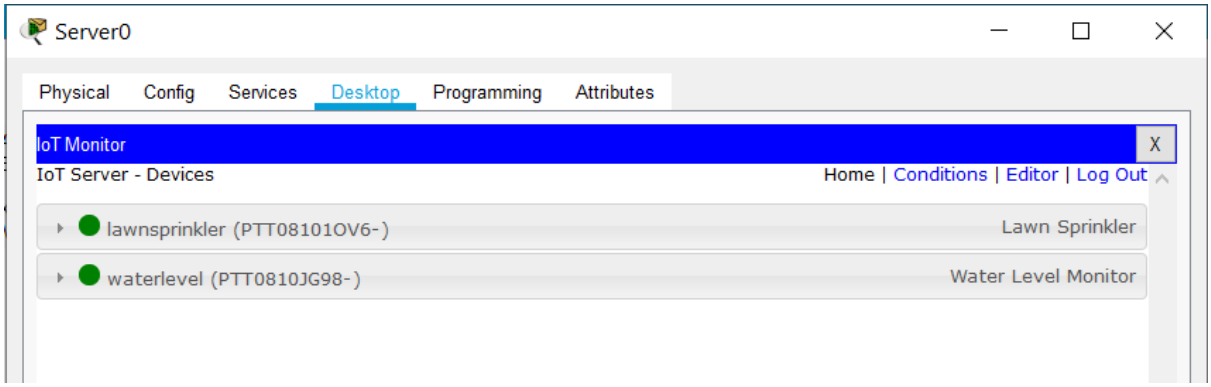
14. After Signup with specific Username and Password, go to **Lawnsprinkler → Config → Settings**. Set Display Name, Gateway/DNS IPv4 and Gateway/DNS IPv6 to be DHCP and in IoT Server select the Remote Server, Server Address will be same as IP Address of Server0 and use same Username & Password as in STEP above. Lastly click on '**Connect**' to get successful connection.



15. Repeat the same **STEP 14** to get successful connection for Water Level Monitor (Waterlevel).



16. To check that both Lawnsprinkler and Waterlevel is connected, go to **Server0 → Desktop → IoT Monitor**. Fill out the IoT Server Address, Username, Password and click on 'Login'. There you can see both the devices.



17. Now, go to **Server0 → Desktop → IoT Monitor → conditions**.

Now, click on 'Add' to add some conditions. Give the name (**TURN ON**) for your **condition1**, in 'if' block select waterlevel and Water level to be less than or equals to 9.0cm (**waterlevel Water Level <= 9.0 cm**) then set the actions for another devices as follow:

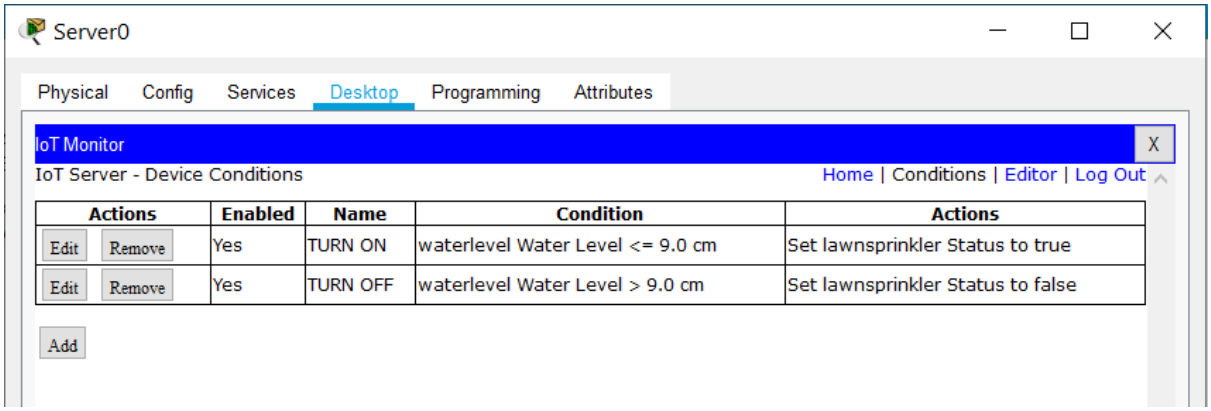
- Set lawnsprinkler Status to true

Click "OK" to save Condition.

Give the name (**TURN OFF**) for your **condition2**, in 'if' block select Smoke Detectorand level to be greater than 9.0cm (**waterlevel Water Level > 9.0 cm**) then set the actions for another devices as follow:

