Experiment 3

Harsh Sandesara
Batch C, 49
UID: 2018130045

CEL 51, DCCN, Monsoon 2020

Lab 4: Prototyping a Network

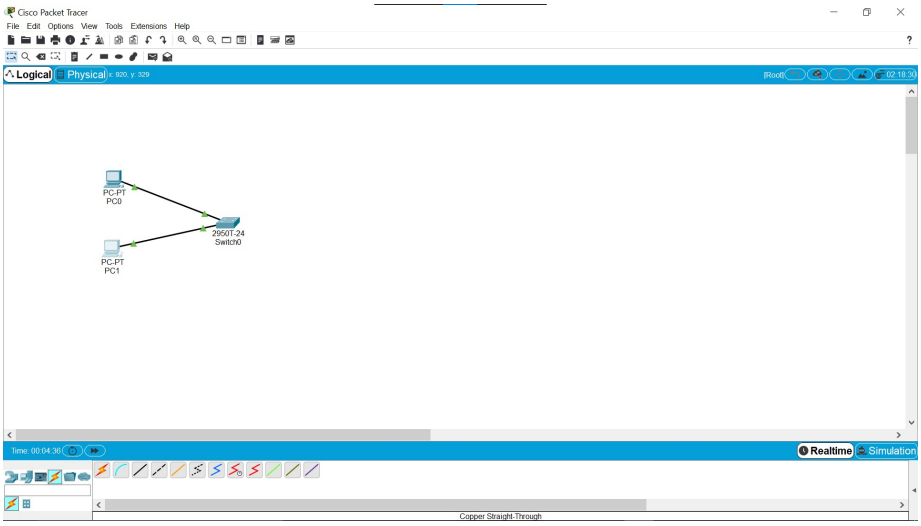
Objective:
Prototype a network using Packet Tracer

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

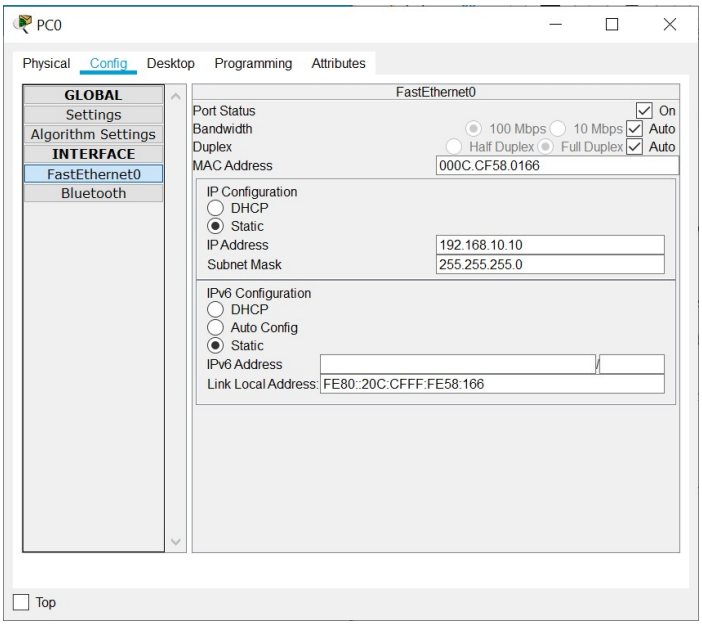
a) Add two PCs and a Cisco 2950T switch

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



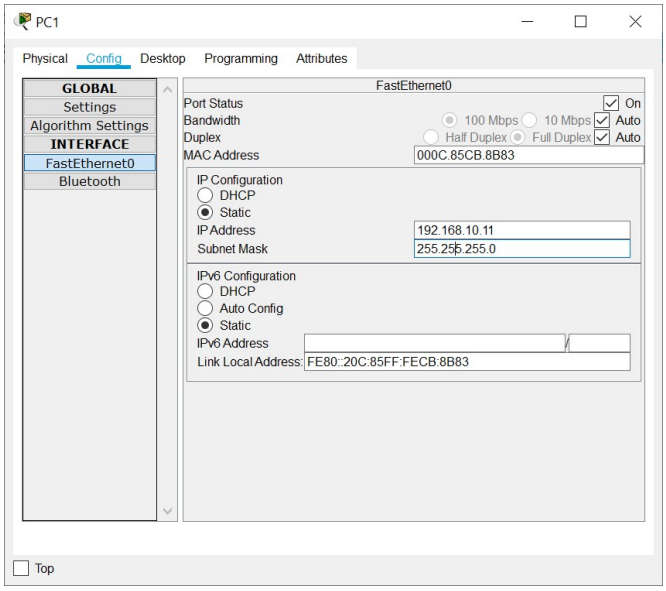
c) Configure PC0 using the **Config** tab in the PC0 configuration window:

   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

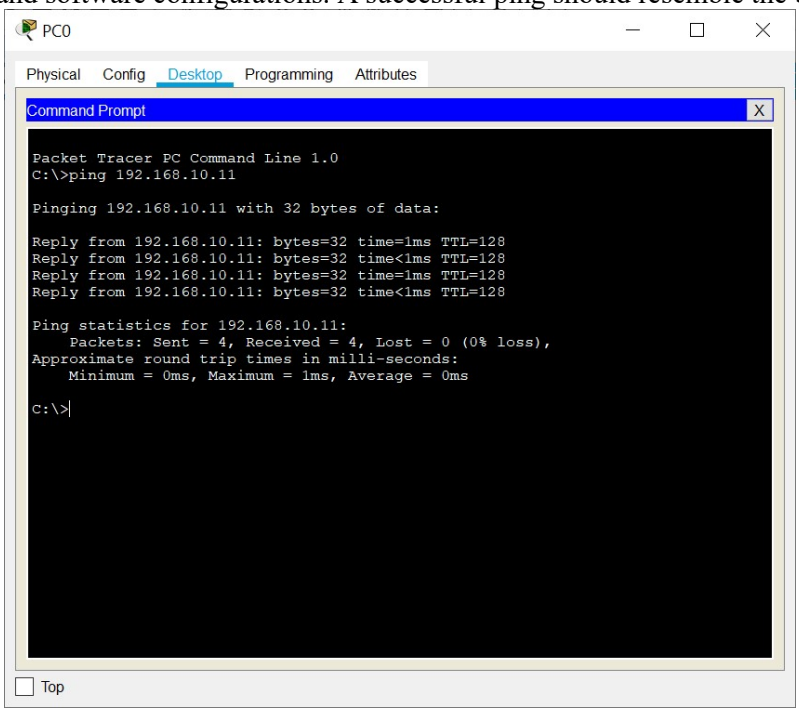
a. IP address: 192.168.10.11
b. Subnet Mask 255.255.255.0



Step 2: Test connectivity from PC0 to PC1

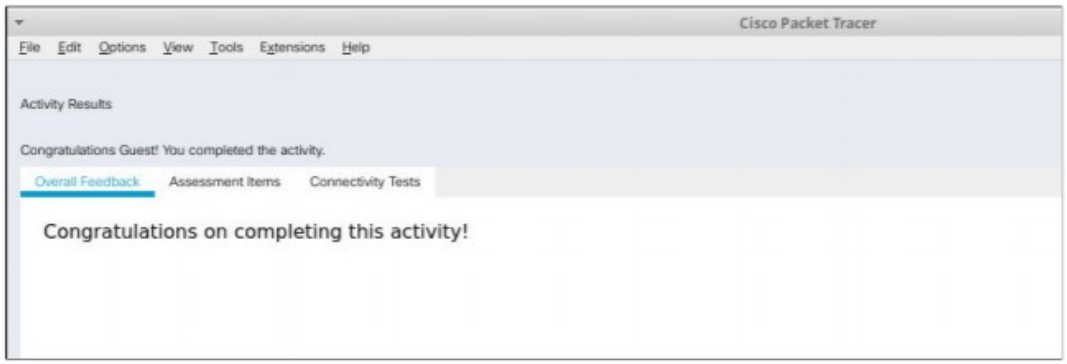
a) Use the **ping** command to test connectivity.
a. Click PC0.
b. Choose the **Desktop** tab.
c. Choose **Command Prompt**.
d. Type: **ping 192.168.10.11** and press *enter*.

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..

