

Practical No.1: Configure Peer-to-Peer Network with at least three hosts

I. Practical Significance

Identify and know the use of peer to peer network
Configure peer to peer network

II. Relevant Programs Outcomes (POs)

- 1. Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
- 2. Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
- 3. Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
- 4. Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
- 5. Communication:** Communicate effectively in oral and written form.

III. Competency and Practical skills

1. Setup peer-to-peer Network

IV. Relevant Course Outcomes

Use Basic Concept of Networking for setting of Computer Network
Setup up computer Network for Specific Requirement

V. Practical Outcomes (POs)

Connect computers in Peer-to-Peer Network

VI. Relevant Affective Domain Related Outcomes

1. Follow safety practices
2. Demonstrate working as a leader/team member
3. Follow ethical practices

VII. Minimum Theoretical Background

In Peer to Peer architecture every node is connected to other node directly for exchanging information instead of connected to central server

Every computer node is referred as peer and they do the job of client as well as server both.

Every peer provides services to other peers as well as uses services provided by other peers.

❖ Configuring peer to peer network

“Crossover cable is used”

One end is used for transmitting and other end for receiving data.

Peer-to-Peer networking is when all computers are on the same network. They are considered as peers and will have to be connected to a hub, switch or a router. There is no server, controller or one in charge. Computers in a workgroup shares resources such as the printer and files.

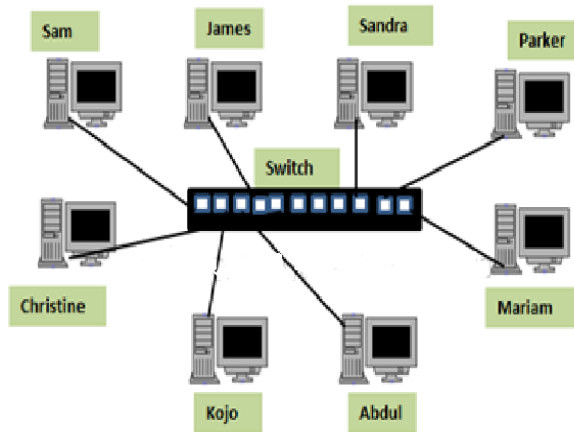
Workgroup is automatically set up when you set up a network and they all share the same subnet.

A workgroup is not protected by a password, no security is provided.

VIII. Diagrams / Experimental set-up /Work Situation

A typical example of a workgroup is shown below:

Computer Workgroup Setup

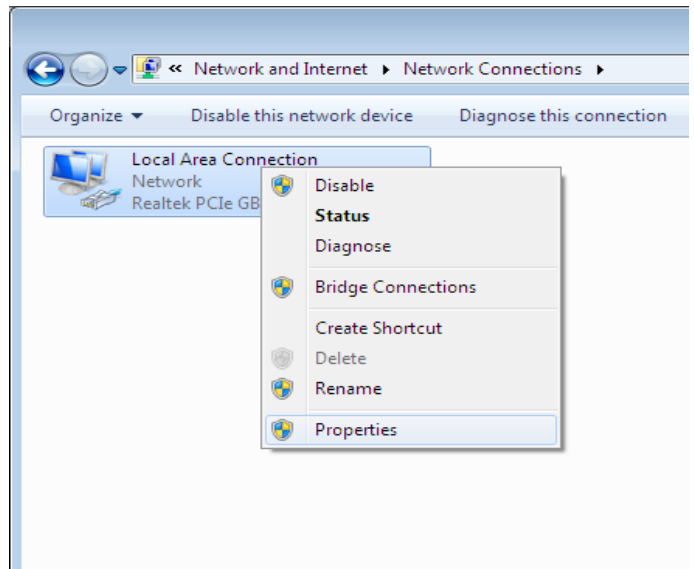
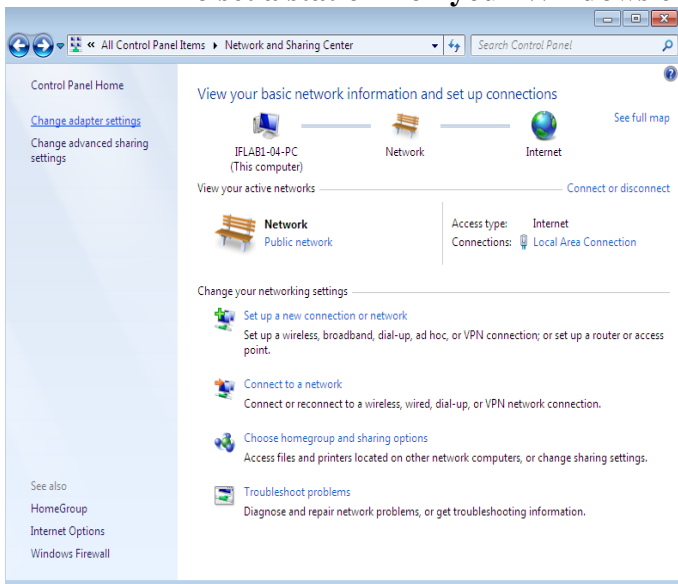


IX. Resources Required

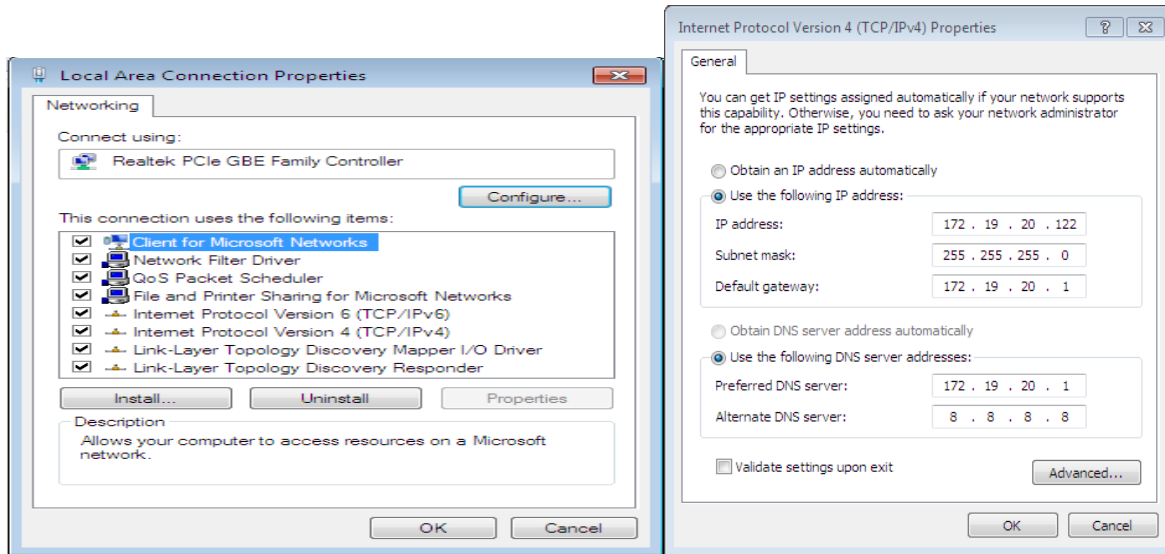
Sr. No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Network Interface Card	Manufacturer: Cisco		
2.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB		
3.	Switch (min. 8 ports)	8 ports		
4.	Crossover Cable			

X. Procedure

❖ **To set a static IP on your Windows computer**



1. Click **Start Menu > Control Panel > Network and Sharing Center**. Click **Change adapter settings**.
2. Right-click on **Local Area Connection** and click on **Properties**.



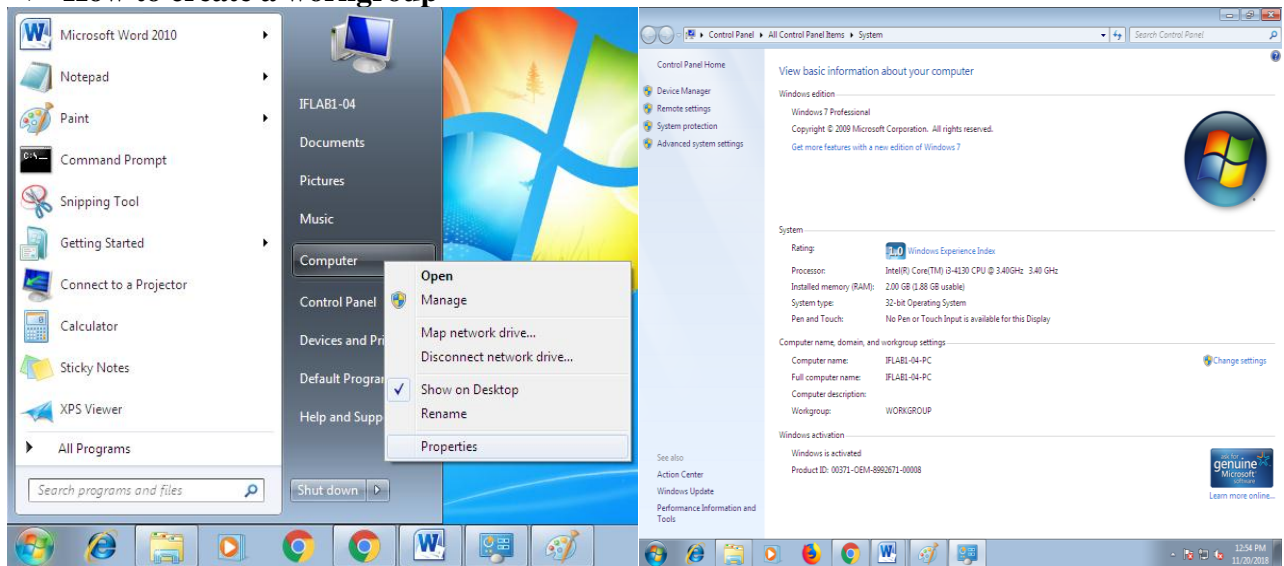
3. Select **Internet Protocol Version 4 (TCP/IPv4)** and click on **Properties**.

Select "Use the following IP address" and enter the IP address, Subnet Mask and DNS server. Click **OK** and close the **Local Area Connection** properties window.

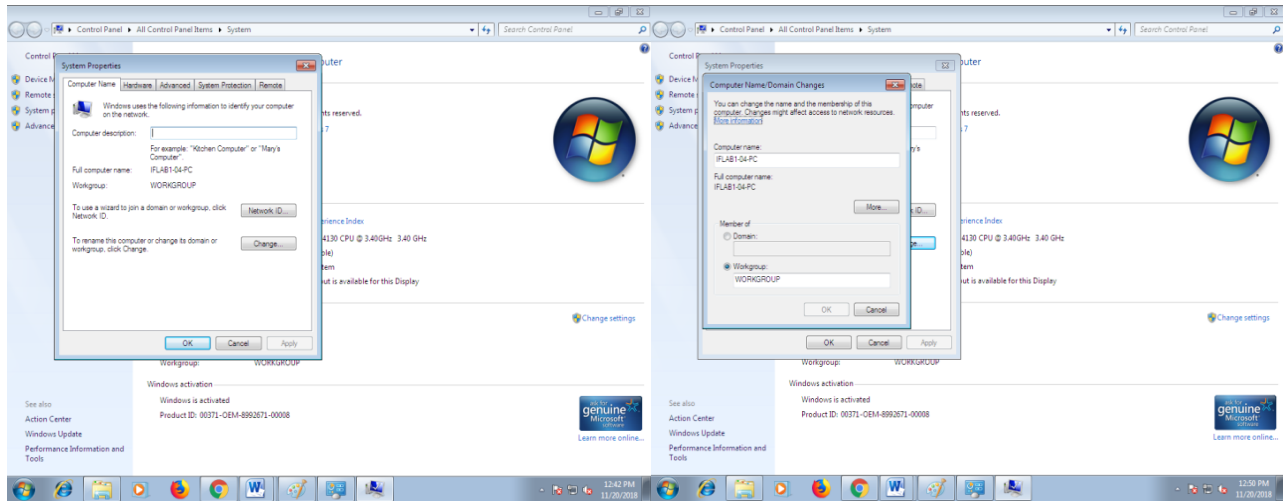
❖ **How Workgroup works**

A computer joining a workgroup is assigned to the same workgroup name this process makes accessing the computers easier.

❖ **How to create a workgroup**



Click on **Start** button Right-click on **Computer** and then click **Properties** 2 Under **Computer** name, domain, and workgroup settings, click **Change settings**.



3. In the **System Properties** dialog box, click the **Computer Name** tab and then click **Change**. In the Computer Name/Domain Changes dialog box, under Member of, click **Workgroup**

4. Then do one of the following:

To join an **existing** workgroup, type the name of the workgroup that you want to join, and then click **OK**.

To create a **new** workgroup, type the name of the workgroup that you want to create, and then click **OK**

Note: Repeat the steps of setup of IP address and setup of Workgroup for third computer

❖ **Peer-to-peer applications.**

- **Skype**, an Internet telephony network, uses P2P technology.
- **Instant messaging** systems and **online chat** networks.
- **Bitcoin** and **PPCoin** are peer-to-peer-based digital currencies.
- **Dalesa** a peer-to-peer web cache for LANs (based on IP multicasting).
- **Open Garden**, connection sharing application that shares Internet access with other devices using Wi-Fi or Bluetooth.
- Streaming media. **P2PTV** and **PDT**

XI. Precaution

1. Handle Computer System and peripherals with care
2. Follow Safety Practices

XII. Resources Used

Sr. No	Name of Resource	Specification
1.	Crossover Cable	
2.	Network Interface Card	Manufacturer: Cisco
3.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
4.	Switch (min. 8 ports)	8 ports
5.	Any other Resource	

XIII. Result/Conclusion

.....
.....
.....

XIV. Practical Related Questions

1. What is peer?
2. What is peer to peer network?
3. How peer to peer is differs from client -server network?
4. Give advantages of peer to peer network.
5. Give disadvantages of peer to peer network.

XV. Exercise

1. Student should Configure peer-to peer Network of minimum three host

(Space for Answer)

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

XVI. References/ Suggestions for further Reading

https://www.webopedia.com/TERM/W/word_processing.html

<http://jan.ucc.edu/lrm22/technology/wpbasics/wpbasics.htm>

XVII. Assessment Scheme

Performance indicator		Weightage
Process Related(35 Marks)		75%
1.	Completion of given task	25%
2.	Correctness of given task	50%
Product Related(15 Marks)		25%
3.	Answer to sample Question	15%
4.	Submit Report in Time	10%
Total(50 Marks)		100%

❖ **List of Students/Team Members**

.....

.....

.....

.....

Marks Obtained			Dated Signature of Teacher
Process Related(35)	Product Related (15)	Total(50)	

Practical No.2: Create a Small Physical Network using Computers, Network Connecting Devices and cables

I. Practical Significance

Identify and know the physical network

Configure small physical network

II. Relevant Programs Outcomes (POs)

1. **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
2. **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
3. **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
4. **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
5. **Communication:** Communicate effectively in oral and written form.

III. Competency and Practical skills

1. Setup small Physical Network

IV. Relevant Course Outcomes

Use Basic Concept of Networking for setting of Computer Network

Setup up computer Network for Specific Requirement

V. Practical Outcomes (POs)

Understand to connect computers, assign Workgroup, and assign IP address

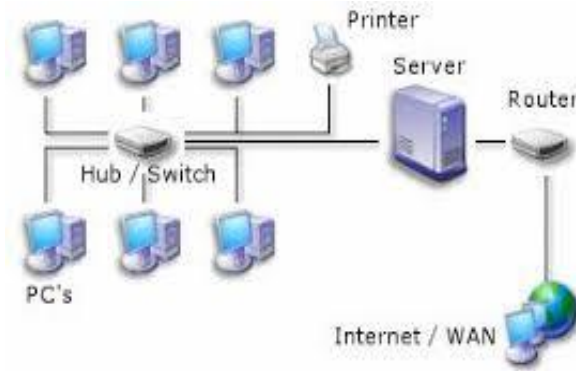
VI. Relevant Affective domain related Outcomes

1. Follow safety practices
2. Demonstrate working as a leader/team member
3. Follow ethical practices

VII. Minimum Theoretical Background

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users

VIII. Diagrams / Experimental set-up /Work Situation



IX. Resources Required

Sr. No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB	10	
2..	Switch (min. 8 ports)	8 ports	1	

X. Procedure

Power up the switch. Connect all the computers to the Switch with standard network cable (CAT - 5).

Insert a one end of cable into NIC port of computer and another end into NIC port of switch.

Put all the computers in the same Workgroup as performed in experiment no.1

Give all the computers IP address in the same subnet mask

❖ Use the following guideline

Open Start > Control Panel > Network Connections

Right-click “Local Area Connection” .This connection uses the following items select “Internet Protocol (TCP/IP)” and click the “Properties” button

Put a tick next to “Use the following IP Address” and type in the IP and subnet mask

Computer 1:
-IP: 192.168.0.10
-Subnet Mask: 255.255.255.0

Computer 2:
-IP: 192.168.0.11
-Subnet Mask: 255.255.255.0

Computer 3:
-IP: 192.168.0.12
-Subnet Mask: 255.255.255.0

Computer 4:
-IP: 192.168.0.13
-Subnet Mask: 255.255.255.0

Type ping command on command prompt of every computer to verify connections.

C:\Documents and Settings>ping 192.168.0.10

Pinging 192.168.0.10 with 32 bytes of data:

Reply from 192.168.0.10: bytes=32 time<1ms TTL=128

Reply from 192.168.0.10: bytes=32 time<1ms TTL=128

Reply from 192.168.0.10: bytes=32 time<1ms TTL=128

Reply from 192.168.0.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.10:

Packets: Sent4, Received= 4, Lost= 0 (0% loss),

Approximate round trip times in milliseconds: Minimum=0ms, Maximum=0ms, Average=0ms

XI. Precaution

1. Handle Computer System and peripherals with care
2. Follow Safety Practices

XII. Resources Used

Sr. No	Name of Resource	Specification
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
2.	Switch (min. 8 ports)	8 ports
3.	Any other Resource	

XIII. Result

.....
.....
.....

XIV. Practical Related Questions

1. What is Computer network?
2. State the need of computer network.
3. Give any two features of network.
4. How internet is an example of network?
5. List Different Network Devices.
6. Which types of connectors are used in Network Lab?
7. Give the use of cable.
8. List components required to connect 4 computers.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

References/ Suggestions for further Reading

https://www.webopedia.com/TERM/W/word_processing.html

<http://jan.ucc.edu/lrm22/technology/wpbasics/wpbasics.htm>

XVI. Assessment Scheme

Performance indicator		Weightage
Process Related(35 Marks)		75%
1.	Completion of given task	25%
2.	Correctness of given task	50%
Product Related(15 Marks)		25%
3.	Answer to sample Question	15%
4.	Submit Report in Time	10%
Total(50 Marks)		100%

❖ **List of Students/Team Members**

.....

.....

.....

.....

Marks Obtained			Dated Signature of Teacher
Process Related(35)	Product Related (15)	Total(50)	

Practical No.3: Draw the Network Layout with its Topology for Network set-up of your Laboratory

I. Practical Significance

Identify network topology

Draw Network Laboratory Topology

II. Relevant Programs Outcomes (POs)

1. **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
2. **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
3. **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
4. **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
5. **Communication:** Communicate effectively in oral and written form.

III. Competency and Practical skills

1. Network Layout with its Topology for Network set-up of your Laboratory

IV. Relevant Course Outcomes

Use Basic Concept of Networking for setting of Computer Network

V. Practical Outcomes (POs)

Understand network topology

Differentiate between all topology

VI. Relevant Affective domain related Outcomes

1. Follow safety practices
2. Follow ethical practices

VII. Minimum Theoretical Background

Network Topology refers to layout of a network. How different nodes in a network are connected to each other and how they communicate is determined by the network's topology.

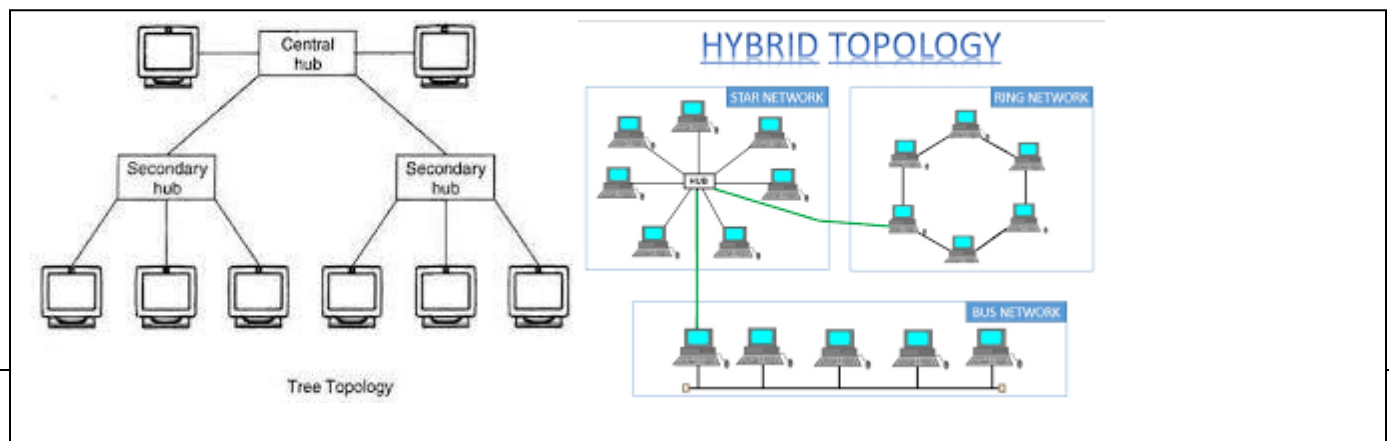
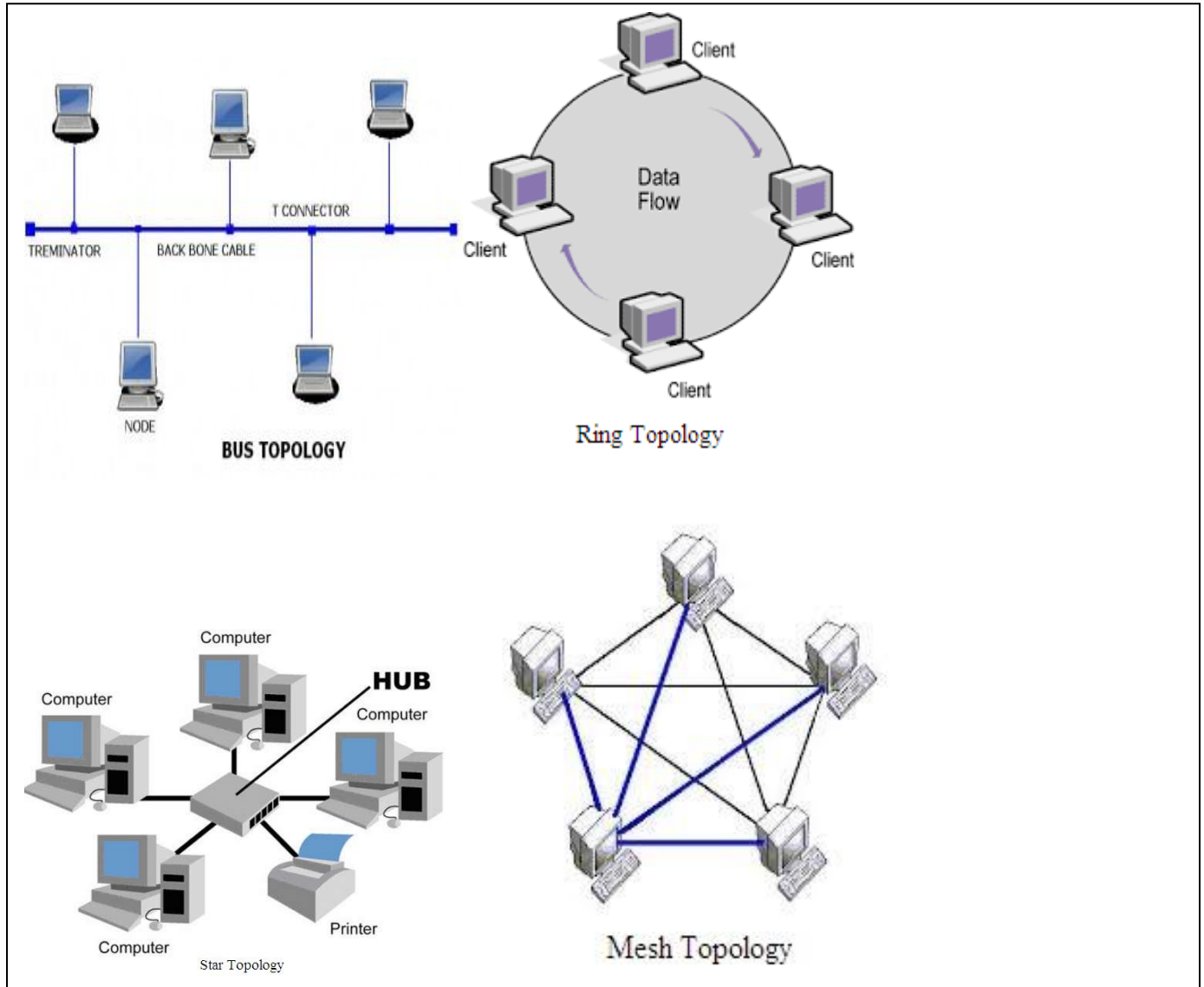
Network Topology refers to the layout of a network and how different nodes in a network are connected to each other and how they communicate. Topologies are either physical (the physical layout of devices on a network) or logical (the way that the signals act on the network media, or the way that the data passes through the network from one device to the next).

Types of Network Topology

Network Topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.

1. BUS

- 2. RING
- 3. STAR
- 4. MESH
- 5. TREE
- 6. HYBRID



Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called Linear Bus topology.

Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

Advantages of Bus Topology

1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbors for each device.

Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.

Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fiber or coaxial cable.

Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has $n(n-1)/2$ physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are :

1. Routing
2. Flooding

MESH Topology: Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

MESH Topology: Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.

Types of Mesh Topology

1. Partial Mesh Topology: In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. Full Mesh Topology: Each and every nodes or devices are connected to each other.

Features of Mesh Topology

1. Fully connected.
2. Robust.
3. Not flexible.

Advantages of Mesh Topology

1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Advantages of Tree Topology

1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

HYBRID Topology

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

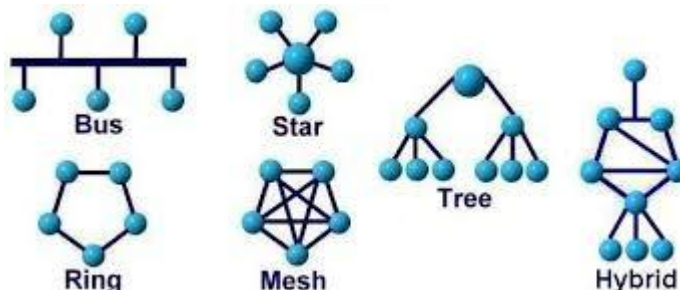
Advantages of Hybrid Topology

1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly

VIII. Diagrams / Experimental set-up /Work Situation



IX. Resources Required

Sr. No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB	10	
2.	Switch (min. 8 ports)	8 ports	1	

X. Procedure

1. Observe the Laboratory Structure
2. Identify the topology used in Laboratory
3. Draw Network Layout for Laboratory

XI. Precaution

1. Handle Computer System and peripherals with care
2. Follow Safety Practices

XII. Resources Used

Sr. No	Name of Resource	Specification
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
2.	Switch (min. 8 ports)	8 ports
3.	Any other Resource	

XIII. Result

.....

.....

.....

XIV. Practical Related Questions

1. List Different Types of Network Topology
2. Differentiate All Topologies with respect to following points
 - a. Physical Arrangement
 - b. Data Flow
 - c. Broadcast/ unicast/ Multicast
 - d. Whether central device required
 - e. Whether terminators required
 - f. What if node fails
 - g. What if link fails
 - h. What if central device fails(if any)

- i. Number of cables required
- j. Cost
- k. Security
- l. Adding node to network
- m. Deleting node to network
- n. Whether troubleshooting is easier?

XV. Exercise

Draw the Network Layout with its Topology for Network set-up of your Laboratory

(Space for Answer)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

XVI. References/ Suggestions for further Reading

<https://www.geeksforgeeks.org/network-topologies-computer-networks/>

XVII. Assessment Scheme

Performance indicator		Weightage
Process Related(35 Marks)		75%
1.	Completion of given task	25%
2.	Correctness of given task	50%
Product Related(15 Marks)		25%
3.	Answer to sample Question	15%
4.	Submit Report in Time	10%
Total(50 Marks)		100%

❖ **List of Students/Team Members**

.....

.....

.....

.....

Marks Obtained			Dated Signature of Teacher
Process Related(35)	Product Related (15)	Total(50)	

Practical No.4: Prepare and Test straight and Cross UTP cable

I. Practical Significance

Identify and know the use of straight and Crossover cable

Create straight cable and crossover cable

II. Relevant Programs Outcomes (POs)

- 1. Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
- 2. Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
- 3. Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
- 4. Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
- 5. Communication:** Communicate effectively in oral and written form.

III. Competency and Practical skills

Understand **straight and Cross UTP cable**

Create **straight and Cross UTP cable**

Understand **straight and Cross UTP cable**

IV. Relevant Course Outcomes

Use Basic Concept of Networking for setting of Computer Network

V. Practical Outcomes (POs)

Create **straight and Cross UTP cable**

VI. Relevant Affective domain related Outcomes

1. Follow safety practices
2. Practice good Housekeeping

VII. Minimum Theoretical Background

Straight network cable:

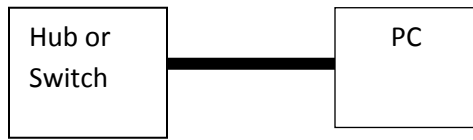
It is a type of Ethernet cable used to connect computing devices together directly.

Straight through or patch cables were used to connect from a host network interface controller (a computer or similar device) to a network switch, hub or router.

Both sides (side A and side B) of cable have wire arrangement with same color.

These are used when connecting Data Terminating Equipment (DTE) to Data Communications Equipment (DCE).

