NAME:Aishwarya Ghaiwat

UID:2018130012

BATCH:A

CEL 51, DCCN, Monsoon 2020

Lab 4: Prototyping a Network

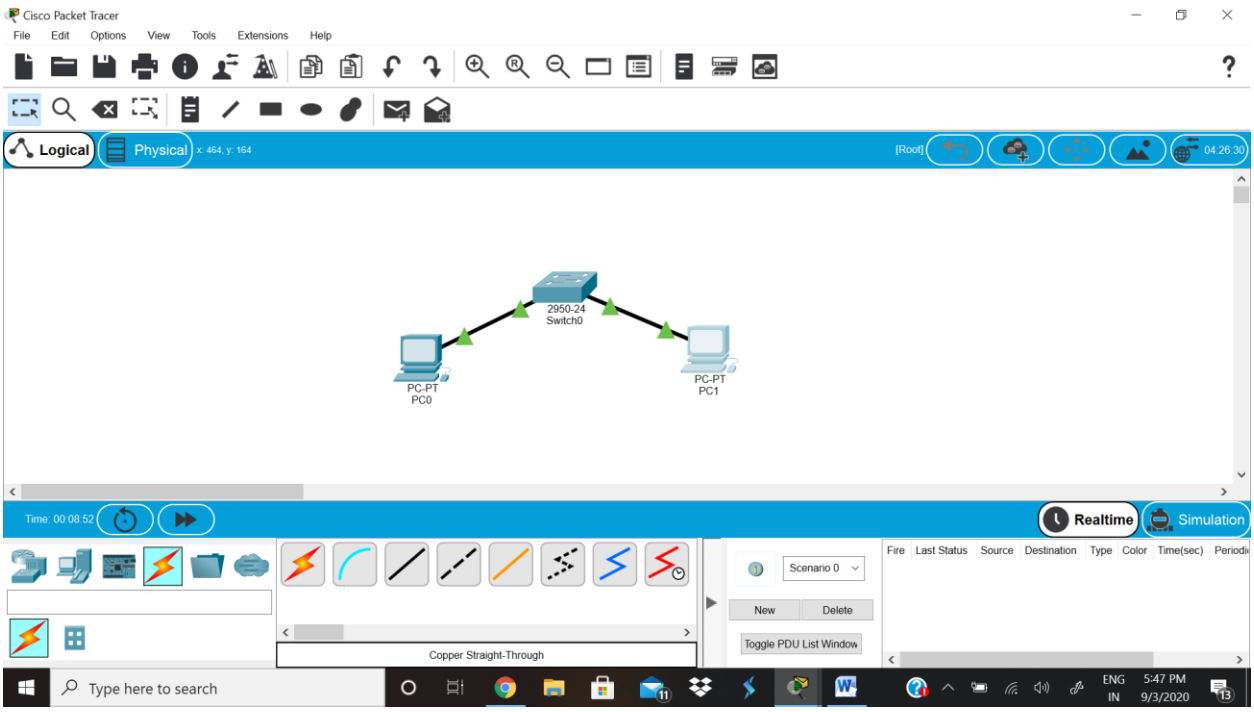
Objective:
Prototype a network using Packet Tracer

Background
A client has requested that you set up a simple network with two PCs connected to a switch. Verify that the hardware, along with the given configurations, meet the requirements of the client.

Step 1: Set up the network topology

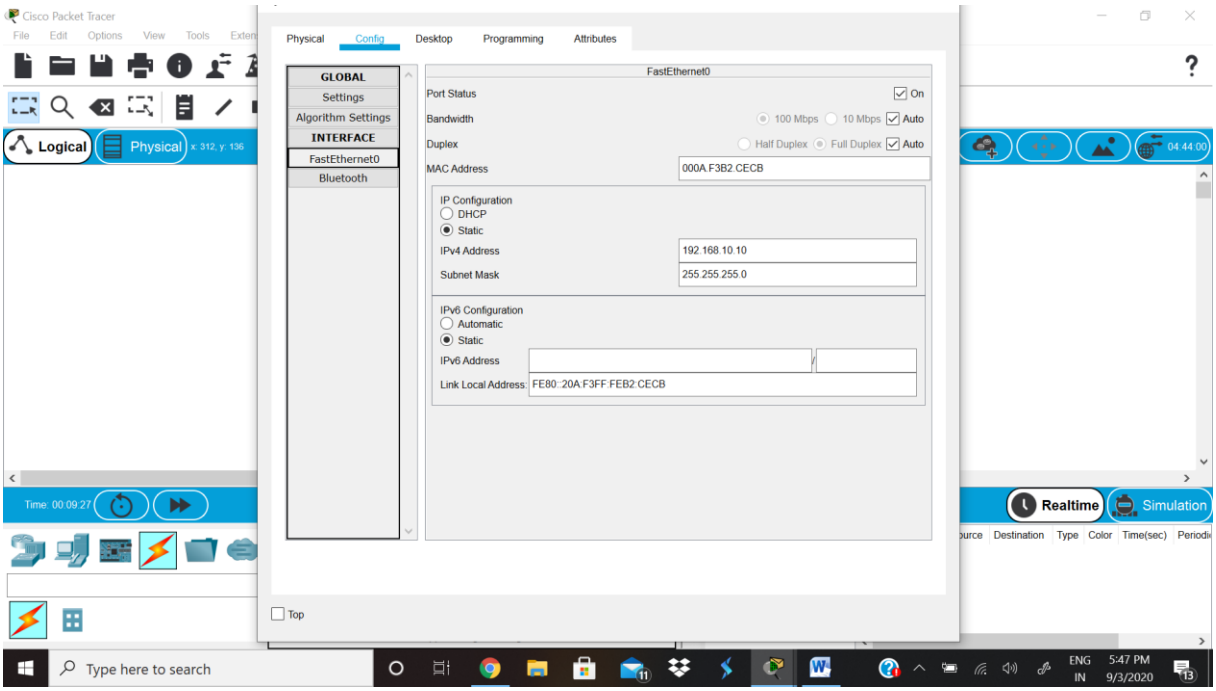
a) Add two PCs and a Cisco 2950T switch

b) Using straight-through cables, connect **PC0** to interface **Fa0/1** on **Switch0** and **PC1** to interface **Fa0/2** on **Switch0**.



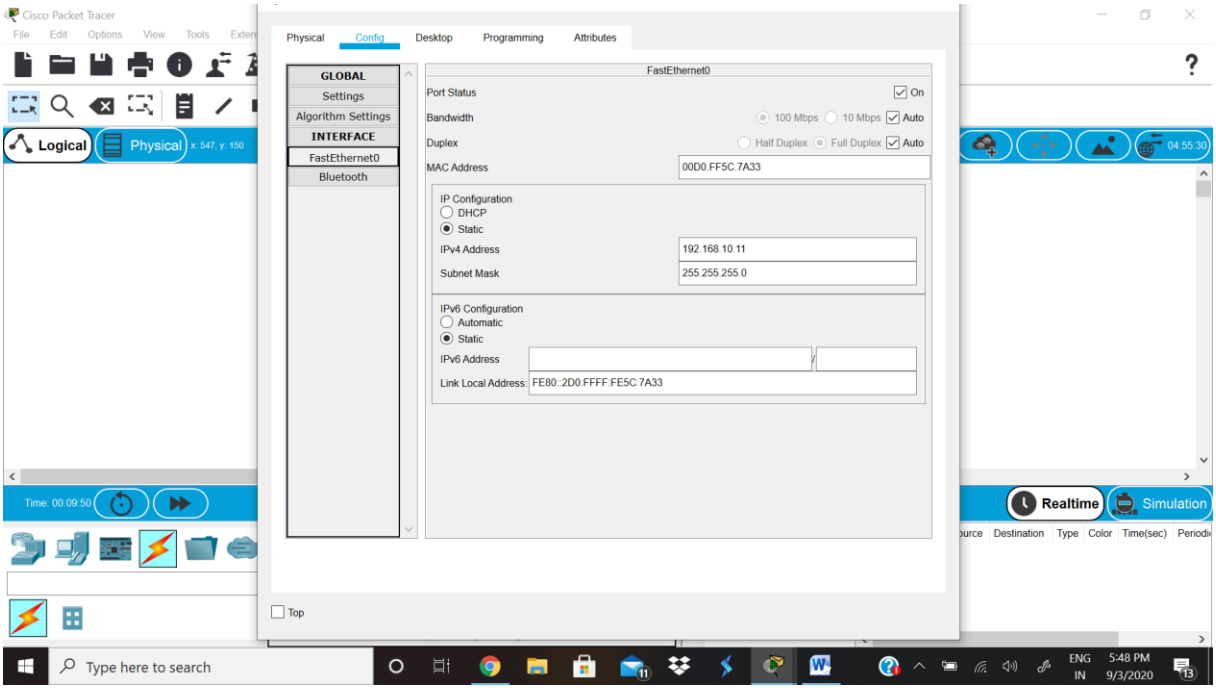
c) Configure PC0 using the **Config** tab in the PC0 configuration window:

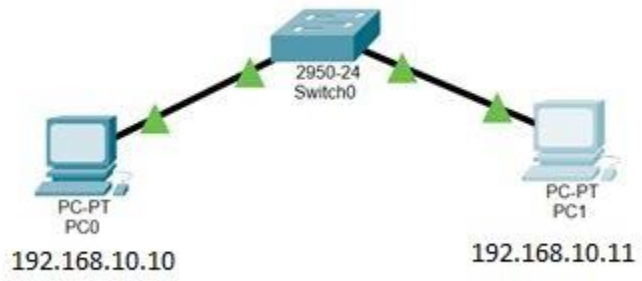
   a. IP address: 192.168.10.10
   b. Subnet Mask 255.255.255.0



d) Configure PC1 using the **Config** tab in the PC1 configuration window

a. IP address: 192.168.10.11
b. Subnet Mask 255.255.255.0





Step 2: Test connectivity from PC0 to PC1

a) Use the **ping** command to test connectivity.
   a. Click PC0.
   b. Choose the **Desktop** tab.

