# Experiment 1

**Aim**: Know your devices.

**Theory:**

- **Cables: -**

Figure: Cisco Netacad Cables

- **Straight Cable:**
  A straight through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router. This type of cable is also sometimes called a patch cable and is an alternative to wireless connections where one or more computers access a router through a wireless signal.

- **Crossover Cable:**
  The wire at pin 1 on one end of the cable connects to pin 3 at the other end of the cable. The wire at pin 2 connects to pin 6 on the other end of the cable. Remaining wires connect in the same positions at both ends.

- **Coaxial Cable:**
  A coaxial cable is an electrical cable with a copper conductor and an insulator shielding around it and a braided metal mesh that prevents signal interference and cross talk. Coaxial cable is also known as coax.

- **Data Terminal Equipment (DTE):**
  It is a device that is an information source or an information sink. It produces data and transfers them to a DCE, with essential control characters. Examples of DTE include computers, printers, and routers, etc.

- **Data Circuit Terminating Equipment (DCE):**
  It is a device used as an interface between a DTE. It converts signals to a format appropriate to transmission medium and introduces it onto network line. Examples of DCE include modem, ISDN adaptors, satellites, and network interface cards, etc.

- **Router:**
  A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.


- Figure: Router Options in Netacad

- **Switch:**

  A switch is a multiport bridge with a buffer and a design that can boost its efficiency (many ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it particularly effective because it only forwards good packets to the right port and does not transmit packets with problems.


Figure: Switch Options in Netacad

- ❖ The Cisco® Catalyst® 2960 Series is a family of fixed- configuration, standalone switches that provide Fast Ethernet and Gigabit Ethernet connectivity and support enhanced switching services, advanced security, IP communications, wireless networking, and scalable management.
- ❖ The Cisco Catalyst 2950 Series is a line of fixed-configuration, stackable, and standalone switches that provide wire-speed Fast Ethernet and Gigabit Ethernet connectivity.

- ❖ The Cisco® Catalyst® 3560 Series is a line of fixed-configuration, enterprise-class switches that include IEEE 802.3af and Cisco prestandard Power over Ethernet (PoE) functionality in Fast Ethernet and Gigabit Ethernet configurations.

- **Hub:**

  In essence, a hub is a multi-port repeater. A hub joins several wires that come from several branches, like the connector in a star topology that joins various stations. Data packets are delivered to all connected devices since hubs are unable to filter data. In other words, all hosts connected by Hub continue to share a single collision domain. Additionally, they lack the intelligence to choose the best route for data packets, which results in waste and inefficiency.

  ○ 


- Figure: Hub Options in Netacad

- **End Devices:**

  An end device is either the source or destination of a message transmitted over the network.

  - Computers (workstations, laptops, file servers, and web servers)
  - Network printers
  - VoIP phones
  - TelePresence endpoints


**Result:** Successfully studied all the devices.

# Experiment 2

**AIM:** To Configure initial Switch Settings.
**Devices Used**: Switches, PCs, and Cable**s**
**Objectives**
Part 1: Verify the Default Switch Configuration
Part 2: Configure a Basic Switch Configuration
Part 3: Configure a MOTD Banner
Part 4: Save Configuration Files to NVRAM
Part 5: Configure S2

Part 1: Verify the Default Switch Configuration

Step 1: Enter privileged EXEC mode.

Step 2: Examine the current switch configuration. Part 2: Create a Basic Switch Configuration

Step 1: Assign a name to a switch.

Step 2: Secure access to the console line.

Step 3: Verify that console access is secured.

Step 4: Secure privileged mode access.

Step 5: Verify that privileged mode access is secure.

Step 6: Configure an encrypted password to secure access to privileged mode.

Step 7: Verify that the enable secret password is added to the configuration file.
Step 8: Encrypt the enable and console passwords.

**Q.) What is Cisco Enable Secret Password (Encrypted Privileged Exec Password)?**
Ans) The "enable secret" password in Cisco networking refers to the password used to protect access to privileged EXEC mode, which is a higher level of command-line access with more advanced configuration and management capabilities. This password is used to restrict unauthorized users from gaining elevated privileges on Cisco networking devices, such as routers and switches.

