





**Dr. D. Y. Patil**

**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**

**President, DYPEF**

**Dr. Suresh Mali**

**Principal, DYPCOEI**

## INDEX

Department of Artificial Intelligence and Data Science

**Class:** T.E.

Sr.No	Title Of Experiment	CO Mapping	Page No
1	Demonstrate the different types of topologies and types of transmission media by using a packet tracer tool.	CO1	
2	Setup a wired LAN using Layer 2 Switch. It includes preparation of cable, testing of cable using line tester, configuration machine using IP addresses, testing using PING utility and demonstrating the PING packets captured traces using Wireshark Packet Analyzer Tool.	CO1	
3	Use packet Tracer tool for configuration of 3 router networks using one of the following protocols RIP/OSPF/BGP.	CO3	
4	Write a program to demonstrate Sub-netting and find subnet masks.	CO3	
5	Write a program using TCP socket for wired network for following a. Say Hello to Each other b. File transfer	CO4	
6	Capture packets using Wireshark and accomplish the following and save the output in file: a. Capture all TCP traffic to/from Facebook, during the time when you log in to your Facebook account b. Capture all HTTP traffic to/from Facebook (other website), when you log in to your Facebook account c. Write a DISPLAY filter expression to count all TCP packets (captured under item #1) that have the flags SYN, PSH, and RST set. Show the fraction of packets that had each flag set. d. Count how many TCP packets you received from / sent to Facebook (other website), and how many of each were also HTTP packets.	CO4	



**Dr. D. Y. Patil**

Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**

President, DYPEF

**Dr. Suresh Mali**

Principal, DYPCOEI

7	Study and Analyze the performance of HTTP, HTTPS and FTP protocol using Packet tracer tool	CO4	
8	To study the SSL protocol by capturing the packets using Wireshark tool while visiting any SSL secured website (banking, e-commerce etc.).	CO5	
9	Illustrate the steps for implementation of S/MIME email security, POP3 through Microsoft® Office Outlook.	CO5	
10	To study the IPsec (ESP and AH) protocol by capturing the packets using Wireshark tool.	CO4	
11	Installing and configuring DHCP server and assign IP addresses to client machines using DHCP server.	CO5	
12	Write a program for DNS lookup. Given an IP address input, it should return URL and vice versa.	CO5	

**Name & Signature of Course In-charge**



---

**Dr. D. Y. Patil**  
Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**  
President, DYPEF

**Dr. Suresh Mali**  
Principal, DYPCEOI

---

# GROUP A



**Dr. D. Y. Patil**  
Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**  
President, DYPEF

**Dr. Suresh Mali**  
Principal, DYPCEOI

## **Experiment No: 1**

**Demonstrate the different types of topologies and types of transmission media by using a packet tracer tool.**

**Name of the Student:**  
Class:

Date: TE

Mark: /10

**Signature of the Course In-charge:**

**Signature of the HOD:**

**Assignment No: 01**

**Problem Definition:**



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

**Demonstrate the different types of topologies and types of transmission media by using a packet tracer tool.**

### **1.1 Prerequisite:**

- a) IP Address
- b) OSI & TCP/IP Model
- c) Networking Devices

### **1.2 Learning Objectives:**

1. Understand how to Create different topology

**1.3 Outcome:** Students could run the practical for all topologies in Packet tracer New Concepts:

#### **1.3.1 Packet tracer**

### **1.4 Theory**

#### **Introduction What is Topology?**

Network topologies describe the methods in which all the elements of a network are mapped. The topology term refers to both the physical and logical layout of a network.

Type of Network Topology

Point to Point

Bus Topology

Ring

Topology

Star

Topology

Mesh

Topology

Tree

Topology

Hybrid

Topology

How to select a Network

Topology? Types of Networking

Topologies



**Dr. D. Y. Patil**

Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**

President, DYPERF

**Dr. Suresh Mali**

Principal, DYPCOEI

Two main types of network topologies in computer networks are

- 1) Physical topology
- 2) Logical topology

### 1) Physical topology:

This type of network is an actual layout of the computer cables and other network devices

### 2) Logical topology:

Logical topology gives insight's about network's physical design.

Different types of Physical Topologies are:

P2P

Topology Bus

Topology

Ring

Topology

Star

Topology

Tree

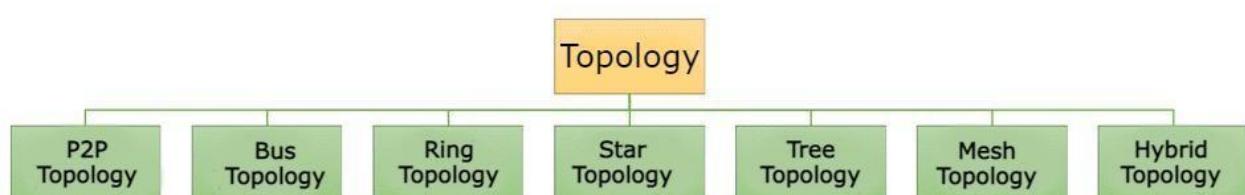
Topology

Mesh

Topology

Hybrid

Topology

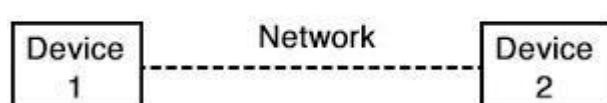


### Network Topology Diagram

#### Point to Point

Point-to-point topology is the easiest of all the network topologies. In this method, the network consists of a direct link between two computers.

#### Point-to-Point topology





**Dr. D. Y. Patil**

Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**

President, DYPERF

**Dr. Suresh Mali**

Principal, DYPCEOI

P2P Topology Diagram

Advantages:



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

This is faster and highly reliable than other types of connections since there is a direct connection.

No need for a network operating system

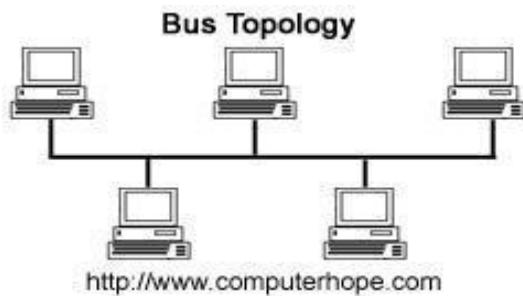
Does not need an expensive server as individual workstations are used to access the files  
No need for any dedicated network technicians because each user sets their permissions  
**Disadvantages:**

The biggest drawback is that it only be used for small areas where computers are in close proximity.

You can't back up files and folders centrally

There is no security besides the permissions. Users often do not require to log onto their workstations.

### *Bus Topology*



Bus Topology Diagram

Bus topology uses a single cable which connects all the included nodes. The main cable acts as a spine for the entire network. One of the computers in the network acts as the computer server. When it has two endpoints, it is known as a linear bus topology.

### Advantages:

Here are pros/benefits of using a bus topology:

Cost of the cable is very less as compared to other topology, so it is widely used to build small networks.

Famous for LAN network because they are inexpensive and easy to install. It is widely used when a network installation is small, simple, or temporary.

It is one of the passive topologies. So computers on the bus only listen for data being sent, that are not responsible for moving the data from one computer to others.



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

### Disadvantages:

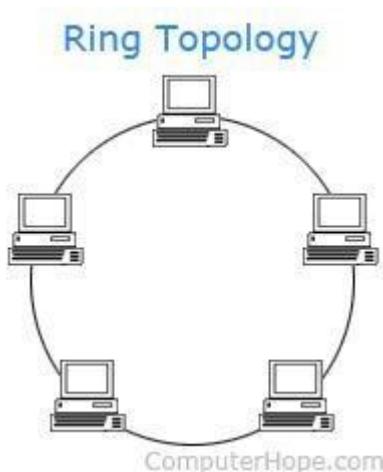
Here are the cons/drawbacks of bus topology:

In case if the common cable fails, then the entire system will crash down. When network traffic is heavy, it develops collisions in the network.

Whenever network traffic is heavy, or nodes are too many, the performance time of the network significantly decreases.

Cables are always of a limited length.

## Ring Topology



**Ring Topology Diagram**

In a ring network, every device has exactly two neighboring devices for communication purpose. It is called a ring topology as its formation is like a ring. In this topology, every computer is connected to another computer. Here, the last node is combined with a first one.

This topology uses token to pass the information from one computer to another. In this topology, all the messages travel through a ring in the same direction.

### Advantages:

Here are pros/benefits of ring topology:

Easy to install and reconfigure.

Adding or deleting a device in-ring topology needs you to move only two connections. The troubleshooting process is difficult in a ring topology.

Failure of one computer can disturb the whole network.



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

Offers equal access to all the computers of the networks

Faster error checking and acknowledgment.

#### Disadvantages:

Here are drawbacks/cons of ring topology:

Unidirectional traffic.

Break in a single ring can risk the breaking of the entire network

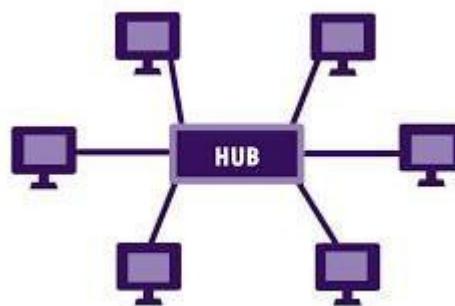
Modern days high-speed LANs made this topology less popular.

In the ring, topology signals are circulating at all times, which develops unwanted power consumption.

It is very difficult to troubleshoot the ring network.

Adding or removing the computers can disturb the network activity.

#### *Star Topology*



#### Star Topology Diagram

In the star topology, all the computers connect with the help of a hub. This cable is called a central node, and all other nodes are connected using this central node. It is most popular on LAN networks as they are inexpensive and easy to install.

#### Advantages:

Here are pros/benefits of start topology:

Easy to troubleshoot, set up, and modify.

Only those nodes are affected, that has failed. Other nodes still work. Fast performance with few nodes and very low network traffic.



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

In Star topology, addition, deletion, and moving of the devices are easy.

#### Disadvantages:

Here are cons/drawbacks of using Star:

If the hub or concentrator fails, attached nodes are disabled. Cost of installation of star topology is costly.

Heavy network traffic can sometimes slow the bus considerably.

Performance depends on the hub's capacity

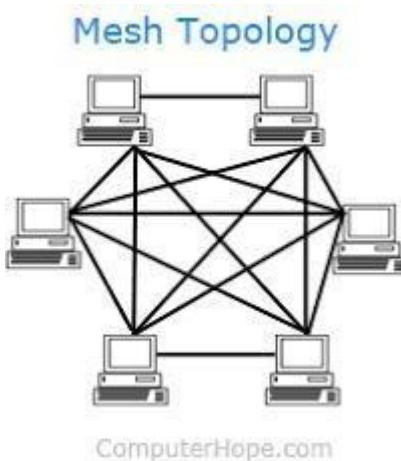
A damaged cable or lack of proper termination may bring the network down.

#### *Mesh Topology*

The mesh topology has a unique network design in which each computer on the network connects to every other. It develops a P2P (point-to-point) connection between all the devices of the network. It offers a high level of redundancy, so even if one network cable fails, still data has an alternative path to reach its destination.

#### Mesh Topology:

In this topology, every nodes or device are directly connected with each other.



#### Mesh Topology

#### Advantages:

Here, are pros/benefits of Mesh topology

The network can be expanded without disrupting current users.

Need extra capable compared with other LAN topologies.



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

No traffic problem as nodes has dedicated links.

Dedicated links help you to eliminate the traffic problem. A mesh topology is robust.

It has multiple links, so if any single route is blocked, then other routes should be used for data communication.

P2P links make the fault identification isolation process easy.

It helps you to avoid the chances of network failure by connecting all the systems to a central node.

Every system has its privacy and security.

#### Disadvantages:

Installation is complex because every node is connected to every node.

It is expensive due to the use of more cables. No proper utilization of systems.

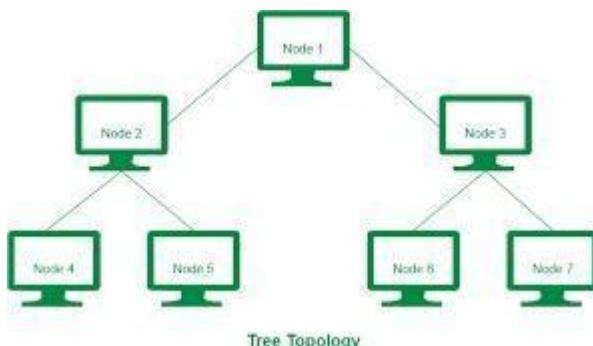
Complicated implementation.

It requires more space for dedicated links.

Because of the amount of cabling and the number of input-outputs, it is expensive to implement.

It requires a large space to run the cables.

#### *Tree Topology*



#### Tree Topology

Tree topologies have a root node, and all other nodes are connected which form a hierarchy. So it is also known as hierarchical topology. This topology integrates various star topologies together in a single bus, so it is known as a Star Bus topology. Tree topology is a very common network which is similar to a bus and star topology.

#### Advantages:

Here are pros/benefits of tree topology:



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

Failure of one node never affects the rest of the network.

Node expansion is fast and easy.

Detection of error is an easy process It is easy to manage and maintain

#### Disadvantages:

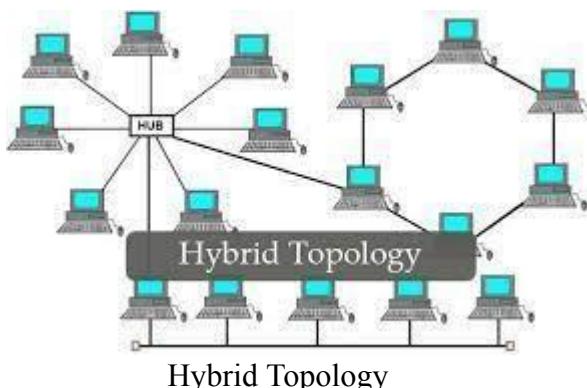
Here are cons/drawback of tree topology:

It is heavily cabled topology

If more nodes are added, then its maintenance is difficult

If the hub or concentrator fails, attached nodes are also disabled.

#### Hybrid Topology



Hybrid topology combines two or more topologies. You can see in the above architecture in such a manner that the resulting network does not exhibit one of the standard topologies.

For example, as you can see in the above image that in an office in one department, Star and P2P topology is used. A hybrid topology is always produced when two different basic network topologies are connected.

#### Advantages:

Here, are advantages/pros using Hybrid topology:

Offers the easiest method for error detecting and troubleshooting

Highly effective and flexible networking topology

It is scalable so you can increase your network size

#### Disadvantages:



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

The design of hybrid topology is complex It is one of the costliest processes

How to select a Network Topology?

Here are some important considerations for selecting the best topology to create a network in your organization:

Bus topology is surely least expensive to install a network.

If you want to use a shorter cable or you planning to expand the network in future, then star topology is the best choice for you.

Fully mesh topology is theoretically an ideal choice as every device is connected to every other device.

If you want to use twisted pair cable for networking, then you should build star topologies.

**Conclusion:** Successfully demonstrated the different types of topologies and types of transmission media by using a packet tracer tool.



**Dr. D. Y. Patil**  
Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**  
President, DYPEF

**Dr. Suresh Mali**  
Principal, DYPCEOI

## **Experiment No: 2**

**Setup a wired LAN using Layer 2 Switch. It includes preparation of cable, testing of cable using line tester, configuration machine using IP addresses, testing using PING utility and demonstrating the PING packets captured traces using Wireshark Packet Analyzer Tool.**

**Name of the Student:**  
**Class:**

Date: **TE**

Mark: /10

**Signature of the Course In-charge:**

**Signature of the HOD:**



**Dr. D. Y. Patil**  
Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**  
President, DYPEF

**Dr. Suresh Mali**  
Principal, DYPCEOI

## Assignment No.2

### Problem Definition:

Setup a wired LAN using Layer 2 Switch. It includes preparation of cable, testing of cable using line tester, configuration machine using IP addresses, testing using PING utility and demonstrating the PING packets captured traces using Wireshark Packet Analyzer Tool.

### 1.1 Prerequisite:

- a) IP Address
- b) OSI & TCP/IP Model
- c) Networking Devices

### 1.2 Learning Objectives:

1. Understand how to Create LAN, PAN & CAN
2. Understand how to Create wireless LAN using Access Point.

**1.3 Outcome:** Students could create packet tracer LAN protocol and understand the concept of Switches, routers etc

### 1.4 New Concepts:

1. Crimping
2. Access Point Configuration

### 1.5 Theory

#### 1.5.1 Introduction

A **computer network** is a system in which multiple computers are connected to each other to share information and resources.





**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

## Characteristics of a Computer Network

- Share resources from one computer to another.
- Create files and store them in one computer, access those files from the other computer(s) connected over the network.
- Connect a printer, scanner, or a fax machine to one computer within the network and let other computers of the network use the machines available over the network.