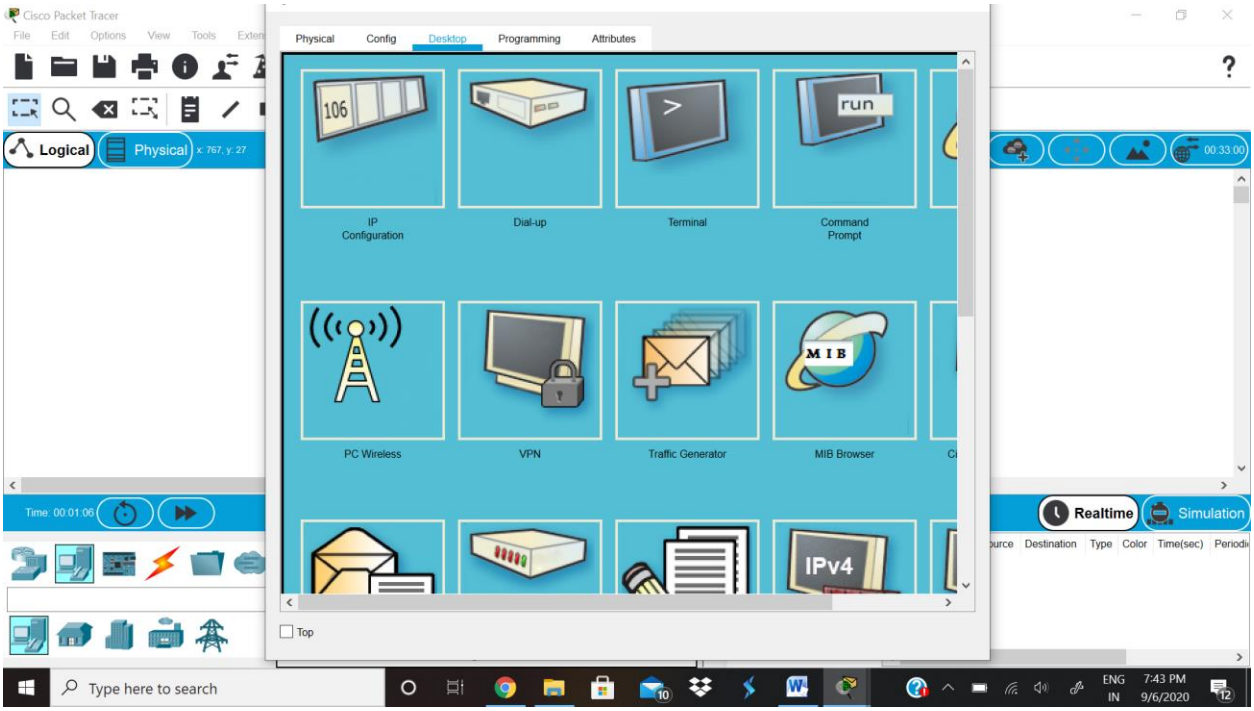
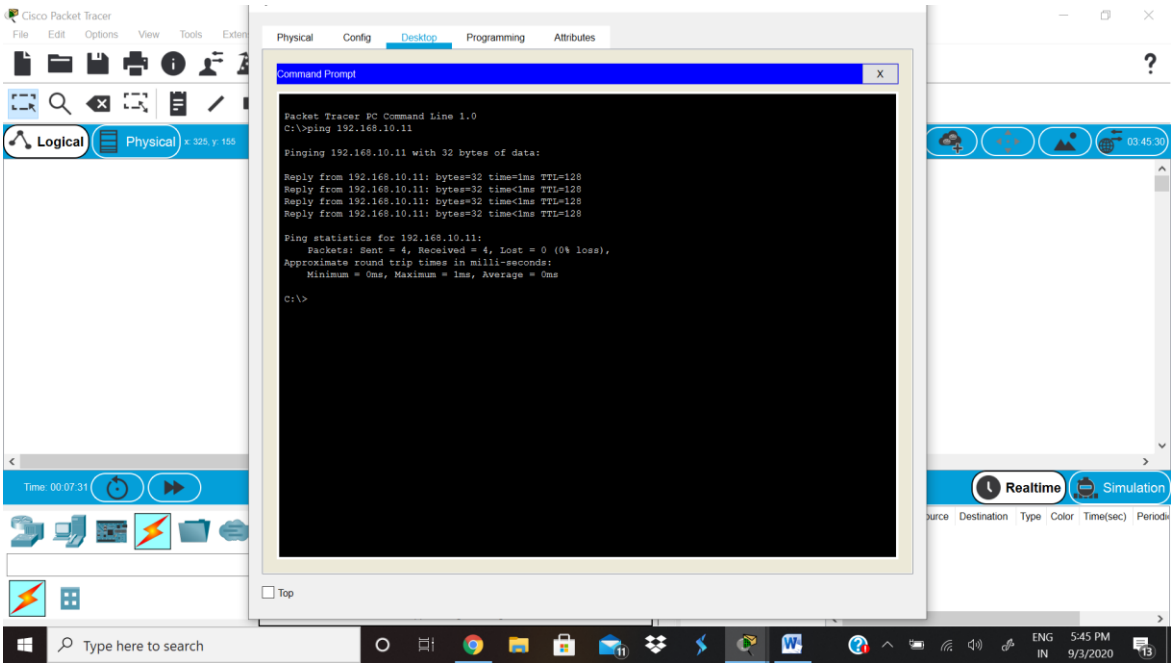
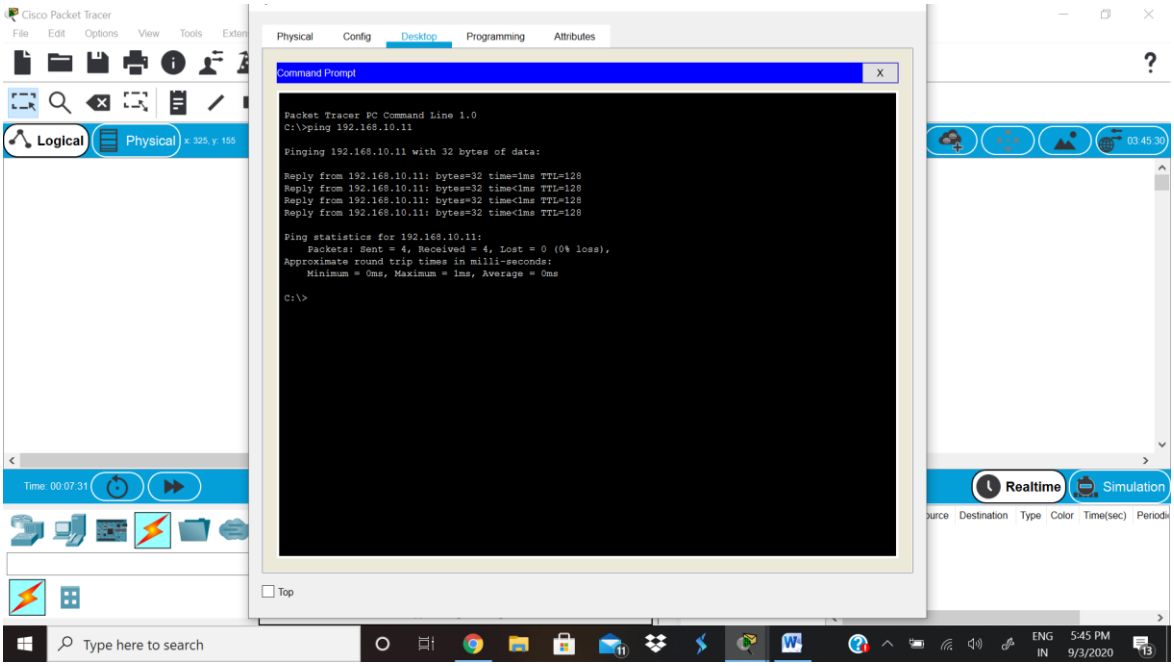