Concept structure:



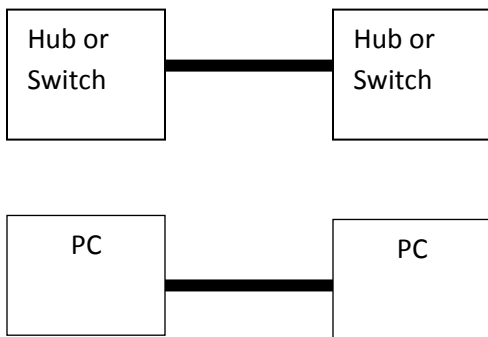
Pin ID	Side A	Side B
1	Orange-white	Orange-white
2	Orange	Orange
3	Green-white	Green-white
4	Blue	Blue
5	Blue-White	Blue-White
6	Green	Green
7	Brown-White	Brown-White
8	Brown	Brown

❖ **Crossover network cable:**

It is used to connect two devices of the same type: two computers or two switches to each other.

Both sides (side A and side B) of cable have wire arrangement with different color.

These are used when connecting Data Terminating Equipment (DTE) to Data Terminating Equipment (DTE) or Data Communications Equipment (DCE) to Data Communications Equipment (DCE).



Pin ID	Side A	Side B
1	Orange-white	Green-white
2	Orange	Green
3	Green-white	Orange-white
4	Blue	Brown-White
5	Blue-White	Brown
6	Green	Orange
7	Brown-White	Blue
8	Brown	Blue-White

❖ **RJ45 Connector and Crimping Tool**

RJ45 Connector for network cables. RJ45 connectors are most common

RJ45 is a standard type of Connector for Network Cables.

RJ4 connectors feature eight pins to which the wire strands of a cable interface electrically. Standard RJ45 pin outs define the arrangement of the individual wires needed when attaching Connector to Cable.

A Crimping Tool is a tool designed to crimp or connect a connector to the end of cable

Network cables and Phone cables are created using crimping tool to connect RJ 45and RJ 11 connectors to the end of the cable

RJ-11 (6-Pin) and RJ-45 (8-Pin) Crimping Tool



ComputerHope.com

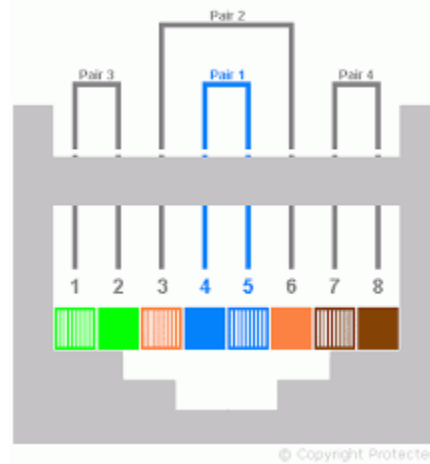


Fig. RJ 445 Pin out

fig. Straight-Thru and Crossover cable

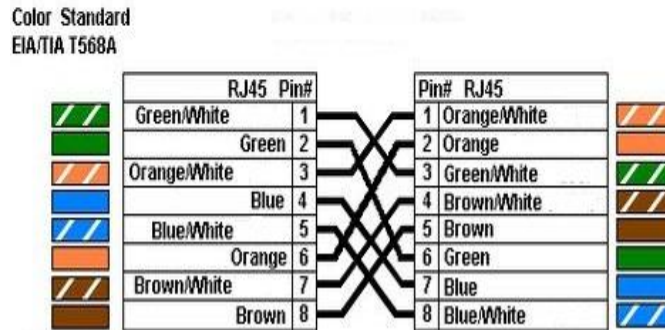


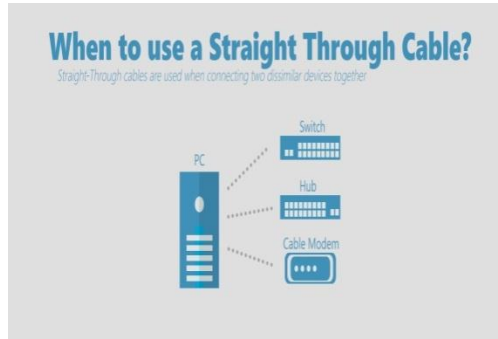
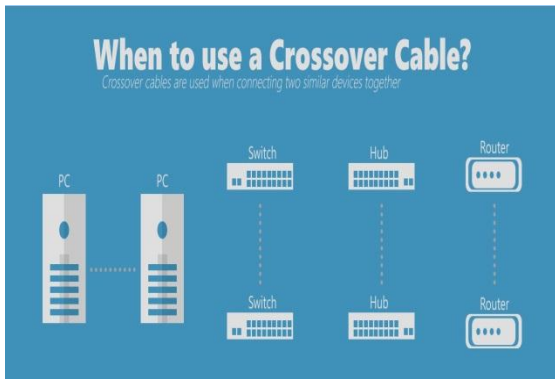
fig. Straight-Thru and Crossover cable

Functionality Difference between Straight Cable and Cross Cable

Crossover cableis used when:

- Connecting a computer to a computer
- Connecting a router to a router
- Connecting a switch to a switch

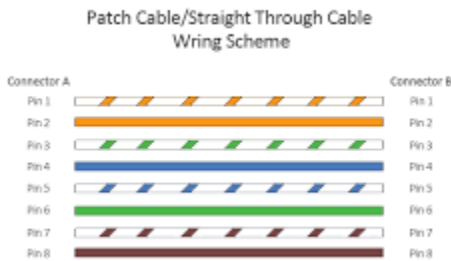
- Connecting a hub to a hub and
- Connecting a router to a PC because both devices have the same components



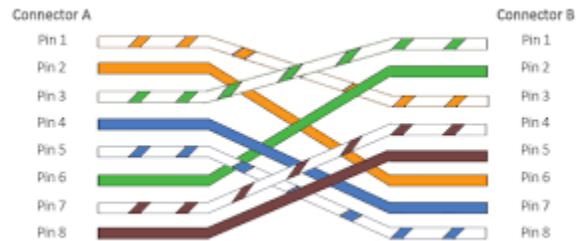
❖ **Straight-through cables are used when:**

- Connecting a router to a hub
- Connecting a computer to a switch
- Connecting a LAN Port to a switch or computer
- Connecting other dissimilar networking equipment

VIII. Diagrams / Experimental set-up /Work Situation



Give the label to below figure.....



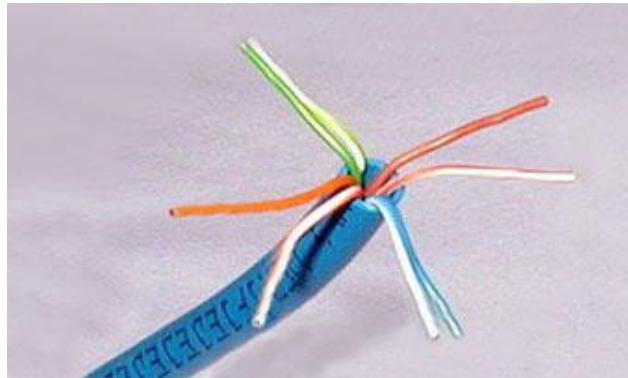
IX. Resources Required

Sr. No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Network Interface Card	Manufacturer: Cisco		
2.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB		
3.	Switch (min. 8 ports)	8 ports		
4.	UTP CAT 6 Cable			
5.	Crimping Tool			
6.	RJ 45 connector			
7.	Line Tester			

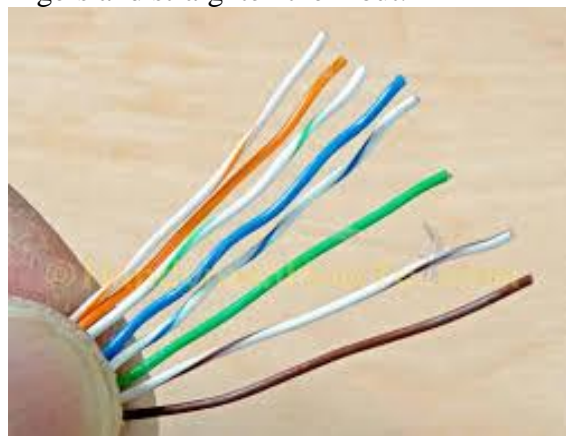
X. Procedure

Prepare straight and crossover cable:

1. Cut into the plastic sheath 1 inch from the end of the cut cable. The crimping tool has a razor blade that will do the trick. Untwist it and pair of the similar colors.

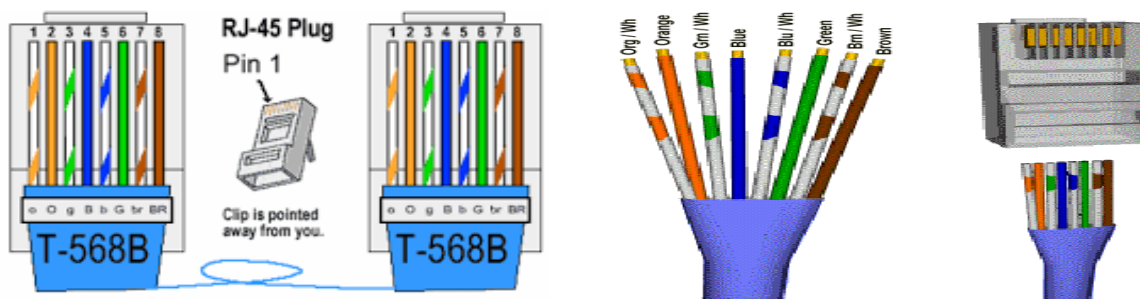


Pinch the wires between your fingers and straighten them out.



(The wire colors line up to form a standard cat 5 cable)

Use scissors to make a straight cut across the wires 1/2 inch from the cut sleeve to the end of the wires. Push the wires into the connector.



A view from the top. All the wires are all the way in. There are no short wires.

Crimping The Cable: carefully place the connector into the Ethernet Crimper and cinch down on the handles tightly. The copper splicing tabs on the connector will pierce into each of the eight wires. There

is also a locking tab that holds the blue plastic Sleeve in place for tight compression fit When you remove the cable from the crimper, the cable is ready



Make sure to test the cables using line tester before installing them. Use Cable Tester



XI. Precaution

1. Follow Safety Practices
2. Cut the plastic cover carefully so that cables would not get cut
3. Arrange color code and check before crimping

XII. Resources Used

Sr. No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Network Interface Card	Manufacturer: Cisco		
2.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB		
3.	Switch (min. 8 ports)	8 ports		
4.	UTP CAT 6 Cable			
5.	Crimping Tool			
6.	RJ 45 connector			
7.	Line Tester			

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

References/ Suggestions for further Reading

<https://www.home-network-help.com/straight.html>

XVI. Assessment Scheme

Performance indicator		Weightage
Process Related(35 Marks)		75%
1.	Completion of given task	25%
2.	Correctness of given task	50%
Product Related(15 Marks)		25%
3.	Answer to sample Question	15%
4.	Submit Report in Time	10%
Total(50 Marks)		100%

❖ **List of Students/Team Members**

.....
.....
.....
.....

Marks Obtained			Dated Signature of Teacher
Process Related(35)	Product Related (15)	Total(50)	

Practical No.5: Install and Configure Network Interface Card and identify its MAC address

I. Practical Significance

Know the NIC

Identify MAC address

II. Relevant Programs Outcomes (POs)

- 1. Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
- 2. Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
- 3. Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
- 4. Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
- 5. Communication:** Communicate effectively in oral and written form.

III. Competency and Practical skills

1. Install NIC and to know the MAC address of Computer

IV. Relevant Course Outcomes

Use Basic Concept of Networking for setting of Computer Network

V. Practical Outcomes (POs)

Understand NIC

VI. Relevant Affective domain related Outcomes

1. Follow safety practices
2. Demonstrate working as a leader/team member
3. Follow ethical practices

VII. Minimum Theoretical Background

What is the NIC?

A network interface card (NIC) is a circuit board or card that is installed in a computer so that it can be connected to a network. A network interface card provides the computer with a dedicated, full-time connection to a network.

Installing a NIC card requires you to have some basic knowledge on computer component and does not necessarily need you to be a computer whiz to do the job.

NIC has Read Only Memory (ROM). that contains firmware i.e. Software that installed on a ‘ small memory chip on a hardware device which allows NIC to Implement MAC (Media Access Control) protocol of LAN standard. A NIC can be wired or wireless. It Works by sending and receiving Signals over some type of media or device. This can be cable or other type of modem The biggest variation between cards is depending upon their connective medium and speed capabilities. 10/100 Ethernet NIC. Gigabit Ethernet NIC, Wireless NIC.

VIII. Diagrams / Experimental set-up /Work Situation



IX. Resources Required

Sr. No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB	10	
2.	Switch (min. 8 ports)	8 ports	1	

X. Procedure

To install the Network Interface Card follow through the following steps to successfully install your card.

Unplug the power cable on your computer power supply.

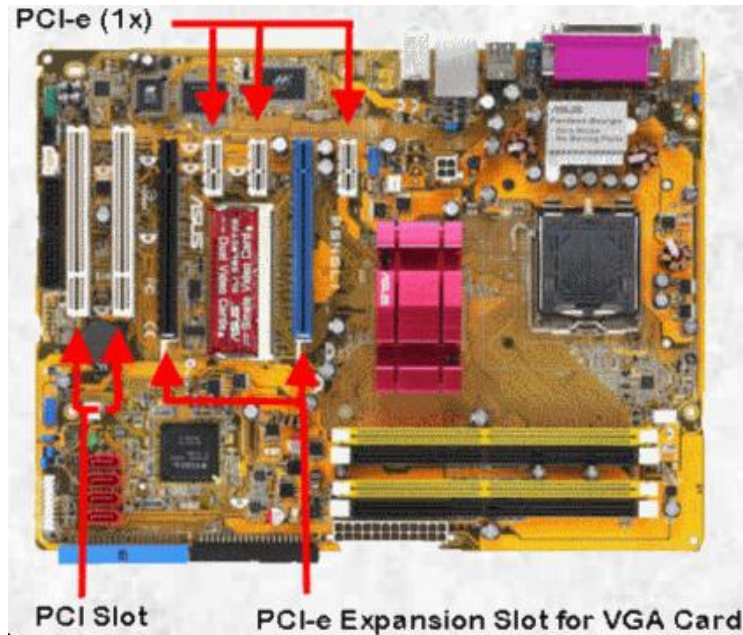
Open your PC case, there are usually two screws at the back of your PC, unscrew it and set aside the screw. Some pc case don't have screws to remove the cover you just have to slide the cover to open, refer to your PC case manual on how to remove the cover of your PC.

Discharge yourself from any static charge that may damage the component before touching any pc component.

You can do this by using an anti-static wrist strap clipping it to the computer casing metallic part or if you don't have this anti-static wrist strap you can touch any non-painted metallic part of the

computer casing to remove any static charge from your body before proceeding to the installation of the component. When working with pc component such as network interface card always avoid touching the golden pins of the cards or the IC chips pins.

Find an available PCI slot on your motherboard. PCI slot can be easily distinguished over PCI-E since PCI slot are shorter in length than PCI-E slots except for PCI-E 1x slot which is shorter than PCI slot. Refer to the image below.



Install the NIC card by aligning the guide notches with the PCI slot and pressing the card gently till it sit firmly on the PCI slot, you'll know if it is sited well if you can't see the pins of the NIC on the PCI slot.

Secure the card by using a single screw, screwing the card bracket firmly to the computer casing. Inspect the card if it moves, a well sited card should not move when you try to move them. A not properly sited card may damage the card when you power on your computer.

Plug in the power cord to the power supply and power on your computer.

Wait for windows to load, a "new device detected" message by windows should appear and it will install the necessary driver or ask you for the device driver, after the installation of device driver you can install its software if it has.

Check device manager if the driver is installed properly, you should see no yellow exclamation on the NIC device.

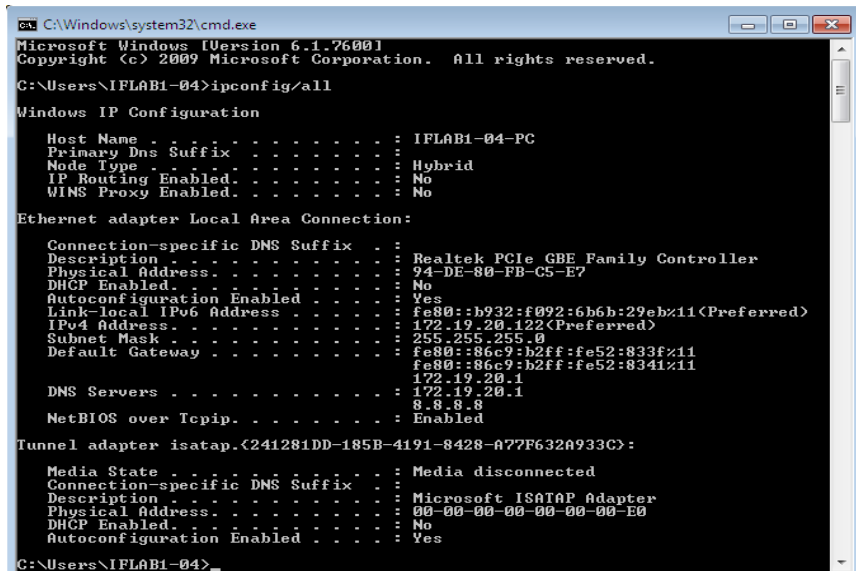
If everything works out right then you can now close your computer casing and return the screw at the back of your PC.

Network Interface Card it IS a piece of hardware allows your computer to be connected to a network of other computers (known as a LAN or Local Area Network). The computers and network control devices are connected to cabling system through NIC

❖ **To find your device’s MAC address:**

1. Click **Windows Start** or press the **Windows** key.
2. In the search box, type **cmd**. And Press **Enter**
A command window displays.
3. Type **ipconfig /all**. And Press **Enter**.

A Physical Address displays for each adapter. The Physical Address is your device’s MAC address.



XI. Precaution

1. Handle Computer System and peripherals with care
2. Follow Safety Practices

XII. Resources Used

Sr. No	Name of Resource	Specification
1.	Network Interface Card	Manufacturer: Cisco
2.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
3.	Any other Resource	

XIII. Result

.....

XIV. Practical Related Questions

1. What Is Local Area Network?
2. State the purpose of Network Interface Card.
3. Where Network Interface Card is placed in computer?
4. State different parameters on the basis of which NIC classified.
5. Which types of connector used by interface Card for cabling?
6. How to check whatever Network Interface Card successfully installed or not.
7. What is USB Adaptor and where it is used?
8. State meaning of IP Address.
9. To whom MAC address is allocated and what is use of it.
10. How MAC address differs from IP address?
11. Give general representation of MAC address
12. MAC address is more secured than IP address”, why?
13. Give the steps to locate MAC address of Computer.
14. A computer MAC address: 02:45: ZD: 65. 02: 1E. What the first three and remaining three blocks
15. It is possible to replace NIC card? If yes then how?

XV. Exercise

Install NIC card check MAC address

(Space for Answer)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

XVI. References/ Suggestions for further Reading

<http://www.omnisecon.com/basic-networking/what-is-nic-card-network-interface-card.php>

XVII. Assessment Scheme

Performance indicator		Weightage
Process Related(35 Marks)		75%
1.	Completion of given task	25%
2.	Correctness of given task	50%
Product Related(15 Marks)		25%
3.	Answer to sample Question	15%
4.	Submit Report in Time	10%
Total(50 Marks)		100%

❖ List of Students/Team Members

.....

.....

.....

.....

Marks Obtained			Dated Signature of Teacher
Process Related(35)	Product Related (15)	Total(50)	

Practical No.6:Share Files/Folder, Devices and Printer in the Network and access the shared resources from the other node

I. Practical Significance

You can share Computer Resources

II. Relevant Programs Outcomes (POs)

- 1. Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
- 2. Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
- 3. Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
- 4. Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
- 5. Communication:**Communicate effectively in oral and written form.

III. Competency and Practical skills

1. Share resources such as File Folder and Printer

IV. Relevant Course Outcomes

Use Basic Concept of Networking for setting of Computer Network
Setup up computer Network for Specific Requirement
Configure Basic network Services

V. Practical Outcomes (POs)

Connect Printer, Install Printer Share printer, Files and Folder

VI. Relevant Affective domain related Outcomes

1. Demonstrate working as a leader/team member
2. Follow ethical practices

VII. Minimum Theoretical Background

A resource, or system resource, is any physical or virtual component of limited availability within a computer system

Every device connected to a computer system is a resource and every internal system component is also a resource.

Major resource types are CPU time, Random access memory, Hard disk space, Network throughput, Electrical power, External Devices, Input/output operations.

Virtual system resources include files, network connections and memory areas, whereas a physical resource includes printer, scanner, fax machine etc.

Types of System Resources

1. Physical
2. Virtual

Types of Physical Resources

1. Printer
2. Scanner
3. Fax Machine

Types of Virtual Resources

1. Memory
2. Files
3. CPU time

Resource Sharing

A shared resource or network share is a device or piece of information on a computer that can be remotely accessed from another computer typically via a local area network or an enterprise Intranet, transparently as if it were a resource in the local machine.

Examples are shared file access (also known as disk sharing and folder sharing), shared printer access (printer sharing), shared scanner access, etc.

Resource sharing means reduction in hardware costs. Shared files mean reduction in memory requirement, which indirectly means reduction in file storage expenses.

A network share can become a security liability when access to the shared files is gained (often by devious means) by those who should not have access to them. Many computer worms have spread through resource sharing

Printer sharing is a feature which allows you to access and use a printer from other computers in network.

If there are ten employees in an organization, each having their own computer, they will require ten printers if they want to use the resource at the same time. Printer sharing allows accessing the computers that can be interconnected using a network, and just one printer can efficiently provide the services to all ten users. Folder sharing is the public or private sharing of computer data or space in a network with various levels of access privilege.

A user sitting at one computer that is connected to network can easily see files present on another computers, provided he is authorized to do so. This saves him/her the hassle of carrying a storage device every time data needs to be transported from one system to another system

VIII. Diagrams / Experimental set-up /Work Situation

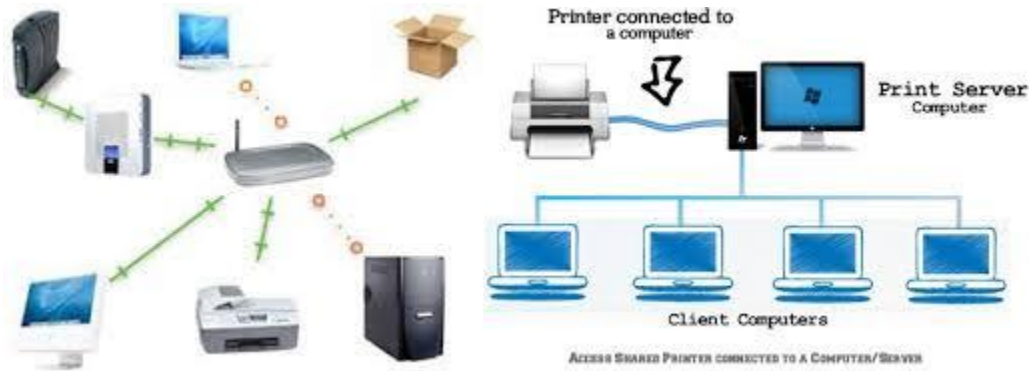


Fig.Resource sharing

Fig. Printer Sharing

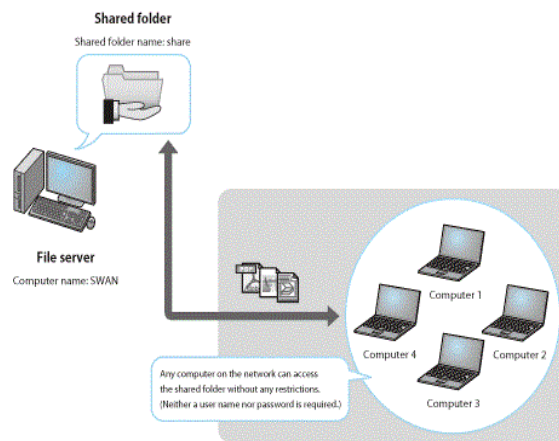


Fig. Folder Sharing

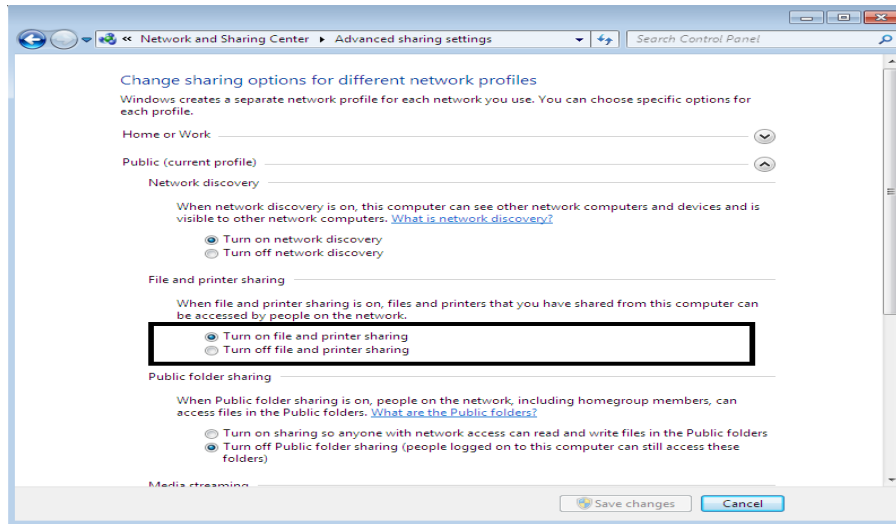
IX. Resources Required

Sr. No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB	10	
2.	Printer	8 ports	1	

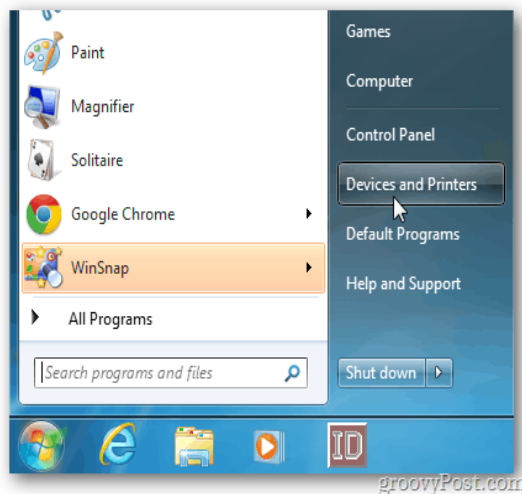
X. Procedure

Share Printer and folder

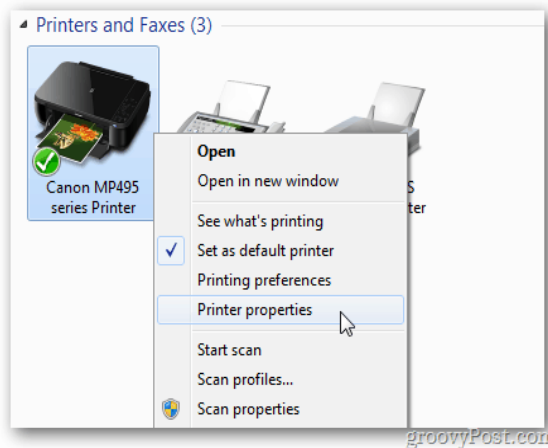
Click on Start Button->Click on Control Panel-> Click on Network and Sharing Center->click on Change advanced sharing settings



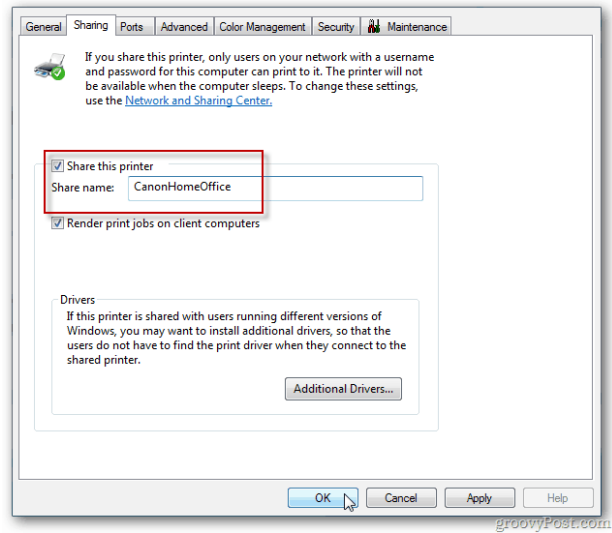
First start with the computer the printer is connected to. Make sure it's installed correctly with the latest drivers. click Start >> Devices and Printers.



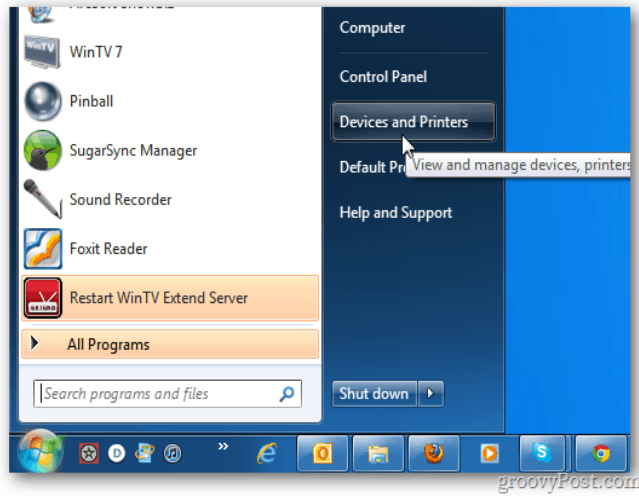
Next, right-click on the printer you want to share and select Printer Properties.



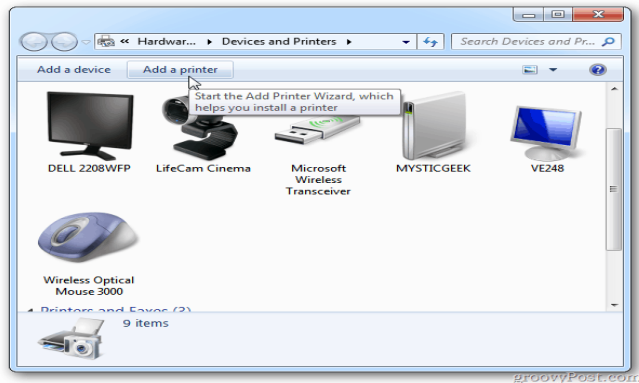
Click the Sharing tab. Make sure Share this Printer is checked and give it an easy to remember share name. Click OK.