**Q.) If** you **configure any more passwords on the switch, will they be displayed in the configuration file as plain text or in encrypted form? Explain.**
**Ans)** When we configure additional passwords on a Cisco switch or any other Cisco networking device, the passwords will be stored in the configuration file in encrypted form, not as plain text. This is a security measure to prevent unauthorized access to sensitive information, such as passwords, in case someone gains access to the configuration files.

Part 3: Configure a MOTD Banner

Step 1: Configure a message of the day (MOTD) banner.

Part 4: Save and Verify Configuration Files to NVRAM

Step 1: Verify that the configuration is accurate using the show run command.

**Q.) Why should every switch have a MOTD banner?**

**Ans**) A MOTD banner is a simple yet effective way to enhance the security, communication, and operational aspects of network device management.

Q.) **Which command will display the contents of NVRAM?**

**Ans**) show startup-config

**Q.) When will this banner be displayed?**

**Ans)** It's displayed at points where users are granted access to the device to ensure that they are aware of any relevant information before interacting with the system.

Par

t 5: Configure S2

**Procedure:** Open the activity through the Cisco Packet Tracer (2.5.5), and use the following commands.

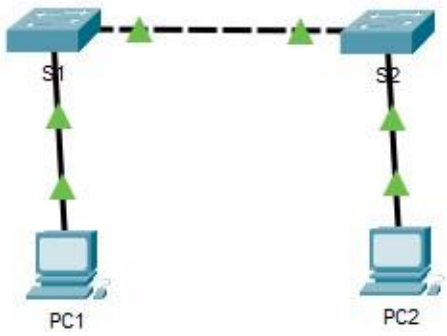



Fig. Diagram Representing connection between devices.

1) *enable*: It allows the user to enter EXEC mode, the prompt will change as shown in fig (1).

```
Switch>enable
Switch#
```

Figure 1: Switch EXEC mode

2) *show running config*: This allows the user to view the current configuration of the switch, it ranges from ethernet port to all the configurations of the switch.

```
Ashish#show running-config
Building configuration...

Current configuration : 1261 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Ashish
!
!
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password 7 08221D0A0A49
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
```

Figure 2: Switch configuration

3) *configure terminal*: It allows the user to configure the parameters of the terminal such as hostname, password, encryption etc.

```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#hostname Ashish
Ashish(config)#
```

Figure 3: Hostname configuration

4) *hostname*: It is used to configure the hostname parameter as shown in fig (3).

5) *password*: It is used to set the password to the console. Fig (4)

```
Ashish#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Ashish(config)#line console 0
Ashish(config-line)#password network
Ashish(config-line)#login
Ashish(config-line)#exit
Ashish(config)#exit
```

Figure 4: Login Password configuration

6) *login*: It is used after password command, to set the password for User Access Verification as shown in fig (5).

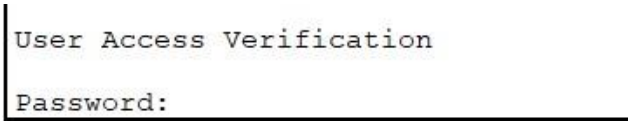



Figure 5: User Login Verification

7) *exit*: This allows the user to exit the EXEC mode, or CLI session.

8) *secret*: It is used to lock the EXEC mode of the terminal. Fig (6)

