Lab Manual
For
Networking Lab

(4th semester E&TC)

Prepared by:

Er. Swagatika Malik
Lecturer (IT)
Government Polytechnic Balasore
Odisha

INDEX

Experiment-1

Aim of the experiment : Recognize the physical topology and cabling (coaxial, OFC, UTP, STP) of a network.

Apparatus Required: Twisted pair cable (STP&UTP), Coaxial and OFC

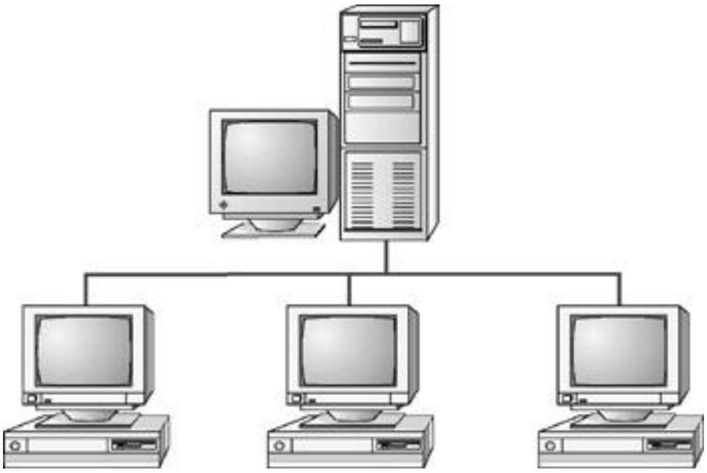
Theory:

Physical Topology: Every LAN has a topology, or the way that the devices on a network are arranged and how they communicate with each other. It is the physical layout of devices on a network. The way that the workstations are connected to the network through the actual cables that transmit data the physical structure of the network is called the physical topology.

We can form four basic types of network topology.

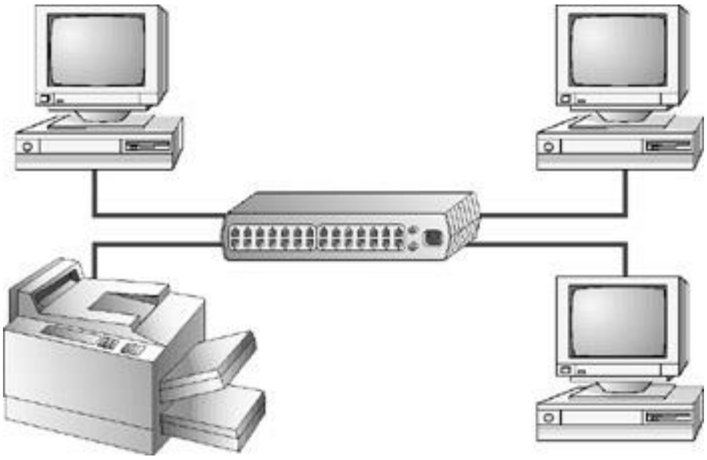
A. Bus:

A single cable to which all network nodes are directly connected.



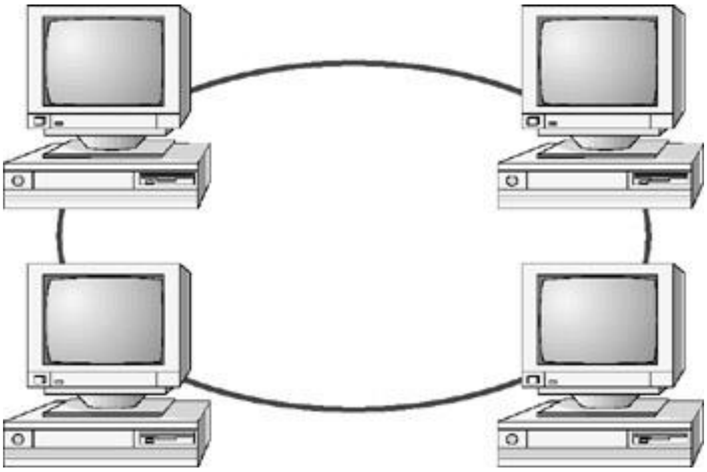
B. Star:

A topology with a single access point or a switch at the center of the topology; all the other nodes are connected directly to this point.



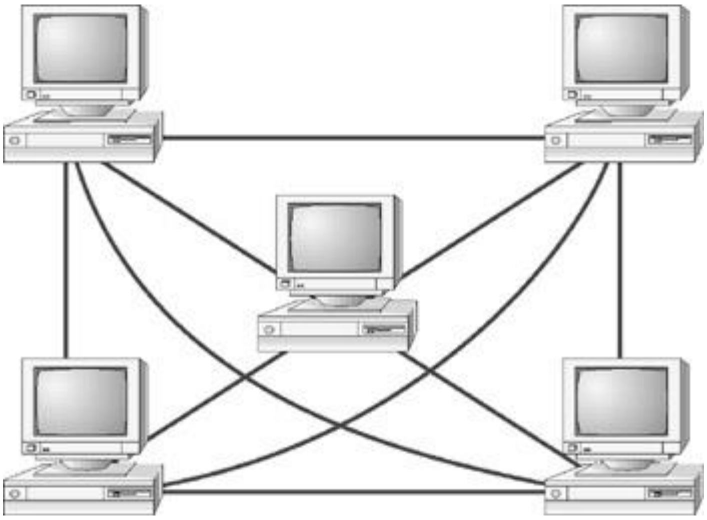
C. Ring:

Each device is connected with the two devices on either side of it. There are two dedicated point to point links a device has with the devices on the either side of it.



D. Mesh:

Each device is connected to every other device on the network through a dedicated point-to-point link.



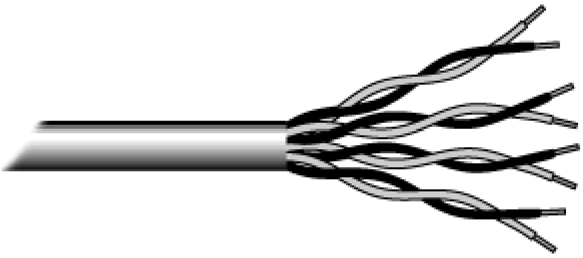
Study of cables:

The following cables are used in the network.

i. UTP
ii. STP
iii. Coaxial
iv. OFC

UTP:

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular.



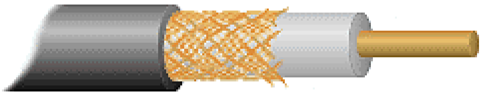
The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. It has six categories.

STP:

STP stands for Shielded twisted pair. STP is similar to unshielded twisted pair (UTP); however, it contains an extra foil wrapping or copper braid jacket to help shield the cable signals from interference. In STP grounding cable is required.

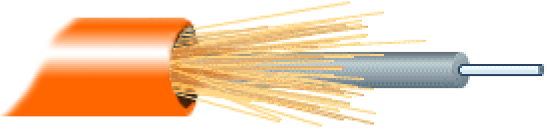
Coaxial:

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield. The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.



OFC:

Fibre optic cabling consists of a center glass core surrounded by several layers of protective materials. It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.



Fibre optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair.

Result:

In the above experiments, different physical topology and different network cables are recognized successfully and understood the function of each topology as well as network cables.

Experiment-2

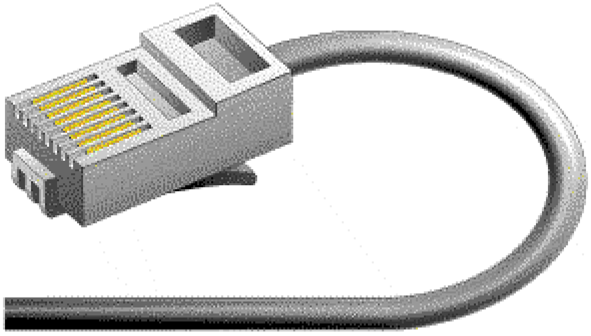
Aim of the experiment: Recognition and use of various types of connectors RJ-45, RJ-11, BNC and SCST.

Apparatus Required: RJ-45, RJ-11, BNC and SCST connectors

Theory:

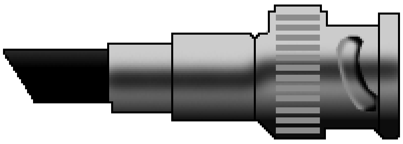
RJ-45:

The standard connector for UPT and STP cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (RJ-11). A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.



BNC Connector:

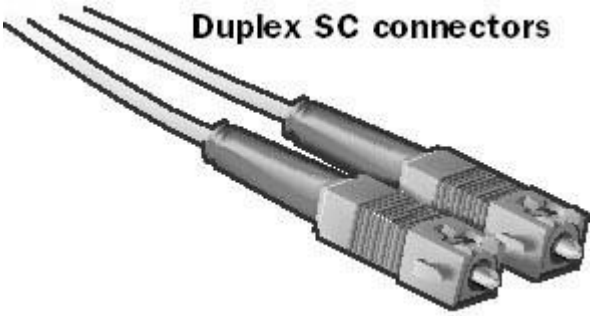
The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector. Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather screw, onto the cable.

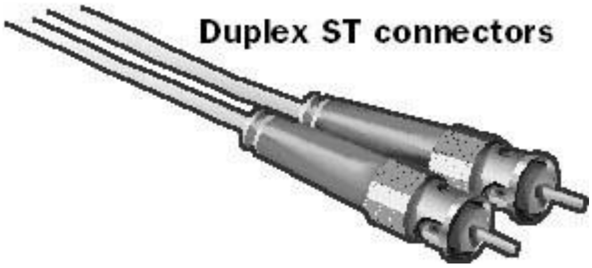


SC and ST Connector:

SC stands for subscriber connector and is a standard-duplex fiber-optic connector with a square moulded plastic body and push-pull locking features. SC connectors are typically used in data communication, CATV, and telephony environments.

ST stands for straight tip, a high-performance fiber-optic connector with round ceramic ferrules and bayonet locking features. ST connectors are more common than SC connectors. Generally the SC and ST connectors used with either single-mode or multimode fiber-optic cabling.





Result:

In the above experiments, different connectors are used in different network cables are recognized successfully.

Experiment-3

Aim of the experiment: Making of cross cable and straight cable.

Apparatus/Tools/Equipments/Components Required:

1. RJ-45 connector,
2. Crimping Tool,
3. Twisted pair Cable,
4. Cable Tester.

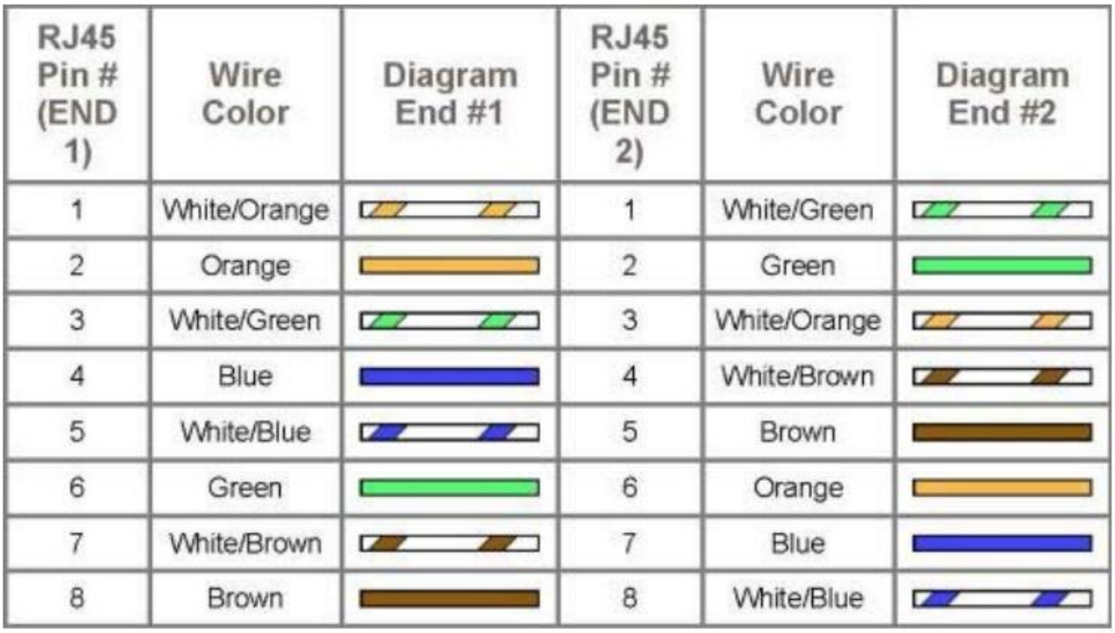
Procedure:

1. Start by stripping off about 2 inches of the plastic jacket off the end of the cable. Be very careful at this point, as to not nick or cut into the wires, which are inside. Doing so could alter the characteristics of your cable, or even worse render is useless. Check the wires, one more time for nicks or cuts. If there are any, just whack the whole end off, and start over.

2. Spread the wires apart, but be sure to hold onto the base of the jacket with your other hand. You do not want the wires to become untwisted down inside the jacket. Category 5 cable must only have 1/2 of an inch of 'untwisted' wire at the end; otherwise it will be 'out of spec'. At this point, you obviously have ALOT more than 1/2 of an inch of un-twisted wire.

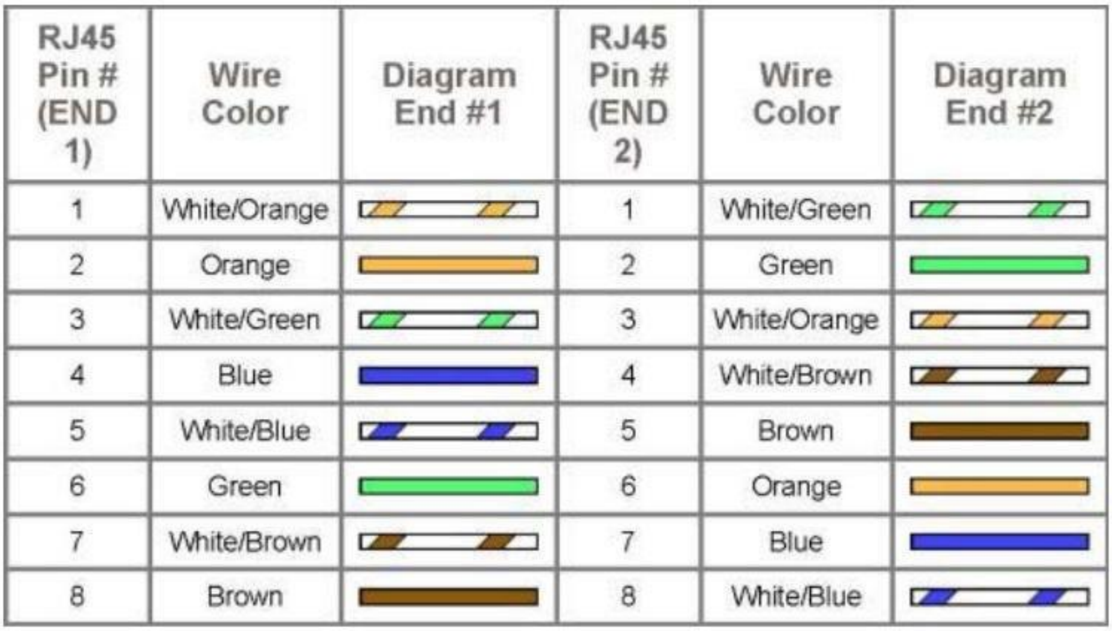
3. You have 2 end jacks, which must be installed on your cable. If you are using a pre-made cable, with one of the ends whacked off, you only have one end to install - the crossed over end. Below are two diagrams, which show how you need to arrange the cables for each type of cable end. Decide at this point which end you are making and examine the associated picture below.

Diagram shows you how to prepare Cross wired connection



RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange	🟧⬜🟧	1	White/Green	🟩⬜🟩
2	Orange	🟧	2	Green	🟩
3	White/Green	🟩⬜🟩	3	White/Orange	🟧⬜🟧
4	Blue	🟦	4	White/Brown	🟫⬜🟫
5	White/Blue	🟦⬜🟦	5	Brown	🟫
6	Green	🟩	6	Orange	🟧
7	White/Brown	🟫⬜🟫	7	Blue	🟦
8	Brown	🟫	8	White/Blue	🟦⬜🟦

Diagram shows you how to prepare straight through wired connection



RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange	⬜🟧	1	White/Green	⬜🟩
2	Orange	🟧	2	Green	🟩
3	White/Green	⬜🟩	3	White/Orange	⬜🟧
4	Blue	🟦	4	White/Brown	⬜🟫
5	White/Blue	⬜🟦	5	Brown	🟫
6	Green	🟩	6	Orange	🟧
7	White/Brown	⬜🟫	7	Blue	🟦
8	Brown	🟫	8	White/Blue	⬜🟦

Cable Crimping Steps:

1. Remove the outmost vinyl shield for 12mm at one end of the cable (we call this side A-side).

2. Arrange the metal wires in parallel

3. Insert the metal wires into RJ45 connector on keeping the metal wire arrangement.

4. Set the RJ45 connector (with the cable) on the pliers, and squeeze it tightly.

5. Make the other side of the cable (we call this side B-side) in the same way.

Testing the crimped cable using a cable tester:

Step 1: Skin off the cable jacket 3.0 cm long cable stripper up to cable

Step 2: Untwist each pair and straighten each wire 190 0 1.5 cm long.

Step 3: Cut all the wires.

Step 4: Insert the wires into the RJ45 connector right white orange left brown the pins facing up

Step 5: Place the connector into a crimping tool, and squeeze hard so that the handle reaches its full swing.

Step 6: Use a cable tester to test for proper continuity.

Result:

Cable Crimping, straight Cabling and Cross Cabling, and testing the crimped cable using a cable tester are done successfully.

Experiment-4

Aim of the experiment: Install and configure a network interface card in a workstation.

Apparatus/ Equipment Required:

1. NIC card
2. Desktop/PC
3. Computer Screw driver set
4. Driver Software

Theory:

NICs (Network Interface Card): Network Interface Card, or NIC is a hardware card installed in a computer so it can communicate on a network. The network adapter provides one or more ports for the network cable to connect to, and it transmits and receives data onto the network cable.

Every networked computer must also have a network adapter driver, which controls the network adapter.

Each network adapter driver is configured to run with a certain type of network adapter.

Procedure:

1. Install the network card:
2. Disconnect all cables connected to the computer and open the case. Locate an available PCI slot (white slots) and insert the network card and secure the card with the screw that came with it. Once the adapter has been installed and secured close the computer case, connect all the cables and turn it on.
3. After installing the adapter driver it should be working find, now let's configure the card for use on a network.
4. Click on the Start button and select Settings then Control Panel. Double click on the System icon
5. Click on the Hardware tab.
6. Click on Device Manager.

You will see a list of devices installed in your computer.

7. If necessary, click on the + sign next to Network Adapters to expand the list.
8. Ensure that there is no yellow exclamation mark (!) next to the Network Adapter. This indicates a possible problem with the card or configuration.
9. Double click on your network driver (e.g. NE2000 Compatible). In the Device Status box you should see the message:
10. This Device is working correctly.

If you do not see this message or if there is no Network Adapter displayed, then your Ethernet card will probably need configuring.

Result:

Installation and configuration of NIC card and transfer files between systems in a LAN have been done successfully.

Experiment-5

Aim of the experiment: Identify the IP address of a workstation and the class of the address and configure the IP Address on a workstation.

Apparatus/ Equipment Required:

PC connected to internet.

Theory:

Identification of IP Address:

An IPv4 address is a 32-bit address that uniquely and universally identifies the connection of a host or a router to the Internet.

The dotted decimal notation an IPv4 address shown below.

Ex: 192.68.12.1

Classification of IP address:

Class A

1.0.0.1 to 126.255.255.254 Supports 16 million hosts on each of 127 networks.

