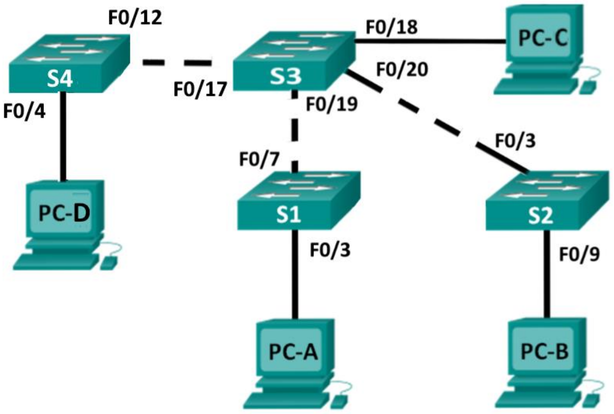
Lab 3 Activity 3.1 – Configuring a small network (Physical Lab)

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
PC-A	NIC	192.168.1.33	255.255.255.0
PC-B	NIC	192.168.1.65	255.255.255.0
PC-C	NIC	192.168.1.97	255.255.255.0
PC-D	NIC	192.168.1.121	255.255.255.0
S1	VLAN 1	192.168.1.1	255.255.255.0
S2	VLAN 1	192.168.1.2	255.255.255.0
S3	VLAN 1	192.168.1.3	255.255.255.0
S4	VLAN 1	192.168.1.4	255.255.255.0

Note:

This on-campus laboratory is intended to be completed in groups of 3 or 4. You will require 3 or 4 switches and 3 or 4 PCs and configure one each.

Objectives

Part 1: Configure Basic Network Devices

Part 2: Verify and Test Network Connectivity

Background / Scenario

Cisco switches have a special interface, known as a Switch Virtual Interface (SVI). The SVI can be configured with an IP address, commonly referred to as the management address. The management address is used for remote access to the switch to display or configure settings.

In this lab, you will build a simple network using Ethernet LAN cabling and access Cisco switches using the console and remote access methods. You will configure basic switch settings, IP addressing, and demonstrate the use of a management IP address for remote switch management.

Part 1: Configure Basic Network Devices

In Part 1, you will set up the network and configure basic settings, such as hostnames, interface IP addresses, and passwords.

Step 1: Create the network

Create the network based on the topology. Refer to Lab 2 if you need a refresher on how to do this and use your journal notes.

Step 2: Cable the network.

Cable the network as shown in the topology.

Establish a console connection to Switch S1 from PC-A.

Establish a console connection to Switch S2 from PC-B.

Establish a console connection to Switch S3 from PC-C.

Establish a console connection to Switch S4 from PC-D.

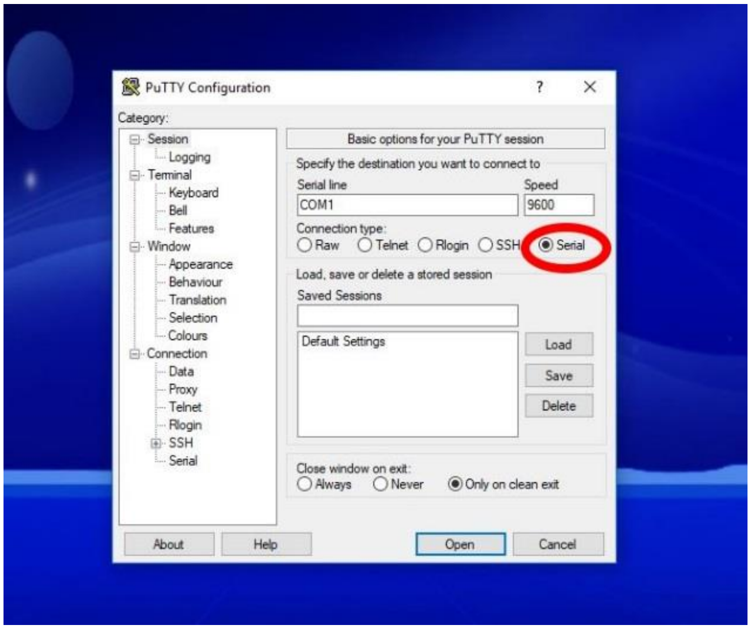
Note: Do not remove the console cables as they form part of the network that will be checked.

Step 3: Configure basic switch settings.

In this step, you will configure basic switch settings, such as hostname, and configure an IP address for the SVI.

