

EXPERIMENT-1

Aim:

Know your devices.

Theory:

➤ 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.



➤ 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.



- ❖ 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.



➤ **End Devices:**

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

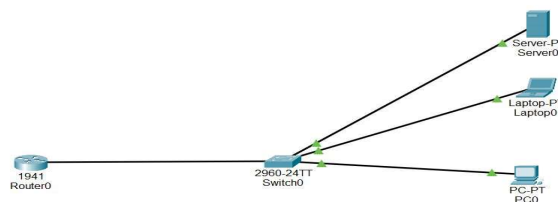
- Computers (workstations, laptops, file servers, and web servers)
- Network printers
- VoIP phones
- TelePresence endpoints
- Security cameras
- Mobile handheld devices



Result:

Successfully studied about all the devices.

Today's Lab Work:



Evaluation Table: -

Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

EXPERIMENT-2

AIM:

To Configure initial Switch Settings.

Devices Used:

Switches, PCs, and Cables

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.

Part 5: Configure S2

Procedure:

Open the activity through the Cisco Packet Tracer (2.5.5)

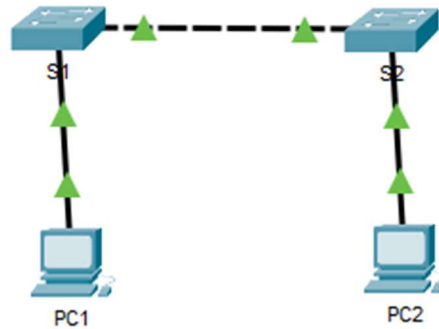


Fig. Diagram Representing connection between devices.

```
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 FastEthernet0/1
```

```
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
```

User Access Verification

Password:

S1>enable

Password:

S1#show running-config

Building configuration...

Current configuration : 1131 bytes

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

hostname S1

```
!
!
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)#enable secret itsasecret

S1(config)#exit

S1#

%SYS-5-CONFIG_I: Configured from console by console

show run

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:

Congratulations Guest! You completed the activity.

Overall Feedback [Assessment Items](#) [Connectivity Tests](#)

[Expand/Collapse All](#) [Show Incorrect Items](#)

Assessment Items	Status	Points	Component(s)	Feedback
Network				
S1				
Banner MOTD	Correct	6	Basic Security C...	
Console Line				
Login	Correct	4	Basic Security C...	
Password	Correct	4	Basic Security C...	
Enable Password	Correct	4	Basic Security C...	
Enable Secret	Correct	4	Basic Security C...	
Host Name	Correct	5	Hostname Config...	
Service Password Encryption	Correct	4	Basic Security C...	
Startup Config	Correct	5	Configuration Ma...	
S2				
Banner MOTD	Correct	6	Basic Security C...	
Console Line				
Login	Correct	4	Basic Security C...	
Password	Correct	4	Basic Security C...	
Enable Password	Correct	4	Basic Security C...	
Enable Secret	Correct	4	Basic Security C...	
Host Name	Correct	5	Hostname Config...	
Service Password Encryption	Correct	4	Basic Security C...	
Startup Config	Correct	5	Configuration Ma...	

Score : 72/72

Item Count : 16/16

Component	Items/Total	Score
Basic Security Configuration	12/12	52/52
Configuration Management	2/2	10/10
Hostname Configuration	2/2	10/10

Evaluation Table: -

CRITERIA	TOTAL MARKS	MARKS OBTAINED	COMMENTS
CONCEPT (A)	2		
IMPLEMENTATION (B)	2		
PERFORMANCE (C)	2		
TOTAL	6		

EXPERIMENT-3

AIM:

To implement basic connectivity.

Devices Used:

Switches, PCs, and Cables

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)

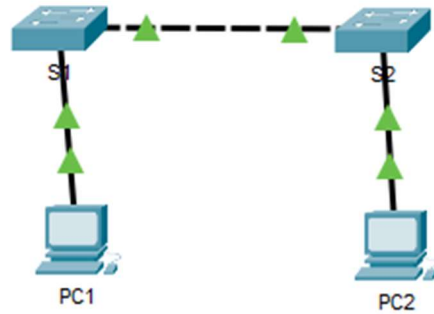


Fig. Diagram Representing Connection Between Devices

```

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

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.