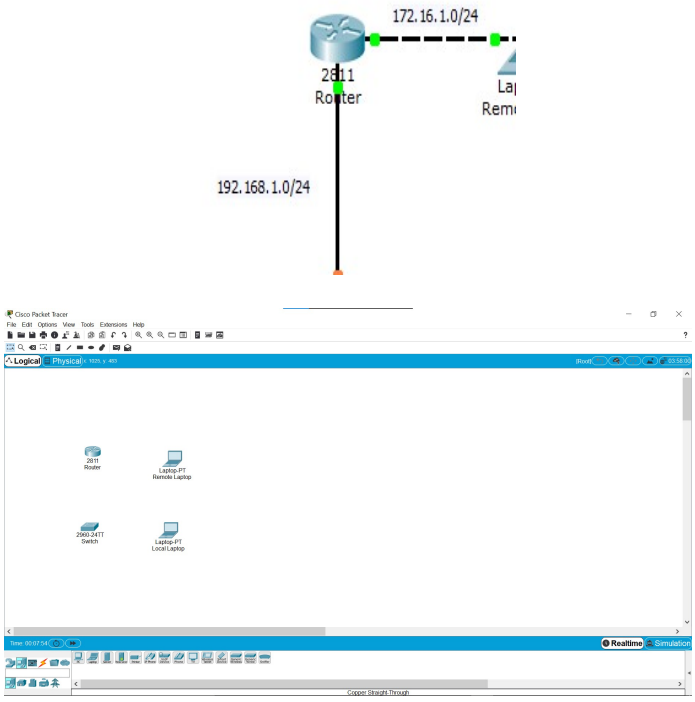


CEL51, DCCN, Monsoon 2020

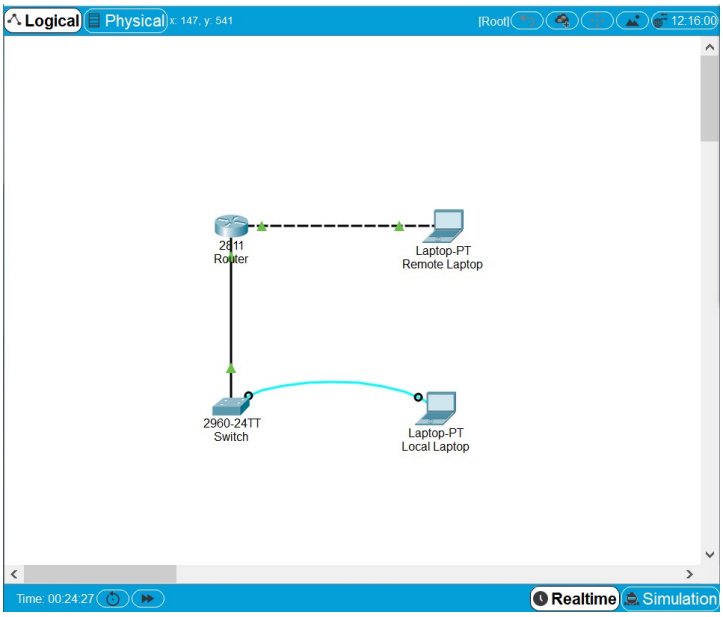
Lab 4.1: Basic configuration - hostname, motd banner, passwd etc

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.