Class B

128.1.0.1 to 191.255.255.254 Supports 65,000 hosts on each of 16,000 networks.

Class

C 192.0.1.1 to 223.255.254.254 Supports 254 hosts on each of 2 million networks.

Class D

224.0.0.0 to 239.255.255.255 Reserved for multicast groups.

Class E

240.0.0.0 to 254.255.255.254 Reserved.

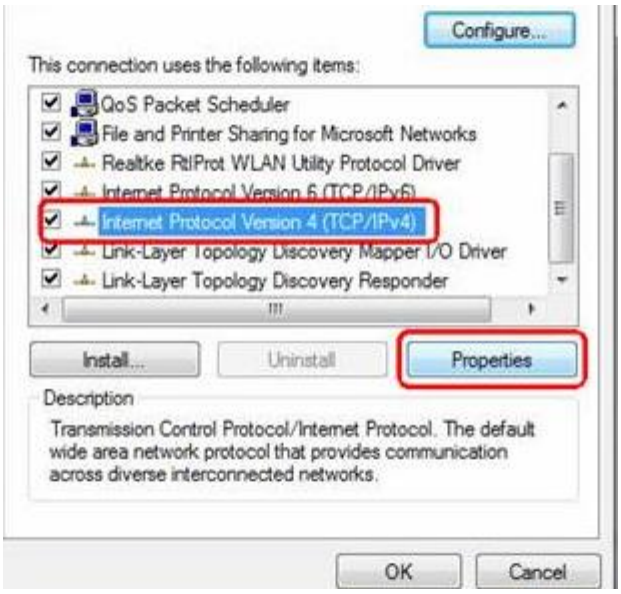
Procedure:

Steps to configure IP address:

Step 1:
1. Click on the Start button and select Control Panel.
2. To check the IP address of the computer, please click on "Network and Internet→ Network and Sharing Center → Change Adapter Settings (on the left)".
3. Then right click on "Ethernet" (right click on Wi-Fi if you want to check the wireless IP address), and go to Status→ Details.
There you will see all the TCP/IP details of this computer.

Step 2:

Right click on “Ethernet”, go to “Properties”, and then choose “Internet Protocol Version 4”, click on Properties;

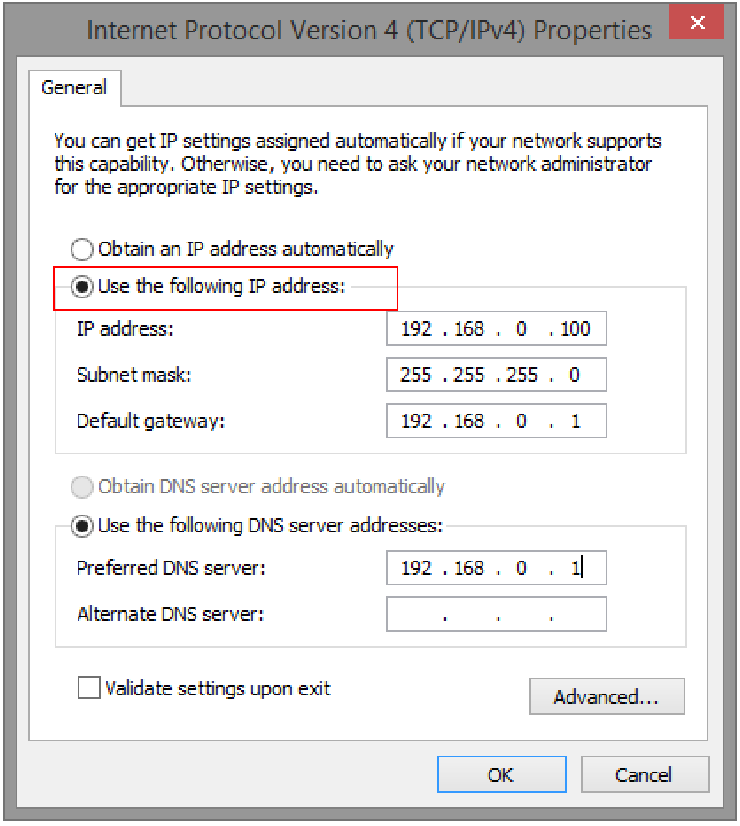


This connection uses the following items:

☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Realtke RtlProt WLAN Utility Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Step 3:
To set manual IP address, please select “Use the following IP address”, and input the IP or DNS address manually.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 0 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 1
Alternate DNS server: . . .

□ Validate settings upon exit

9. Click OK, then Close to close all boxes.

Result:

Configuration of IP Address in a system in LAN (TCP/IP Configuration) have been done successfully

Experiment-6

Aim of the experiment: Managing user accounts in windows and LINUX

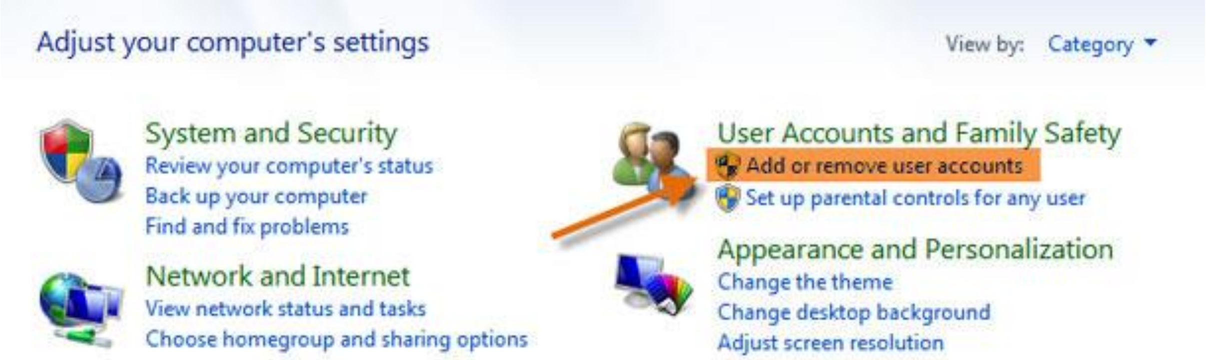
Apparatus/ Equipment Required:

PC with windows OS installed and Linux OS installed.

Procedure:

To go to your user accounts:

1. Go to the Control Panel from the Start Menu.
2. Click Add or remove user accounts.



Adjust your computer's settings

View by: Category

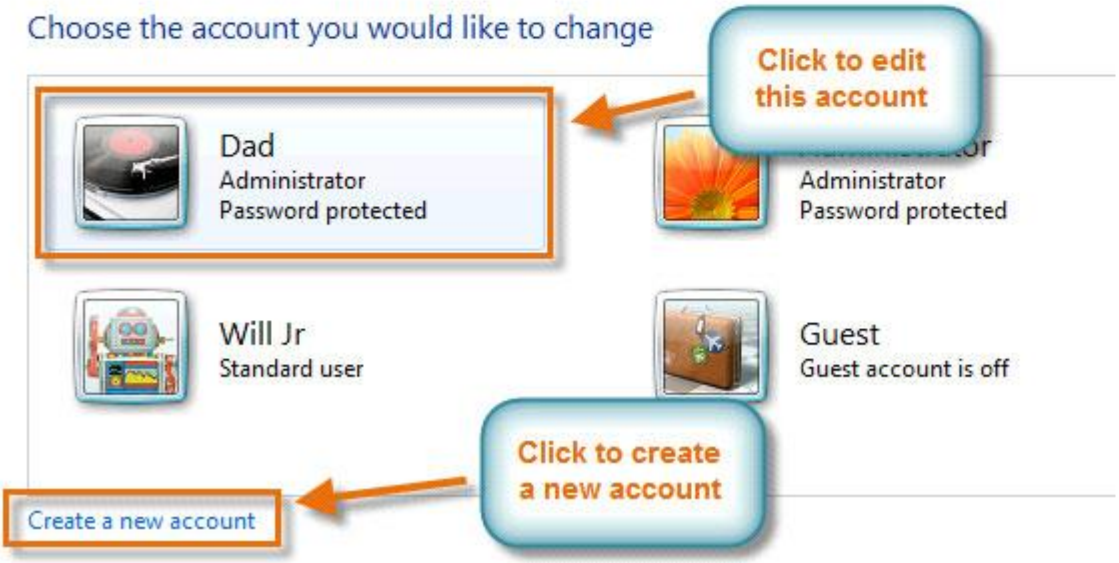
System and Security
Review your computer's status
Back up your computer
Find and fix problems

Network and Internet
View network status and tasks
Choose homegroup and sharing options

User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user

Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution

3. The Manage Accounts pane will appear. You will see all of the user accounts here, and you can add more accounts or manage existing ones.



Choose the account you would like to change

Click to edit this account

Dad
Administrator
Password protected

Administrator
Password protected

Will Jr
Standard user

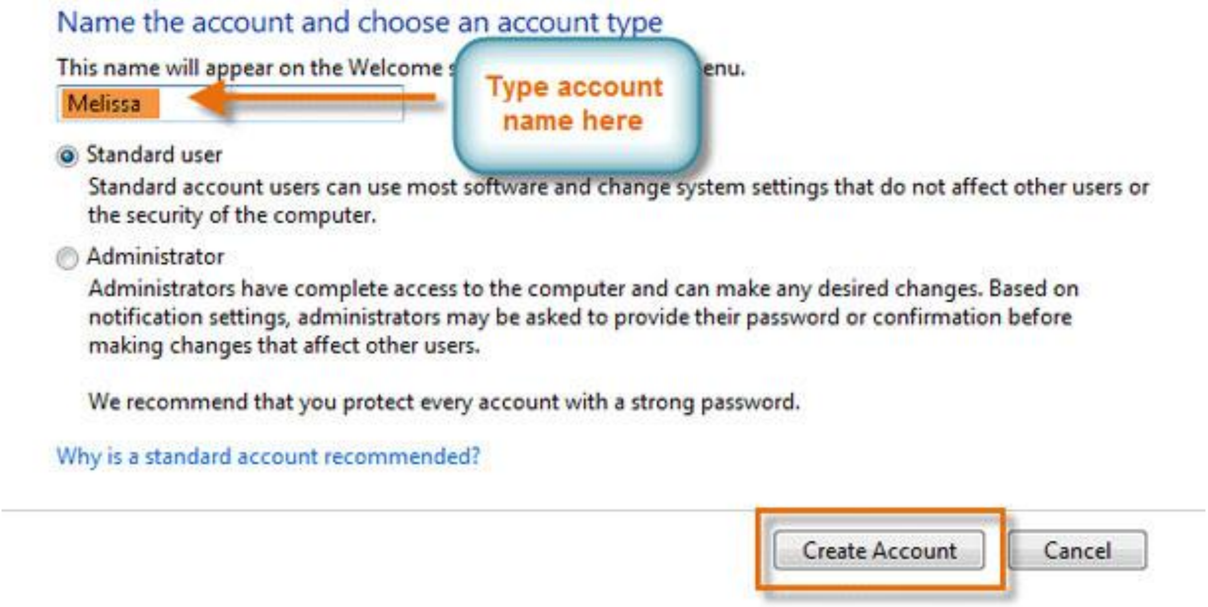
Guest
Guest account is off

Click to create a new account

Create a new account

To create a new account:

1. From the Manage Accounts pane, click Create a new account.
2. Type an account name.



Name the account and choose an account type

This name will appear on the Welcome s enu.

Melissa

● Standard user

Standard account users can use most software and change system settings that do not affect other users or the security of the computer.

○ Administrator

Administrators have complete access to the computer and can make any desired changes. Based on notification settings, administrators may be asked to provide their password or confirmation before making changes that affect other users.

We recommend that you protect every account with a strong password.

Why is a standard account recommended?

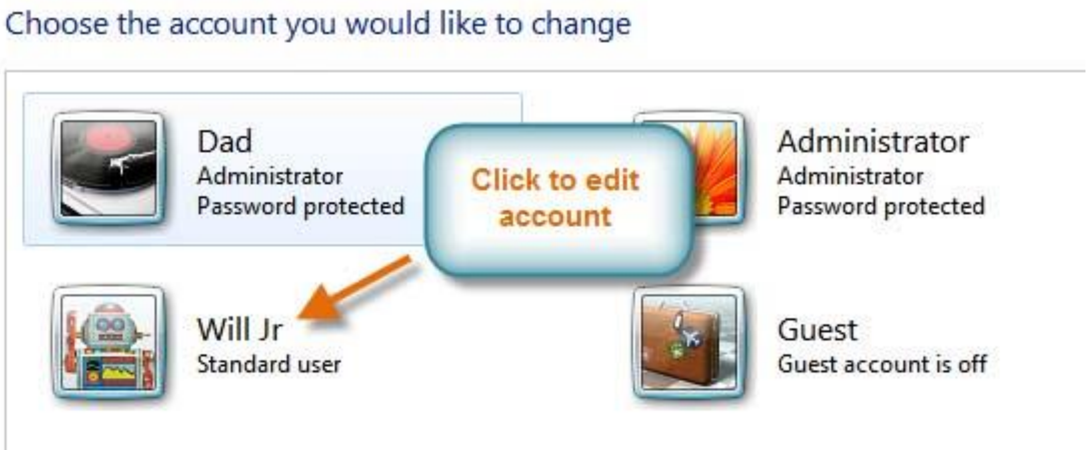
3. Select Standard user or Administrator.
4. Click Create Account.

<u>Changing an account's settings</u>

Once you've created a new account, you may want to add a password or make other changes to the account's settings.

To create a password:

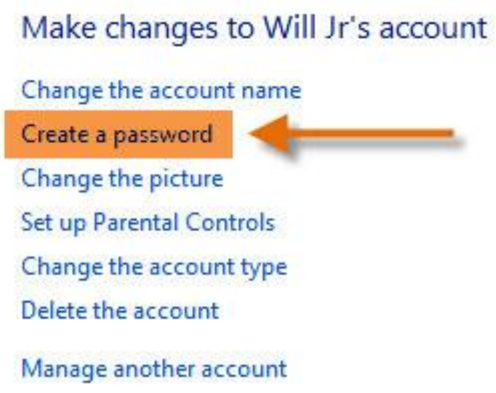
1. From the Manage Accounts pane, click the account name or picture.



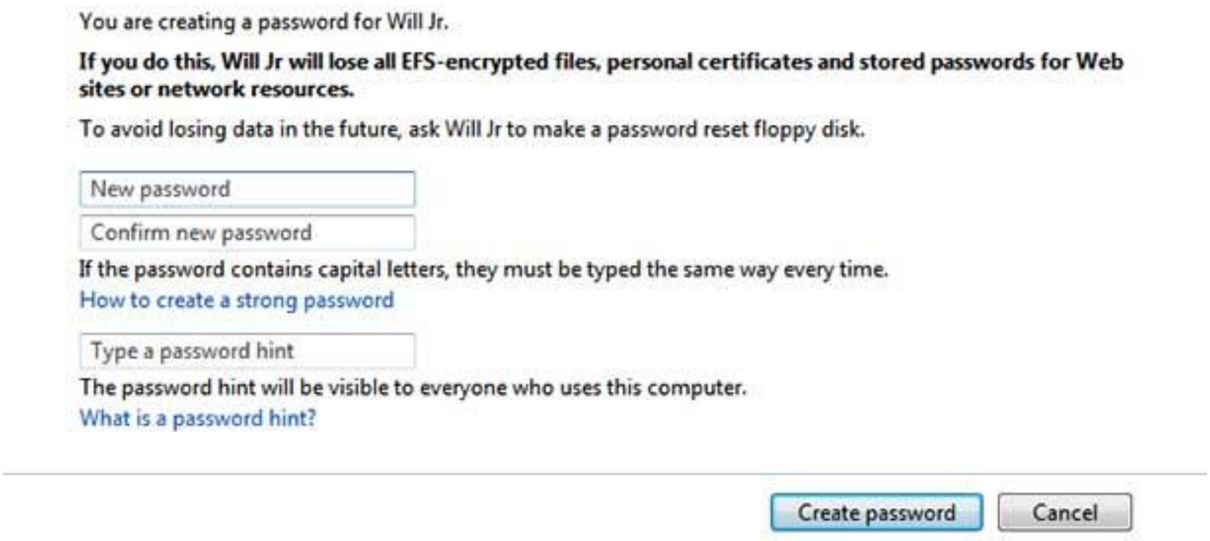
Choose the account you would like to change

Dad Administrator Password protected	Administrator Administrator Password protected
Will Jr Standard user	Guest Guest account is off

2. Click Create a password.



3. Type a password in the New password field, and retype it in the Confirm new password field.


You are creating a password for Will Jr.

If you do this, Will Jr will lose all EFS-encrypted files, personal certificates and stored passwords for Web sites or network resources.

To avoid losing data in the future, ask Will Jr to make a password reset floppy disk.

If the password contains capital letters, they must be typed the same way every time.

The password hint will be visible to everyone who uses this computer.

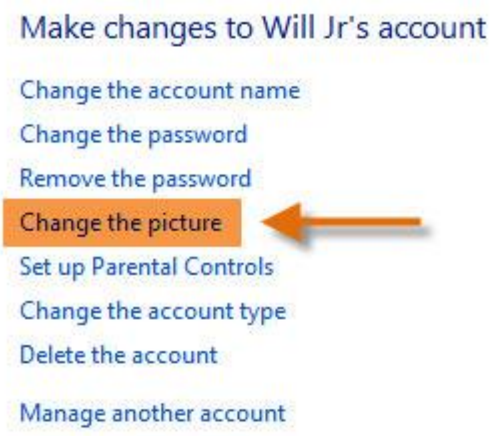
4. If you want, you can type a password hint to help you remember your password.
5. Click Create password.
6. To go back to the Manage Accounts pane, click Manage another account.

Account passwords are case sensitive, which means capital and lowercase letters are treated as different characters. For example, aBc1 is not the same as abc1.

To change your account picture:

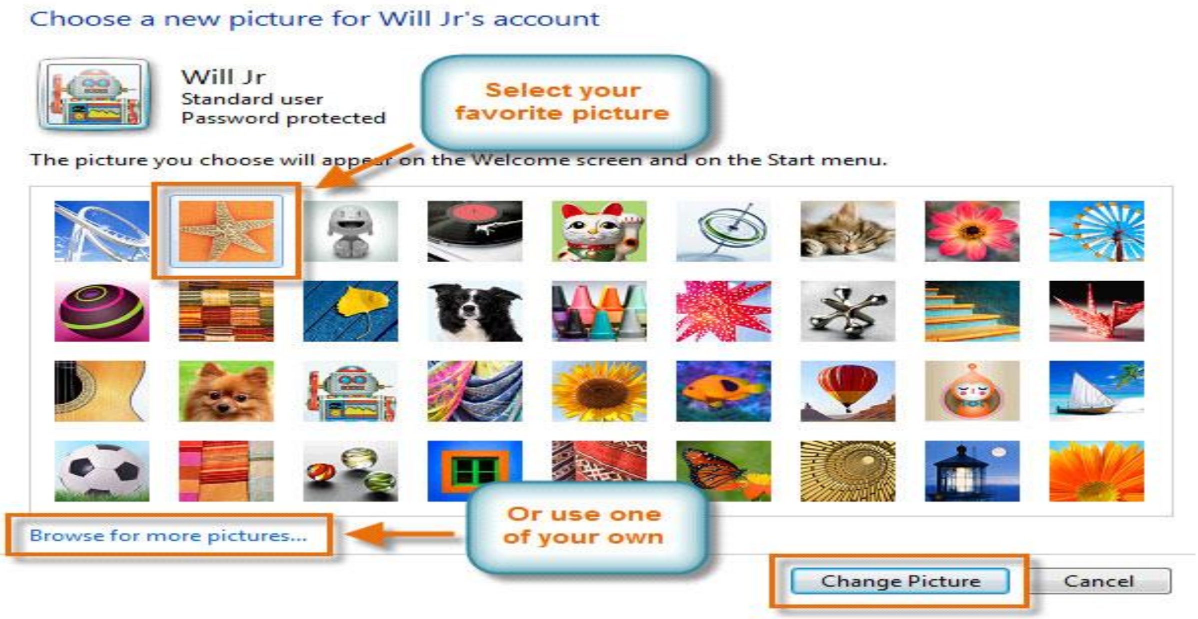
You can also change the picture for any account. This picture appears next to the account name and helps you easily identify the account.