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

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:

Congratulations Jigyasa! You completed the activity.

Overall Feedback

Assessment Items

Connectivity Tests

Expand/Collapse All

Show Incorrect Items

Assessment Items	Status	Points	Component(s)	Feedback
Network				
PC1				
Ports				
FastEthernet0				
IP Address	Correct	15	IPv4 Host Address...	
Subnet Mask	Correct	2	IPv4 Host Address...	
PC2				
Ports				
FastEthernet0				
IP Address	Correct	15	IPv4 Host Address...	
Subnet Mask	Correct	2	IPv4 Host Address...	
S1				
Banner MOTD	Correct	1	Basic Security C...	
Console Line				
Login	Correct	1	Basic Security C...	
Password	Correct	1	Basic Security C...	
Enable Secret	Correct	1	Basic Security C...	
Host Name	Correct	1	Hostname Config...	
Ports				
Vlan1				
IP Address	Correct	5	IPv4 Host Address...	
Port Status	Correct	10	IPv4 Host Address...	
Subnet Mask	Correct	5	IPv4 Host Address...	
Startup Config	Correct	2	Configuration Ma...	
S2				
Banner MOTD	Correct	1	Basic Security C...	
Console Line				
Login	Correct	1	Basic Security C...	
Password	Correct	1	Basic Security C...	
Enable Secret	Correct	1	Basic Security C...	
Host Name	Correct	1	Hostname Config...	
Ports				
Vlan1				
IP Address	Correct	5	IPv4 Host Address...	
Port Status	Correct	10	IPv4 Host Address...	
Subnet Mask	Correct	5	IPv4 Host Address...	
Startup Config	Correct	2	Configuration Ma...	

Score

: 88/88

Item Count

: 22/22

Component	Items/Total	Score
Basic Security Configuration	8/8	8/8
Configuration Management	2/2	4/4
Hostname Configuration	2/2	2/2
IPv4 Host Address Configuration	10/10	74/74

Evaluation Table: -

Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

EXPERIMENT-4

AIM:

Basic switch and end device configuration.

Devices Used:

Switches, PCs, and Cables.

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 FastEthernet 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)

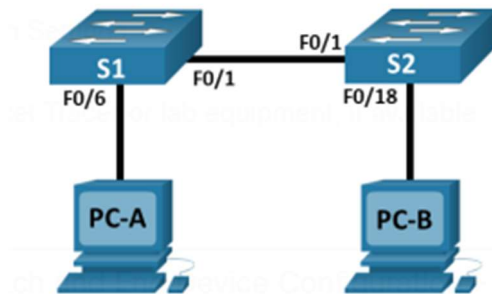


Fig. Diagram representing connection between devices.

PC-A

```

Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
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)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S1(config-if)#exit
S1(config)#banner motd "Authorized Access Only!"
S1(config)#end
S1#
%SYS-5-CONFIG I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
S1#show run
Building configuration...

Current configuration : 1199 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
enable secret 5 $1$mE$Rr$ScT4UIE$N$GuroiFU.ZeCii

```

PC-B

```

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up

Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#enable secret class
S2(config)#line con 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#int vlan 1
S2(config-if)#ip address 192.168.1.2 255.255.255.0
S2(config-if)#no shutdown
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S2(config-if)#end
S2#
%SYS-5-CONFIG I: Configured from console by console
S2#config t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#banner motd "Authorized Access Only!"
S2(config)#
S2(config)#exit
S2#
%SYS-5-CONFIG I: Configured from console by console
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

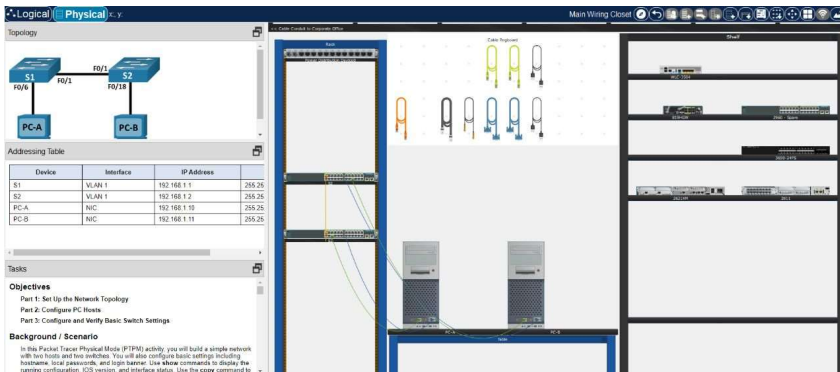
```