Assigning an IP address on the switch is only the first step. As the network administrator, you must specify how the switch will be managed. Telnet and SSH are two of the most common management methods. However, Telnet is a very insecure protocol. All information flowing between the two devices is sent in plaintext. Passwords and other sensitive information can be easily viewed if captured by a packet sniffer. In practice you would not use telnet but would configure SSH instead. For now, for the purposes of demonstrating connectivity, we will be using telnet for this activity. We will investigate SSH later in the course. In order to configure the switch for use via Telnet, we first have to configure it using the console cable.

Connect PC-A to switch S1 using the console cable and PuTTY.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM1

Speed: 9600

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

The prompt will be `Switch>`. Enter privileged EXEC mode.

```
Switch> enable
Switch#
```

Enter global configuration mode and assign the switch hostname.

```
Switch# configure terminal
Switch(config)# hostname S1
S1(config)#
```

Configure the switch password access.

```
S1(config)# enable secret class
S1(config)#
```

Prevent unwanted DNS lookups.

```
S1(config)# no ip domain-lookup
S1(config)#
```

Configure a login MOTD banner.

```
S1(config)# banner motd 'Unauthorised access is strictly prohibited.'
```

In global configuration mode to set the SVI IP address to allow remote switch management.

(depending on which PC and Switch you configure in your group select the corresponding IP addresses)

```
S1#(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.1 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)#
```

Restrict console port access. The default configuration is to allow all console connections with no password needed.

```
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# logging synchronous
S1(config-line)# exit
S1(config)#
```

Configure the VTY line for the switch to allow Telnet access. If you do not configure a VTY password, you will not be able to telnet to the switch.

```
S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# logging synchronous
S1(config-line)# end
S1#
```

Step 4: Configure an IP address on PC-A.

Assign the IP address and subnet mask to the PC, as shown in the Addressing Table.

Step 5: Verify the configurations for PC-A and switch S1

(depending on which PC and Switch you have configured note the corresponding IP addresses etc)

Display the S1 device configuration.

Return to your console connection using the terminal program on PC-A. Issue the **show run** command to display and verify your switch configuration. A sample configuration is shown below. The settings you configured are highlighted in yellow. The other configuration settings are IOS defaults.

```
S1# show run
Building configuration...

Current configuration : 1508 bytes
!
! Last configuration change at 00:06:11 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
```

```
<output omitted>

interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.1 255.255.255.0
!
ip http server
ip http secure-server
!
banner motd ^C
Unauthorised access is strictly prohibited.^C
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Verify the status of your SVI management interface. Your VLAN 1 interface should be up/up and have an IP address assigned. Notice that switch port F0/3 is also up because PC-A is connected to it and port 7 is up because it connects to switch S3. Because all switch ports are initially in VLAN 1, by default, you can communicate with the switch using the IP address you configured for VLAN 1.

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.1     YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  up                    up
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  down                  down
FastEthernet0/6        unassigned      YES unset  down                  down
FastEthernet0/7        unassigned      YES unset  up                    up
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
```

```
FastEthernet0/15       unassigned      YES unset  down                    down
FastEthernet0/16       unassigned      YES unset  down                    down
FastEthernet0/17       unassigned      YES unset  down                    down
FastEthernet0/18       unassigned      YES unset  down                    down
FastEthernet0/19       unassigned      YES unset  down                    down
FastEthernet0/20       unassigned      YES unset  down                    down
FastEthernet0/21       unassigned      YES unset  down                    down
FastEthernet0/22       unassigned      YES unset  down                    down
FastEthernet0/23       unassigned      YES unset  down                    down
FastEthernet0/24       unassigned      YES unset  down                    down
GigabitEthernet0/1     unassigned      YES unset  down                    down
GigabitEthernet0/2     unassigned      YES unset  down                    down
```