## Network Cables

Network cables are used to connect computers. The most commonly used cable is CAT cable & RJ-45.



## Network Card

Network card is a necessary component of a computer without which a computer cannot be connected over a network. It is also known as the network adapter or Network Interface Card (NIC). Most branded computers have network card pre-installed. Network cards are of two types: Internal and External Network Cards.

### Straight Through & Crossover Cable:

The information listed here is to assist Network Administrators in the color coding of Ethernet cables. Please be aware that modifying Ethernet cables improperly may cause loss of network connectivity.

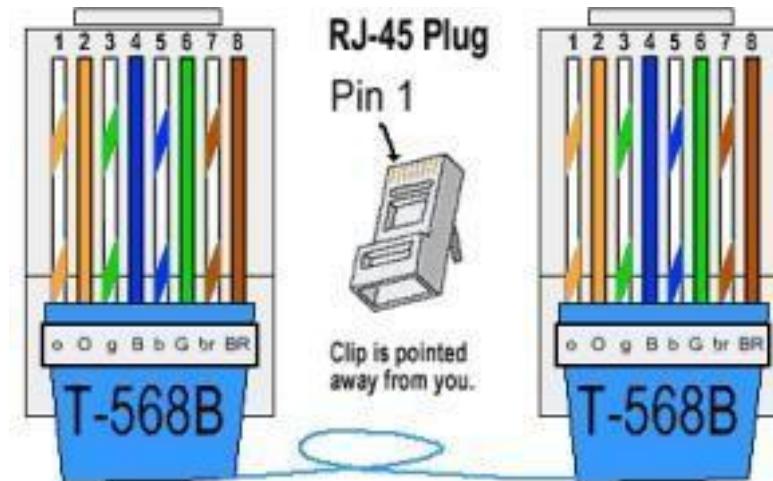
### Straight-Through Ethernet Cable



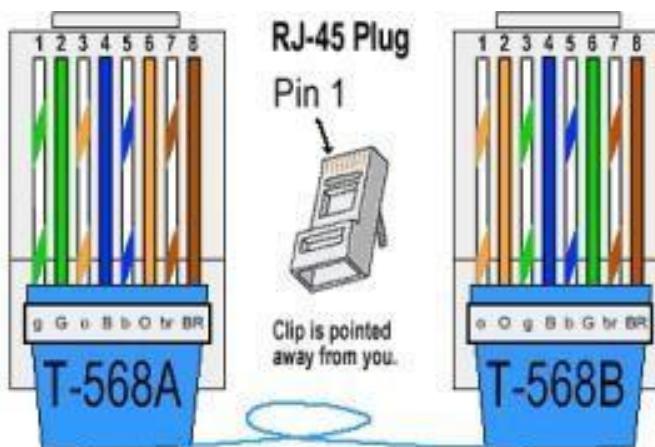
**Dr. D. Y. Patil**  
Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**  
President, DYPEF

**Dr. Suresh Mali**  
Principal, DYPCOEI



**Straight-Through Ethernet Cable**



### ■ Local Area Network:

A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building and has its network equipment and interconnects locally managed. By contrast, a wide area network (WAN) not only covers a larger geographic distance, but also generally involves leased telecommunication circuits or Internet links. An even greater contrast is the Internet, which is a system of globally connected business and personal computers. Ethernet and Wi-Fi are the two most common transmission technologies in use for local area networks.



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

#### ■ Wireless LAN:

A wireless local area network (WLAN) is a wireless computer network that links two or more devices using a wireless distribution method (often spread-spectrum or OFDM radio) within a limited area such as a home, school, computer laboratory, or office building. This gives users the ability to move around within a local coverage area and yet still be connected to the network. A WLAN can also provide a connection to the wider Internet.

Most modern WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name.

#### Benefits of Wireless LAN:

- People can access the network from where they want; they are no longer limited by the length of the cable
- Some places and vehicles have Wireless LANs. This means that people can access the internet even outside their normal work environment, for example when they ride a train.
- Setting up a wireless LAN can be done with one box called wireless access point or wireless router. This box can handle many connections at the same time. Wired networks require cables to be laid. This can be difficult for certain places.
- Access points can serve a varying number of computers.

#### Using Packet tracer tool :

Cisco Packet Tracer designed to be used as multi-tasking, that's been to examine varied network exercises like application of dissimilar topologies, development of apt servers, subnetting and study of different network setups, configuration and different troubleshooting defined commands. To initialise communication among two networking devices i.e., user networking devices and to organise a network, we intend to demand to pick applicable networking devices like routers hubs, switches or interconnecting devices and build physical change of integrity by connecting cables, quick local area network seaports from the module list of packet trace



**Dr. D. Y. Patil**

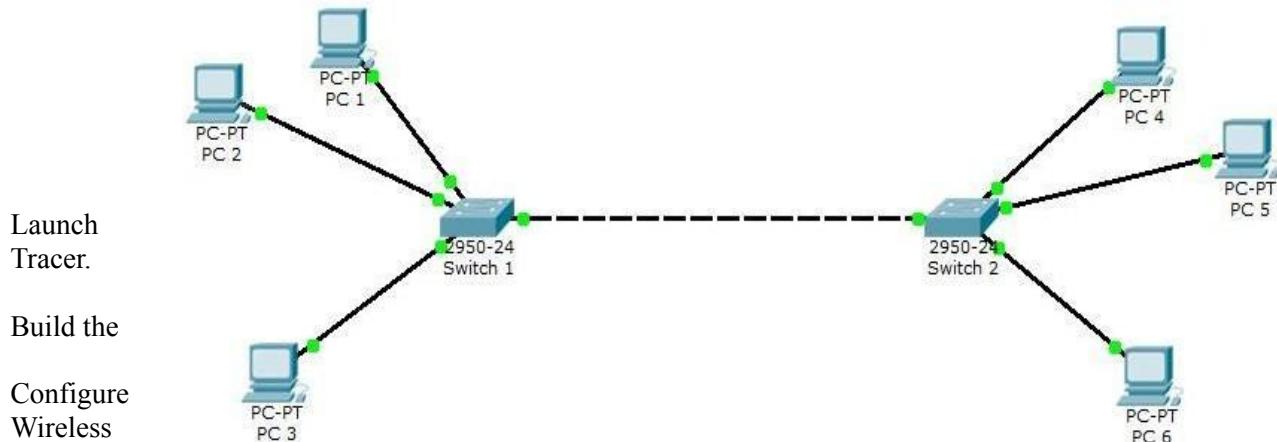
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**

**President, DYPEF**

**Dr. Suresh Mali**

**Principal, DYPCEOI**



Launch  
Tracer.

Build the

Configure  
Wireless

Configure the Laptop. Or

Step 5: Configure the PC.

Step 6 : Send the packets from one PC to another

**Steps:**

Step 1:  
Packet

Step 2:  
topology.

Step 3:  
the  
Router.  
Step 4:

**Conclusion:** Successfully done the Setup of wired LAN using Layer 2 Switch. It includes preparation of cable, testing of cable using line tester, configuration machine using IP addresses, testing using PING utility and demonstrating the PING packets captured traces using Wireshark Packet Analyzer Tool.



**Dr. D. Y. Patil**  
Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**  
President, DYPEF

**Dr. Suresh Mali**  
Principal, DYPCEOI

## **Experiment No: 3**

**Use packet Tracer tool for configuration of 3 router networks using one  
of the following protocols RIP/OSPF/BGP**

**Name of the Student:**

**Class:**

**TE**  
Date:

**Mark: /10**

**Signature of the Course In-charge:**

**Signature of the HOD:**



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

### **3.1 Problem Definition:**

**Use packet Tracer tool for configuration of 3 router networks using one of the following protocols RIP/OSPF/BGP.**

#### **Prerequisite:**

Use packet Tracer tool for configuration of 3 router networks using one of the following protocols  
RIP/OSPF/BGP

### **3.2 Learning Objectives:**

- To learn how to configure a topology with RIP

### **3.3 Outcome:** Test and verify the configuration

### **3.4 New Concepts:** Routing Information Protocol (RIP)

### **3.5 Theory**

#### **Protocols**

Routing protocols maintains routing tables where routing table contains a route to every destination network

#### **Dynamic Routing Protocols**

There are three types of it as follows:

1. Routing Information Protocol (RIP)
2. Open Shortest Path First (OSPF)
3. Border Gateway Protocol (BGP)

RIP and OSPF are Interior Gateway Protocols (IGPs); they are designed to operate in a single autonomous system (AS). (An AS is a group of networks administered by the same authority). BGP is an Exterior Gateway Protocol (EGP), which allows routers in different autonomous systems to exchange routes. Because BGP routers must regulate traffic between networks controlled by organizations with different policies.

#### **How Routing Protocols Work**

A router constructs its routing table using the information it receives from other routers. The router changes its routing table in response to routing updates that



**Dr. D. Y. Patil**

**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**

**President, DYPEF**

**Dr. Suresh Mali**

**Principal, DYPCEOI**

provide additional information or notification that conditions in the network have changed (for example, a link has failed). This responsiveness explains why using a routing protocol is often called dynamic routing

The protocol must dictate parameters such as the following:

- How routers compute a route's metric and select the best route for their routing table: Routing protocols can have a relatively complicated system for calculating a route's metric. So that you can select the best routing protocol (or protocols) for your network environment. If necessary, you can change which routes are chosen by altering the default metrics that a protocol assigns certain routes.
- What information routers include in routing updates: With some routing protocols, routers exchange their entire routing tables. With other routing protocols, routers exchange only portions of the routing table.
- Which routers and router interfaces send and receive updates: Most protocols specify that when routers receive an update on an interface, they do not send the same update from that interface. This common sense rule minimizes overhead.
- When routers send and receive updates and hellos: To lower overhead and conserve bandwidth, you can alter how often routers send certain messages.

## 1. Routing Information Protocol (RIP)

RIP is one of the oldest dynamic routing protocols on the Internet that is still in use. RIP is an intradomain routing protocol that uses a distance vector approach to determine the paths between routers. RIP minimizes the number of hops on each path, where each point-to-point link or LAN constitutes a hop. Each RIP-enabled router periodically sends the content of its routing table to all its neighbouring routers in an update message. For each routing table entry, the router sends the destination (host IP address or network IP address and associated prefix) and the distance to the destination measured in hops. When a router receives an update message from a neighbouring router, it updates its own routing table



**Dr. D. Y. Patil**

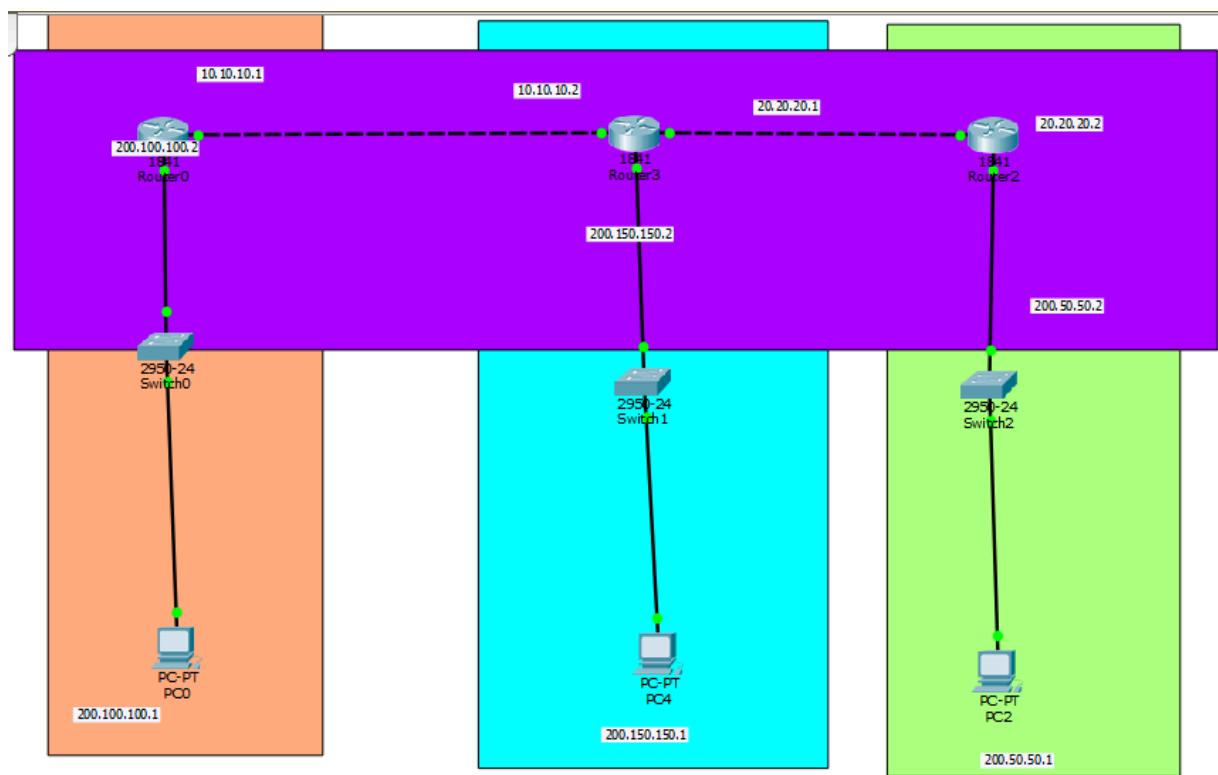
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**

**President, DYPEF**

**Dr. Suresh Mali**

**Principal, DYPCEOI**



### Procedure:

1. Establish network as shown in figure below using 3 routers, 3 switches, 3 PCs.
2. Configure PCs of network 1 with ip address such that network id will be same for both. Also assign ip address with same network id to router-1 interface (fa0/0 or fa0/1 or gig0/0/0 or gig0/0/1) to which switch is connected under which above 1 PCs connected.
3. Configure PCs of network 2 with ip address such that netid will be same for both but different from network 1. Also assign ip address with same netid to router-2 interface (fa0/0 or fa0/1 or gig0/0/0 or gig0/0/1) to which switch is connected under which above 1 PCs connected.
4. Now assign ip address to router-1 interface (fa0/0 or fa0/1 or gig0/0/0 or gig0/0/1) which connects router-2 using copper straight over cable (Network 2). This ip address & netid should be different than network 1 & Network 2.
5. Now assign ip address to router-2 interface (fa0/0 or fa0/1 or gig0/0/0 or gig0/0/1) which connects router-1 using copper straight over cable (Network 2) keeping network id same as router-1 interface. So that router-1 & router-2 & router-3 will be forming network-3.
6. Now click on router-1->config->RIP-> add netid of network-1 & netid of network-2.
7. Similarly click on router-2->config->RIP-> add netid of network-3 & netid of network-2.
8. Now wait for 30 seconds as routers need to update & share their routing tables.
9. After 30 seconds , select simple PDU , put it on PC on network 1 to PC of network 3.
10. Check whether communication succeeds or not.

**Conclusion:** successfully done using packet Tracer tool for configuration of 3 router networks using RIP.



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

## Experiment No: 4

**Write a program to demonstrate Sub-netting and find subnet masks..**

**Name of the Student:**

**Class:**

Date: **TE**

Mark: /10

**Signature of the Course In-charge:**

**Signature of the HOD:**

## Assignment No. 04

**Problem Definition:** Write a program to demonstrate Sub-netting and find subnet masks.

**PROBLEM STATEMENT:** Write a program to demonstrate Sub-netting and find subnet masks.



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

#### **4.1 Prerequisite:**

1. IP Address Classes
2. Classless & Classful IP Addressing

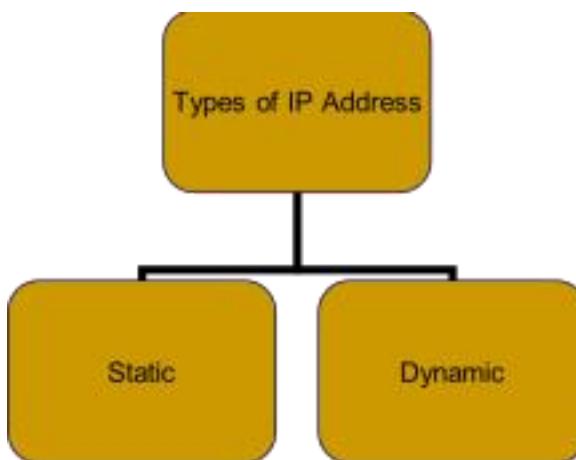
#### **4.2 Learning Objectives:**

- 4.2.1 Understand the concept Subnetting.
- 4.2.2 Understand the Concept of Supernet.