1. From the Manage Accounts pane, click the account name or picture.
2. Click Change the picture.



Make changes to Will Jr's account

3. Select a picture, or click Browse for more pictures to select one of your own.



Choose a new picture for Will Jr's account

Will Jr
Standard user
Password protected

The picture you choose will appear on the Welcome screen and on the Start menu.

4. Click Change Picture.

Result:

Managing user accounts in Windows has successfully done.

Experiment-7

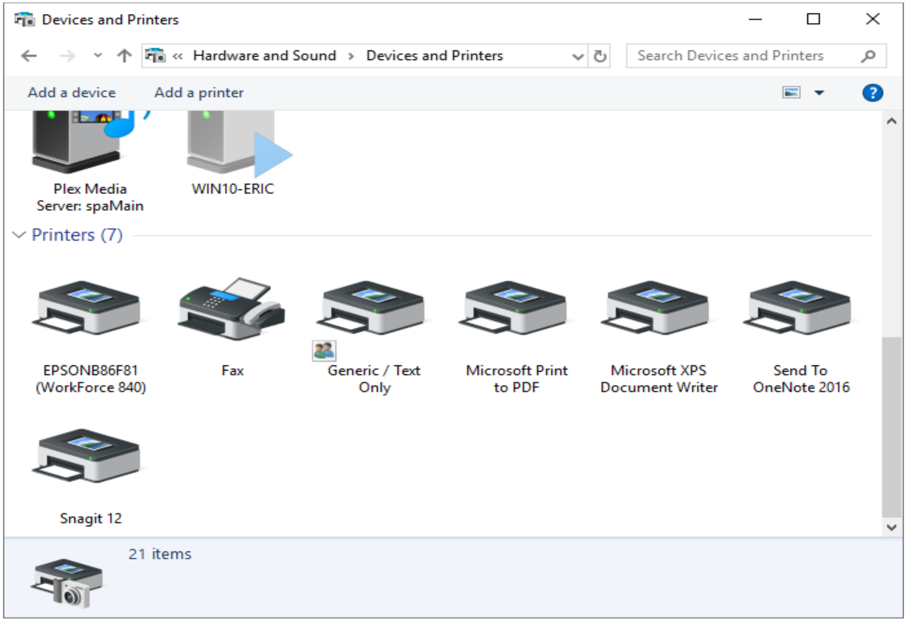
Aim of the experiment: Sharing of Hardware resources in the network.

Apparatus/ Equipment Required:

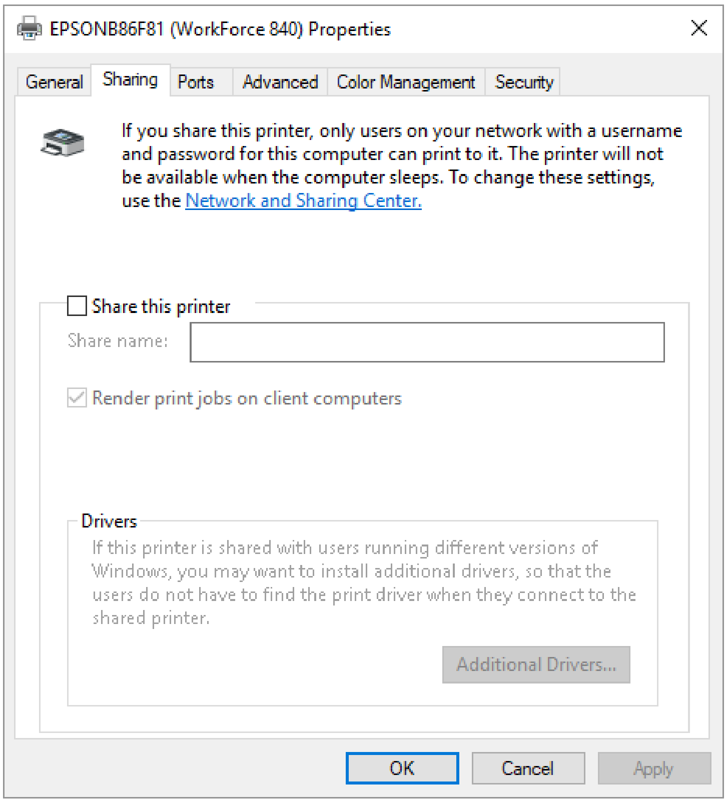
1. Minimum 02 nos. of PCs
2. Printer

Procedure:

1. Network printer can be configured as shared devices so that others on the network can use them.
2. Follow the steps to share printer.
3. Go to the Control Panel from the Start Menu.
4. click View Devices and Printers (under the Hardware and Sound heading).


Devices and Printers
« Hardware and Sound › Devices and Printers
Search Devices and Printers
Add a device
Add a printer
Plex Media Server: spaMain
WIN10-ERIC
Printers (7)
EPSONB86F81 (WorkForce 840)
Fax
Generic / Text Only
Microsoft Print to PDF
Microsoft XPS Document Writer
Send To OneNote 2016
Snagit 12
21 items

5. click the printer you want to share from Devices and Printers dialog box.
6. select Printer Properties from the Context menu.



If you share this printer, only users on your network with a username and password for this computer can print to it. The printer will not be available when the computer sleeps. To change these settings, use the Network and Sharing Center.

□ Share this printer

Share name:

☑ Render print jobs on client computers

Drivers

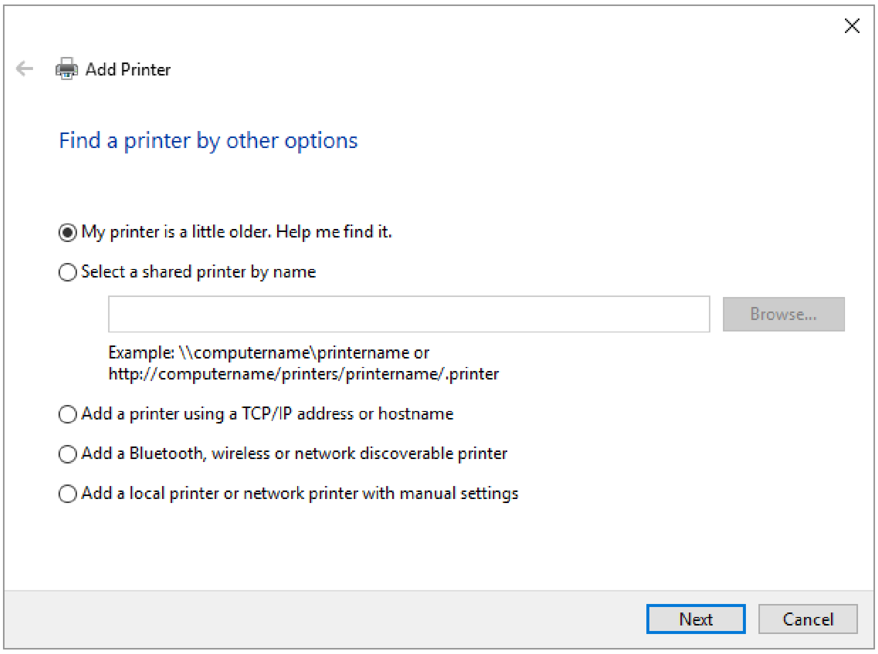
If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer.

7. Click on the Sharing tab of the printer's Properties dialog box.
8. Click the Share this Printer check box and optionally change the Share Name of the printer.
9. click OK to close the printer's Properties dialog box.

How to access the shared printer:

Now the shared printer is made available to others on your network. In order to access the shared printer from a different system, go to that system

1. Go to the Control Panel from the Start Menu.
2. click View Devices and Printers (under the Hardware and Sound heading).
3. click the Add a Printer option, at the top of the dialog box.
4. Click on The Printer I want isn't Listed if our printer isn't found. Windows displays the Find a Printer by Other Options section of the Add Printer wizard.



Add Printer

Find a printer by other options

● My printer is a little older. Help me find it.

○ Select a shared printer by name

Example: \\computername\printername or
http://computername/printers/printername/.printer

○ Add a printer using a TCP/IP address or hostname

○ Add a Bluetooth, wireless or network discoverable printer

○ Add a local printer or network printer with manual settings

5. Click the second option, starts scanning the network for available printers.
6. After all of the printers have been found, select the printer name that you want to use and click Next.
7. The network printer is added to the computer's list of available printers. Click Finish to finish the process.

Result:

Sharing of hardware resources (Network Printer) successfully done in a network among devices connected to it.

Experiment-8

Aim of the experiment: Use of Netstat and its options.
Apparatus/ Equipment Required:

PC connected with internet connection.

Theory:

The **netstat** command is used to display the TCP/IP network protocol statistics and information.

Procedure:

1. **Netstat is a command for checking network and Internet connections.**
2. **Netstat command uses following syntax and switches.**

Syntax and switches:

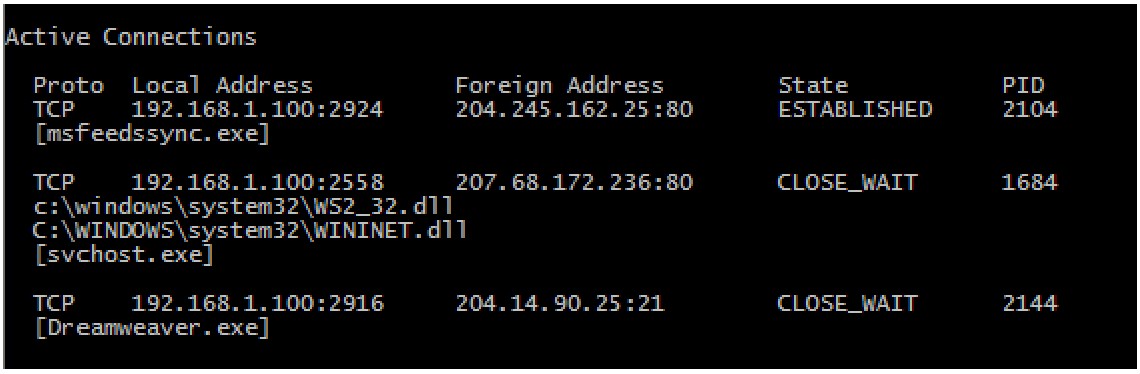
```
NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]
```

Switches	Description
-a	Displays all connections and listening ports.
-b	Displays the executable involved in creating each connection or listening port. In some cases, well-known executables host multiple independent components, and in these cases, the sequence of components involved in creating the connection or listening port is displayed. In this case, the executable name is in [] at the bottom. Note that this option can be time-consuming and fails unless you have sufficient permissions.
-e	Displays Ethernet statistics. This option may be combined with the -s option.
-f	Displays FQDN (fully qualified domain names) for foreign addresses.
-n	Displays addresses and port numbers in numerical form.
-o	Displays the owning process ID associated with each connection.
-p proto	Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s option to display per-protocol statistics, proto may

	be any of: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-r	Displays the routing table.
-s	Displays per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6; the -p option may be used to specify a subset of the default.
-t	Displays the current connection offload state.
-x	Displays NetworkDirect connections, listeners, and shared endpoints.
-y	Displays the TCP connection template for all connections. Cannot be combined with the other options.
interval	Redisplays selected statistics, pausing interval seconds between each display. Press Ctrl+C to stop redisplaying statistics. If omitted, netstat prints the current configuration information once.

Command:

C:\>NETSTAT



```
Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    192.168.1.100:2924     204.245.162.25:80      ESTABLISHED     2104
  [msfeedssync.exe]

  TCP    192.168.1.100:2558     207.68.172.236:80      CLOSE_WAIT      1684
  c:\windows\system32\WS2_32.dll
  C:\WINDOWS\system32\WININET.dll
  [svchost.exe]

  TCP    192.168.1.100:2916     204.14.90.25:21        CLOSE_WAIT      2144
  [Dreamweaver.exe]
```

Command:

C:\>NETSTAT -S

```
C:\Windows\system32>netstat -s | findstr Errors
 Received Header Errors = 0
 Received Address Errors = 0
 Received Header Errors = 0
 Received Address Errors = 0
 Errors 0 0
 Errors 0 0
 Receive Errors = 0
 Receive Errors = 0
C:\Windows\system32>
```

Command:

C:\>NETSTAT -E

```
C:\Windows\system32>netstat -e
Interface Statistics
 Received Sent
Bytes 8988576 2105244
Unicast packets 12972 11880
Non-unicast packets 0 0
Discards 0 0
Errors 0 0
Unknown protocols 0
C:\Windows\system32>
```

Result:

All the option of netstat command used and executed successfully.

Experiment-9

Aim of the experiment: Connectivity troubleshooting using PING, IPCONFIG

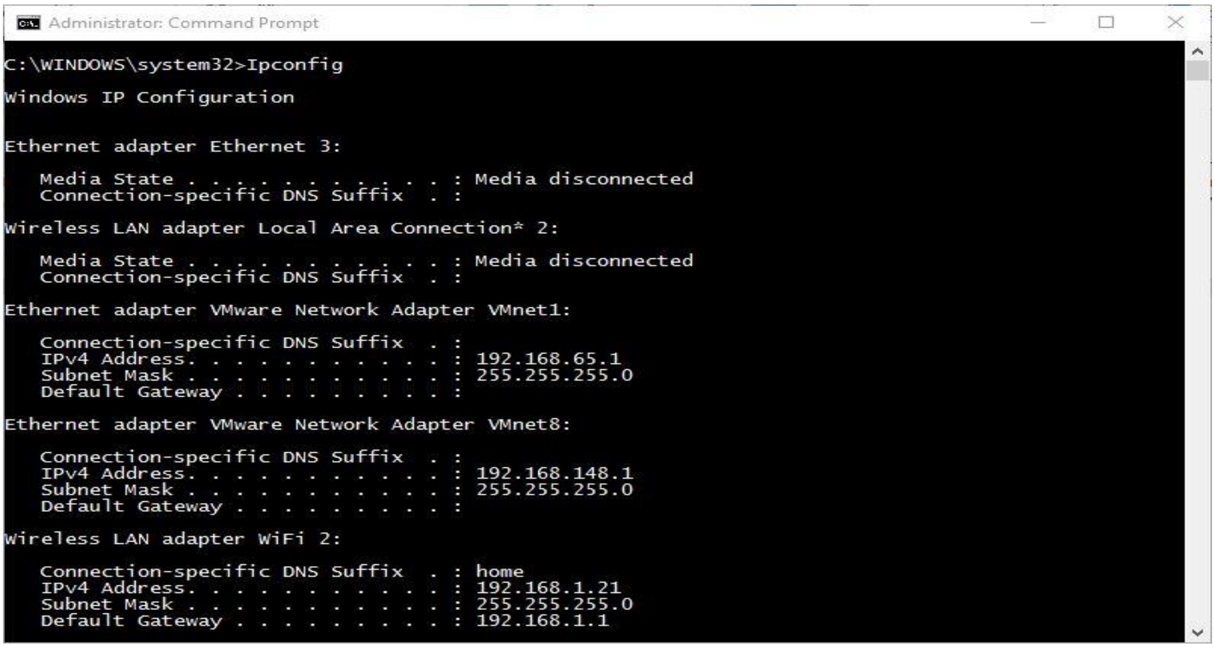
Apparatus/ Equipment Required:

PC connected with internet connection.

Procedure:

Troubleshoot the internet connectivity by using PING and IPCONFIG.

