



Vidyavardhini's College of Engineering & Technology  
Department of Electronics and Telecommunication Engineering



# **Vidyavardhini's**

## **College of Engineering & Technology**

Vasai Road (W)

**Department of**  
**Electronics and Telecommunication Engineering**

### **Lab Manual**

Semester	VI	Class	TE
Course Code	ECL602	Academic Year	R-2019 scheme
Course Name	Computer Communication Networks Lab		
Name of Faculty	Mrs. Ashwini Katkar		
Suppoting Staff	Mrs Madhu Lade		



# **Vidyavardhini's College of Engineering & Technology**

## **Vision**

To be a premier institution of technical education, aiming at becoming a valuable resource for industry and society.

## **Mission**

- To provide technologically inspiring environment for learning.
- To promote creativity, innovation and professional activities.
- To inculcate ethical and moral values.
- To cater personal, professional and societal needs through quality education.



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

---

**Department Vision:**

To contrive educational and research environment to serve industry and society needs in the field of electronics and telecommunication engineering.

**Department Mission:**

1. To enrich soft skills, ethical values, environmental and societal awareness.
2. To develop technical proficiency through projects and laboratory work.
3. To encourage students for lifelong learning through interaction with outside world.

**Program Education Objectives (PEOs):**

- The graduates will exhibit knowledge of mathematics, science, electronics, and communication, and will be able to apply the same in diversified field.
- The graduates will develop a habit of continuous learning while working in multidisciplinary environment.
- The graduates will grow as an individual with proficiency in technical skills, ethical values, communication skills, teamwork and professionalism.

**Program Specific Outcomes (PSOs):**

At the end of the program engineering graduate will be able to:

1. Apply the knowledge of Electronics and Communication to analyse, design and implement application specific problems with modern tools.
2. Adapt emerging technologies with continuous learning in the field of Electronics and Telecommunication engineering with appropriate solutions to real life problems.



## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

---

#### Program Outcomes (POs):

Engineering Graduates will be able to:

- **PO1. Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
- **PO2. Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
- **PO3. Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
- **PO4. Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
- **PO5. Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
- **PO6. The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
- **PO7. Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
- **PO8. Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
- **PO9. Individual and teamwork:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
- **PO10. Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
- **PO11. Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
- **PO12. Life-long learning:** Recognize the need for and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

---

<b>Sr. No.</b>	<b>Content</b>
1.	Syllabus
2.	Course Objectives and Course Outcomes
3.	Mapping of Experiments with Course Outcomes
4.	Mapping of COs with POs and PSOs
5.	List of Experiments
1.	To study Networking Devices using cisco packet tracer.
2.	To configure and compare various network topologies using cisco packet tracer
3.	To configure network to implement static routing using Cisco packet tracer.
4.	To configure network to implement dynamic routing using Cisco packet tracer.
5.	To configure DHCP using Cisco packet tracer.
6.	To configure DNS server using Cisco packet tracer.
7.	To determine optimum persistence of a p-persistence CSMA/CD network for a heavily loaded bus capacity using Netsim
8.	To study networking commands
9.	To Study the steps for installing Wireshark, the packet-sniffing tool for performing Network packet analysis.
10.	To study working with captured packets in Wireshark.
11.	To compare TCP (connection oriented) and UDP (connectionless) performance using Netsim
12.	To study the throughputs of Slow Start + Congestion avoidance (Old Tahoe) and Fast Retransmit (Tahoe) Congestion Control Algorithm



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

Course Code	Course Name	Teaching Scheme (Hrs.)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Practical	Tutorial	Total
ECL602	Computer Communication Network Laboratory	-	02	-	--	01	--	01

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Practical and Oral	Total
		Internal assessment			End Sem. Exam			
		Test 1	Test 2	Avg. of Test 1 and Test 2				
ECL602	Computer Communication Network Laboratory	--	--	--	--	25	25	50

**Lab Course Outcomes: -**

Upon completion of the computer communication networks lab, the students will be able to:

- Design a small or medium sized computer network including media types, end devices, and interconnecting devices that meets a customer's specific needs.
- Perform configurations on routers and Ethernet switches.
- Demonstrate knowledge of programming for network communications.
- Simulate computer networks and analyze the simulation results.
- Troubleshoot connectivity problems in a host occurring at multiple layers of the OSI model.
- Develop knowledge and skills necessary to gain employment as computer network engineer and network administrator.

**Laboratory plan**

Minimum of 8 practicals should be conducted and a mini project.



## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

---

#### Suggested list of experiments:

1. To study basic networking commands. (Linux/Netkit)
2. To prepare a patch cable (straight-through, crossover, rollover) using UTP, RJ-45 and crimping tool. Test the cable using a cable tester and use it in LAN.
3. To configure and compare different network topologies using Cisco Packet Tracer
4. To study and compare network hardware components using Cisco Packet Tracer
5. To configure static routes in a network using Cisco Packet Tracer.
6. To configure a network with Distance Vector Routing Protocol-RIP using Cisco Packet Tracer and check the updated routing tables.
7. To configure a network with Path Vector Routing Protocol- BGP using Cisco Packet Tracer and check the updated routing tables.

8. To configure a network with Link state Routing Protocol- OSPF using Cisco Packet Tracer and check the updated routing tables.
9. To configure a network with Hybrid Routing Protocol- EIGRP using Cisco Packet Tracer and check the updated routing tables.
10. To perform subnetting using Cisco Packet Tracer/Netkit
11. To install a network simulator (NS2.35), create a wired network and compare the performance of TCP and UDP or Compare TCP and UDP performance using Netsim
12. To Simulate and study stop and Wait protocol using NS 2.35/ C++
13. To Simulate Sliding Window protocol using NS 2.35/C++
14. To Simulate and study the implementation of TCP/IP stack using Wireshark (observe the protocols, data formats, header structures, addresses, payload sizes and encapsulation at each layer)
15. To perform HDLC bit stuffing and de-stuffing using C++
16. To configure DNS, DHCP, TELNET, FTP, SMTP server (any one) on Cisco Packet Tracer
17. To compare performance of ALOHA and Slotted ALOHA using Netsim.

**Term Work:** At least 08 Experiments covering entire syllabus must be given during the "Laboratory session batch wise". Computation/simulation based experiments are also encouraged. The experiments should be students centric and attempt should be made to make experiments more meaningful, interesting and innovative. Application oriented **one mini-project** can be conducted for a batch of maximum four students.

Term work assessment must be based on the overall performance of the student with every experiment and assignment graded from time to time. The grades will be converted to marks as per "**Credit and Grading System**" manual and should be added and averaged. Based on above scheme grading and term work assessment should be done. The practical and oral examination will be based on entire syllabus.

**Termwork marks distribution:** Journal and practical Performance: 15 marks

Attendance: 5 marks

Assignment: 5 marks



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

---

**Course Objectives**

1	To build an understanding of protocols and their functionalities.
2	To build an understanding of design of computer networks for given requirements.
3	To develop knowledge to create virtual network world for exploration, experimentation of networking concepts.
4	To build knowledge to simulate computer networks and analyse the simulation results.

**Course Outcomes**

At the end of the course, students will be able to:		Action verb	Bloom Level
ECL602.1	Design a small or medium-sized computer network including media types, end devices, and interconnecting devices that meet a customer's specific needs.	Design	Level 6
ECL602.2	Demonstrate/illustrate the use of network layer protocol, addressing and subnetting	Demonstrate	Level 3
ECL602.3	Compare routing algorithms and protocols.	Compare	Level 4
ECL602.4	Demonstrate an understanding of the significance and purpose of protocols and their use in computer networks using simulators.	Demonstrate	Level 3
ECL602.5	Troubleshoot problems in a host occurring at multiple layers of the OSI model.	Troubleshoot	Level 4
ECL602.6	Compare connectionless and connection-oriented services and protocols	Compare	Level 4





### Mapping of Experiments with Course Outcomes

Experiment	Course Outcomes					
	ECL 602.1	ECL 602.2	ECL 602.3	ECL 602.4	ECL 602.5	ECL 602.6
To study Networking Devices using cisco packet tracer.	2	2	-	-	-	-
To configure and compare various network topologies using cisco packet tracer	2	2	-	-	-	-
To configure network to implement static routing using Cisco packet tracer.	-	-	3	-	-	-
To configure network to implement dynamic routing using Cisco packet tracer.	-	-	3	-	-	-
To configure DHCP using Cisco packet tracer.	-	-	-	3	-	-
To configure DNS server using Cisco packet tracer.	-	-	-	3	-	-
To determine optimum persistence of a p-persistence CSMA/CD network for a heavily loaded bus capacity using Netsim	-	-	-	3	-	-
To study networking commands	-	-	-	-	3	-
To Study the steps for installing Wireshark, the packet-sniffing tool for performing Network packet analysis.	-	-	-	-	3	-
To study working with captured packets in Wireshark.	-	-	-	-	3	-
To compare TCP (connection oriented) and UDP (connectionless) performance using Netsim	-	-	-	-	-	3



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

---

To study the throughputs of Slow Start + Congestion avoidance (Old Tahoe) and Fast Retransmit (Tahoe) Congestion Control Algorithm	-	-	-	3	-	-
--	---	---	---	---	---	---



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

---

**Experiment 1**

**AIM:** To compare various network hardware devices using cisco packet tracer

**OBJECTIVES:** To compare Hub, switch, bridge, router and repeater

**THEORY:** Cisco network devices such as routers, switches, and other generic devices such as bridges, hubs, repeaters, and WAN emulators are available to work in the cisco packet tracer. Network devices enable the end devices to communicate with each other. These devices can be configured from the config tab. You will be able to configure routers and switches using the config tab without using Cisco commands.