Step 6: Repeat Steps 3, 4, and 5 for the remaining PCs and switches

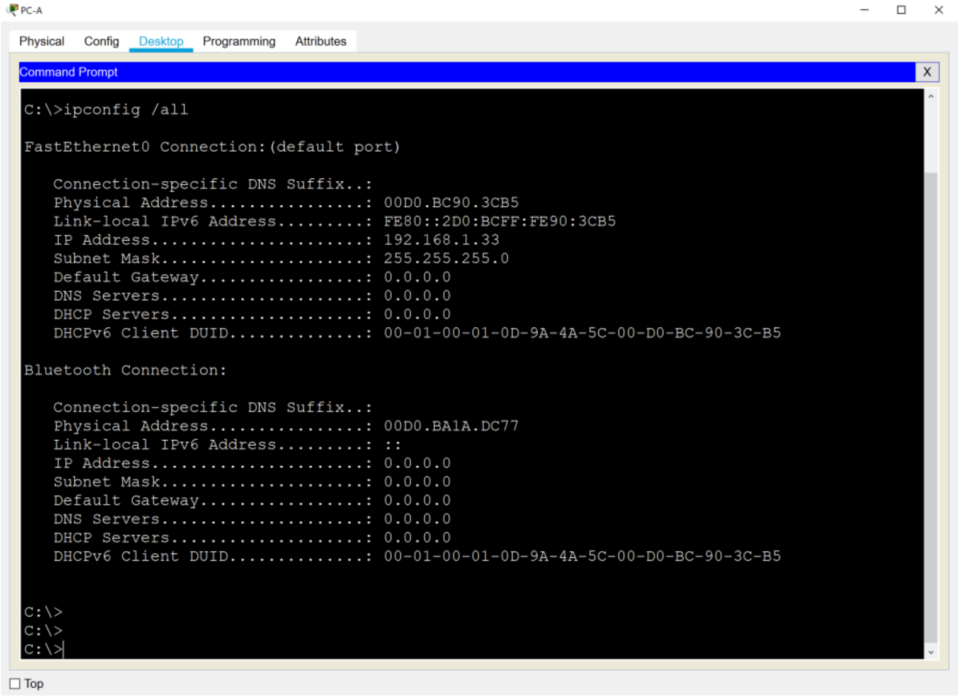
Configure and Check the remaining switches and PCs within your group as per the Addressing Table and the configuration instructions in steps 3, 4, and 5 above.

Part 2: Verify and Test Network Connectivity

You will now verify and document the switch configuration, test end-to-end connectivity between the PCs and the switches. Note that this part is normally assessed based on whether your network is configured correctly. Verifying connectivity is an important process and forms part of the troubleshooting activities that you will be performing when configuring a network. You will first test connectivity for S1, then repeat the steps to test connectivity for S2, S3, S4.

Step 1: Test end-to-end connectivity.

Open a command prompt window on PC-A. Verify the IP address of PC-A by using the **ipconfig /all** command. This command displays the PC hostname and the IPv4 address information.



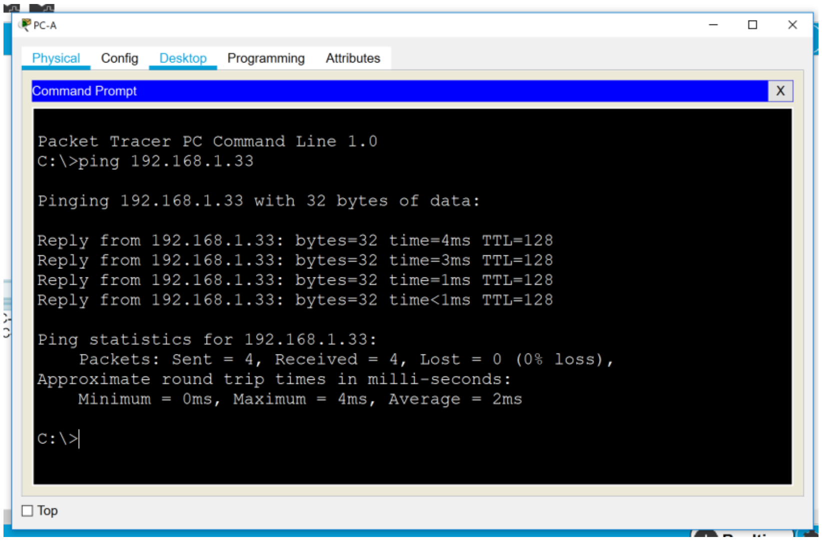
```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 00D0.BC90.3CB5
   Link-local IPv6 Address.........: FE80::2D0:BCFF:FE90:3CB5
   IP Address......................: 192.168.1.33
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 0.0.0.0
   DNS Servers.....................: 0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 Client DUID..............: 00-01-00-01-0D-9A-4A-5C-00-D0-BC-90-3C-B5

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 00D0.BA1A.DC77
   Link-local IPv6 Address.........: ::
   IP Address......................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: 0.0.0.0
   DNS Servers.....................: 0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 Client DUID..............: 00-01-00-01-0D-9A-4A-5C-00-D0-BC-90-3C-B5


C:\>
C:\>
C:\>
```

Ping PC-A's address and the management address of S1.