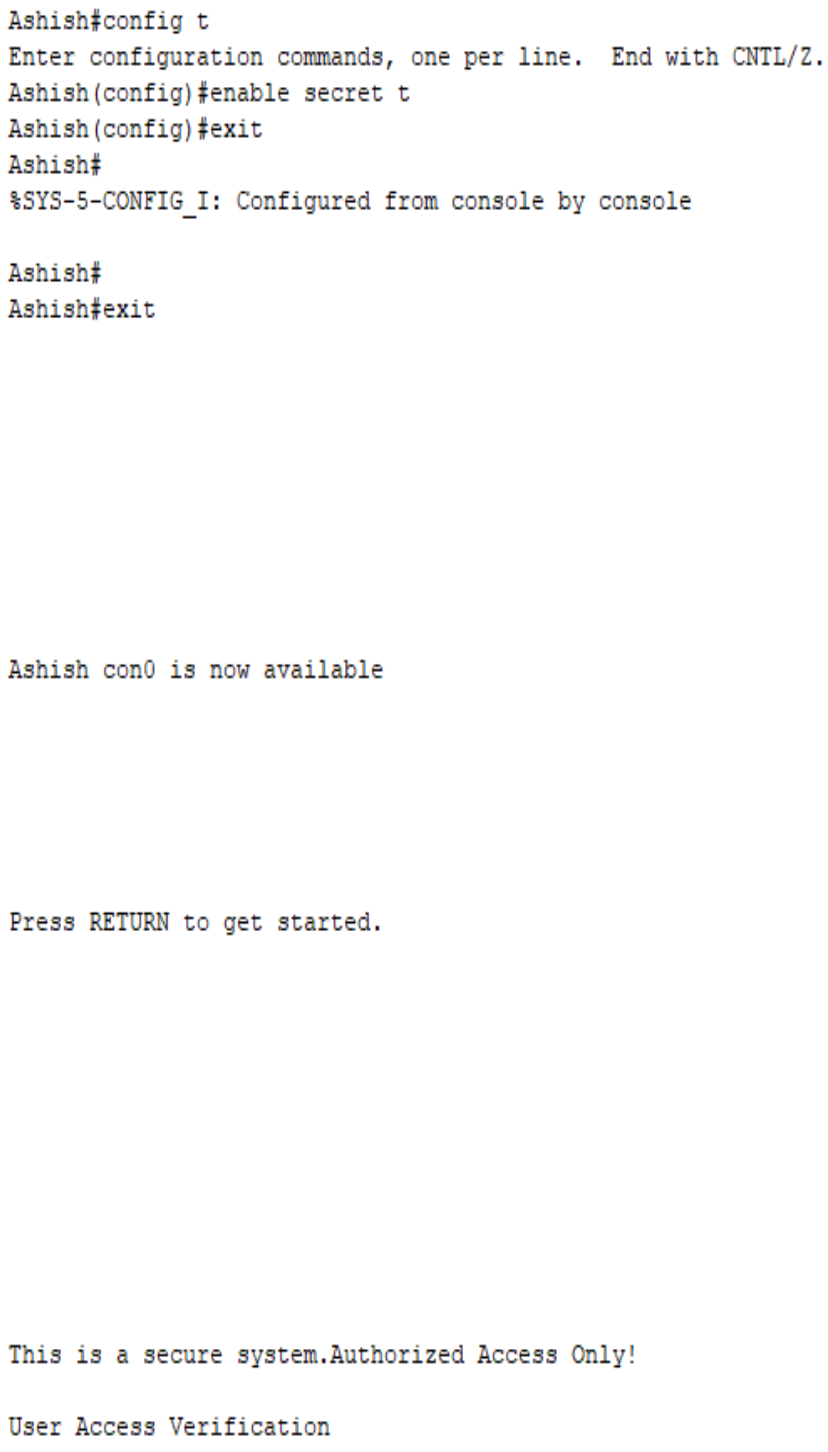



Figure 6: EXEC mode Login Verification

9) *service password-encryption*: It is used to encrypt the password. Fig (7)

```
Ashish#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Ashish(config)#service password-encryption
Ashish(config)#exit
Ashish#
%SYS-5-CONFIG_I: Configured from console by console

Ashish#show run
Building configuration...

Current configuration : 1261 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Ashish
!
!
enable secret 5 $1$mERr$li.ZEMxVINz5HJDwox0ls1
enable password 7 08221D0A0A49
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
 --More-- |
```