PC-A

Physical Config **Desktop** Programming

IP Configuration

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.1.10
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0



Result:

Congratulations Jigyasa! You completed the activity.

Overall Feedback [Assessment Items](#) Connectivity Tests

Expand/Collapse All Show Incorrect Items

Assessment Items	Status	Points	Component(s)	Feedback
Network				
PC-A				
Physical Location	Correct	1	Physical	
Ports				
FastEthernet0				
IP Address	Correct	1	Ip	
Link to S1				
Connects to FastEthernet0/6	Correct	1	Physical	
Type	Correct	1	Physical	
Subnet Mask	Correct	1	Ip	
Power	Correct	1	Physical	
PC-B				
Physical Location	Correct	1	Physical	
Ports				
FastEthernet0				
IP Address	Correct	1	Ip	
Link to S2				
Connects to FastEthernet0/18	Correct	1	Physical	
Type	Correct	1	Physical	
Subnet Mask	Correct	1	Ip	
Power	Correct	1	Physical	
S1				
Banner MOTD	Correct	1	Other	
Console Line				
Login	Correct	1	Physical	
Password	Correct	1	Other	
Enable Secret	Correct	1	Other	
Host Name	Correct	1	Other	
Physical Location	Correct	1	Physical	
Ports				
FastEthernet0/1				
Link to S2				
Connects to FastEthernet0/1	Correct	1	Physical	
Type	Correct	1	Physical	
Vlan1				
IP Address	Correct	1	Ip	

Score: 36/36
Item Count: 36/36

Component	Items/Total	Score
Ip	8/8	8/8
Other	10/10	10/10
Physical	18/18	18/18

Evaluation Table: -

Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

EXPERIMENT-5

AIM:

To connect the physical layer.

Devices Used:

Switches, PCs, and Cables

Objectives

Part 1: Identify Physical Characteristics of Internetworking Devices

Part 2: Select Correct Modules for Connectivity

Part 3: Connect Devices

Part 4: Check Connectivity

Part 1: Identify Physical Characteristics of Internetworking Devices

Step 1: Identify the management ports of a Cisco router.

Step 2: Identify the LAN and WAN interfaces of a Cisco router.

Step 3: Identify module expansion slots.

Part 2: Select Correct Modules for Connectivity

Step 1: Determine which modules provide the required connectivity.

Step 2: Add the correct modules and power up devices.

Part 3: Connect Devices

Device	Interface	Cable Type	Device	Interface
East	GigabitEthernet0/0	Copper Straight-Through	Switch1	GigabitEthernet0/1
East	GigabitEthernet0/1	Copper Straight-Through	Switch4	GigabitEthernet0/1
East	FastEthernet0/1/0	Copper Straight-Through	PC1	FastEthernet0
East	FastEthernet0/1/1	Copper Straight-Through	PC2	FastEthernet0
East	FastEthernet0/1/2	Copper Straight-Through	PC3	FastEthernet0
Switch1	FastEthernet0/1	Copper Straight-Through	PC4	FastEthernet0
Switch1	FastEthernet0/2	Copper Straight-Through	PC5	FastEthernet0
Switch1	FastEthernet0/3	Copper Straight-Through	PC6	FastEthernet0
Switch4	GigabitEthernet0/2	Copper Cross-Over	Switch3	GigabitEthernet3/1
Switch3	GigabitEthernet5/1	Fiber	Switch2	GigabitEthernet5/1
Switch2	FastEthernet0/1	Copper Straight-Through	PC7	FastEthernet0
Switch2	FastEthernet1/1	Copper Straight-Through	PC8	FastEthernet0
Switch2	FastEthernet2/1	Copper Straight-Through	PC9	FastEthernet0
Switch2	Gigabit3/1	Copper Straight-Through	AccessPoint	Port 0

Fig. Reference Table for connecting devices.