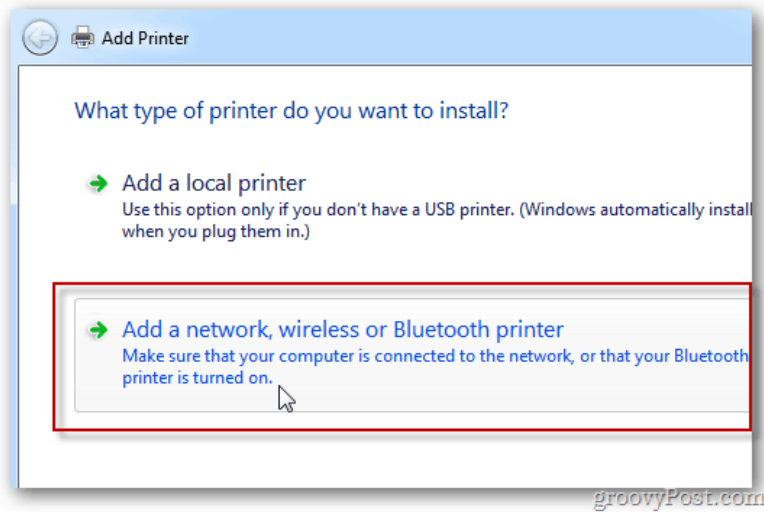
The computer the printer is attached to will need to be powered on to find and print to it. Now go to the other computer you want to print from. Click *Start >> Devices and Printers*.



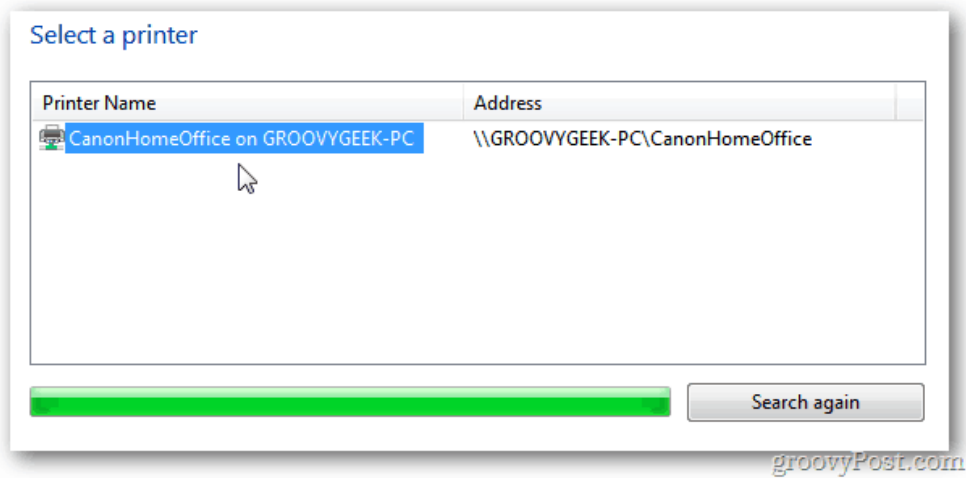
Click Add a Printer.



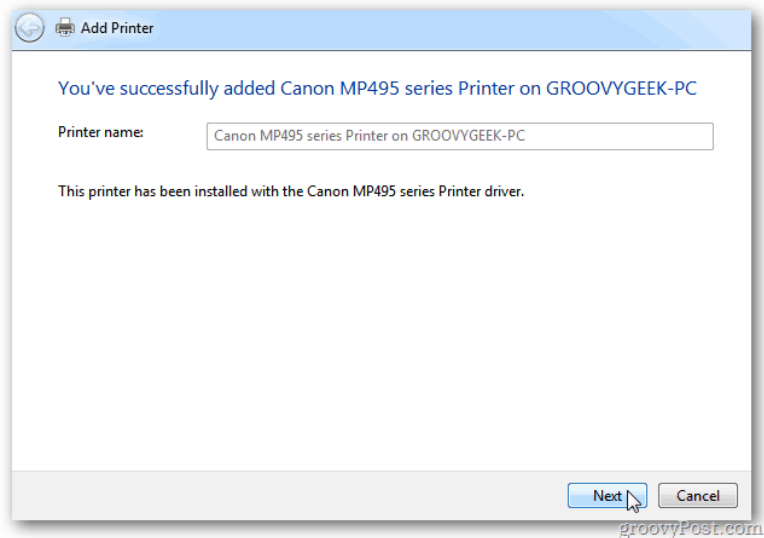
Next, click Add a Network, Wireless or Bluetooth Printer.



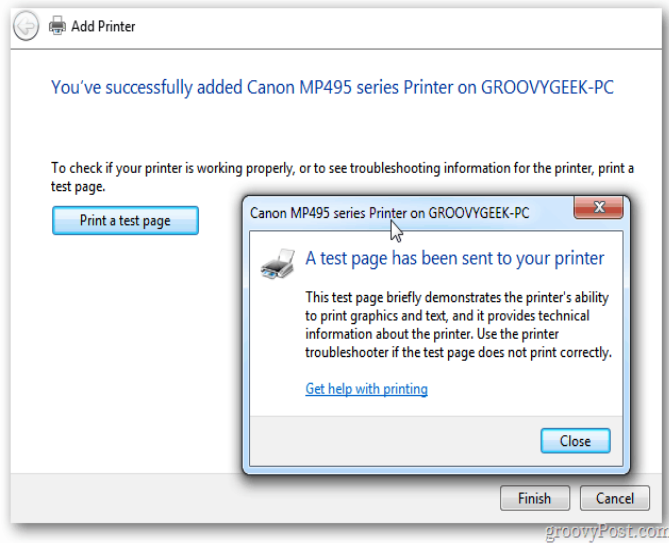
The system will search your network for the shared printer. When it finds the printer, highlight it and click Next.



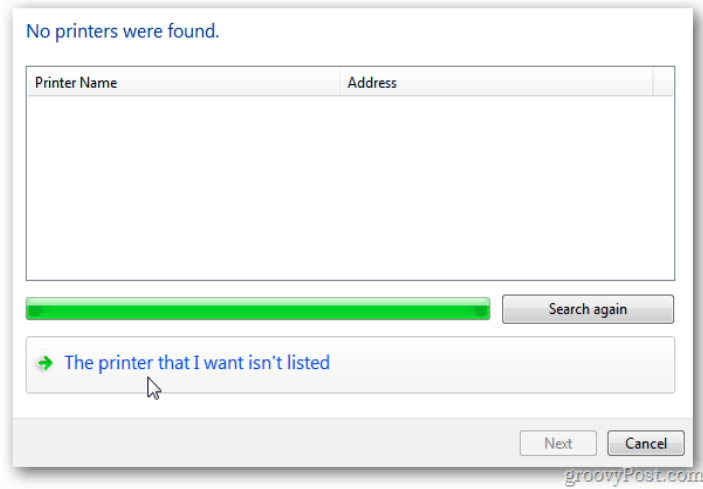
Success. Click Next.



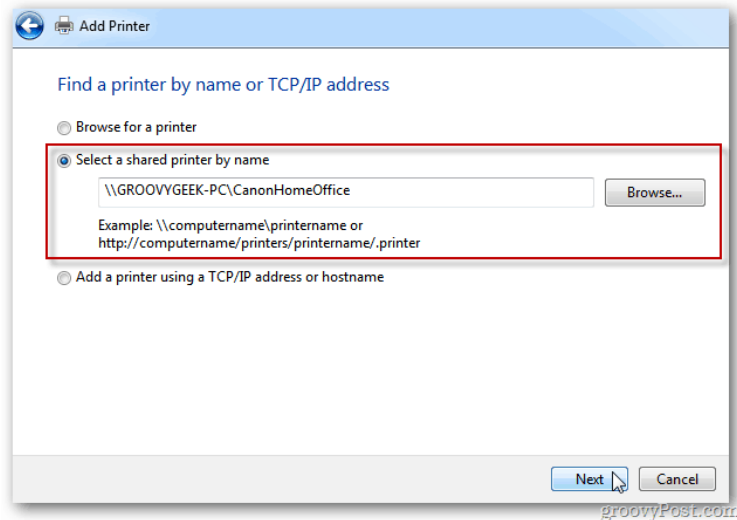
Back in Devices and Printers, you'll find the printer listed. Send a test page to the printer to verify it's working.



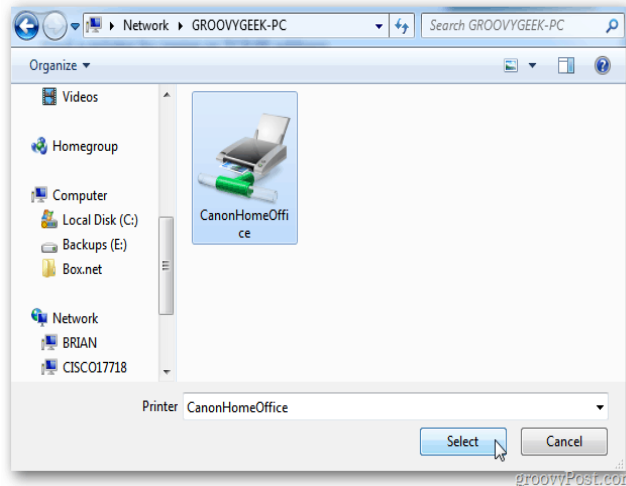
If Windows doesn't automatically find the printer, click The Printer That I Want Isn't Listed.



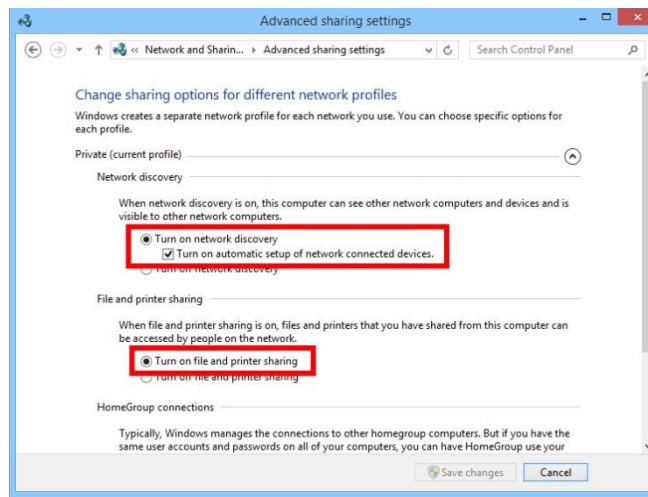
Check Select a Shared Printer by Name and type the path in directly.



Or click Browse to find the printer and select it.



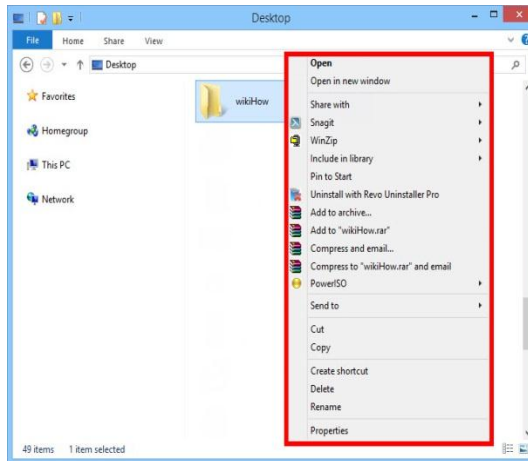
Sharing Specific Folders



Ensure that File and Printer Sharing is enabled. In order to share specific folders, you will need to have this feature enabled. The method for enabling it varies slightly depending on which version of Windows you are using. It is highly recommended that you do not enable folder sharing when on a public network such as a school or coffee shop.

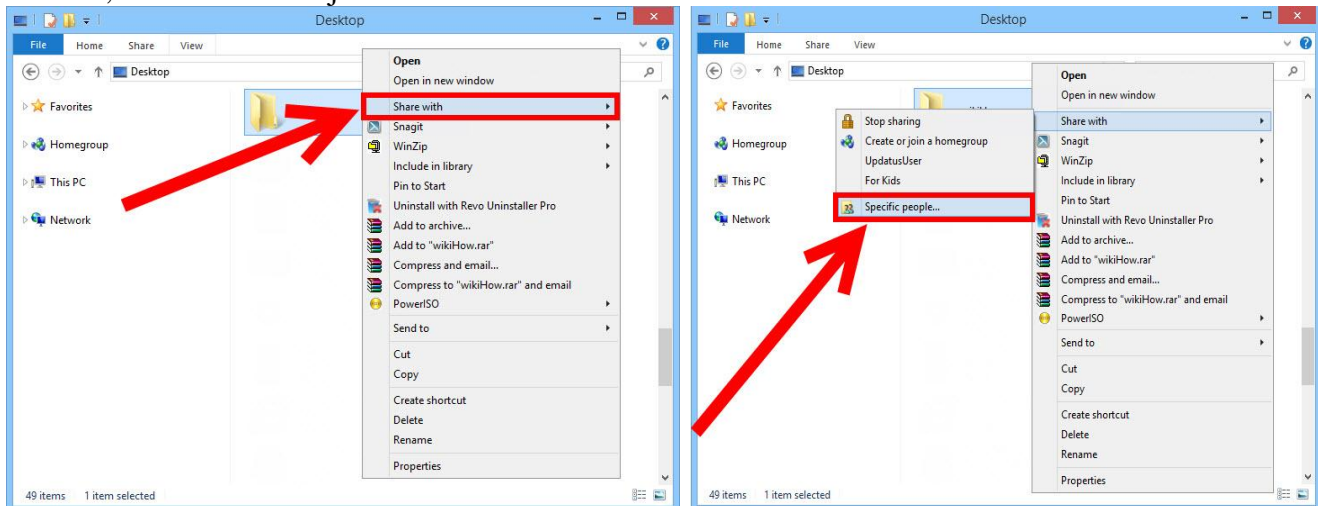
Windows 7 - Click the Start button, type "control panel", and press \leftarrow Enter. Double-click the "Network and Sharing Center" icon. Click the "Change advanced sharing settings" link. Expand the profile that you want to enable sharing on (Home/Work or Public). Turn on both "Network discovery" and "File and printer sharing". Click the "Save changes" button and enter your administrator password if necessary.

Find the folder you wish to share. Once File and Printer Sharing has been enabled, you can share any folder on your hard drive with other people on your network. Navigate to the folder that you want to share using Explorer. Right-click on it.



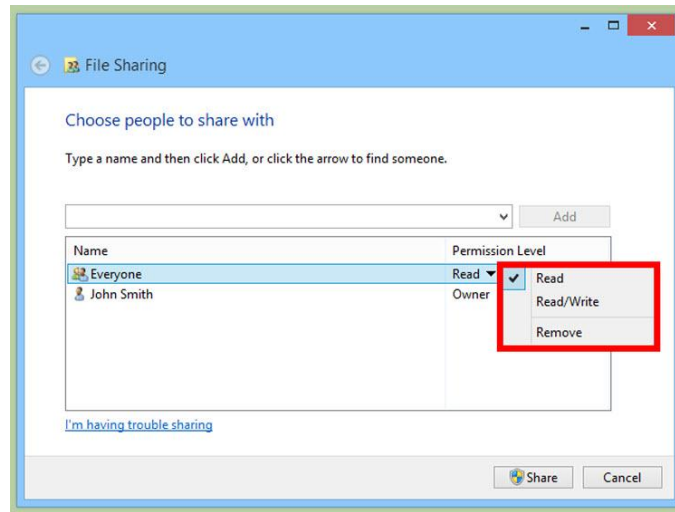
3. Select the "Share with" option. This will open the Sharing submenu. You can choose to share it with everyone in your Homegroup or select specific people to share it with.

When choosing a Homegroup option, you can allow other Homegroup members to both read and write to the folder, or limit them to just read from it.



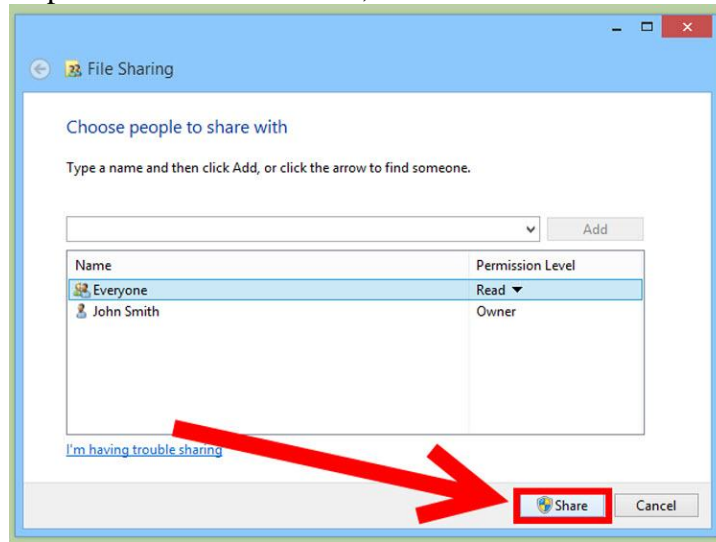
Click the "Specific people" option to select which users you want to share with. This will open a new window with a list of all the users that currently have access to the folder. You can add users to this list and give them specific permissions for the folder.

- To share the folder with everyone, click the dropdown menu at the top and select "Everyone". Click the Add button.
- To share with specific users, click the dropdown menu and select them or type in the name and click Add.



Set permissions for users on the list. Find a user on the list that you want to change the permissions for. Look in the Permissions Level column, and click the arrow next to the existing permission. Select the new one from the list.

- Read - User can see, copy, and open files from the folder, but cannot change files or add new ones.
- Read/Write - Besides Read abilities, users can change files and add new files to the shared folder. Files can be deleted by users with Read/Write permissions.
- Remove - Removes permissions for this user, and removes them from the list.



6Click the Share button. Your permission settings will be saved, and the folder will be available on the network for all allowed users.

XI. Precaution

1. Handle Computer System and peripherals with care
2. Follow Safety Practices

XII. Resources Used

Sr. No	Name of Resource	Specification
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
2.	Printer	
3.	Any other	

XIII. Result

.....
.....
.....

XIV. Practical Related Questions

1. Define system resource. List resources that can be shared in network?
2. Give the examples of physical and virtual resource. Define resource sharing and state its needs.
3. Give advantages and disadvantages of printer sharing and folder sharing.
4. How security is measure issue in resource sharing?
5. Which are different privileges associated with folder?

XV. Exercise

Student should share folder and printer

(Space for Answer)

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

XVI. References/ Suggestions for further Reading

<https://computer.howstuffworks.com/share-printer-home-network-windows>

XVII. Assessment Scheme

Performance indicator		Weightage
Process Related(35 Marks)		75%
1.	Completion of given task	25%
2.	Correctness of given task	50%
Product Related(15 Marks)		25%
3.	Answer to sample Question	15%
4.	Submit Report in Time	10%
Total(50 Marks)		100%

❖ **List of Students/Team Members**

.....
.....
.....
.....

Marks Obtained			Dated Signature of Teacher
Process Related(35)	Product Related (15)	Total(50)	

Practical No.7:Run the following TCP/IP Command with options record their output :

Ping, ipconfig, Tracert, Netstat, Wireshark,ARP

I. Practical Significance

To know the use of TCP/IP utilities

Run the TCP/IP utilities

II. Relevant Programs Outcomes (POs)

1. **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
2. **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
3. **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
4. **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
5. **Communication:**Communicate effectively in oral and written form.

III. Competency and Practical skills

1. Run TCP/IP utilities

IV. Relevant Course Outcomes

Configure Basic network Services

Configure TCP/IP services

V. Practical Outcomes (POs)

Understand TCP/IP utilities

VI. Relevant Affective domain related Outcomes

1. Follow safety practices
2. Demonstrate working as a leader/team member
3. Follow ethical practices

VII. Minimum Theoretical Background

❖ **TCP/IP utilities**

To assist with the management of TCP/IP. There are three types of TCP/IP-based utilities.

Connectivity utilities that you can use to interact with and use resources on a variety of systems.

Diagnostic utilities that you can use to detect and resolve networking problems.

TCP/IP server software that provides printing and publishing services to TCP/IP based Microsoft Windows client

❖ **PING(Packet Internet groper):**

It is a command used to verify the network connectivity of a computer. It checks the host name,

IP address, and that the remote system can be reached.

It uses a special protocol called the Internet Control Message Protocol (ICMP) to determine whether the. Remote machine (website, server, etc.) can receive the test packet and reply

This command is used to test a machine's connectivity to another system and to verify that the target system is active. Usually this command is the first step to any troubleshooting if a connectivity problem is occurring between two computers.

The Ping utility executes an end-to-end connectivity test to other devices and obtains the round-trip time between source and destination device. Ping uses the ICMP Echo and Echo Reply packets to test connectivity. Excessive usage may appear to be a denial of service (DoS) attack.

Syntax: ping <ip address>

ping [-t] [-a] [-n *count*] [-l *size*] [-f] [-i *TTL*] [-v *TOS*]

Following table shows use of ping command with different options.

Parameter	Description
-t	Pings the specified host until interrupted (press Ctrl+C to stop sending).
-a	Resolves addresses to hostnames.
-n <i>count</i>	Indicates the number of Echo Requests to send.
-l <i>size</i>	Sends a specific size of data. If this size is greater than the local network can handle, the sender will generate fragmented packets directly on the network.
-f	Sets the Don't Fragment flag in the packet.
-i <i>TTL</i>	Sets the Time to Live value in the packet.
-v <i>TOS</i>	Sets the type of service in the packet.
-r <i>count</i>	Indicates that the Ping process should record the route for the number of count hops specified.
-s <i>count</i>	Indicates that the Ping process should maintain Timestamp information for the number of count hops specified.
-j <i>host_list</i>	Indicates that the Ping process should follow a loose source route path along the <i>host_list</i> path
-k <i>host_list</i>	Indicates that the Ping process should follow a strict source route along the <i>host_list</i> path.
-w <i>timeout</i>	Indicates the number of milliseconds the host should wait for each reply.
-R	Use the router header to test the reverse route as well (IPv6 only).
-S <i>srcaddr</i>	What address to use to source ping from.
-p	Ping yper-V Network Virtualization provider address.
-4	Use IPv4 specifically.
-6	Use IPv6 specifically.

❖ IPCONFIG

The Ipconfig utility displays and modifies IP address configuration information.

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings.

Used without parameters ipconfig displays the IP address, subnet mask, and default gateway for all adapters.

By default, this command displays only the IP address, subnet mask, and default gateway for each adapter bound to TCP/IP

Syntax

ipconfig /? | /all |

Following table shows use of ipconfig command with different options

Parameter	Description
/?	Displays the help message
/all	Displays complete configuration information
/release	Uses DHCP to release the IP address for the specified adapter
/release6	Uses DHCPv6 to release the IPv6 address for the specified adapter
/renew	Uses DHCP to renew the IP address for the specified adapter
/renew6	Uses DHCPv6 to renew the IPv6 address for the specified adapter
/flushdns	Purges the DNS cache
/registerdns	Uses DHCP to refresh all DHCP leases and re-registers DNS names
/displaydns	Displays the contents of the DNS cache
/showclassid	Displays all the DHCP class IDs allowed for the adapter
/setclassid	Modifies the DHCP class ID
/showclassid6	Displays all the DHCPv6 class IDs allowed for the adapter
/setclassid6	Modifies the DHCPv6 class ID

❖ Tracert

It is used to determine the route data takes to get to a particular router to trace the

The ICMP protocol sends out Time Exceeded messages to the

route. Each time a packet is sent, the time-to-live (TTL) value is reduced before the packet

is forwarded. This allows TTL to count how many hops it is to the destination. if there is a trouble connecting to a rerhote host 'use Tracert to see where that connection fails. .

Syntax: tracert <ip address>.

Following table shows use of tracert command With different options.

Parameter	Description
-d	Tells the system not to resolve addresses to host names
-h <i>maxHops</i>	Specifies the maximum number of hops to search for target
-w <i>timeout</i>	Specifies the number of milliseconds to wait for each reply
-4	Specifies to use IPv4 specifically
-6	Specifies to use IPv6 specifically

❖ NETSTAT

It is used to shows the status of each active network connection.

Netstat will display statistics for both TCP and UDP, including protocol, local address, foreign address, and the TCP connection state. Because UDP is connectionless, no connection information will be shown for UDP packets.

It's a helpful tool in funding problems and determining the amount of traffic on the network as a performance measurement.

Syntax:

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

Following table shows use of netstat command with different options.

Parameter	Description
-a	Lists all current connections and open, listening ports on the local system.
-b	Displays executable for creating connection or listening port.
-e	Displays Data Link layer statistics (also can be used with the -s parameter).
-f	Displays fully qualified domain names (FQDN).
-n	Displays addresses and port numbers in numerical form.
-o	Displays the owning process ID associated with a connection.

<i>-p protocol</i>	Shows the connections for the specified protocol. The protocol defined may be UDP or TCP. When used with the <i>-s</i> parameter, the protocol definition IP, IPv6, ICMP, ICMPv6, TCP, or UDP also may be used.
<i>-r</i>	Displays the routing table (also see the <i>route</i> command).
<i>-s</i>	Displays statistics organized based on the protocols, such as IP, UDP, and TCP, by default (also can be used with the <i>-p</i> parameter to define a subset of the default).
<i>-t</i>	Displays the current connection offload state.
<i>-x</i>	Displays NetworkDirect connections, listeners, and shared endpoints.
<i>interval</i>	Redisplays the statistics on a regular basis using the interval (in seconds) value between displays. Press Ctrl+C to stop displaying the statistics. If this parameter is not included, the statistics appear only once.

❖ ARP

The ARP utility helps diagnose problems associated with the Address Resolution Protocol (ARP). TCP/IP hosts use ARP to determine the physical (MAC) address that corresponds with a specific IP address.

Once the MAC address is determined by the ARP reply, the IP and MAC address of the destination system are stored in the ARP cache (stored in memory) so that next time the address will be resolved from the cache and a broadcast will not be needed.

Syntax: arp -a

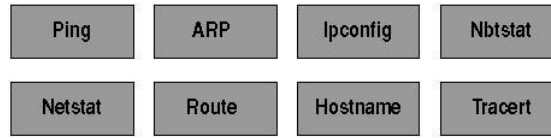
Following table shows use of *arp* command with different options.

Parameter	Description
<i>-a or -g</i>	Displays current entries in the ARP cache. If <i>inet_addr</i> is specified, the IP and data link address of the specified computer appear. If more than one network interface uses ARP, entries for each ARP table appear.
<i>inet_addr</i>	Specifies an Internet address.
<i>-N if_addr</i>	Displays the ARP entries for the network interface specified by <i>if_addr</i> .
<i>-v</i>	Displays the ARP entries in verbose mode.
<i>-d</i>	Deletes the host specified by <i>inet_addr</i> .
<i>-s</i>	Adds the host and associates the Internet address <i>inet_addr</i> with the data link address <i>eth_addr</i> . The physical address is given as six hexadecimal bytes separated by hyphens. The entry is permanent.
<i>eth_addr</i>	Specifies physical address.

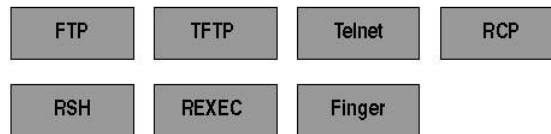
<i>if_addr</i>	If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.
----------------	---

VIII. Diagrams / Experimental set-up /Work Situation

Tools for troubleshooting TCP/IP



Tools for testing TCP/IP connectivity



IX. Resources Required

Sr. No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB		

X. Procedure

1. Open Command Prompt
2. Run Utilities with options

XI. Precaution

1. Handle Computer System and peripherals with care
2. Follow Safety Practices

XII. Resources Used

Sr. No	Name of Resource	Specification
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
2.	Any other Resource	

XIII. Result

.....

Practical Related Questions

1. What is a purpose of TCP/ IP utilities? Give the use of connectivity utility and also write 2 examples of it.
2. Which are the different things are checked using ping command?
3. What is a use of IPconfig utility?
4. What is a use of “/release” and “/renew” option used in Ipconfig? Why Tracert command is used? Give the syntax of Tracert command
5. What is a use of ARP utility? Which are different statistics is display for TCP using Netstat utility?
6. “TCP/IP utilities are used for troubleshooting in industry” comment on this statement

XIV. Exercise

Run all utilities with options and attach printout (Suggested by Teacher)

Give the use and syntax of Hostname and Nslookup utility.

(Space for Answer)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

XV. References/ Suggestions for further Reading

<https://www.pluralsight.com/blog/it-ops/top-7-tcpip-utilities-every-networking-pro-should-know>

XVI. Assessment Scheme

Performance indicator		Weightage
Process Related(35 Marks)		75%
1.	Completion of given task	25%
2.	Correctness of given task	50%
Product Related(15 Marks)		25%
3.	Answer to sample Question	15%
4.	Submit Report in Time	10%
Total(50 Marks)		100%

List of Students/Team Members

.....

.....

.....

.....

Marks Obtained			Dated Signature of Teacher
Process Related(35)	Product Related (15)	Total(50)	

Practical No.8:Use Wireshark Packet sniffer software and captures TCP,UDP, IP, ARP, ICMP, Telnet, FTP packets

I. Practical Significance

Capture the different packets in the network

II. Relevant Programs Outcomes (POs)

- 1. Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
- 2. Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
- 3. Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
- 4. Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
- 5. Communication:**Communicate effectively in oral and written form.

III. Competency and Practical skills

Understand Wireshark Packet sniffer software

IV. Relevant Course Outcomes

Use Basic Concept of Networking for setting of Computer Network
Setup up computer Network for Specific Requirement

V. Practical Outcomes (POs)

Use software for capturing packet

VI. Relevant Affective domain related Outcomes

- 1.** Follow safety practices
- 2.** Follow ethical practices

VII. Minimum Theoretical Background

A **packet** is the unit of data that is routed between an origin and a destination on the internet or any other packet-switched network.

The individual packets for a given file may travel different routes through the Internet.

A packet consists of two kinds of data: control information and user data (also known as payload).

The control information provides data that the network needs to deliver the user data, for example: source and destination network addresses, error detection codes, and sequencing information.