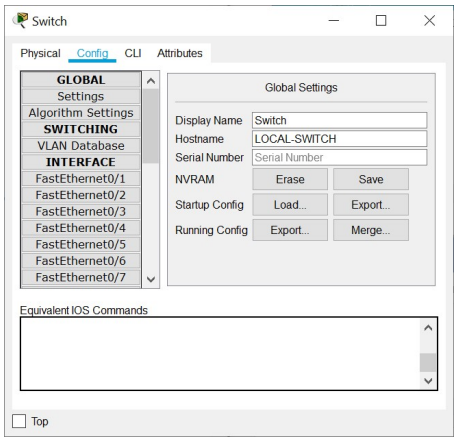


1. Use the local laptop connect to the switch console.



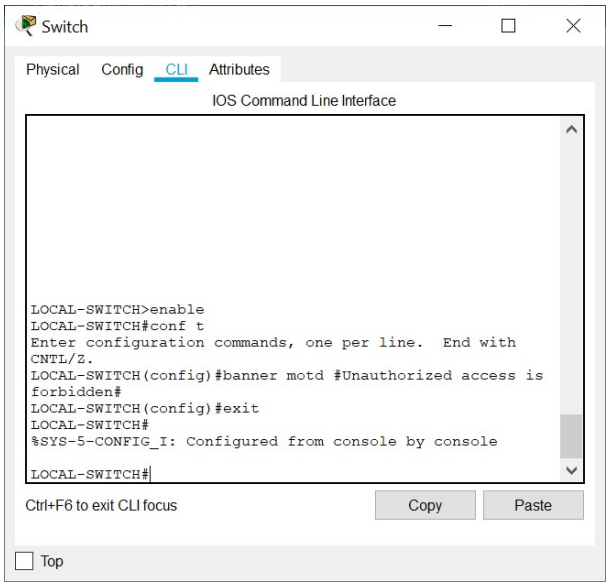
Network set up

2. Configure Switch hostname as LOCAL-SWITCH

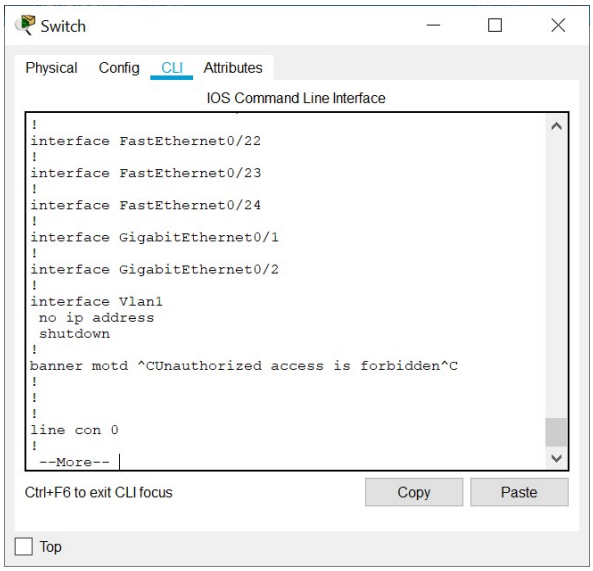


Host name configured

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

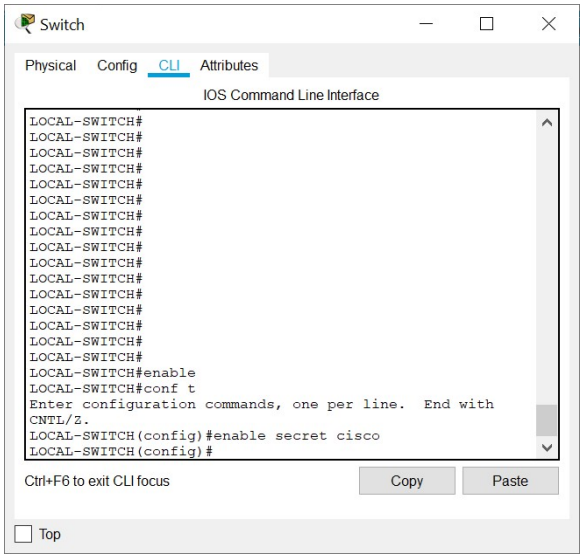