#### **4.3 Theory**

#### **4.4 Introduction**

**A Unique, 32-bit address used by computers to communicate over a computer network**



#### **Classes of Address**

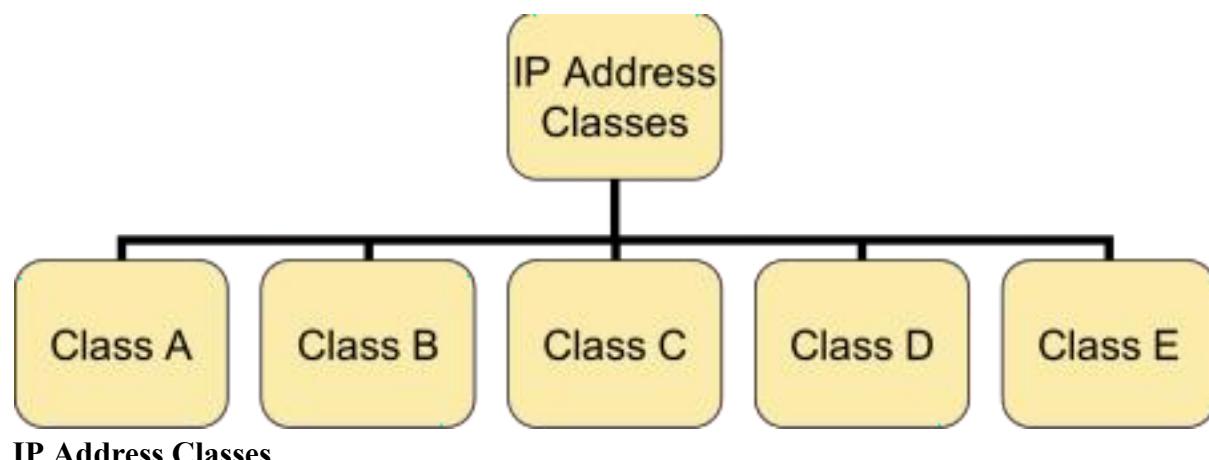
**IP address structure consists of two addresses, Network and Host ■**  
**IP address is divided into five classes**



**Dr. D. Y. Patil**  
Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**  
President, DYPEF

**Dr. Suresh Mali**  
Principal, DYPCEOI



### IP Address Classes

The 5 IP classes are split up based on the value in the 1<sup>st</sup> octet: Class

A: 0-127

Class B: 128-191

Class C: 192-223

Class D: 224-239

Class E: 240-255

### IP Address Classes(Cont.)

	Byte 1	Byte 2	Byte 3	Byte 4
Class A	Network ID		Host ID	
Class B		Network ID		Host ID
Class C			Network ID	Host ID
Class D			Multicast Address	
Class E			Reserved for future use	



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

### Examples of IP Address

- 14.23.120.8 - The first byte of the address represents 14 which lies between 0 and 127, hence Class A address.
- 134.11.78.56 - The first byte of address is 134 which lies between 128 and 191 hence the address belongs to Class B.
- 193.14.56.22 - As first byte is 193 which is between 192 and 223, hence the address belongs to Class C.

### Subnet Mask

An IP address has 2 parts:

- The Network identification.
- The Host identification.

Frequently, the Network & Host portions of the address need to be separately extracted.

- In most cases, if you know the address class, it's easy to separate the 2 portions.
- Specifies part of IP address used to identify a subnetwork.
- Subnet mask when logically ANDed with IP address provides 32-bit network address

### Default Mask:

- Has predetermined number of 1s
- Class A, B and C contains 1s in network ID fields for default subnet mask.

<b>Address Class</b>	<b>Default Mask (in Binary)</b>
Class A	<b>11111111.00000000.00000000.00000000</b>
Class B	<b>11111111.11111111.00000000.00000000</b>
Class C	<b>11111111.11111111.11111111.00000000</b>



**Dr. D. Y. Patil**  
Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**  
President, DYPEF

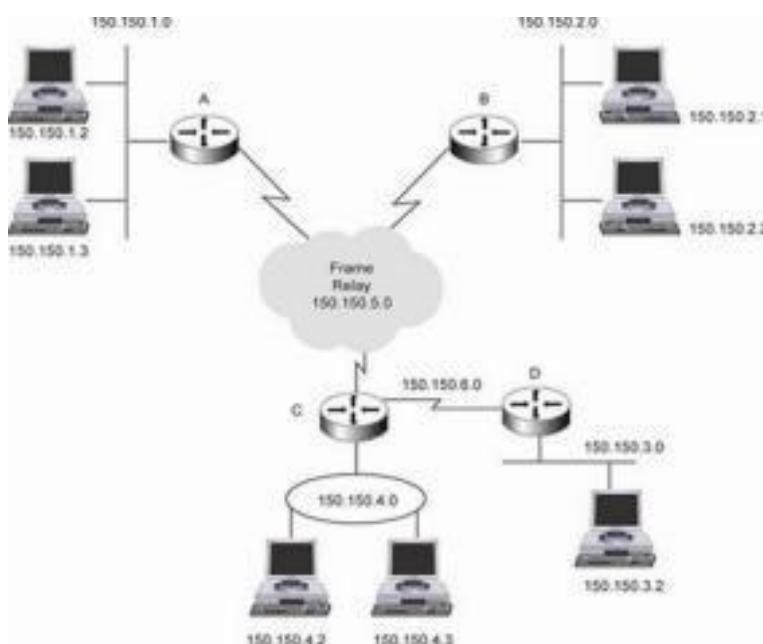
**Dr. Suresh Mali**  
Principal, DYPCEOI

### *Default Standard Subnet Masks*

<b>Default Subnet Masks</b>	
<b>Address Class</b>	<b>Subnet Mask</b>
<b>Class A</b>	<b>255.0.0.0</b>
<b>Class B</b>	<b>255.255.0.0</b>
<b>Class C</b>	<b>255.255.255.0</b>

### *IP Subnetting:*

- Allows you to divide a network into smaller sub-networks
- Each subnet has its own sub-network address
- Subnet can be created within Class A, B, or C based networks





**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

### *Subnetting:*

- Division of a network into subnets
  - For example, division of a Class B address into several Class C addresses
  - Some of the host IDs are used for creating subnet IDs

### *Need for Subnetting:*

- Classes A and B have a large number of hosts corresponding to each network ID
  - It may be desirable to subdivide the hosts in Class C subnets
- Often, there is a limitation on the number of hosts that could be hosted on a single network segment
  - The limitation may be imposed by concerns related to the management of hardware
- Smaller broadcast domains are more efficient and easy to manage

### *Subnetting Principle:*

- Use parts of the host IDs for subnetting purpose

A subnet mask is used to facilitate the flow of traffic between the different subnets and the outside network (hops)

- A hop is the distance a data packet travels from one node to the other .

### *How to Calculate Subnets:*

- To determine the number of subnets & hosts per subnet available for any of the available subnet masks, 2 simple formulas to calculate these numbers:
  - Number of Subnets= $(2^n)$
  - Number of Host per Subnets= $(2^{h-2})$
- Although the 2 formulas look identical, the key is to remember the number you're trying to calculate, hosts or subnets.
- Eg., suppose you are asked to determine the number of subnets available & the number of hosts available on each subnet on the network 192.168.1.0
- Using the subnet & hosts formulas, the answers are easily calculated. Of course, you must know your powers of 2 to calculate the answers



---

**Dr. D. Y. Patil** **Dr. Sushant Patil** **Dr. Suresh Mali**  
**Founder, Dr. D. Y. Patil Group** **President, DYPEF** **Principal, DYPCEOI**

---

*Conclusion:*

Hence we have studied Subnetting and the importance of subnetting.



**Dr. D. Y. Patil**  
Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**  
President, DYPEF

**Dr. Suresh Mali**  
Principal, DYPCEOI

# GROUP B

## Experiment No: 5

Write a program using TCP socket for wired network for following a.

Say Hello to Each other b. File transfer.

Name of the Student:

TE
Date:

Mark: /10
-----------

Signature of the Course In-charge:

Signature of the HOD:



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

## Assignment No. 05

**Problem Definition:** Write a program using TCP socket for wired network for following a. Say Hello to Each other b. File transfer

### 1.1 Prerequisite:

- a) Socket Header
- b) Network Programming
- c) Ports

### Learning Objectives:

1. To understand Work of Socket
2. Different methods associated with Client & Server Socket

### New Concepts:

1. Client Server Communication
2. Port Address



**Dr. D. Y. Patil**

**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**

**President, DYPERF**

**Dr. Suresh Mali**

**Principal, DYPCEOI**

### 1.3 Theory:

#### Theory:

Socket Programming: The Berkeley socket interface, an API, allows communications between hosts or between processes on one computer, using the concept of a socket. It can work with many different I/O devices and drivers, although support for these depends on the operating system implementation. This interface implementation is implicit for TCP/IP, and it is therefore one of the fundamental technologies underlying the Internet. It was first developed at the University of California, Berkeley for use on Unix systems. All modern operating systems now have some implementation of the Berkeley socket interface, as it has become the standard interface for connecting to the Internet. Programmers can make the socket interfaces accessible at three different levels, most powerfully and fundamentally at the RAW socket level. Very few applications need the degree of control over outgoing communications that this provides, so RAW sockets support was intended to be available only on computers used for developing Internet related technologies. TCP TCP provides the concept of a connection. A process creates a TCP socket by calling the socket() function with the parameters PF\_INET or PF\_INET6 and SOCK\_STREAM. Server Setting up a simple TCP server involves the following steps: Creating a TCP socket, with a call to socket(). Computer Networks Lab 2 Binding the socket to the listen port, with a call to bind(). Before calling bind(), a programmer must declare a sockaddr\_in structure, clear it (with bzero() or memset()), and the sin\_family (AF\_INET or AF\_INET6), and fill its sin\_port (the listening port, in network byte order) fields. Converting a short int to networkbyte order can be done by calling the function htons() (host to network short). Preparing the socket to listen for connections (making it a listening socket), with a call to listen(). Accepting incoming connections, via a call to accept(). This blocks until an incoming connection is received, and then returns a socket descriptor for the accepted connection. The initial descriptor remains a listening descriptor, and accept() can be called again at any time with this socket, until it is closed. Communicating with the remote host, which can be done through send() and recv(). Eventually closing each socket that was opened, once it is no longer needed, using close(). Note that if there were any calls to fork(), each process must close the sockets it knew about (the kernel keeps track of how many processes have a descriptor open), and two processes should not use the same socket at once. Client: Setting up a TCP client involves the following steps: 1. Creating a TCP socket, with a call to socket(). 2. Connecting to the server with the use of connect, passing a sockaddr\_in structure with the sin\_family set to AF\_INET or AF\_INET6, sin\_port set to the port the endpoint is listening (in network byte order), and sin\_addr set to the IPv4 or IPv6 address of the listening server (also in network byte order.) 1. Communicating with the server by send()ing and recv()ing. Terminating the connection and cleaning up with a call to close(). Again, if there were any calls to fork(), each process must close() the socket. Functions: 1. socket(): socket() creates an endpoint for communication and returns a descriptor. socket() takes three arguments: domain, which specifies the protocol family of the created socket. For example: PF\_INET for network protocol IPv4 or PF\_INET6 for IPv6. type, one of: Computer Networks Lab 3 SOCK\_STREAM (reliable stream-oriented service) SOCK\_DGRAM (datagram service) SOCK\_SEQPACKET (reliable sequenced packet service), or SOCK\_RAW (raw protocols atop the network layer). protocol usually set to 0 to represent the default transport protocol for the specified domain and type values (TCP for PF\_INET or PF\_INET6 and SOCK\_STREAM, UDP for those PF\_values and SOCK\_DGRAM), but which can also explicitly specify a protocol. The function returns -1 if an error occurred. Otherwise, it returns an integer representing the newly-assigned descriptor. Prototype: int socket(int domain, int type, int protocol); connect(): connect() returns an integer representing the error code: 0 represents success, while -1 represents an error. Certain types of sockets are connectionless, most commonly user datagram protocol sockets. For these sockets, connect takes on a special meaning: the default target for sending and receiving data gets set to the given address, allowing the use of functions such as send() and recv() on connectionless sockets. Prototype: int connect(int sockfd, const struct sockaddr \*serv\_addr, socklen\_t addrlen); bind(): bind() assigns a socket an address. When a socket is created using socket(), it is given an address family, but not assigned an address. Before a socket may accept incoming connections, it must be bound. bind() takes three arguments:



**Dr. D. Y. Patil**

**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**

**President, DYPCEF**

**Dr. Suresh Mali**

**Principal, DYPCOEI**

sockfd, a descriptor representing the socket to perform the bind onmy\_addr, a pointer to a sockaddr structure representing the address to bind to. addrlen, a socklen\_t field representing the length of the sockaddr structure. It returns 0 on success and -1 if an error occurs. Prototype: int bind(int sockfd, struct sockaddr \*my\_addr, socklen\_t addrlen); listen() listen() prepares a bound socket to accept incoming connections. This function is only applicable to the SOCK\_STREAM and SOCK\_SEQPACKET socket types. It takes two arguments: sockfd, a valid socket descriptor. Computer Networks Lab 4 backlog, an integer representing the number of pending connections that can be queued up at any one time. The operating system usually places a cap on this value. Once a connection is accepted, it is dequeued. On success, 0 is returned. If an error occurs, -1 is returned. Prototype: int listen(int sockfd, int backlog); accept() Programmers use accept() to accept a connection request from a remote host. It takes the following arguments: sockfd, the descriptor of the listening socket to accept the connection from. cliaddr, a pointer to the sockaddr structure that accept() should put the client's address information into. addrlen, a pointer to the socklen\_t integer that will indicate to accept() how large the sockaddr structure pointed to by cliaddr is. When accept() returns, the addrlen\_t integer then indicates how many bytes of the cliaddr structure were actually used. The function returns a socket corresponding to the accepted connection, or -1 if an error occurs. Prototype: int accept(int sockfd, struct sockaddr \*cliaddr, socklen\_t \*addrlen);

Blocking vs. nonblocking Berkeley sockets can operate in one of two modes: blocking or non-blocking. A blocking socket will not "return" until it has sent (or received) all the data specified for

the operation. This may cause problems if a socket continues to listen: a program may hang as the socket waits for data that may never arrive. A socket is typically set to blocking or nonblocking mode using the fcntl() or ioctl() functions. Cleaning up The system will not release the resources allocated by the socket() call until a close() call occurs. This is especially important if the connect() call fails and may be retried. Each call to socket() must have a matching call to close() in all possible execution paths.

Algorithm: Server Program

1. Open the Server Socket: ServerSocket server = new ServerSocket( PORT );
2. Wait for the Client Request: Socket client = server.accept();
3. Create I/O streams for communicating to the client DataInputStream is = new DataInputStream(client.getInputStream()); DataOutputStream os = new DataOutputStream(client.getOutputStream());
4. Perform communication with client Receive from client: String line = is.readLine(); Send to client: os.writeBytes("Hello\n")
5. Close socket: client.close(); Client Program
  - 1) Create a Socket Object: Socket client = new Socket(server, port\_id);
  - 2) Create I/O streams for communicating with the server. is = new DataInputStream(client.getInputStream()); os = new DataOutputStream(client.getOutputStream());
  - 3) Perform I/O or communication with the server: Receive data from the server: String line = is.readLine(); Send data to the server: os.writeBytes("Hello\n");
  - 4) Close the socket when done:
  - 5) client.close();



**Dr. D. Y. Patil**

**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**

**President, DYPEF**

**Dr. Suresh Mali**

**Principal, DYPCEOI**

## Socket Types

There are four types of sockets available to the users. The first two are most commonly used and the last two are rarely used.

Processes are presumed to communicate only between sockets of the same type but there is no restriction that prevents communication between sockets of different types.

- Stream Sockets – Delivery in a networked environment is guaranteed. If you send through the stream socket three items "A, B, C", they will arrive in the same order – "A, B, C". These sockets use TCP (Transmission Control Protocol) for data transmission. If delivery is impossible, the sender receives an error indicator. Data records do not have any boundaries.
- Datagram Sockets – Delivery in a networked environment is not guaranteed. They're connectionless because you don't need to have an open connection as in Stream Sockets – you build a packet with the destination information and send it out. They use UDP (User Datagram Protocol).
- Raw Sockets – These provide users access to the underlying communication protocols, which support socket abstractions. These sockets are normally datagram oriented, though their exact characteristics are dependent on the interface provided by the protocol. Raw sockets are not intended for the general user; they have been provided mainly for those interested in developing new communication protocols, or for gaining access to some of the more cryptic facilities of an existing protocol.

Here is the description of the parameters –

- `socket_family` – This is either `AF_UNIX` or `AF_INET`, as explained earlier.
- `socket_type` – This is either `SOCK_STREAM` or `SOCK_DGRAM`.
- `protocol` – This is usually left out, defaulting to 0.

Once you have socket object, then you can use required functions to create your client or server program. Following is the list of functions required –



**Dr. D. Y. Patil**  
Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**  
President, DYPEF

**Dr. Suresh Mali**  
Principal, DYPCEOI

### SERVER SOCKET METHODS

Sr.No.	Method & Description
1	<b>s.bind()</b> This method binds address (hostname, port number pair) to socket.
2	<b>s.listen()</b> This method sets up and start TCP listener.
3	<b>s.accept()</b> This passively accept TCP client connection, waiting until connection arrives (blocking).