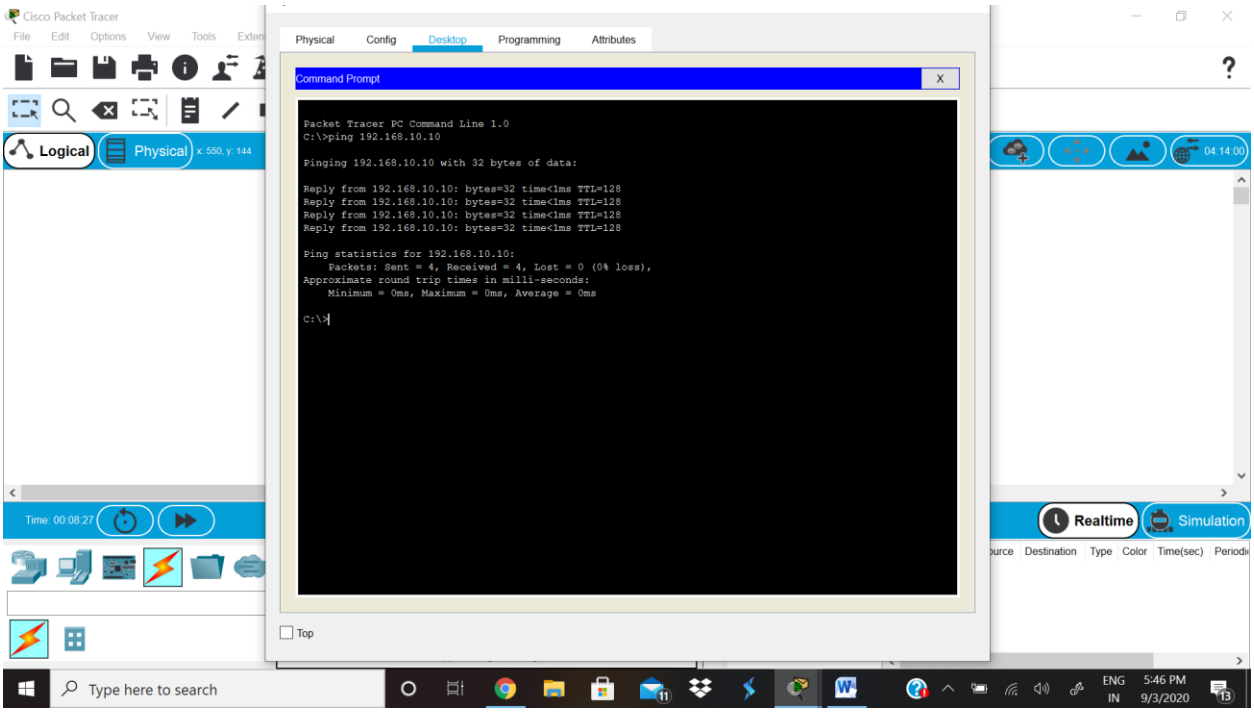
Fig 4.4 Shows the Desktop tab of PC-0

   c. Choose **Command Prompt**.
   d. Type: **ping 192.168.10.11** and press *enter*.

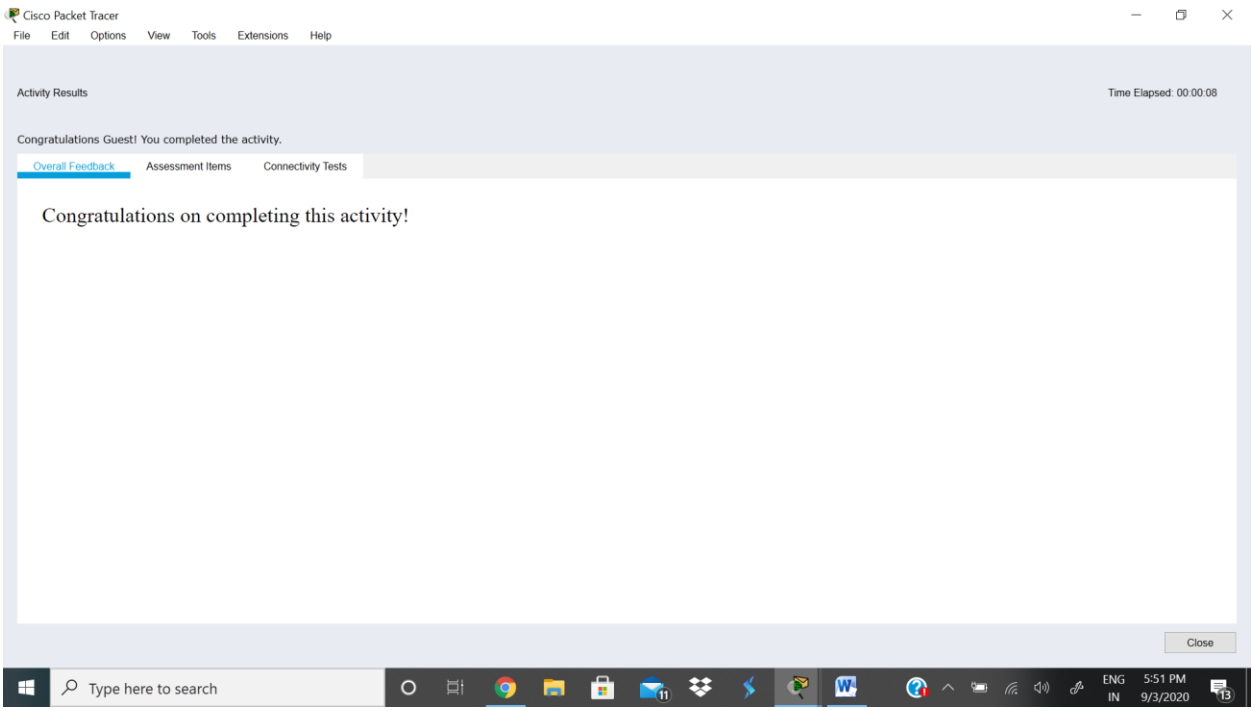


b) A successful **ping** indicates the network was configured correctly and the prototype validates the hardware and software configurations. A successful ping should resemble the below output:





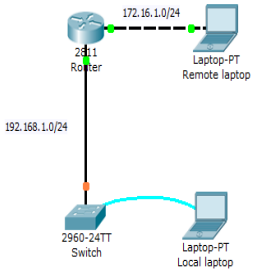
c) Close the configuration window.
d) Click the **Check Results** button at the bottom of the instruction window to check your work..



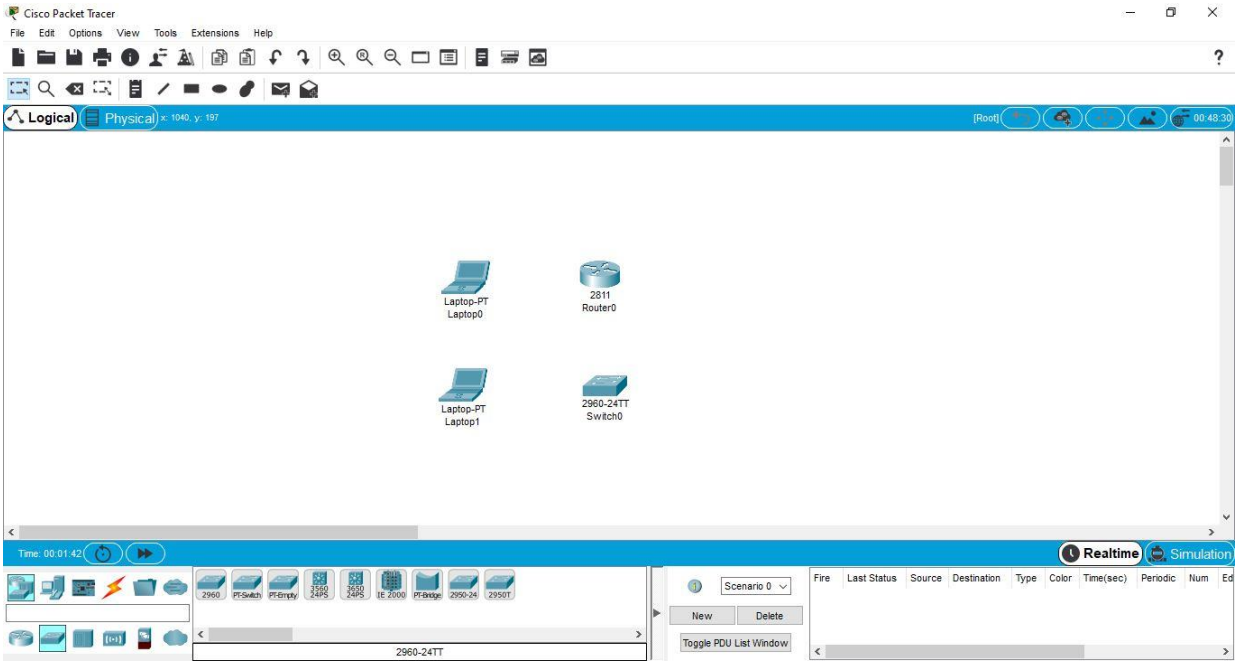
CEL51, DCCN, Monsoon 2020

Lab 4.1: Basic configuration - hostname, motd banner, passwd etc

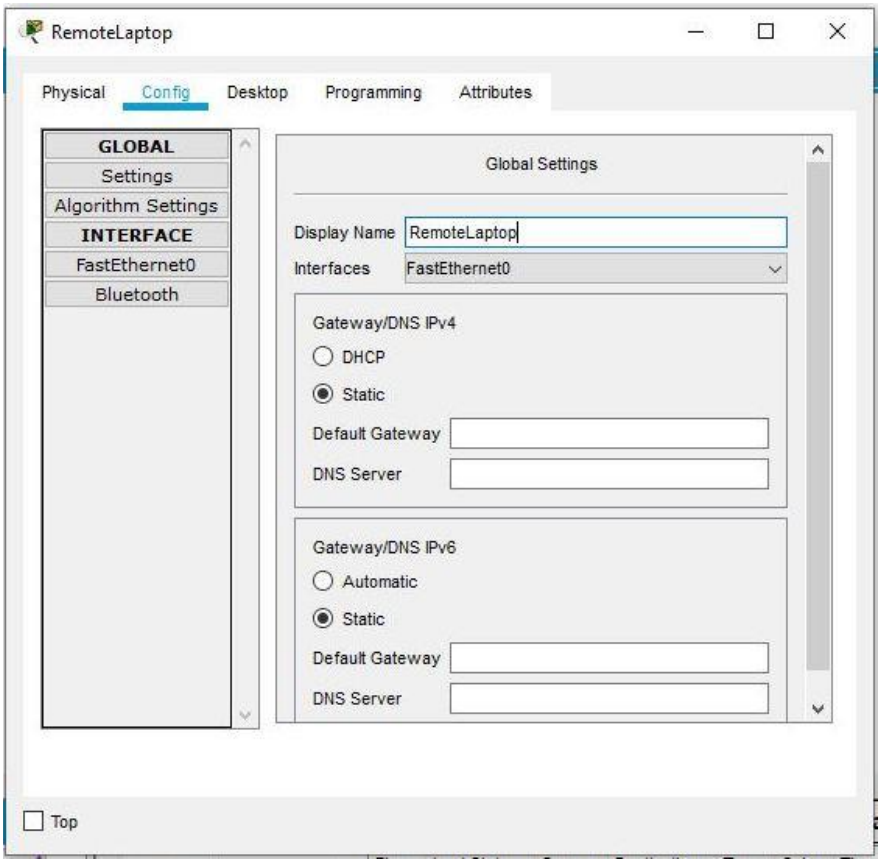
Objective:
This lab will test your ability to configure basic settings such as hostname, motd banner, encrypted passwords, and terminal options on a Packet Tracer 6.2 simulated Cisco Catalyst switch.

