NAME: Ebrahim Hirani

UID: 2018130015

BATCH: B

CEL 51, DCCN, Monsoon 2020

Lab 4: Prototyping a Network

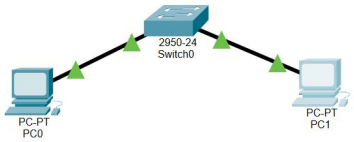
Objective:
Prototype a network using Packet Tracer

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

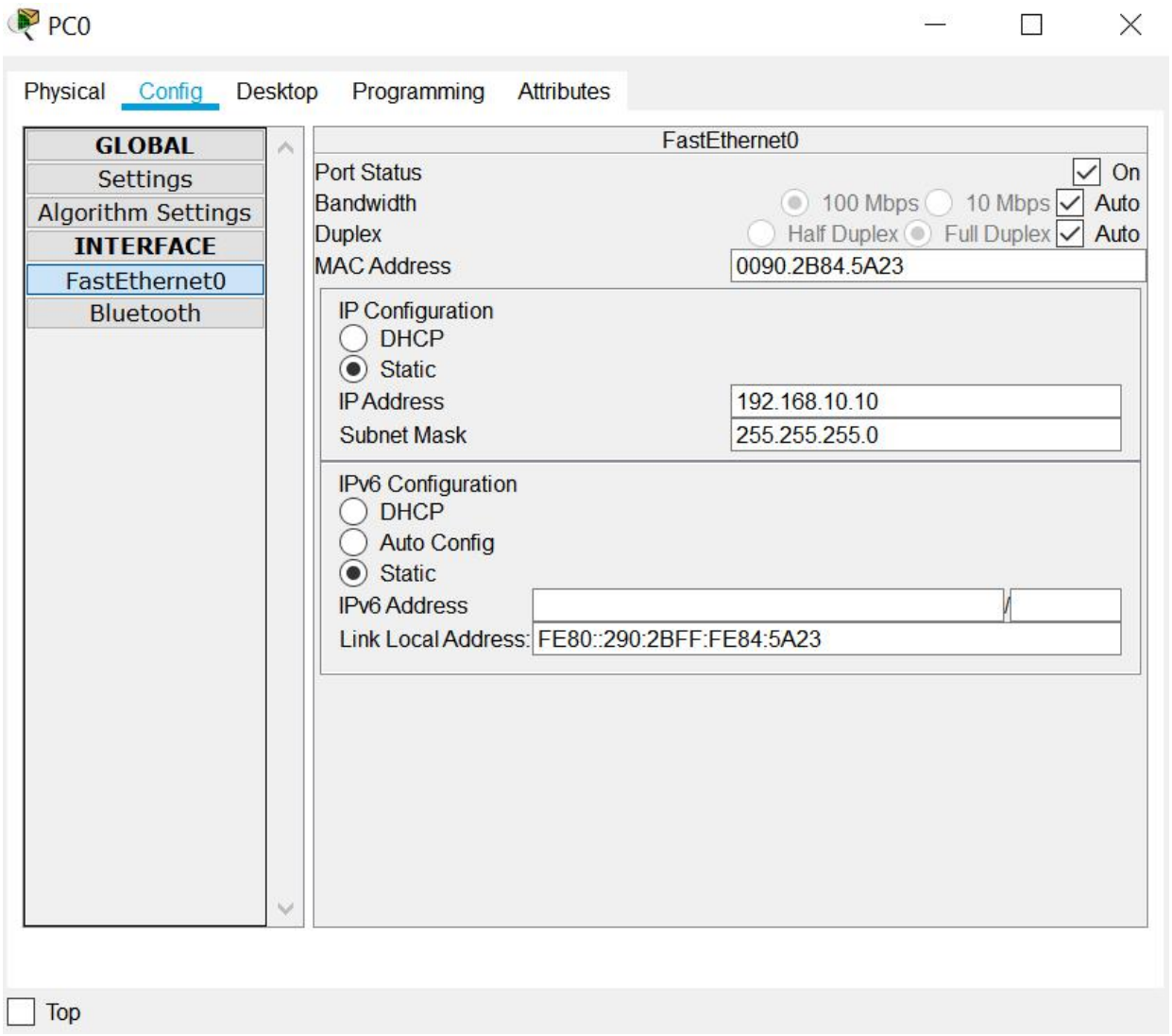
a) Add two PCs and a Cisco 2950T switch

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

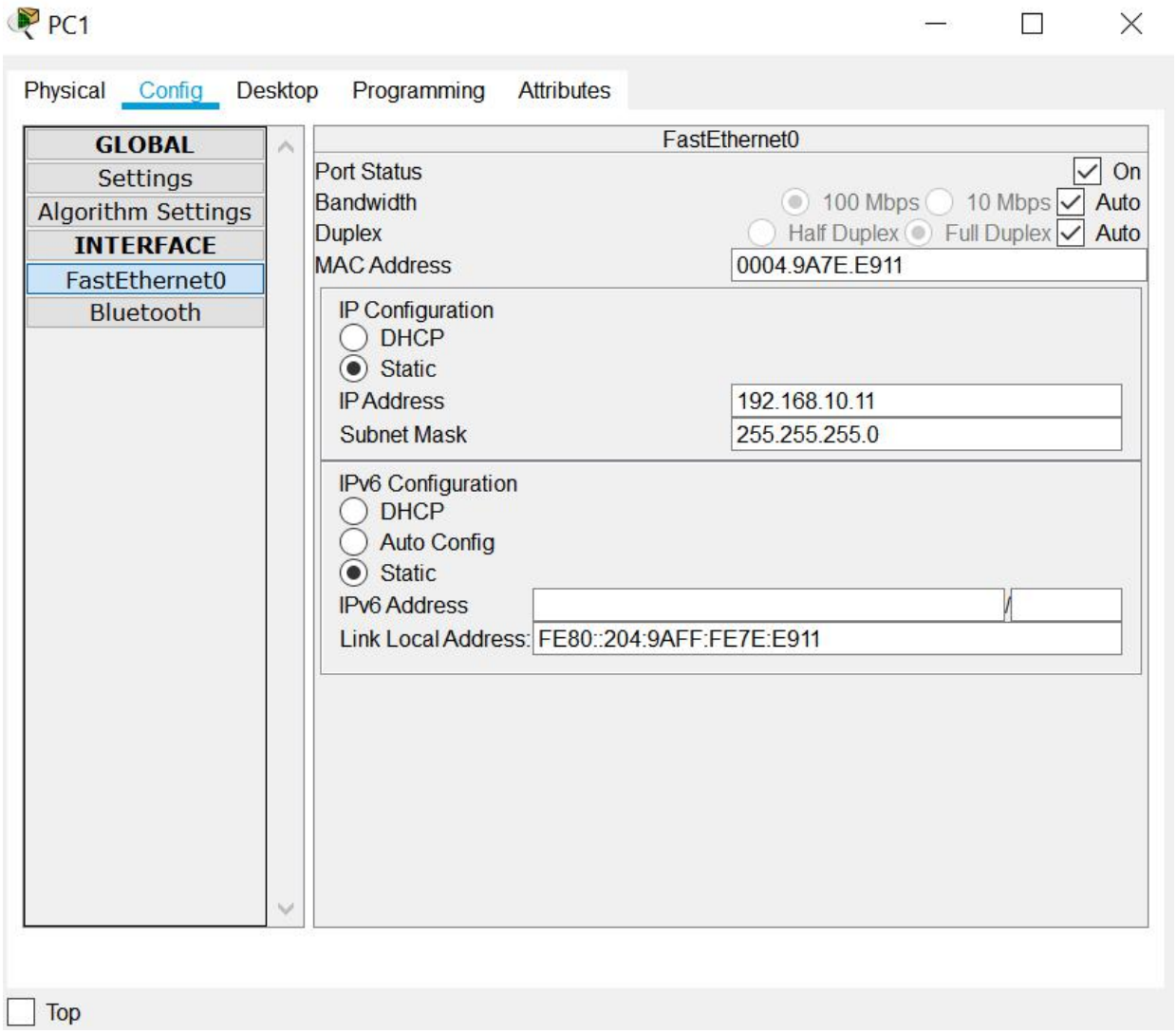


c) Configure PC0 using the **Config** tab in the PC0 configuration window:

   a. IP address: 192.168.10.10
   b. Subnet Mask 255.255.255.0

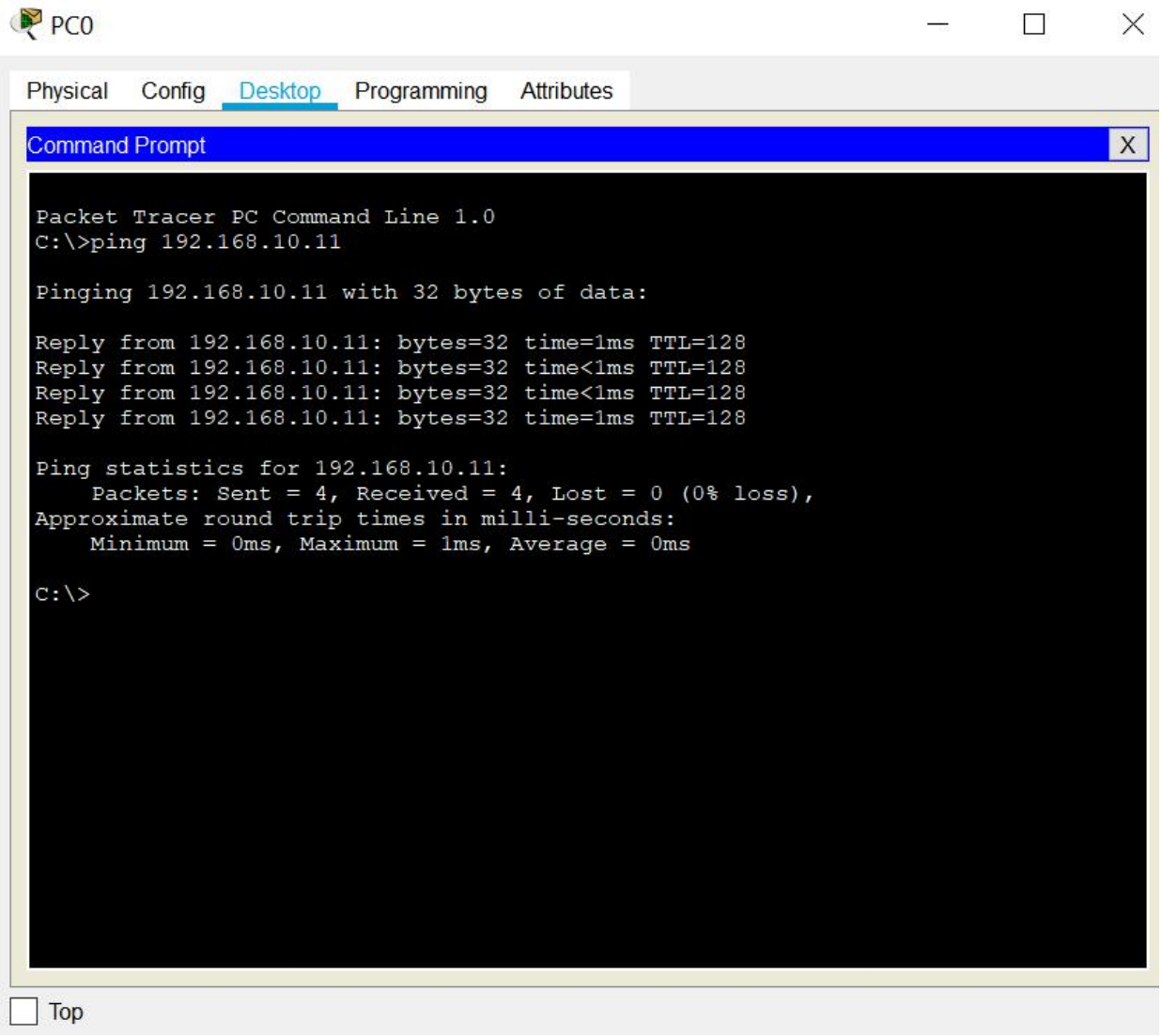


d) Configure PC1 using the **Config** tab in the PC1 configuration window
   a. IP address: 192.168.10.11
   b. Subnet Mask 255.255.255.0



Step 2: Test connectivity from PC0 to PC1

a) Use the **ping** command to test connectivity.
   a. Click PC0.
   b. Choose the **Desktop** tab.
   c. Choose **Command Prompt**.
   d. Type: **ping 192.168.10.11** and press *enter*.