### CLIENT SOCKET METHODS

Sr.No.	Method & Description
1	<b>s.connect()</b> This method actively initiates TCP server connection.

### GENERAL SOCKET METHODS

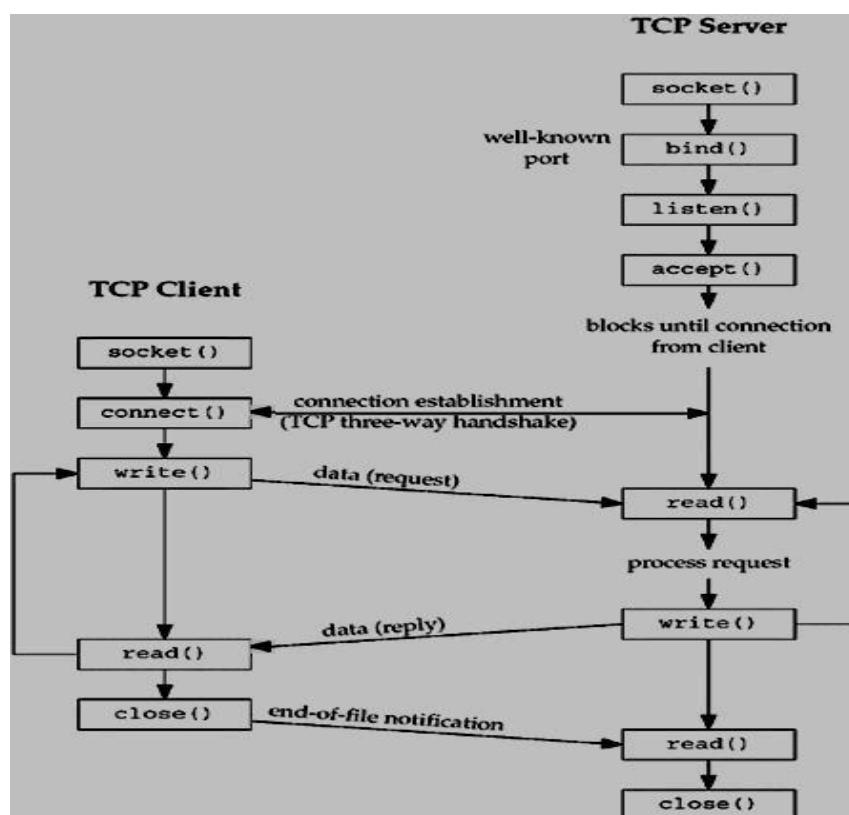
Sr.No.	Method & Description
1	<b>s.recv()</b> This method receives TCP message
2	<b>s.send()</b> This method transmits TCP message
3	<b>s.recvfrom()</b> This method receives UDP message
4	<b>s.sendto()</b> This method transmits UDP message
5	<b>s.close()</b> This method closes socket
6	<b>socket.gethostname()</b> Returns the hostname.



**Dr. D. Y. Patil**  
Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**  
President, DYPEF

**Dr. Suresh Mali**  
Principal, DYPCEOI



**CONCLUSION** Thus we have successfully implemented the socket programming for TCP



**Dr. D. Y. Patil**  
Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**  
President, DYPEF

**Dr. Suresh Mali**  
Principal, DYPCEOI

## Experiment No: 6

Capture packets using Wireshark and accomplish the following and save the output in file:  
a. Capture all TCP traffic to/from Facebook, during the time when you log in to your Facebook account  
b. Capture all HTTP traffic to/from Facebook (other website), when you log in to your Facebook account  
c. Write a DISPLAY filter expression to count all TCP packets (captured under item #1) that have the flags SYN, PSH, and RST set. Show the fraction of packets that had each flag set.  
d. Count how many TCP packets you received from / sent to Facebook (other website), and how many of each were also HTTP packets.

Name of the Student:

TE  
Date:

Mark: /10

Signature of the Course In-charge:

Signature of the HOD:

## Assignment No: 06

Problem Definition:



**Dr. D. Y. Patil**

**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**

**President, DYPEF**

**Dr. Suresh Mali**

**Principal, DYPCEOI**

**analyze network traffic using Wireshark** to understand how data packets are exchanged between a user's computer and web services, specifically Facebook. The problem involves capturing **TCP and HTTP packets**, applying **filter expressions**, identifying specific **TCP flags**, and quantifying the nature of the traffic exchanged during a Facebook login session.

### **Learning Objectives::**

- To capture and analyze TCP and HTTP traffic between a host machine and Facebook.
- To learn how to use Wireshark effectively for filtering and analyzing network packets.
- To observe and filter packets with specific TCP flags (SYN, PSH, RST) and calculate their frequency.

### **New Concepts:**

**TCP flags-** Control bits used in TCP headers to manage the state of connections. Common flags include SYN, ACK, PSH, RST, and FIN.

### **Theory:**

#### **Introduction**

##### **1. Wireshark Packet Capturing**

Wireshark allows users to capture data packets traversing a network in real time. These packets can be filtered, analyzed, and saved for later inspection. It is widely used in network security, troubleshooting, and education.

##### **2. TCP Protocol**

Transmission Control Protocol (TCP) is a connection-oriented protocol that ensures reliable data delivery. TCP packets have flags that indicate control information, including:

- SYN (Synchronize): Initiates a TCP connection.
- ACK (Acknowledgment): Acknowledges received packets.
- PSH (Push): Instructs the receiver to pass data to the application immediately.
- RST (Reset): Abruptly terminates the connection.

##### **3. HTTP Protocol**

Hypertext Transfer Protocol (HTTP) is an application layer protocol used by web browsers to communicate with websites. HTTP traffic is typically visible in Wireshark unless encrypted (i.e., HTTPS).

#### **4. Filters in Wireshark**

- Capture Filters: Used to limit the packets captured.
- Display Filters: Used to show only relevant packets in the capture.



<b>Dr. D. Y. Patil</b> <b>Founder, Dr. D. Y. Patil Group</b>	<b>Dr. Sushant Patil</b> <b>President, DYPEF</b>	<b>Dr. Suresh Mali</b> <b>Principal, DYPCEOI</b>
---	---	---

- Example: `tcp.flags.syn == 1` to display packets with SYN flag.
- To show only Facebook traffic: `ip.addr == x.x.x.x` (replace with Facebook IP address).

## Steps

### a. Capture all TCP traffic to/from Facebook:

- Open Wireshark and start capturing.
- Login to Facebook.
- Stop capture after login completes.
- Use **Display Filter**: `tcp && ip.addr == <Facebook IP>`

### b. Capture all HTTP traffic to/from Facebook:

- Apply **Display Filter**: `http && ip.addr == <Facebook IP>`
- Note: Facebook uses HTTPS, so HTTP data may be limited.

### c. Display Filter for TCP Flags (SYN, PSH, RST):

- Use:
  - `tcp.flags.syn == 1`
  - `tcp.flags.psh == 1`
  - `tcp.flags.rst == 1`
- Count number of packets with each flag.

### d. Count packets:

- Count total **TCP** packets to/from Facebook.
- Count total **HTTP** packets among those.
- Use filters like:
  - `ip.addr == <Facebook IP> && tcp`
  - `ip.addr == <Facebook IP> && http`

## output:

## conclusion:



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

## **Experiment No: 7**

**Study and Analyze the performance of HTTP, HTTPS and FTP protocol  
using Packet tracer tool..**

**Name of the Student:**

**TE**  
Date:

Mark: /10

**Signature of the Course In-charge:**

**Signature of the HOD:**



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

## Assignment No: 07

**Problem Definition:** Study and analyze the performance of HTTP, HTTPS and FTP protocol using Packet tracer tool.

The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network.

FTP employs a client-server architecture whereby the client machine has an FTP client installed and establishes a connection to an FTP server running on a remote machine. After the connection has been established and the user is successfully authenticated, the data transfer phase can begin.

Worth noting: Although FTP does support user authentication, all data is sent in clear text, including usernames and passwords. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS) or replaced with SSH File Transfer Protocol (SFTP).

Let's now do FTP configuration in Packet Tracer:

1. Build the network topology.





---

**Dr. D. Y. Patil**

**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**

**President, DYPEF**

**Dr. Suresh Mali**

**Principal, DYPCEOI**

---

2. Configure static IP addresses on the Laptop and the server.



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

Laptop: IP address: 192.168.1.1 Subnet Mask: 255.255.255.0

Server: IP address: 192.168.1.2 Subnet Mask: 255.255.255.0

3. Now try using an FTP client built in the Laptop to send files to an FTP server configured in the Server.

From the Laptop's command prompt, FTP the server using the server IP address by typing:  
ftp 192.168.1.2

Provide the username(cisco) and password(cisco) [which are the defaults] for ftp login.

```
C:\>
C:\>ftp 192.168.1.2
Trying to connect...192.168.1.2
Connected to 192.168.1.2.
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

ftp from laptop.PNG

You are now in the FTP prompt .

PC0 has an FTP client which can be used to read, write, delete and rename files present in the FTP server.

The FTP server can be used to read and write configuration files as well as IOS images. Additionally, the FTP server also supports file operations such rename, delete and listing directory.

With that in mind, we can do something extra. So let's do this:

4. Create a file in the Laptop then upload it to the server using FTP.

To do this, open the Text Editor in the Laptop, create a file and give it your name of choice. Type any text in the editor then save your file. e.g. myFile.txt.



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

5. Now upload the file from the Laptop to the server using FTP. (An FTP connection has to be started first. But this is what we've done in step 3)

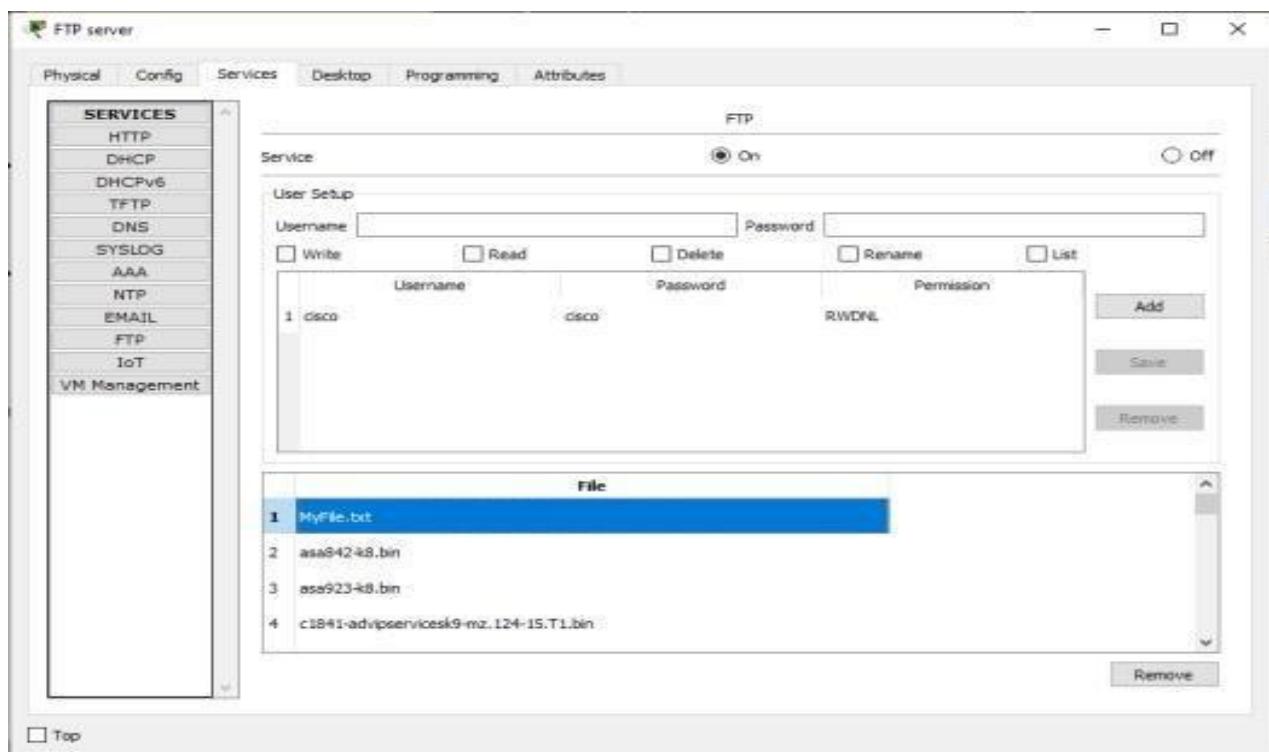
So to do an FTP upload, we'll type:

```
put MyFile.txt
```

```
ftp>
ftp>put MyFile.txt
Writing file MyFile.txt to 192.168.1.2:
File transfer in progress...
[Transfer complete - 47 bytes]
47 bytes copied in 0.023 secs (2043 bytes/sec)
ftp>
```

put MyFile to FTP directory.PNG

6. Once file upload is successful, go to the Server FTP directory to verify if the file sent has been received . To do this, go to Server-> Services->FTP. Here look for MyFile.txt sent from the laptop.





**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

MyFile.txt really send to sever.PNG

Something extra: To check other FTP commands supported by the FTP client running on the Laptop(or PC), you can use a question mark (?) on the Laptop's command prompt as shown below:

All FTP commands supported

You can see the put command that we used to upload our file to the FTP server. Other commands listed include:

get—used to get(download) a file from the server.

For example: get MyFile.txt

delete— to delete a file in the FTP directory with the server

For example: delete

MyFile.txt Rename— used

to Rename a file cd – used

to change directory.

For example, we can open an HTTP directory in the server by typing: cd /http. This will change the current directory from FTP directory to HTTP directory

Once the http directory is open, you can upload a file to the HTTP server. You're now uploading a file to an HTTP folder(directory) using FTP.

For example: put MyFile.txt

```
ftp>cd /http
ftp>
Working directory changed to /http successfully
ftp>put MyFile.txt

Writing file MyFile.txt to 192.168.1.2:
File transfer in progress...
[Transfer complete - 47 bytes]
47 bytes copied in 0.01 secs (4700 bytes/sec)
```

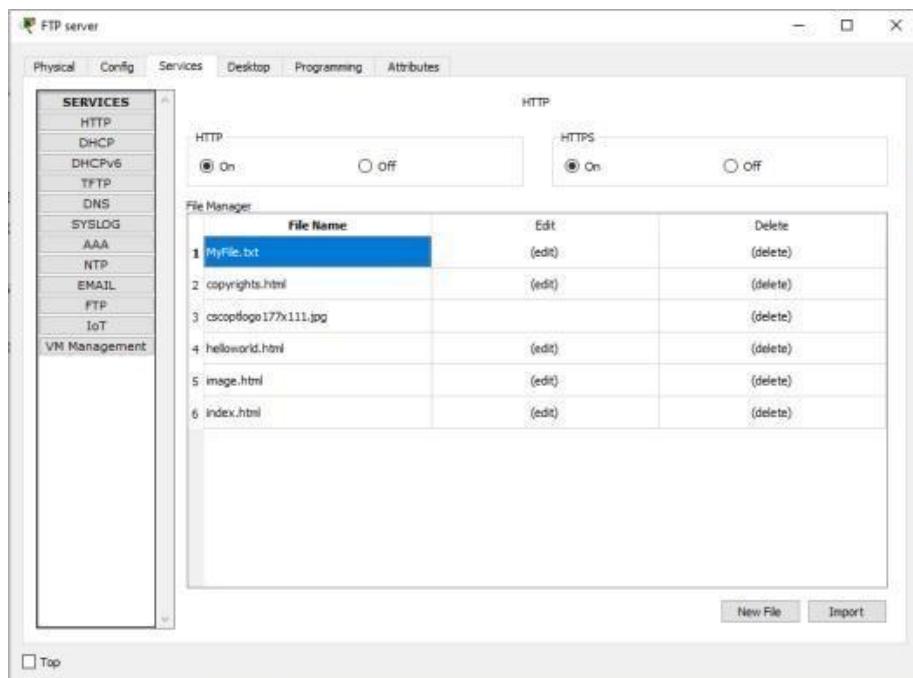


**Dr. D. Y. Patil**                   **Dr. Sushant Patil**                   **Dr. Suresh Mali**  
**Founder, Dr. D. Y. Patil Group**   **President, DYPEF**                   **Principal, DYPCEOI**

To see this working, let's open an HTTP directory and upload(put) a file to it using FTP:

changing directory then put files to HTTP directory using FTP

You can now check up in the HTTP directory in the server and verify that the file uploaded from the Laptop(MyFile.txt) is well received:



MyFile.txt really send to HTTP server

Notice that we are uploading files to an HTTP Server directory using File Transfer Protocol.(FTP). This is what actually happens when you use an FTP client such as FileZilla client to upload files to a website. In our case here, we are using an FTP client built-in the Laptop.

This may interest you: The first FTP client applications were command-line programs developed before operating systems had graphical user interfaces, and are still shipped with most Windows and Linux operating systems. (Actually this is what we have been using this far). Many FTP clients(e.g. FileZilla) and automation utilities have since been developed for desktops, servers, mobile devices, and hardware. FTP has also been incorporated into productivity applications, such as HTML editors.

We'll create an html file in our Laptop, upload it to HTTP server directory using FTP, then try to access the file from the Laptop's browser.

On the Laptop, open the text editor, then type some markup(html) and save the file with the extension .html. See all this below:



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