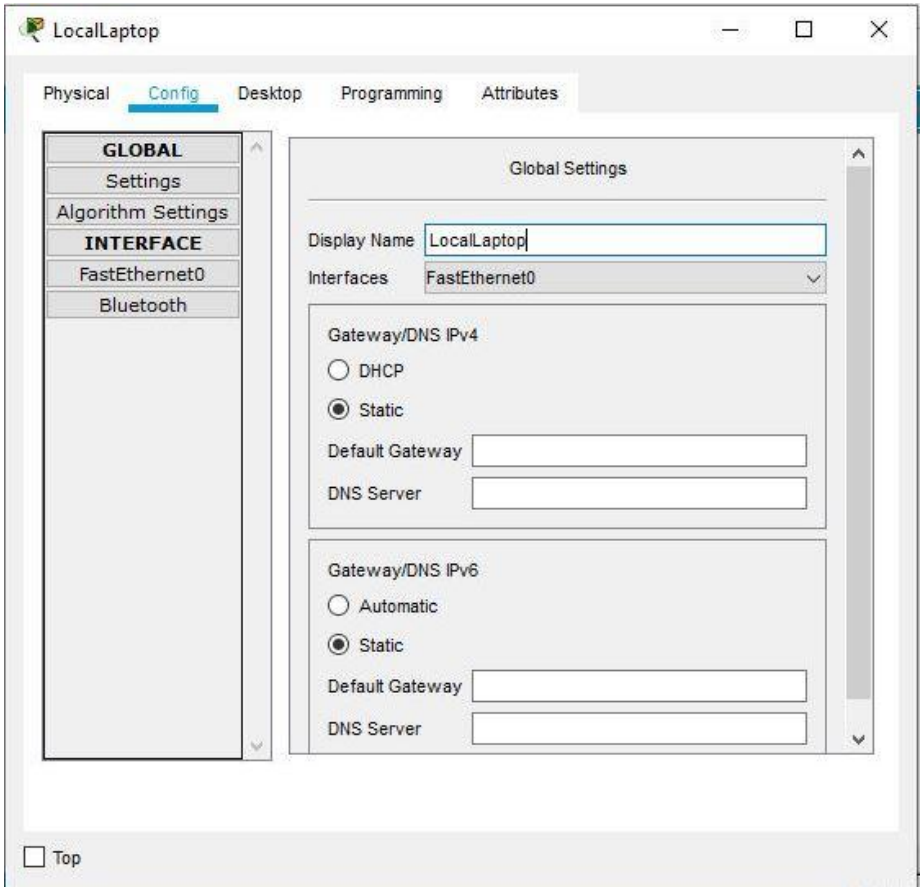


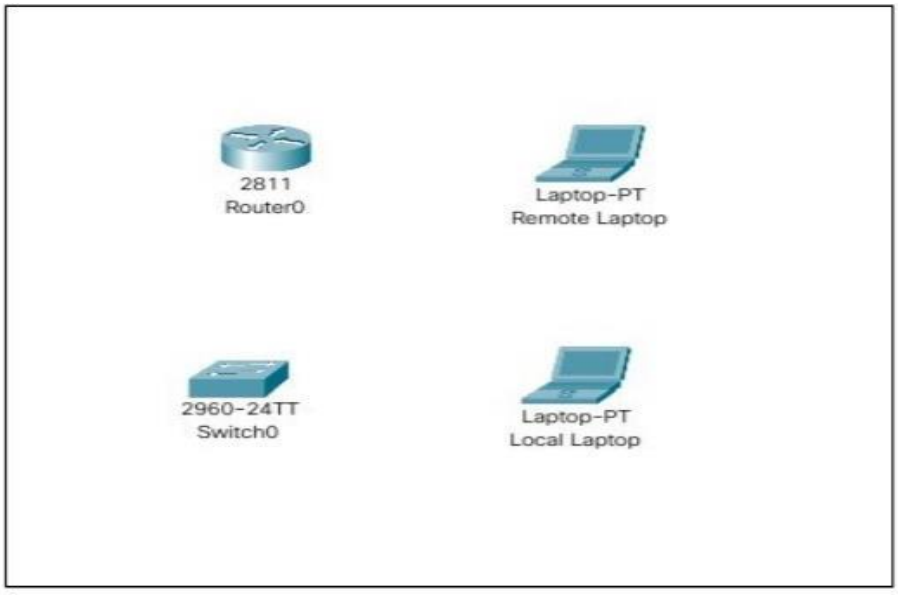
1. Use the local laptop connect to the switch console.

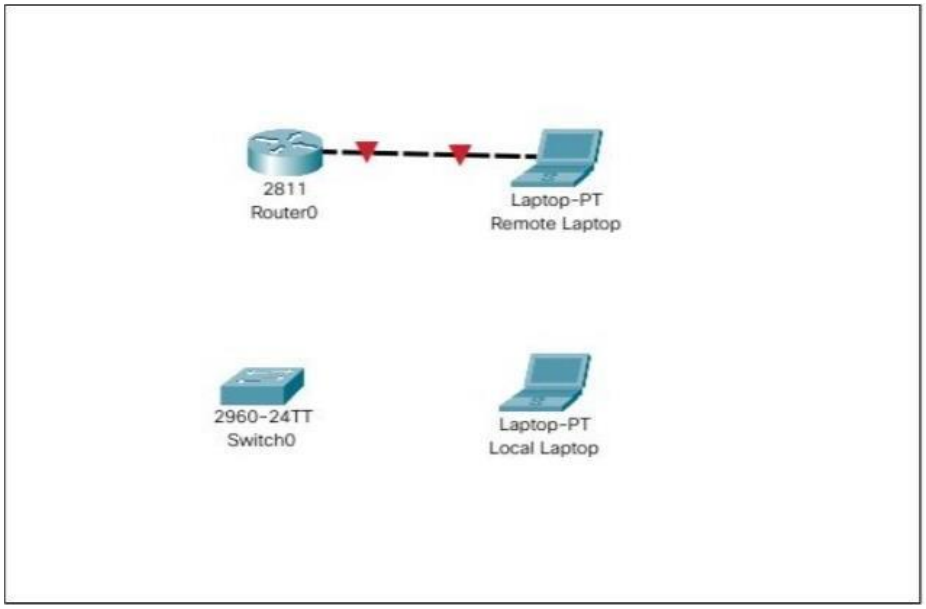


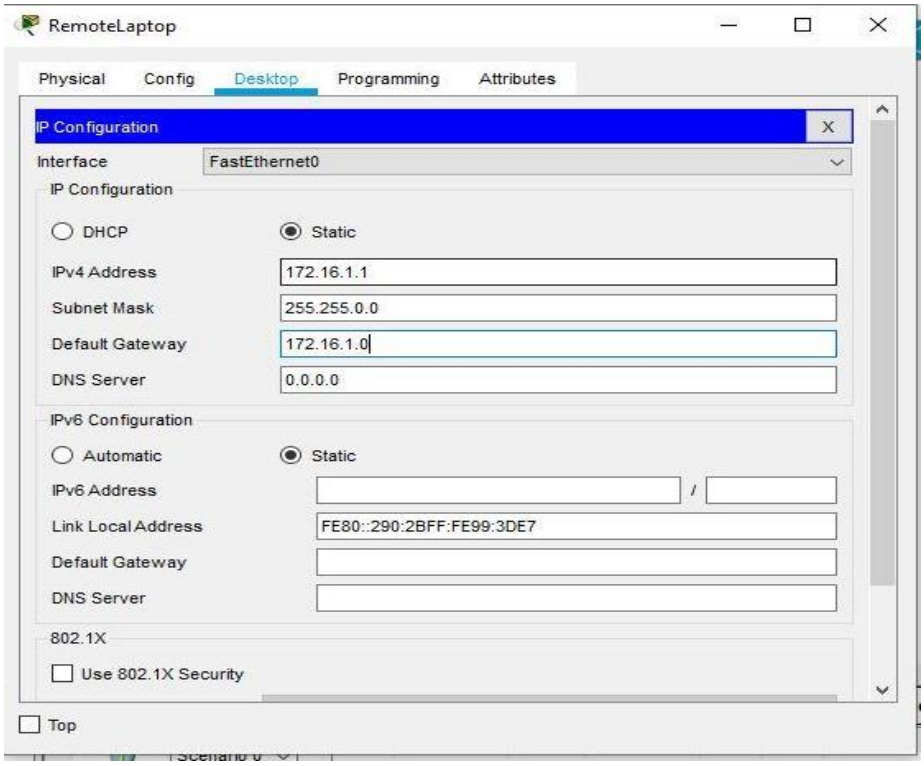
Rename Laptop 0 →Local Laptop
Rename Laptop 1→Remote Laptop


RemoteLaptop
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
Global Settings
Display Name
RemoteLaptop
Interfaces
FastEthernet0
Gateway/DNS IPv4
DHCP
Static
Default Gateway
DNS Server
Gateway/DNS IPv6
Automatic
Static
Default Gateway
DNS Server
Top