Network Packet Consist of Control information and User data

Control Information consist of Network address, Error detection codes and sequencing information .**Packet Sniffer**

It is a basic tool for observing the messages exchanged between executing protocol entities.

It captures messages being send/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured messages.

A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer.

It has two major components:

a. **Packet capture library:** receives a copy of every link-layer frame that is sent from Or received by your computer.

b. **Packet analyzer:** displays the contents of all fields within a protocol message.

It is an open source protocol analyzer that is used to capture packets in a network to see their contents.

It is the most widely used graphical application for network monitoring and analysis. It runs on most popular computing platforms, including UNIX, Linux, and Windows.

The Wireshark GUI interface has five major components: a. Command menus: standard pull down menus located at the top of the window.

b. Packet listing window: Display a one-line summary for each packet captured, including the packet number, time, source and destination address, protocol type.

c. Packet-header details window: provides details about the packet selected (highlighted) in the packet listing window.

d. Packet-contents window: displays the entire contents of the captured frame, in both ASCII and hexadecimal format.

e. Packet display filter field: a protocol name or other information can be entered in order to filter the information displayed in the packet-listing window.

Uses of Wireshark

- 1.Capture live packet data.
2. Import and Export packets.
- 3.Filter and Search packets.
- 4.Display and save packet data Colorize packet display.
- 5.Statistics in graphical way.

VIII. Diagrams / Experimental set-up /Work Situation



Fig.Wireshark logo

IX. Resources Required

Sr. No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB		
2.	Wireshark			
3.				

X. Procedure

Step 1 – Download Wireshark

<http://www.wireshark.org/download.html>

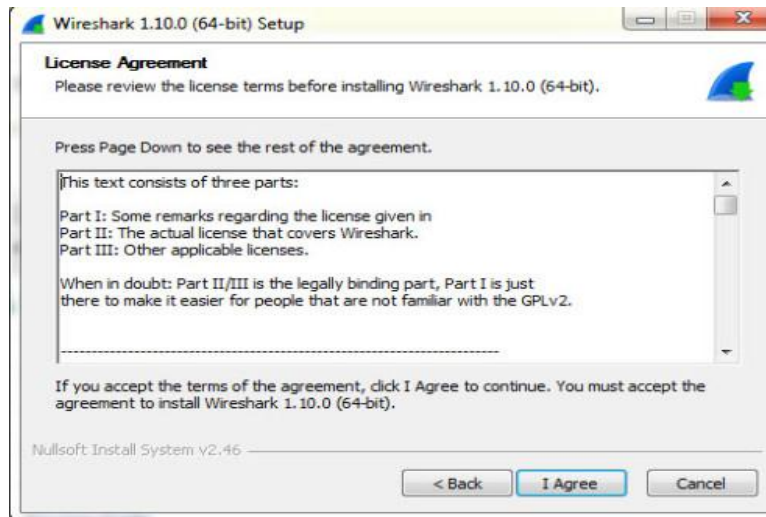
Run as Administrator

Step 2 – Install

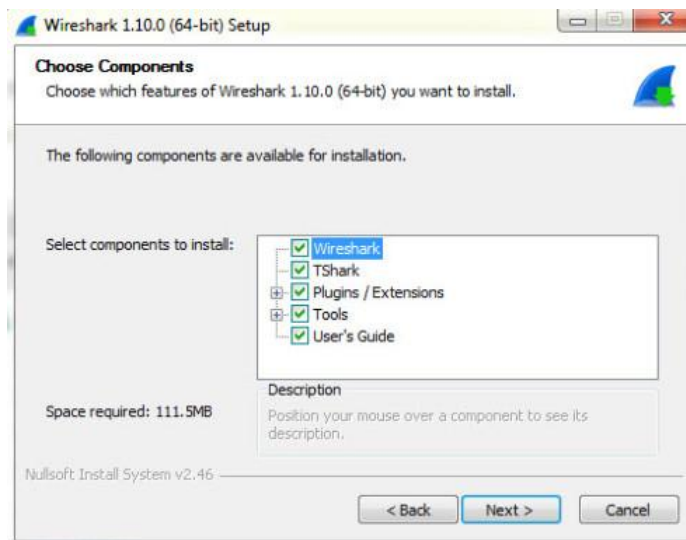
Next



I Agree

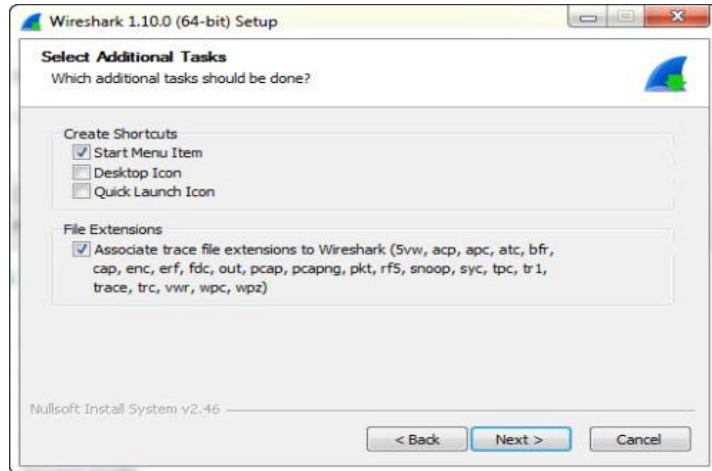


NextDisk space needed is 112 mb



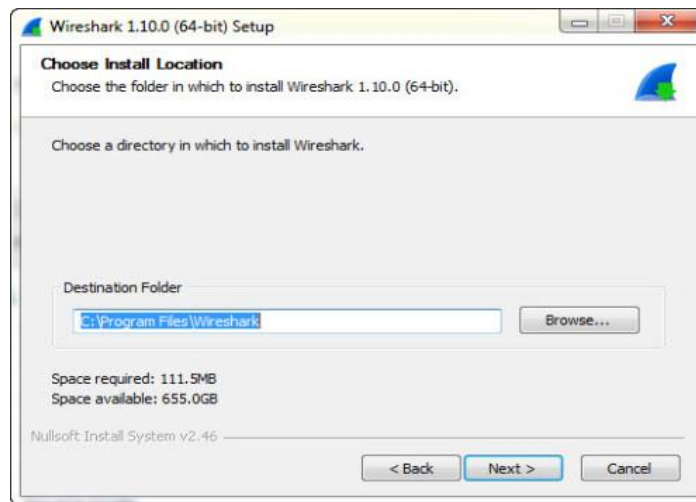
Next

Choose if Start Menu or Desktop Icon is preferred

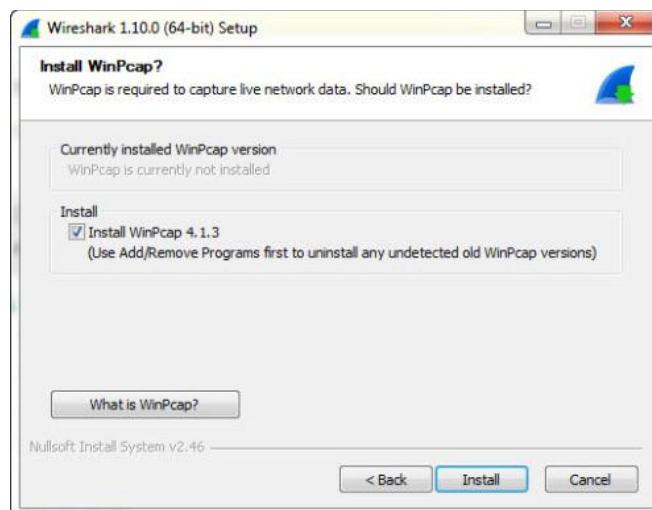


Next

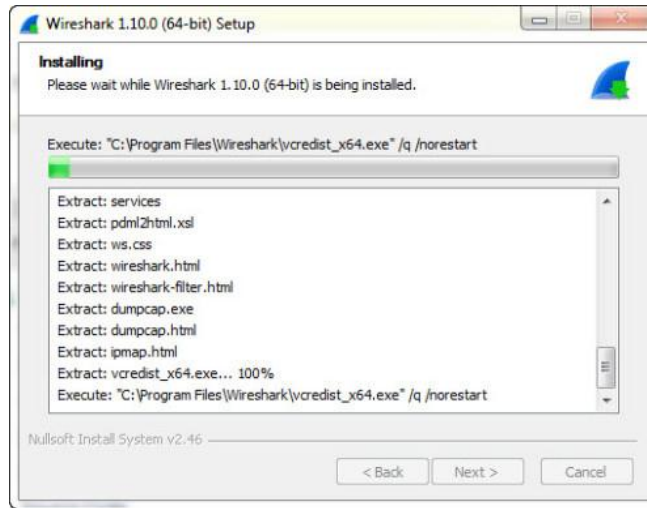
By default it installs into the directory c:\ Program Files\ Wireshark



Install WinPcap – as Wireshark won't work otherwise
Install



Wait for the files to extract...



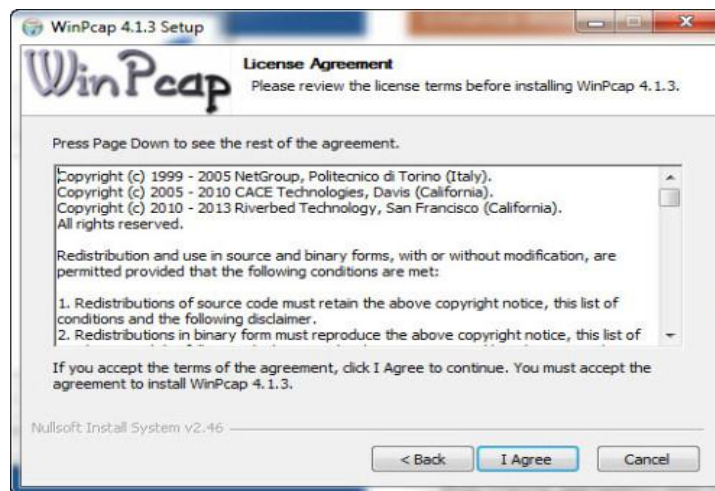
Step 2 – Install WinPcap

Wireshark won't install unless WinPcap is installed. Watch out for a second install to be launched. If you're not looking for it, you could miss it.

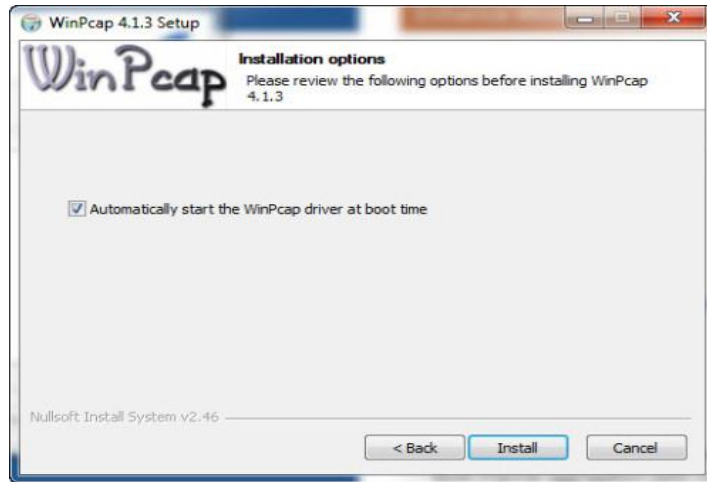
Next



I Agree



Install



Finish

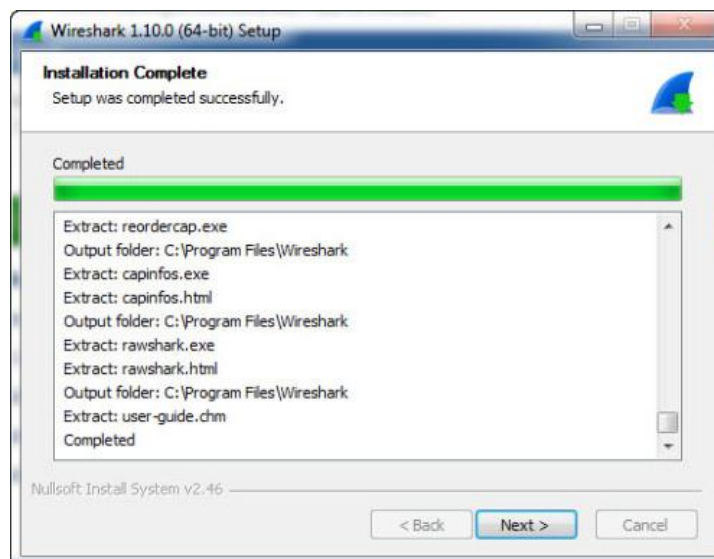


That's it!

Wireshark will now completely install for you.

If the install hangs half way through, it's because WinPcap has not been installed yet.

Next



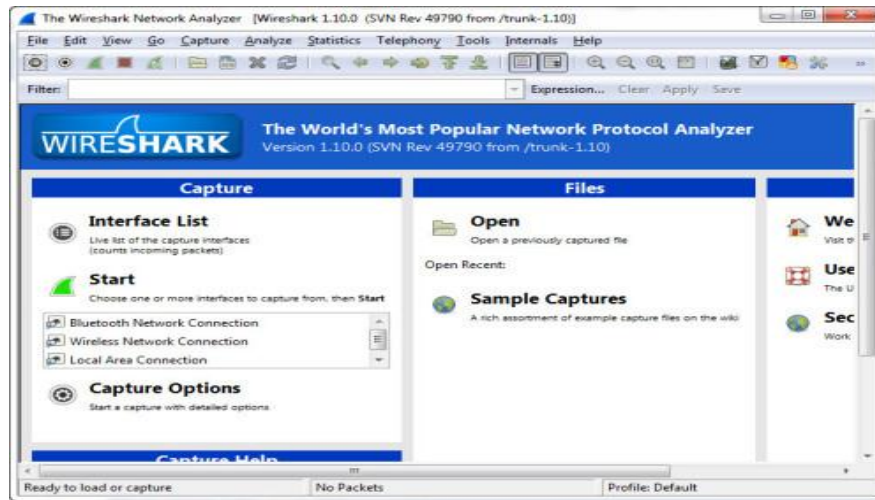


Launch Wireshark

Start > All Programs > Wireshark Icon

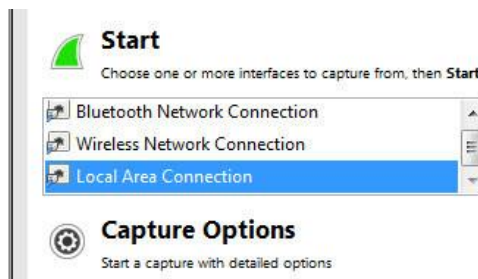


Wireshark launches



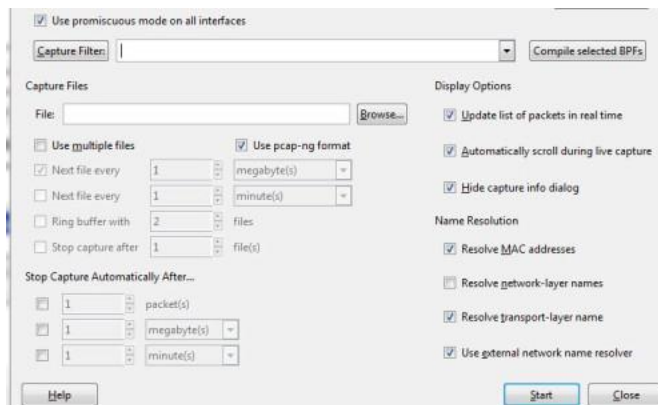
Select your Interface (ie Wired or Wireless)

Then Capture Options



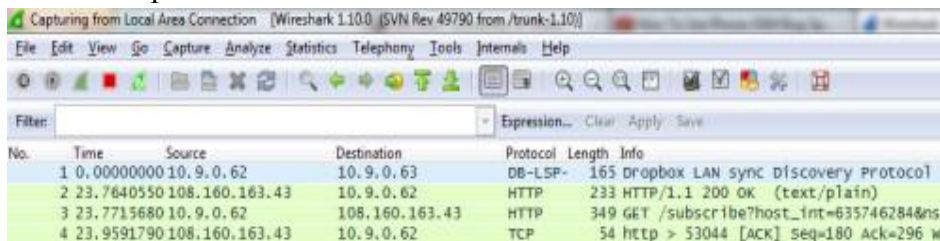
Promiscuous Mode > Start

Promiscuous mode means that it picks up packets and data for all devices on the network
That's it – Wireshark will now listen in to all transmissions



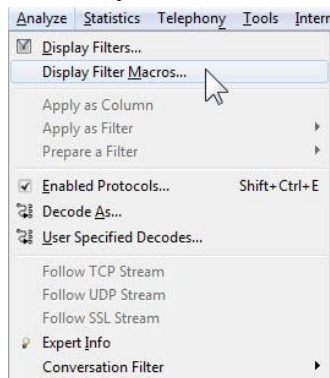
Wireshark launches – by default it's split into 3 panes

The top pane shows IP's & protocols



You can filter these results by protocol and by IP, and I'll cover that another time.

For now, select the Protocol header – and your results will sort by protocol.

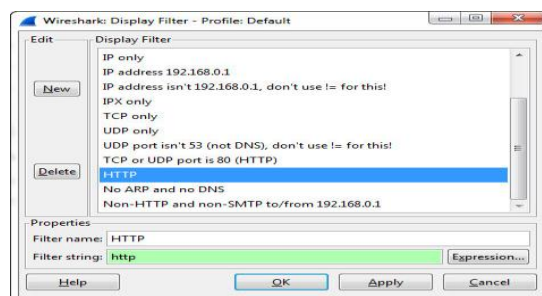


ANALYSE > Display Filter

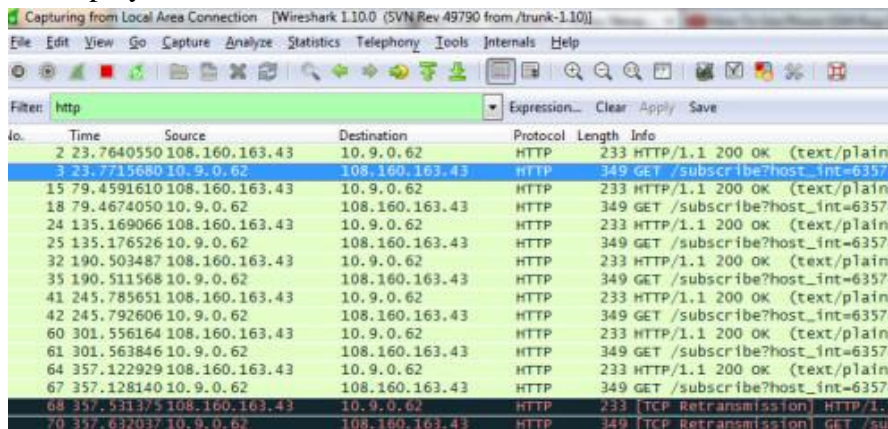
HTTP

Select HTTP

OK



HTTP ONLY is now displayed



XI. Precaution

1. Handle Computer System and peripherals with care
2. Follow Safety Practices

XII. Resources Used

Sr. No	Name of Resource	Specification
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
2.	Wireshark	
3.		

XIII. Result

.....

.....

.....

XIV. Practical Related Questions

1. Define protocol and give names of any two protocols.
2. Define packet and give its use.
3. What kinds of data are present in packet?
4. What is meaning of packet sniffer?
5. “Packet sniffer itself is passive.” state True or false and justify your answer.
6. Give the name of two components of packet sniffer with its use.
7. What is wireshark ?Give the names of wireshark GUI components.Write any 5 usage of wireshark?
8. Give the use of filter and search in wireshark.
9. List names of different operating system on which wireshark can be installed.

- 10. What is use of wincap software? Is it necessary to install for wireshark? Why?
- 11. Give the meaning of “configure as packet sniffer”.
- 12. How wireshark is useful in industry?

XV. Exercise

Student should Capture packet of TCP,UDP, HTTP, FTP using wireshark

(Space for Answer)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

References/ Suggestions for further Reading

https://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureFilterSection.html

XVI. Assessment Scheme

Performance indicator		Weightage
Process Related(35 Marks)		75%
1.	Completion of given task	25%
2.	Correctness of given task	50%
Product Related(15 Marks)		25%
3.	Answer to sample Question	15%
4.	Submit Report in Time	10%
Total(50 Marks)		100%

❖ **List of Students/Team Members**

.....

Marks Obtained			Dated Signature of Teacher
Process Related(35)	Product Related (15)	Total(50)	

Practical No.9: Setup FTP Client/Server and Transfer the File using FTP

I. Practical Significance

Use of FTP client server

II. Relevant Programs Outcomes (POs)

1. **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
2. **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
3. **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
4. **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
5. **Communication:** Communicate effectively in oral and written form.

III. Competency and Practical skills

1. Setup FTP client server
2. Transfer file using FTP

IV. Relevant Course Outcomes

Setup up computer Network for Specific Requirement
Configure Basic network Services
Configure TCP/IP services

V. Practical Outcomes (POs)

Create FTP Client server network

VI. Relevant Affective domain related Outcomes

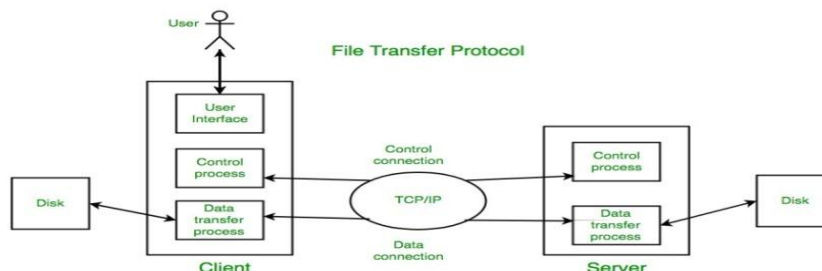
1. Follow safety practices
2. Practice good Housekeeping
3. Demonstrate working as a leader/team member
4. Follow ethical practices

VII. Minimum Theoretical Background

File Transfer Protocol (FTP) is the commonly used protocol for exchanging files over the Internet.

FTP uses the Internet's TCP/IP protocols to enable data transfer.

VIII. Diagrams / Experimental set-up /Work Situation



IX. Resources Required

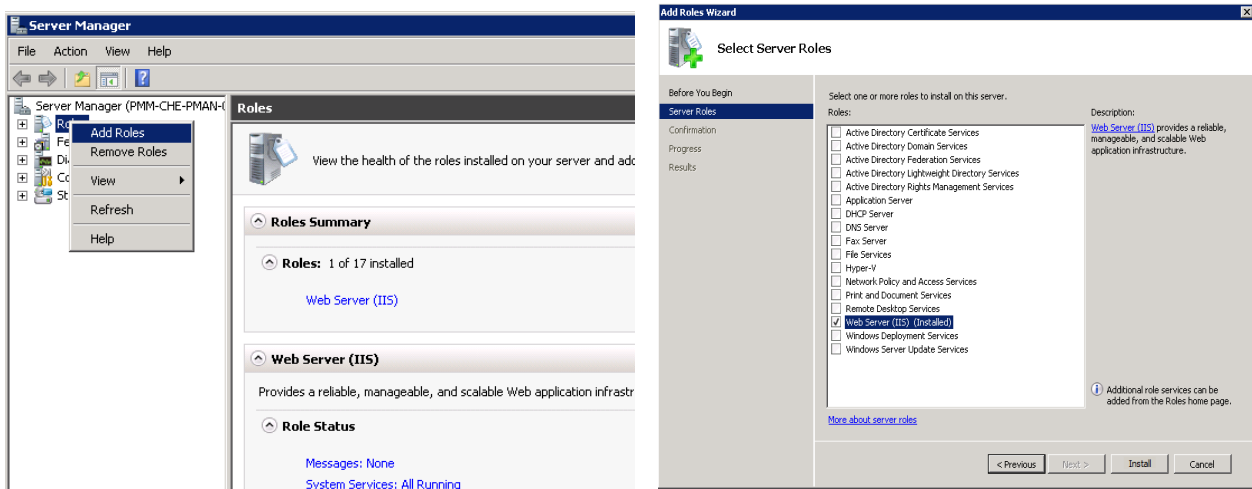
Sr. No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computers with Windows Server 2008 R2			

X. Procedure

We will use Windows Server 2008 R2 to configure FTP.

If IIS is not installed,

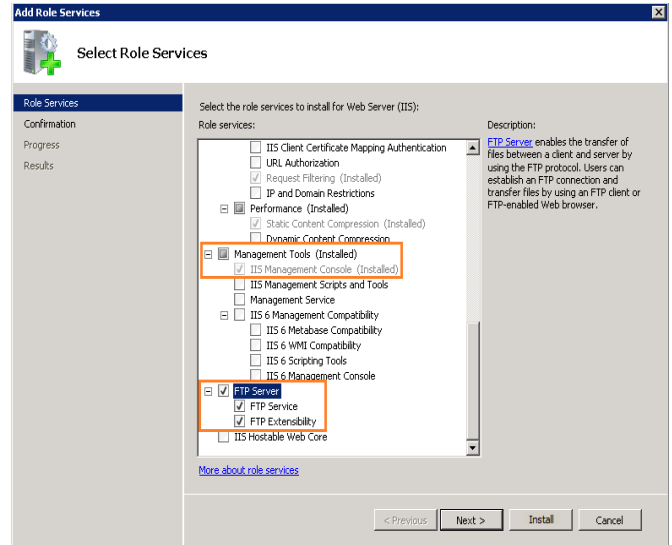
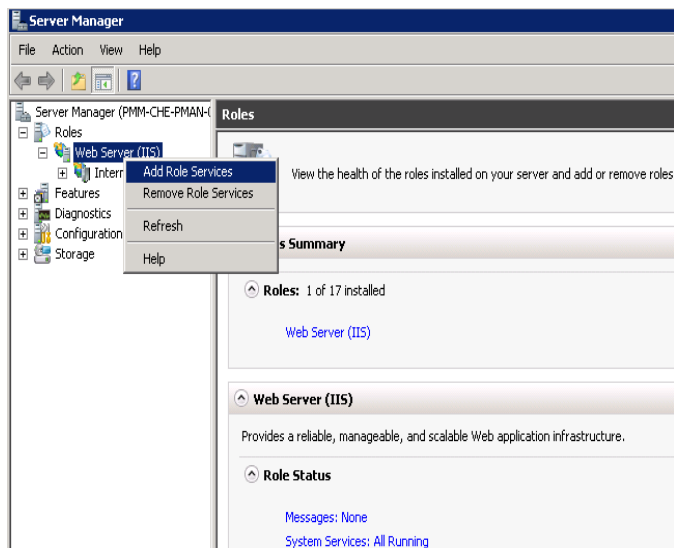
1. Navigate to **Start > Control Panel > Administrative Tools > Server Manager** in Windows Server Manager
2. Go to **Roles** node. Right-click on **Roles**, and click **Add Roles**.



3. In the Add Roles window, open **Server Roles** and check **Web Server (IIS)**.
4. Proceed through the setup wizard, and click **Install**. Wait for the installation to complete.

If IIS is installed already (as a Web server),

1. Navigate to **Start > Control Panel > Administrative Tools > Server Manager**
2. In the Windows Server Manager, go to **Roles** node, and expand **Web Server (IIS)**.
3. Right-click on **Web Server (IIS)**, and click on **Add Role Services**.
4. In the **Add Role Services** window, go to **Roles Services**, and check **FTP Server**.
5. Confirm that **IIS Management Console** is checked under **Management Tools**.



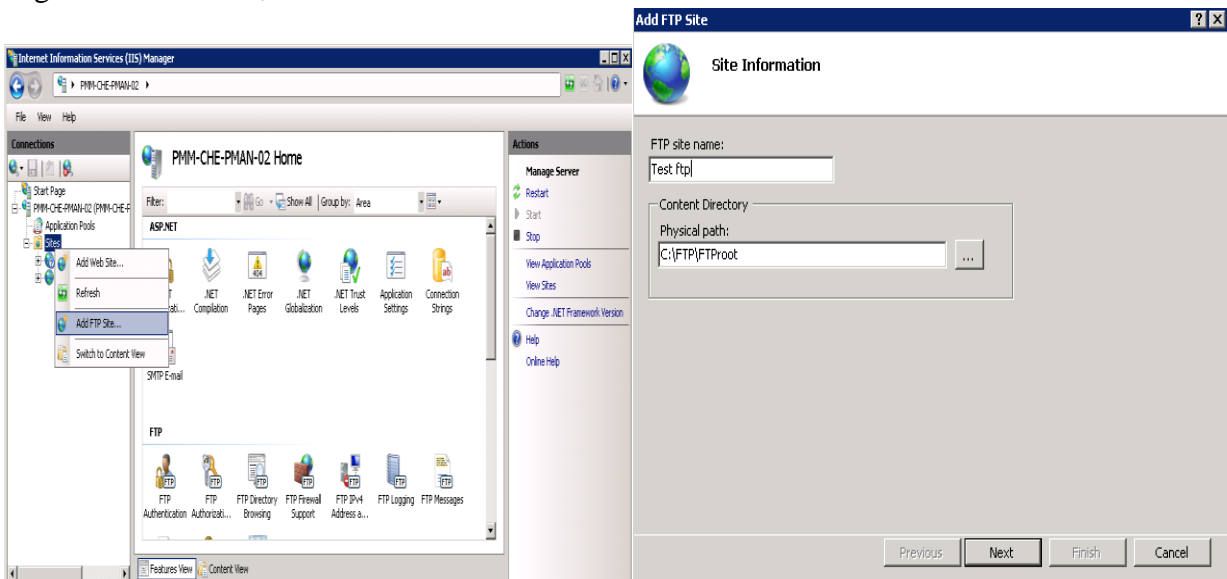
6. Click **Next**, and then **Install**. Wait for the installation to complete.