```
<html>
<head>
<title> my File</title>
</head>
<body>
WAOH! WAOH! WAOH!
</body>
</html>
```

File2 HTML code

```
C:\>ftp 192.168.1.2
Trying to connect...192.168.1.2
Connected to 192.168.1.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(anonymous mode On)
ftp>cd /http
ftp>
Working directory changed to /http successfully
ftp>put File2.html
Writing file File2.html to 192.168.1.2:
File transfer in progress...
[Transfer complete - 136 bytes]
136 bytes copied in 0.041 secs (3317 bytes/sec)
ftp>
```

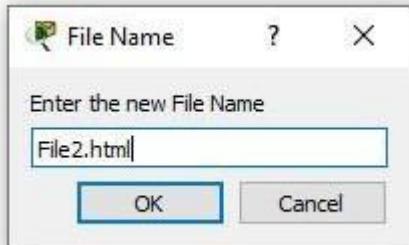
Save your file as an html file like this:



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**



File2.html.PNG

Now upload the file( File2.html) to the HTTP server using FTP. This is easy. We've already done it previously!

If you're already in the HTTP directory, you just need to type: put File2.html. If no, first ftp the server(ftp 192.168.1.2), provide the login username(cisco) and password(cisco); change the current directory to HTTP(cd /http) , and finally upload the html file onto the HTTP directory(put File2.html)

```
C:\>ftp 192.168.1.2
Trying to connect...192.168.1.2
Connected to 192.168.1.2.
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
 (passive mode On)
ftp>cd /http
ftp>
Working directory changed to /http successfully
ftp>put File2.html

Writing file File2.html to 192.168.1.2:
File transfer in progress...
[Transfer complete - 136 bytes]