Banner message (MOTD) set



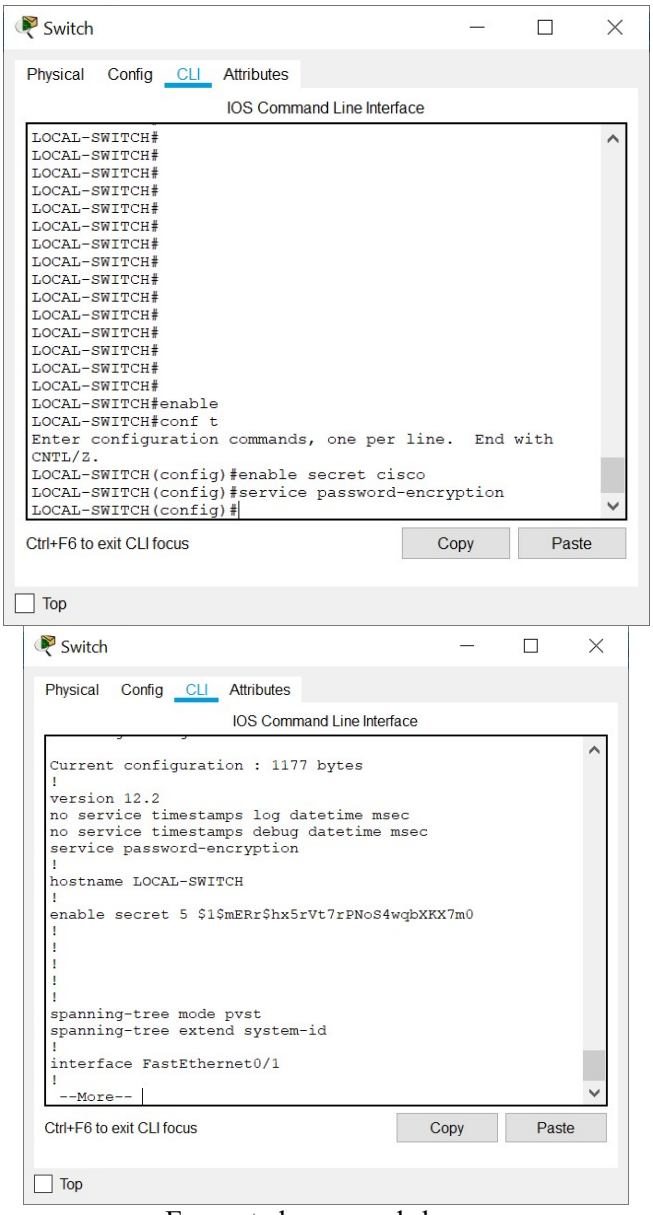
Banner message shown

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

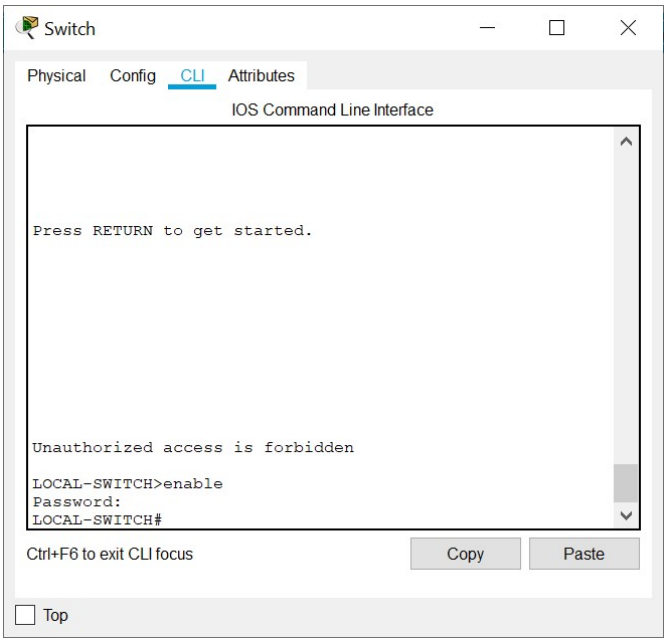


Password set and md5 encrypted

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

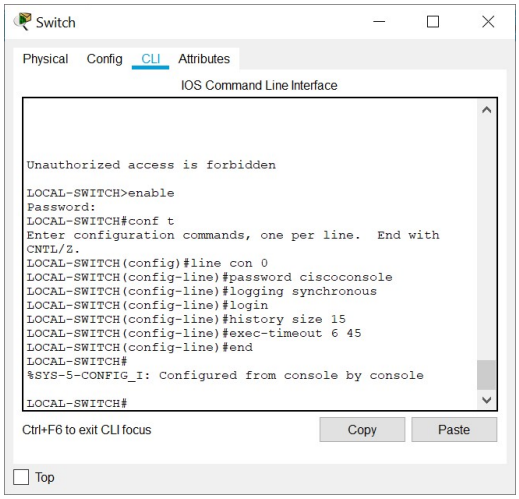


Encrypted password shown