Ping the PC-A address first.

```
C:\Users\NetAcad> ping 192.168.1.33
```

Your output should be similar to the following screen:



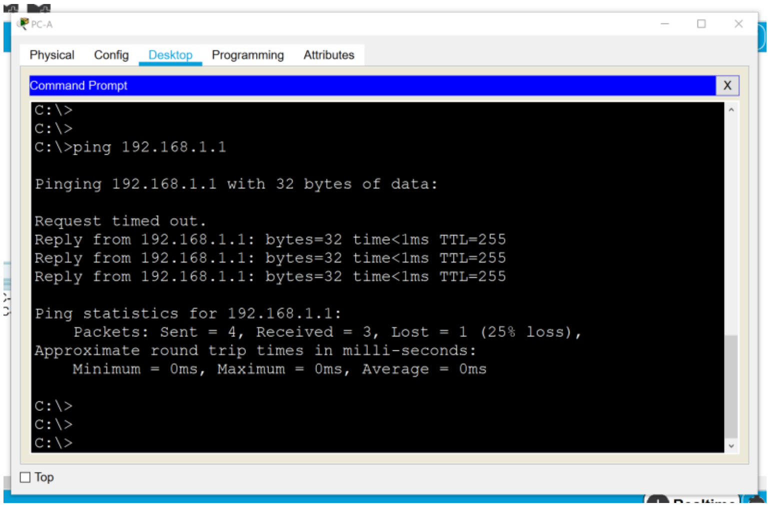
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=4ms TTL=128
Reply from 192.168.1.33: bytes=32 time=3ms TTL=128
Reply from 192.168.1.33: bytes=32 time=1ms TTL=128
Reply from 192.168.1.33: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 2ms

C:\>
```

From PC-A Ping the SVI management address of S1.

```
C:\Users\NetAcad> ping 192.168.1.1
```

Your output should be similar to the following screen. If no ping results are successful, troubleshoot the basic device configurations. You should check both the physical cabling and IP addressing if necessary.

Note: as in the example below, the first one or two ping results may fail as the connection may still be in the configuration process.

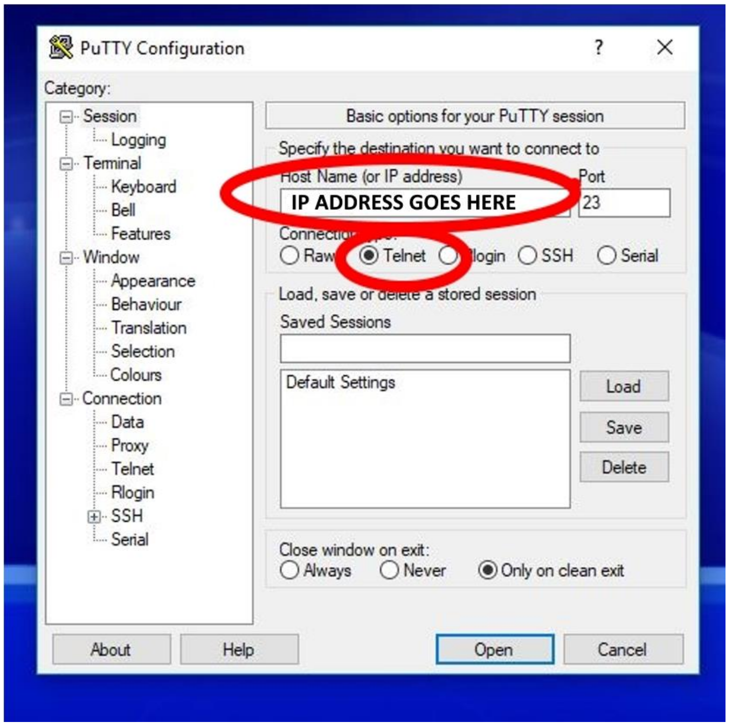