**PROCEDURE:**

**HUB:**

1. Connect four PCs to a HUB in cisco packet tracer.
2. configure each PC with IP address and subnet mask.
3. select the simulation tab.
4. Edit filters for ARP and ICMP.
5. Take a simple PDU, and select a source and destination PC for it.
6. Press Auto Capture/Play button
7. observe the HUB operation.

**SWITCH:**

1. Connect four PCs to a switch in cisco packet tracer.
2. configure each PC with IP address and subnet mask.
3. select the simulation tab.
4. Take a simple PDU, and select a source and destination PC for it.
5. Press Auto Capture/Play button
6. observe the switch operation.
7. ping all other PCs from each



Vidyavardhini's College of Engineering & Technology  
Department of Electronics and Telecommunication Engineering

Scenario (Hub and Switch)

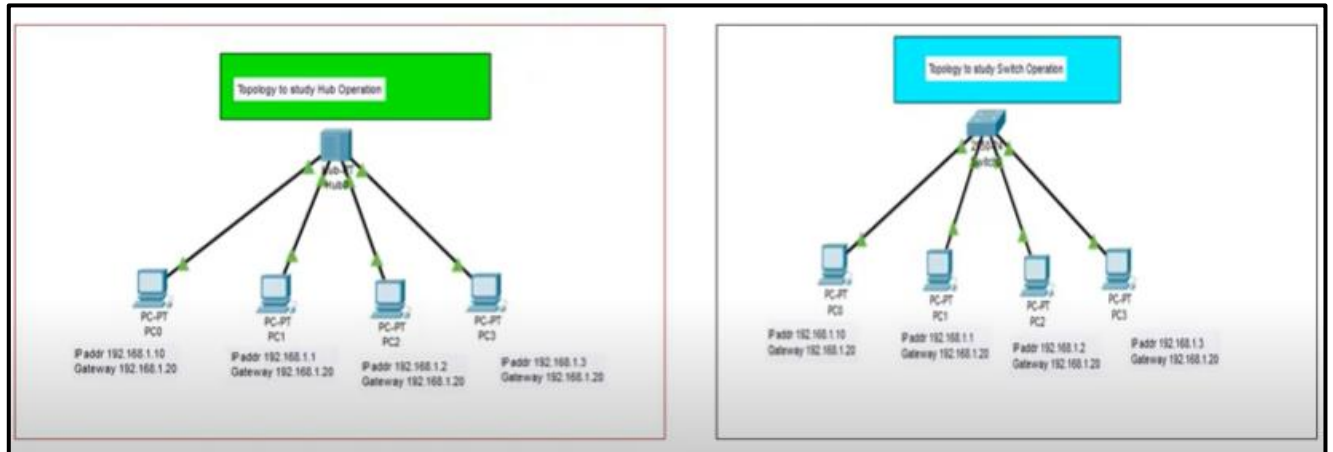


Figure 1: Network using Hub/ Switch

Scenario (Bridge)

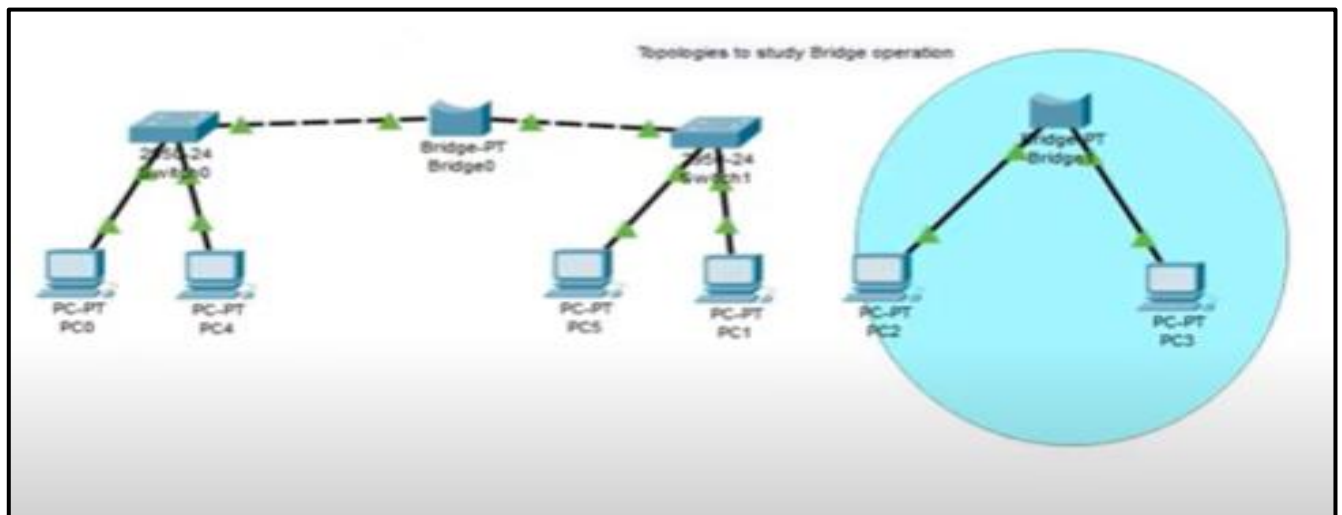


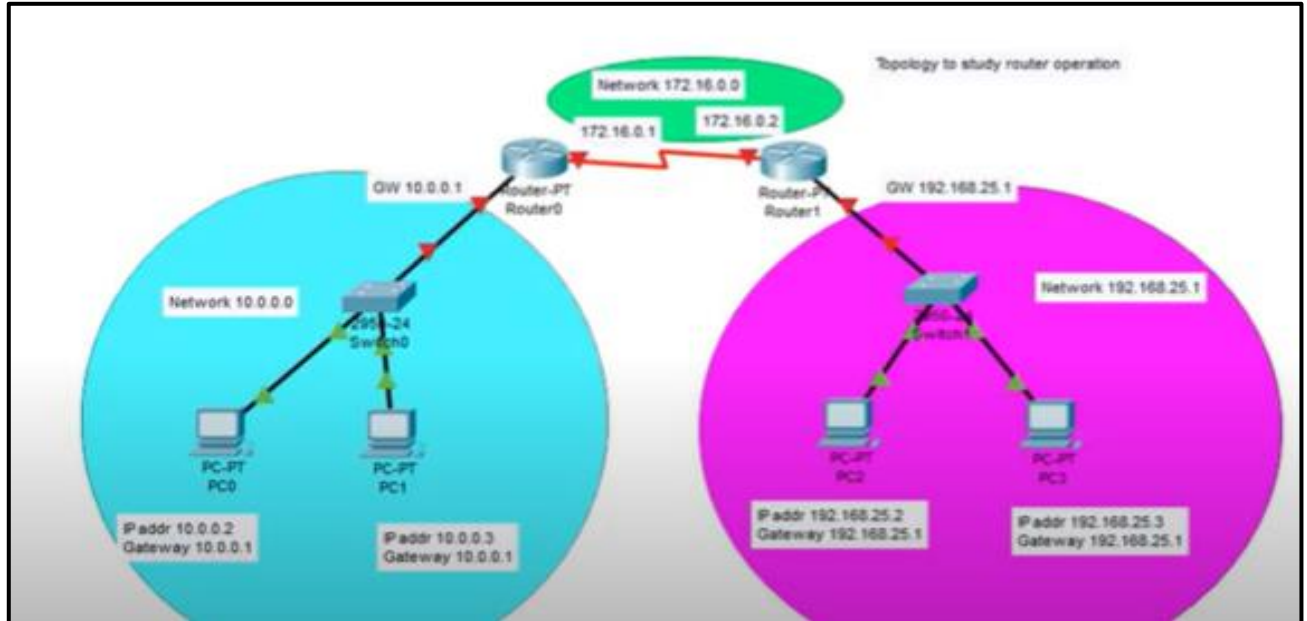
Figure 2: Network using Bridge.



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

---

Scenario (Router)



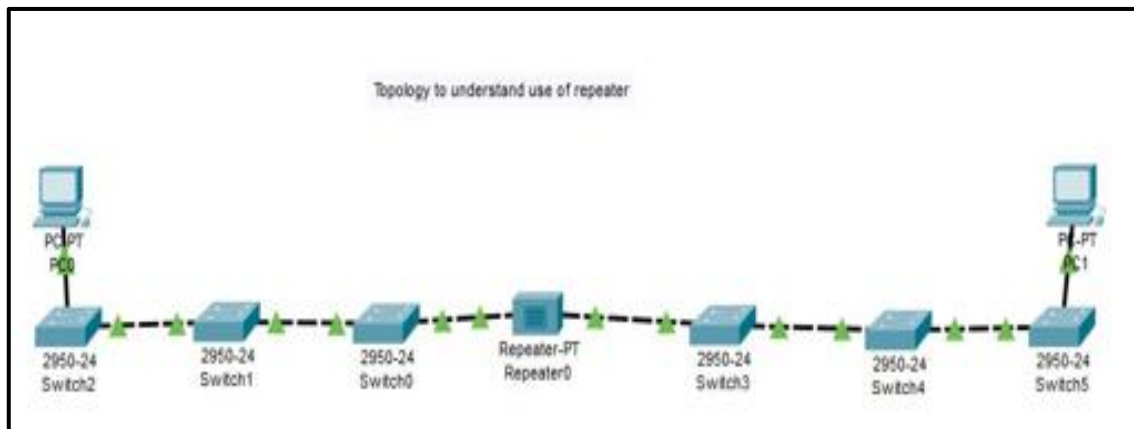
**Figure 3: Network using Router.**

1. Connect Two routers with a serial connection and connect a switch to each router in cisco packet tracer.
2. connect four PCs to each switch.
3. configure the serial and fastethernet interfaces for ip addresses on each router
4. Define static routes on each router
5. configure each PC with IP address and subnet mask.
6. check the connectivity between two PCs belonging to different networks (routers)
7. select the simulation tab.
8. Take a simple PDU, and select a source and destination PC for it.
9. Press Auto Capture/Play button
10. observe the router operation.