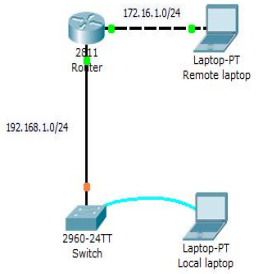
b) A successful **ping** indicates the network was configured correctly and the prototype validates the hardware and software configurations. A successful ping should resemble the below output:
c) Close the configuration window.
d) Click the **Check Results** button at the bottom of the instruction window to check your work.

Congratulations on completing this activity!

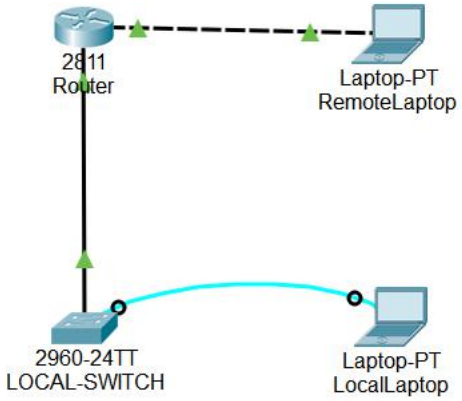
CEL51, DCCN, Monsoon 2020

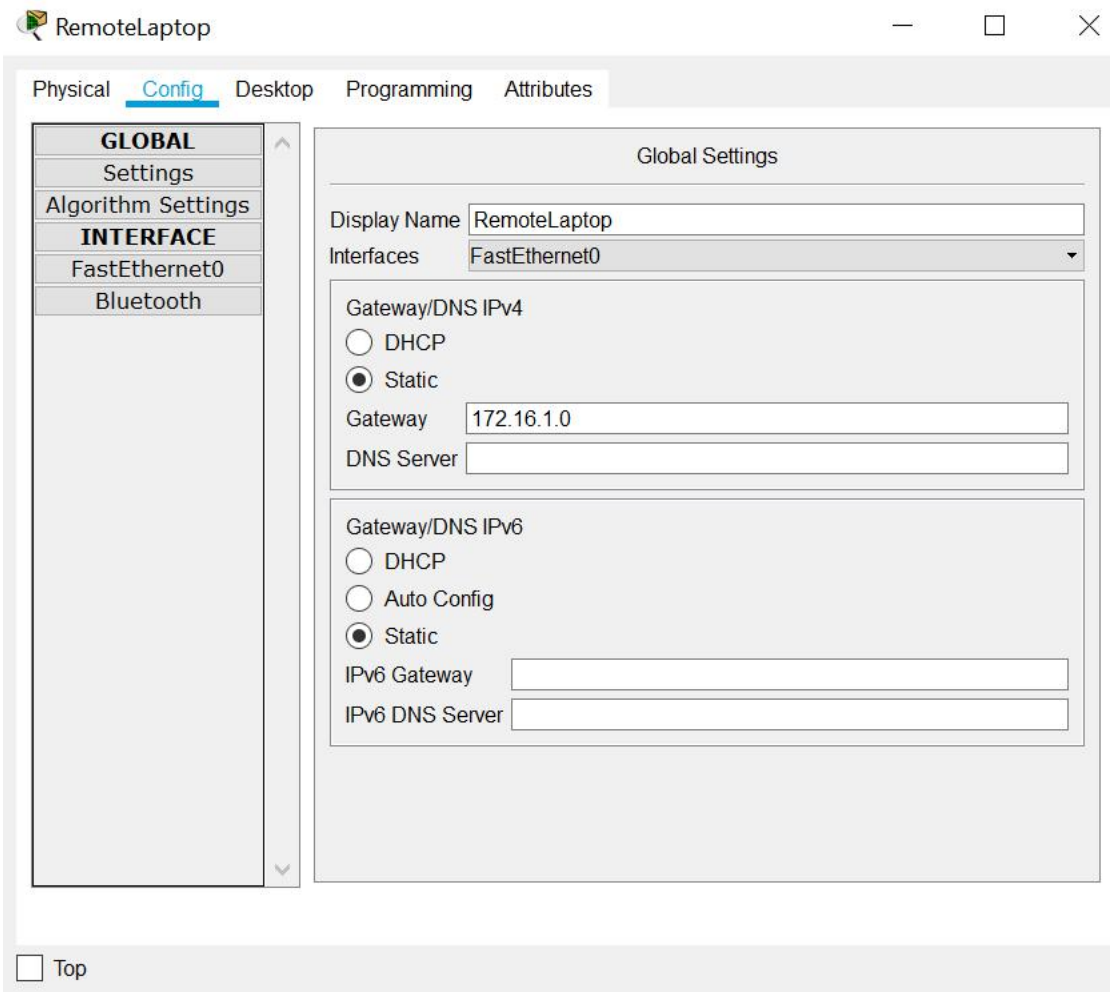
Lab 4.1: Basic configuration - hostname, motd banner, passwd etc