Figure 7: Password Encryption

10) *banner motd*: It is a feature which allows the user to configure messages that anyone logging on the switch sees. These messages are known as Message of the Day. Fig (8)

```
Ashish#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Ashish(config)#banner motd "Ashish's System"
Ashish(config)#exit
Ashish#
%SYS-5-CONFIG_I: Configured from console by console
```

```

Ashish's System

User Access Verification

Password: |
```

Figure 8: Motd configuration

11) *copy running-config startup-config*: It allows the user to save the configuration file to NVRAM of the switch, which can be used when the switch is rebooted. It creates a startup script which ensures that changes made are not lost. Fig (9)

```
Password:
Ashish#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Ashish#
```

Figure 9: Startup configuration

**Result:** Switch was configured successfully.

# Experiment 3

**AIM:** To implement basic connectivity.

**Devices Used**: Switches, PCs, and Cable**s**

**Objectives**

Part 1: Perform a Basic Configuration on S1 and S2

Part 2: Configure the PCs

Part 3: Configure the Switch Management Interface

**Addressing Table**

| Device | Interface | IP Address | Subnet Mask |
|---|---|---|---|
| S1 | VLAN 1 | 192.168.1.253 | 255.255.255.0 |
| S2 | VLAN 1 | 192.168.1.254 | 255.255.255.0 |
| PC1 | NIC | 192.168.1.1 | 255.255.255.0 |
| PC2 | NIC | 192.168.1.2 | 255.255.255.0 |

Fig. Addressing Table

Part 1: Perform a Basic Configuration on S1 and S2

Step 1: Configure S1 with a hostname.

Step 2: Configure the console and encrypted privileged EXEC mode passwords.

Step 3: Verify the password configurations for S1.

Step 4: Configure an MOTD banner.

Step 5: Save the configuration file to NVRAM.

Step 6: Repeat Steps 1 to 5 for S2.

Part 2: Configure the PCs

Step 1: Configure both PCs with IP addresses.

Step 2: Test connectivity to switches. Part 3:

Configure the Switch Management Interface

Step 1: Configure S1 with an IP address.

Step 2: Configure S2 with an IP address.

Step 3: Verify the IP address configuration on S1 and S2.

Step 4: Save configurations for S1 and S2 to NVRAM.

Step 5: Verify network connectivity.

**Q.) Which command do you issue to accomplish this step?**

**Ans)** copy running-config startup-config

**Q.) Why do you enter the no shutdown command?**

**Ans)** The no shutdown command is used within the interface configuration mode to enable the interface "GigabitEthernet0/1".

**Procedure:** Open the activity through the Cisco Packet Tracer (2.7.6)

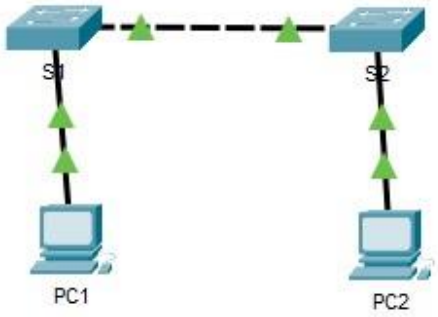



Fig. Diagram Representing Connection Between Devices

```
Switch>enable
Switch#
Switch#show run
Building configuration...

Current configuration : 1086 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/2
!

Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#line console 0
S1(config-line)#password letmein
S1(config-line)#login
S1(config-line)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

```
Password:


S1>enable
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#enable password c1$c0
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
exit




S1 con0 is now available




Press RETURN to get started.
```

```
Building configuration...