Transferring files

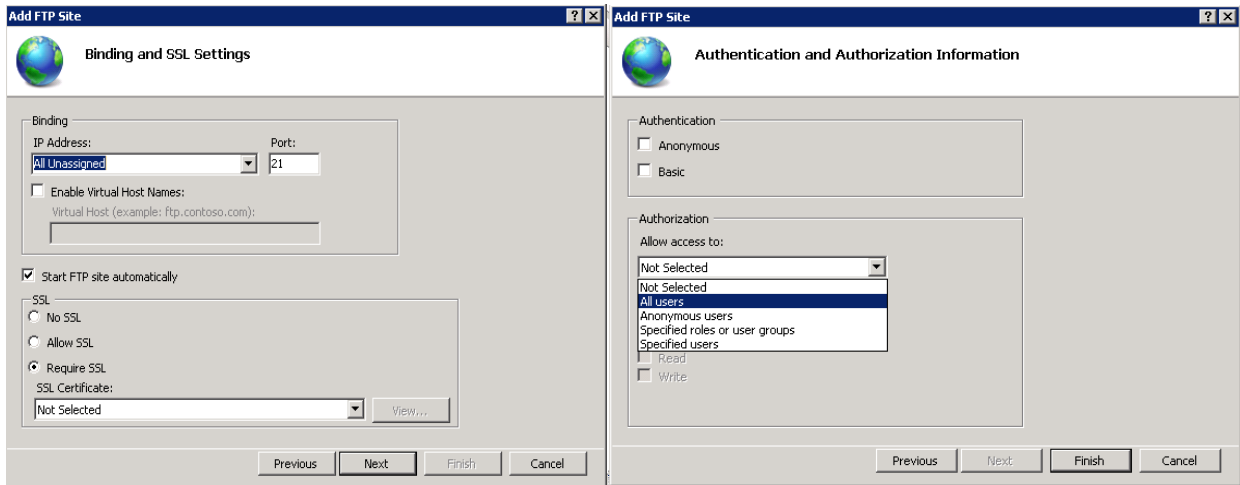
To transfer files, you should add an FTP site. Once the FTP site is enabled, clients can transfer to and from the site using the FTP protocol.

Setting up an FTP site

1. Navigate to **Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Once the IIS console is open, expand the local server.
3. Right-click on **Sites**, and click on **Add FTP Site**.



4. In the Add FTP Site window, type the FTP server name and the content directory path, and click Next. The directory path should be the same as the one we set permissions to allow anonymous access above, we used: **%SystemDrive%\ ftp \ftproot**
5. In the Binding and SSL Settings window, type the IP address of the server. Check the **Start FTP Site Automatically** option. Choose **SSL Based on Constraint**. Click **Next**.



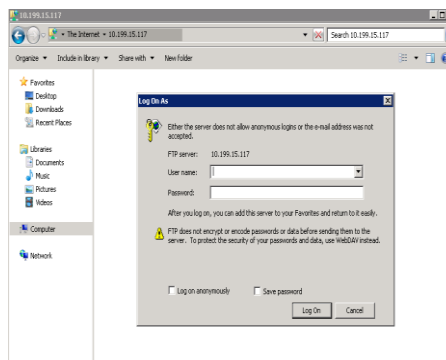
6. Now, select **Basic** for authentication.

Note: Basic authentication means there is no encryption used. Thus, username/password are sent in clear text. Basic authentication matches the username/password from the Active Directory database. You can also create accounts in IIS. This can be done from under Management Tools in Web Server (IIS) role. Under **Authorization**, you can select **All Users** to allow FTP access to all users from the domain. Also, check both **Read** and **Write** under **Permissions Based on Requirement**.

7. Click **Finish**. Now, the FTP site creation is complete.

Accessing files on the FTP server

To access files on the FTP server, open a file explorer and type **ftp://serverIP**. The FTP server asks for a username and password. Enter the username and password (Windows or Active Directory credentials) and click **Logon**. The files and folders display under the FTP server.



XI. Precaution

1. Handle Computer System and peripherals with care
2. Follow Safety Practices

XII. Resources Used

Sr. No	Name of Resource	Specification
1.	Computers with Windows Server 2008 R2	
2.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB

XIII. Result

.....
.....
.....

XIV. Practical Related Questions

1. FTP is built on _____ architecture(Client-server/P2P)
2. Identify the incorrect statement
 - a) FTP stands for File Transfer Protocol
 - b) FTP uses two parallel TCP connections
 - c) FTP sends its control information in-band
 - d) FTP sends exactly one file over the data connection
3. Draw Diagram for FTP
4. What is FTP? How it works?

XV. Exercise

Student should setup FTP client server and transfer file using FTP

(Space for Answer)

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

XVI. References/ Suggestions for further Reading

<https://www.deskshare.com/resources/articles/ftp-how-to.aspx>

XVII. Assessment Scheme

Performance indicator		Weightage
Process Related(35 Marks)		75%
1.	Completion of given task	25%
2.	Correctness of given task	50%
Product Related(15 Marks)		25%
3.	Answer to sample Question	15%
4.	Submit Report in Time	10%
Total(50 Marks)		100%

❖ List of Students/Team Members

.....

.....

.....

.....

Marks Obtained			Dated Signature of Teacher
Process Related(35)	Product Related (15)	Total(50)	

Practical No.10: Install TCP/IP protocol and configure Advanced features of TCP/IP Protocols like IP address,Subnet mask,gateway, primary and secondary DNS

I. Practical Significance

Install TCP/IP protocol with advanced features

II. Relevant Programs Outcomes (POs)

- 1. Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
- 2. Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
- 3. Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
- 4. Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
- 5. Communication:** Communicate effectively in oral and written form.

III. Competency and Practical skills

1. Setup Network with TCP/IP protocol

IV. Relevant Course Outcomes

Use Basic Concept of Networking for setting of Computer Network

Configure TCP/IP services

Implement Sub netting for improved Network address Management

V. Practical Outcomes (POs)

Install TCP/IP Protocol

VI. Relevant Affective domain related Outcomes

1. Demonstrate working as a leader/team member
2. Follow ethical practices

VII. Minimum Theoretical Background

Protocol:

It is a set of rules and conventions used for communication between network devices.

Protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received.

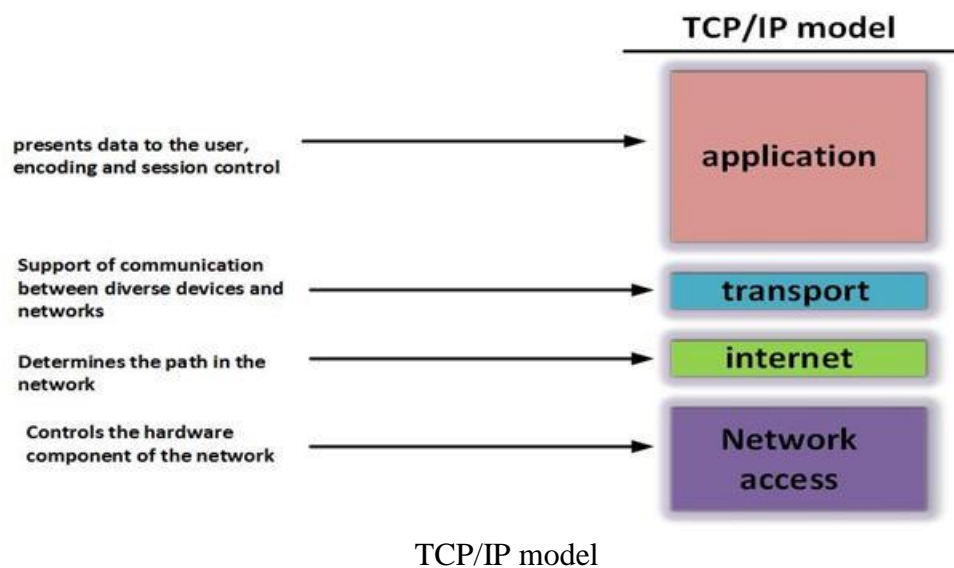
Some protocols also support message acknowledgement and data compression designed for reliable and/or high-performance network communication.

It determines the type of error checking to be used.

Transmission control protocol (TCP), Internet protocol (IP), Hyper Text Transfer Protocol (HTTP), File transfer protocol (FTP) etc.

TCP/IP:

- ❖ Transmission Control protocol/Internet Protocol, used to connect computers on the Internet or network.
- ❖ TCP/IP is built into the UNIX Operating system and is used by the Internet, making it the de facto standard for transmitting data over networks.
- ❖ Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message.
- ❖ Internet Protocol, handles the address part of each packet so that it gets to the right destination.
- ❖ TCP/IP protocols map to a four-layer conceptual model known as the DARPA model, named after the US Government agency that initially developed TCP/IP. The four layers of the DARPA model are: Application, Transport, Internet, and Network Interface.



IP address:

- ❖ An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.
- ❖ An IP address is an identifier for a computer or device on a TCP/IP network.
Two versions of the Internet Protocol (IP) are in use: IP Version4 (IPv4) and IP Version6 (IPv6).
- ❖ IPv4 addresses are of 32 bits that are canonically represented in dot-decimal notation, which consists of four decimal numbers, each ranging from 0 to 255, separated by dots, e.g., 172.16.254.1

- ❖ IPv6 addresses are of 128 bits that are represented as eight groups of four hexadecimal digits separated by colons.
e.g. 2001:0db8:85a3:0042:1000:8a2e:0370:7334
- ❖ The IPv4 address space can be subdivided into 5 classes Class A, B, C, D and E. Each class consists of a contiguous subset of the overall IPv4 address range.

VIII. Diagrams / Experimental set-up /Work Situation

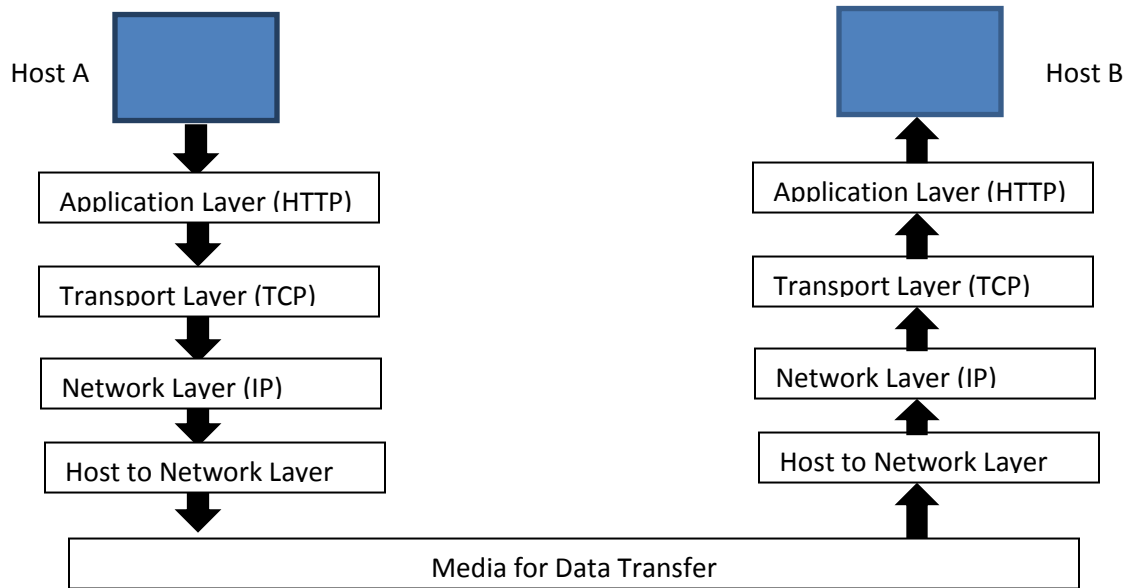


Fig. Communication in TCP/IP model

IX. Resources Required


Sr. No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB		

X. Procedure

Complete the following steps to install and configure the TCP/IP protocol.

1. Start->Control Panel->Network and Internet->Network Sharing center,Change adapter setting
2. Right-click the connection to which you want to add a network component, and then click **Properties**.
3. If **Internet Protocol (TCP/IP)** is listed, skip to Step 6. If **Internet Protocol (TCP/IP)** is not listed, click **Install**.
4. In the **Select Network Component Type** dialog box, click **Protocol**, and then click **Add**.
5. From the **Network Protocol** list, select **TCP/IP Protocol** and click **OK**.
6. From the **General** tab (for local area connections) or the **Networking** tab (for all other connections), select **Internet Protocol (TCP/IP)**, and then click **Properties**.

7. Configure TCP/IP either automatically or manually.

 Contact your network administrator to find out if there is a DHCP server installed on your network.

- **Automatically** – You can automatically configure TCP/IP services if you have a DHCP server on your network. This automatic process ensures easy and accurate installation of TCP/IP because your local computer is configured with the correct IP address, subnet mask, and default gateway.

To configure automatically, select **Obtain an IP address automatically**, and then click **OK**.

- **Manually** – You must configure TCP/IP manually if you do not have a DHCP server on your network, or if you are configuring a Windows server to be a DHCP server. In this case, you must manually enter valid addressing information after the TCP/IP protocol software is installed on your computer. To avoid duplicate addresses, be sure to use the values for IP addresses and subnet masks that are supplied by your network administrator.

To configure manually, select **Use the following IP address**, specify the necessary parameters, and then click **OK**.

XI. Precaution

1. Handle Computer System and peripherals with care
2. Follow Safety Practices

XII. Resources Used

Sr. No	Name of Resource	Specification
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
2.	Any other Resource	

XIII. Result

.....

XIV. Practical Related Questions

1. Define protocol
2. Give four examples of protocol with its full name.
3. Write the name of layers in TCP/IP?
4. Give the use of IP address.
5. Give and explain the address format of IPv4 and IPv6. Give the use of network layer in TCP/IP.
6. How 192.168.276 is type of class C IP address?
7. Convert the IPv4 address “192168.276” to binary format of 32 bits.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

XVI. References/ Suggestions for further Reading

<https://searchnetworking.techtarget.com/definition/TCP-IP>

XVII. Assessment Scheme

Performance indicator		Weightage
Process Related(35 Marks)		75%
1.	Completion of given task	25%
2.	Correctness of given task	50%
Product Related(15 Marks)		25%
3.	Answer to sample Question	15%
4.	Submit Report in Time	10%
Total(50 Marks)		100%

❖ List of Students/Team Members

.....

.....

.....

.....

Marks Obtained			Dated Signature of Teacher
Process Related(35)	Product Related (15)	Total(50)	

Practical No.11:Configure and use Telnet Client Server

I. Practical Significance

Know the use of Telnet Server

Configure TelnetServer

II. Relevant Programs Outcomes (POs)

- 1. Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
- 2. Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
- 3. Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
- 4. Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
- 5. Communication:**Communicate effectively in oral and written form.

III. Competency and Practical skills

1. Configure Telnet Server

IV. Relevant Course Outcomes

Use Basic Concept of Networking for setting of Computer Network

Setup up computer Network for Specific Requirement

Configure Basic network Services

V. Practical Outcomes (POs)

Install TelnetServer

VI. Relevant Affective domain related Outcomes

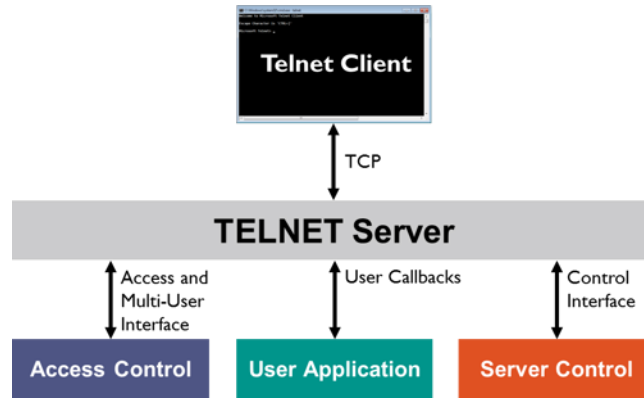
1. Follow safety practices
2. Practice good Housekeeping
3. Demonstrate working as a leader/team member
4. Follow ethical practices

VII. Minimum Theoretical Background

Telnet is a client-server protocol, based on a reliable connection-oriented transport. Typically, this protocol is used to establish a connection to Transmission Control Protocol (TCP) port number 23

Telnet is a protocol used on the Internet or local area network to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection

VIII. Diagrams / Experimental set-up /Work Situation



IX. Resources Required

Sr. No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB		

X. Procedure

Enabling the Telnet Server

1. Go to **Start -> Control Panel -> Programs**.
2. In the **Programs and Features** section, click **Turn Windows features on or off**. If the **User Account Control** permission warning pops up, click on **Continue**. And if you are prompted for an administrator password, type it in.
3. In the **Windows Features** dialog box, select the **Telnet Server** check box.
4. Click **OK** and wait for the installation to finish.

Starting the Telnet Server

1. Go to **Control Panel**, and then go to **System -> Administrator Tools**.
2. Click on the **Services** applet (**services.msc** if you prefer to use **Run** command or **Start Search**).
3. Locate the “**Telnet**” service, right-click on it and select **Properties**.
4. In the **Startup Type** drop down menu, select “**Automatic**” instead of “**Disabled**”.
5. Click on **Apply** button.
6. Right-click on the “**Telnet**” service again, but this time select **Start** option on right-click context menu. Telnet Server service should be running after this.
7. Click **OK**

XI. Precaution

- 1. Handle Computer System and peripherals with care
- 2. Follow Safety Practices

XII. Resources Used

Sr. No	Name of Resource	Specification
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
2.	Any other Resource	

XIII. Result

.....
.....
.....

XIV. Practical Related Questions

- 1. What is Telnet server
- 2. List Applications of Telnet Server
- 3. Which Port number is used by Telnet Service

XV. Exercise

Student should Setup Telnet server and use Telnet Server

(Space for Answer)

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

References/ Suggestions for further Reading

<https://www.windows-commandline.com/enable-telnet-server-windows/>

XVI. Assessment Scheme

Performance indicator		Weightage
Process Related(35 Marks)		75%
1.	Completion of given task	25%
2.	Correctness of given task	50%
Product Related(15 Marks)		25%
3.	Answer to sample Question	15%
4.	Submit Report in Time	10%
Total(50 Marks)		100%

❖ List of Students/Team Members

.....

.....

.....

.....

Marks Obtained			Dated Signature of Teacher
Process Related(35)	Product Related (15)	Total(50)	

Practical No.12: Configure and work with Remote desktop application available with Operating System

I. Practical Significance

Understand Remote desktop application

II. Relevant Programs Outcomes (POs)

- 1. Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
- 2. Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
- 3. Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
- 4. Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
- 5. Communication:** Communicate effectively in oral and written form.

III. Competency and Practical skills

1. Setup Remote Desktop Application

IV. Relevant Course Outcomes

Use Basic Concept of Networking for setting of Computer Network
Setup up computer Network for Specific Requirement
Configure Basic network Services
Configure TCP/IP services

V. Practical Outcomes (POs)

Understand system based remote desktop application

VI. Relevant Affective domain related Outcomes

1. Demonstrate working as a leader/team member
2. Follow ethical practices

VII. Minimum Theoretical Background

The RemoteApp and Desktop Connections feature offers several benefits:

RemoteApp programs launch from the Start menu just like any other application.

Published Remote Desktop connections are included alongside RemoteApp programs on the Start menu.

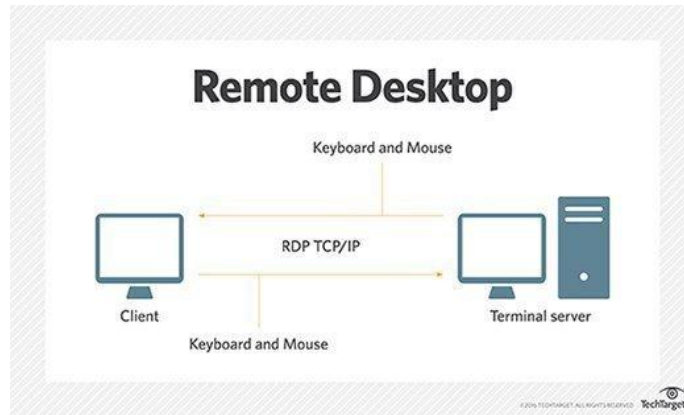
Changes to the published connection (such as newly published RemoteApp programs) are automatically reflected on the user's Start menu, without any effort on the user's part.

RemoteApp programs can be easily launched with Windows Search.

Users only have to log on once, to create the connection. From that point on, updates happen with no prompt for user credentials.

RemoteApp and Desktop Connections does not require domain membership for client computers. RemoteApp and Desktop Connections benefits from new features in Windows Server 2008 R2, such as Personal Desktop assignment or per-user application filtering. RemoteApp and Desktop Connections is built on standard technologies such as XML and HTTPS, making it possible for developers to build solutions around it. It also offers APIs that allow the client software to support other types of resources, in addition to RemoteApp programs and Remote Desktop connections.

VIII. Diagrams / Experimental set-up /Work Situation

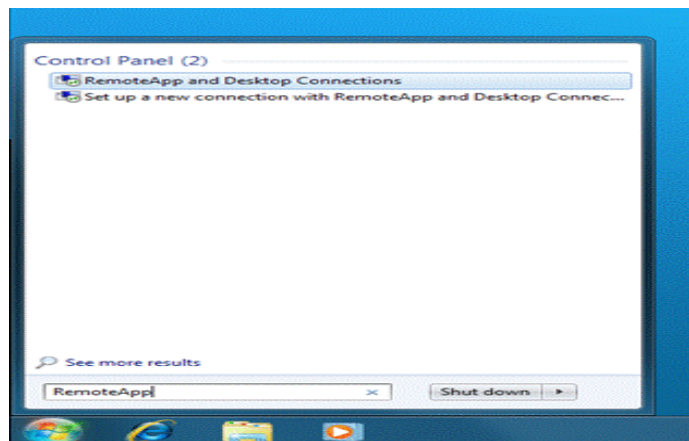


IX. Resources Required

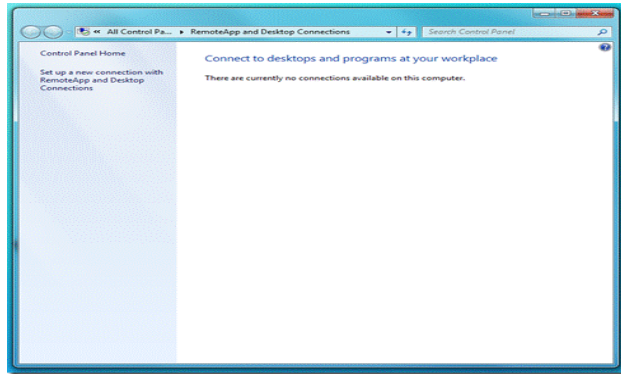
Sr. No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB		

X. Procedure

1. Open RemoteApp and Desktop Connections in Control Panel, either by opening Control Panel, or by using Windows Search.



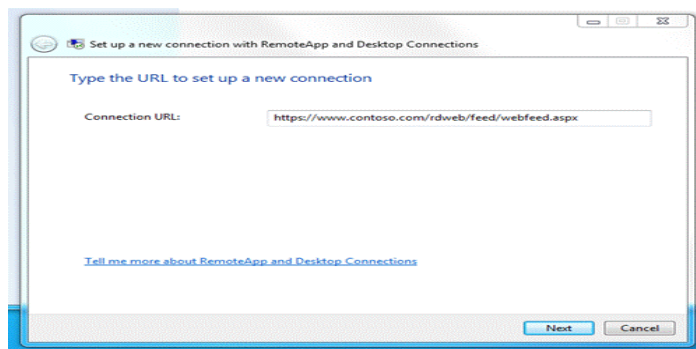
2. Click **Set up a new connection with RemoteApp and Desktop Connections** . This will start the new connection wizard.



3. Enter the URL of the connection. This URL will generally be of the form:

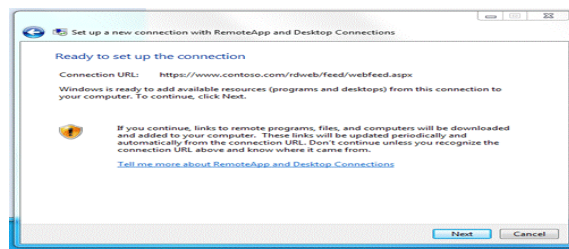
`https://<servername>/rdweb/feed/webfeed.aspx`

Here, “<servername>” is the host name of the RD Web Access server. The wizard should look like this:

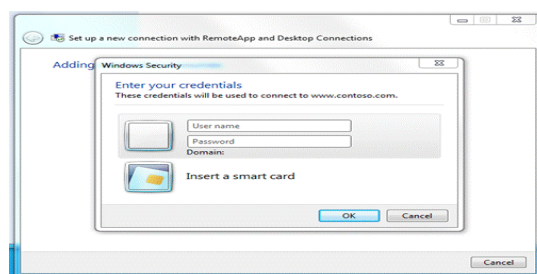


Note: RemoteApp and Desktop Connections uses HTTPS to connect to the server. In order to connect properly, the client operating system must trust the SSL certificate of the RD Web Access server. Also, the server name in the URL must match the one in the server’s SSL certificate.

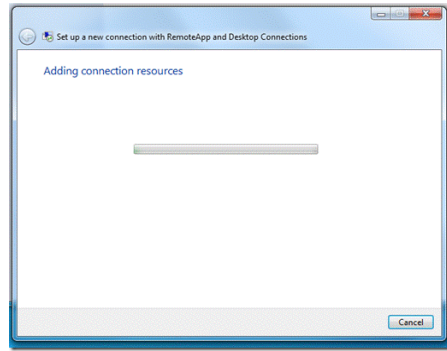
4. Click **Next** .



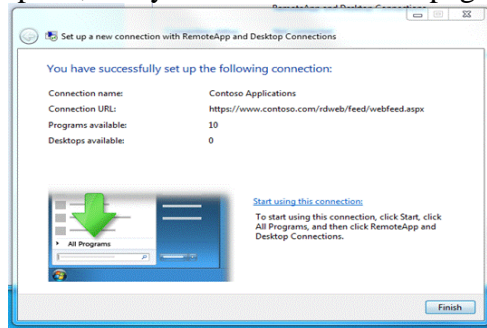
5. Click **Next** . The RemoteApp and Desktop Connections client software will now contact the RD Web Access server to set up the connection. You will be prompted to authenticate to the web server.



6. Enter your credentials. Now the RemoteApp and Desktop Connections client software will finish setting up the connection.

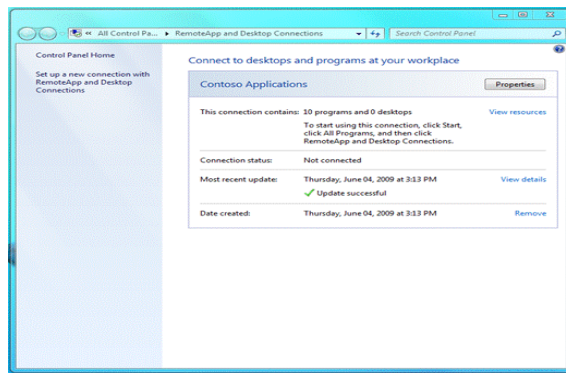


In a moment, the process will complete, and you will see a wizard page that summarizes the results.



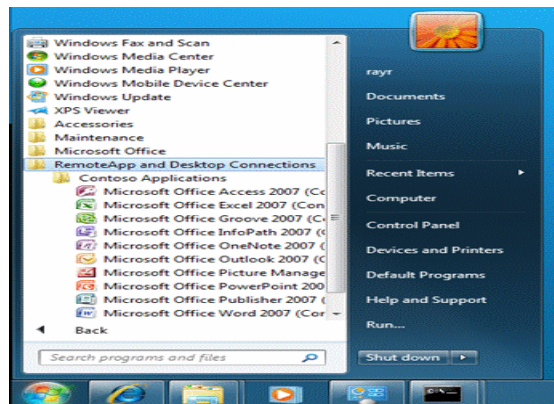
7. Click **Finish** .

Now the RemoteApp and Desktop Connections Control Panel will show your newly created connection:

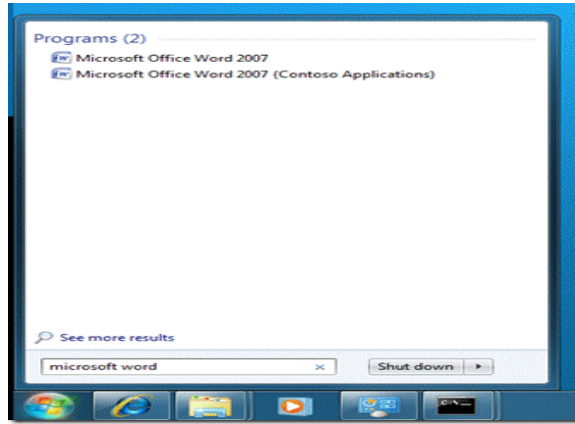


You can return to this summary page anytime you need to manage your connections.

The Start menu will now contain the RemoteApp programs from the new connection:



You can also access these programs by using Windows Search:



XI. Precaution

- 1. Handle Computer System and peripherals with care
- 2. Follow Safety Practices

XII. Resources Used

Sr. No	Name of Resource	Specification
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB

XIII. Result

.....
.....
.....

XIV. Practical Related Questions

- 1. What is Remote Desktop Application
- 2. How to Use to Remote Desktop Application
- 3. Which other remote desktop applications are available
- 4. Which are benefits of Remote Desktop Application

XV. Exercise

Use Remote Desktop Application show the output

(Space for Answer)

.....
.....
.....
.....
.....
.....

.....

XVI. References/ Suggestions for further Reading

<https://www.computerworlduk.com/galleries/it-business/best-remote-desktop-software-for-small-businesses-3673923/>

XVII. Assessment Scheme

Performance indicator		Weightage
Process Related(35 Marks)		75%
1.	Completion of given task	25%
2.	Correctness of given task	50%
Product Related(15 Marks)		25%
3.	Answer to sample Question	15%
4.	Submit Report in Time	10%
Total(50 Marks)		100%

❖ **List of Students/Team Members**

.....

Marks Obtained			Dated Signature of Teacher
Process Related(35)	Product Related (15)	Total(50)	

Practical No.13:Configure DHCP server

I. Practical Significance

Configure DHCP server

II. Relevant Programs Outcomes (POs)

1. **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
2. **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
3. **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
4. **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
5. **Communication:**Communicate effectively in oral and written form.