1. Open Command Prompt, and then type ipconfig. From the display of the ipconfig command, ensure that the network adapter for the TCP/IP configuration you are testing is not in a Media disconnected state.



```
C:\WINDOWS\system32>Ipconfig
Windows IP Configuration

Ethernet adapter Ethernet 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.65.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.148.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
Wireless LAN adapter WiFi 2:

   Connection-specific DNS Suffix  . : home
   IPv4 Address. . . . . . . . . . . : 192.168.1.21
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

3. At the command prompt, ping the loopback address by typing ping 127.0.0.1.

Command:

C:\>ping 127.0.0.1

4. Ping the IP address of the computer.

Command:

C:\> ping 192.168.1.1

5. Ping the IP address of the default gateway. If the ping command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.

6. Ping the IP address of a remote host (a host that is on a different subnet).

If the ping command fails, verify that the remote host IP address is correct, that the remote host is operational, and that all of the gateways (routers) between this computer and the remote host are operational.

7. Ping the IP address of the DNS server.

If the ping command fails, verify that the DNS server IP address is correct that the DNS server is operational, and that all of the gateways (routers) between this computer and the DNS server are operational.

Result:

Troubleshoot the internet connectivity by using IPCONFIG and PING command successfully.

Experiment-10

Aim of the experiment: Installation of Network Operating System (NOS)

Apparatus/ Equipment Required:

1. High configuration Computer for server
2. NOS software

Theory:

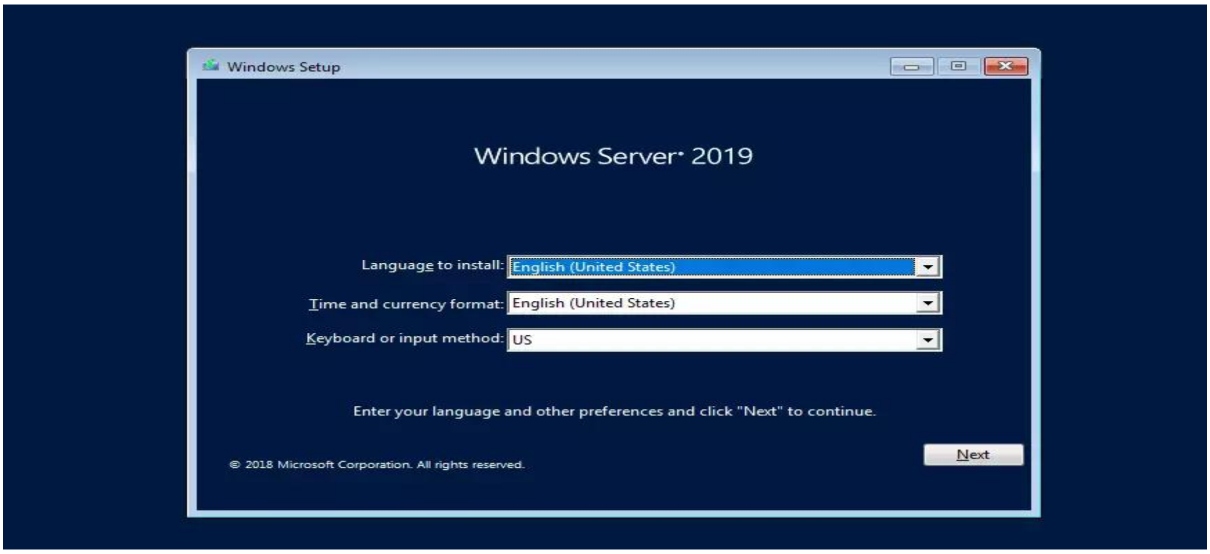
Network Operating System is a computer operating system that facilitates to connect and communicate various autonomous computers over a network.

Some of the NOS are Microsoft Windows server

Procedure:

Installation step of NOS- Microsoft Windows Server 2019

1. **Insert** a bootable USB or DVD medium and start your Computer.
2. On the first screen, select installation language, Time and keyboard layout the click "**Next**".



Language to install: English (United States)

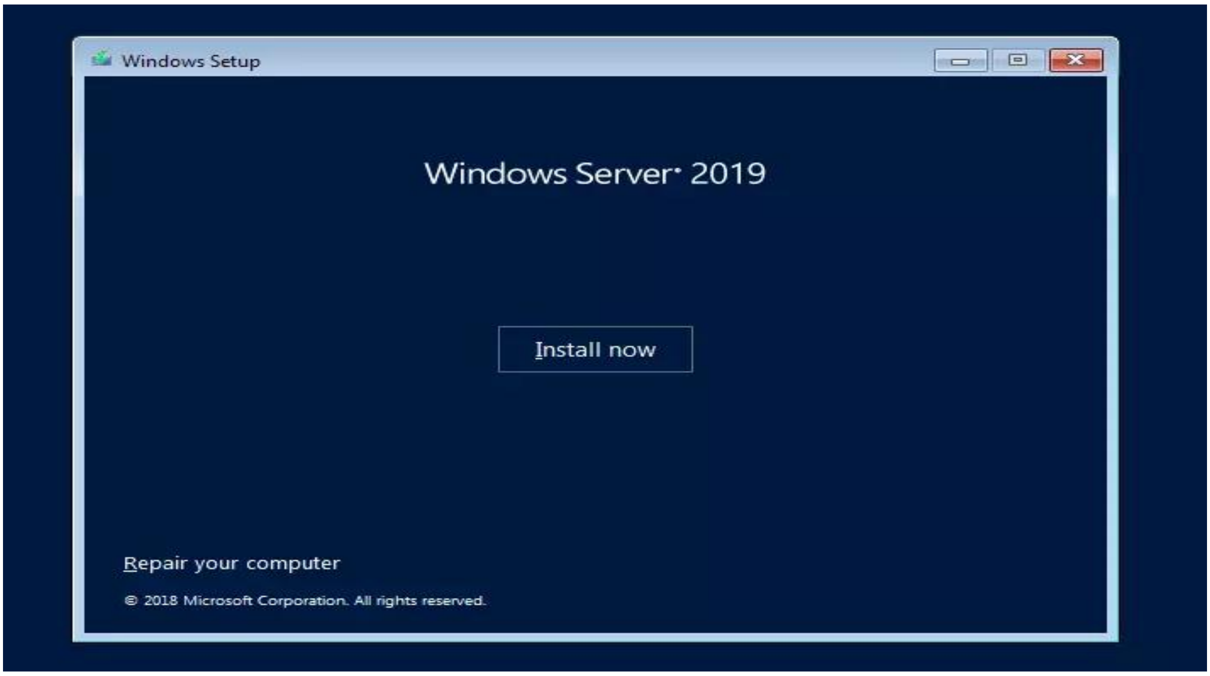
Time and currency format: English (United States)

Keyboard or input method: US

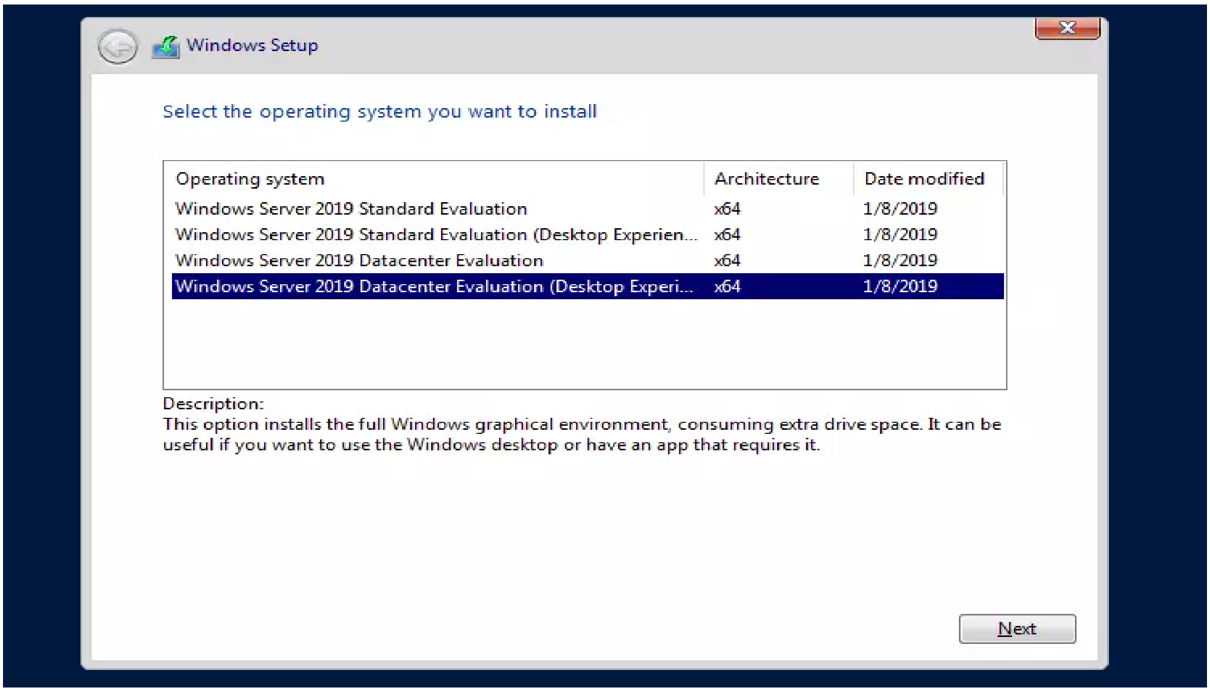
Enter your language and other preferences and click "Next" to continue.

© 2018 Microsoft Corporation. All rights reserved.

3. Start the installation by clicking on "**Install Now**".



4. The setup should start in a short while.
5. Select the Windows Server 2019 edition to install and click **Next**.

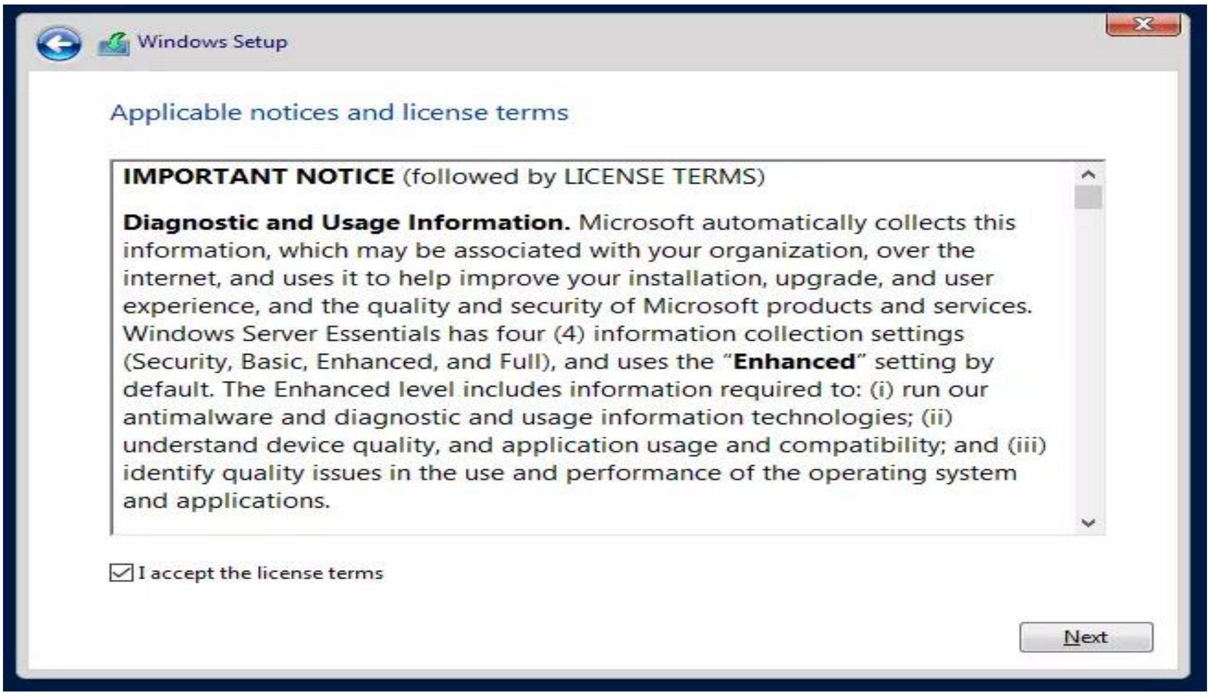


Select the operating system you want to install

Operating system	Architecture	Date modified
Windows Server 2019 Standard Evaluation	x64	1/8/2019
Windows Server 2019 Standard Evaluation (Desktop Experien...	x64	1/8/2019
Windows Server 2019 Datacenter Evaluation	x64	1/8/2019
Windows Server 2019 Datacenter Evaluation (Desktop Experi...	x64	1/8/2019

Description:
This option installs the full Windows graphical environment, consuming extra drive space. It can be useful if you want to use the Windows desktop or have an app that requires it.

6. Read the License terms and agree to them to start the installation by checking the box **“I accept the license terms**“.



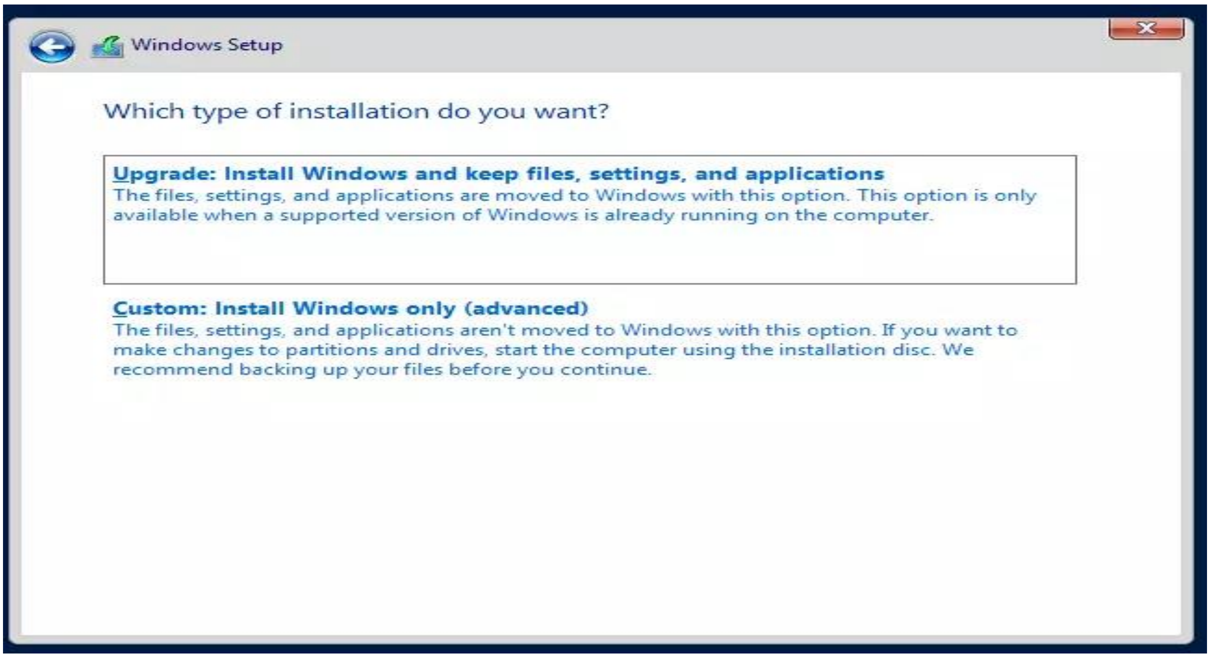
Applicable notices and license terms

IMPORTANT NOTICE (followed by LICENSE TERMS)

Diagnostic and Usage Information. Microsoft automatically collects this information, which may be associated with your organization, over the internet, and uses it to help improve your installation, upgrade, and user experience, and the quality and security of Microsoft products and services. Windows Server Essentials has four (4) information collection settings (Security, Basic, Enhanced, and Full), and uses the "**Enhanced**" setting by default. The Enhanced level includes information required to: (i) run our antimalware and diagnostic and usage information technologies; (ii) understand device quality, and application usage and compatibility; and (iii) identify quality issues in the use and performance of the operating system and applications.

☑ I accept the license terms

7. if this is the first installation of Windows Server 2019 on the server, select (Custom: Install Windows only).

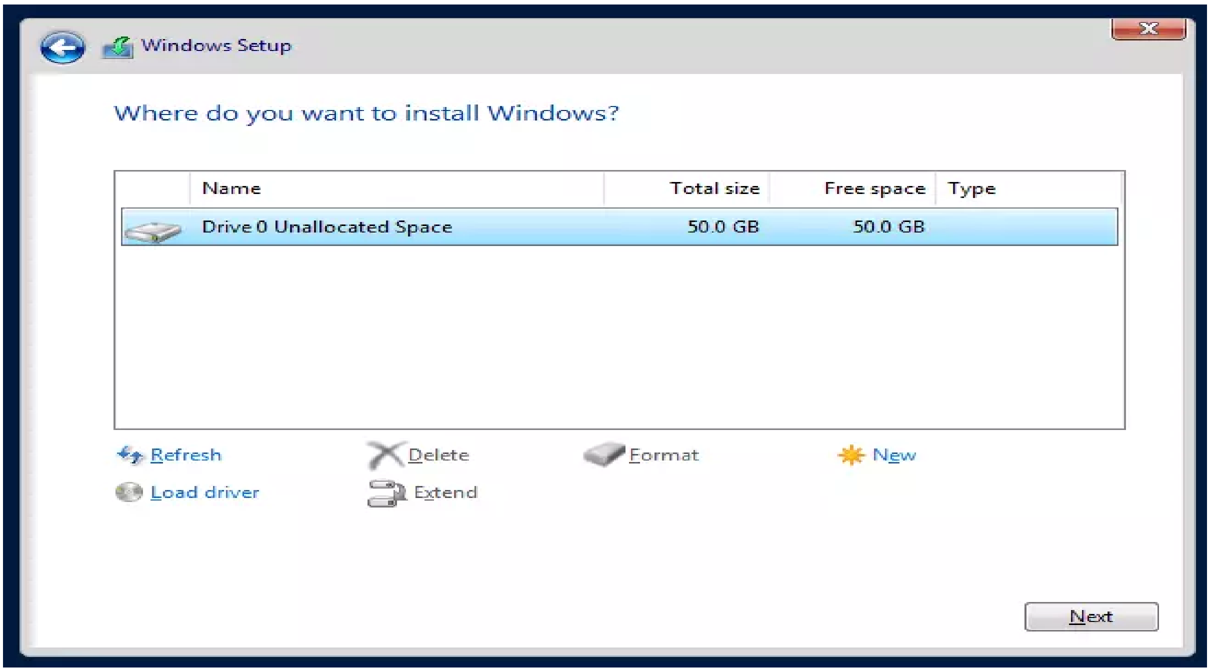


Which type of installation do you want?

Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.

Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.

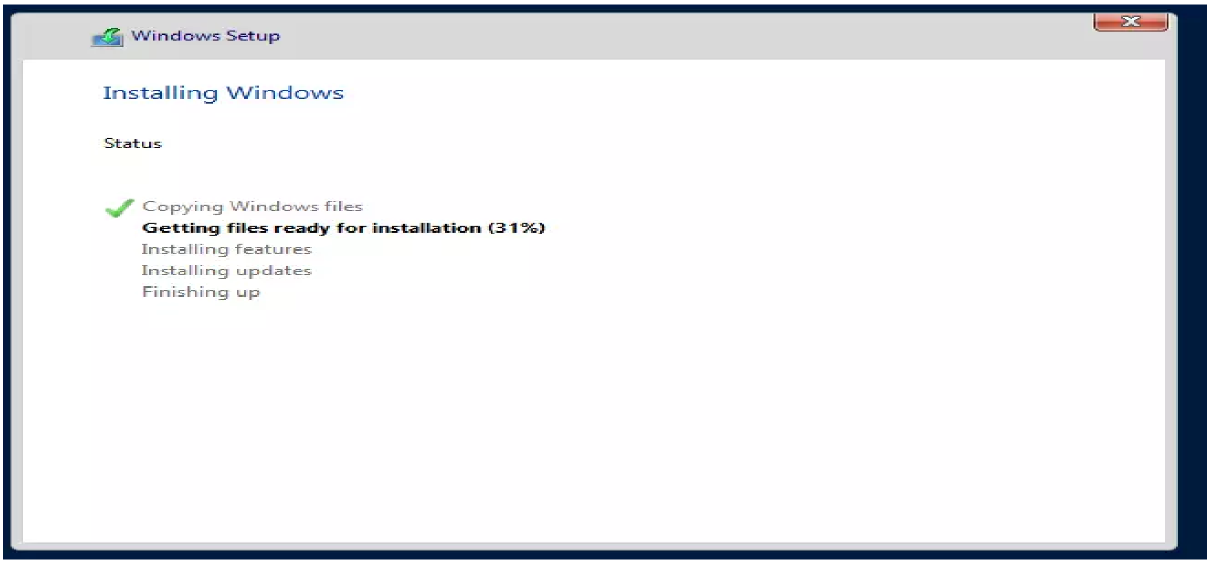
8. Select a partition to install Windows Server, you can optionally create new one from available or use total available size by clicking “**Next**“.



Where do you want to install Windows?

	Name	Total size	Free space	Type
	Drive 0 Unallocated Space	50.0 GB	50.0 GB	

9. The installation should start, wait for it to finish.



Installing Windows

Status

✓ Copying Windows files
Getting files ready for installation (31%)
Installing features
Installing updates
Finishing up

10. The system should automatically reboot after the installation. Set Administrator password when prompted on the next screen.
11. Click **Finish** to complete the installation. To login with the Administrator user, use Ctrl + Alt + Del key combination.

Result:

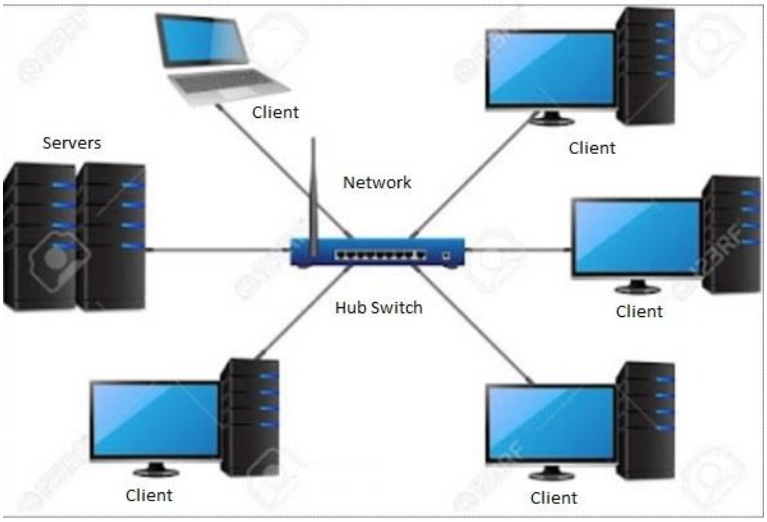
The network operating system “Windows Server 2019” successfully installed.

Experiment-11

Aim of the experiment: Create a network of at least 6 computers.
Apparatus/ Equipment Required:

1. 06 no's of computers (01 server and 05 clients)
2. Switch
3. Required Cables

Procedure:



1. Take the computer for which you are making server, insert the second LAN in that computer.
2. Connect your internet connection into the first LAN (inbuilt) on that computer.
3. Enter the IP address which you got from your ISP and check whether you can able to use internet on that system.
4. Now make sure that the second LAN is detected and is showing Unplugged.
5. Open properties of the first LAN (inbuilt LAN) and then go to "Advanced" option which is available on the top, then check both the boxes and say ok. and close everything.
6. Now take an Internet cable which is crimped on both the sides with same colours of wires.
7. Connect one end to the second LAN and the other end to the switch.
8. Now open your second LAN properties and go to the TCP/IP properties and there enter IP address as (192.168.0.1) or anything you wish Subnet Mask (255.255.255.0) and the gateway as (192.168.0.1).
9. Now open click on the switch and you will get a notification on your server saying that "Local Area Connection 2" is connected.
10. Now take another Internet cable and one end of that cable should be in any one port of the Switch and the other should be in the second computer.
11. Now you will get a notification that you are connected to internet, open the LAN properties and enter the IP address as (192.168.0.2) subnet mask and gateway should be same as server.

Result:

Successfully created a network using 06 nos of computers.

Experiment-12

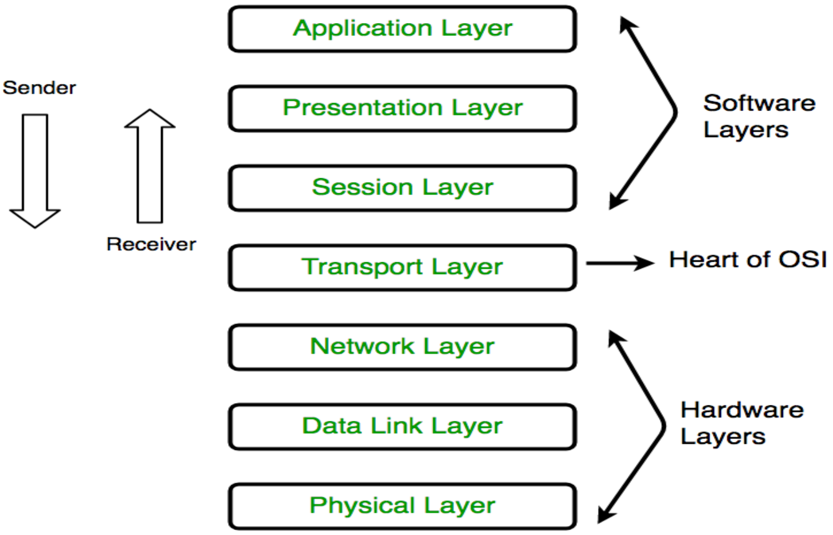
Aim of the experiment: Study of Layers of Network and Configuring Network Operating System.

Apparatus/ Equipment Required:

PC connected with internet connection.

Theory:

Layers of Network:



1. Physical Layer (Layer 1):

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. This layer is responsible for Bit synchronization, Bit rate control, Physical topologies, Transmission mode.

2. Data Link Layer (DLL) (Layer 2):

The data link layer is responsible for the node to node delivery of the message. This layer is responsible for Framing, Physical addressing, Error control, Flow Control, Access control.

3. Network Layer (Layer 3):

Network layer works for the transmission of data from one host to the other located in different networks. This layer is responsible for Routing, Logical Addressing.

4. Transport Layer (Layer 4):

Transport layer provides services to application layer and takes services from network layer. This layer is responsible for Segmentation and Reassembly, Service Point Addressing.

5. Session Layer (Layer 5):

This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.

6. Presentation Layer (Layer 6):

Presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

7. Application Layer (Layer 7):

At the very top of the OSI Reference Model stack of layers is Application layer which produce the data, which has to be transferred over the network.

Ex: Application – Browsers, Skype Messenger etc.

Procedure:

Configuring Network Operating System.

Basic Task:

- Check for System update
- Setup time zone
- Assign Static IP Address
- Enable Remote Desktop
- Rename server

Configuration steps:

1. Open server manger on virtual box.
2. Click on local server and download windows update and update the window.
3. Click on the Time zone to set the time accordingly.
4. Click on the Ethernet, it will redirect to the network connection wizard (Control panel→network and internet→ network connection)
5. Right click on the Ethernet, go to properties, select internet protocol version4(TCP/IP4).
6. Click on the properties, select the second option
   “Use the following IP address”
   IP Address 172.16.72.5
   Subnet mask 255.255.255.0
   Default gateway 172.16.72.1
   “Use the following DNS server address”
   Preferred DNS server 172.16.72.5
   Alternate DNS server 8.8.8.8
7. Click on ok and close all the console.
8. Click on the remote desktop and turn it to enable and click on refresh button.
9. Close all the open window and restart the computer.

Result:

Network operating system “Windows server 2019” successfully configured.

Experiment-13

Aim of the experiment: Study of Routing and Switching, configuring of Switch and Routers, troubleshooting of networks.

Apparatus/ Equipment Required:

CISCO Packet Tracer software

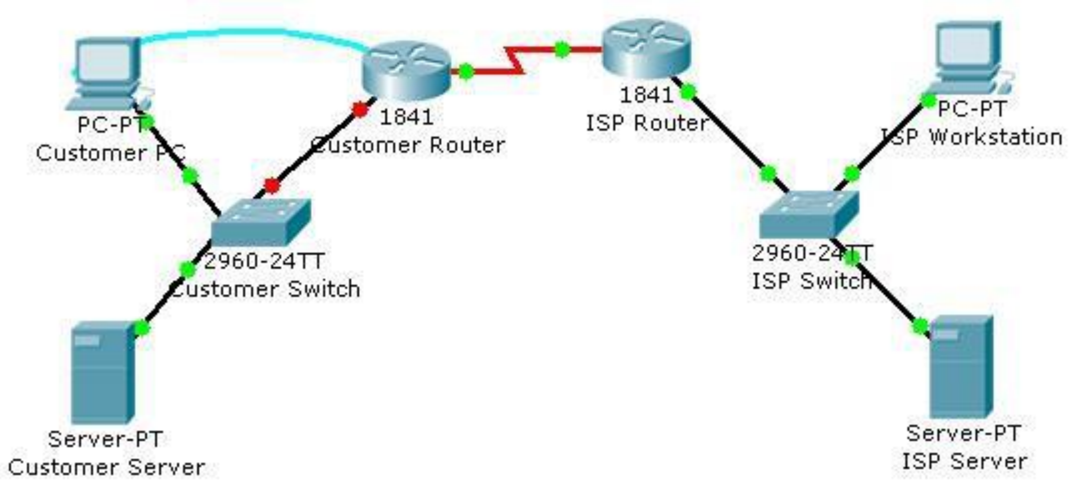
Theory:

Routing and Switching:

Routing and switching are the basic functions of network communication. Routing and Switching are different functions of network communications. The function of Switching is to switch data packets between devices on the same network (or same LAN - Local Area Network). The function of Routing is to Route packets between different networks (between different LANs - Local Area Networks).

Procedure:

Switch configuration (configuration of Cisco Catalyst 2960 switch.):



Topology Diagram

Step 1: Configure the switch host name.

a. From the Customer PC, use a console cable and terminal emulation software to connect to the console of the customer Cisco Catalyst 2960 switch.

b. Set the host name on the switch to **GpblsSwitch** using these commands.

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname GpblsSwitch
```