Current configuration : 1178 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
!
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password c1$c0
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id

S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#banner motd "This is a secure system. Authorized Access Only!"
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

**Result:** Switch configuration was made and verified.

# Experiment 4

**AIM:** Basic switch and end device configuration.

**Devices Used**: Switches, PCs, and Cable**s.**

**Objectives**

Part 1: Set Up the Network Topology

Part 2: Configure PC Hosts

Part 3: Configure and Verify Basic Switch Settings

**Addressing Table**

| Device | Interface | IP Address | Subnet Mask |
|---|---|---|---|
| S1 | VLAN 1 | 192.168.1.1 | 255.255.255.0 |
| S2 | VLAN 1 | 192.168.1.2 | 255.255.255.0 |
| PC-A | NIC | 192.168.1.10 | 255.255.255.0 |
| PC-B | NIC | 192.168.1.11 | 255.255.255.0 |

Fig. Addressing Table

**Q.) Why are some Fast Ethernet ports on the switches up while others are down?**

Ans) The state of a port depends on various factors, and here are some common reasons why some FastEthernet ports might be up while others are down:

- Administrative Shutdown: If a FastEthernet port is in a "down" state, it might have been intentionally administratively shut down using the shutdown command in the interface configuration.
- Configuration Errors: Configuration errors, such as incorrect IP addressing, VLAN assignment, or security settings, can result in an interface being down. Misconfigured interfaces might not be able to establish a valid link, leading to the "down" state.
- Cable or Hardware Issues: Physical problems, such as faulty cables, damaged connectors, or hardware issues, can prevent an interface from establishing a link with the connected device. This can cause the port to remain in a "down" state.
- Link Status: The link status of an interface depends on whether a valid link has been established with the connected device. If the connected device (like another switch, router, or computer) is powered off, its interface might not be able to establish a link, resulting in the "down" state.
- Speed and Duplex Mismatch: If the speed and duplex settings of two connected interfaces do not match, it can lead to connectivity issues and cause the interface to remain down.
- STP (Spanning Tree Protocol) Blocking: In a redundant network topology, STP might temporarily block certain interfaces to prevent loops. These blocked interfaces will be in a "down" state until they are unblocked by the STP protocol.
- Auto-negotiation Issues: Auto-negotiation, which allows devices to automatically determine the best link settings, can sometimes fail. This can result in an interface being down if the auto-negotiation process is not successful.

**Q.) What could prevent a ping from being sent between the PCs?**

**Ans)** Given below are few reasons that could prevent a ping from being sent between the two PCs :

- Network Connectivity Issues
- IP Address Conflicts
- Incorrect Subnet Mask
- Firewall Settings
- Switch or Router Configuration
- Routing and Gateway Issues
- Network Load or Congestion
- Remote PC Settings