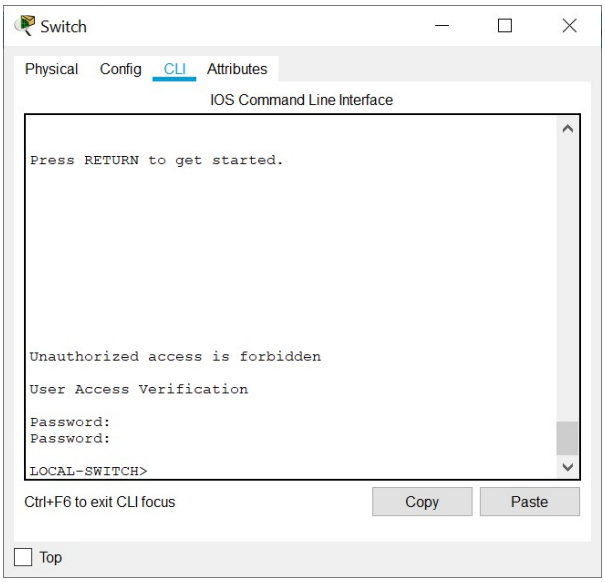


Password set up shown

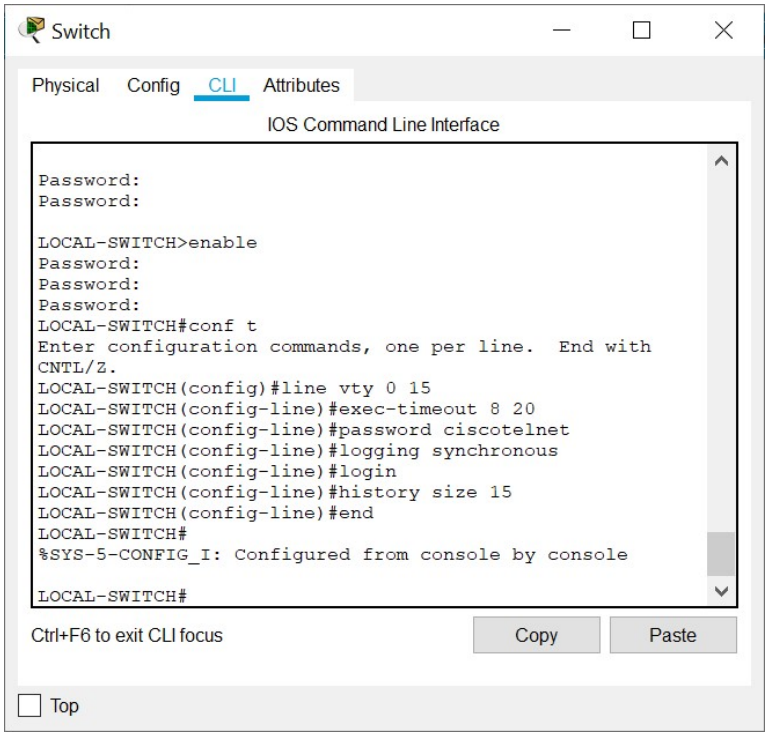
6. Configure CONSOLE access with the following settings :
- Login enabled
- Password : whatever you like
- History size : 15 commands
- Timeout : 6'45"
- Synchronous logging



Login enabled, password set up, synchronised login, set history size to 15 and timeout to 6 min 45 sec