III. Competency and Practical skills

1. Setup DHCP server

IV. Relevant Course Outcomes

Setup up computer Network for Specific Requirement
Configure TCP/IP services

V. Practical Outcomes (POs)

Understand assigning IP address Dynamically

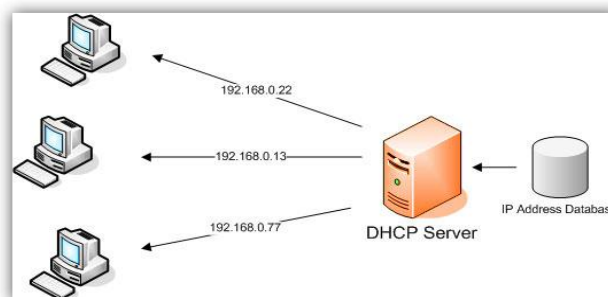
VI. Relevant Affective domain related Outcomes

1. Follow safety practices
2. Demonstrate working as a leader/team member
3. Follow ethical practices

VII. Minimum Theoretical Background

Dynamic Host Configuration Protocol (DHCP) is to assign network settings automatically to every workstation in the network by a central server rather than configuring them locally on each. A host configured to use DHCP is enabled to configure itself completely and automatically according to directions from the server.

VIII. Diagrams / Experimental set-up /Work Situation



IX. Resources Required

Sr. No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computers with Windows Server 2016			

X. Procedure

How to Configure DHCP on Windows Server 2016

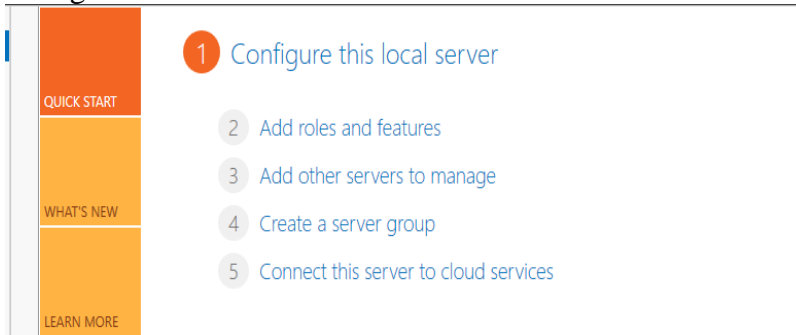
DHCP is used to dynamically assign IP addresses to client machines. This tutorial is written to help you to install and configure DHCP on Windows Server 2016. Once you have followed this article, go ahead with creating scopes and start leasing out IP addresses

Prerequisites

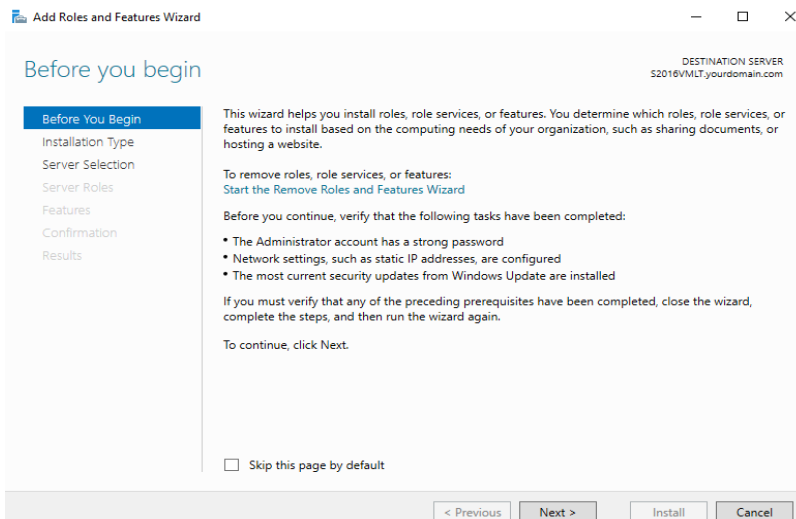
1. The administrator account has a strong password.
2. Latest updates are installed.
3. Firewall is turned off.
4. Static IP is configured.

Configure DHCP on Windows Server 2016

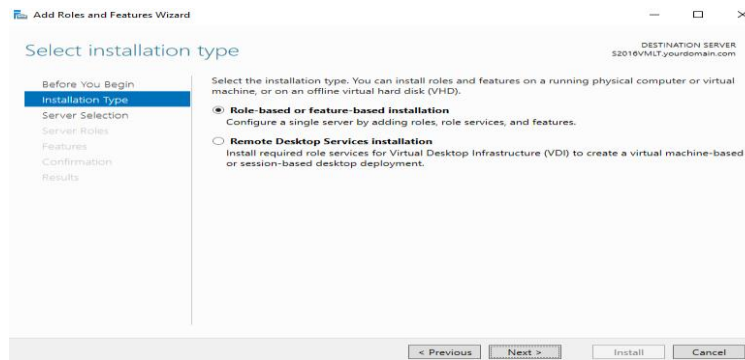
Step 1. Open Server Manager and click Add roles and features.



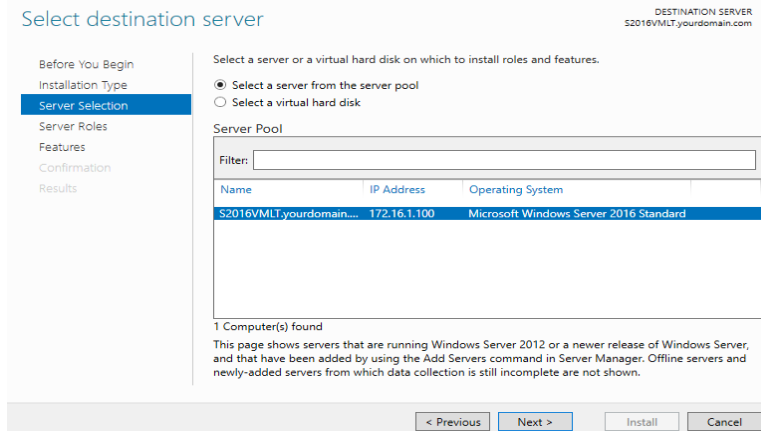
Step 2. Click Next to start the Role and Feature Wizard.



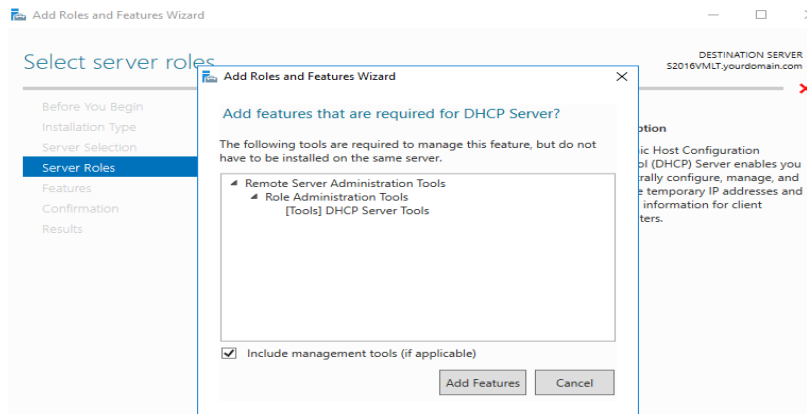
Step 3. Choose Role-based or feature-based installation and click Next.



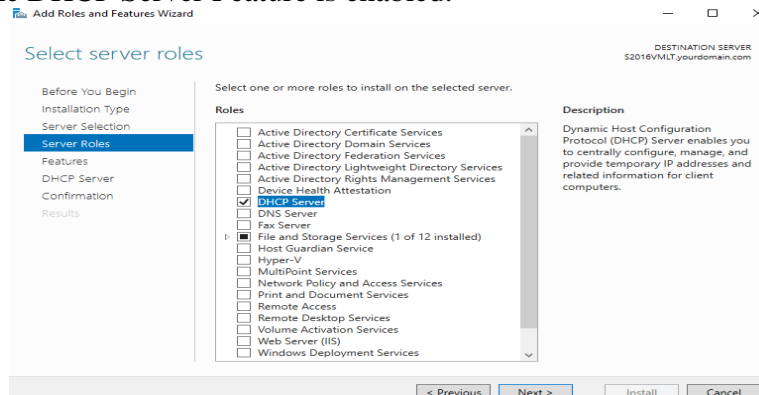
Step 4. Choose the server on which you want to configure DHCP and click Next.



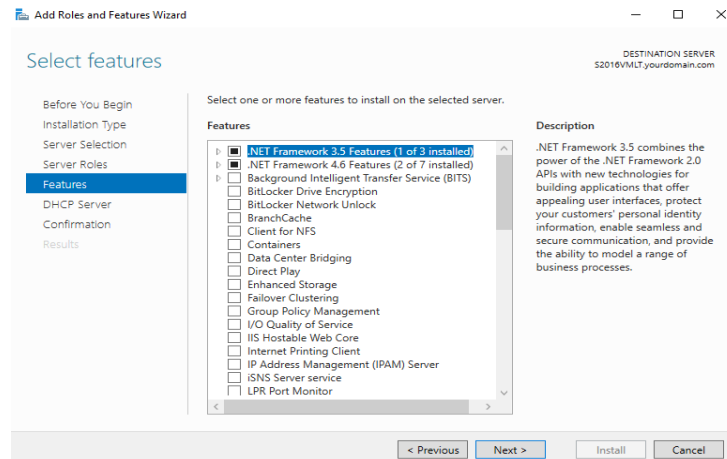
Step 5. Choose DHCP from server roles. As soon as you choose DHCP, a new window appears. Click Add Features.



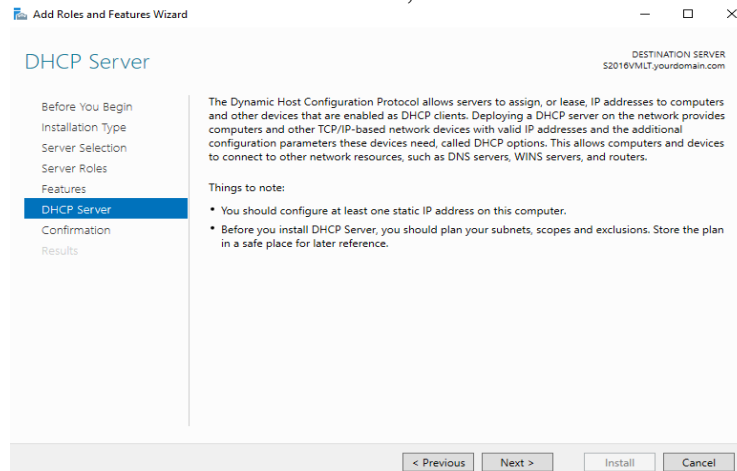
Step 6. Click Next. The DHCP Server Feature is enabled.



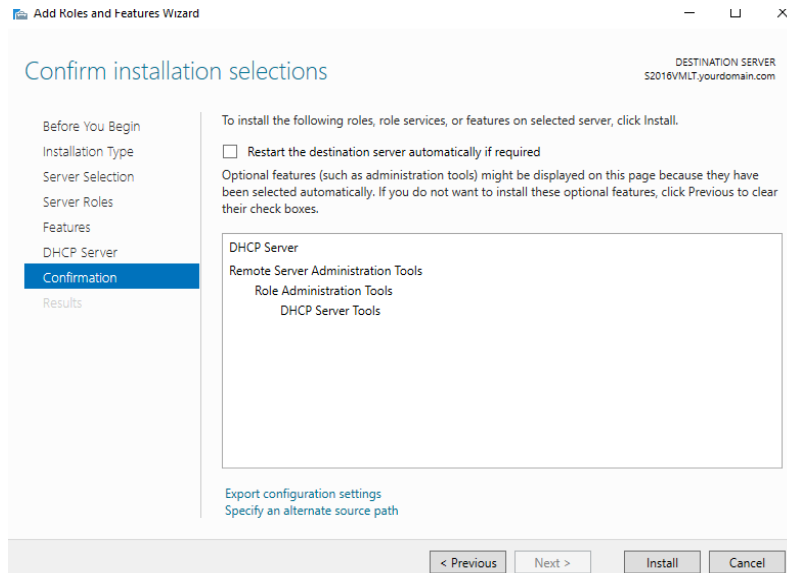
Step 7. Click Next. The .NET Frameworks that are required for the DHCP server are already pre-selected.



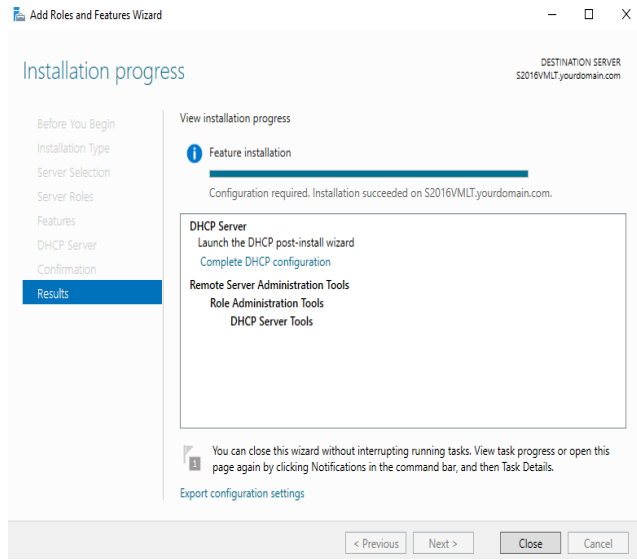
Step 8. Read the explanation about the DHCP function, then click Next.



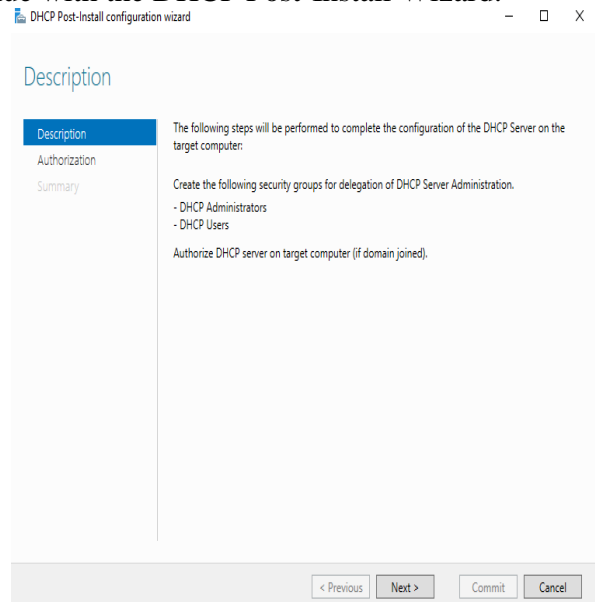
Step 9. Click Install.



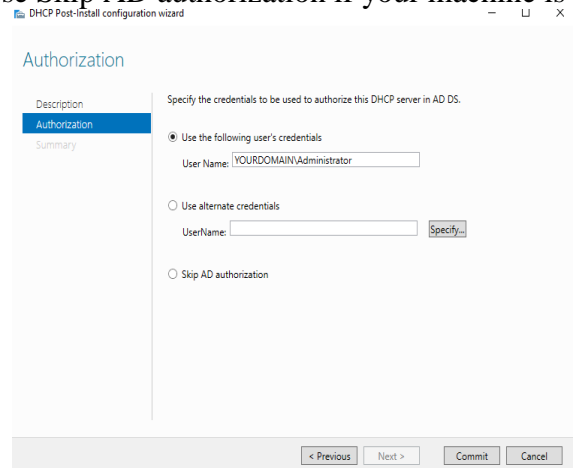
Step 10. Click "Complete DHCP configuration".



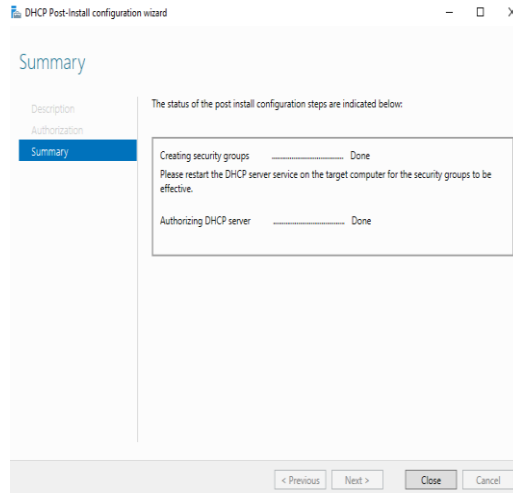
Step 11. Click Next to continue with the DHCP Post-Install Wizard.



Step 12. Click Commit (Choose Skip AD authorization if your machine is on workgroup).



Step 13. Click Close and you are done with configuring DHCP.



XI. Precaution

- 3. Handle Computer System and peripherals with care
- 4. Follow Safety Practices

XII. Resources Used

Sr. No	Name of Resource	Specification
1.	Computers with Windows Server 2016	
2.	Any other Resource	

XIII. Result

.....
.....
.....

XIV. Practical Related Questions

- 1. Explain DHCP
- 2. What is the use of DHCP server
- 3. Explain working of DHCP server
- 4. Differentiate between Dynamic IP and Static IP address

XV. Exercise

Student should configure DHCP server

(Space for Answer)

.....
.....
.....
.....

.....

References/ Suggestions for further Reading

https://en.wikipedia.org/wiki/Windows_Server_2016

XVI. Assessment Scheme

Performance indicator		Weightage
Process Related(35 Marks)		75%
1.	Completion of given task	25%
2.	Correctness of given task	50%
Product Related(15 Marks)		25%
3.	Answer to sample Question	15%
4.	Submit Report in Time	10%
Total(50 Marks)		100%

❖ List of Students/Team Members

.....

Marks Obtained			Dated Signature of Teacher
Process Related(35)	Product Related (15)	Total(50)	

Practical No.14: Create two subnets and implement it with calculated subnet masking**I. Practical Significance**

Understand subnet and use of subnet

Calculate subnet mask

II. Relevant Programs Outcomes (POs)

1. **Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
2. **Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
3. **Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
4. **Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
5. **Communication:** Communicate effectively in oral and written form.

III. Competency and Practical skills

1. Create two subnets

IV. Relevant Course Outcomes

Setup up computer Network for Specific Requirement

Implement Sub netting for improved Network address Management

V. Practical Outcomes (POs)

Create two subnet

VI. Relevant Affective domain related Outcomes

1. Follow safety practices
2. Follow ethical practices

VII. Minimum Theoretical Background**What is Subnetting?**

Subnetting is a process of dividing a single large network in multiple smaller networks.

Subnet: A subnet allows the flow of network traffic between host: to be segregated based on a network configuration. By organizing hosts into logical groups, subnetting can improve network security and performance. Sub netting can be useful in variety of ways, including simplifying network administration, enabling you to use different physical media such as Ethernet and FDDI and adding a layer of security to your network. The most common use of sub netting is to control network traffic.

Subnetting is done by borrowing host bits and using them as network bits. For example network address (192.168.1.0) and its subnet mask (255.255.255.0) as expressed in binary. Notice that the address bits that have corresponding mask bite set to 1 represents the network address. Address bits that have corresponding mask bits set to 0 represents the individual host address.

Network address	11000000	10101000	00000001	00000000
Subnet mask	11111111	11111111	11111111	00000000

With this address, the bits from octets 1, 2, and 3 are used to identify the network portion of the address. However, multiple subnets of network can be created by borrowing bits from the fourth octet. To do 30 bits from left to right are taken. In the following table, the bit with a value of 128 is borrowed.

Network address	11000000	10101000	00000001	00000000
Subnet mask	11111111	11111111	11111111	10000000

This changes the subnet mask from 255.255.255.0 to 255.255.255.128.

The more host bits are used for subnets, the more subnets are available. However, as more subnets are created, the less host addresses are available per subnet. In the following table, both the 128 and the 64 bit are borrowed. Only 6 bits are left for the host addresses, and the mask is now 255.255.255.192.

Network address	11000000	10101000	00000001	00000000
Subnet mask	11111111	11111111	11111111	11000000

Subnet Mask: A subnet mask is used to divide an IP address into two parts. One part identifies the host (computer); and the other part identifies the network to which it belongs.

It is called a subnet mask because it is used to identify network address of an IP address by performing bitwise AND operation on the Net mask.

Subnet Mask is the most recognizable aspect of subnetting. Similar to IP addresses, Subnet Mask consists four bytes (32 bits) and is often written using the same “dotted-decimal” notation. For example, a very common subnet mask in its binary representation:

11111111 11111111 11111111 00000000, is typically shown in the equivalent and in more readable form as given below
255.255.255.0

IP address has two component network and host address. Network address refers to the address of the network to which Host address refers to the host of that network.

e.g. IP address 192.168.7.21 has two parts

1. 192.168.7.0 -> refers network address
2. 0.0.0.21 -> refers host address

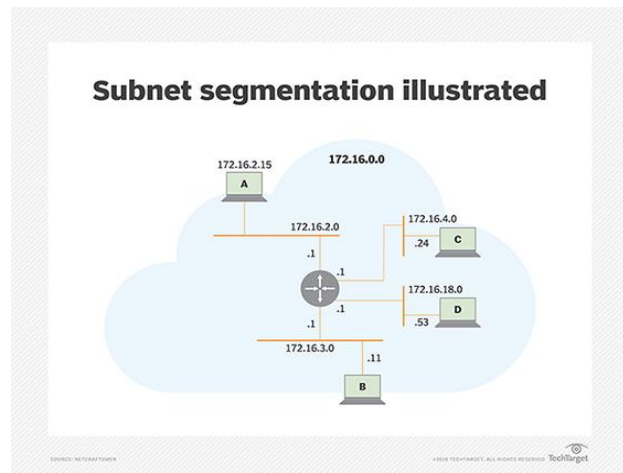
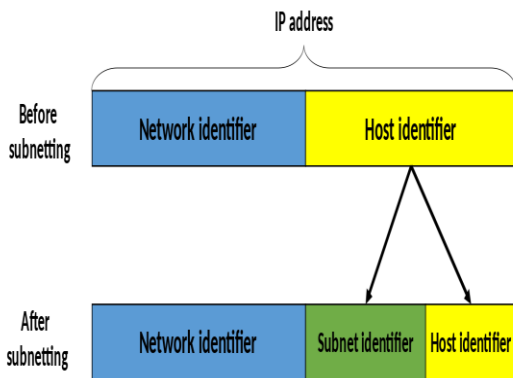
TCP/IP requires subnet mask to work. For example using a 255.255.255.0 subnet mask, which shows that the network ID is 192.168.7.0, and the host address is 0.0.0.21. When a packet arrives on the 192.168.7.0 subnet (from the local subnet or a remote network), having a destination address of 192.168.7.21, host computer will receive it from the network and process it.

IMP TIP: 00000000 00000000 00000000 00000000, is an Invalid subnet mask because the leftmost bit is set to ‘0’. ‘Conversely, the rightmost bits in a valid subnet mask must be set to ‘0’, not ‘1’. So: 11111111 11111111 11111111 11111111 is also invalid.

Mask	Binary (Fourth Field)	# Subnet bits	# Host bits	Subnets	Hosts
255.255.255.128	10000000	1	7	2	126
255.255.255.192	11000000	2	6	2	62
255.255.255.224	11100000	3	5	6	30
255.255.255.240	11110000	4	4	14	14
255.255.255.248	11111000	5	3	30	6
255.255.255.252	11111100	6	2	62	2

Class C masks

VIII. Diagrams / Experimental set-up /Work Situation



IX. Resources Required

Sr. No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB	10	
2..	Switch (min. 8 ports)	8 ports	1	

X. Procedure

Creating Subnet Mask

Step.1 Determine the network class (Suppose Class C) 192.168.7.0 falls in Class C range (192 - 223). The default Subnet Mask is 255.255.255.0, leaving the last octet available

Step. 2 Determine how many bits are needed to create subnets. For example calculate for 20 hosts using formula $2^x - 2$ where x represents the no of bits in host mask. Refer the table given above.

Step.3 From above table new assign 255.255.255.224 address for subnet mask.

Creating two Subnets

step 1 Borrow host bit from IP address (Example. 192.168.7.0) and use them as network bits.
 step.2 Create first subnet by borrowing one rightmost bit of host address as per below table.

Network address	192	168	7	0
	11000000	10101000	00000111	00000000
Subnet Mask	255	255	255	128
	11111111	11111111	11111111	10000000

Step. 3 Create second subnet by borrowing two rightmost bit of host address as per below table.

Network address	192	168	7	0
	11000000	10101000	00000111	00000000
Subnet Mask	255	255	255	192
	11111111	11111111	11111111	11000000

Step 4: Two subnets created are:

- 1.192.168.7.128
- 2.192.168.7.192

XI. Precaution

1. Handle Computer System and peripherals with care
2. Follow Safety Practices

XII. Resources Used

Sr. No	Name of Resource	Specification
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
2..	Switch (min. 8 ports)	8 ports
3.	Any otherResource	

XIII. Result

.....

XIV. Practical Related Questions

1. What is Subnet?
2. What is Subnet Mask?

.....

XVI. References/ Suggestions for further Reading

<https://www.pluralsight.com/blog/it-ops/simplify-routing-how-to-organize-your-network-into-smaller-subnets>

XVII. Assessment Scheme

Performance indicator		Weightage
Process Related(35 Marks)		75%
1.	Completion of given task	25%
2.	Correctness of given task	50%
Product Related(15 Marks)		25%
3.	Answer to sample Question	15%
4.	Submit Report in Time	10%
Total(50 Marks)		100%

❖ **List of Students/Team Members**

.....

Marks Obtained			Dated Signature of Teacher
Process Related(35)	Product Related (15)	Total(50)	

Practical No.15:Create IPv6 environment in a small network using simulator (preferably open source based)Part-I

I. Practical Significance

Knowthe use IPv6

Create IPv6 Environment

II. Relevant Programs Outcomes (POs)

- 1. Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
- 2. Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
- 3. Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
- 4. Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
- 5. Communication:**Communicate effectively in oral and written form.

III. Competency and Practical skills

1. Create IPv6 Environmentusing simulator

IV. Relevant Course Outcomes

Use Basic Concept of Networking for setting of Computer Network

Setup up computer Network for Specific Requirement

Configure Basic network Services

Configure TCP/IP services

V. Practical Outcomes (POs)

IPv6 environment

VI. Relevant Affective domain related Outcomes

1. Follow safety practices
2. Follow ethical practices

VII. Minimum Theoretical Background

IPv6 BASICS


WHAT YOU NEED TO KNOW

"IP" stand for Internet Protocol

It is a set of rules governing the format of data packets sent over the Internet or other network.

In Simple terms, an Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet.

Every device from Laptops, Smartphone, Tablets, E - readers, Cameras, Printer, iPad to PC's (or other networked device) which connects to the Internet is assigned a unique number called as its IP address.

Each device on the internet has an identity as an IP Address. 

NO. OF PEOPLE * NO OF SUCH DEVICES THAT MAY USE UNIQUE IP = RESULT IN UNIQUE IP ADDRESS REQUIRED.

- ✦ The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the Internet.
- ✦ Internet Protocol Version 6 (IPv6) is the successor to IPv4 
- ✦ IPv6 is designed to solve the problems of IPv4
- ✦ IPv6 provides far more IP addresses than IPv4.
- ✦ World IPv6 was launched on 6 June 2012 
- ✦ In format, IPv6 addresses are 128 bits long (4 times more address bits than IPv4) creating 3.4×10^{38} possible address (in trillion-trillion-trillion). This number of new IPv6 addresses will meet the internet demand for the expected future. 

IPv4

IPv6

Address range of IPv4:

32 bit = 232 addresses = 4.3 billion addresses

Address range of IPv6:

128 bit = 2128 addresses = 340 sextillion address

- ✦ IPv6 addresses use hexadecimal.
- ✦ Everyone gets public IPv6 addresses. There is no need for NAT.
- ✦ IPv6 networks are easier and cheaper to manage.
- ✦ IPv6 restores end-to-end transparency
- ✦ The smallest typical subnet of IPv6 is a /64 or 2^{64} addresses.
- ✦ Many Big international companies have already started to use IPv6:

INCLUDING



BENEFITS OF IPV6

- ⇨ IPv6 provides **larger IP address** space than IPv4.
- ⇨ It provides better security as it designed to ensure **end-to-end security** over a connection.
- ⇨ It has a built-in feature to support multicast. **With this multicast, bandwidth-intensive packets** can be sent to multiple locations simultaneously.
- ⇨ It reduces the need of **NAT (Network Address Translation)**
- ⇨ No **Geographical** Limitations
- ⇨ It enables **hierarchical** and efficient routing as it reduces the size of routing tables
- ⇨ Better Quality of **Service (QoS) in IPv6**
- ⇨ Network renumbering and assigning of new address schemes can be achieved automatically with **IPv6** providing administration easiness.
- ⇨ It provides ease to beginner users to connect their machines to the **network with plug and play**. It provides better support for real-time traffic such as **video conferencing**.

WHY YOUR BUSINESS NEEDS IPV6?

Business using IPv4 as their primary address are at risk of

Increased costs Limited website functionality Fail to penetrate emerging markets.

IPv6 For Business Benefits:

- ⇨ Prevent Increased Costs
- ⇨ Avoid Website Disruption
- ⇨ Improved Performance Provide Better Experience to Customers
- ⇨ Global Business Growth & Success
- ⇨ Maintain A Competitive Edge As Many Competitors Have Already Deployed Ipv6
- ⇨ Maintain Business Continuity



SOME QUICK STEPS

- ⇨ Test your existing internet connection and if it's not IPv6 then talk to your ISP (Internet Service Provider) about it.
- ⇨ Check if your office network is running on IPv6 or not. Contact your IT supplier if this is not so.
- ⇨ Check if your website is running on IPv6 or not. Take advice from your web hosting company.



Wavedirect.net

Internet Service Provider

FAST & RELIABLE INTERNET FOR EVERYONE

VIII. Diagrams / Experimental set-up /Work Situation

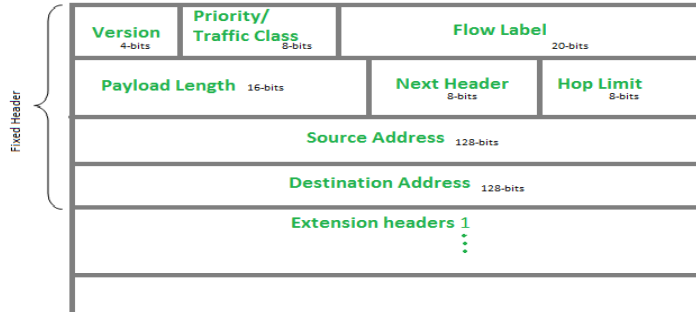


Fig. IPv6 Header

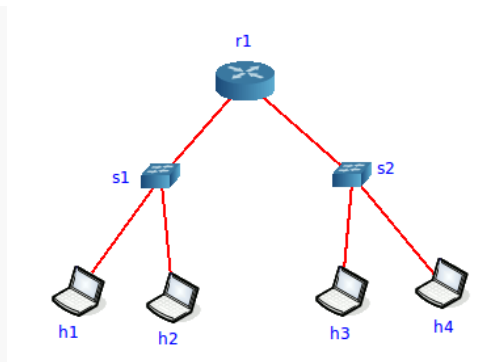
IX. Resources Required

Sr. No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB	10	
2.	Switch (min. 8 ports)	8 ports	2	
3.	Router			
4.	Linux OS			
5.	CORE Network Simulator			

X. Procedure

Set up the network configuration

Use the **CORE Network Simulator** to set up the network shown in the diagram below with one router, two switches, and four hosts. We will investigate IPv6 addressing fundamentals using this simple network.