**Procedure:** Open the activity through the Cisco Packet Tracer (2.9.2)

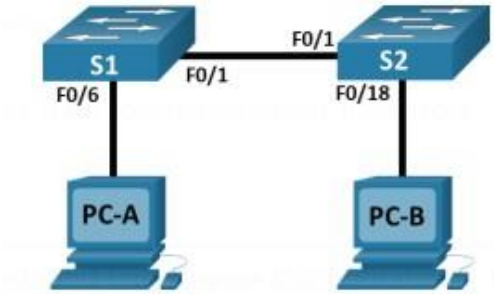
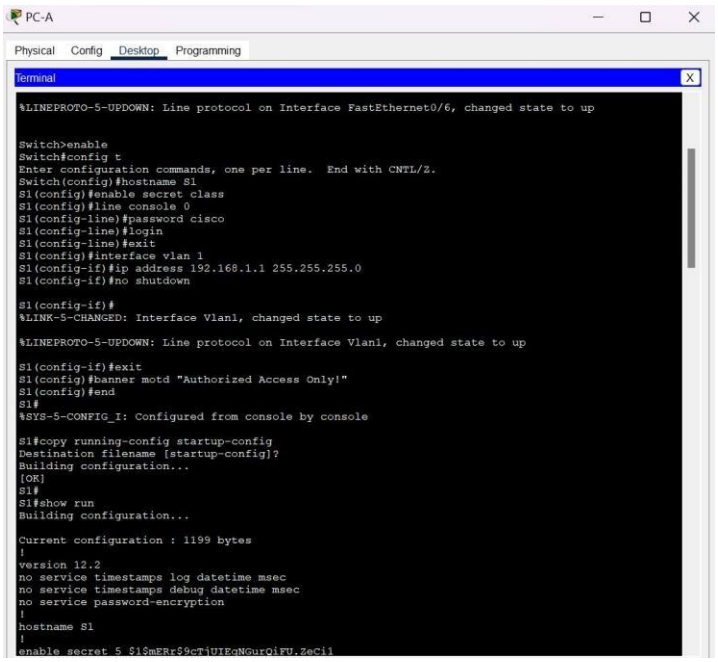
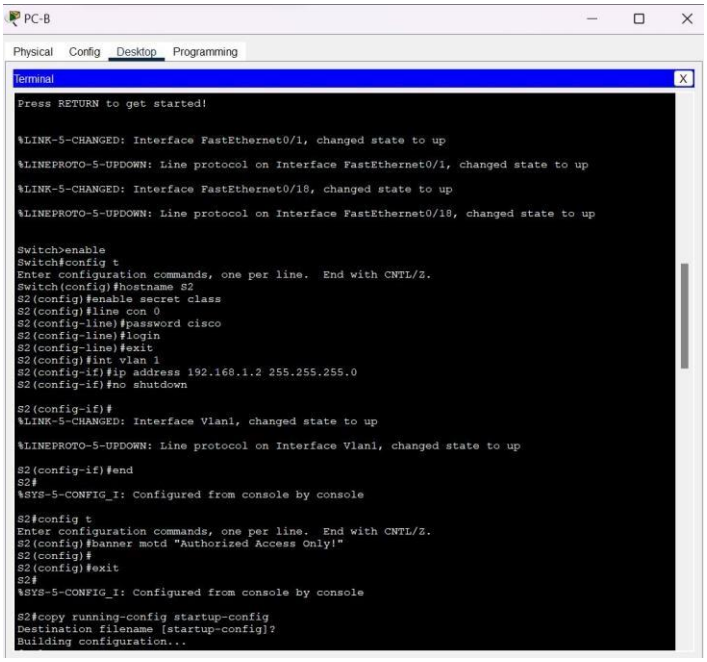
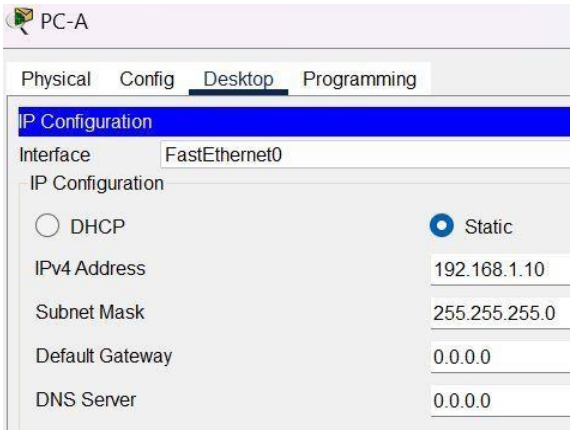
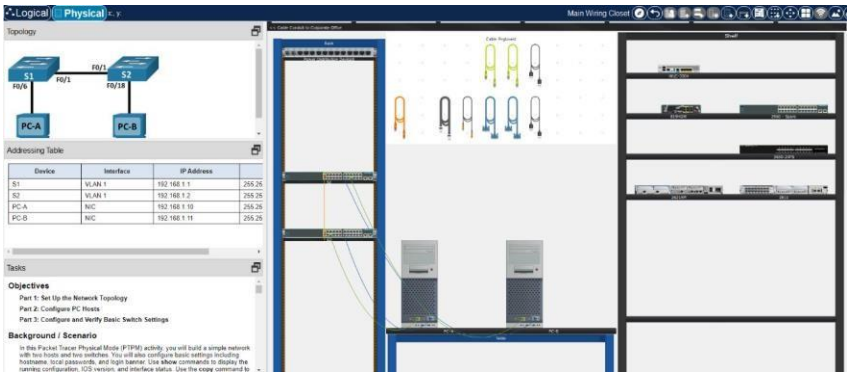



Fig. Diagram representing connection between devices.






**Result**: Basic Switch and Device configuration was done successfully.