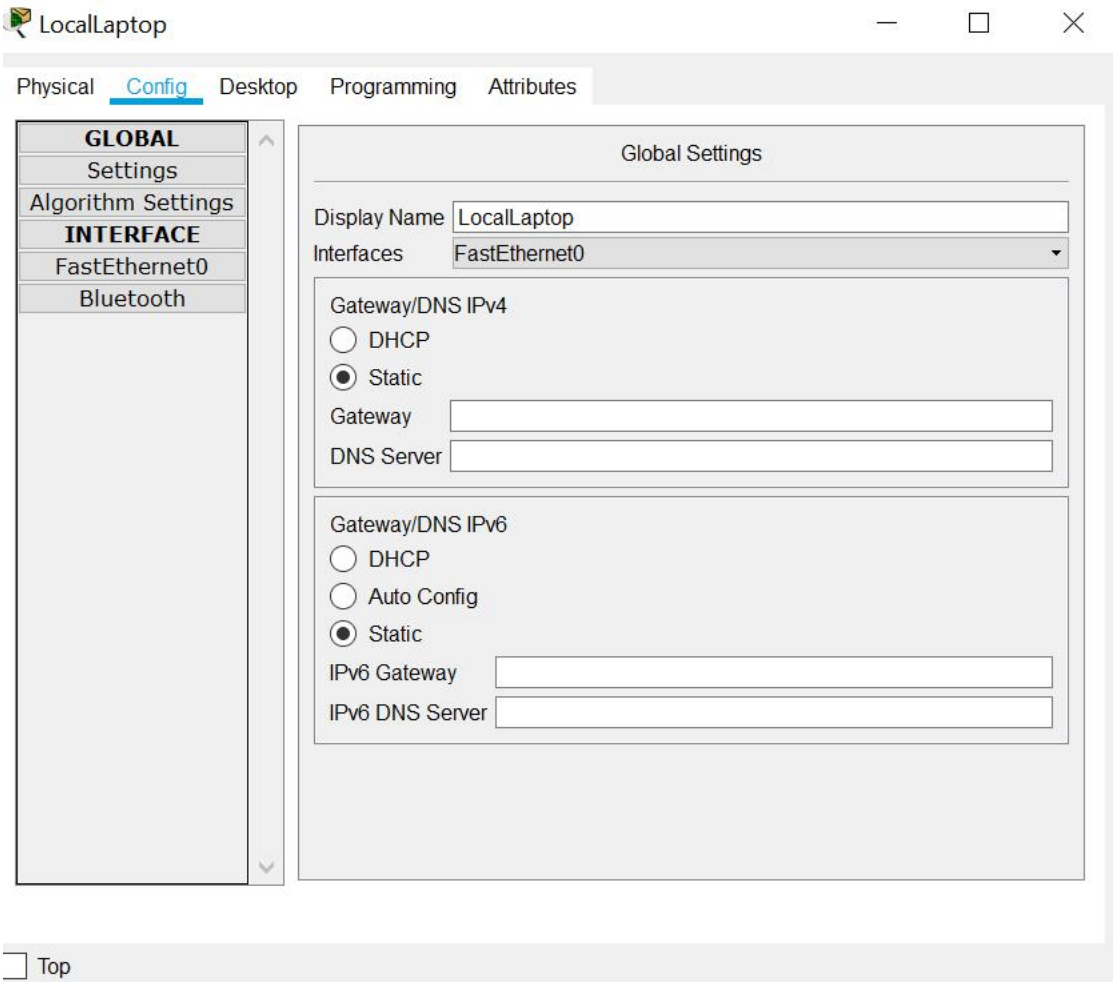
Objective:
This lab will test your ability to configure basic settings such as hostname, motd banner, encrypted passwords, and terminal options on a Packet Tracer 6.2 simulated Cisco Catalyst switch.