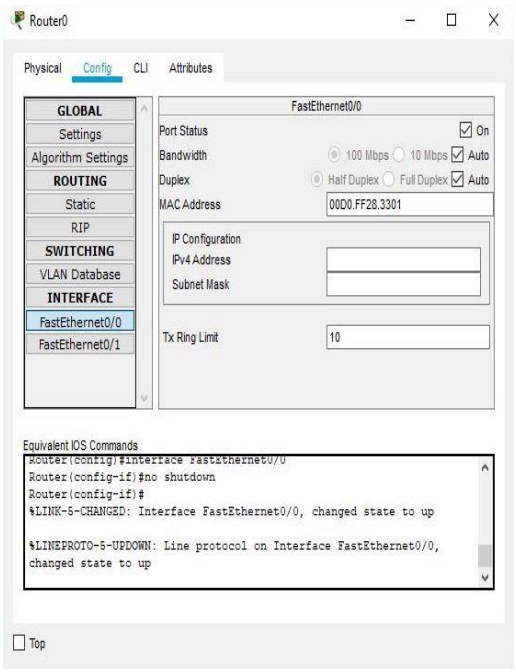

LocalLaptop
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
Global Settings
Display Name
LocalLaptop
Interfaces
FastEthernet0
Gateway/DNS IPv4
DHCP
Static
Default Gateway
DNS Server
Gateway/DNS IPv6
Automatic
Static
Default Gateway
DNS Server
Top

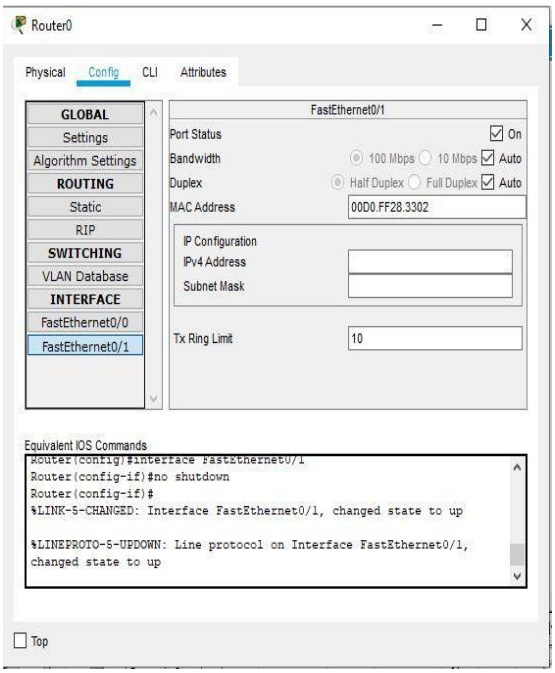

2811
Router0
Laptop-PT
Remote Laptop
2960-24TT
Switch0
Laptop-PT
Local Laptop



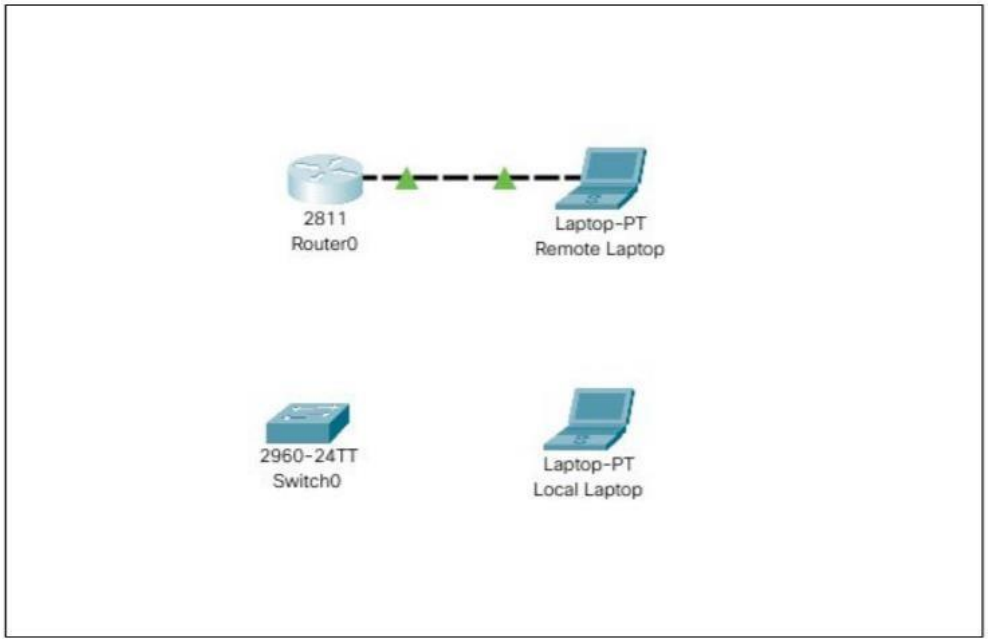


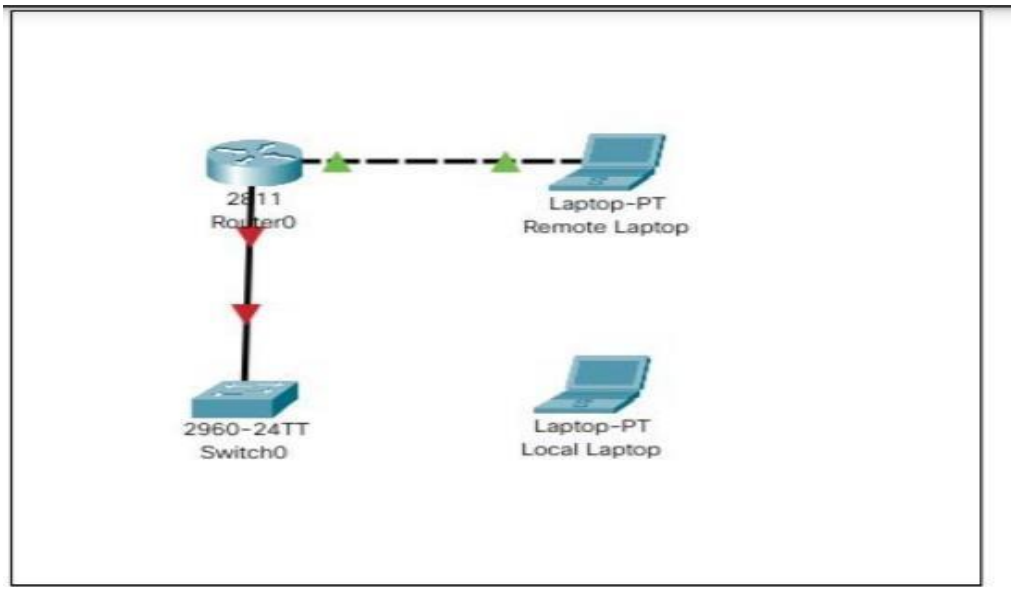
Shows the IP configuration of remote laptop where IP address is 172.16.1.2 and Default Gateway is 172.16.1.1

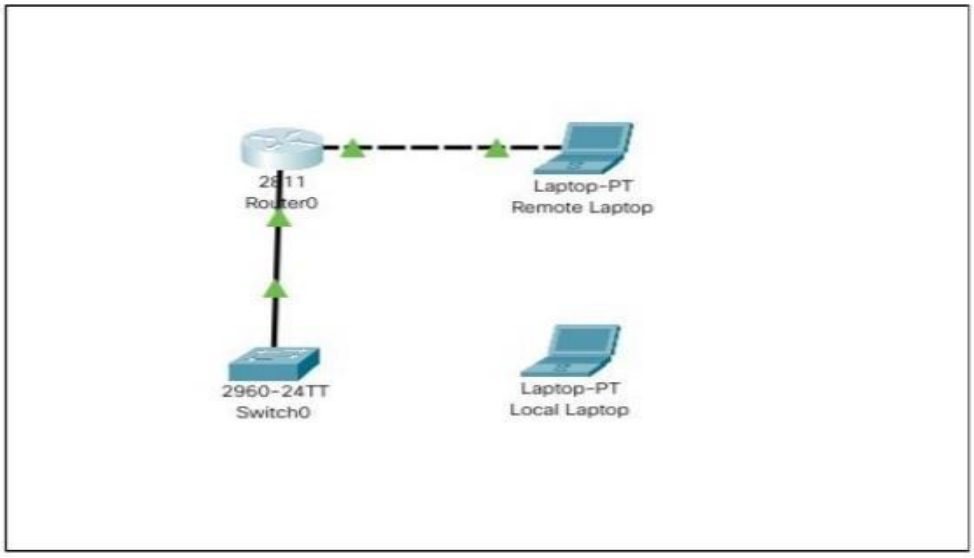




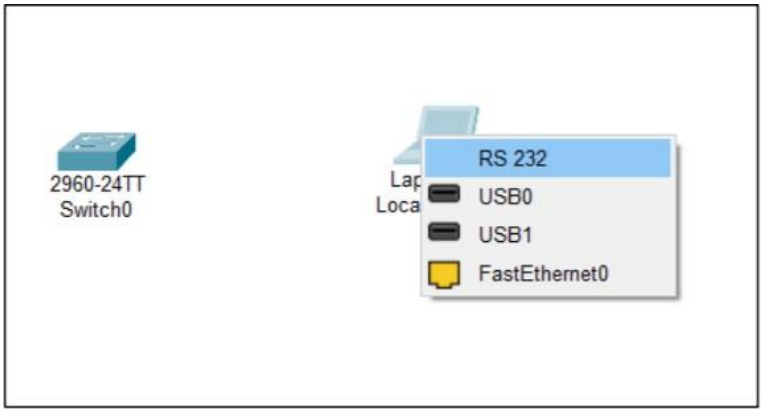
Shows the Fast ethernet Settings of Router connecting the switch where we turn the Port Status to ON