136 bytes copied in 0.041 secs (3317 bytes/sec)
ftp>
```

Sending File2.html to HTTP directory.PNG

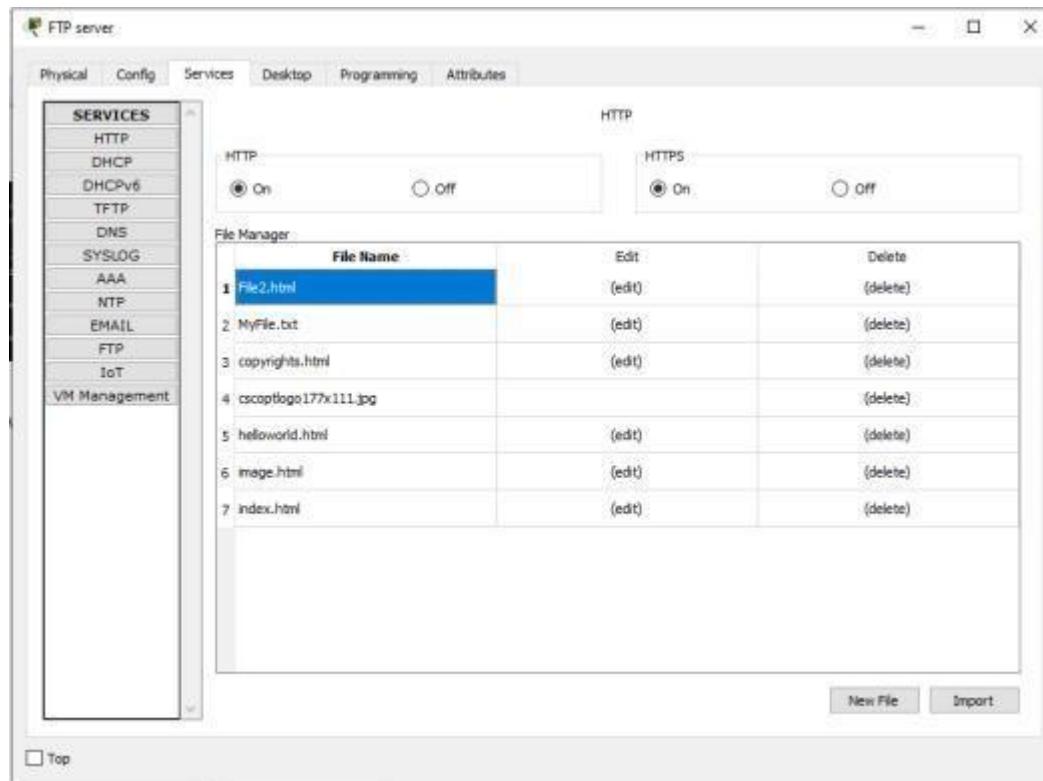
Check whether the html file uploaded has been received in the HTTP directory: Go to Server->Services-> HTTP. Then look up for the file in the File Manager.



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

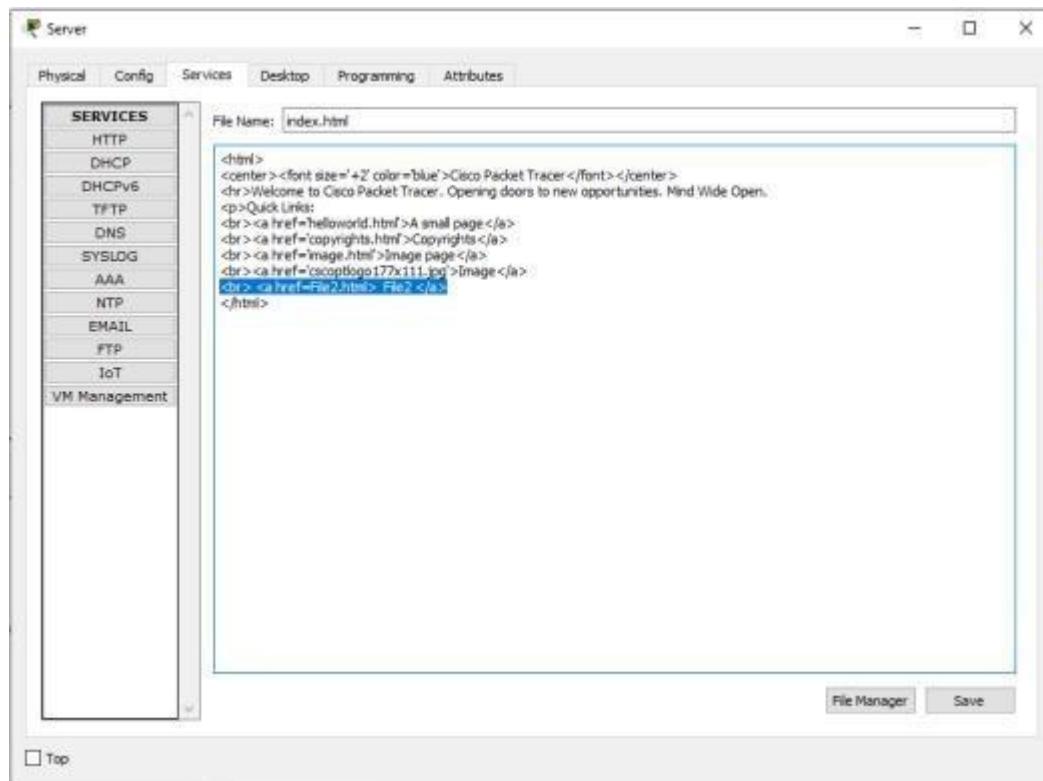


File2 HTML really uploaded into HTTP directory.PNG

Now edit index.html file in the HTTP directory so as to include a link to File2 that we've just uploaded. This will make File2 accessible from the Laptop's browser. To do this, locate index.html then click edit. Proceed to edit it as shown below. Then save and accept overwrite. Index.html editing to include File2 html.PNG.



**Dr. D. Y. Patil**                   **Dr. Sushant Patil**                   **Dr. Suresh Mali**  
**Founder, Dr. D. Y. Patil Group**   **President, DYPEF**                   **Principal, DYPCEOI**



Finally, try to access the newly uploaded file from the Laptop's browser.

So go to the Laptop's browser and access the server using the server's IP address. By doing this, the browser is making an http request to the server. The server will respond to the Laptop with the index.html file containing a link to File2 which we've uploaded from the Laptop using FTP.

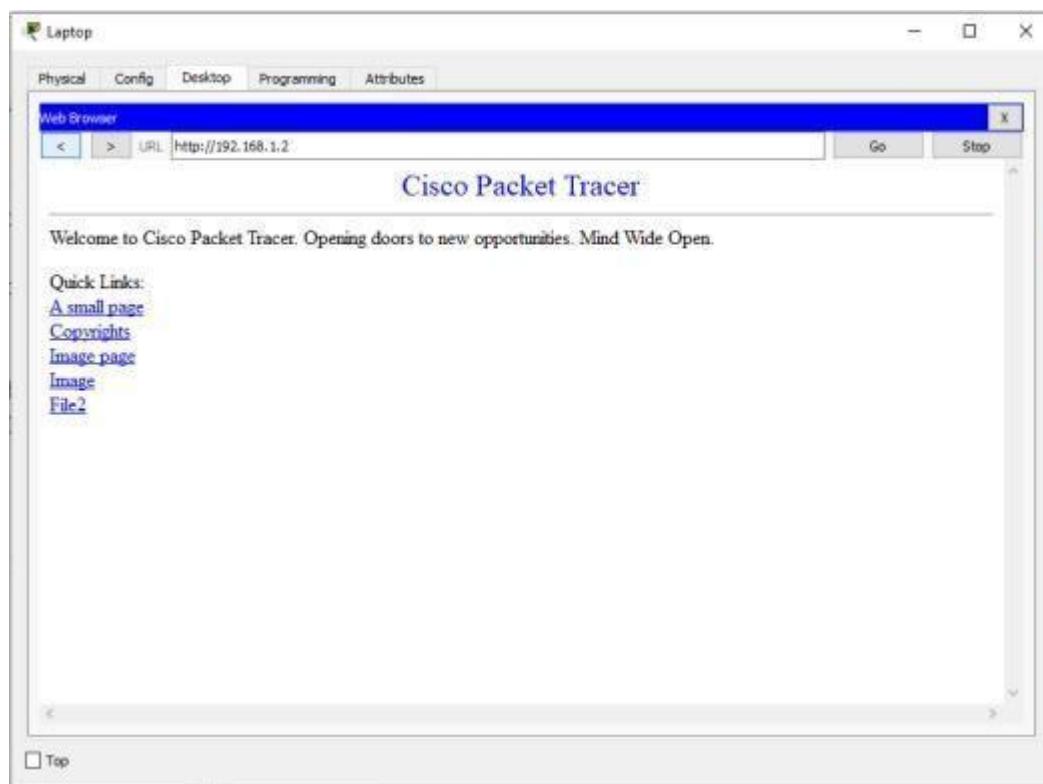
Http response with File2.PNG



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**



Click File2 link to view the contents of the file in the browser.

**Conclusion::** Successfully studied and Analyze the performance of HTTP, HTTPS and FTP protocol using Packet tracer tool.



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

## **Experiment No: 8**

**To study the SSL protocol by capturing the packets using Wireshark tool while visiting any SSL secured website (banking, e-commerce etc.)**

**Name of the Student:**  
**Class:**

**Date:**

**TE**

**Mark: /10**

**Signature of the Course In-charge:**

**Signature of the HOD:**

## **Assignment No: 08**



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

### **Title:**

To study the SSL protocol by capturing the packets using Wireshark tool while visiting any SSL secured website (banking, e-commerce etc.)

### **Outcomes:**

Retrieve SSL protocol by capturing the packets using Wireshark.

### **Theory:**

**SSL, or Secure Sockets Layer,** is an encryption-based Internet security protocol. It was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern TLS encryption used today.

### **How does SSL/TLS work?**

In order to provide a high degree of privacy, SSL encrypts data that is transmitted across the web. This means that anyone who tries to intercept this data will only see a garbled mix of characters that is nearly impossible to decrypt.

SSL initiates an authentication process called a handshake between two communicating devices to ensure that both devices are really who they claim to be.

SSL also digitally signs data in order to provide data integrity, verifying that the data is not tampered with before reaching its intended recipient.

There have been several iterations of SSL, each more secure than the last. In 1999 SSL was updated to become TLS.

### **Why is SSL/TLS important?**

Originally, data on the Web was transmitted in plaintext that anyone could read if they intercepted the message. For example, if a consumer visited a shopping website, placed an order, and entered their credit card number on the website, that credit card number would travel across the Internet unconcealed.



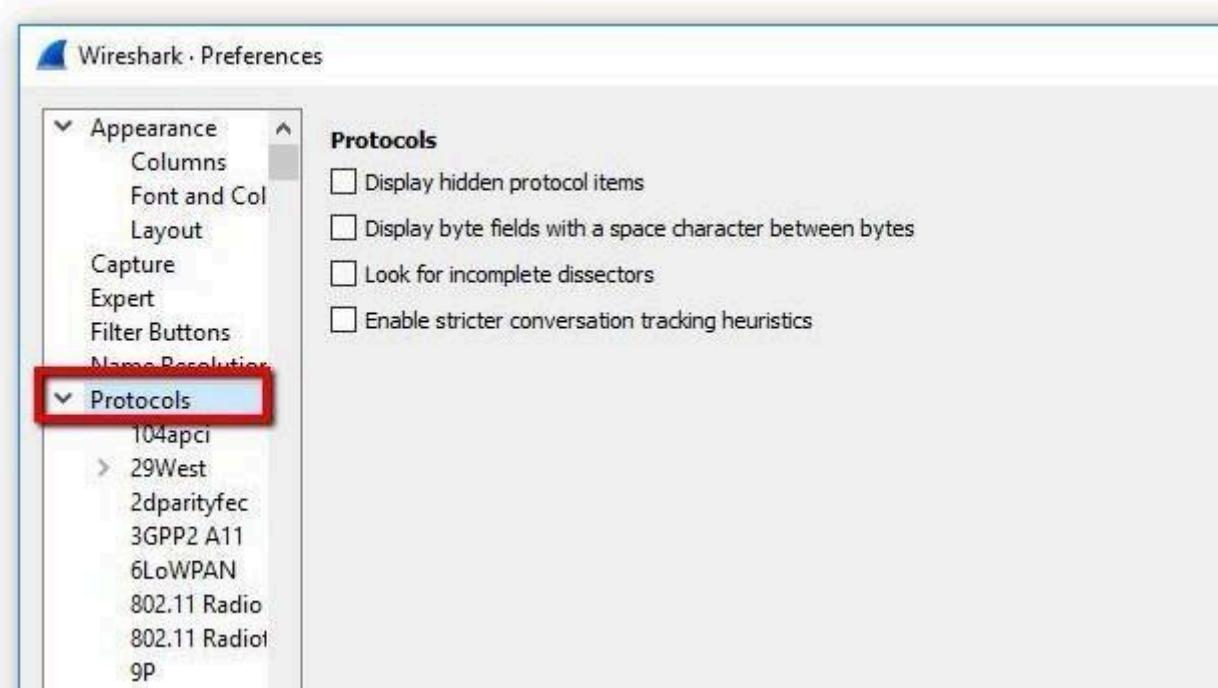
**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

## Configure Wireshark to decrypt SSL

Once your browser is logging pre-master keys, it's time to configure Wireshark to use those logs to decrypt SSL.



Open Wireshark and click **Edit**, then **Preferences**. The **Preferences** dialog will open, and on the left, you'll see a list of items. Expand **Protocols**, scroll down, then click **SSL**.

## Capture the session and decrypt SSL

The final step is to capture a test session and make sure that Wireshark decrypts SSL successfully.

- Start an unfiltered capture session, minimize it, and open your browser.
- Visit a secure site in order to generate data, and optionally set a display filter of 'ssl' to minimize the session noise.
- Click on any frame containing encrypted data.

In my case, I'll select one that contains HTTP traffic with text/HTML encoding, since I'd like to see the source code the web server is sending to my browser. But any encrypted transmissions that use a pre-master secret or private key will work with this method. That includes all data utilizing Perfect Forward Encryption (PFE) through Diffie-Hellman or comparable key exchanges.



**Dr. D. Y. Patil**

**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**

**President, DYPEF**

**Dr. Suresh Mali**

**Principal, DYPCEOI**

ssl							
No.	Time	Source	Destination	Protocol	Length	Info	
708	18.596638	192.168.1.2	192.168.1.219	HTTP	619	HTTP/1.1 404 Not Found (text/html)	
712	23.494173	192.168.1.219	192.168.1.2	HTTP	619	GET / HTTP/1.1	
713	23.501821	192.168.1.2	192.168.1.219	TLSv1.1	1514	[SSL segment of a reassembled PDU]	
715	23.501824	192.168.1.2	192.168.1.219	TLSv1.1	669	HTTP/1.1 200 OK (text/html)	
717	24.390387	192.168.1.219	192.168.1.2	HTTP	539	GET / HTTP/1.1	
718	24.397797	192.168.1.2	192.168.1.219	TLSv1.1	1514	[SSL segment of a reassembled PDU]	
720	24.397799	192.168.1.2	192.168.1.219	TLSv1.1	669	HTTP/1.1 200 OK (text/html)	
722	24.422796	192.168.1.219	192.168.1.2	HTTP	507	GET /icons/openlogo-75.png HTTP/1.1	
723	24.426900	192.168.1.2	192.168.1.219	TLSv1.1	1514	[SSL segment of a reassembled PDU]	

Once you've selected an encrypted data frame, look at the **Packet byte view**, and specifically the tabs underneath the view. You should see an entry for **Decrypted SSL data**, among others.

0030	9e 03 80 14 6f a2 9c 6c 53 4e 53 89 24 70 2e 1f	...o...l SNS-\$p..
0040	ce 5d 3e 98 7c 73 fd f1 6a fa eb dd 0d 59 9a 44	...]> s... j.....Y.D
0050	90 bb 5f de 7e 78 7f 45 06 a3 30 fc d7 cb ab 30	...~x.E ..0.....0
0060	bc 9e 5e 93 7f bf 9b fe f8 81 1c 05 87 64 aa 68	..^..... d-h
0070	aa b9 e1 32 a5 22 0c 6f 7e 1a 90 c1 d2 98 6c 1c	...2."o ~.....1.
0080	86 eb f5 3a 58 bf 0c a4 5a 84 d3 4f e1 23 d2 3a	....:X... Z..0.#::
0090	c2 cd fe eb c8 54 76 06 b1 89 07 97 07 13 cb f0	....:Tv.....
00a0	31 11 a9 be e8 20 73 74 76 76 e6 76 c3 5a 42 26	1.... st vv.v.ZB&
00b0	4b 46 63 fc 02 5f 13 66 28 c1 1d 23 f6 df 9c af	KFc... f ( ..#....

Frame (669 bytes) Reassembled TCP (3077 bytes) **Decrypted SSL (3023 bytes)** Decrypted SSL (8 bytes) Reassem

Bytes 0-3022: SSL segment data (ssl.segment.data)

You'll notice that my session still looks like it's full of garbage, and no HTML is visible. That's because my web server (and most Apache servers) use GZIP compression by default.

00e0	74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d	t/html; charset=
00f0	55 54 46 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 74	UTF-8" / >.. <t
0100	69 74 6c 65 3e 41 70 61 63 68 65 32 20 44 65 62	itle>Apa che2 Deb
0110	69 61 6e 20 44 65 66 61 75 6c 74 20 50 61 67 65	ian Defa ult Page
0120	3a 20 49 74 20 77 6f 72 6b 73 3c 2f 74 69 74 6c	: It wor ks</title>
0130	65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79	e>.. < style ty
0140	70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 6d 65	pe="text /css" me
0150	64 69 61 3d 22 73 63 72 65 65 6e 22 3e 0a 20 20	dia="scr een">.
0160	2a 20 7b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20	* { margin:
0170	30 70 78 20 30 70 78 20 30 70 78 20 30 70 78 3b	0px 0px 0px 0px;

Frame (669 bytes) Reassembled TCP (3077 bytes) Decrypted SSL (3023 bytes) Decrypted SSL (8 bytes) Reassem

When you click the **Uncompressed entity body** tab, which only shows up in this case with SSL decryption enabled, you can view the source code of the site. For instance, here's the title element of the default Apache page in plaintext.



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

SSDP  
SSH  
SSL  
STANAG 5061  
STANAG 5061  
StarTeam  
Steam IHS Di  
STP  
STT  
STUN  
SIA

RSA keys list (deprecated)

Reassemble SSL records spanning multiple TCP segments

Reassemble SSL Application Data spanning multiple SSL records

Message Authentication Code (MAC), ignore "mac failed"

Pre-Shared-Key

(Pre)-Master-Secret log filename  :\\Users\\Aaron\\Documents\\Wireshark\\ssl-keys.log

In the list of options for the SSL protocol, you'll see an entry for **(Pre)-Master-Secret log filename**. Browse to the log file you set up in the previous step, or just paste the path.

When you've finished setting the **(Pre)-Master-Secret log filename**, click **OK** and return to Wireshark.

### Conclusion:

Successfully studied the SSL protocol by capturing the packets using Wireshark tool while visiting any SSL secured website (banking, e-commerce etc.)



**Dr. D. Y. Patil**  
Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**  
President, DYPEF

**Dr. Suresh Mali**  
Principal, DYPCEOI

## **Experiment No: 9**

**Illustrate the steps for implementation of S/MIME email security through Microsoft® Office Outlook.**

**Name of the Student:**

**Class:**

TE  
Date: \_\_\_\_\_

Mark: /10

**Signature of the Course In-charge:**

**Signature of the HOD:**



**Dr. D. Y. Patil**

**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**

**President, DYPEF**

**Dr. Suresh Mali**

**Principal, DYPCEOI**

**Problem Definition:** Illustrate the steps for implementation of S/MIME email security through Microsoft® Office Outlook.

Prerequisite:

**Learning Objectives:**

1. Understand the concept and working of Encrypted mails

Theory

### **MIME (Secure/Multipurpose Internet Mail Extensions)**

S/MIME allows users to send encrypted and digitally signed emails . This protocol allows recipients of the email to be certain the email they receive is the exact message that began with the sender. It also helps ensure that a message going to an outbound recipient is from a specific sender and not someone assuming a false identity.

How does S/MIME work?

S/MIME provides cryptographic-based security services like authentication, message integrity, and digital signatures. All these elements work together to enhance privacy and security for both the sender and recipient of an email.

S/MIME also works with other technologies such as Transport Layer Security (TLS) which encrypts the path between two email servers. The protocol is also compatible with Secure Sockets Layer (SSL) which masks the connection between email messages and Office 365 (a common email service) servers.



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

In addition, BitLocker works in conjunction with S/MIME protocol, which encrypts data on a hard drive in a data center so if a hacker gets access, he or she won't be able to interpret the information.

### Benefits of encrypted email

#### **1. Safeguards sensitive data**

If you're sending information like your Social Security number over email, it's important that it's not easily stolen by hackers.

#### **2. Economical**

Instead of purchasing security equipment, you can simply rely on email encryption that's integrated directly on the server.

#### **3. Timesaving**

Instead of wasting time using several programs to make sure a connection is secure, you can rely on email encryption to do most of the work for you.

#### **4. Regulation compliance**

If you work in the healthcare industry, for example, and you haven't taken the right steps to secure medical data, you could be in violation of HIPAA laws [6]. Encryption helps you avoid those missteps.

#### **5. Protects against malware**

Malicious emails sometimes contain viruses masked as innocent email attachments. If you or someone else send an attachment using encrypted email, the email has a digital signature to prove its authenticity.

### How does email encryption work?



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

If you don't want anyone but the receiver to see the contents of a message, encryption is vital. To the outsider, an encrypted email will have a bunch of random letters, digits, or symbols instead of readable text. The person with the private key to decrypt it, typically the receiver, will be able to read the email as usual.

There are generally three encryption types available:

- S/MIME encryption works as long as both the sender and recipient have mailboxes that support it. Windows Outlook is the most popular version that works with this method.  
Gmail uses it as well.
- Office 365 Message Encryption is best for users with valid Microsoft Office licenses who can use this tool to encrypt the information and files sent via email. It's also a top choice for Outlook users
- PGP/MIME is a more affordable and popular option that other email clients may prefer to use. It's reliable and integrated into many of the apps we use today

Other email products may have their own brand of encryption, but the science behind it is the same. Only senders and recipients who have exchanged keys or digital signatures can communicate within the encrypted network.

How to send encrypted email in Outlook

Encrypting email may sound complicated, but it's not. Microsoft has a reputation for providing its users with simple ways to encrypt data, from files to folders to emails, too. It makes sense that they would include built-in tools for Outlook, their proprietary email system. You don't need a



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

separate software tool or plug-in to start sending secure messages. Just follow these steps to begin.

## 1. Create a digital certificate

For Outlook users, encrypting a single email is simple. First, you must have a digital signature. To create a digital signature:

1. Start in your Outlook window and click on the File tab
2. Select Options, then Trust Center, then Trust Center Settings
3. Select Email Security, Get a Digital ID
4. You'll be asked to choose a certification authority. This is entirely up to you as most are rated the same
5. You'll receive an email with your digital certificate/ID included
6. Go back into Outlook and select Options and the Security tab
7. In the Security Settings Name field, type in a name of your choosing
8. Ensure that S/MIME is selected from the Secure Message Format box and that Default Security Settings is checked as well
9. Go to Certificates and Algorithms, select Signing Certificate, and click Choose
10. Make sure the box is checked next to Secure Email Certificate, and check the box next to "Send These Certificates with Signed Messages"
11. Click OK to save your settings and start using Outlook

## 2. Use your digital signature



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

## Now that you have a digital ID, you need to start using it:

1. Open a new message to access the Tools tab
  2. Click that, then Customize, and finally the Commands tab
  3. From Categories, select Standard
  4. From Categories, select Digitally Sign Message
- 3. Encrypt Outlook messages**
- You can now send encrypted messages to a recipient with the next steps.
1. Open the window to compose a new message and select the Options tab, then More Options
  2. Click the dialog box (triangle with arrow pointing down) in the lower-right corner
  3. Choose Security Settings and check the box next to Encrypt message contents and attachments
  4. Write your message as normal and send

After you've sent and received a message that you've both signed and encrypted, you don't have to sign it again. Outlook will remember your signature.

- 4. Encrypt all Outlook messages**



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

You can encrypt each one, or you can use the steps below to encrypt all outgoing messages in Outlook:

- Open the File tab in Outlook
- Select Options, then Trust Center, and Trust Center Settings
- From the Email Security tab, select Encrypted email
- Check the box next to Encrypt content and attachments for outgoing messages
- Use Settings to customize additional options, including certificates

#### *How to Send Encrypted Email*

Have you ever wondered about the security of your private email conversations? Whether at work, school, or home, sending emails comes with a bit of a risk. There's one thing you can do to discourage data breaches and attacks on your sensitive data, however. Use encrypted email. Learn how to practice this common-sense method for communicating in our step-by-step guide. But first, let's look at why you should embrace encryption for your email correspondence.

#### *How to Encrypt Email and Send Secure Messages*

Emails sent over an open network can be intercepted and malicious actors can see email contents, attachments, or even take over your account. To drive home the importance of email security, take a look at some alarming statistics that show the widespread cybersecurity issues that may have affected you in the past and still pose a threat today: In 2016, 3 billion Yahoo accounts were hacked. According to research by cybersecurity company, Symantec, emails with a malicious URL make up a total of 12.3% of all emails. As these numbers illustrate, emails are a point of



**Dr. D. Y. Patil**

**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**

**President, DYPEF**

**Dr. Suresh Mali**

**Principal, DYPCEOI**

vulnerability for many unsuspecting users. However, it's not all doom and gloom, there are ways to protect yourself and your information. To help safeguard against hackers and ensure your privacy is maintained, you can use encryption. Encryption ensures that your emails remain unreadable, even if they fall into the wrong hands.

**Conclusion:** Thus we have studied the steps for implementation of S/MIME email security through Microsoft® Office Outlook.ets received from / sent to Face book, and how many of each were also HTTP packets successfully.



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

## Experiment No: 10

**To study the IPsec (ESP and AH) protocol by capturing the packets using Wireshark tool.**

**Name of the Student:**

**Class:**

**TE**

Date:

Mark: /10