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

Scenario (Repeater)



**Figure 4: Network using Hub**

**Comparison of Network Hardware Devices**

Hardware Device/Parameter	Hub	Switch	Router	Bridge	Repeater
Used at which layer of OSI Model	Layer 1	Layer 2	Layer 3	Layer 2	Layer 1
Function	LAN	LAN	LAN to WAN	LAN to LAN	Extend LAN
Filtering capability	Does not	Filters frames based on MAC Address	Filters packets based on IP Address	Filters frames based on MAC Address	Does Not
No of ports/interfaces	4	24/48	5(console, auxiliary, VSO, LAN, WAN port)	2-3	2
Memory	NO	Yes, stores MAC Address	Yes, stores IP Address	Yes, stores MAC Address	No



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

---

**Result analysis and Conclusion:**

**Post experiment Questions:**

1. What are one or two key features of each device that stood out to you?



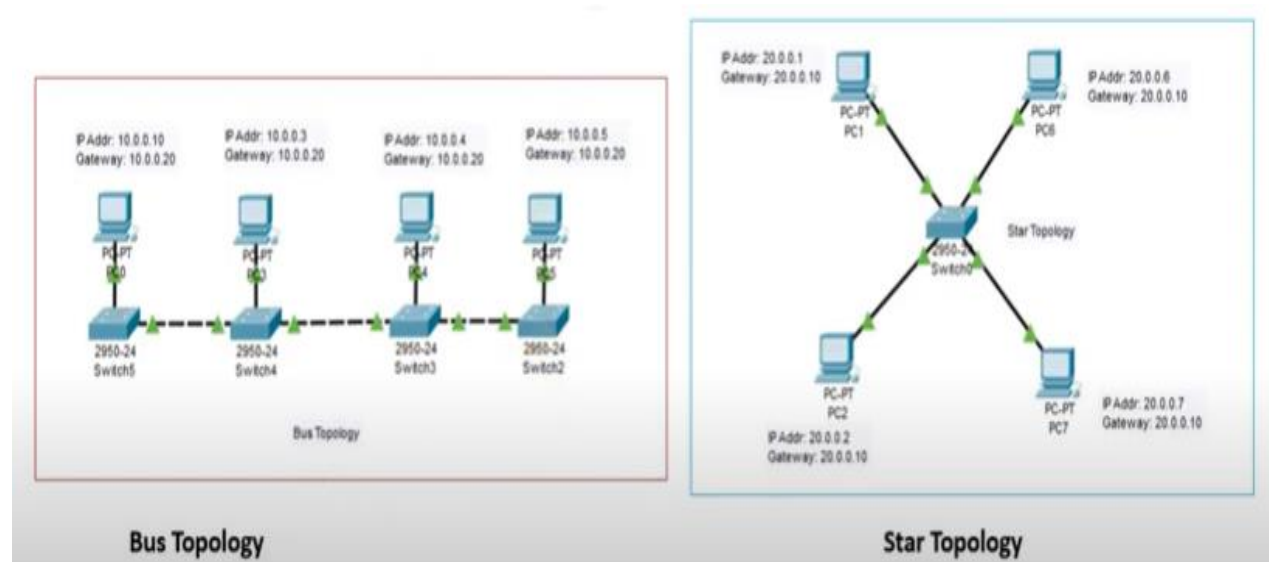
## Experiment No. 2

**AIM:** To configure and compare various network topologies using a Cisco packet tracer.

### **OBJECTIVES:**

- Part 1: To configure the following network topologies:  
Bus, Star, Mesh, Ring, dual ring, tree, and hybrid topology
- Part 2: To compare the network topologies

Scenario (Bus and Star Topology)



**Figure 1: Bus Topology**

**Figure 2: Star Topology**





Vidyavardhini's College of Engineering & Technology  
Department of Electronics and Telecommunication Engineering

Scenario (Mesh Topology)

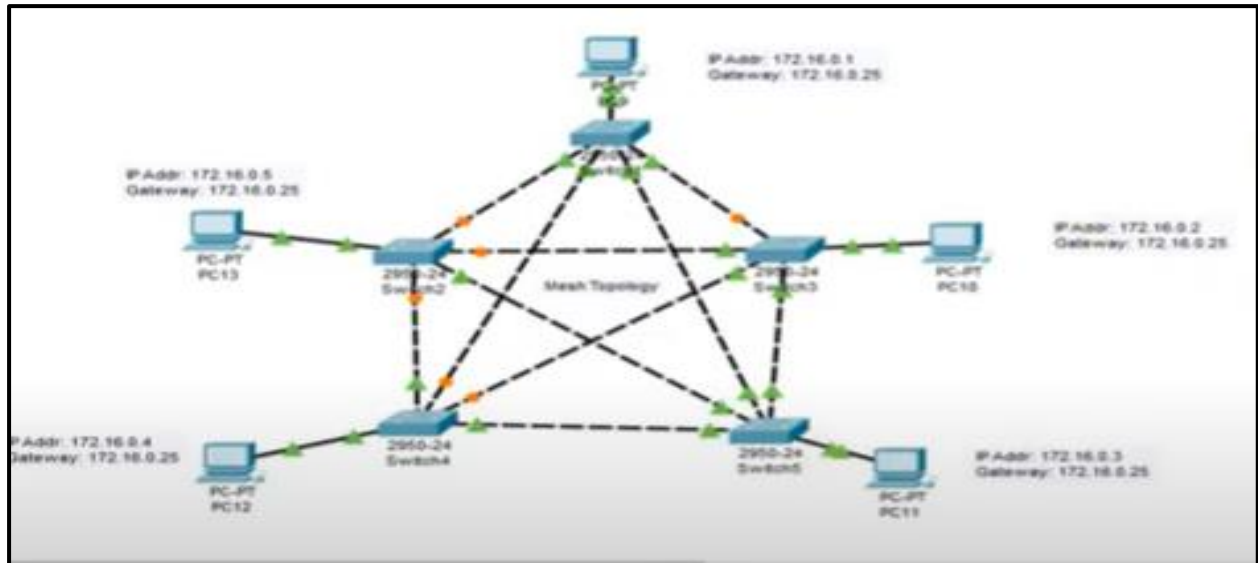


Figure 3: Mesh Topology

Scenario (Ring and Dual Ring Topology)

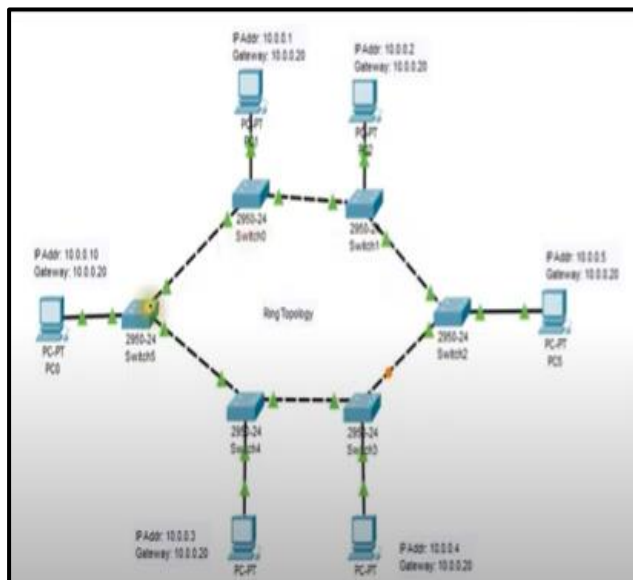


Figure 4: Ring Topology

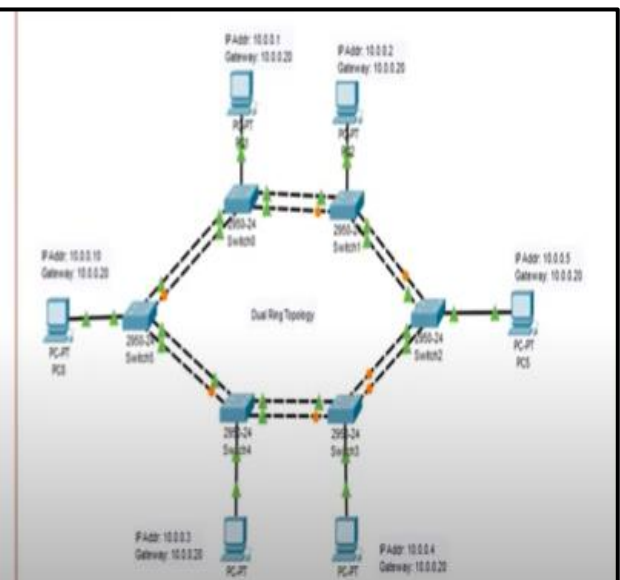


Figure 5: Dual Ring Topology



Vidyavardhini's College of Engineering & Technology  
Department of Electronics and Telecommunication Engineering