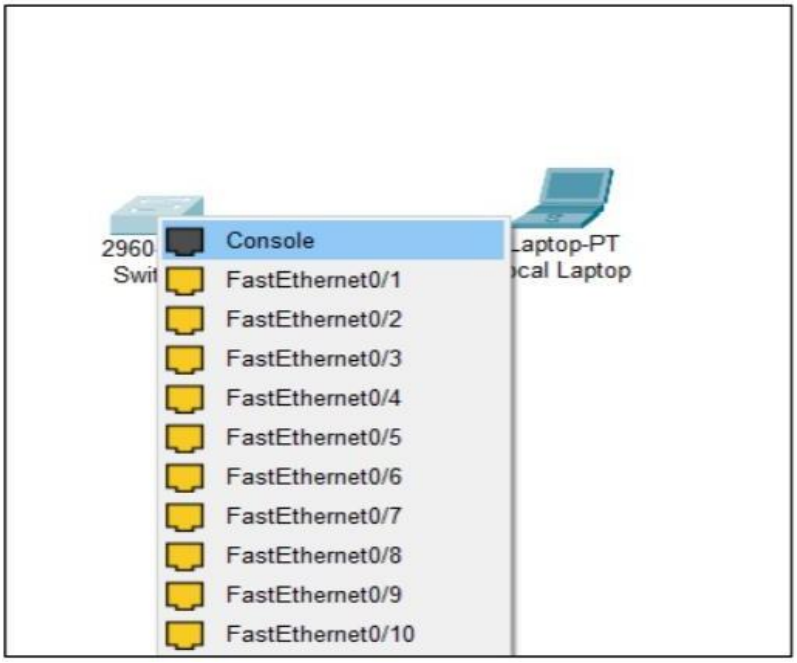


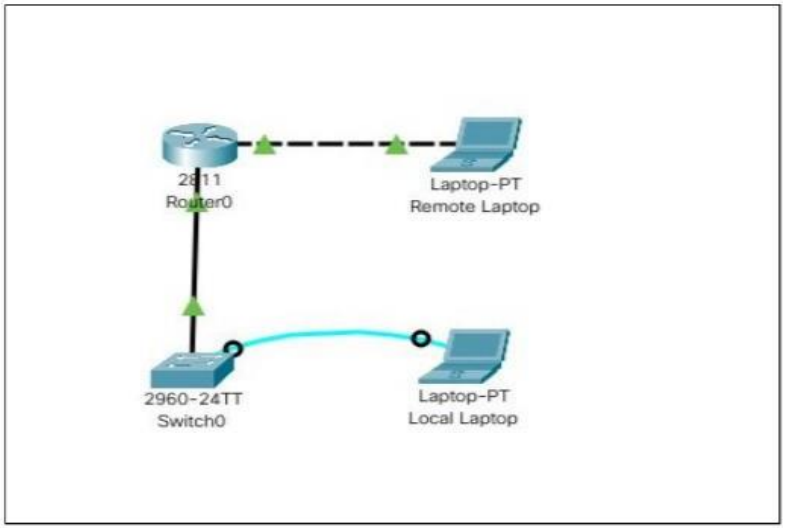


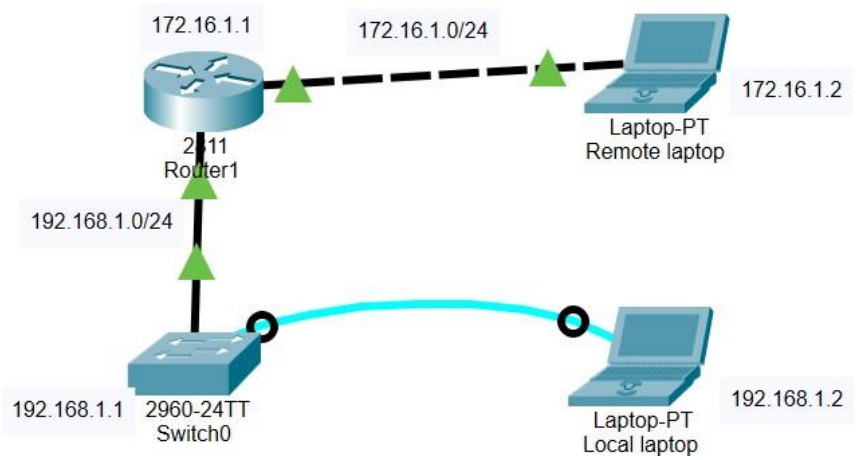


Connect console connection to RS232 port of Local Laptop and Console port of Switch



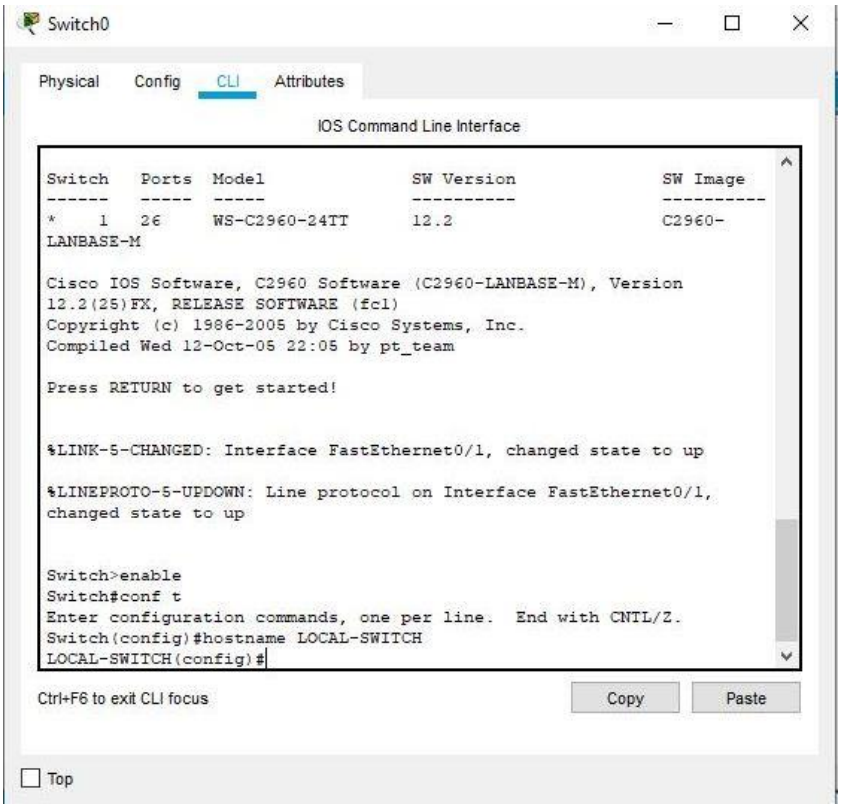

Console
FastEthernet0/1
FastEthernet0/2
FastEthernet0/3
FastEthernet0/4
FastEthernet0/5
FastEthernet0/6
FastEthernet0/7
FastEthernet0/8
FastEthernet0/9
FastEthernet0/10


Router0
Laptop-PT
Remote Laptop
2960-24TT
Switch0
Laptop-PT
Local Laptop


172.16.1.1
172.16.1.0/24
172.16.1.2
Laptop-PT
Remote laptop
Router1
192.168.1.0/24
192.168.1.1
2960-24TT
Switch0
Laptop-PT
Local laptop
192.168.1.2

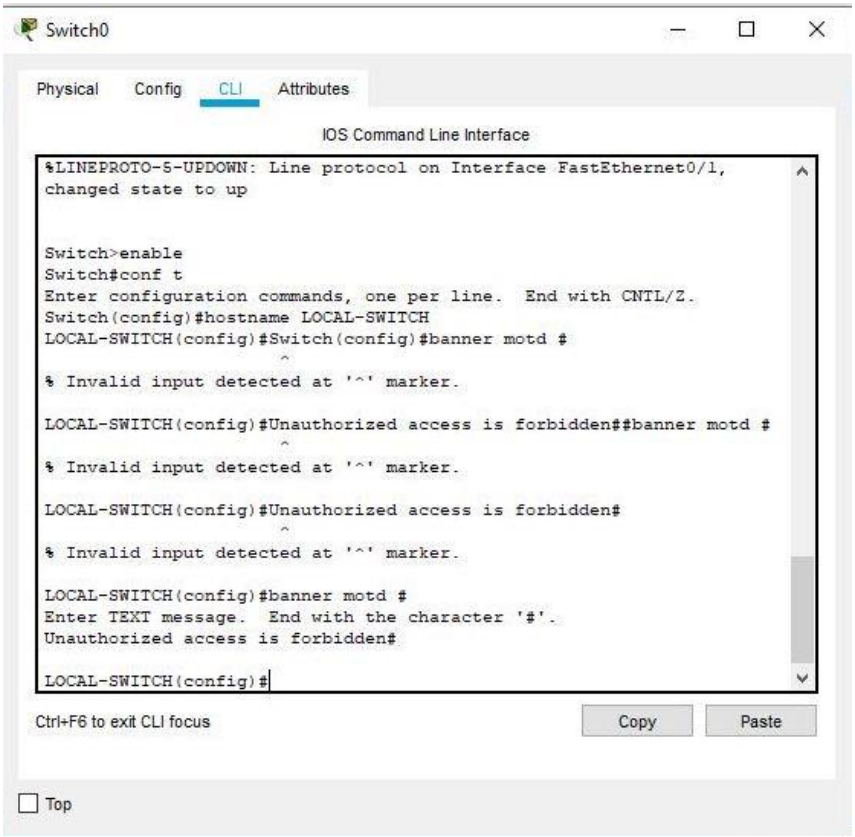
Shows 2 Laptops ,Remote Laptop connected to router via copper cross-over wire,Local Laptop connnected to Switch via console and router is connected to switch via copper straight wire.