**Signature of the Course In-charge:**

**Signature of the HOD:**

## Assignment No: 10

**Title:** To study the IPsec (ESP and AH) protocol by capturing the packets using Wireshark tool.

**Outcomes:**

Retrieve IPsec (ESP and AH) protocol by capturing the packets using Wireshark tool.

**Theory:**

**The IP security (IPSec)** is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

**What Ports Does IPSEC Operate On?**

UDP port 500 should be opened as should IP protocols 50 and 51. UDP port 500 should be opened to allow for



**Dr. D. Y. Patil**

**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**

**President, DYPEF**

**Dr. Suresh Mali**

**Principal, DYPCEOI**

ISAKMP to be forwarded through the firewall while protocols 50 and 51 allow ESP and AH traffic to be forwarded respectively.<sup>2</sup>

### **What is ISAKMP?**

ISAKMP stands for Internet Security Association and Key Management Protocol. These are two key components of an IPSEC VPN that must be placed in order for it to function normally and protect the public traffic that is being forwarded between the client and VPN server or VPN server to VPN server.

### **What are ESP and AH?**

No, ESP is not Extra-Sensory Perception! ESP stands for Encapsulating Security Protocol and AH stands for Authentication Header.

### **Encapsulating Security Protocol**

ESP gives protection to upper layer new protocols, with a Signed area indicating where a protected data packet has been signed for integrity, and an Encrypted area which indicates the information that's protected with confidentiality. Unless a data packet is being tunneled, ESP protects only the IP data payload (hence the name), and not the IP header.<sup>3</sup>

ESP may be used to ensure confidentiality, the authentication of data origins, connectionless integrity, some degree of traffic-level confidentiality, and an anti-replay service (a form of partial sequence integrity which guards against the use of commands or credentials which have been captured through password sniffing or similar attacks).<sup>3</sup>

### **Authentication Header**

Authentication Header (AH) is a new protocol and part of the Internet Protocol Security (IPsec) protocol suite, which authenticates the origin of IP packets (datagrams) and guarantees the integrity of the data. The AH confirms the originating source of a packet and ensures that its contents (both the header and payload) have not been changed since transmission.

If security associations have been established, AH can be optionally configured to defend against replay attacks using the sliding window technique.<sup>4</sup>

### **How Do They All Work Together?**

When properly configured, an IPSEC VPN provides multiple layers of security that ensure the security mode and integrity of the data that is being transmitted through the encrypted tunnel. This way an organization can feel confident that the data has not been intercepted and altered in transit and that they can rely on what they are seeing.

### **AH and ESP protocols**

IPSec uses two distinct protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP), which are defined by the IETF.

The AH protocol provides a mechanism for authentication only. AH provides data integrity, data origin authentication, and an optional replay protection service. Data integrity is ensured by using a message digest that is generated by an algorithm such as HMAC-MD5 or HMAC-SHA.

Data origin authentication is ensured by using a shared secret key to create the message digest. Replay protection is provided by using a sequence number field with the AH header. AH authenticates IP headers and



**Dr. D. Y. Patil**

**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**

**President, DYPEF**

**Dr. Suresh Mali**

**Principal, DYPCEOI**

their payloads, with the exception of certain header fields that can be legitimately changed in transit, such as the Time To Live (TTL) field.

The ESP protocol provides data confidentiality (encryption) and authentication (data integrity, data origin authentication, and replay protection). ESP can be used with confidentiality only, authentication only, or both confidentiality and authentication. When ESP provides authentication functions, it uses the same algorithms as AH, but the coverage is different. AH- style authentication authenticates the entire IP packet, including the outer IP header, while the ESP authentication mechanism authenticates only the IP datagram portion of the IP packet.

Either protocol can be used alone to protect an IP packet, or both protocols can be applied together to the same IP packet. The choice of IPSec protocol is determined by the security needs of your installation, and is configured by the administrator. It does not have to be applied system-wide, and can be configured differently for each set of connection endpoints. For a dynamic tunnel, the choice of IPSec protocol is configured using the IpDataOffer statement in an IP security policy configuration file. For a manual tunnel, the choice of IPSec protocol is configured using the IpManVpnAction statement in an IP security policy configuration file. For more details about the [IpDataOffer statement](#) and the [IpManVpnAction statement](#), see [z/OS](#) Communications Server: IP Configuration Reference.

**Conclusion :** Successfully studied the IPsec (ESP and AH) protocol by capturing the packets using Wireshark tool.



---

**Dr. D. Y. Patil**  
Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**  
President, DYPEF

**Dr. Suresh Mali**  
Principal, DYPCEOI

---

# GROUP C



**Dr. D. Y. Patil**  
Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**  
President, DYPEF

**Dr. Suresh Mali**  
Principal, DYPCEOI

## Experiment No: 11

Installing and configuring DHCP server and assign IP addresses to client machines using DHCP server.

**Name of the Student:**

**Class:**

TE  
Date:

Mark: /10

**Signature of the Course In-charge:**

**Signature of the HOD:**

## Assignment No: 11

**Problem Definition:**  
Installing and configuring DHCP server and assign IP addresses to client machines using DHCP server

**Objective:**



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

To install DHCP server.  
To configure DHCP server.

**Input:** Pool of IP addresses, Subnet mask, Gateway IP address, Lease Time

## **Theory:**

### **Dynamic Host Configuration Protocol:**

The Dynamic Host Configuration Protocol (DHCP) is a client/server protocol designed to provide the four pieces of information for a diskless computer or a computer that is booted for the first time. DHCP is a successor to BOOTP and is backward compatible with it. Although BOOTP is considered deprecated, there may be some systems that may still use BOOTP for host configuration. The part of the discussion in this chapter that does not deal with the dynamic aspect of DHCP can also be applied to BOOTP. The DHCP client and server can either be on the same network or on different networks. Let us discuss each situation separately.

### **Same Network:**

Although the practice is not very common, the administrator may put the client and the server on the same network as shown in Figure 1.

In this case, the operation can be described as follows:

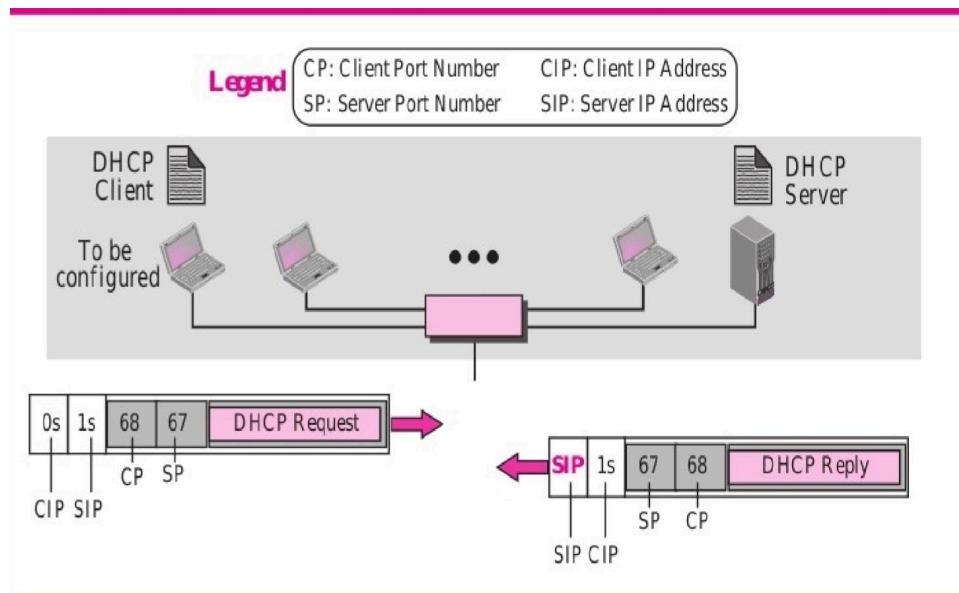


**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

1. The DHCP server issues a passive open command on UDP port number 67 and waits for a client.
2. A booted client issues an active open command on port number 68. The message is encapsulated in a UDP user datagram, using the destination port number 67 and the source port number 68. The UDP user datagram, in turn, is encapsulated in an IP datagram. The reader may ask how a client can send an IP datagram when it knows neither its own IP address (the source address) nor the server's IP address (the destination address). The client uses all 0s as the source address and all 1s as the destination address.



**Figure 1: Client and server on the same network**

3. The server responds with either a broadcast or a unicast message using UDP source port number 67 and destination port number 68. The response can be unicast because the server knows the IP address of the client. It also knows the physical address of the client, which means it does not need the services of ARP for logical to physical address mapping. However, some systems do not allow the bypassing of ARP, resulting in the use of the broadcast address.



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

## **Different Networks:**

As in other application-layer processes, a client can be in one network and the server in another, separated by several other networks. Figure 2 shows the situation.

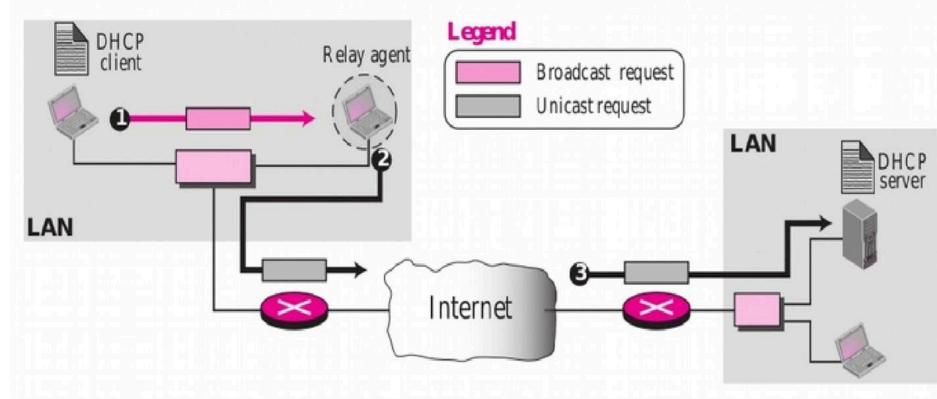


Figure 2 : Client and server on two different networks

However, there is one problem that must be solved. The DHCP request is broadcast because the client does not know the IP address of the server. A broadcast IP datagram cannot pass through any router. A router receiving such a packet discards it. Recall that an IP address of all 1s is a limited broadcast address. To solve the problem, there is a need for an intermediary. One of the hosts (or a router that can be configured to operate at the application layer) can be used as a relay. The host in this case is called a relay agent. The relay agent knows the unicast address of a DHCP server and listens for broadcast messages on port 67. When it receives this type of packet, it encapsulates the message in a unicast datagram and sends the request to the DHCP server. The packet, carrying a unicast destination address, is routed by any router and reaches the DHCP server. The DHCP server knows the message comes from a relay agent because one of the fields in the request message defines the IP address of the relay agent. The relay agent, after receiving the reply, sends it to the DHCP client.

## **DHCP packet format:**

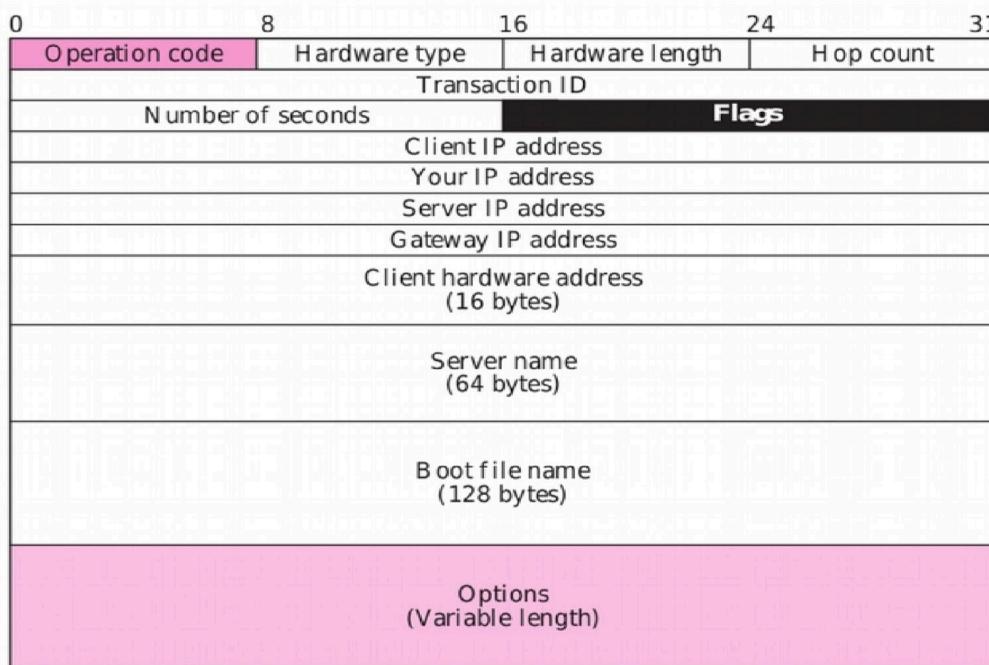
The following briefly describes each field:

- Operation code. This 8-bit field defines the type of DHCP packet: request (1) or reply (2).
- Hardware type. This is an 8-bit field defining the type of physical network. Each type of network has been assigned an integer. For example, for Ethernet the value is 1.



**Dr. D. Y. Patil**                   **Dr. Sushant Patil**                   **Dr. Suresh Mali**  
**Founder, Dr. D. Y. Patil Group**   **President, DYPEF**                   **Principal, DYPCEOI**

- ❑ Hardware length. This is an 8-bit field defining the length of the physical address in bytes. For example, for Ethernet the value is 6.
- ❑ Hop count. This is an 8-bit field defining the maximum number of hops the packet can travel.
- ❑ Transaction ID. This is a 4-byte field carrying an integer. The transaction identification is set by the client and is used to match a reply with the request. The server returns the same value in its reply.
- ❑ Number of seconds. This is a 16-bit field that indicates the number of seconds elapsed since the time the client started to boot.
- ❑ Flag. This is a 16-bit field in which only the leftmost bit is used and the rest of the bits should be set to 0s. A leftmost bit specifies a forced broadcast reply (instead of unicast) from the server. If the reply were to be unicast to the client, the destination IP address of the IP packet is the address assigned to the client. Since the client does not know its IP address, it may discard the packet. However, if the IP datagram is broadcast, every host will receive and process the broadcast message.



**Figure 3 :DHCP packet format**



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

## **Flag Format:**

- ❑ Client IP address. This is a 4-byte field that contains the client IP address. If the client does not have this information, this field has a value of 0.
- ❑ Your IP address. This is a 4-byte field that contains the client IP address. It is filled by the server (in the reply message) at the request of the client.
- ❑ Server IP address. This is a 4-byte field containing the server IP address. It is filled by the server in a reply message.
- ❑ Gateway IP address. This is a 4-byte field containing the IP address of a router. It is filled by the server in a reply message.
- ❑ Client hardware address. This is the physical address of the client. Although the server can retrieve this address from the frame sent by the client, it is more efficient if the address is supplied explicitly by the client in the request message.
- ❑ Server name. This is a 64-byte field that is optionally filled by the server in a reply packet. It contains a null-terminated string consisting of the domain name of the server. If the server does not want to fill this field with data, the server must fill it with all 0s.
- ❑ Boot filename. This is a 128-byte field that can be optionally filled by the server in a reply packet. It contains a null-terminated string consisting of the full pathname of the boot file. The client can use this path to retrieve other booting information. If the server does not want to fill this field with data, the server must fill it with all 0s.
- ❑ Options. This is a 64-byte field with a dual purpose. It can carry either additional information (such as the network mask or default router address) or some specific vendor information. The field is used only in a reply message. The server uses a number, called a magic cookie, in the format of an IP address with the value of 99.130.83.99. When the client finishes reading the message, it looks for this magic cookie. If present, the next 60 bytes are options. An option is composed of three fields: a 1-byte tag field, a 1-byte length field, and a variable-length value field. The length field defines the length of the value field, not the whole option.



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

## **DHCP client transition:**

### **INIT State :**

When the DHCP client first starts, it is in the INIT state (initializing state). The client broadcasts a DHCPDISCOVER message (a request message with the DHCPDISCOVER option), using port 67.

### **SELECTING State:**

After sending the DHCPDISCOVER message, the client goes to the selecting state. Those servers that can provide this type of service respond with a DHCPOFFER message. In these messages, the servers offer an IP address. They can also offer the lease duration. The default is 1 hour. The server that sends a DHCPOFFER locks the offered

IP address so that it is not available to any other clients. The client chooses one of the offers and sends a DHCP REQUEST message to the selected server. It then goes to the requesting state. However, if the client receives no DHCPOFFER message, it tries four more times, each with a span of 2 seconds. If there is no reply to any of these DHCP DISCOVER s, the client sleeps for 5 minutes before trying again.

### **REQUESTING State:**

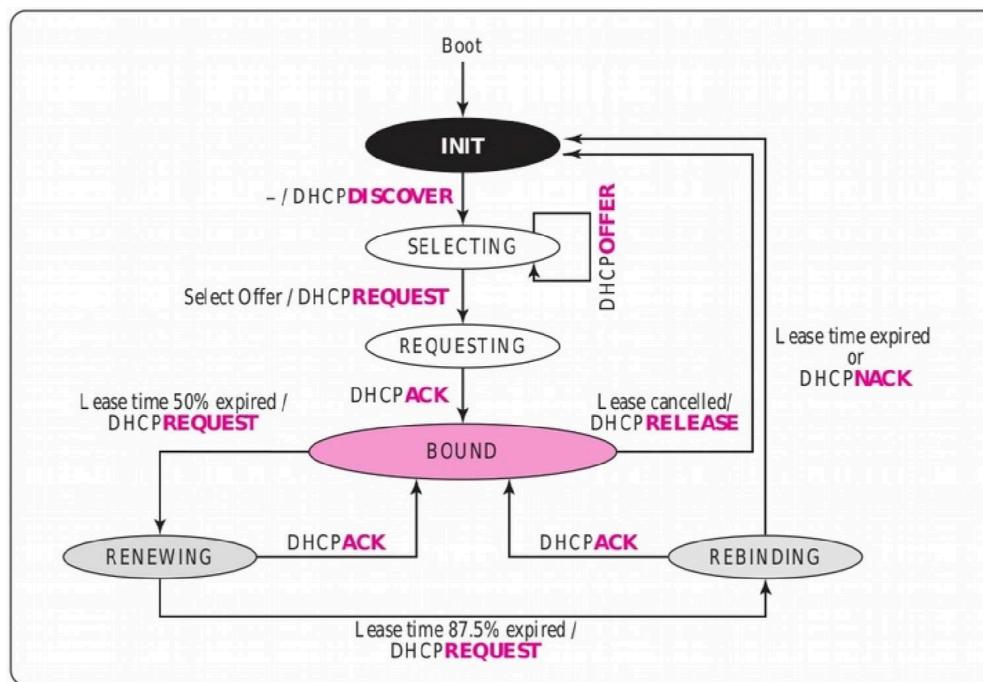
The client remains in the requesting state until it receives a DHCPACK message from the server that creates the binding between the client physical address and its IP address. After receipt of the DHCPACK, the client goes to the bound state.

### **BOUND State:**

In this state, the client can use the IP address until the lease expires. When 50 percent of the lease period is reached, the client sends another DHCPREQUEST to ask for renewal. It then goes to the renewing state. When in the bound state, the client can also cancel the lease and go to the initializing state.



**Dr. D. Y. Patil** **Dr. Sushant Patil** **Dr. Suresh Mali**  
**Founder, Dr. D. Y. Patil Group** **President, DYPEF** **Principal, DYPCEOI**



**Figure 4: DHCP client transition**

### **RENEWING State:**

The client remains in the renewing state until one of two events happens. It can receive a DHCPACK, which renews the lease agreement. In this case, the client resets its timer and goes back to the bound state. Or, if a DHCPACK is not received, and 87.5 percent of the lease time expires, the client goes to the rebinding state.

### **REBINDING State**

The client remains in the rebinding state until one of three events happens. If the client receives a DHCPNACK or the lease expires, it goes back to the initializing state and tries to get another IP address. If the client receives a DHCPACK, it goes to the bound state and resets the timer.

### **Configuring a DHCP Server:**

- You can configure a DHCP server using the configuration file `/etc/dhcpd.conf`.
- DHCP also uses the file `/var/lib/dhcp/dhcpd.leases` to store the client leasedatabase.



<b>Dr. D. Y. Patil</b> <b>Founder, Dr. D. Y. Patil Group</b>	<b>Dr. Sushant Patil</b> <b>President, DYPEF</b>	<b>Dr. Suresh Mali</b> <b>Principal, DYPCEOI</b>
---	---	---

- This file should not be modified by hand. DHCP lease information for each recently assigned IP address is automatically stored in the lease database. The information includes the length of the lease, to whom the IP address has been assigned, the start and end dates for the lease, and the

MAC address of the network interface card that was used to retrieve the lease

- Many RPM packages don't automatically install a /etc/dhcpd.conf file, but you can find a sample copy of dhcpd.conf in the following directory which you can always use as a guide:
- /usr/share/doc/dhcp-<version-number>/dhcpd.conf.sample
- # cp /usr/share/doc/dhcp-3.0pl1/dhcpd.conf.sample \ /etc/dhcpd.conf

### **/etc/dhcpd.conf**

- There are two types of statements in the configuration file:
  - Parameters — state how to perform a task, whether to perform a task, or what network configuration options to send to the client.
  - Declarations — describe the topology of the network, describe the clients, provide addresses for the clients, or apply a group of parameters to a group of declarations.
- Some parameters must start with the option keyword and are referred to as options.  
**/etc/dhcpd.conf**
- The routers, subnet-mask, domain-name, domain-name-servers, and time-offset options are used for any host statements declared below it
- You must include a subnet declaration for every subnet in your network. If you do not, the DHCP server will fail to start
- Clients are assigned an IP address within the range
- To assign an IP address to a client based on the MAC address of the network interface card, use the hardware ethernet parameter within a host declaration.

### **/etc/dhcpd.conf**