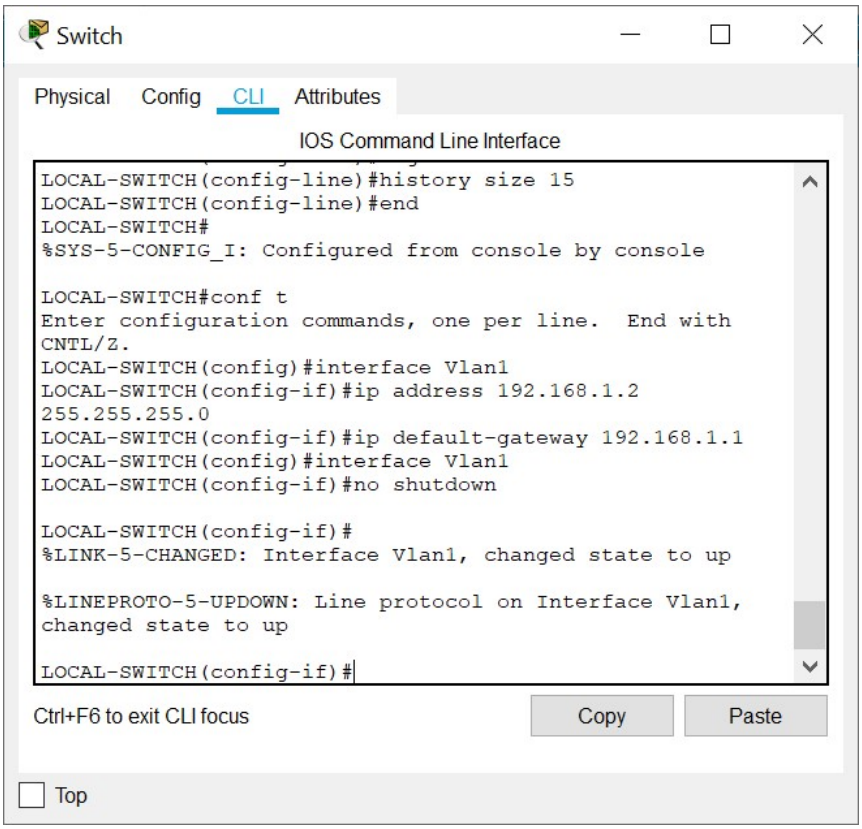


6. Configure TELNET access with the following settings :
- Login enabled
- Password : whatever you like
- History size : 15 commands
- Timeout : 8'20"
- Synchronous logging



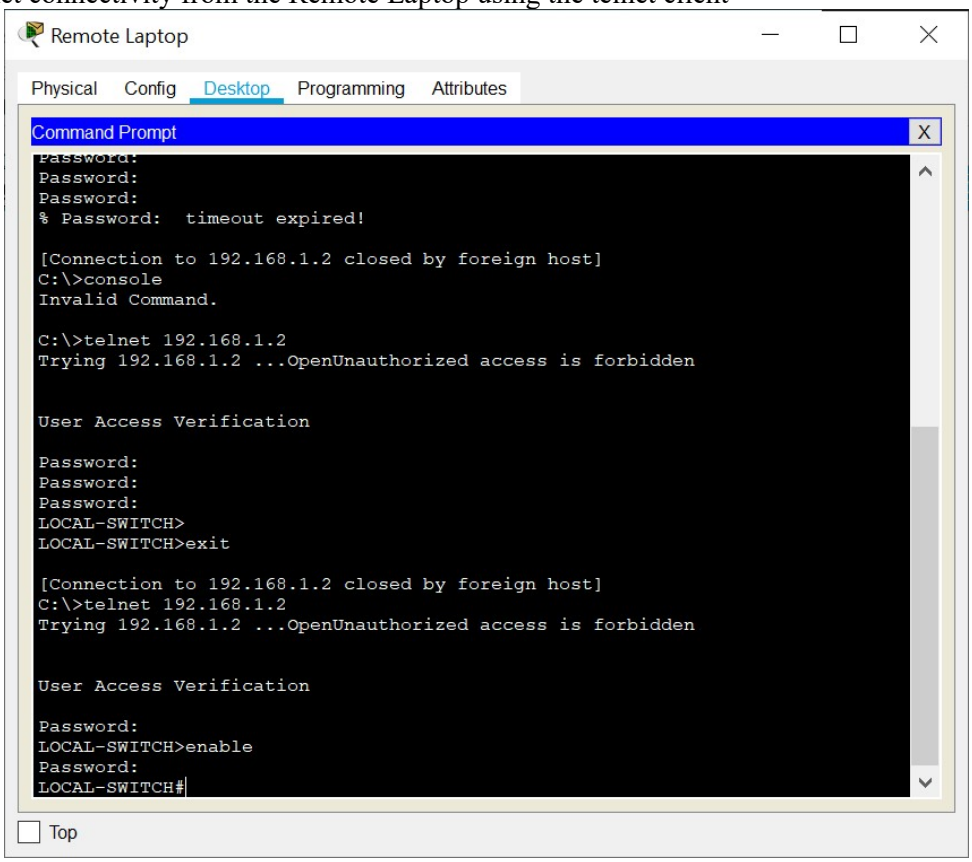
Telnet configured, login enabled, history size set to 15, timeout set to 8 min 20 sec, synchronised login