Scenario (Tree Topology)

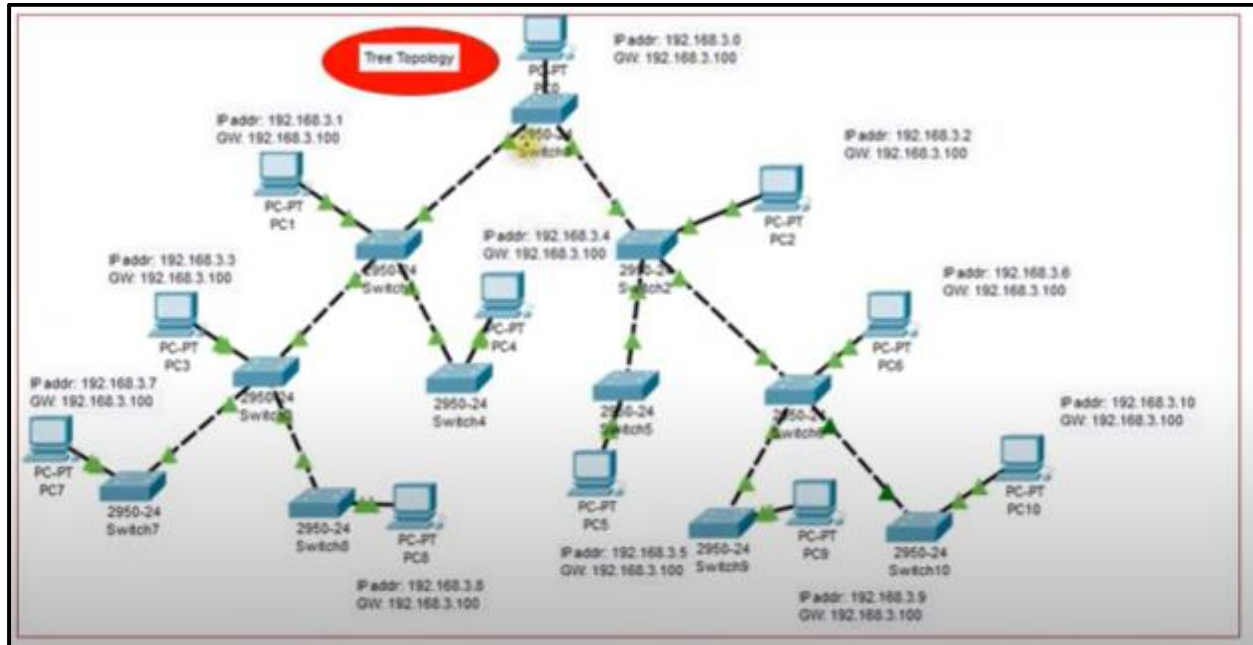


Figure 6: Ring Topology

Scenario (Hybrid Topology)

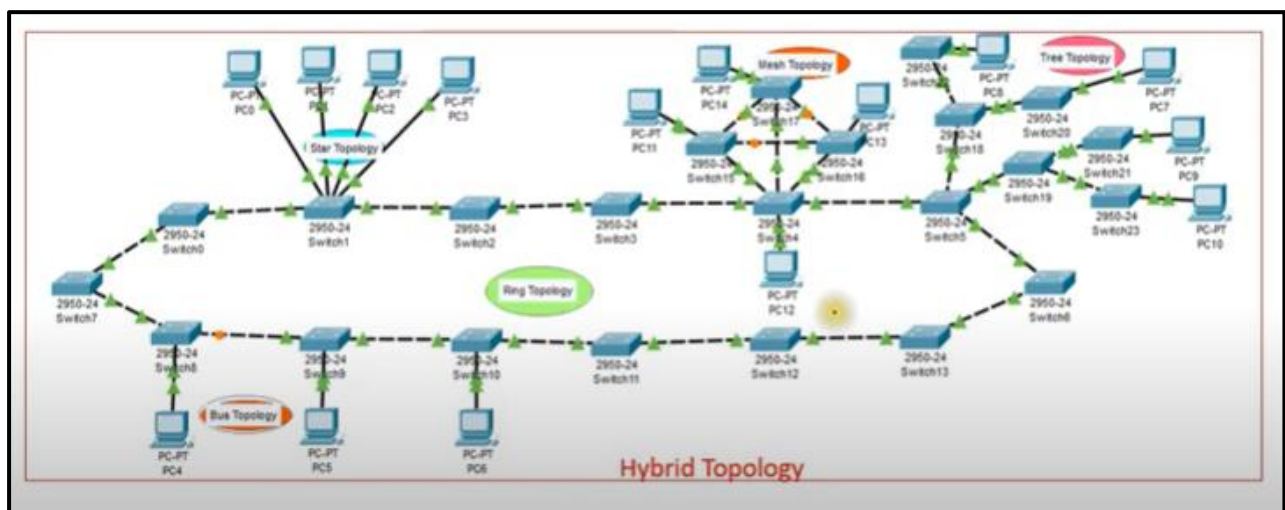


Figure 7: Hybrid Topology



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

---

**Comparison of Network Topologies:**

Topology	Total No of Links	Privacy	I/O lines with each device	Installation on and Reconnection	Fault Identification and Isolation	Application	Cost	Line Configuration
Bus	Single backbone with n drop lines	No	one	Difficult	Difficult	Multipoint	Least Expensive	Not used in large network
Star	n	No	one	Easy	Easy	P2P	Less Expensive	LAN High speed LAN
Mesh	$n(n-1)/2$	Yes	n-1	Difficult	Easy	P2P	Expensive	Regional Telephone offices
Ring	n	No	one	Difficult	Easy	Multipoint	Moderate	IBM Token Ring Standard  Not referred in High speed LAN



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

---

Output:

- Include ping responses for each topology
- Include packet flow sequences

**Result Analysis and Conclusion:**

**Post experiment Questions:**

1. To set up a computer lab in your department which topology would you prefer and why?

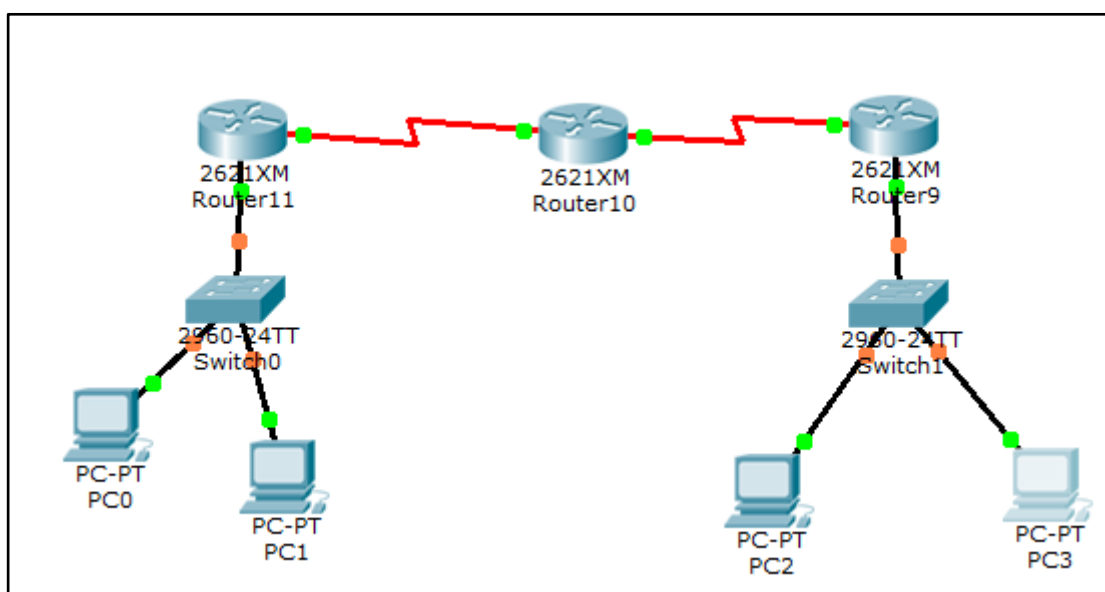


### **Experiment No. 3**

**Aim:** To configure a network to implement static routing using a Cisco packet tracer.

**Software:** CISCO PACKET TRACER 6.0.1/7.3.1

**Topology Diagram:**



**Theory:**

#### ***Static routing***

Static routing is the most secure way of routing. It reduces overhead from network resources. In this type of routing we manually add routes in routing table. It is useful where numbers of route are limited. Static routing has several primary uses, including:

- Providing ease of routing table maintenance in smaller networks that are not expected to grow significantly.
- Routing to and from a stub network, which is a network with only one default route out and no knowledge of any remote networks.
- Accessing a single default route (which is used to represent a path to any network that does not have a more specific match with another route in the routing table). Like other routing methods static routing also has its pros and cons.

#### ***Advantages of static routing***

- It is easy to implement.
- It is most secure way of routing, since no information is shared with other routers.
- It puts no overhead on resources such as CPU or memory.

#### ***Disadvantages of static routing***



## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

---

- It is suitable only for small network.
- If a link fails it cannot reroute the traffic.
- Managing the static configurations can become time consuming.