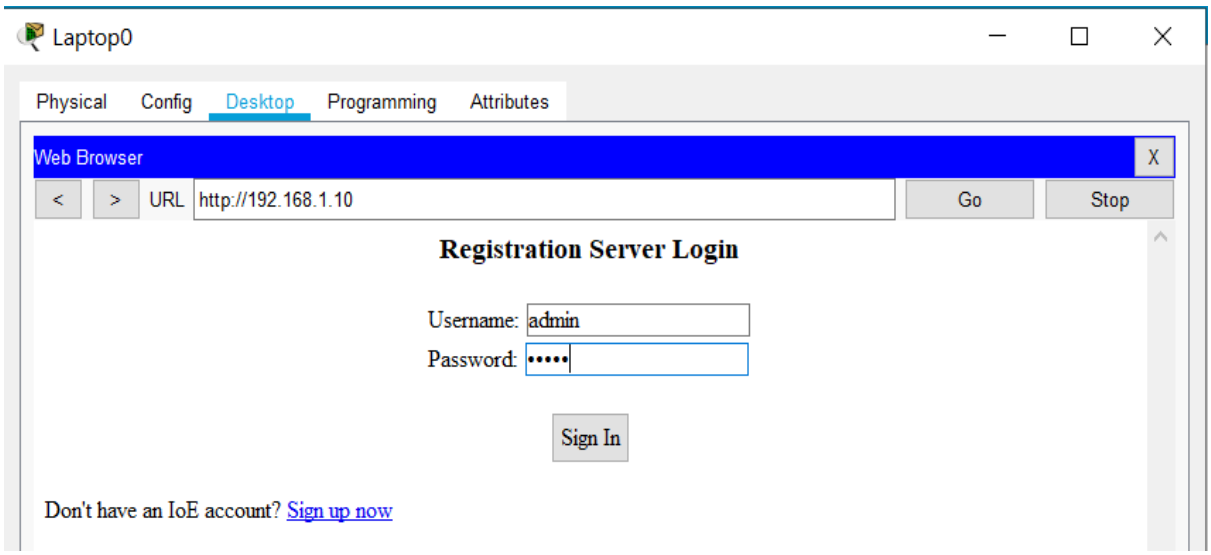
- Set lawnsprinkler Status to false

Click "OK" to save Condition.

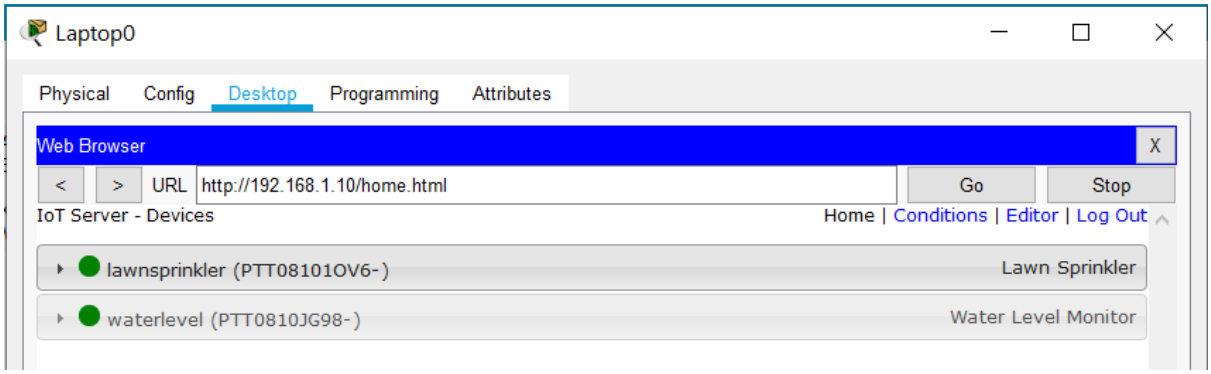


Output:

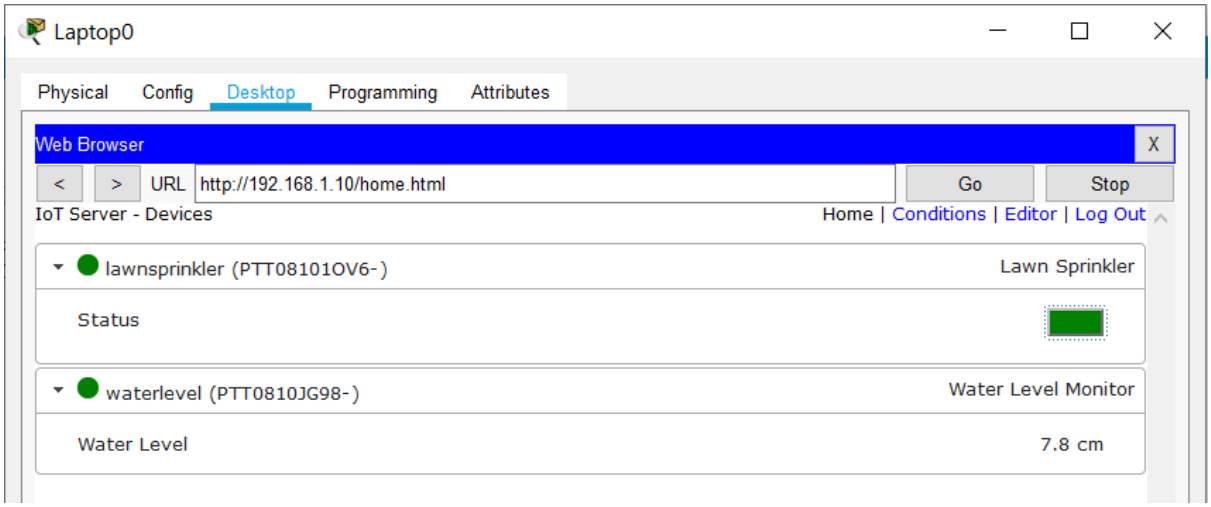
To see the output of IoT Devices, go to **Laptop0 → Desktop → Web Browser**. Fill out the **URL that is your IP Address of Server0 (192.168.1.10)** and click on '**Go**'. You can see a Web Page Asking about Username & Password, fill out the same **Username (admin) & Password (admin)**. Click on '**Sign In**'.



After successful Sign In, you can see your IoT Devices with the URL.



In output screenshot 1, We can see that whenever the level of Waterlevel is less than or equals to 9.0cm (**waterlevel Water Level <= 9.0 cm**) then condition1 came to an action i.e., **lawnsprinkler Status to true**



In output screenshot 2, We can see that whenever the level of Waterlevel is greater than 9.0cm (**waterlevel Water Level > 9.0 cm**) then condition2 came to an action i.e., **lawnsprinkler Status to false**