Part 4: Check Connectivity

Step 1: Check the interface status on East.

Step 2: Connect wireless devices, Laptop and TabletPC

Step 3: Change the access method of the TabletPC.

Step 4: Check connectivity of the other PCs.

Q.) Which management ports are available?

Ans) AUX and console ports are available.

Q.) Which LAN and WAN interfaces are available on the East router and how many are there?

Ans) There are 2 WAN interfaces and 2 Gigabit Ethernet interfaces.

Ans) 4

Ans) 1000000 Kbit

Ans) 5 slots are available.

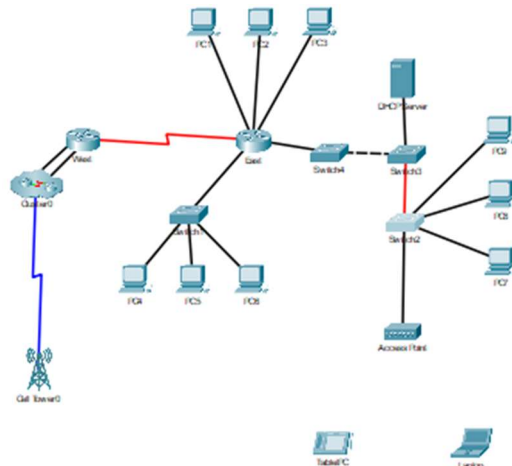


Fig. Diagram with all the connections

Result:

Congratulations Jigyasa! You completed the activity.

Overall Feedback
Assessment Items
Connectivity Tests

Expand/Collapse All
Show Incorrect Items

Assessment Items	Status	Points	Component(s)	Feedback
<ul style="list-style-type: none"> Network <ul style="list-style-type: none"> Access Point <ul style="list-style-type: none"> Ports <ul style="list-style-type: none"> Port 0 <ul style="list-style-type: none"> Link to Switch2 <ul style="list-style-type: none"> Connects to GigabitEthernet3/1 Correct Type Correct East <ul style="list-style-type: none"> Ports <ul style="list-style-type: none"> FastEthernet0/1/0 <ul style="list-style-type: none"> Link to PC 1 <ul style="list-style-type: none"> Connects to FastEthernet0 Correct Type Correct FastEthernet0/1/1 <ul style="list-style-type: none"> Link to PC2 <ul style="list-style-type: none"> Connects to FastEthernet0 Correct Type Correct FastEthernet0/1/2 <ul style="list-style-type: none"> Link to PC3 <ul style="list-style-type: none"> Connects to FastEthernet0 Correct Type Correct GigabitEthernet0/0 <ul style="list-style-type: none"> Link to Switch1 <ul style="list-style-type: none"> Connects to GigabitEthernet0/1 Correct Type Correct GigabitEthernet0/1 <ul style="list-style-type: none"> Link to Switch4 <ul style="list-style-type: none"> Connects to GigabitEthernet0/1 Correct Type Correct Serial0/0/0 <ul style="list-style-type: none"> Link to West <ul style="list-style-type: none"> Connects to Serial0/0/0 Correct PC1 <ul style="list-style-type: none"> Ports <ul style="list-style-type: none"> FastEthernet0 <ul style="list-style-type: none"> Link to East <ul style="list-style-type: none"> Connects to FastEthernet0/0 Correct 				

Score
51/51
Item Count
51/51

Component	Items/Total	Score
Connect Devices	35/35	35/35
Physical	16/16	16/16

Evaluation Table: -

Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