#### **Procedure:**

1. Drag routers (2621 type), switches (2960 type) & terminals onto workspace.
2. For each router, add 2 – port synchronous/asynchronous serial network module (WIC-2T module)
3. Select automatic connection type & connect devices to form desired network.
4. Select each node & configure IP address, subnet mask & default gateways.
5. Select each router & configure fast Ethernet port on LAN side and serial ports on WAN side with appropriate IP address and subnet masks.
6. Create statics routing table.
7. Send packets within LAN'S & from one LAN to other & observe packet flow.

#### **Result analysis and Conclusion:**

#### **Post experiment Questions:**

What are the specific scenarios where static routing is more suitable?

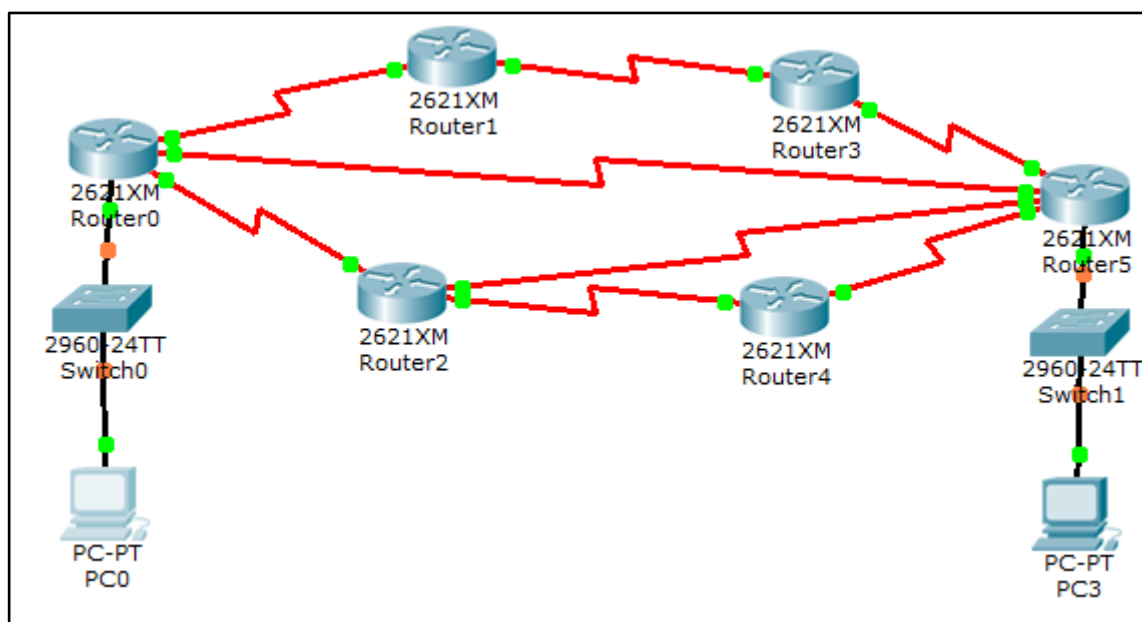


### **Experiment No. 4**

**Aim:** To configure network to implement dynamic routing using Cisco packet tracer.

**Software:** CISCO PACKET TRACER 6.0.1/7.3.1

**Topology Diagram:**



**Theory:**

***Dynamic Routing:***

Dynamic routing protocols help the network administrator manage the time-consuming and exacting process of configuring and maintaining routes. Dynamic routing protocols work well in any type of network consisting of several routers. They are scalable and automatically determine better routes if there is a change in the topology. Although there is more to the configuration of dynamic routing protocols, they are simpler to configure in a large network.

There are disadvantages to dynamic routing: Dynamic routing requires knowledge of additional commands, it is also less secure than static routing because the interfaces identified by the routing protocol send routing updates out.

- **Procedure:**

1. Drag routers (2621) bytes, switches (2960) (generic types) and terminals (PCs) on workspace.



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

---

2. For each router add 2\*2 WIC-2T cards (2 ports) (sync/async) (serial n/w mode).
3. Select automatic connection type & connect device with each other to form the desired/W as shown.
4. Select each terminal and configure IP address, subnet mask and default gateway as per network.
5. Select each router & configure fast Ethernet part on LAN side and serial ports on WAN side with appropriate IP address and subnet masks.
6. To create dynamic routing table for shortest path, Select RIP option
7. Find packet from one node to another and observe the packet flow.
8. Select link 1 as shown in the fig. and make it down and observe the packet flow in the network.
9. Select the link 2 as shown and follow same procedure mentioned in step 8.

**Results:**

Event	Action occurring in network
When all link are up and packet is sent from PC0 to PC1.	Path taken by packet from PC0 - Router 0- Router 5- PC3
When link 1 is down and packet is send from PC0 to PC 1	Path taken by packet from PC0 - Router 0- Router 2- Router 4- Router 5-PC3
When link 1 & link 2 are down and packet is sent from PC0 to PC1	Path taken by packet from PC0 - Router 0- Router 2- Router 4- Router 5-PC3

**Output:**

**Result analysis and Conclusion:**

**Post experiment Questions:**

Compare the experience of configuring dynamic routing with your experience in setting up static routing. In what scenarios do you think dynamic routing is more advantageous, and are there any drawbacks compared to static routing in your specific network setup?



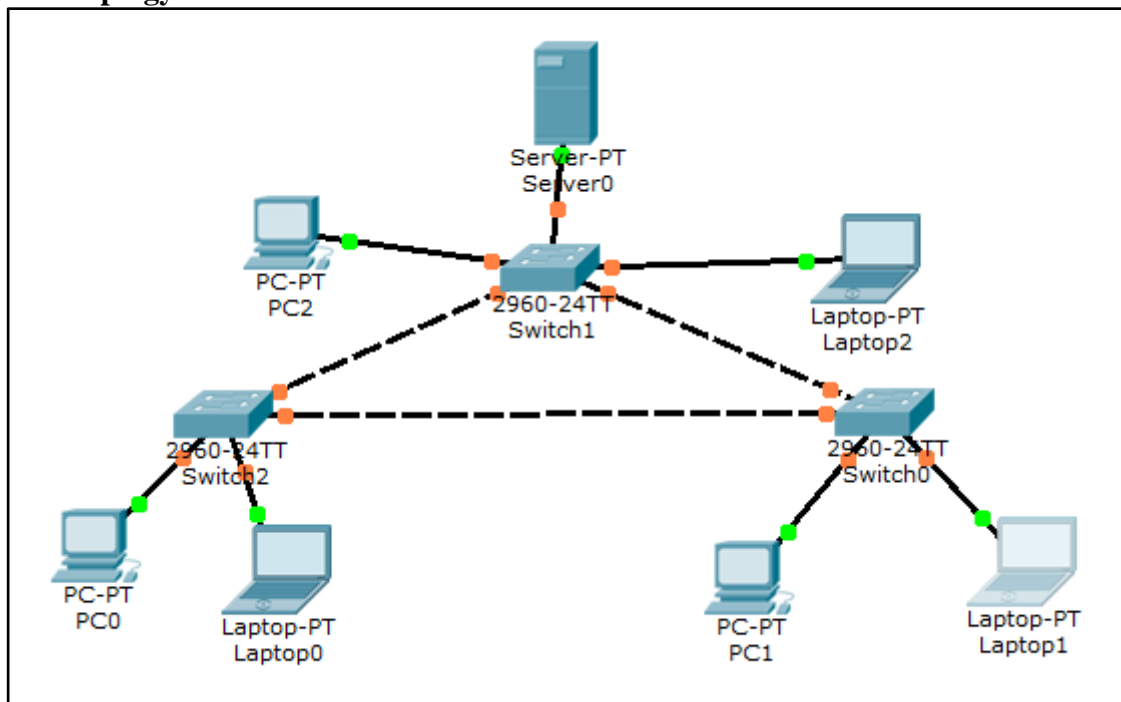


## Experiment 5

**Aim:** To configure DHCP using Cisco packet tracer.

**Software:** CISCO PACKET TRACER 6.0.1/7.3.1

**Network Topology:**



**Theory:**

DHCP is used by workstations (hosts) to get initial configuration information, such as an IP address, subnet mask, and default gateway upon boot up. Since each host needs an IP address to communicate in an IP network, DHCP eases the administrative burden of manually configuring each host with an IP address. Furthermore, if a host moves to a different IP subnet, it must use a different IP address than the one it previously used. DHCP takes care of this automatically. It allows the host to choose an IP address in the correct IP subnet.

The Cisco DHCP server feature is a full implementation that assigns and manages IP addresses from specified address pools to DHCP clients. After a DHCP client has booted, the client begins sending packets to its default router. The IP address of the default router should be on the same subnet as the client.