Step 2: Configure the privileged mode password and secret.

a. From global configuration mode, configure the password as **cisco**.

```
GpblsSwitch (config)#enable password gpbls
```

b. From global configuration mode, configure the secret as **gpbls123**.

```
GpblsSwitch (config)#enable secret gpbls123
```

Step 3: Configure the console password.

a. From global configuration mode, switch to configuration mode to

configure the console line. GpblsSwitch (config)#**line console 0**

b. From line configuration mode, set the password to **cisco** and require the password to be entered at login.

```
GpblsSwitch (config-
line)#password gpbls
GpblsSwitch (config-line)#login
GpblsSwitch (config-line)#exit
```

Step 4: Configure the vty password.

a. From global configuration mode, switch to the configuration mode for the vty lines 0 through 15.

```
GpblsSwitch (config)#line vty 0 15
```

b. From line configuration mode, set the password to **cisco** and require the password to be entered at login.

```
GpblsSwitch (config-
line)#password gpbls
GpblsSwitch (config-line)#login
GpblsSwitch (config-line)#exit
```

Step 5: Configure an IP address on interface VLAN1.

a. From global configuration mode, switch to interface configuration mode for VLAN1, and assign the IP address 192.168.1.5 with the subnet mask of 255.255.255.0.

```
GpblsSwitch (config)#interface vlan 1
GpblsSwitch (config-if)#ip address 192.168.1.5  255.255.255.0
GpblsSwitch (config-if)#no shutdown
GpblsSwitch (config-if)#exit
```

Step 6: Configure the default gateway.

a. From global configuration mode, assign the default gateway to 192.168.1.1.

```
GpblsSwitch (config)#ip default-gateway 192.168.1.1
```

b. Click the **Check Results** button at the bottom of this instruction window to check your work.

Step 7: Verify the configuration.

a. The Customer Switch should now be able to ping the ISP Server at 209.165.201.10. The first one or two pings may fail while ARP converges.

```
GpblsSwitch (config)#end
GpblsSwitch #ping 209.165.201.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.10, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 181/189/197 ms
  GpblsSwitch #
```

b. Router configuration (Cisco Router 1841 ISR)

Step 1: Configure the router host name.

a. On Customer PC, use the terminal emulation software to connect to the console of the customer Cisco

1841 ISR.

b. Set the host name on the router to **GpblsRouter** by using these commands.

```
Router>enable
Router#configure terminal
Router(config)#hostname
GpblsRouter
```

Step 2: Configure the privileged mode and secret passwords.

a. In global configuration mode, set the password to **cisco**.
b. GpblsRouter(config)#**enable password gpbls**
c. Set an encrypted privileged password to **gpbls123** using the **secret** command.
d. GpblsRouter (config)#**enable secret gpbls123**

Step 3: Configure the console password.

a. In global configuration mode, switch to line configuration mode to specify the console line.

```
GpblsRouter (config)#line console 0
```

Set the password to **gpbls123**, require that the password be entered at login, and then exit line configuration mode.

```
GpblsRouter (config-line)#password gpbls123
GpblsRouter (config-
line)#login GpblsRouter
(config-line)#exit
GpblsRouter (config)#
```

Step 4: Configure the vty password to allow Telnet access to the router.

a. In global configuration mode, switch to line configuration mode to specify the vty lines.

```
GpblsRouter (config)#line vty 0 4
```

Set the password to **gpbls123**, require that the password be entered at login, exit line configuration mode, and then

exit the configuration session.

```
GpblsRouter (config-line)#password gpbls123
GpblsRouter (config-
line)#login GpblsRouter
(config-line)#exit
GpblsRouter (config)#
```

Step 5: Configure password encryption, a MOTD banner, and turn off domain server lookup.

a. Currently, the line passwords and the enable password are shown in clear text when you show the running configuration. Verify this now by entering the **show running-config** command.

b. To avoid the security risk of someone looking over your shoulder and reading the passwords, encrypt all clear text passwords.

```
GpblsRouter (config)#service password-encryption
```

c. Use the **show running-config** command again to verify that the passwords are encrypted. To provide a warning when someone attempts to log in to the router, configure a MOTD banner.

```
GpblsRouter (config)#banner motd $Authorized Access Only!
```

d. Test the banner and passwords. Log out of the router by typing the **exit** command twice. The banner displays before the prompt for a password. Enter the password to log back into the router.

e. You may have noticed that when you enter a command incorrectly at the user or privileged EXEC prompt, the router pauses while trying to locate an IP address for the mistyped word you entered. For example, this output shows what happens when the **enable** command is mistyped.

```
GpblsRouter >emable
```

f. Translating "enable"...domain server (255.255.255.255)

g. To prevent this from happening, use the following command to stop all DNS lookups from the router CLI.

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

h. Save the running configuration to the startup configuration.

```
GpblsRouter(config)#end
GpblsRouter#copy run start
```

Step 6: Verify the configuration.

a. Log out of your terminal session with the Cisco 1841 customer router.

b. Log in to the Cisco 1841 Customer Router. Enter the console password when prompted.

c. Navigate to privileged EXEC mode. Enter the privileged EXEC password when prompted.

d. Click the **Check Results** button at the bottom of this instruction window to check your work

Result:

configuration of Cisco Catalyst 2960 switch and 1841 Router successfully done.

Experiment-14

Aim of the experiment: Study of Scaling of Networks, Design verities of LAN and forward of Traffic.

Apparatus/ Equipment Required:

CISCO Packet Tracer software

Theory:

The Scaling Networks defines the architecture, components, and operations of routers and switches in a larger and more complex network. It includes how to configure routers and switches for advanced functionality. It also includes configuration and troubleshoot routers and switches and resolve common issues with OSPF, EIGRP, STP, and VTP in both IPv4 and IPv6 networks.

Procedure:

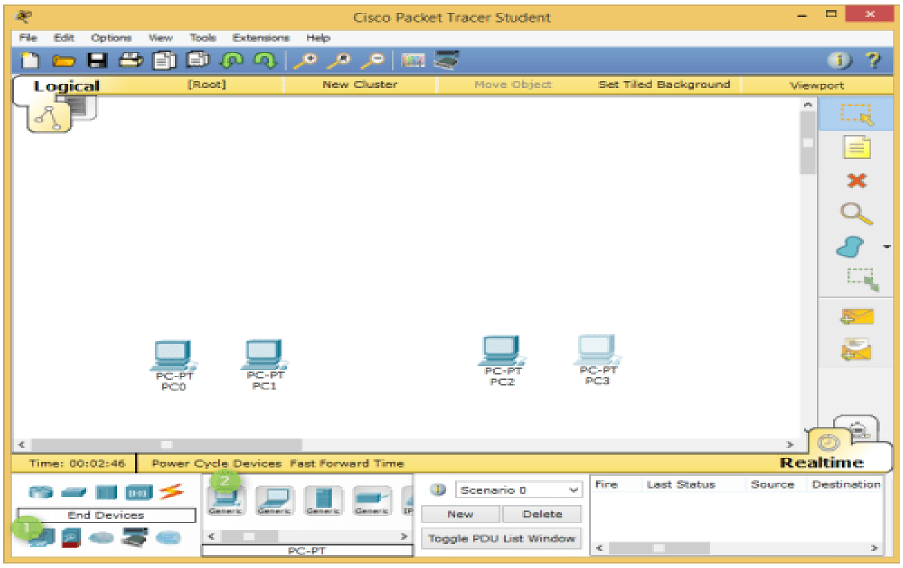
Design varieties of LAN and forward of Traffic:

Adding PCs in Cisco Packet Tracer

To add PCs in Cisco Packet Tracer, you need to perform the following steps:

In the Cisco Packet Tracer console, click on the PC icon, click Generic, and then click in the logical view area to add a Generic PC.

Repeat the same step to add three more Generic PCs in the logical view area, as shown in the following figure.



Adding Switches in Cisco Packet Tracer

To add a switch in Cisco Packet Tracer, click the Switch icon, select a switch type, such as 2960, and then add the selected switch in the logical view area.

Repeat the same step to add one more switch.

Adding Routers in Cisco Packet Tracer

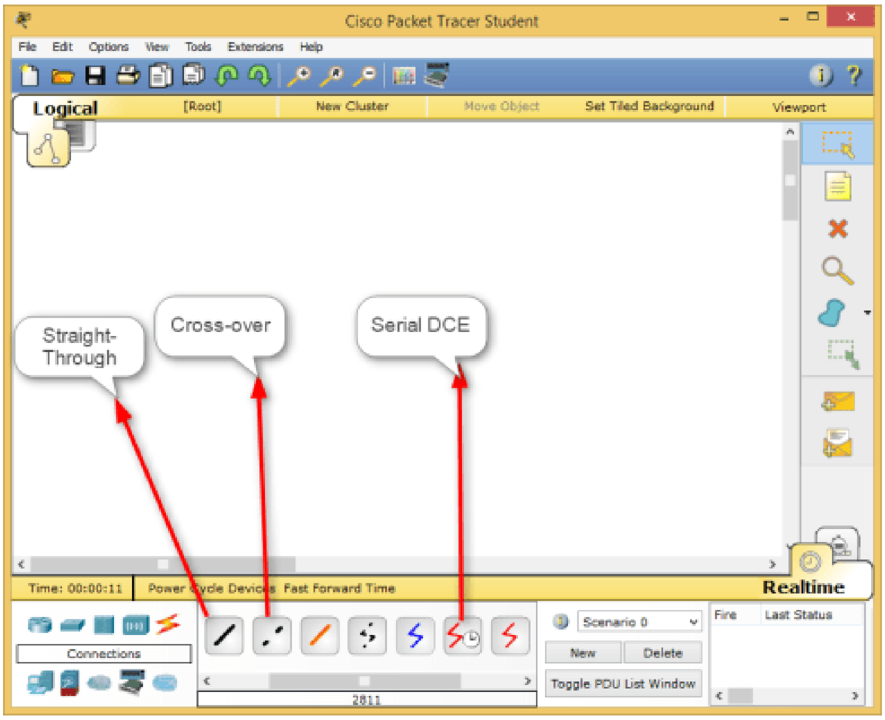
To add a router in Cisco Packet Tracer, click the Router icon, select a router type, such as 2811, and then add the selected router in the logical view area.

Repeat the same step to add one more router.

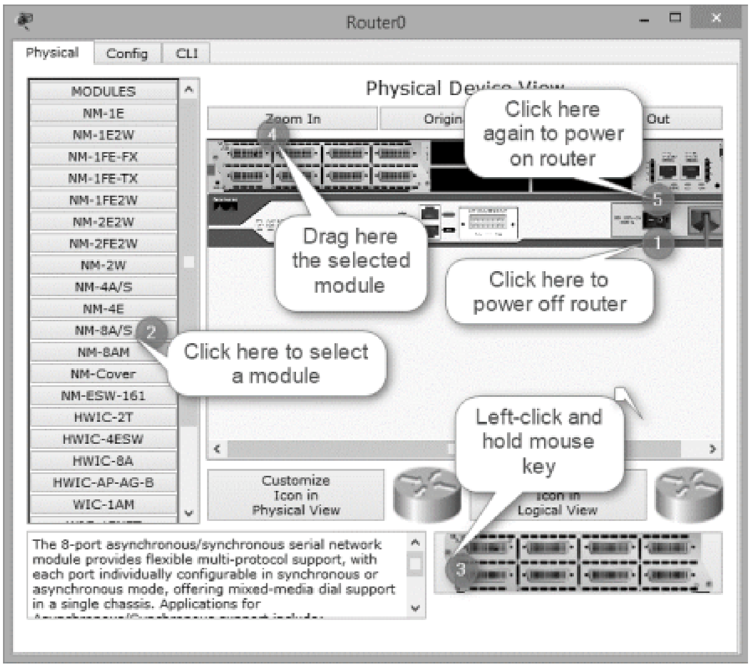
Types of Connection in Cisco Packet Tracer

Straight-through: Used to connect different types of devices (devices that use different wiring standards), such as Router-to-Switch and Switch-to-PC.

Cross-over: Used to connect same types of devices, such as router-to-router, PC-to-PC, and switch-to-switch.
Serial DCE: Used to connect router-to-router in a WAN network.
Console: Used to take console (using hyper terminal) of a router on a PC.



Customize the interfaces before it can be used to connect other network devices. To do this, double-click Router0, on the Router0 properties dialog box, click the Power button to power off Router0.