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

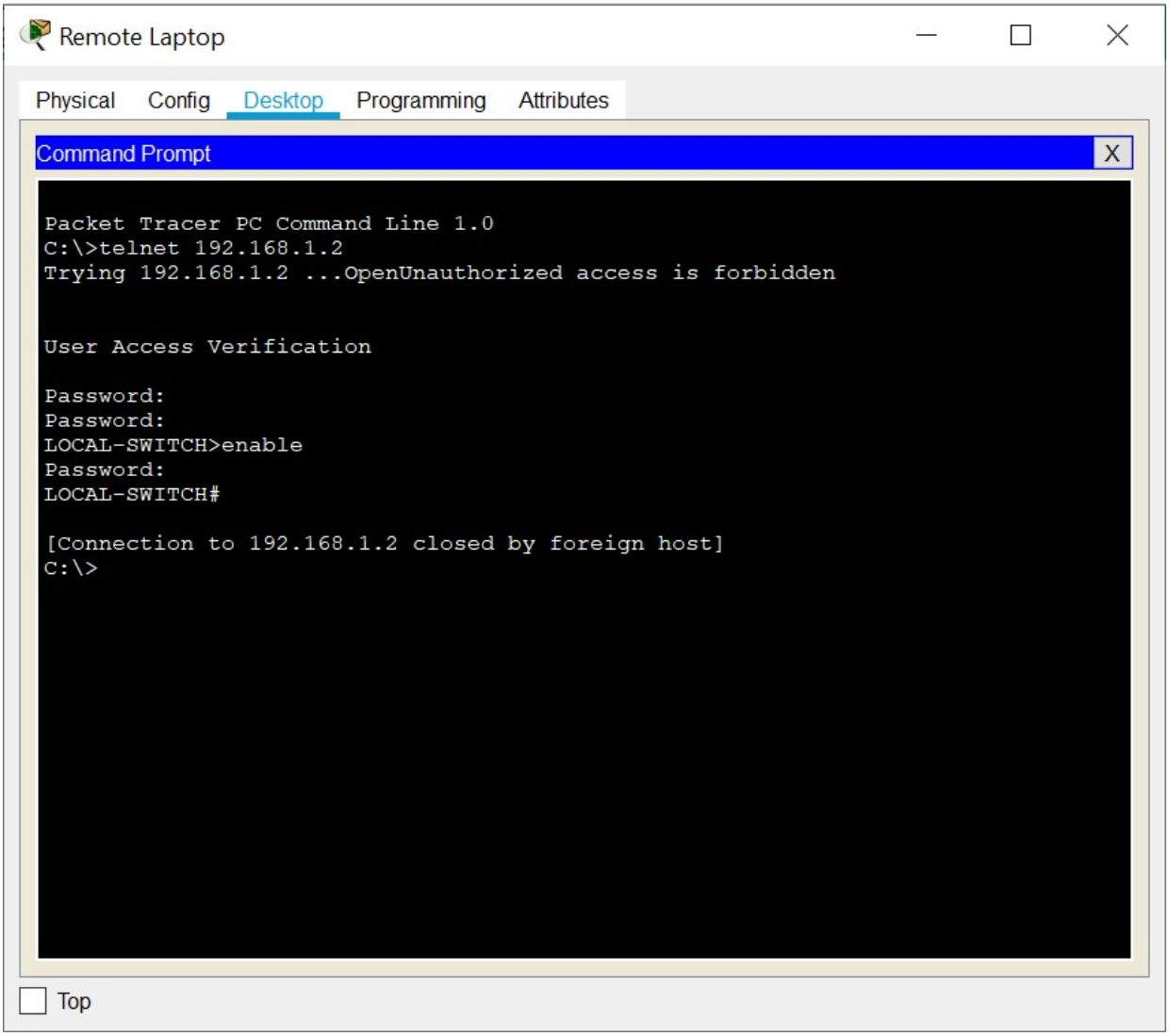


IP address and default gateway configured

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



Testing telnet connectivity



Telnet connection ended by host after timeout period elapses