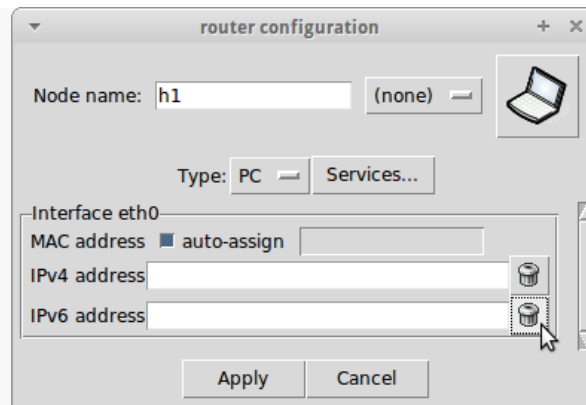
Simple IPv6 network

To make the network diagram easier to read, use the *View* → *Show* menu command to hide all information except node names (to clean up the display). Also, you can click on *Selection Tool* and grab the text that represents each node name and move it to a spot where it is not hidden by the link. Then, use

the *Configure* right-click menu command on each node to change the node name so that the network look like the following image:

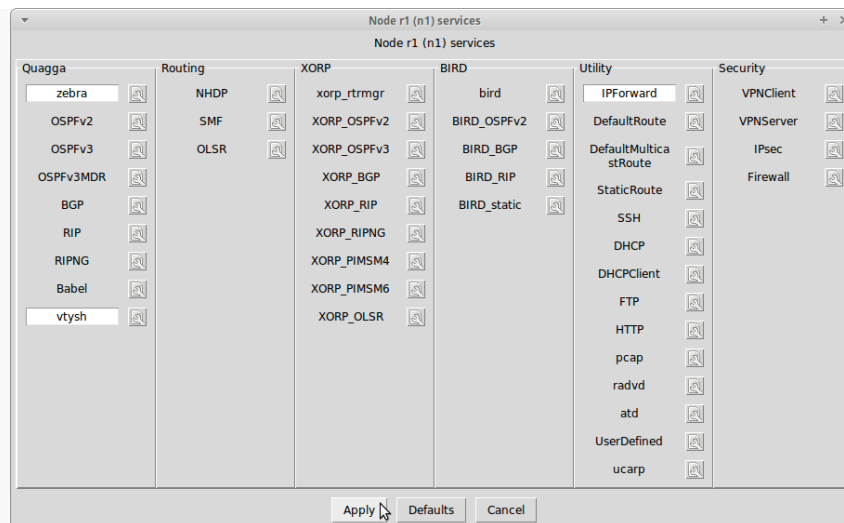
Configure the simulated nodes

We want to study the same procedures we would use in a real network without allowing the CORE Network Emulator to set the network configurations for us, so we will clear the IP addresses that the CORE Network Emulator configures by default on every interface before starting the simulation. Right-click on each router and host and select the *Configure* contextual menu command. Then, clear the IPv4 address and IPv6 address field on every node.



Delete IP addresses by clicking on the trash icon next to each field

Also, since we will not use dynamic routing in this scenario, we will change the settings on the router *r1* so that dynamic routing protocols are not started when the node starts up.



Clear dynamic routing protocol services from the router *r1*

In the *Configure* dialog box, after clearing the IP addresses on both of the router's interfaces, click on the *Services...* button, then clear the *OSPFv2* and *OSPFv3* services. Also clear the *radvd* service (because we will explore stateless address autoconfiguration in a later post). Then press the *Apply* button.

Start the simulation

Start the network emulation by clicking in the *start the session* icon in the tool bar or by clicking on the menu command, *Session* → *Start*.

Examine the link-local unicast IPv6 addresses

After we start the network simulation we created, we expect to observe that the interfaces on each simulated router and on each simulated host have link-local IPv6 addresses automatically configured. We will also run some simple network tests and observe the results. With the current configuration, nodes on the same link should be able to communicate with each other but nodes that are separated by the router should not be able to communicate with each other¹. For example, host *h1* should be able to ping host *h2*, but not host *h4*.

Link-local unicast IPv6 address, defined

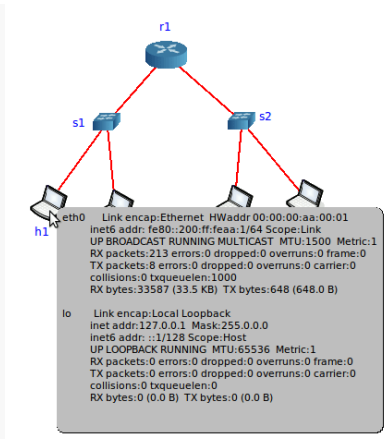
When an IPv6 interface starts up, it is required to automatically configure itself with a *link-local* unicast IPv6 address². Link-local IPv6 addresses consist of a specific 64-bit IPv6 prefix, `fe80::/64`, and a unique 64-bit *interface identifier* derived from the MAC address of the interface³.

Link-Local unicast IPv6 addresses are created for purposes such as auto-address configuration and neighbor discovery on a single link. A link may be a point-to-point connection between two interfaces or a switched layer-2 domain such as an Ethernet network.

Link-local unicast addresses only work on the link on which they are configured because IPv6 routers are required to not forward any packets with link-local source or destination addresses to other links.

Using the ifconfig Observer Widget

We can use the Core Network Emulator's *Observer Widget* tool to view the interface configuration on each node and take note of the IPv6 address on each interface. Click on the Observer Widget tool (the magnifying glass icon in the toolbar) and select the *ifconfig* widget. Then, hover the mouse pointer over each node to see the displayed interface configuration.



Using the *ifconfig* Observer Widget**Using the *ip* command**

Alternatively, we can open up a terminal window on each node running in the simulated network and use normal Linux commands to view the configuration.

Double-click on any node to open a terminal window (for example, host *h1*). Then, execute the command:

```
root@h1:~# ipaddr show
1: lo: mtu 65536 qdiscnoqueue state UNKNOWN
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
8: eth0: mtu 1500 qdiscpfifo_fast state UP qlen 1000
link/ether 00:00:00:aa:00:01 brdff:ff:ff:ff:ff:ff
   inet6 fe80::200:ff:feaa:1/64 scope link
valid_lft forever preferred_lft forever
```

Record all IPv6 addresses

Write down the IP addresses and MAC addresses on each node in a table for future reference. This will be useful when we are running programs like *ping* where we need to know the IPv6 address of the destination node. Knowing the MAC addresses is useful when we are analyzing packets in the *Wireshark* protocol analyzer.

In our example, the CORE Network Emulator assigns MAC addresses, in numerical order⁴, starting with 00:00:00:aa:00:00 and incrementing by one for every other interface attached to a link.

After inspecting each node using either the *Observer Widget* or the Linux *ip* command, we generate the following table:

Node name	Interface	MAC address	IPv6 addresses
Router <i>r1</i>	eth0	00:00:00:aa:00:00	fe80::200:ff:feaa:0/64
	eth1	00:00:00:aa:00:03	fe80::200:ff:feaa:3/64
Host <i>h1</i>	eth0	00:00:00:aa:00:01	fe80::200:ff:feaa:1/64

Host <i>h2</i>	eth0	00:00:00:aa:00:02	fe80::200:ff:feaa:2/64
Host <i>h3</i>	eth0	00:00:00:aa:00:04	fe80::200:ff:feaa:4/64
Host <i>h4</i>	eth0	00:00:00:aa:00:05	fe80::200:ff:feaa:5/64

Network tests with link-local addresses

Before we configure the network, let's see how the IPv6 network works in its initial state.

From host *h1*, ping host *h2*, the eth0 interface on router *r1*, and host *h4*.

Host *h1* interface eth0 to Host *h2* interface eth0

We see that Host *h1* can send and receive IPv6 data packets to and from Host *h2* using the *ping* command with the link-local IPv6 address. The interfaces of both hosts are on the same link.

```
root@h1:~# ping6 -c 1 -I eth0 fe80::200:ff:feaa:2
PING fe80::200:ff:feaa:2(fe80::200:ff:feaa:2) from fe80::200:ff:feaa:1 eth0: 56 data bytes
64 bytes from fe80::200:ff:feaa:2: icmp_seq=1 ttl=64 time=0.105 ms

--- fe80::200:ff:feaa:2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.105/0.105/0.105/0.000 ms
```

Note that we use the `-I eth0` option to indicate that the destination address is reachable through interface *eth0*. Link-local IPv6 addresses are not routable so the source system does not know which interface on which to send the *ping* packet. We need to specify the source interface when using link-local IPv6 addresses.

On a Linux system, the same command can be written with a “zone” suffix as:

```
$ ping6 fe80::200:ff:feaa:2%eth0
```

But the `-I eth0` option is supported the same way on most operating systems, while the “zone” suffix is not.

Host *h1* interface eth0 to Router *r1* interface eth0

We see that Host *h1* can send and receive IPv6 data packets to and from the *eth0* interface on Router *r1* using the *ping* command with the link-local IPv6 address. These interfaces are on the same link.

```
root@h1:~# ping6 -c 1 -I eth0 fe80::200:ff:feaa:0
PING fe80::200:ff:feaa:0(fe80::200:ff:feaa:0) from fe80::200:ff:feaa:1 eth0: 56 data bytes
64 bytes from fe80::200:ff:feaa:0: icmp_seq=1 ttl=64 time=0.335 ms
```

```
--- fe80::200:ff:feaa:0 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.335/0.335/0.335/0.000 ms
```

Host h1 interface eth0 to Host h4 interface eth0

We see that Host *h1* cannot send and receive IPv6 data packets to and from Host *h4*. These interfaces are on different links.

To reach Host *h4*, a data packet from Host *h1* must first arrive at the router's interface *eth0* and then be forwarded on to the router's interface *eth1* toward Host *h4*. By definition, the router is not allowed to do this because the source IPv6 address of the ICMP (ping6) packet is a link-local address.

```
root@h1:~# ping6 -c 1 -I eth0 fe80::200:ff:feaa:5  
PING fe80::200:ff:feaa:5(fe80::200:ff:feaa:5) from fe80::200:ff:feaa:1 eth0: 56 data bytes  
From fe80::200:ff:feaa:1icmp_seq=1 Destination unreachable: Address unreachable
```

```
--- fe80::200:ff:feaa:5 ping statistics ---  
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

```
root@h1:~#
```

Experiment with globally reachable unicast IPv6 addresses

With no additional configuration, devices on the same subnet can reach each other using IPv6 but in order for nodes on one subnet to communicate with nodes on another subnet and with nodes in other networks, a unique and reachable unicast IPv6 prefix must be assigned to each subnet.

The IPv6 protocol expects that more than one IPv6 address may be added to each interface. In this case, we already have a link-local address on each interface in the simulation and we will now add a globally unique reachable address to each interface.

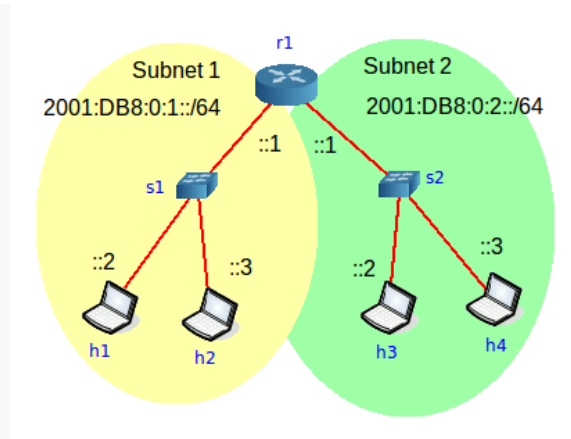
The documentation IPv6 prefix

The authorities that assign IPv6 addresses have thoughtfully reserved a special prefix for use in documentation and in examples like this one, so if we ever connect this simulation to a real IPv6 networks it will not cause any problems. The prefix allocated for documentation purposes is `2001:0DB8::/32`.⁵

So, in our example, we will assign the following prefixes to each subnet:

Subnet	Router Interface	Subnet prefix
Subnet 1	Router <i>r1</i> eth0	2001:DB8:0:1::/64
Subnet 2	Router <i>r1</i> eth1	2001:DB8:0:2::/64

We use the *Background Annotation Tools* (from the tool bar) to mark up the Core Network Emulator canvas so we have a visual reminder of the subnets and addresses we will use.



Marked up canvas showing subnets and prefix addresses

Manually configure global IPv6 addresses

Now, let's assign addresses to each interface. We do this manually because we imagine we're a network administrator who wants to configure addresses that are easy to remember and who wants the default router interfaces on a subnet to end in "1", as some network admins would, in an IPv4 network. So, we do not use stateless autoconfiguration of IPv6 addresses in this example (we'll discuss it in a later post). On each host and router, enter the commands as follows to manually configure a global IPv6 address on each interface. Each host also needs a default route configured:

```
root@r1:~# ip -6 addr add 2001:DB8:0:1::1/64 dev eth0
```

```
root@r1:~# ip -6 addr add 2001:DB8:0:2::1/64 dev eth1
```

```
root@h1:~# ip -6 addr add 2001:DB8:0:1::100/64 dev eth0
```

```
root@h1:~# ip -6 route add ::/0 via 2001:db8:0:1::1 dev eth0
```

```
root@h2:~# ip -6 addr add 2001:DB8:0:1::101/64 dev eth0
```

```
root@h2:~# ip -6 route add ::/0 via 2001:db8:0:1::1 dev eth0
```

```
root@h3:~# ip -6 addr add 2001:DB8:0:2::100/64 dev eth0
```

```
root@h3:~# ip -6 route add ::/0 via 2001:db8:0:2::1 dev eth0
```

```
root@h4:~# ip -6 addr add 2001:DB8:0:2::101/64 dev eth0
```

```
root@h4:~# ip -6 route add ::/0 via 2001:db8:0:2::1 dev eth0
```

After manually configuring the IPv6 interface addresses, we can inspect each interface using the `ipaddr show` command (or Core Network Emulator's *Observer Widget* tool) and see that the IPv6 addresses are configured on each interface and we see that the prefixes `2001:DB8:0:1::/64` and `2001:DB8:0:2::/64` have a *global* scope (as opposed to a *link* scope). For example, on router *r1*:

```
root@r1:~# ip -6 addr show
1: lo: mtu 65536
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
6: eth0: mtu 1500 qlen 1000
   inet6 2001:db8:0:1::1/64 scope global
valid_lft forever preferred_lft forever
   inet6 fe80::200:ff:feaa:0/64 scope link
valid_lft forever preferred_lft forever
12: eth1: mtu 1500 qlen 1000
   inet6 2001:db8:0:2::1/64 scope global
valid_lft forever preferred_lft forever
   inet6 fe80::200:ff:feaa:3/64 scope link
valid_lft forever preferred_lft forever
root@r1:~#
```

Network tests with global addresses

We verify that all addresses are configured according to our address plan. We see each interface now has a *link local* IPv6 address and a *global* IPv6 address.

Node name	Interface	MAC address	IPv6 addresses
Router <i>r1</i>	eth0	00:00:00:aa:00:00	fe80::200:ff:feaa:0/64 2001:DB8:0:1::1/64
	eth1	00:00:00:aa:00:03	fe80::200:ff:feaa:3/64 2001:DB8:0:2::1/64

Host <i>h1</i>	eth0	00:00:00:aa:00:01	fe80::200:ff:feaa:1/64 2001:DB8:0:1::100/64
Host <i>h2</i>	eth0	00:00:00:aa:00:02	fe80::200:ff:feaa:2/64 2001:DB8:0:1::101/64
Host <i>h3</i>	eth0	00:00:00:aa:00:04	fe80::200:ff:feaa:4/64 2001:DB8:0:2::100/64
Host <i>h4</i>	eth0	00:00:00:aa:00:05	fe80::200:ff:feaa:5/64 2001:DB8:0:2::101/64

Host h1 to Host h3

Because packets with global address prefixes in the source and destination address fields can be forwarded by a router, we expect that a node in Subnet 1 should be able to communicate with a Node in Subnet 2 (because both subnets are directly connected to the router). We test that using the *ping6* command to test if Host *h1* can reach host *h3*:

```
root@h1:~# ping6 -c 1 2001:DB8:0:2::100
PING 2001:DB8:0:2::100(2001:db8:0:2::100) 56 data bytes
64 bytes from 2001:db8:0:2::100: icmp_seq=1 ttl=63 time=0.280 ms

--- 2001:DB8:0:2::100 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.280/0.280/0.280/0.000 ms
root@h1:~#
```

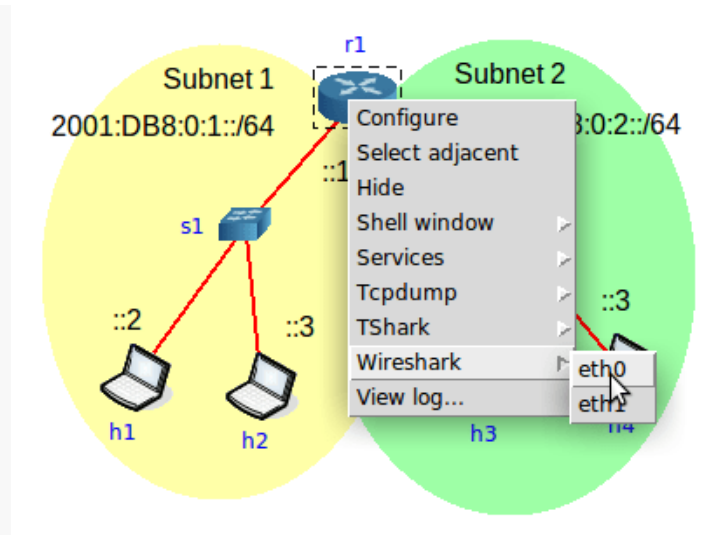
Note that we no longer need to specify the source interface when using global addresses because there is no ambiguity about to which subnet a global prefix is associated.

Inspect IPv6 packets

We will use the Wireshark packet analyzer to capture and view IPv6 packets on the interfaces of router *r1*. This will give us some insight into how the IPv6 protocol resolves addresses in a local subnet and between two subnets.

Start Wireshark

First we start Wireshark using the contextual menu in the CORE Network Emulator. Right-click on router *r1* and select *Wireshark* and then *eth0*. Repeat the process and also select *eth1*.



Start Wireshark on both router interfaces, *eth0* and *eth1*

Now we should see two Wireshark windows open, each one displaying data on a different interface.

SSH session between two nodes on same link

Now, start a connection within subnet 1, between host *h1* and the *eth0* interface on router *r1*. For this example, we will start an SSH session between *h1* and *r1*.

First, we need to enable the SSH server daemon on the router *r1* with the command:

```
root@r1:~# /etc/init.d/ssh start
```

Then, on host *h1*, start the SSH session to *r1*. Since each node is linux container, use your own userid (in my case it is *brianl*) and your user password to access the remote node because Xubuntu will not allow you access to the *root* user on the Linux container.

```
root@h1:~# ssh brianl@2001:DB8:0:1::1
```

```
brianl@2001:db8:0:1::1's password:
```

```
Welcome to Ubuntu 13.10 (GNU/Linux 3.11.0-19-generic x86_64)
```

```
* Documentation: https://help.ubuntu.com/
```

```
0 packages can be updated.
```

```
0 updates are security updates.
```

```
brianl@r1:~$ ls
```

```
Desktop Downloads Music Public Videos
```

```
Documents Dropbox Pictures Templates
```

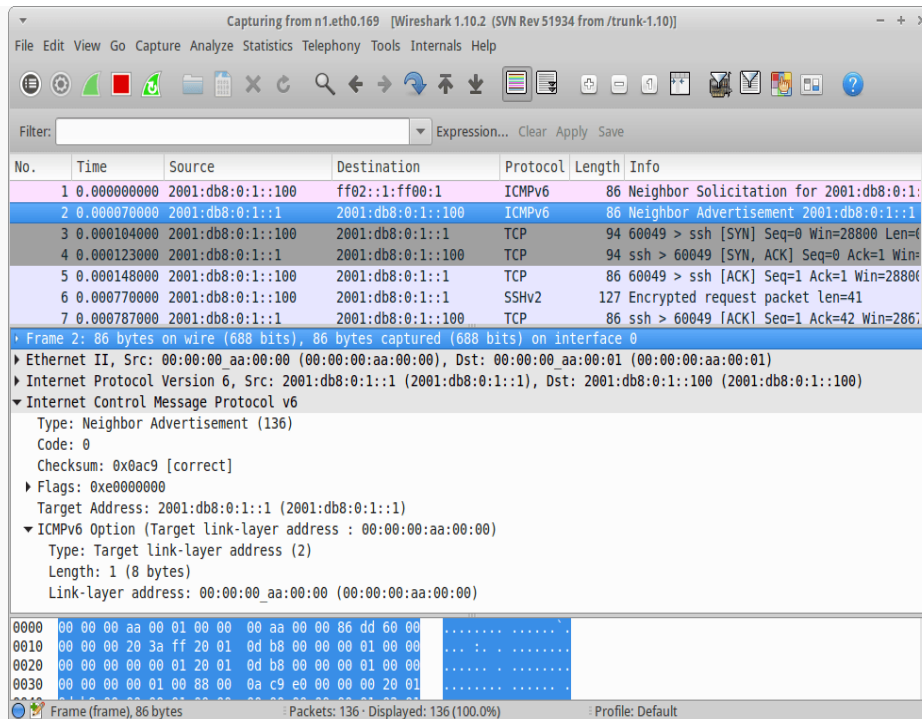
```
brianl@r1:~$ exit
```

```
logout
```

```
Connection to 2001:DB8:0:1::1 closed.
```

```
root@h1:~#
```

Looking at the Wireshark window on *r1* interface *eth0*, we see some new destination addresses (these are multicast addresses used by the Neighbor Discovery Protocol) and we see the two systems communicate to match the MAC address of router *r1*'s interface *eth0* with the destination IPv6 address.



Captured packets on Router *r1* interface *eth0*

We'll cover more about the Neighbor Discovery Protocol, which in this case operates like the IPv4 ARP protocol, in a future post.

SSH session between two nodes on different links

Next, we'll open an SSH session that passes between the two subnets, from host *h1* to host *h4*.

We need to enable the SSH server on host *h4*, first:

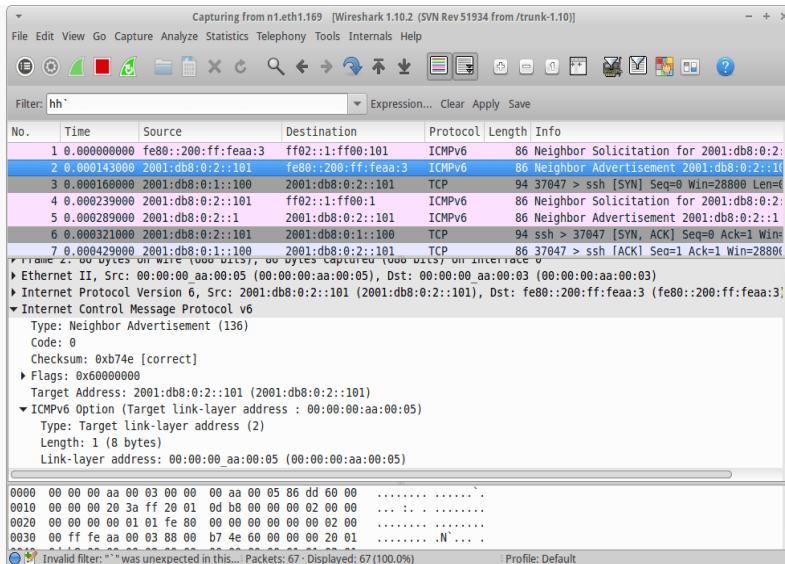
```
root@h4:~# /etc/init.d/ssh start
```

Then, we start the SSH session from host *h1* to host *h4*:

```
root@h1:~# ssh brianl@2001:DB8:0:2::101
```

```
brianl@2001:db8:0:2::101's password:
```

Looking at the Wireshark window that is capturing traffic on *r1* interface *eth1*, we see that the Neighbor Discovery Protocol uses both multicast addresses and the link local addresses as part of the process to resolve the destination MAC address with the destination IPv6 address.



Captured packets on Router *r1* interface *eth1*

Again, we’ll discuss the neighbor discovery process more in another post.

Finish and clean up

We end the simulation and save the configuration. Click on the red *Stop the session* button on the tool bar or use the menu command:

Session → Stop

Then save the configuration using the menu command:

File → Save

XI. Precaution

3. Handle Computer System and peripherals with care
4. Follow Safety Practices

XII. Resources Used

Sr. No	Name of Resource	Specification
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
2.	Switch (min. 8 ports)	8 ports
3.	Any other Resources	
4.		
5.		

XIII. Result

.....
.....
.....

XIV. Practical Related Questions

1. Differentiate between IPv4 and IPv6
2. Explain IPv6 Packet Format

XV. Exercise

Student should setup IPv6 Environment using Simulator

(Space for Answer)

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

.....

XVI. References/ Suggestions for further Reading

<https://getipv6.info/display/IPv6/Educating+Yourself+about+IPv6>

<http://www.brianlinkletter.com/tag/core/>

XVII. Assessment Scheme

Performance indicator		Weightage
Process Related(35 Marks)		75%
1.	Completion of given task	25%
2.	Correctness of given task	50%
Product Related(15 Marks)		25%
3.	Answer to sample Question	15%
4.	Submit Report in Time	10%
Total(50 Marks)		100%

❖ **List of Students/Team Members**

.....

Marks Obtained			Dated Signature of Teacher
Process Related(35)	Product Related (15)	Total(50)	

Practical No.16: Create IPv6 environment in a small network using simulator (preferably open source based) Part-II

I. Practical Significance

Know the use of IPv6

Create IPv6 Environment

II. Relevant Programs Outcomes (POs)

- 1. Basic knowledge:** Apply knowledge of basic mathematics, sciences and basic engineering to solve the broad-based Information Technology problems.
- 2. Discipline knowledge:** Apply Information Technology knowledge to solve Information Technology related problems.
- 3. Experiments and practice:** Plan to perform experiments and practices to use the results to solve broad-based Information Technology problems.
- 4. Engineering tools:** Apply relevant Information Technologies and tools with an understanding of the limitations.
- 5. Communication:** Communicate effectively in oral and written form.

III. Competency and Practical skills

1. Create IPv6 Environment using simulator

IV. Relevant Course Outcomes

Use Basic Concept of Networking for setting of Computer Network
Setup up computer Network for Specific Requirement

V. Practical Outcomes (POs)

Create IPv6 Environment using simulator

VI. Relevant Affective domain related Outcomes

1. Follow safety practices
2. Follow ethical practices

VII. Minimum Theoretical Background

VIII. Diagrams / Experimental set-up /Work Situation

IX. Resources Required

Sr. No	Name of Resource	Specification	Quantity	Remarks/Use
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB	10	
2.	Switch (min. 8 ports)	8 ports	1	

X. Procedure

In [Part 1 of this series](#), we performed some practical experiments to show how interfaces in an IPv6 network configure themselves with link-local IPv6 addresses when they start up. We also showed how to manually configure IPv6 addresses on a Linux system. In this post, we will use an open-source network simulator to demonstrate another method of assigning an IPv6 address to an interface: [Stateless Address Auto-configuration \(SLAAC\)](#).

We will use the [CORE Network Emulator](#) to set up a simple IPv6 network and then run some practical exercises to show how to set up a open-source IPv6 router to perform auto-configuration using either *radvd* or *quagga*. We'll use open-source routing software to demonstrate real router configuration procedures and investigate how IPv6 routers and hosts communicate to assign globally unique unicast IPv6 addresses to hosts the using Stateless Address Auto-configuration and the [Neighbor Discovery Protocol \(NDP\)](#).

Stateless Address Auto-configuration

Stateless Address Auto-configuration (SLAAC) is an IPv6 function that simplifies network administration¹. SLAAC is the preferred way to assign IPv6 addresses on hosts in an IPv6 network. To enable auto-configuration, the network administrator manually enters in the router's configuration file the prefixes that routers will advertise to the hosts on each link. Then, the router advertises that prefix to all hosts on the link via the Neighbor Discovery Protocol.

Host Interface ID

The hosts use a combination of the IPv6 network prefix learned from the router and their own interface MAC address to create a unique IPv6 address.

Router Interface ID

Routers do not allow their interface addresses to be auto-configured². The network administrator must manually configure IPv6 addresses on each router interface.

Default Routes on Hosts

Each host uses the Neighbor Discovery Protocol to learn about all routers attached to the same link and automatically configure default routes to the advertising routers.

When using IPv6, hosts may have multiple default routes to different routers on the same link, which may provide for more efficient routing to different destinations.

Router Advertisement Daemon (radvd)

The Router Advertisement Daemon (radvd) is open-source software that implements stateless address auto-configuration using the Neighbor Discovery Protocol (NDP). It listens for messages from hosts requesting prefix information and periodically sends out advertisement messages describing information about the router to all hosts on the link.

Default configurations and file locations

To realistically emulate SLAAC configuration procedures on a simulated Linux IPv6 router, we need to use the built-in functions of the CORE Network Emulator and some undocumented information about the virtual node configuration files.

CORE uses LXC Network Namespaces to implement virtual nodes in the simulation. The CORE GUI hides from the user the complexities involved in starting routing daemons on Linux containers using network namespaces (which is what the designers intended). To show how we would configure a router using Linux commands we will modify the configuration procedures that take into account the way CORE virtualizes nodes and starts services on the virtual nodes.

Each node in the simulation consists of a lightweight virtual machine that only isolates the network stack and a few selected files. Because the rest of the filesystem is shared between all the virtual nodes and the host Linux system, we need to know which files on the simulated nodes we can modify and which we should not. The configuration files will be in non-standard locations on the simulated nodes and, unfortunately, this is not well documented. It is better to use only Linux configuration commands and leave configuration files and startup scripts alone.

Set up the network topology

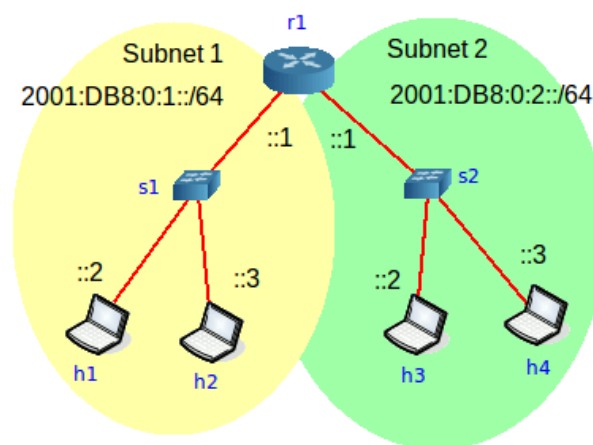
Start the CORE Network Emulator with the following commands:

```
$ sudo /etc/init.d/core-daemon start
```

```
$ core-gui
```

Load a network configuration file

We will use the same network configuration that we created and saved in [Part 1 of this series](#). Open the *.*imn* file you saved. In my case, I named it *IPv6-addresses.imn*.



Simulated IPv6 network topology

Configure the network initial state

If we allow it to, the CORE Network Emulator will set up IP addresses, generate the contents of configuration files, and start daemons for us. However, in a case where we wish to practise using the Linux command-line to configure each virtual node, we need to change the CORE default settings before we start the simulation.

Complete the following steps to set up the network scenario so that we can use (mostly) realistic command-line procedures to configure the nodes in the simulated network.

Determine the services we will use on each node

To keep things simple, we will start only the services we need on each node.

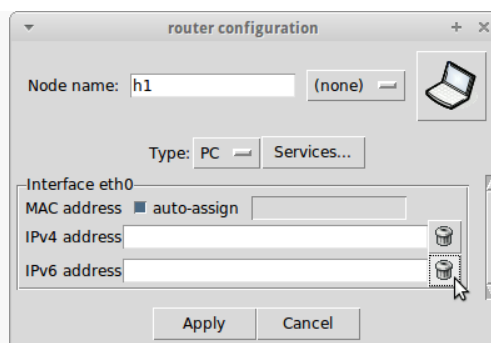
On router *r1*, we need only two services: *IPForward* and *radvd*.

On each host, *h1* to *h4*, we do not need any services configured. Even the *DefaultRoute* service can be cleared because it is only useful if we configure a static IP address using the CORE GUI, and we won't do that in this case.

Verify that no IP addresses are assigned in the CORE Network Emulator

IP addresses should not be configured on any of the interfaces because we want to configure these using Linux commands on each simulated node after starting the simulation. Since we are using a saved network scenario from [Part 1 of this series](#), where we already cleared the IP addresses, we should already have the correct configuration. But, it never hurts to check.

Right-click on each node and select *Configure* from the drop-down menu. In the configuration window, ensure every IP address field is blank. If not, clear them by clicking on the trash icon next to the field and then click *Apply*.

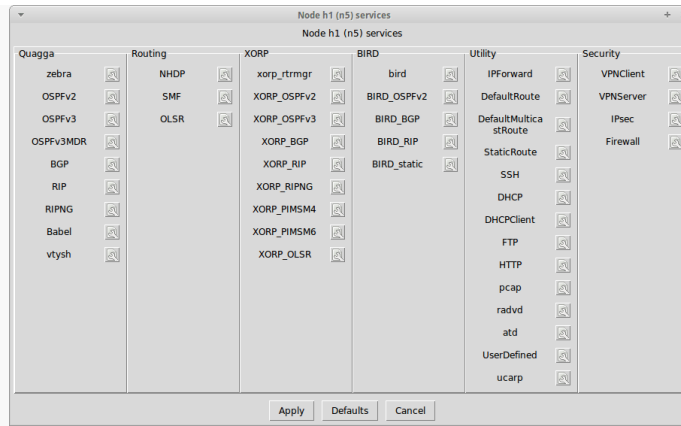


Delete IP addresses by clicking on the trash icon next to each field

Clear all services on each host, h1 to h4

Right-click on each host node in the CORE canvas and select *Services...*

Then, clear all services on the host nodes so that nothing is selected. Click on *Apply* to save the changes.

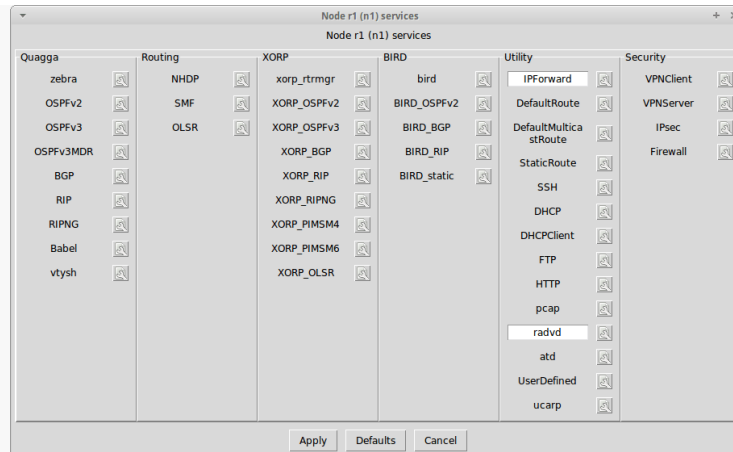


Clear all services on each host node

Enable the radvd service on the router r1

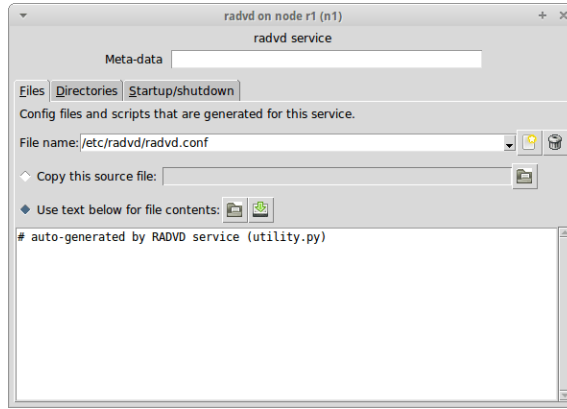
We need to enable *radvd* so we can manage it after we start the scenario in the CORE Network Emulator, but we do not want CORE to create a *radvd* configuration file for us. Because we ensured no IP addresses were assigned in CORE in Step 1 above, CORE will not automatically generate the contents of the *radvd.conf*.

Right-click on router *r1*, then select *Services* from the drop-down menu. Clear all services so that none are selected. Then, click on the *radvd* service to enable it.



Enable only the *radvd* service in IPv6 router

Next, click on the small “tool” icon next to *radvd* in the *Services* window. This will open the *radvd* configuration window. You don’t change anything in this window. Confirm that the *radvd.conf* file that CORE will generate on router *r1* is empty. Also note that CORE will create the file in a non-standard location: */etc/radvd/radvd.conf*. This is because CORE creates a mount namespace for the new file */etc/radvd/radvd.conf* so it does not affect the host computer’s configuration of the configurations of other nodes in the simulation. (Remember: all virtual nodes share the same filesystem, except where specific folders are provided with their own *mount namespace* by CORE Services scripts).



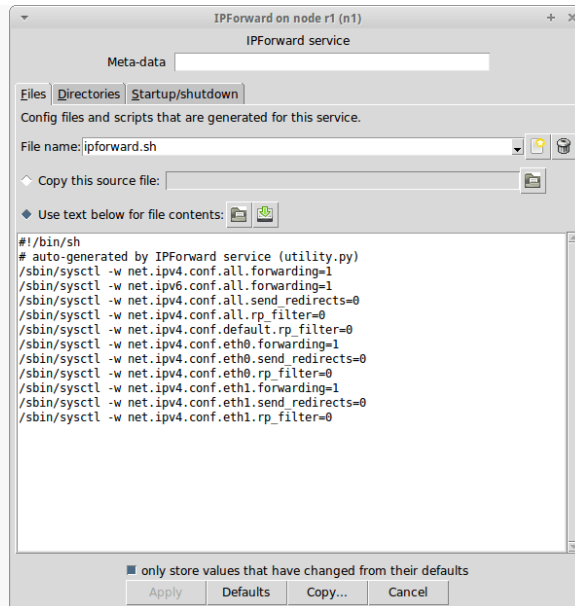
Check *radvd.conf* contents and location

Close the *radvd* window. Then, click *Apply* on the *Services* window.

Verify the IPForward service configuration on router r1

When starting a simulation scenario, the CORE Network Emulator executes commands on the router that configure Linux kernel parameters to enable IP Forwarding. It does not update the */etc/sysctl.conf* file because that file is not isolated to the simulated node.

Click on the “tool” icon next to the *IPForward* service. This will open the *IPForward* service configuration window. You can see the kernel parameters that will be set by this service. The CORE Network Emulator will execute the script shown when the router is started. We see the IP Forwarding configurations will enable IPv4 and IPv6 forwarding. (These configurations can be changed in this window and then saved, if you want the router to start with a different set of parameters.)



Details of the *IPForward* service configuration

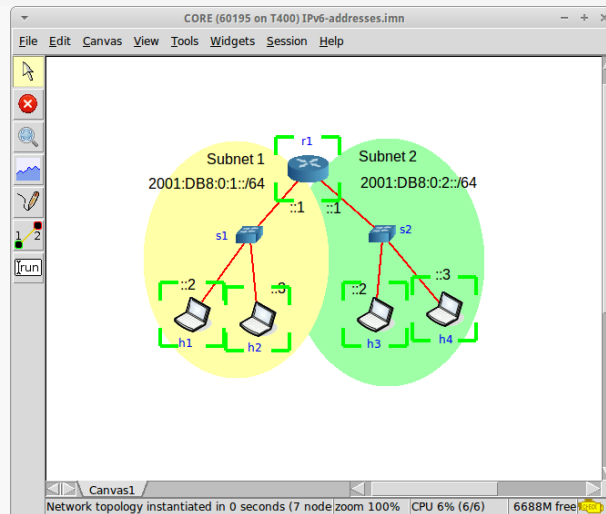
On the simulated router, after it is running in the simulation, you can verify the IP Forwarding parameter values with the following command³:

```
root@r1:~# sysctl -a | grep forwarding
```

Run the simulation

Start the simulation by clicking on the green *start the session* icon in the CORE toolbar or use the menu command:

Session → Start



CORE simulation starting up

Configure the simulated IPv6 router

Double-click on the router *r1* in the canvas. This will open a terminal window on *r1*.

The radvd.conf configuration file

First we create the configuration file. On this simulated Linux router, the *radvd* service expects the configuration file is `/etc/radvd/radvd.conf`.

```
root@r1:~# vi /etc/radvd/radvd.conf
```

Enter the following text to configure the prefixes we have chosen to use on each link. These are the same prefixes we used in [Part 1 of this series](#).

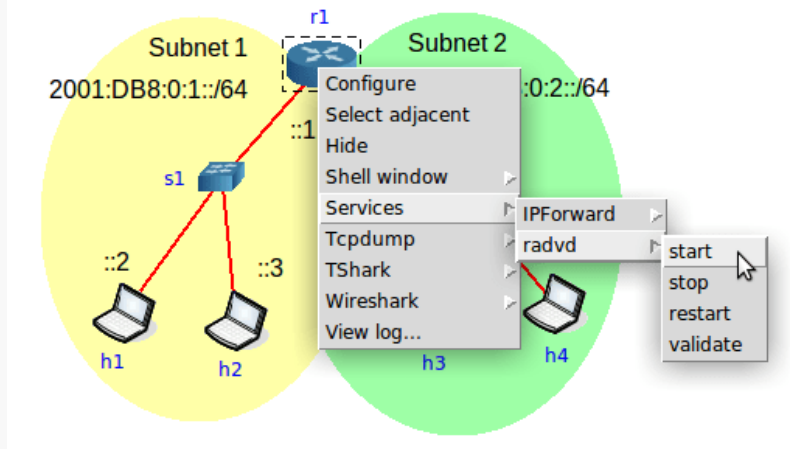
```
interface eth0
{
AdvSendAdvert on;
prefix 2001:db8:0:1::/64 { };
};
interface eth1
{
AdvSendAdvert on;
prefix 2001:db8:0:2::/64 { };
};
```

};

There are other *radvd* configurations that can be entered in this file but we'll just keep it simple for now. Unless they are explicitly configured, all other *radvd* parameters use their default values.

Start radvd

Now, start the *radvd* service⁴. Right-click on the router *r1* and select the following menu command from the contextual menu:



Start *radvd* service on *r1*

This starts the *radvd* daemon. You can verify this by checking the processes running on *r1* with the `ps -ef` command:

```
root@r1:~# ps -ef
UID    PID  PPID  C  STIME TTY      TIME CMD
root     1    0  0  23:38 ?        00:00:00 /usr/local/sbin/vnoded -v -c /tm
root    52    1  0  23:38 ?        00:00:00 /usr/lib/quagga/zebra -u root -g
root   126    1  0  23:57 pts/7    00:00:00 /bin/bash
root   191    1  0  23:58 ?        00:00:00 radvd -C /etc/radvd/radvd.conf -
root   193    1  0  23:58 ?        00:00:00 radvd -C /etc/radvd/radvd.conf -
root   195   126  0  23:58 pts/7    00:00:00 ps -ef
root@r1:~#
```

If *radvd* does not start, it is probably due to a syntax error in the configuration file.

Check IP assigned addresses

After starting *radvd*, we should see that the hosts have automatically configured IPv6 addresses using the prefixes we configured on the router.

We can verify this using the CORE Network Emulator's *Observer Widget* tool or by entering the `ip -6 addr show` command on each simulated node's terminal window. For example, on host *h1*, we see the link-local address with the link-local prefix `fe80::/64` and a global unique address using the prefix advertised by the router `2001:db8:0:1::/64`:

```
root@h1:~# ip -6 addr show
1: lo: mtu 65536
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
50: eth0: mtu 1500 qlen 1000
    inet6 2001:db8:0:1:200:ff:feaa:1/64 scope global dynamic
valid_lft 86400sec preferred_lft 14400sec
    inet6 fe80::200:ff:feaa:1/64 scope link
valid_lft forever preferred_lft forever
root@h1:~#
```

Checking the *r1*, we see that only the IPv6 link-local address is assigned, as expected. We need to manually assign IP addresses on routers.

```
root@r1:~# ip -6 addr show
1: lo: mtu 65536
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
48: eth0: mtu 1500 qlen 1000
    inet6 fe80::200:ff:feaa:0/64 scope link
valid_lft forever preferred_lft forever
54: eth1: mtu 1500 qlen 1000
    inet6 fe80::200:ff:feaa:3/64 scope link
valid_lft forever preferred_lft forever
root@r1:~#
```

Router interface IP addresses

Stateless Address Auto-configuration will not assign an interface ID to the router's interfaces — neither to the router's own interfaces nor to interfaces on another router connected to the same IPv6 link. We need to assign IPv6 addresses on the router interfaces with the following commands:

```
root@h1:~# ip -6 addr add 2001:DB8:0:1::1/64 dev eth0
root@h1:~# ip -6 addr add 2001:DB8:0:2::1/64 dev eth1
```

We can verify the addresses are assigned using the `ip -6 addr show` command.

```
root@r1:~# ip -6 addr show
1: lo: mtu 65536
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
48: eth0: mtu 1500 qlen 1000
    inet6 2001:db8:0:1::1/64 scope global
valid_lft forever preferred_lft forever
    inet6 fe80::200:ff:feaa:0/64 scope link
valid_lft forever preferred_lft forever
54: eth1: mtu 1500 qlen 1000
    inet6 2001:db8:0:2::1/64 scope global
valid_lft forever preferred_lft forever
    inet6 fe80::200:ff:feaa:3/64 scope link
valid_lft forever preferred_lft forever
root@r1:~#
```

Network experiments

Now we can run some tests to see how stateless address auto-configuration and *radvd* works.

First, we will make a note of the IPv6 addresses assigned to each interface. Check the IPv6 addresses on each node with the `ip -6 addr show` command and write them down. In this case, the IPv6 addresses on each interface are listed in the table below:

Node name	Interface	MAC address	IPv6 addresses
Router <i>r1</i>	eth0	00:00:00:aa:00:00	fe80::200:ff:feaa:0/64 2001:DB8:0:1::1/64
	eth1	00:00:00:aa:00:03	fe80::200:ff:feaa:3/64 2001:DB8:0:2::1/64
Host <i>h1</i>	eth0	00:00:00:aa:00:01	fe80::200:ff:feaa:1/64 2001:DB8:0:1:200:ff:feaa:1/64

Host <i>h2</i>	eth0	00:00:00:aa:00:02	fe80::200:ff:feaa:2/64 2001:DB8:0:1:200:ff:feaa:2/64
Host <i>h3</i>	eth0	00:00:00:aa:00:04	fe80::200:ff:feaa:4/64 2001:DB8:0:2:200:ff:feaa:4/64
Host <i>h4</i>	eth0	00:00:00:aa:00:05	fe80::200:ff:feaa:5/64 2001:DB8:0:2:200:ff:feaa:5/64

Communication tests

Now, let's verify that nodes can communicate with each other using the assigned IPv6 configurations.

We can test this using the *ping6* command.

For example, we ping from host *h1* to host *h4*:

```
root@h1:~# ping6 2001:DB8:0:2:200:ff:feaa:5
PING 2001:DB8:0:2:200:ff:feaa:5(2001:db8:0:2:200:ff:feaa:5) 56 data bytes
64 bytes from 2001:db8:0:2:200:ff:feaa:5: icmp_seq=1 ttl=63 time=0.212 ms
64 bytes from 2001:db8:0:2:200:ff:feaa:5: icmp_seq=2 ttl=63 time=0.171 ms
64 bytes from 2001:db8:0:2:200:ff:feaa:5: icmp_seq=3 ttl=63 time=0.170 ms
64 bytes from 2001:db8:0:2:200:ff:feaa:5: icmp_seq=4 ttl=63 time=0.169 ms
^C
--- 2001:DB8:0:2:200:ff:feaa:5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.169/0.180/0.212/0.022 ms
root@h1:~#
```

Inspect configuration information

Now, let's have a look at the information on the hosts' interfaces. Here we see the configurations that *radvd* makes on the host.

For example, a default address is automatically configured using information provided to the host about the router running *radvd*. We can see this by entering the command:

```
root@h1:~# ip -6 route show
2001:db8:0:1::/64 dev eth0 proto kernel metric 256 expires 86205sec
fe80::/64 dev eth0 proto kernel metric 256
default via fe80::200:ff:feaa:0 dev eth0 proto ra metric 1024 expires 1605sec
root@h1:~#
```

Here we see the default route is via the address `fe80::200:ff:feaa:0`, which is the link-local address of router *r1*. We also see some other information about the route.

Next, we look at the IPv6 addresses configured on the hosts, such as *h1*:

```
root@h1:~# ip -6 addr show
1: lo: mtu 65536
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
50: eth0: mtu 1500 qlen 1000
    inet6 2001:db8:0:1:200:ff:feaa:1/64 scope global dynamic
valid_lft 85979sec preferred_lft 13979sec
    inet6 fe80::200:ff:feaa:1/64 scope link
valid_lft forever preferred_lft forever
root@h1:~#
```

Compare these address configurations to the static addresses configured on the router. We see that the automatically-configured addresses on the hosts have a expiration timers set (valid for 85,979 more seconds and preferred for 13,797 more seconds, in the example above) but the manually configured static IPv6 addresses have no expiration time set (they will remain valid “forever”):

```
root@r1:~# ip -6 addr show
1: lo: mtu 65536
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
48: eth0: mtu 1500 qlen 1000
    inet6 2001:db8:0:1::1/64 scope global
valid_lft forever preferred_lft forever
    inet6 fe80::200:ff:feaa:0/64 scope link
valid_lft forever preferred_lft forever
54: eth1: mtu 1500 qlen 1000
    inet6 2001:db8:0:2::1/64 scope global
valid_lft forever preferred_lft forever
    inet6 fe80::200:ff:feaa:3/64 scope link
valid_lft forever preferred_lft forever
root@r1:~#
```

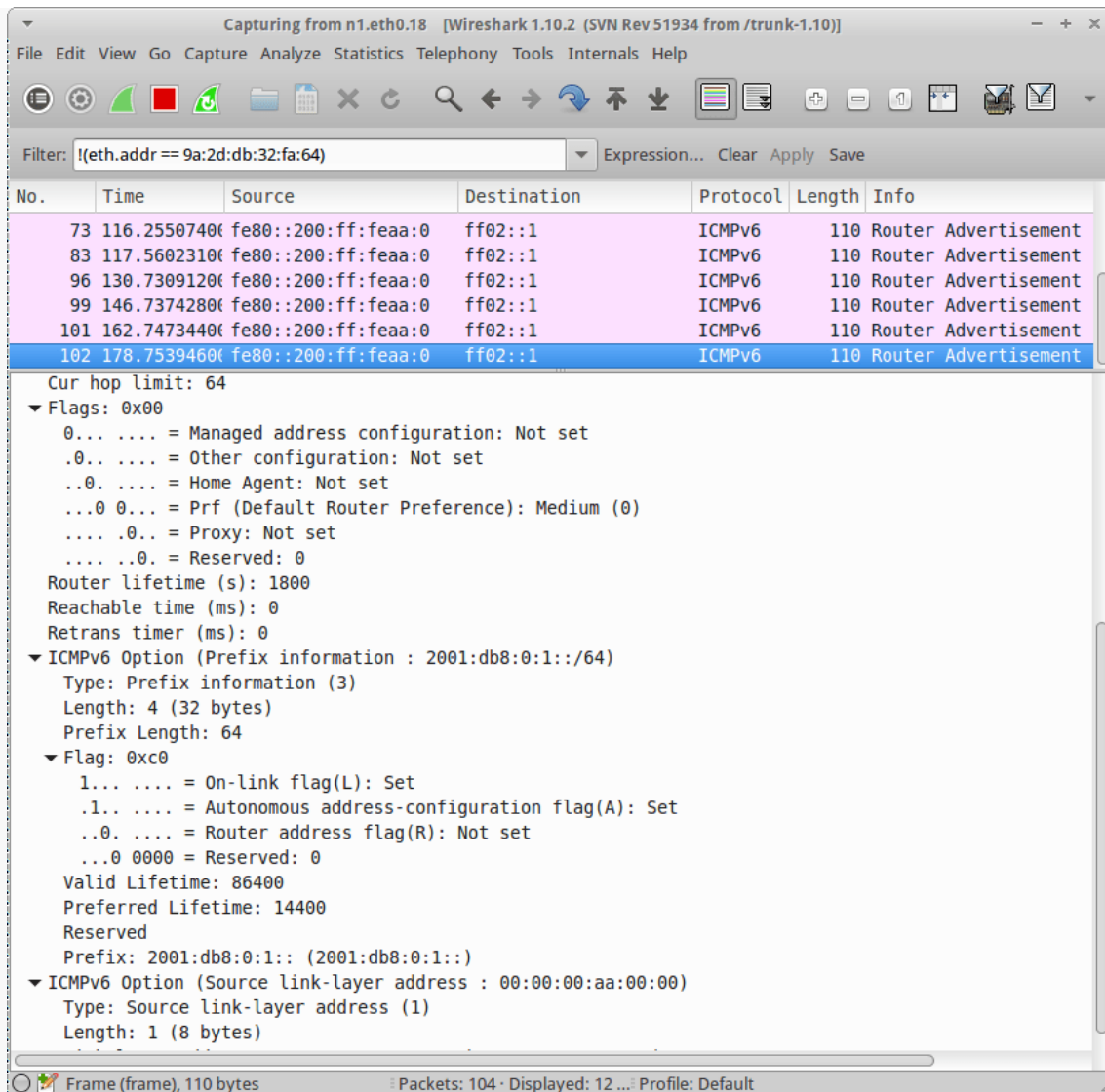
Stop the *radvd* service on the router *r1* (use the CORE contextual menu command). We should see that the timers of the automatically-configure IPv6 addresses on the hosts now keep counting down to zero (if we wanted to wait that long), because they no longer periodically receive *Router Advertisement* messages with new timer information.

Inspect the auto-configuration protocol messages

Start Wireshark on router *r1* interface *eth0*.

Start the *radvd* service again.

Look at the *Router Advertisement* messages sent from the router to the hosts. You can see the default parameters used by *radvd* in each message.



No.	Time	Source	Destination	Protocol	Length	Info
73	116.25507400	fe80::200:ff:feaa:0	ff02::1	ICMPv6	110	Router Advertisement
83	117.56023100	fe80::200:ff:feaa:0	ff02::1	ICMPv6	110	Router Advertisement
96	130.73091200	fe80::200:ff:feaa:0	ff02::1	ICMPv6	110	Router Advertisement
99	146.73742800	fe80::200:ff:feaa:0	ff02::1	ICMPv6	110	Router Advertisement
101	162.74734400	fe80::200:ff:feaa:0	ff02::1	ICMPv6	110	Router Advertisement
102	178.75394600	fe80::200:ff:feaa:0	ff02::1	ICMPv6	110	Router Advertisement

```

Cur hop limit: 64
Flags: 0x00
 0... .. = Managed address configuration: Not set
 .0.. .. = Other configuration: Not set
 ..0. .. = Home Agent: Not set
 ...0 0... = Prf (Default Router Preference): Medium (0)
 .... .0.. = Proxy: Not set
 .... ..0. = Reserved: 0
Router lifetime (s): 1800
Reachable time (ms): 0
Retrans timer (ms): 0
ICMPv6 Option (Prefix information : 2001:db8:0:1::/64)
  Type: Prefix information (3)
  Length: 4 (32 bytes)
  Prefix Length: 64
  Flag: 0xc0
    1... .. = On-link flag(L): Set
    .1.. .. = Autonomous address-configuration flag(A): Set
    ..0. .... = Router address flag(R): Not set
    ...0 0000 = Reserved: 0
  Valid Lifetime: 86400
  Preferred Lifetime: 14400
  Reserved
  Prefix: 2001:db8:0:1:: (2001:db8:0:1::)
ICMPv6 Option (Source link-layer address : 00:00:00:aa:00:00)
  Type: Source link-layer address (1)
  Length: 1 (8 bytes)

```

Wireshark capture of Router *r1* interface *eth0*

As a last test, add new prefixes to the *radvd.conf* file. Restart the *radvd* service. Look at the Wireshark capture to see the new messages. Also, check the IPv6 address configuration on the hosts to see the new addresses added to each host's interface *eth0*.

Configuring a real Linux router

For reference, I will describe below how to configure *radvd* on a real Linux router, where we are using a normal filesystem. Previously, we showed some modified procedure when working with a simulated router but we should also know the actual procedures we would use on a real router.

We will cover only the configurations that would configure a router the same way we configured our simulated router, above. We omit other real-world configuration scenarios, for now.

On a Linux router, we create the *radvd* configuration file and then start the *radvd* daemon using the [service initialization scripts](#). Then we permanently configure the router's interface addresses by updating the *interfaces* configuration file.

The *radvd.conf* configuration file

On a real Linux router we would first we create the *radvd.conf* configuration file. Check your documentation to see where the configuration file is located⁵. In an Ubuntu filesystem, *radvd* expects the configuration file is */etc/radvd.conf*.

```
$ sudo vi /etc/radvd.conf
```

We would configure the prefixes we have chosen to use on each link. For example:

```
interface eth0
{
AdvSendAdvert on;
prefix 2001:db8:0:1::/64 { };
};
interface eth1
{
AdvSendAdvert on;
prefix 2001:db8:0:2::/64 { };
};
```

Next, we would ensure that the file permissions are correct. *Radvd* will not start unless the configuration file has secure permissions so that no other users can write to the file.

```
&sudochmod 644 /etc/radvd.conf
```

```
$ ls -l /etc/radvd.conf
```

```
-rw-r--r-- 1 root root 642 Apr 26 22:57 /etc/radvd.conf
```

Start radvd

Now, we would start the *radvd* service.

```
$ sudo service radvd start
```

Then, we would permanently configure *radvd* to start when the system starts or reboots:

```
$ sudo update-rc.dradvd defaults
```

```
$ sudo update-rc.dradvd enable
```

Router interface IP addresses

We would assign the router's interface IPv6 addresses. On a normal router, we would permanently configure these interfaces by adding information to the file `/etc/network/interfaces`. For example:

```
$ sudo vi /etc/network/interfaces
```

Then add interface configurations, such as:

```
iface eth0 inet6 static
address 2001:db8:0:1::1
netmask 64
iface eth1 inet6 static
address 2001:db8:0:2::1
netmask 64
```

Then we would restart the networking service. *NOTE:* we assume the Linux router is based on a minimal system and that there is no other software managing networking, such as the *Ubuntu Network Manager*.

```
$ sudo service networking restart
```

Or,

```
$ sudo /etc/init.d/networking restart
```

XI. Precaution

1. Handle Computer System and peripherals with care
2. Follow Safety Practices

XII. Resources Used

Sr. No	Name of Resource	Specification
1.	Computer / Networked Computers	i3 processor, 2 GB RAM, HDD 250GB
2.	Switch (min. 8 ports)	8 ports
3.	Any other Resources	

XIII. Result

.....
.....
.....

XIV. Practical Related Questions

1. How IPv6 Environment is created

XV. Exercise

Student should implement IPv6 environment using simulator

(Space for Answer)

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

References/ Suggestions for further Reading

<https://getipv6.info/display/IPv6/Educating+Yourself+about+IPv6>
<http://www.brianlinkletter.com/tag/core/>

XVI. Assessment Scheme

Performance indicator		Weightage
Process Related(35 Marks)		75%
1.	Completion of given task	25%
2.	Correctness of given task	50%
Product Related(15 Marks)		25%
3.	Answer to sample Question	15%
4.	Submit Report in Time	10%
Total(50 Marks)		100%

❖ **List of Students/Team Members**

.....

Marks Obtained			Dated Signature of Teacher
Process Related(35)	Product Related (15)	Total(50)	