```
C:\>
C:\>
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
C:\>
C:\>
```

Step 2: Test and verify the remote management of S1.

You will now use Telnet to remotely access the switch S1 using the SVI management address. Telnet is not a secure protocol. However, you will use it in this lab to test remote access. All information sent by Telnet, including passwords and commands, is sent across the session in plaintext. In subsequent labs, you will use SSH to remotely access network devices.

Open a new Telnet/SSH window via PuTTY on PC-A. Select Telnet and enter the S1 VLAN1 IP address in the Hostname field to connect to S1 via the SVI management address. Click Connect.



PuTTY Configuration

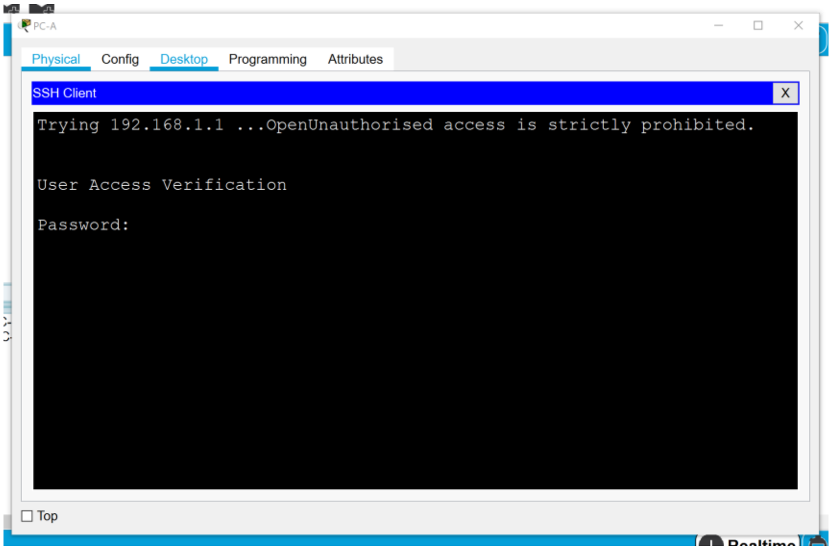
Host Name (or IP address): IP ADDRESS GOES HERE

Port: 23

Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

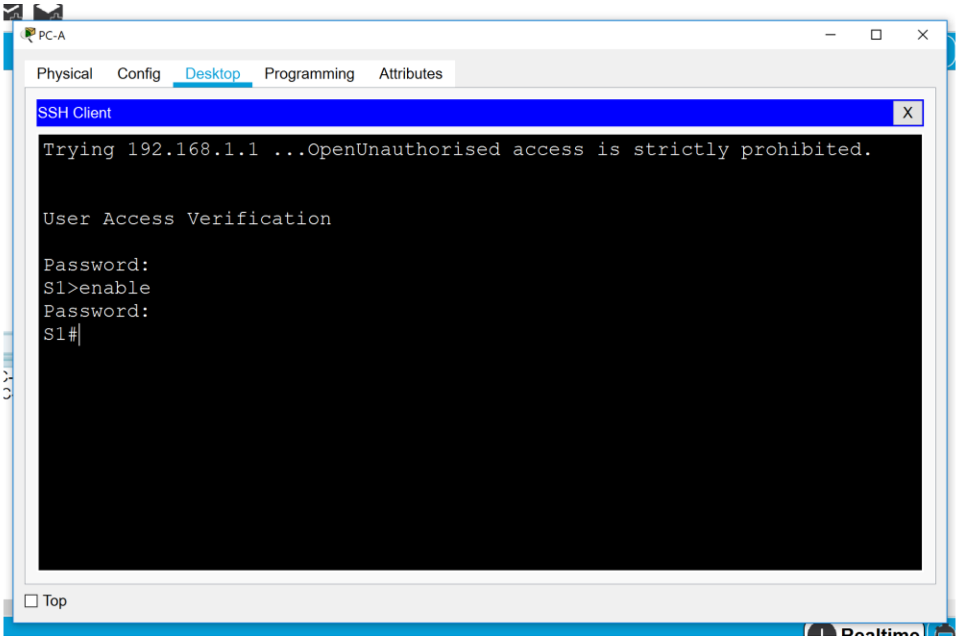
Close window on exit: ○ Always ○ Never ● Only on clean exit

In the diagram below, note the banner message at the top before the password prompt. The password is **cisco.**



```
Trying 192.168.1.1 ...OpenUnauthorised access is strictly prohibited.


User Access Verification

Password:
```

After entering the **cisco** password, you will be at the user EXEC mode prompt. Type **enable** at the prompt. Enter the **class** password to enter privileged EXEC mode and issue a **show run** command.



```
Trying 192.168.1.1 ...OpenUnauthorised access is strictly prohibited.


User Access Verification

Password:
S1>enable
Password:
S1#
```

You have now successfully connected to the Switch via Telnet. If you did not reach this stage perform troubleshooting until this step is successful.

Step 3: Test and verify the remote management of S2, S3, and S4.

a) Repeat Steps 1 and 2 to test the connectivity for PC-B to S2, PC-C to S3, PC-D to S4.

b) Test connectivity between PC-A and PC-B

c) Test connectivity between PC-A and PC-C

d) Test connectivity between PC-A and PC-D

Reflection

Why must you use a console connection to initially configure the switch? Why not connect to the switch via Telnet or SSH?

____

Can you also telnet to S1 from PC-B and PC-C? __________

Why?

____