2. Configure Switch hostname as LOCAL-SWITCH

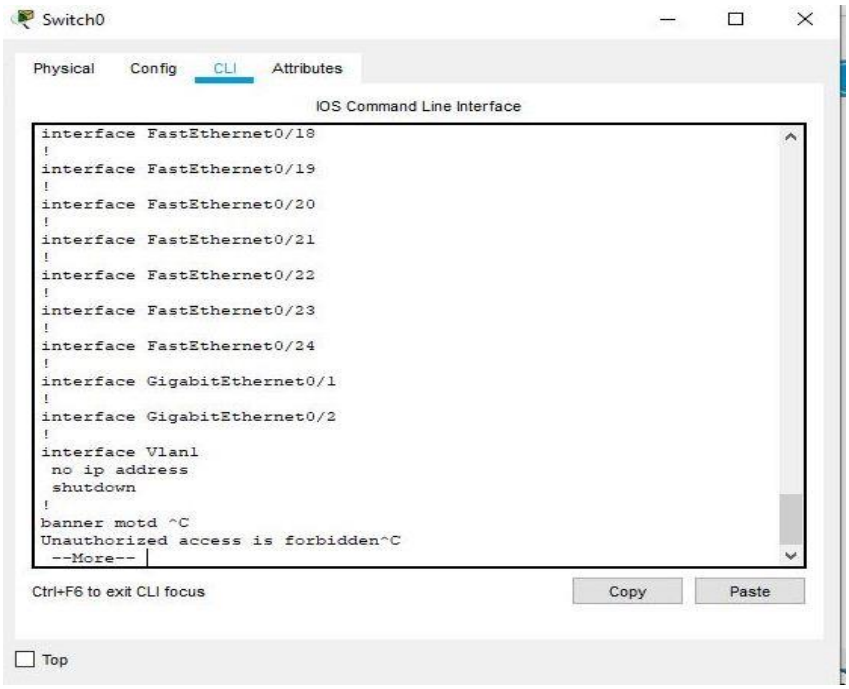


CLI of switch where we configure switch hostname as LOCAL- SWITCH

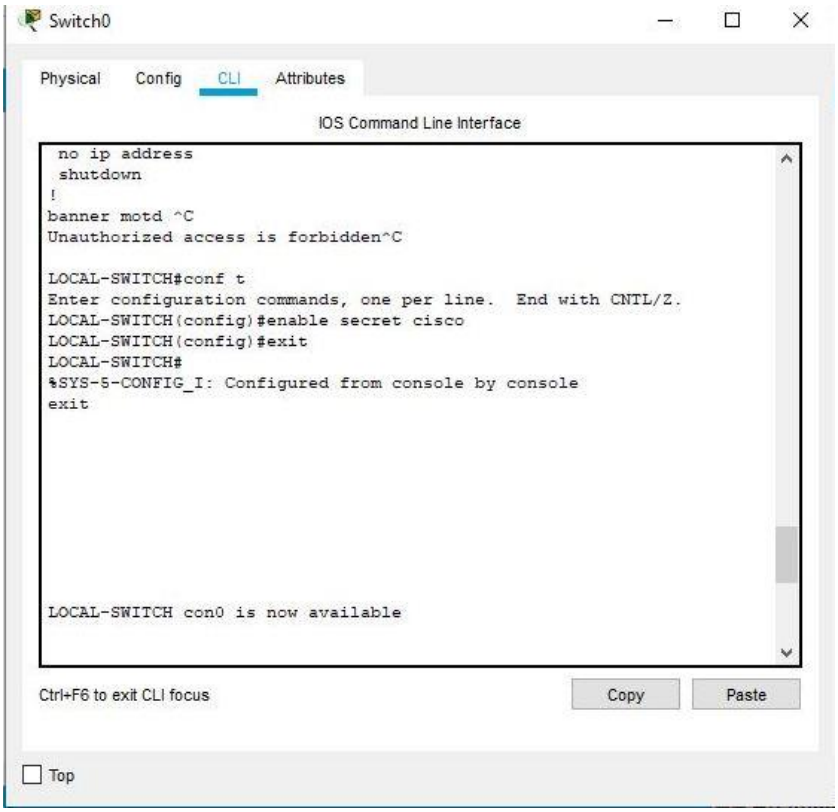
3. Configure the message of the day as "Unauthorized access is forbidden"



CLI of switch to configure the message of the day as Unauthorized access is forbidden

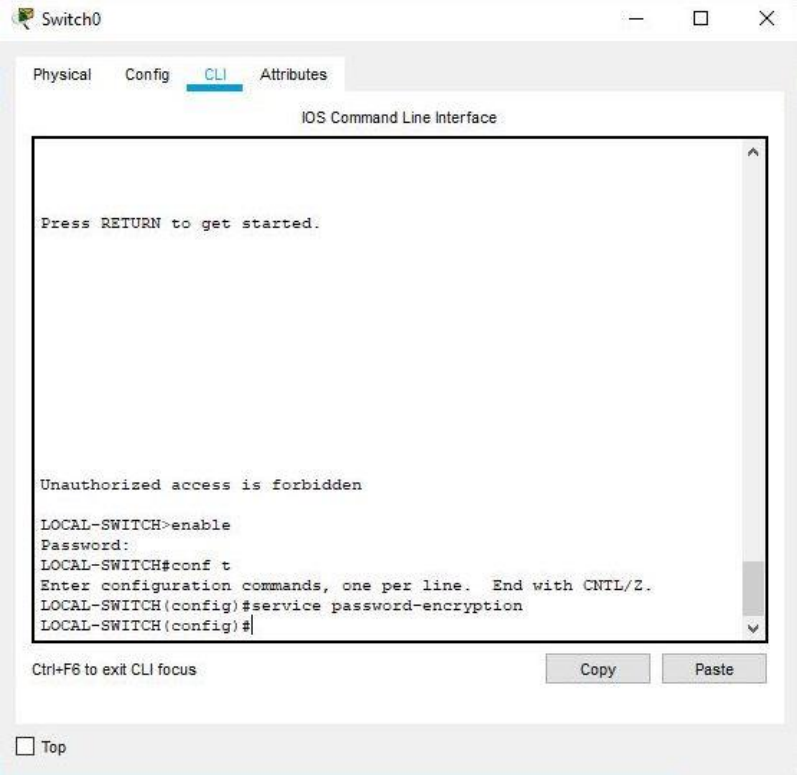


4. Configure the password for privileged mode access as "cisco". The password must be md5 encrypted



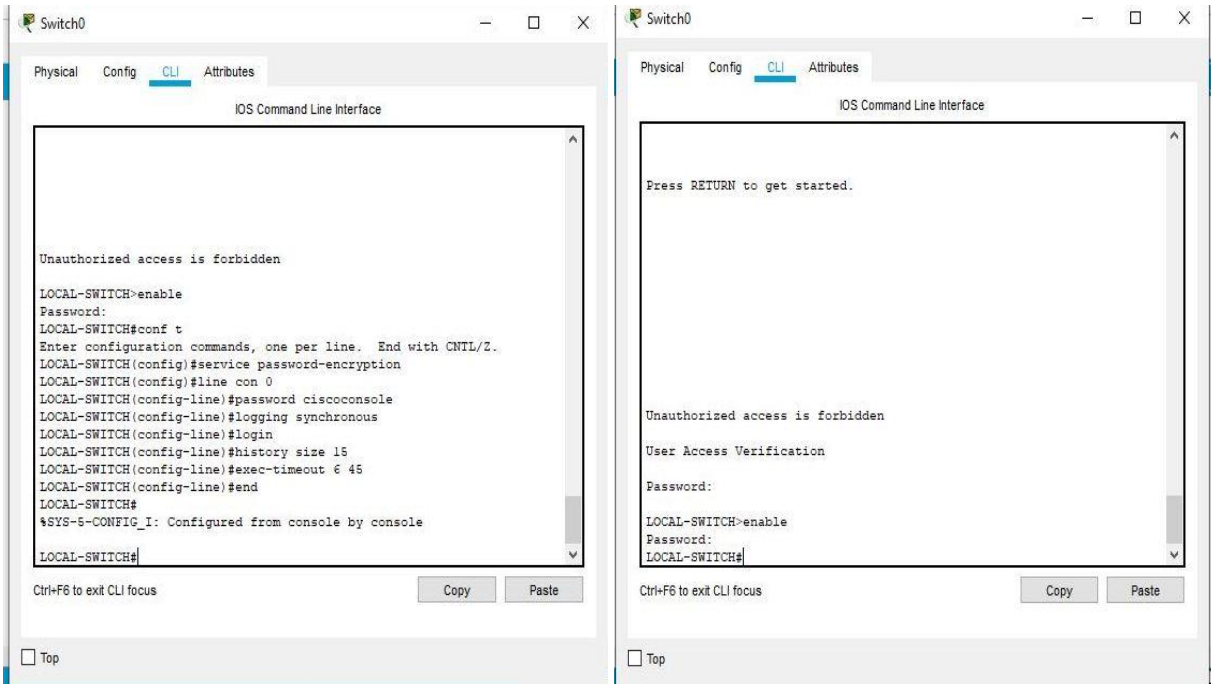
CLI to configure the password for privileged mode access as cisco