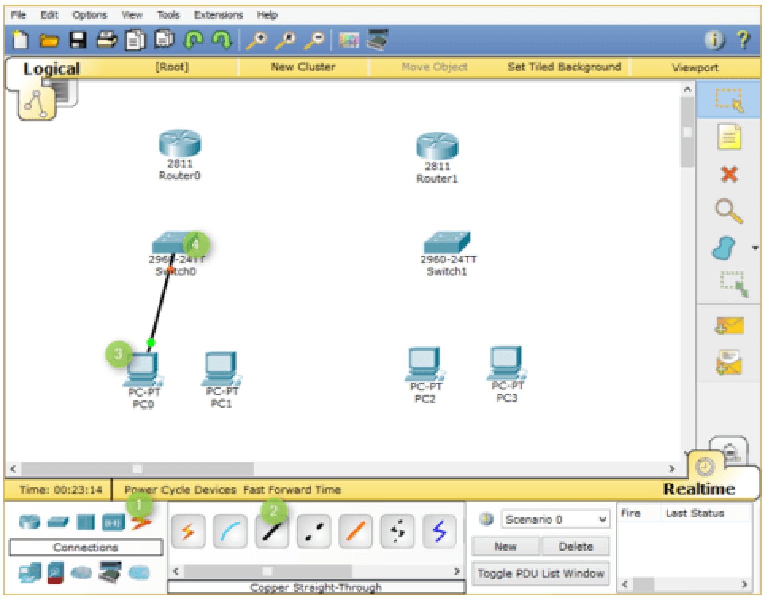
The 8-port asynchronous/synchronous serial network module provides flexible multi-protocol support, with each port individually configurable in synchronous or asynchronous mode, offering mixed-media dial support in a single chassis. Applications for

Now, open the Router1 properties dialog box, add the same module to Router1 also, and then close the Router1 properties dialog box.

Connecting Devices in Cisco Packet Tracer

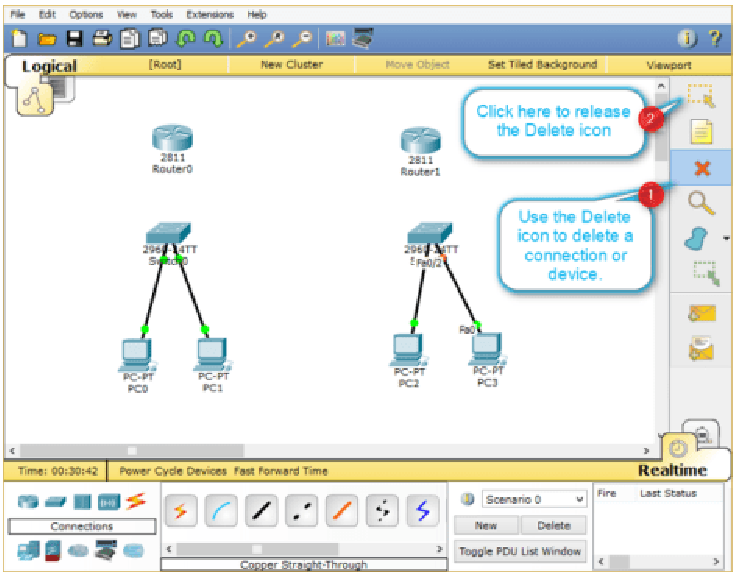
To connect devices in Cisco Packet Tracer, click the connection type icon, and select an appropriate cable. For example, to connect PC0 to Switch0, select the straight-through cable, click on PC0, select the FastEthernet0 interface.

Next, click on Switch0, and then select the FastEthernet0/1 interface. The following figure displays how to connect a PC to a switch in Cisco Packet Tracer.



Now, add PC1 to Switch0 using the FastEthernet0/2 interface. Also, add PC2 and PC3 to the FastEthernet0/1 and FastEthernet0/2 interfaces of Switch1, respectively.

If you have connected a wrong device to a wrong interface, you can use the Delete option to delete a connection or device. The following figure displays how to use the Delete option to delete a device or connection in Cisco Packet Tracer.


1 Use the Delete icon to delete a connection or device.

2 Click here to release the Delete icon

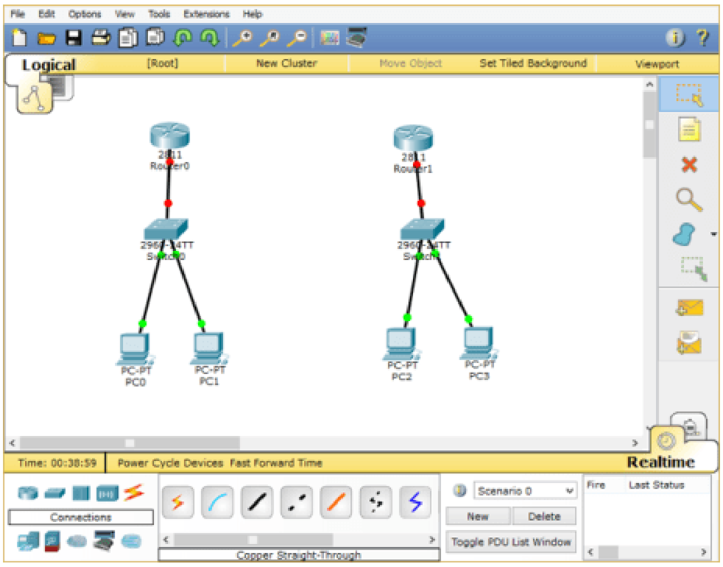
Once, you have connected all the PCs to switches, now, connect Switch0 to Router0, and Switch1 to Router1 using the straight-through cables.

Select the straight-through cable, click on Switch0, and then select FastEthernet0/3 interface.

Click Router0 and select the FastEthernet0/0 interface.

Select again the straight-through cable, click on Switch1, and select FastEthernet0/3 interface.

Next, click Router1 and then select the FastEthernet0/0 interface.

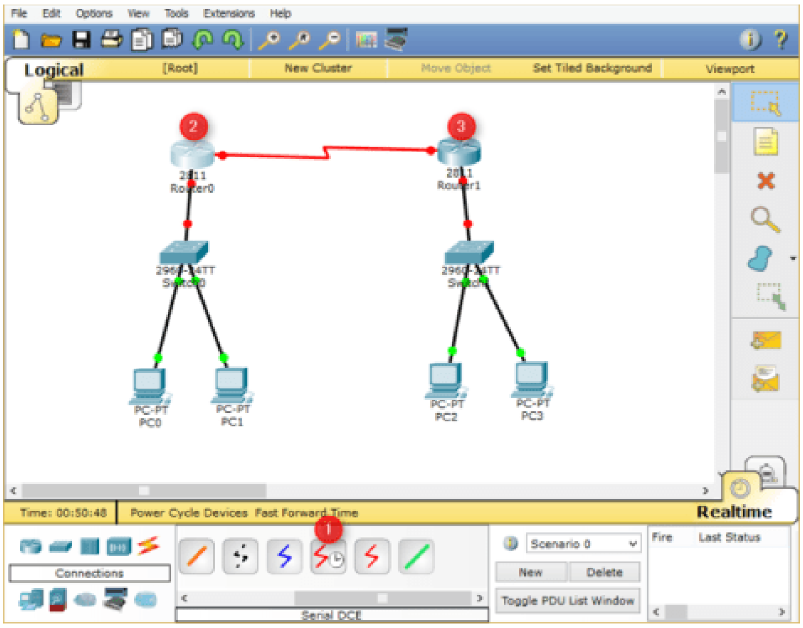


Interconnecting Routers in Cisco Packet Tracer

Now, connect Router0 to Router1 using the serial connection. To do this, you need to perform the following steps:

Select the Serial DCE cable, click on Router0, and select the Serial1/0 interface.

Click on Router1 and select the Serial1/0 interface, as shown in the following figure.



Result:

Verities of LAN is created successfully.

Experiment-15

Aim of the experiment: Study WAN concepts and Configure and forward Traffic in WAN.

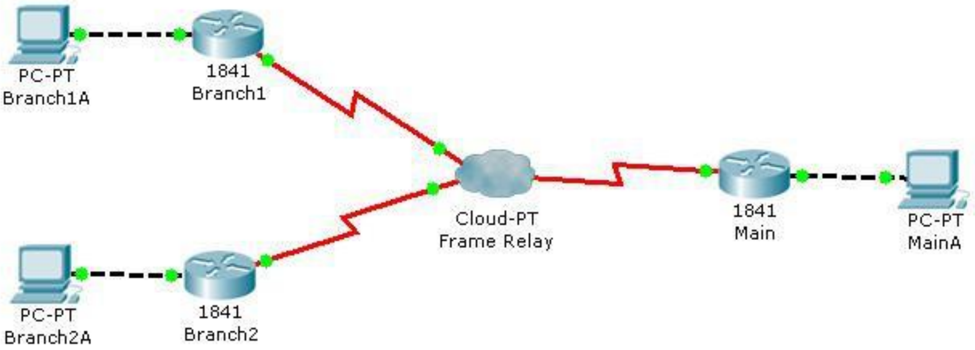
Apparatus/ Equipment Required:

CISCO Packet Tracer software

Theory:

Wide Area Network, or WAN, is used to connect physically separated locations on a network. WANs can connect buildings that are across town or across the world on the same network. There are various techniques to do this, but two of the most common are hub and spoke and full mesh networks topologies.

Configure and forward Traffic in WAN:



Step 1: Configuration of Branch1 and Branch2 (Switch).

a. Click on Branch1 and use various show commands to view the connectivity to the network. b. Use the show running-configuration command to view the router configuration.

c. Use the show ip interface brief command to view the status of the interfaces.

d. Use the various show frame-relay map, show frame-relay pvc, and show frame-relay lmi commands to see the status of the Frame-relay circuit.

e. Click on Branch 2 and use various show commands to view the connectivity to the network. f. Use the show running-configuration command to view the router configuration.

g. Use the show ip interface brief command to view the status of the interfaces.

h. Use the various show frame-relay map, show frame-relay pvc, and show frame-relay lmi commands to see the status of the Frame-relay circuit.

Step 2: Configuration of Main (Router).

a. Click on Main and use a variety of show commands to view the connectivity to the network. b. Use the show running-configuration command to view the router configuration.

c. Use the show ip interface brief command to view the status of the interfaces.

d. To view the status of the frame-relay configurations use the show frame-relay lmi, show frame- relay map, and show frame-relay pvc commands.

Result:

Configuration of WAN done successfully.

Experiment-16

Aim of the experiment: Configure IPv4 and IPv6 and learn Quality, security and other services.

Procedure:

Configure IPv4:

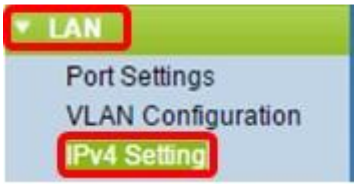
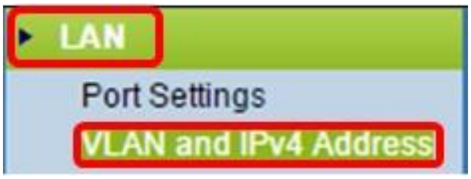
Configure IPv4 DHCP

Step 1. Log in to the web-based utility and choose LAN > IPv4 Setting or LAN > VLAN and IPv4 Address depending on the WAP model you have.

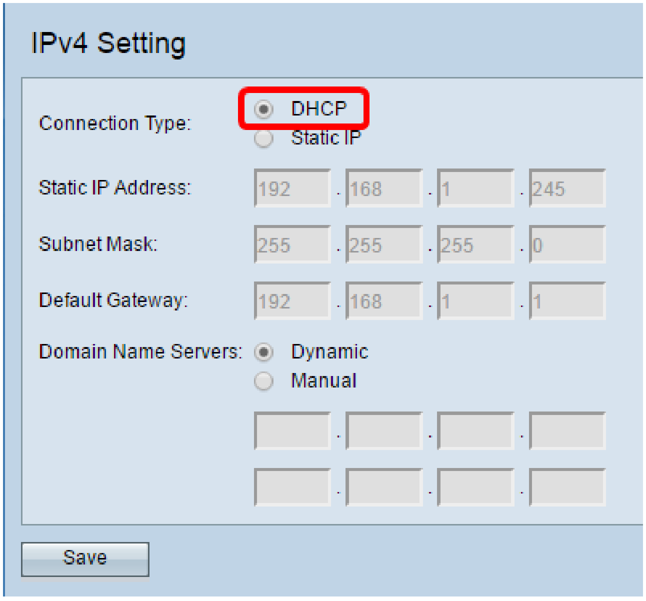
Configure IPv4

Configure IPv4 DHCP

Step 1. Log in to the web-based utility and choose LAN > IPv4 Setting or LAN > VLAN and IPv4 Address depending on the WAP model you have.

WAP131, WAP150, WAP351, WAP361, WAP571, WAP571E	WAP121, WAP321, WAP371, WAP551, WAP561
	

Step 2. In the Connection Type area, click **DHCP** radio button to automatically obtain an IP address. This setting is chosen by default.



IPv4 Setting

Connection Type: ● DHCP ○ Static IP

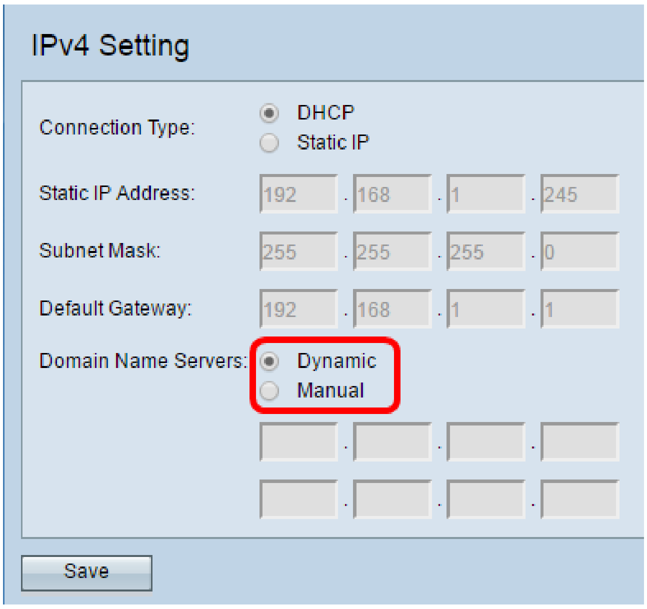
Static IP Address: 192 . 168 . 1 . 245

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 1 . 1

Domain Name Servers: ● Dynamic ○ Manual

Step 3. Choose your preferred DNS configuration from the Domain Name Servers radio buttons.



IPv4 Setting

Connection Type: ● DHCP ○ Static IP

Static IP Address: 192 . 168 . 1 . 245

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 1 . 1

Domain Name Servers: ● Dynamic ○ Manual

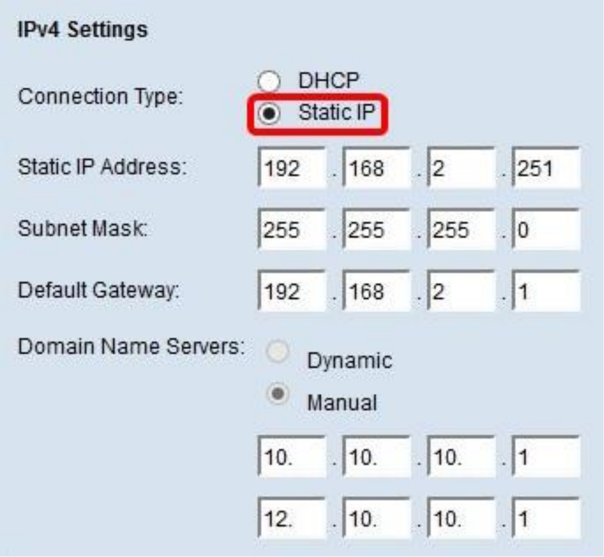
The available options are defined as follows:

- Dynamic — WAP acquires the Domain Name Server (DNS) addresses from a DHCP server on the Local Area Network (LAN). If you choose this option, skip to Step 4.
- Manual — Allows you to manually configure one or more DNS server addresses in the Domain Name Servers fields.

Step 4. Click Save.

Configure Static IPv4 Address

Step 1. Click the radio button for Static IP.



IPv4 Settings

Connection Type: ○ DHCP ● Static IP

Static IP Address: 192 . 168 . 2 . 251

Subnet Mask: 255 . 255 . 255 . 0

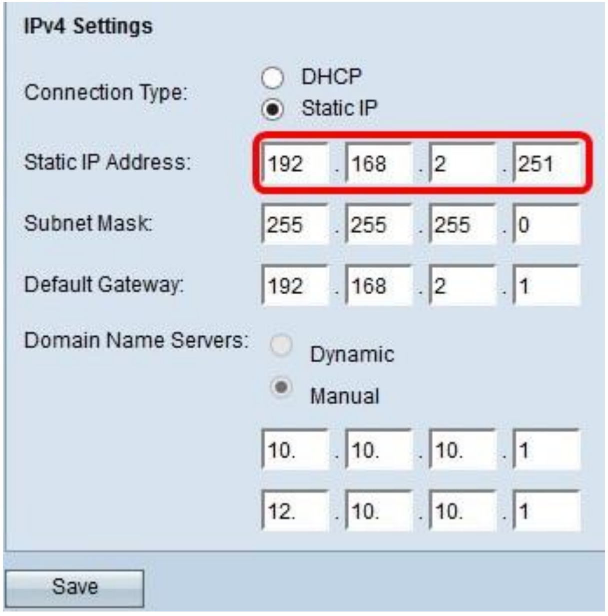
Default Gateway: 192 . 168 . 2 . 1

Domain Name Servers: ○ Dynamic ● Manual

10. . 10. . 10. . 1

12. . 10. . 10. . 1

Step 2. Enter an IP address for the access point in the Static IP Address field.



IPv4 Settings

Connection Type: ○ DHCP ● Static IP

Static IP Address: 192 . 168 . 2 . 251

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 2 . 1

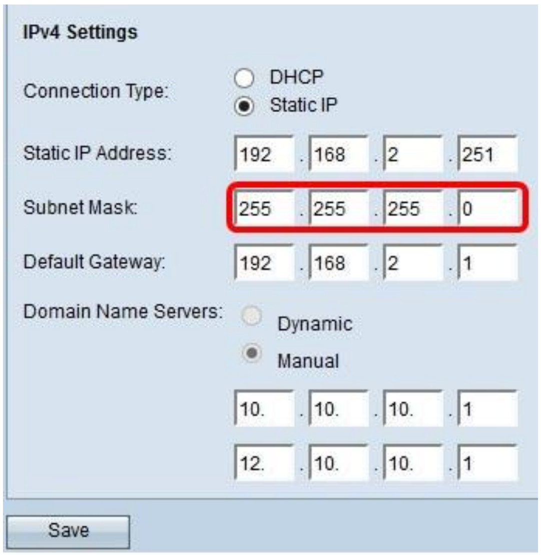
Domain Name Servers: ○ Dynamic ● Manual

10. . 10. . 10. . 1

12. . 10. . 10. . 1

Step 3. Enter the subnet mask of the network in the *Subnet Mask* field.

Note: The default mask is 255.255.255.0



IPv4 Settings

Connection Type: ○ DHCP ● Static IP

Static IP Address: 192 . 168 . 2 . 251

Subnet Mask: 255 . 255 . 255 . 0

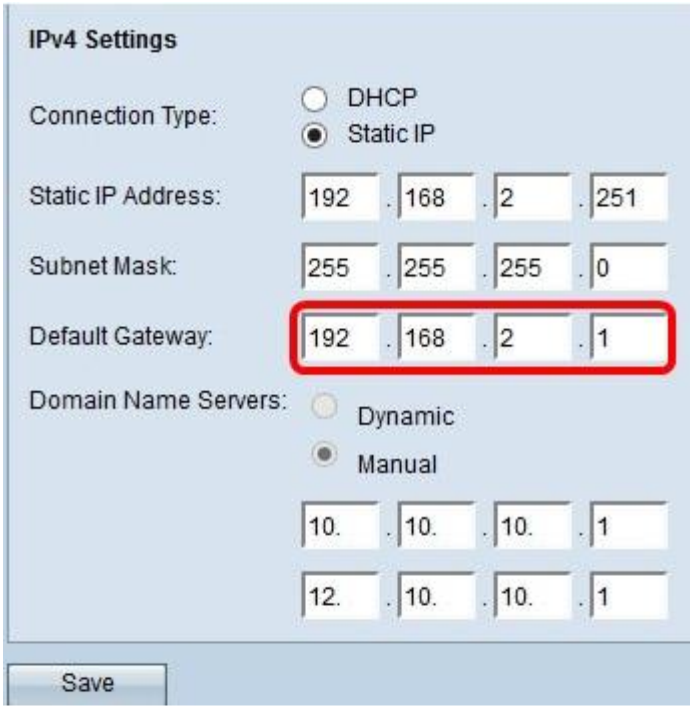
Default Gateway: 192 . 168 . 2 . 1

Domain Name Servers: ○ Dynamic ● Manual

10. . 10. . 10. . 1

12. . 10. . 10. . 1

Step 4. Enter the default gateway IP address in the *Default Gateway* field.