**Procedure:**

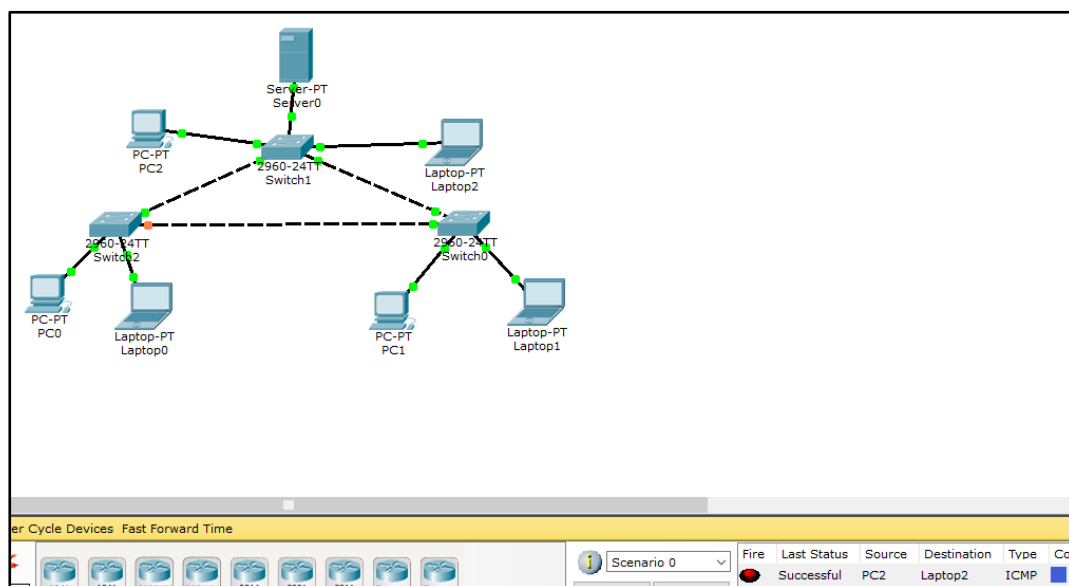


## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

- Drag and drop Switches (2960), Server and End terminals
- Make connection between terminals, switches and server as shown in figure.
- Server > Desktop > 192.168.0.1
- Server > Configuration > DHCP > Make ON
- Default Gateway- 192.168.0.1
- DNS Server 10.0.0.1
- Max users depending on requirement eg 255
- PC > Desktop > IP Config > DHCP
- For all PCs and Laptops provide dynamic IP address
- Send packet between any two PCs or Laptops
- Check packet transfer status.

#### **Output:**



#### **Result analysis and Conclusion:**

#### **Post experiment questions:**

Compare the experience of using DHCP for IP assignment with manually configuring static IP addresses. What are the pros and cons of each approach?



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

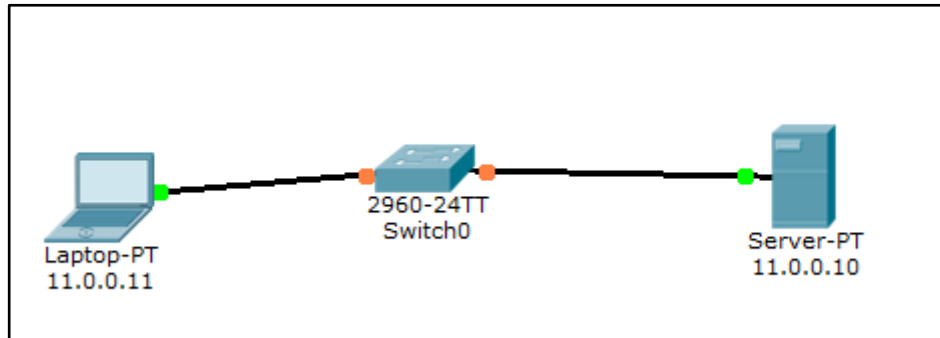
---

### Experiment 6

**Aim:** To configure DNS using Cisco packet tracer.

**Software:** CISCO PACKET TRACER 6.0.1/7.3.1

**Network Topology:**



**Theory:**

DNS stands for Domain Name System. The main function of DNS is to translate domain names into IP Addresses, which computers can understand. It also provides a list of mail servers which accept Emails for each domain name. Each domain name in DNS will nominate a set of name servers to be authoritative for its DNS records.

This is where all other name servers will be pointed when looking for information about the domain name. Name servers are a program or computer server that implements a name-service protocol. This is where the zone file is stored and your DNS records are stored within. A zone file is a small set of instructions that points domain names to IP addresses.

**Procedure:**

- Drag and drop PC on workplace
- Drag and drop server
- Drag and drop switch (2960)
- Make connection as shown in diagram with copper straight through
- Select server : Go to config> DNS> Make DNS ON
- Give name eg [www.mywebsite.com](http://www.mywebsite.com)



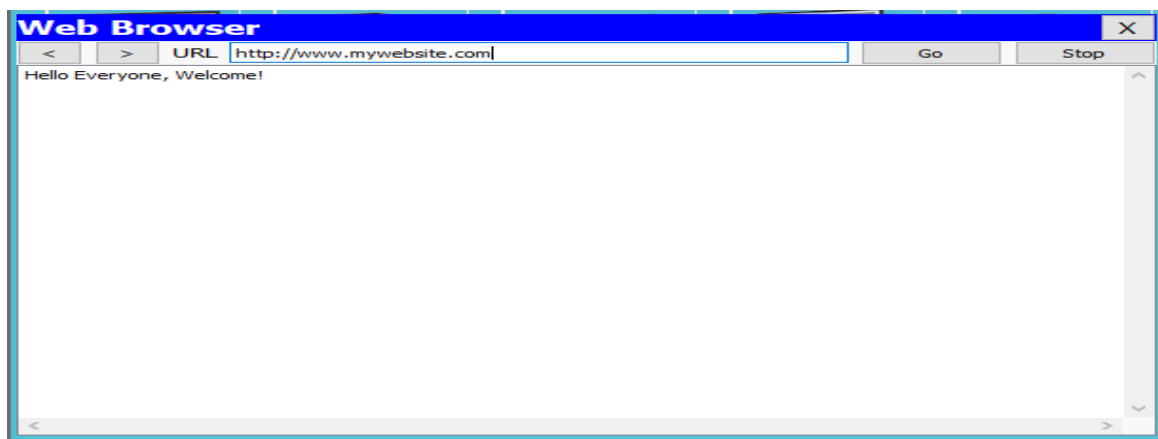
**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

---

- Give address 11.0.0.1 (for example)
  - Select HTTP > Type message in body  

```
<html>  
Hello Everyone, Welcome!  
</html>
```
  - Select PC > static IP 10.0.0.1
  - Select PC> Web browser> type [www.mywebsite.com](http://www.mywebsite.com)
- Output:            Hello Everyone, Welcome!

**Output:**



**Result analysis and Conclusion:**

**Post Experiment Questions:** When selecting a domain name for your institute, what key considerations would you consider ensuring it is meaningful, memorable, and aligns with the identity or purpose of the institution?



## Experiment 7

**Aim:** To determine the optimum persistence of a p persistent CSMA/CD network for a heavily loaded bus capacity.

**Software:** Netsim

### **Theory:**

#### **Carrier Sense Multiple Access Collision Detection (CSMA/CD)**

This protocol includes the improvements for stations to abort their transmissions as soon as they detect a collision. Quickly terminating frames saves time and bandwidth. This protocol is widely used on LANs in the MAC sub layer. If two or more stations decide to transmit simultaneously, there will be a collision. Collisions can be detected by looking at the power or pulse width of the received signal and comparing it to the transmitted signal. After a station detects a collision, it aborts its transmission, waits a random period of time and then tries again, assuming that no other station has started transmitting in the meantime.

There are mainly three theoretical versions of the CSMA/CD protocol:

**1-persistent CSMA/CD:** When a station has data to send, it first listens to the channel to see if anyone else is transmitting at that moment. If the channel is busy, the station waits until it becomes idle. When station detects an idle channel, it transmits a frame. If a collision occurs, the station waits a random amount of time and starts all over again. The protocol is called 1-persistent because the station transmits with a probability of 1 whenever it finds the channel idle.

Ethernet, which is used in real-life, uses 1-persistence. A consequence of 1-persistence is that, if more than one station is waiting for the channel to get idle, and when the channel gets idle, a collision is certain. Ethernet then handles the resulting collision via the usual exponential back off. If  $N$  stations are waiting to transmit, the time required for one station to win the back off is linear in  $N$ .

**Non-persistent CSMA/CD:** In this protocol, before sending, a station senses the channel. If no one else is sending, the station begins doing so itself. However, if the channel is already in use, the channel does not continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission. Instead, it waits a random period of time and then repeats the algorithm. Intuitively this algorithm should lead to better channel utilization and longer delays than 1-persistent CSMA.

**P-persistent CSMA/CD:** This protocol applies to slotted channels. When a station becomes ready to send, it senses the channel. If it is idle, it transmits with a probability of  $p$ . With a probability  $q=1-p$  it defer until the next slot. If that slot is also idle, it either transmits or defers again, with probabilities  $p$  and  $q$  resp. This process is repeated until either the frame has been transmitted or another station has begun transmitting. In the latter case, it acts as if there had been a collision (i.e. it waits a random time and starts again). If the station initially senses the channel busy, it waits until the next slot and applies the above algorithm.

#### **How does the performance of LAN (throughput) that uses CSMA/CD protocol gets affected as the numbers of logged in user varies:**

Performance studies indicate that CSMA/CD performs better at light network loads. With the increase in the number of stations sending data, it is expected that heavier traffic have to be carried on CSMA/CD LANs (IEEE 802.3). Different studies have shown that CSMA/CD performance tends



## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

to degrade rapidly as the load exceeds about 40% of the bus capacity. Above this load value, the number of packet collision raise rapidly due to the interaction among repeated transmissions and new packet arrivals. Collided packets will back off based on the truncated binary back off algorithm as defined in IEEE 802.3 standards. These retransmitted packets also collide with the newly arriving packets.

#### **Procedure:**

1. **Create Scenario:** “Simulation→New→Legacy Networks→Traditional Ethernet”.
2. **Sample Input:** In this sample experiment 12 nodes & 2 hubs need to be clicked and dropped onto the Environment Builder.