```
subnet 192.168.1.0 netmask 255.255.255.0 { #  
The range of IP addresses the server will issue to  
#DHCP enabled PC clients booting up on the  
network range 192.168.1.10 192.168.1.100;  
range 192.168.1.201
```



<b>Dr. D. Y. Patil</b> <b>Founder, Dr. D. Y. Patil Group</b>	<b>Dr. Sushant Patil</b> <b>President, DYPEF</b>	<b>Dr. Suresh Mali</b> <b>Principal, DYPCEOI</b>
---	---	---

```
192.168.1.220; # Set the amount of time in
seconds that
# a client may keep the IP address
default-lease-time 86400;
max-lease-
time 86400;
# Set the default gateway to be used
by # the PC clients
option routers 192.168.1.1;
# Don't forward DHCP requests from
this # NIC interface to any other NIC
interfaces optionip-forwarding off;
```

### **/etc/dhcpd.conf**

```
# Set the broadcast address and subnet
mask # to be used by the DHCP clients
option broadcast-address 192.168.1.255;
option
subnet-mask 255.255.255.0;
# Set the DNS server to be used by the DHCP clients
option domain-name-servers 192.168.1.100;
# If you specify a WINS server for your Windows clients,
# you need to include the following option in the dhcpd.conf file: optionnetbios-name- servers
192.168.1.100;
```

### **Starting and Stopping the Server:**

- Before you start the DHCP server for the first time, it will fail unless there is an existing dhcpd.leases file. To create the file if it does not exist, use the command
- #touch /var/lib/dhcp/dhcpd.leases
- If you have more than one network interface attached to the system, but you only want the DHCP server to start on one of the interface, you can configure the DHCP server to start only on that device. In

/etc/sysconfig/dhcpd, add the name of the interface to the list of DHCPDARGS:

- DHCPDARGS=eth0
- Use the chkconfig command to get DHCP configured to start at boot:
- # chkconfigdhcpd on
- Use the /etc/init.d/dhcpd script to start/stop/restart DHCP after booting



<b>Dr. D. Y. Patil</b> <b>Founder, Dr. D. Y. Patil Group</b>	<b>Dr. Sushant Patil</b> <b>President, DYPEF</b>	<b>Dr. Suresh Mali</b> <b>Principal, DYPCEOI</b>
---	---	---

- #  
/etc/init.d/dhcpd start  
# /etc/init.d/dhcpd  
stop  
# /etc/init.d/dhcpd restart

### **Configuration Steps:**

- 1 . To install DHCP server on ubuntu, Type following command on terminal. – sudo apt-get install isc-dhcp-server
- 2 . Now we should configure DHCP server. Configuration file is stored at location /etc/dhcp/dhcpd.conf .
- Use gedit to edit dhcpd.conf  
# A slightly different configuration for an internal subnet.  
subnet 172.16.5.0 netmask 255.255.255.0  
{ range 172.16.5.2 172.16.5.5; option domain-name-servers 8.8.8.8; option routers 172.16.1.1; option broadcast-address 172.16.5.255;  
  
default-lease-time 600; max-lease-time 7200; }
- 3 . Now restart service by using following command. – sudo service isc-dhcp-server restart
- 4 . Now on client computer, in network configuration setting just choose automatic configuration. Thats it client get IP address automatically

### **Steps for installation of Software on Remote Machine:**

- 1. Type following command for installation of ssh in command prompt–  
> sudo apt-get install ssh
- 2 . Proceed with installation steps on Remote machine
- 3. After installation, for obtaining remote access, type following command–  
> sudosshhostname@ipaddress  
– For Example. >sudossh student@172.25.28.60
- 4 . Enter the password for host machine then enter the password for remote machine.
- 5. After login for installation of any package such as SBCL package type following command:-> sudo apt-get installpackage\_name. – Example: >sudo apt-get installsbc



---

**Dr. D. Y. Patil** **Dr. Sushant Patil** **Dr. Suresh Mali**  
**Founder, Dr. D. Y. Patil Group** **President, DYPEF** **Principal, DYPCEOI**

---

*Conclusion:*

Hence we Installed and Configured DHCP and studied Installation of Software .



**Dr. D. Y. Patil**  
Founder, Dr. D. Y. Patil Group

**Dr. Sushant Patil**  
President, DYPEF

**Dr. Suresh Mali**  
Principal, DYPCEOI

## Experiment No: 12

**Write a program for DNS lookup. Given an IP address input, it should return URL and vice versa.**

**Name of the Student:**

**Class:**

**TE**

Date:

Mark: /10

**Signature of the Course In-charge:**

**Signature of the HOD:**



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

### Problem Definition:

Write a program for DNS lookup. Given an IP address input, it should return URL and vice versa.

#### 1.1 Prerequisite:

1. IP Address and OSI & TCP/IP Model.
2. Role of different servers.
3. Working of internet.

#### 1.2 Learning Objectives:

1. Understand what is Domain Name System and DNS lookup working.
2. Understand what is DNS Structure and Hierarchy.

#### 1.3 New Concepts:

1. Name Server and Domain Name System.
2. DNS lookup, Zone

#### 1.4 Theory

##### 1.4.1 Introduction

The Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.

it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, the Domain Name System is an essential component of the functionality on the Internet that has been in use since 1985.

#### HOST.TXT files:

The ARPANET, the predecessor of the Internet, had no distributed host name database. Each network node maintained its own map of the network nodes as needed and assigned those names that were memorable to the users of the system.

The hosts file contains lines of text consisting of an IP address in the first text field followed by one or more host names. Each field is separated by white space – tabs are often preferred for historical reasons, but spaces are also used. Comment lines may be included; they are indicated by an octothorpe (#) in the first position of such lines. Entirely blank lines in the file are ignored. For example, a typical hosts file may contain the following:

127.0.0.1 localhost loopback

::1 localhost



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**

#### 1.4.2 Domain Name Space

The domain name space refers a hierarchy in the internet naming structure. This hierarchy has multiple levels (from 0 to 127), with a root at the top. The following diagram shows the domain name space hierarchy:

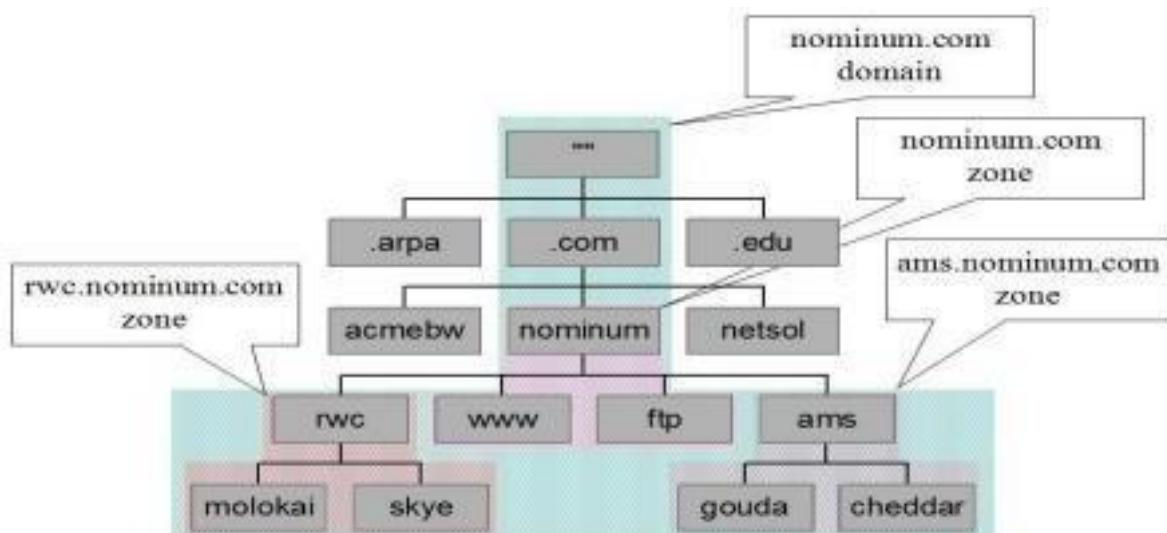
#### 1.4.3 Name Server

Name server contains the DNS database. This database comprises of various names and their corresponding IP addresses. Since it is not possible for a single server to maintain entire DNS database, therefore, the information is distributed among many DNS servers.

- Hierarchy of server is same as hierarchy of names.
- The entire name space is divided into the zones

#### 1.4.4 Zones

Zone is collection of nodes (sub domains) under the main domain. The server maintains a database called zone file for every zone.



If the domain is not further divided into sub domains then domain and zone refers to the same thing.

The information about the nodes in the sub domain is stored in the servers at the lower levels however; the original server keeps reference to these lower levels of servers.

#### 1.4.5 Types of Name Servers

Following are the three categories of Name Servers that manages the entire Domain Name System:

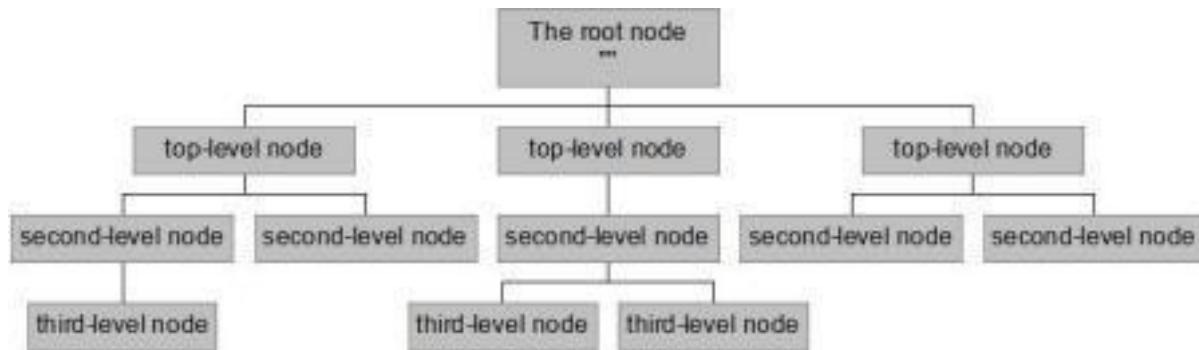
1. Root Server
2. Primary Server
3. Secondary Server



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPEF**

**Dr. Suresh Mali**  
**Principal, DYPCEOI**



#### 1.4.5.1 Root Server

Root Server is the top level server which consists of the entire DNS tree. It does not contain the information about domains but delegates the authority to the other server

#### 1.4.5.2 Primary Servers

Primary Server stores a file about its zone. It has authority to create, maintain, and update the zone file.

#### 1.4.5.3 Secondary Server

Secondary Server transfers complete information about a zone from another server which may be primary or secondary server. The secondary server does not have authority to create or update a zone file.

### 2.1 How does DNS work?

DNS servers answer questions from both inside and outside their own domains. When a server receives a request from outside the domain for information about a name or address inside the domain, it provides the authoritative answer. When a server receives a request from inside its own domain for information about a name or address outside that domain, it passes the request out to another server -- usually one managed by its internet service provider. If that server does not know the answer or the authoritative source for the answer, it will reach out to the DNS servers for the top-level domain -- e.g., for all of .com or .edu. Then, it will pass the request down to the authoritative server for the specific domain -- e.g., techtarget.com or stkate.edu; the answer flows back along the same path.

### 2.2 How DNS Lookup Works

By now, you know that there are different servers hosting databases that contain the IP addresses of different domains and their sub-domains. You also know that there are Root Servers that hold the IP address of servers hosting Top Level Domains. These Root Servers help in reaching the servers containing databases that hold IP address of the main domain name. If there are sub-domains, their address can be on the same servers as of the main domain name or on a different server. All these servers are accessible for finding out the IP address of the exact URL that you need to use.

- **Forward Lookup:** When a name query is send to the DNS server against to IP address, it is generally said a forward lookup.
- **Reverse Lookup:** DNS also provides a reverse lookup process, enabling clients to use a known IP address during a name query and look up a computer name based on its address.



**Dr. D. Y. Patil**

**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**

**President, DYPEF**

**Dr. Suresh Mali**

**Principal, DYPCEOI**

The process of finding out the IP address of any URL on the Internet is known as DNS lookup.

To find out how DNS Lookup works, take the following example.

**Example:** Consider a network of ten computers. Each computer has its own address so that data packets travelling in the network know where to go. There is a 11th computer that hosts a database containing the alias names of each of these ten computers and their IP addresses. While the computer users can refer to the computers using their names, the data packets need the IP addresses of the computers so that they can reach the intended recipient. If computer A needs to use the printer attached to computer B, A will check the database on 11th computer to know the IP address of B and then find out the address of printer attached to B. Only after obtaining the address of the printer, A will route the print command to printer attached to B.

In this case, the following iterations happen:

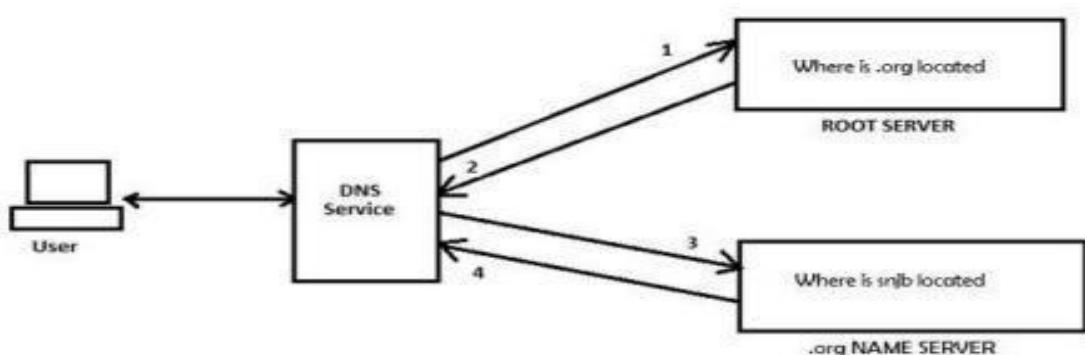
A contacts Computer

**11 A contacts B**

A contacts printer attached to B

A similar method is used to lookup DNS records. For example, when you click on <http://snjb.org>, your router will contact your default DNS Service for DNS resolution. The DNS service will contact Root Servers and ask for the IP address of server containing .org records. This address is sent back to your DNS service. The DNS service again reaches the Name Server containing addresses of .org domains and asks it for the address of <http://snjb.org>. Upon obtaining the IP address of the servers that host snjb.org, your DNS service will return the IP address to your computer which then fires up your browser to download the main webpage. This means your DNS service is sending at least two requests to receive the IP address of a simple domain name.

Following is an image that explains how DNS lookup works:





<b>Dr. D. Y. Patil</b> <b>Founder, Dr. D. Y. Patil Group</b>	<b>Dr. Sushant Patil</b> <b>President, DYPEF</b>	<b>Dr. Suresh Mali</b> <b>Principal, DYPCEOI</b>
---	---	---

In the above case, if you were to look for <http://snjb.academiaerp.com/snjb/Login> , your DNS service had to run a request extra to know its IP address.

Since resolving DNS from scratch every time takes up time, many ISPs and DNS Service Providers create local caches that contain already resolved addresses. These are primarily the addresses they already fetched from Root Servers and other Name Servers at some point of time. In this case, when you send a request for a URL, instead of contacting the Root server directly, the DNS service would look up for the resolved address of the URL in its local DNS cache. If found, it would send the resolution back to your computer

instantly else would go ahead and resolve the DNS using the above method of contacting Root Servers and other Name Servers.

Some operating systems too contain a local cached copy of addresses that you commonly use on your computer. This too, helps in saving time while using the Internet. We will talk about DNS caches in a different article at some later point of time.

#### **Conclusion:**

Hence we conclude that we have lookup the URL which we want to visit the request is travels to local router to DNS server and it resolve the query as possible otherwise it forwards the query to next DNS hop.



*Dr. D. Y. Patil Educational Federation's*  
**Dr. D. Y. PATIL COLLEGE OF ENGINEERING & INNOVATION**  
**, AUTONOMOUS INSTITUTE AFFILIATED TO SAVITRIBAI PHULE PUNE UNIVERSITY**  
**Accredited by NAAC with "A" Grade**  
APPROVED BY AICTE, RECOGNIZED BY GOVT. OF MAHARASHTRA



**Dr. D. Y. Patil**  
**Founder, Dr. D. Y. Patil Group**

**Dr. Sushant Patil**  
**President, DYPCEF**

**Dr. Suresh Mali**  
**Principal, DYPCOEI**