IPv4 Settings

Connection Type: ○ DHCP ● Static IP

Static IP Address: 192 . 168 . 2 . 251

Subnet Mask: 255 . 255 . 255 . 0

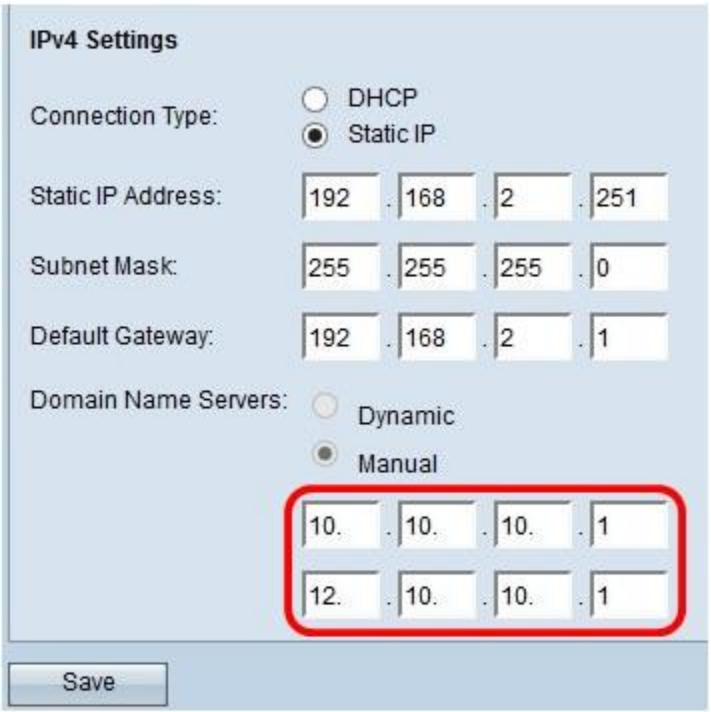
Default Gateway: 192 . 168 . 2 . 1

Domain Name Servers: ○ Dynamic ● Manual

10. . 10. . 10. . 1

12. . 10. . 10. . 1

Step 5. Enter the IP address of the DNS in the *Domain Name Ser*ver fields.



IPv4 Settings

Connection Type: ○ DHCP ● Static IP

Static IP Address: 192 . 168 . 2 . 251

Subnet Mask: 255 . 255 . 255 . 0

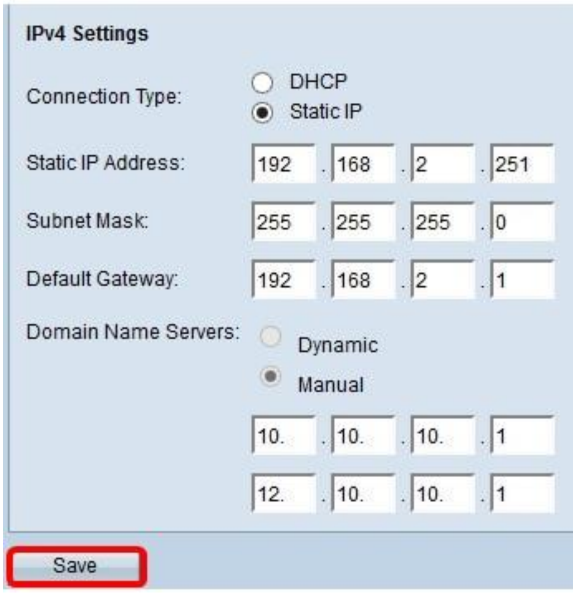
Default Gateway: 192 . 168 . 2 . 1

Domain Name Servers: ○ Dynamic ● Manual

10. . 10. . 10. . 1

12. . 10. . 10. . 1

Step 6. Click **Save**.



IPv4 Settings

Connection Type: ○ DHCP ● Static IP

Static IP Address: 192 . 168 . 2 . 251

Subnet Mask: 255 . 255 . 255 . 0

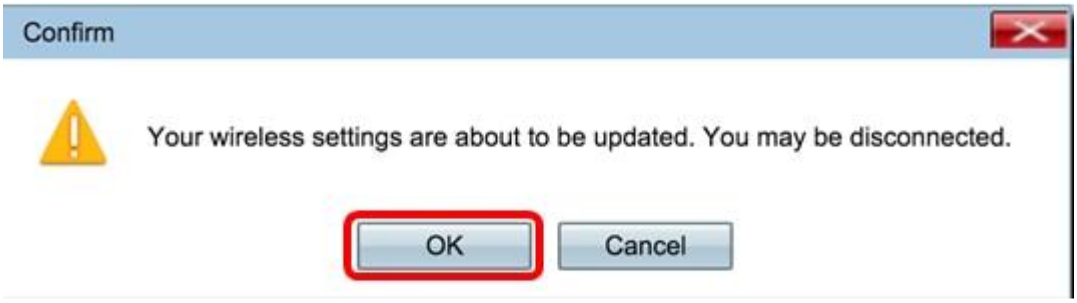
Default Gateway: 192 . 168 . 2 . 1

Domain Name Servers: ○ Dynamic ● Manual

10. . 10. . 10. . 1

12. . 10. . 10. . 1

Step 7. If you have pre-configured settings before, a pop-up window will appear confirming the wireless settings are about to be updated and that possible disconnections may happen. Click OK.



Confirm

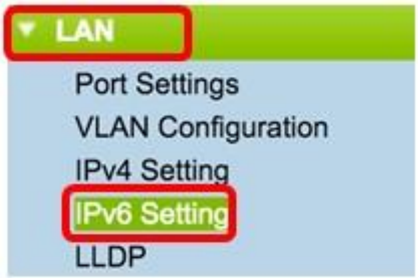
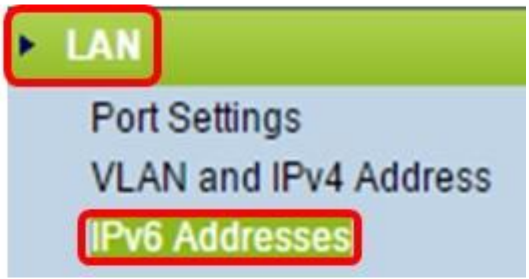
Your wireless settings are about to be updated. You may be disconnected.

You should now have statically configured the IPv4 address.

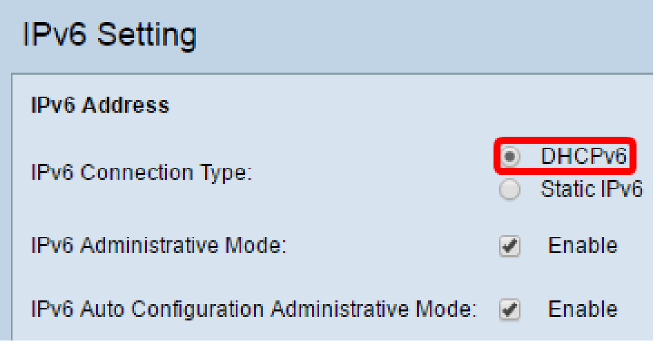
Configure IPv6

Configure IPv6 DHCP

Step 1. Log in to the web-based utility and choose LAN > IPv6 Setting or LAN > IPv6 Addresses.

WAP131, WAP150, WAP351, WAP361, WAP571, and WAP571E	WAP121, WAP321, WAP371, WAP551, and WAP561
 LAN Port Settings VLAN Configuration IPv4 Setting IPv6 Setting LLDP	 LAN Port Settings VLAN and IPv4 Address IPv6 Addresses

Step 2. Click **DHCPv6** as the IPv6 Connection Type. The IPv6 connection type tells the device how to obtain IPv6 address.



IPv6 Setting

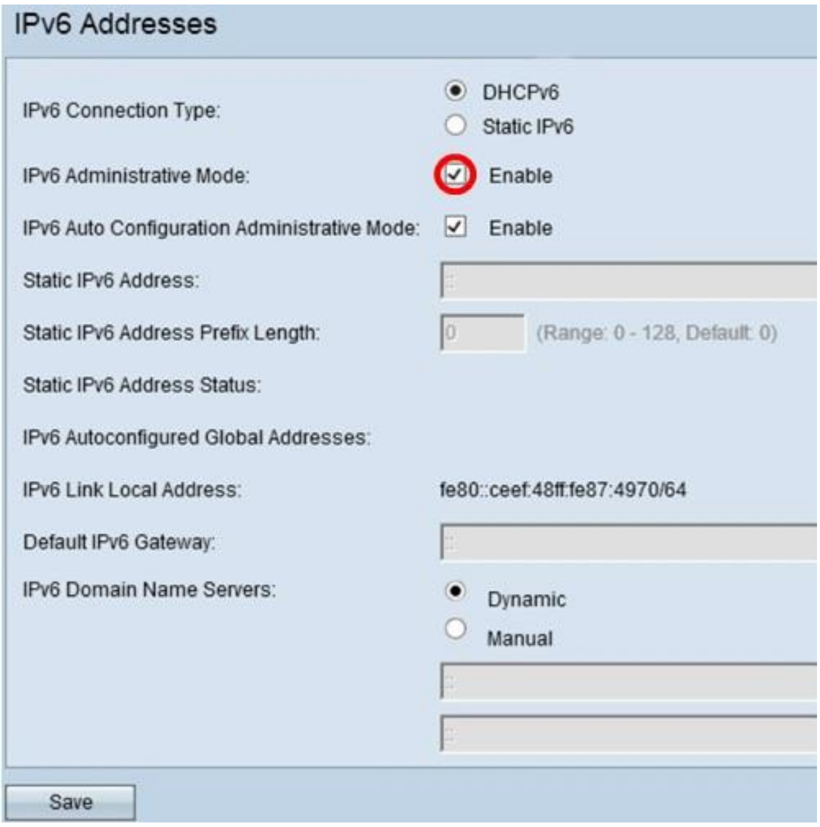
IPv6 Address

IPv6 Connection Type: ● DHCPv6 ○ Static IPv6

IPv6 Administrative Mode: ☑ Enable

IPv6 Auto Configuration Administrative Mode: ☑ Enable

Step 3. To permit IPv6 management access to the access point, check the Enable IPv6 Administrative Mode check box.



IPv6 Addresses

IPv6 Connection Type: ● DHCPv6 ○ Static IPv6

IPv6 Administrative Mode: ☑ Enable

IPv6 Auto Configuration Administrative Mode: ☑ Enable

Static IPv6 Address: ::

Static IPv6 Address Prefix Length: 0 (Range: 0 - 128, Default: 0)

Static IPv6 Address Status:

IPv6 Autoconfigured Global Addresses:

IPv6 Link Local Address: fe80::ceef:48ff:fe87:4970/64

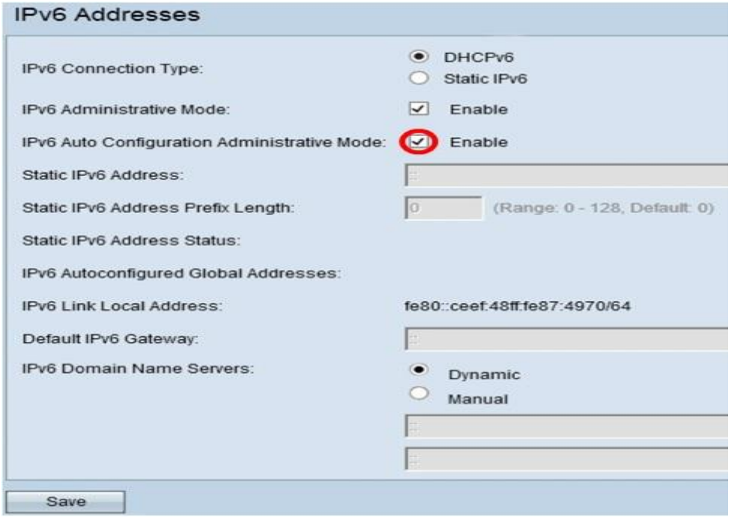
Default IPv6 Gateway: ::

IPv6 Domain Name Servers: ● Dynamic ○ Manual

::

::

Step 4. To learn its IPv6 addresses and gateway through router advertisements received on the LAN port, check the Enable IPv6Auto Configuration Administrative Mode check box. Access points can have multiple auto-configured IPv6 addresses.



IPv6 Addresses

IPv6 Connection Type: ● DHCPv6 ○ Static IPv6

IPv6 Administrative Mode: ☑ Enable

IPv6 Auto Configuration Administrative Mode: ☑ Enable

Static IPv6 Address: ::

Static IPv6 Address Prefix Length: 0 (Range: 0 - 128, Default: 0)

Static IPv6 Address Status:

IPv6 Autoconfigured Global Addresses:

IPv6 Link Local Address: fe80::ceef:48ff:fe87:4970/64

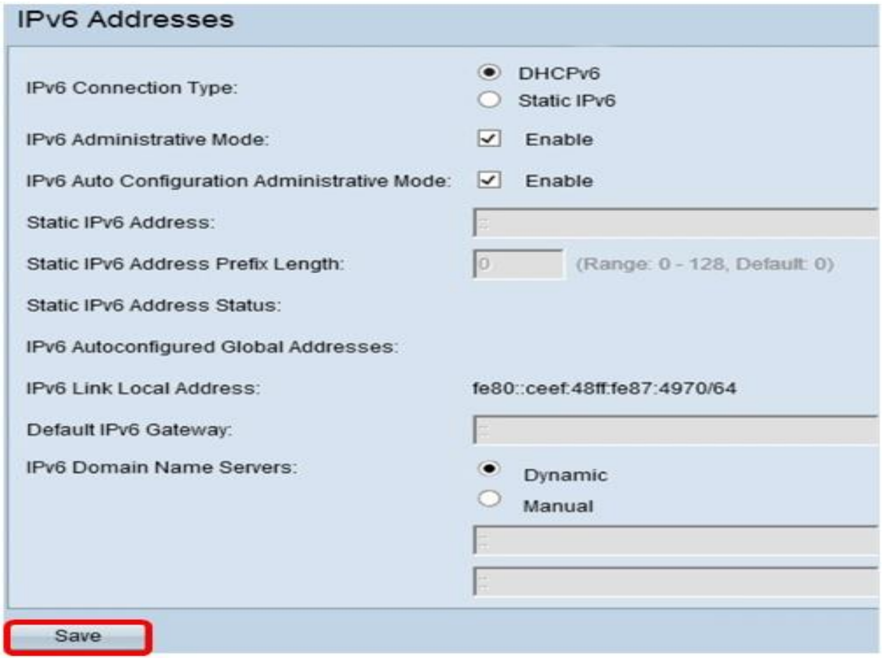
Default IPv6 Gateway: ::

IPv6 Domain Name Servers: ● Dynamic ○ Manual

::

::

Step 5. Click Save.



IPv6 Addresses

IPv6 Connection Type: ● DHCPv6 ○ Static IPv6

IPv6 Administrative Mode: ☑ Enable

IPv6 Auto Configuration Administrative Mode: ☑ Enable

Static IPv6 Address: ::

Static IPv6 Address Prefix Length: 0 (Range: 0 - 128, Default: 0)

Static IPv6 Address Status:

IPv6 Autoconfigured Global Addresses:

IPv6 Link Local Address: fe80::ceef:48ff:fe87:4970/64

Default IPv6 Gateway: ::

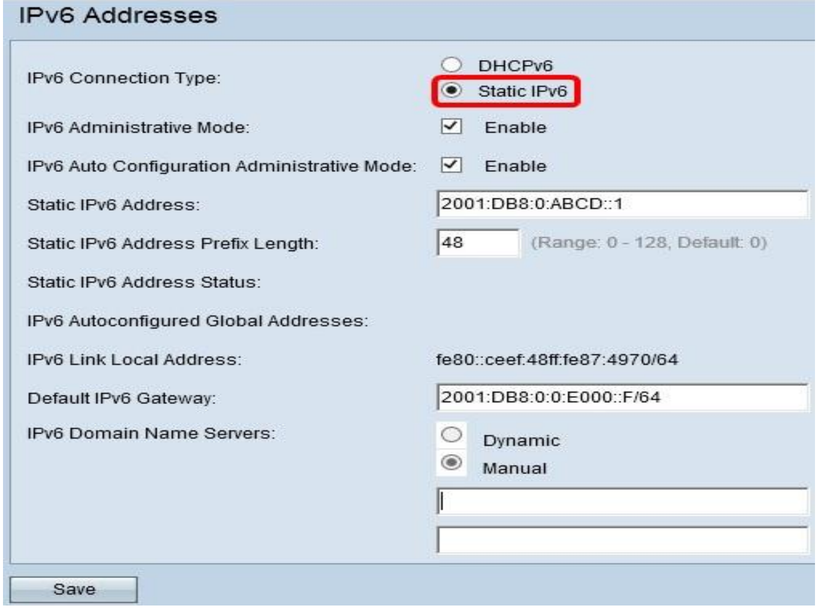
IPv6 Domain Name Servers: ● Dynamic ○ Manual

::

::

Configure Static IPv6 Address

Step 1. Click Static IPv6 as the IPv6 Connection Type to assign an IPv6 address manually to the access point.



IPv6 Addresses

IPv6 Connection Type: ○ DHCPv6 ● Static IPv6

IPv6 Administrative Mode: ☑ Enable

IPv6 Auto Configuration Administrative Mode: ☑ Enable

Static IPv6 Address: 2001:DB8:0:ABCD::1

Static IPv6 Address Prefix Length: 48 (Range: 0 - 128, Default: 0)

Static IPv6 Address Status:

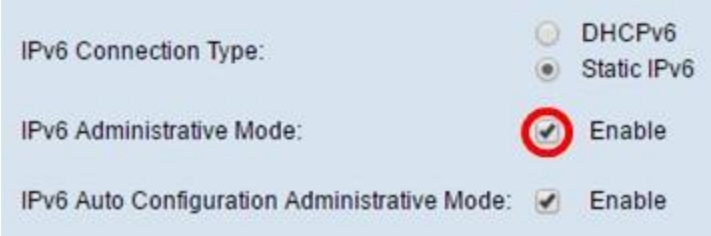
IPv6 Autoconfigured Global Addresses:

IPv6 Link Local Address: fe80::ceef:48ff:fe87:4970/64

Default IPv6 Gateway: 2001:DB8:0:0:E000::F/64

IPv6 Domain Name Servers: ○ Dynamic ● Manual

Step 2. Check the IPv6 Administrative Mode check box to enable IPv6 management access. This allows the device management interface to be accessed via an IPv6 address.

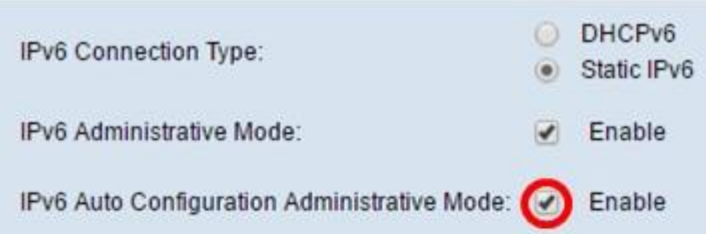


IPv6 Connection Type: ○ DHCPv6 ● Static IPv6

IPv6 Administrative Mode: ☑ Enable

IPv6 Auto Configuration Administrative Mode: ☑ Enable

Step 3. Check the IPv6 Auto Configuration Administrative Mode check box to enable IPv6 automatic address configuration on the device. This is enabled by default.