In the first sample for each node the following properties have to be set,

<i>Node properties</i>	<i>Values to be selected</i>
<i>Transmission Type</i>	<i>Broadcast</i>
<i>Traffic Type</i>	<i>Data</i>
<i>No. of Nodes Transmitting</i>	<i>12</i>
<i>Persistence</i>	<i>1</i>
<i>MTU Size(bytes)</i>	<i>1500</i>

Vary persistence from  $\frac{1}{2}$ ,  $\frac{1}{3}$ ,  $\frac{1}{4}$ .... $\frac{1}{11}$ ,  $\frac{1}{12}$  to generate other **experiments**.

3. **Data Input Configuration:** (this window is obtained when data is selected in traffic type):

<i>Packet Size</i>	<i>Distribution</i>	<i>Constant</i>
	<i>Application Data Size(bytes)</i>	<i>1472</i>
<i>Inter Arrival Time</i>	<i>Distribution</i>	<i>Exponential</i>
	<i>Mean Inter Arrival Time(<math>\mu s</math>)</i>	<i>1000</i>

4. **Hub Properties common for Hub1 & Hub2:**

<i>Hub Properties</i>	<i>Values to be selected</i>
<i>Port Rate(Mbps)</i>	
<i>Error Rate(bit error rate)</i>	<i>Error</i>



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

---

<i>Physical Medium</i>	<i>Twisted Pair</i>
------------------------	---------------------

**5. Simulation Time: 10 sec**

**Note:** (The simulation time can be selected only after the following two tasks

- a. Set the properties for the nodes & the hub
  - b. Click on Run Simulation button.)
- 6.** After simulation of each experiment, click on the network statistics and note down the user level throughput values. Open an excel sheet and plot a graph for these noted values against their respective persistence values.

**Result analysis and Conclusion:**

**Post Experiment Question:**

Based on your experimentation with different persistence values in the p-persistent CSMA/CD network on a heavily loaded bus, what persistence value did you find to be optimum? Describe the factors that influenced your choice, and how did this value contribute to the overall performance and efficiency of the network?



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

---

## Experiment 8

**Aim:** Study of basic network commands and Network configuration commands.

**Software:** Command Prompt

**Objectives:**

1. To become familiar with some of the commands used for basic network configuration and troubleshooting functions on host computers.
2. To become familiar with some of the Cisco IOS commands used for basic device configuration and troubleshooting.

**Procedure:**

**Part 1: Examining Network Properties Settings**

*Ipconfig :*

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays the IP address, subnet mask, and default gateway for all adapters.

```
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    IP Address. . . . . : 172.16.1.2
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 172.16.255.254
```

1. IP address for this host computer
2. Subnet mask
3. Default gateway address

**Part 2: Testing TCP/IP Network Connectivity**

Two tools that are indispensable when testing TCP/IP network connectivity are ping and tracert.

*Ping :*

Is a utility for testing IP connectivity between hosts. Ping sends out requests for responses from a specified host address. Ping uses a Layer 3 protocol that is a part on the TCP/IP suite called Internet Control Message Protocol (ICMP). Ping uses an ICMP Echo Request.





## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

---

If the host at the specified address receives the Echo request, it responds with an ICMP Echo Reply datagram. For each packet sent, ping measures the time required for the reply. As 6 each response is received, ping provides a display of the time between the ping being sent and the response received. This is a measure of the network performance. Ping has a timeout value for the response. If a response is not received within that timeout, ping gives up and provides a message indicating that a response was not received.

After all the requests are sent, the ping utility provides an output with the summary of the responses. This output includes the success rate and average round-trip time to the destination.

#### Step 1 Access the command prompt

Use the Start menu to open the Command Prompt window. Press

Start > Programs > Accessories > Command Prompt or Start > run > cmd

#### Step 2 Ping the IP address of another computer

In the window, type ping, a space, and the IP address of a computer in the lab.

The following figure shows the successful results of ping to this IP address.

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<10ms TTL=128
Reply from 192.168.1.10: bytes=32 time<10ms TTL=128
Reply from 192.168.1.10: bytes=32 time<10ms TTL=128
Reply from 192.168.1.10: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Ping uses the ICMP echo request and echo reply feature to test physical connectivity. Since ping reports on four attempts, it gives an indication of the reliability of the connection. Look over the results and verify that the ping was successful. Is the ping successful? If not, perform appropriate troubleshooting.

#### Step 3 Ping the Cisco web site

Type the following command: ping [www.cisco.com](http://www.cisco.com)



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

---

The first output line shows the Fully Qualified Domain Name (FQDN) followed by the IP address. A Domain Name Service (DNS) server somewhere in the network was able to resolve the name to an IP address. DNS servers resolve domain names, not hostnames, to IP addresses. Without this name resolution, the ping would have failed because TCP/IP only understands valid IP addresses.

```
C:\>ping www.cisco.com

Pinging www.cisco.com [198.133.219.25] with 32 bytes of data:

Reply from 198.133.219.25: bytes=32 time=170ms TTL=239
Reply from 198.133.219.25: bytes=32 time=160ms TTL=239
Reply from 198.133.219.25: bytes=32 time=160ms TTL=239
Reply from 198.133.219.25: bytes=32 time=160ms TTL=239

Ping statistics for 198.133.219.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 160ms, Maximum = 170ms, Average = 162ms

C:\>
```

It would not be possible to use the web browser without this name resolution. With DNS, connectivity to computers on the Internet can be verified using a familiar web address, or domain name, without having to know the actual IP address. If the nearest DNS server does not know the IP address, the server asks a DNS server higher in the Internet structure.

**Step 4** Ping the Microsoft web site

Type the following command: ping [www.microsoft.com](http://www.microsoft.com)



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

```
Command Prompt

C:\>ping www.microsoft.com

Pinging www.microsoft.akadns.net [207.46.197.100] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 207.46.197.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Notice that the DNS server was able to resolve the name to an IP address, but there is no response. Some Microsoft routers are configured to ignore ping requests. This is a frequently implemented security measure.

**Step 5** Trace the route to the Cisco web site Type `tracert` [www.cisco.com](http://www.cisco.com) and press Enter.

```
Command Prompt

C:\>tracert www.cisco.com

Tracing route to www.cisco.com [198.133.219.25]
over a maximum of 30 hops:

  0  <10 ms    <10 ms    <10 ms    10-37-00-1.internal.alp.dillingen.de [10.37.0.1]
  1  <10 ms    <10 ms    <10 ms    194.95.207.11
  2  20 ms     <10 ms    10 ms     ar-augsburg2.g-win.dfn.de [188.1.37.145]
  3  <10 ms    <10 ms    10 ms     ar-augsburg1.g-win.dfn.de [188.1.74.193]
  4  <10 ms    <10 ms    10 ms     cr-muenchen1.g-win.dfn.de [188.1.74.33]
  5  10 ms     10 ms     10 ms     cr-frankfurt1.g-win.dfn.de [188.1.18.81]
  6  10 ms     10 ms     10 ms     so-6-0-0.ar2.FRA2.gblx.net [208.48.23.141]
  7  10 ms     10 ms     10 ms     pos3-0-622M.cr1.FRA2.gblx.net [62.16.32.73]
  8  30 ms     30 ms     20 ms     so0-0-0-2488M.cr2.LON3.gblx.net [195.8.96.174]
  9  30 ms     30 ms     20 ms     pos1-0-622M.br1.LON3.gblx.net [195.8.96.189]
 10  30 ms     30 ms     20 ms     sl-bb21-lon-5-0.sprintlink.net [213.206.131.25]
 11  100 ms    100 ms    90 ms     sl-bb20-msq-10-0.sprintlink.net [144.232.19.69]
 12  110 ms    110 ms    110 ms    sl-bb20-rlv-15-1.sprintlink.net [144.232.19.94]
 13  171 ms    160 ms    170 ms    sl-bb22-sj-5-i.sprintlink.net [144.232.9.125]
 14  161 ms    160 ms    170 ms    sl-bb25-sj-12-0.sprintlink.net [144.232.3.210]
 15  160 ms    181 ms    160 ms    sl-gw11-sj-10-0.sprintlink.net [144.232.3.134]
 16  170 ms    151 ms    160 ms    sl-ciscopsn2-11-0-0.sprintlink.net [144.228.44.14]
 17  170 ms    151 ms    160 ms    sjck-dirty-gw1.cisco.com [128.107.239.5]
 18  160 ms    160 ms    161 ms    sjck-sdf-cioc-gw1.cisco.com [128.107.239.106]
 19  160 ms    150 ms    161 ms    www.cisco.com [198.133.219.25]
 20

Trace complete.
```

The first output line shows the FQDN followed by the IP address. Therefore, a DNS server was able to resolve the name to an IP address. Then there are listings of all routers the `tracert` requests had to pass through to get to the destination.

`tracert` uses the same echo requests and replies as the `ping` command but in a slightly different way. Observe that `tracert` actually contacted each router three times. Compare the results to



## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

---

determine the consistency of the route. Notice in the above example that there were relatively long delays after router 11 and 13, possibly due to congestion. The main thing is that there seems to be relatively consistent connectivity.

Each router represents a point where one network connects to another network and the packet was forwarded through.

#### **Step 6** Trace other IP addresses or domain names

Try `tracert` on other domain names or IP addresses and record the results.

An example is `tracert www.msn.de`.

#### **Step 7** Trace a local host name or IP address

Try using the `tracert` command with a local host name or IP address. It should not take long because the trace does not pass through any routers.