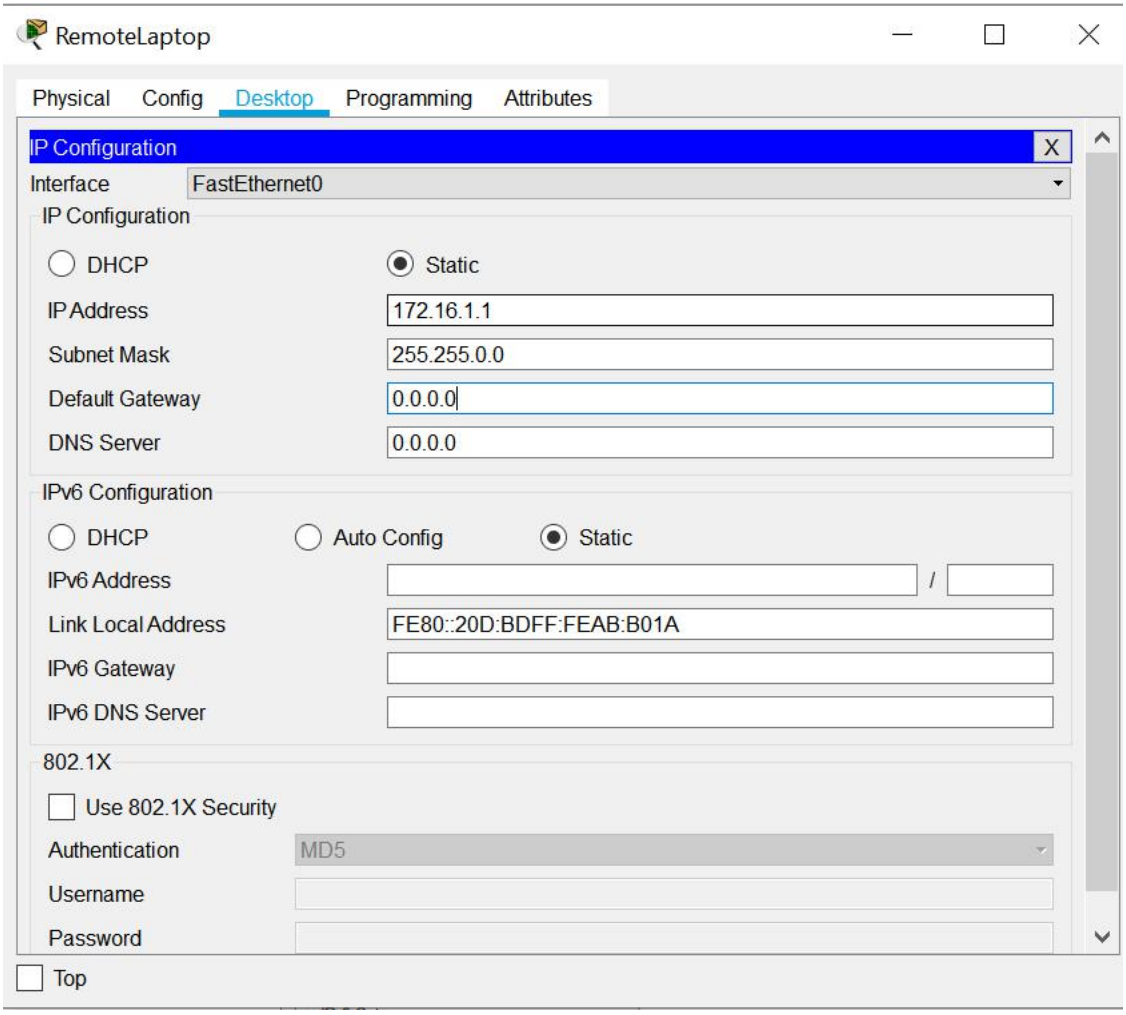


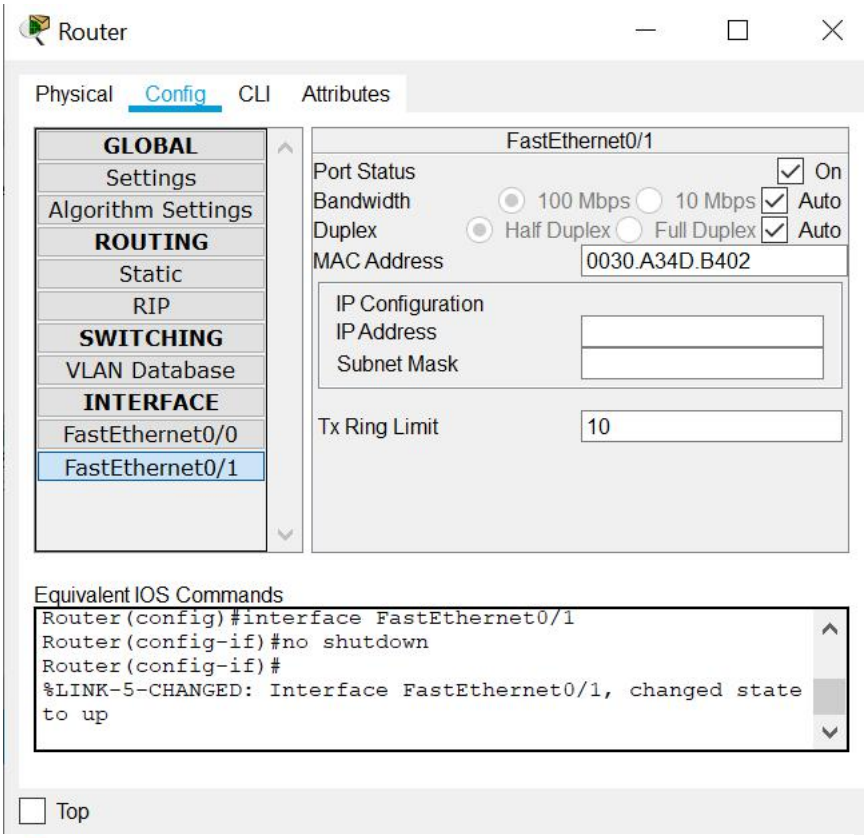
1. Use the local laptop connect to the switch console.