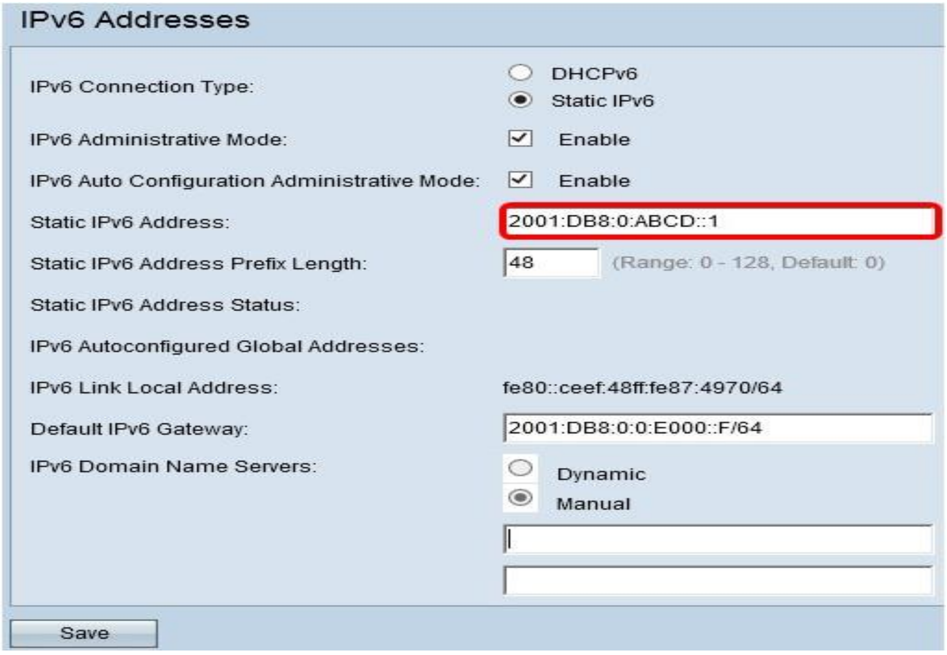


IPv6 Connection Type: ○ DHCPv6 ● Static IPv6

IPv6 Administrative Mode: ☑ Enable

IPv6 Auto Configuration Administrative Mode: ☑ Enable

Step 4. Enter the IPv6 address of the access point in the *Static IPv6 Address* field.



IPv6 Addresses

IPv6 Connection Type: ○ DHCPv6 ● Static IPv6

IPv6 Administrative Mode: ☑ Enable

IPv6 Auto Configuration Administrative Mode: ☑ Enable

Static IPv6 Address: 2001:DB8:0:ABCD::1

Static IPv6 Address Prefix Length: 48 (Range: 0 - 128, Default: 0)

Static IPv6 Address Status:

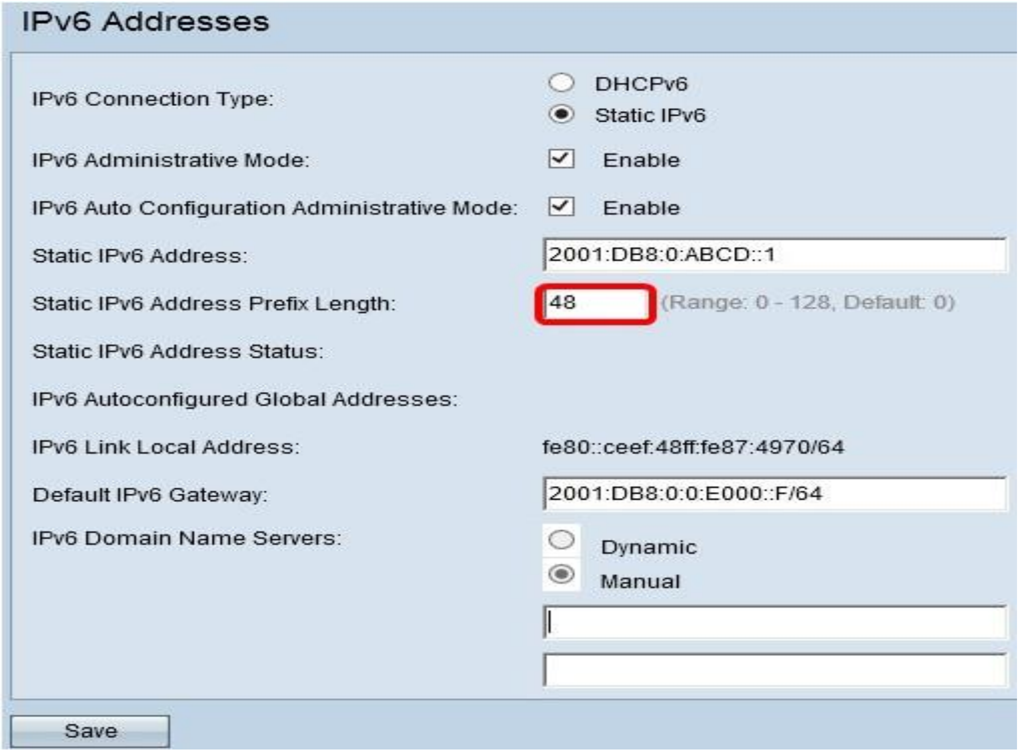
IPv6 Autoconfigured Global Addresses:

IPv6 Link Local Address: fe80::ceef:48ff:fe87:4970/64

Default IPv6 Gateway: 2001:DB8:0:0:E000::F/64

IPv6 Domain Name Servers: ○ Dynamic ● Manual

Step 5. Enter the prefix length of the static address in the Static IPv6 Address Prefix Length field.



IPv6 Addresses

IPv6 Connection Type: ○ DHCPv6 ● Static IPv6

IPv6 Administrative Mode: ☑ Enable

IPv6 Auto Configuration Administrative Mode: ☑ Enable

Static IPv6 Address: 2001:DB8:0:ABCD::1

Static IPv6 Address Prefix Length: 48 (Range: 0 - 128, Default: 0)

Static IPv6 Address Status:

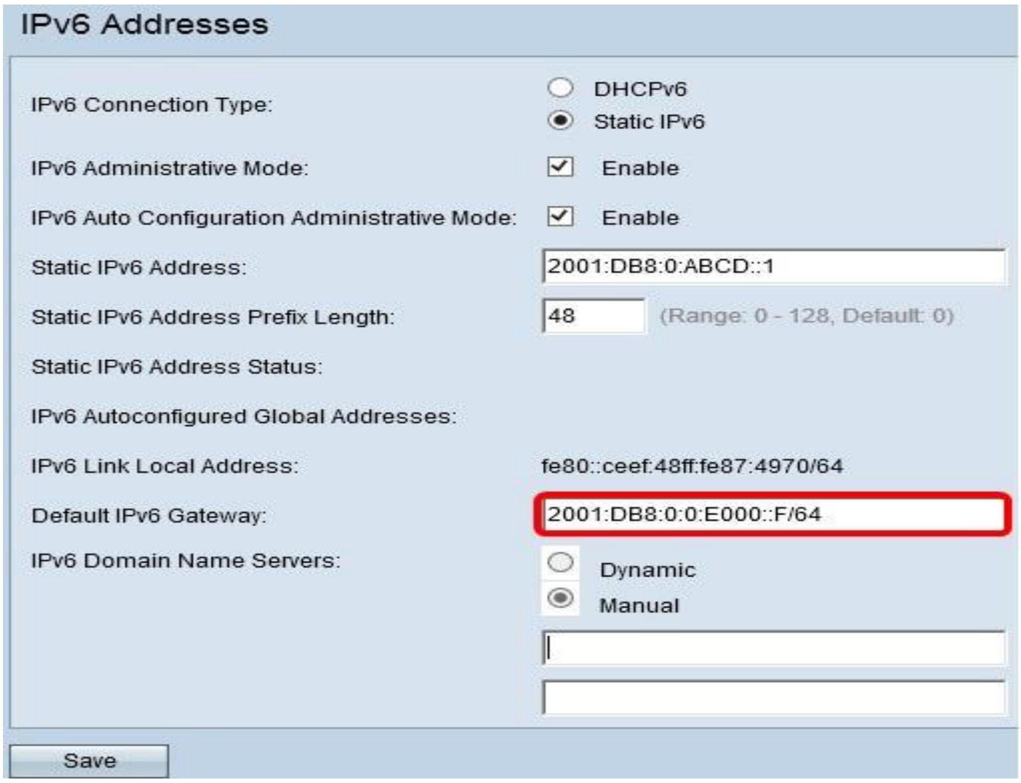
IPv6 Autoconfigured Global Addresses:

IPv6 Link Local Address: fe80::ceef:48ff:fe87:4970/64

Default IPv6 Gateway: 2001:DB8:0:0:E000::F/64

IPv6 Domain Name Servers: ○ Dynamic ● Manual

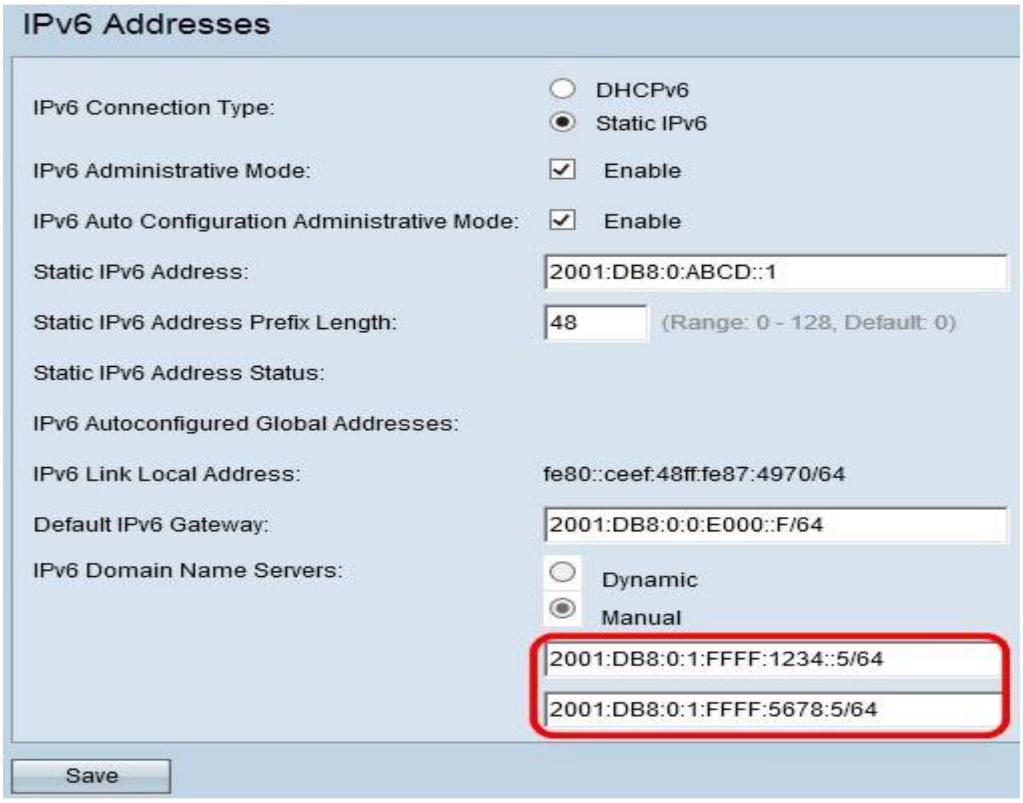
Step 6. Enter the IPv6 address of the default gateway in the Default IPv6 Gateway field.



IPv6 Addresses

IPv6 Connection Type:	○ DHCPv6 ● Static IPv6
IPv6 Administrative Mode:	☑ Enable
IPv6 Auto Configuration Administrative Mode:	☑ Enable
Static IPv6 Address:	2001:DB8:0:ABCD::1
Static IPv6 Address Prefix Length:	48 (Range: 0 - 128, Default: 0)
Static IPv6 Address Status:	
IPv6 Autoconfigured Global Addresses:	
IPv6 Link Local Address:	fe80::ceef:48ff:fe87:4970/64
Default IPv6 Gateway:	2001:DB8:0:0:E000::F/64
IPv6 Domain Name Servers:	○ Dynamic ● Manual

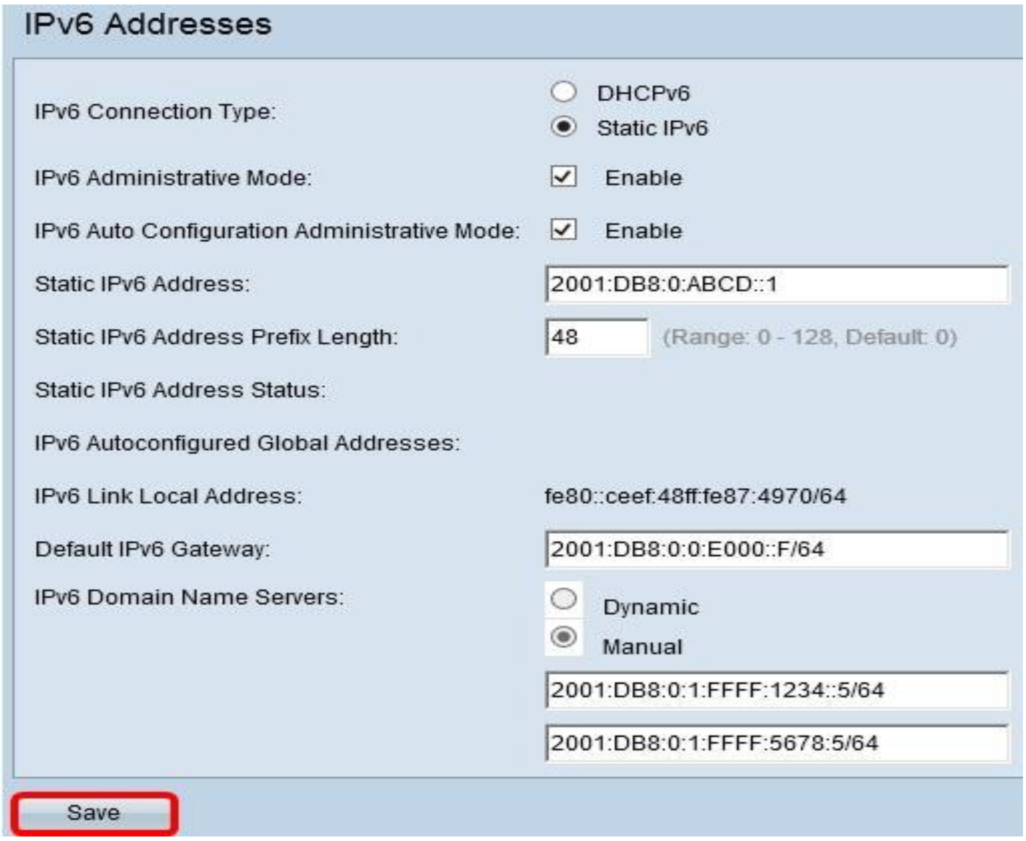
Step 7. Enter the IPv6 DNS server address in the IPv6 Domain Name Servers fields.



IPv6 Addresses

IPv6 Connection Type:	○ DHCPv6 ● Static IPv6
IPv6 Administrative Mode:	☑ Enable
IPv6 Auto Configuration Administrative Mode:	☑ Enable
Static IPv6 Address:	2001:DB8:0:ABCD::1
Static IPv6 Address Prefix Length:	48 (Range: 0 - 128, Default: 0)
Static IPv6 Address Status:	
IPv6 Autoconfigured Global Addresses:	
IPv6 Link Local Address:	fe80::ceef:48ff:fe87:4970/64
Default IPv6 Gateway:	2001:DB8:0:0:E000::F/64
IPv6 Domain Name Servers:	○ Dynamic ● Manual 2001:DB8:0:1:FFFF:1234::5/64 2001:DB8:0:1:FFFF:5678:5/64

Step 8. Click Save.



IPv6 Addresses

IPv6 Connection Type: ○ DHCPv6 ● Static IPv6

IPv6 Administrative Mode: ☑ Enable

IPv6 Auto Configuration Administrative Mode: ☑ Enable

Static IPv6 Address: 2001:DB8:0:ABCD::1

Static IPv6 Address Prefix Length: 48 (Range: 0 - 128, Default: 0)

Static IPv6 Address Status:

IPv6 Autoconfigured Global Addresses:

IPv6 Link Local Address: fe80::ceef:48ff:fe87:4970/64

Default IPv6 Gateway: 2001:DB8:0:0:E000::F/64

IPv6 Domain Name Servers: ○ Dynamic ● Manual

2001:DB8:0:1:FFFF:1234::5/64

2001:DB8:0:1:FFFF:5678:5/64

Result:

Configuration of IPv4 and IPv6 successfully done.

Experiment-18

Aim of the experiment: Troubleshoot networks.

Apparatus/ Equipment Required:

PC with internet connection.

Procedure:

1. Check the hardware. When you're beginning the troubleshooting process, check all your hardware to make sure it's connected properly, turned on, and working. If a cord has come loose or somebody has switched off an important router, this could be the problem behind your networking issues. There's no point in going through the process of troubleshooting network issues if all you need to do is plug a cord in. Make sure all switches are in the correct positions and haven't been bumped accidentally.

Next, turn the hardware off and back on again. This is the mainstay of IT troubleshooting, and while it might sound simplistic, often it really does solve the problem. Power cycling your modem, router, and PC can solve simple issues—just be sure to leave each device off for at least 60 seconds before you turn it back on.

2. Use ipconfig. Open the command prompt and type "ipconfig" (without the quotes) into the terminal. The Default Gateway (listed last) is your router's IP. Your computer's IP address is the number next to "IP Address." If your computer's IP address starts with 169, the computer is not receiving a valid IP address. If it starts with anything other than 169, your computer is being allocated a valid IP address from your router.

Try typing in "ipconfig /release" followed by "ipconfig /renew" to get rid of your current IP address and request a new one. This will in some cases solve the problem. If you still can't get a valid IP from your router, try plugging your computer straight into the modem using an ethernet cable. If it works, the problem lies with the router.

3. Use ping and tracert. If your router is working fine, and you have an IP address starting with something other than 169, the problem's most likely located between your router and the internet. At this point, it's time to use the ping tool. Try sending a ping to a well-known, large server, such as Google, to see if it can connect with your router. You can ping Google DNS servers by opening the command prompt and typing "ping 8.8.8.8"; you can also add "-t" to the end (ping 8.8.8.8 -t) to get it to keep pinging the servers while you troubleshoot. If the pings fail to send, the command prompt will return basic information about the issue. You can use the tracert command to do the same thing, by typing "tracert 8.8.8.8"; this will show you each step, or "hop," between your router and the Google DNS servers. You can see where along the pathway the error is arising. If the error comes up early along the pathway, the issue is more likely somewhere in your local network.

4. Perform a DNS check. Use the command "nslookup" to determine whether there's a problem with the server you're trying to connect to. If you perform a DNS check on, for example, google.com and receive results such as "Timed Out," "Server Failure," "Refused," "No Response from Server," or "Network Is Unreachable," it may indicate the problem originates in the DNS server for your destination. (You can also use nslookup to check your own DNS server.)

5. Contact the ISP. If all of the above turn up no problems, try contacting your internet service provider to see if they're having issues. You can also look up outage maps and related information on a smartphone to see if others in your area are having the same problem.

6. Check on virus and malware protection. Next, make sure your virus and malware tools are running correctly, and they haven't flagged anything that could be affecting part of your network and stopping it from functioning.

7. Review database logs. Review all your database logs to make sure the databases are functioning as expected. If your network is working but your database is full or malfunctioning, it could be causing problems that flow on and affect your network performance.