5. Configure password encryption on the switch using the global configuration command



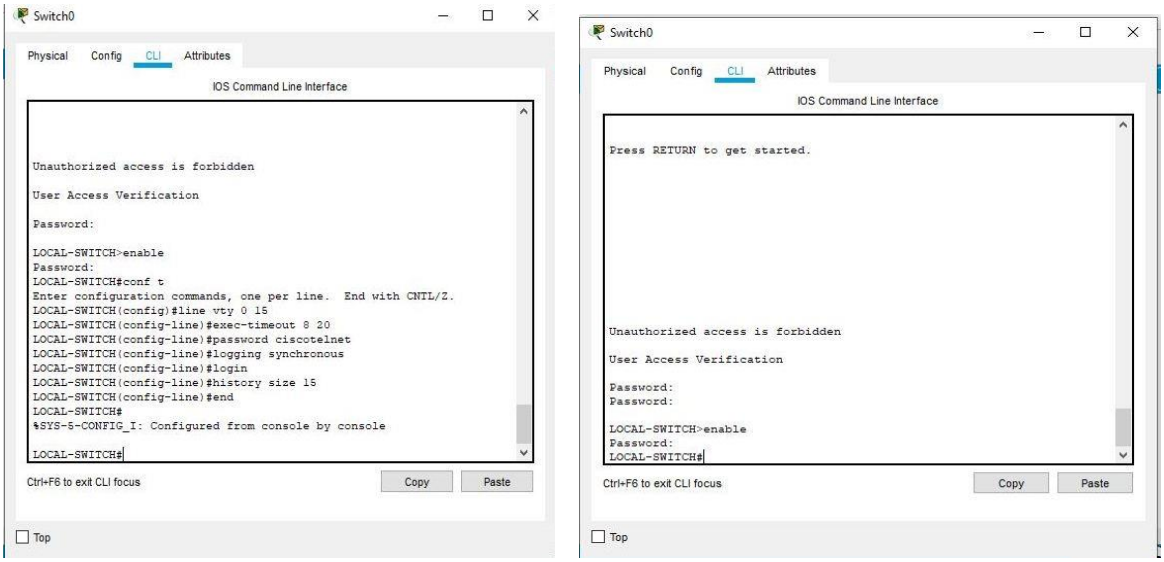
The CLI to configure password encryption on the switch

6. Configure CONSOLE access with the following settings :
- Login enabled
- Password : whatever you like
- History size : 15 commands
- Timeout : 6'45"
- Synchronous logging



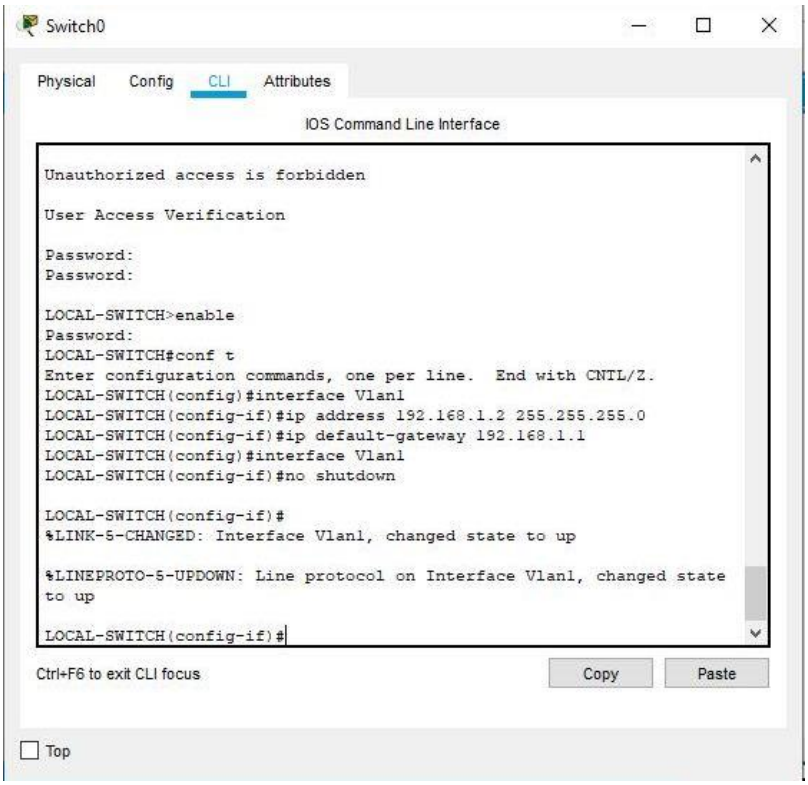
To configure console access with following settings- Login enabled, Password : whatever you like,History size : 15 commands,Timeout : 6'45",Synchronous logging and the CLI asks for password before it goes to console

6. Configure TELNET access with the following settings :
- Login enabled
- Password : whatever you like
- History size : 15 commands
- Timeout : 8'20"
- Synchronous logging



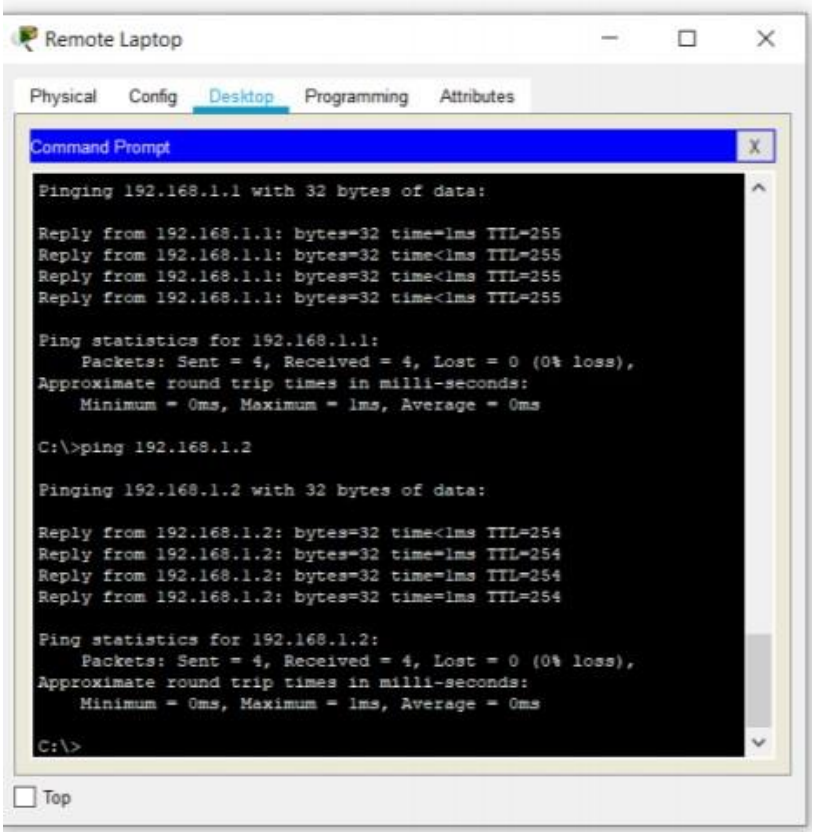
Configure Telnet access with following settings- Login enabled, Password: whatever you like, History size : 15 commands, Timeout : 8'20",Synchronous logging

7. Configure the IP address of the switch as 192.168.1.2/24 and it's default gateway IP (192.168.1.1).

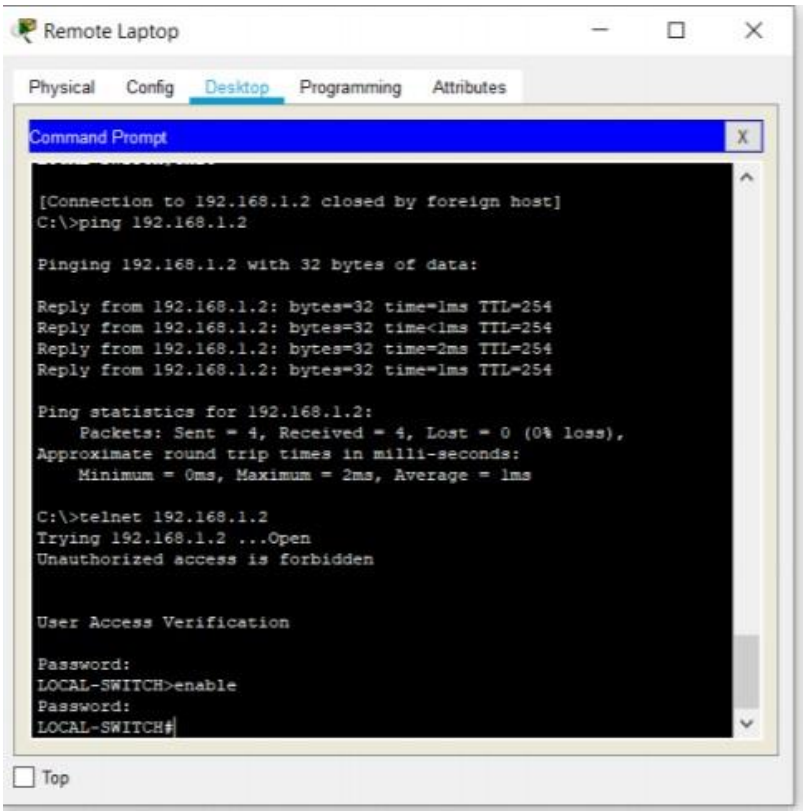


The CLI to configure the IP address of the switch as 192.168.1.2/24 and it's default gateway IP (192.168.1.1).

8. Test telnet connectivity from the Remote Laptop using the telnet client.



Pinging Switch from Remote Laptop



Telnet Switch from Remote Laptop after enterting the password for telnet and enabling switch from Remote Laptop