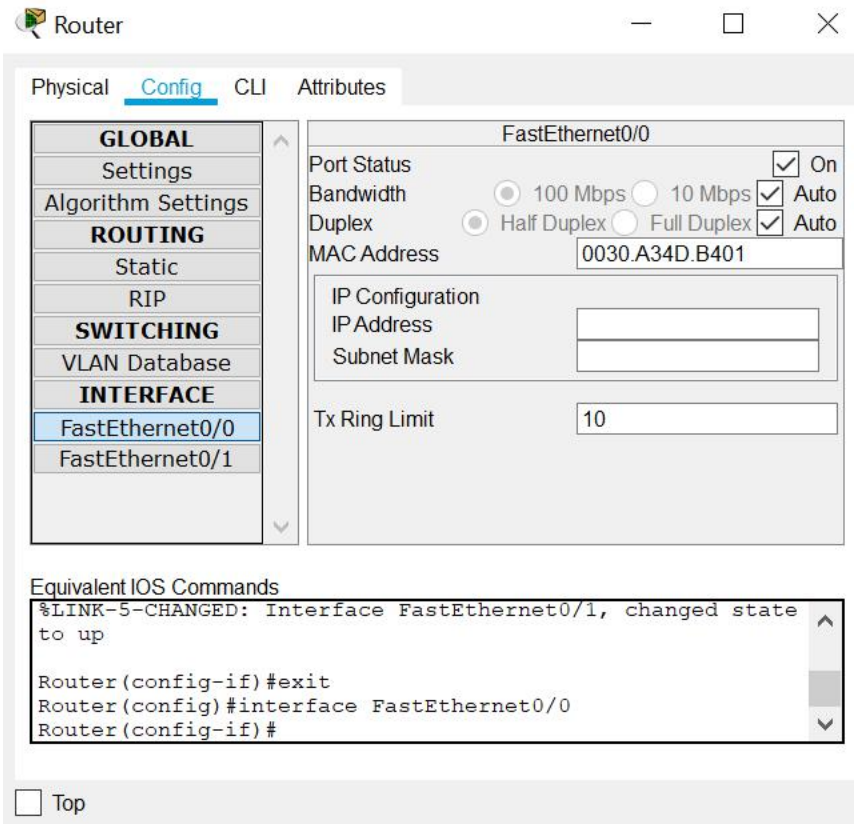



RemoteLaptop
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
Global Settings
Display Name
RemoteLaptop
Interfaces
FastEthernet0
Gateway/DNS IPv4
DHCP
Static
Gateway
172.16.1.0
DNS Server
Gateway/DNS IPv6
DHCP
Auto Config
Static
IPv6 Gateway
IPv6 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
Gateway
DNS Server
Gateway/DNS IPv6
DHCP
Auto Config
Static
IPv6 Gateway
IPv6 DNS Server
Top


RemoteLaptop
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
172.16.1.1
Subnet Mask
255.255.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::20D:BDFF:FEAB:B01A
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top





2. Configure Switch hostname as LOCAL-SWITCH

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#hostname LOCAL-SWITCH
LOCAL-SWITCH(config)#
```

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

```
LOCAL-SWITCH(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Unauthorized access is forbidden#

LOCAL-SWITCH(config)#
```

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

```
LOCAL-SWITCH(config)#enable secret cisco
LOCAL-SWITCH(config)#exit
LOCAL-SWITCH#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
LOCAL-SWITCH#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
LOCAL-SWITCH(config)#service password-encryption
LOCAL-SWITCH(config)#
```

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

```
LOCAL-SWITCH>enable
Password:
LOCAL-SWITCH#config
Configuring from terminal, memory, or network [terminal]?
terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
LOCAL-SWITCH(config)#line con 0
LOCAL-SWITCH(config-line)#password ciscoc
LOCAL-SWITCH(config-line)#logging synchronous
LOCAL-SWITCH(config-line)#login
LOCAL-SWITCH(config-line)#history size 15
LOCAL-SWITCH(config-line)#exec-timeout
% Incomplete command.
LOCAL-SWITCH(config-line)#exec-timeout 6 45
LOCAL-SWITCH(config-line)#
```

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

```
LOCAL-SWITCH(config-line)#line vty 0 15
LOCAL-SWITCH(config-line)#exec-timeout 8 20
LOCAL-SWITCH(config-line)#password ciscot
LOCAL-SWITCH(config-line)#logging synchronous
LOCAL-SWITCH(config-line)#login
LOCAL-SWITCH(config-line)#history size 15
LOCAL-SWITCH(config-line)#
```

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

```
LOCAL-SWITCH(config-if)#ip address 192.168.1.2
255.255.255.0
LOCAL-SWITCH(config-if)#ip default-gateway 192.168.1.1
LOCAL-SWITCH(config)#
```

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

```
LOCAL-SWITCH(config)#interface Vlan1
LOCAL-SWITCH(config-if)#no shutdown

LOCAL-SWITCH(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
to up
```

```
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.1.2
Trying 192.168.1.2 ...OpenUnauthorized access is forbidden


User Access Verification

Password:
LOCAL-SWITCH>enable
Password:
LOCAL-SWITCH#exit

[Connection to 192.168.1.2 closed by foreign host]
```