```
C:\>tracert lh-1700us

Tracing route to lh-1700us [10.37.0.186]
over a maximum of 30 hops:

  1  <10 ms  <10 ms  <10 ms  lh-1700us [10.37.0.186]

Trace complete.

C:\>
```

### **Round Trip Time (RTT)**

Using traceroute provides round trip time (RTT) for each hop along the path and indicates if a hop fails to respond. The round trip time (RTT) is the time a packet takes to reach the remote host and for the response from the host to return. An asterisk (\*) is used to indicate a lost packet.

This information can be used to locate a problematic router in the path. If we get high response times or data losses from a particular hop, this is an indication that the resources of the router or its connections may be stressed.

### **Time to Live (TTL)**

Traceroute makes use of a function of the Time to Live (TTL) field in the Layer 3 header and ICMP Time Exceeded Message. The TTL field is used to limit the number of hops that a packet can cross. When a packet enters a router, the TTL field is decremented by 1. When the TTL reaches zero, a router will not forward the packet and the packet is dropped.

In addition to dropping the packet, the router normally sends an ICMP Time Exceeded message addressed to the originating host. This ICMP message will contain the IP address of the router that responded. The first sequence of messages sent from traceroute will have a TTL field of one. This causes the TTL to time out the packet at the first router. This router then responds with an ICMP Message. Traceroute now has the address of the first hop.

Traceroute then progressively increments the TTL field (2, 3, 4...) for each sequence of messages. This provides the trace with the address of each hop as the packets timeout further down the path. The TTL field continues to be increased until the destination is reached or it is incremented to a predefined maximum. Once the final destination is reached, the host responds with either an ICMP Port Unreachable message or an ICMP Echo Reply message instead of the ICMP Time Exceeded message. The tracert utility, available on Windows, (a similar utility, traceroute, is available on Linux and Cisco IOS).

### **Part 3: Address Resolution Protocol (ARP)**



## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

---

ARP is used as a tool for confirming that a computer is successfully resolving network Layer 3 addresses to Media Access Control (MAC) Layer 2 addresses. The TCP/IP network protocol relies on IP addresses like 192.168.14.211 to identify individual devices and to assist in navigating data packets between networks. While the IP address is essential to move data from one LAN to another, it cannot deliver the data in the destination LAN by itself. Local network protocols, like Ethernet or Token Ring, use the MAC, or Layer 2, address to identify local devices and deliver all data.

This is an example of a MAC address: 00-02-A5-9A-63-5C

A MAC address is a 48-bit address displayed in Hexadecimal (HEX) format as six sets of two HEX characters separated by dashes. In this format each hex symbol represents 4 bits. With some devices, the 12 hex characters may be displayed as three sets of four characters separated by periods or colons (0002.A59A.635C).

ARP maintains a table in the computer of IP and MAC address combinations. In other words, it keeps track of which MAC address is associated with an IP address. If ARP does not know the MAC address of a local device, it issues a broadcast using the IP address. This broadcast searches for the MAC address that corresponds to the IP address. If the IP address is active on the LAN, it will send a reply from which ARP will extract the MAC address. ARP will then add the address combination to the local ARP table of the requesting computer.

MAC addresses and therefore ARP are only used within the LAN. When a computer prepares a packet for transmission, it checks the destination IP address to see if it is part of the local network. It does this by checking to see if the network portion of the IP address is the same as the local network. If it is, the ARP process is consulted to get the MAC address of the destination device using the IP address. The MAC address is then applied to the data packet and used for delivery.

If the destination IP address is not local, the computer will need the MAC address of the default gateway. The default gateway is the router interface that the local network is connected to in order to provide connectivity with other networks. The gateway MAC address is used because the packet will be delivered there and the router will then forward it to the network it is intended for.

#### **Step 1** Access a command prompt

Use the Start menu to open the Command Prompt window.

Start > Programs > Accessories > Command Prompt or Start > run > cmd

#### **2** Display the ARP table

1. In the window type `arp -a` and press Enter. Do not be surprised if there are no entries. The message displayed will probably be, 'No ARP Entries Found'. Windows computers remove any addresses that are unused after a couple minutes.
2. Try pinging a couple local addresses and a website URL. Then re-run the command. The figure below shows a possible result of the `arp -a` command. The MAC address for the website will be listed because it is not local, but that will cause the default gateway to be listed. In the example

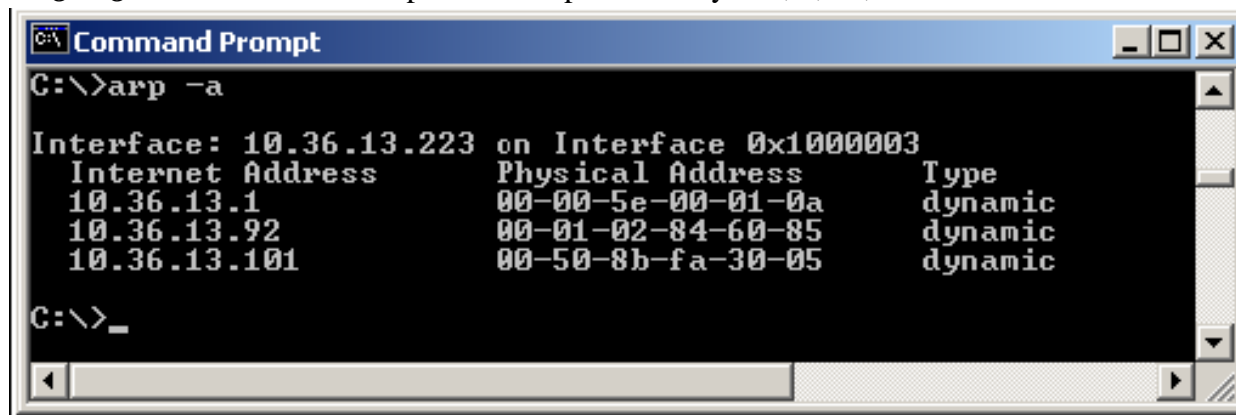


## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

below 10.36.13.1 is the default gateway while the 10.36.13.92 and 10.36.13.101 are other network computers. Notice that for each IP address there is a physical address, or MAC, and type, indicating how the address was learned.

3. From the figure below, it might be logically concluded that the network is 10.36.13.1 and the host computers are represented by 223, 1, 92, and 101.



```
C:\>arp -a

Interface: 10.36.13.223 on Interface 0x10000003
Internet Address      Physical Address      Type
10.36.13.1            00-00-5e-00-01-0a    dynamic
10.36.13.92           00-01-02-84-60-85    dynamic
10.36.13.101          00-50-8b-fa-30-05    dynamic

C:\>_
```

#### nslookup:

Displays information from Domain Name System (DNS) name servers.

NOTE :If you write the command as above it shows as default your pc's server name firstly.

All commands related to Network configuration which includes how to switch to privilege mode and normal mode and how to configure router interface and how to save this configuration to flash memory or permanent memory.

This commands includes

#### Configuring the Router commands

In any command mode, you can get a list of available commands by entering a question mark (?).

Router>?

To obtain a list of commands that begin with a particular character sequence, type in those characters followed immediately by the question mark (?).

Router#co?

configure connect copy

#### Configuration Files

Any time you make changes to the router configuration, you must save the changes to memory because if you do not they will be lost if there is a system reload or power outage. There are two types of configuration files: the running (current operating) configuration and the startup configuration.

Use the following privileged mode commands to work with configuration files.

- configure terminal – modify the running configuration manually from the terminal.



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

---

### **IP Address Configuration**

Take the following steps to configure the IP address of an interface.

**Step 1:** Enter privileged EXEC mode:

Router>enable password

**Step 2:** Enter the configure terminal command to enter global configuration mode.

Router#config terminal

**Step 3:** Enter the interface type slot/port (for Cisco 7000 series) or interface type port (for Cisco 2500 series) to enter the interface configuration mode.

Example:

Router (config)#interface fastethernet 0/1

**Step 4:** Enter the IP address and subnet mask of the interface using the ip address ip address subnetmask command.

Example,

Router (config-if)#ip address 192.168.10.1 255.255.255.0

**Step 5:** Exit the configuration mode by pressing Ctrl-Z Router(config-if)#[Ctrl-Z]

### **Result analysis and Conclusion:**

**Post Experiment Questions:** How has this troubleshooting experience contributed to your learning and skill development in network management?





## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

---

#### Experiment 9A

**Aim:** To Study the steps for installing Wireshark, the packet-sniffing tool for performing Network packet analysis.

#### **Learning Objectives:**

At the end of the session, you will be able to

- Use one of the best packets sniffing tool i.e. “Wireshark”.
- Control upon ports, protocols, and data packets.
- Quick protocol identification.
- Start capturing and analyzing packets

#### **A Brief History of Wireshark**

Wireshark has a very rich history. Gerald Combs, a computer science graduate of the University of Missouri at Kansas City, originally developed it out of necessity. The first version of Combs's application, called Ethereal, was released in 1998 under the GNU Public License (GPL). Eight years after releasing Ethereal, Combs left his job to pursue other career opportunities. Unfortunately, his employer at that time had full rights to the Ethereal trademarks, and Combs was unable to reach an agreement that would allow him to control the Ethereal “brand.” Instead, Combs and the rest of the development team rebranded the project as Wireshark in mid-2006 thereafter it is continuing.

#### **The Benefits of Wireshark**

Wireshark offers several benefits that make it appealing for everyday use. It is aimed at both the journeyman and the expert packet analyst and offers a variety of features to entice each. Let's examine Wireshark according to the criteria defined for selecting a packet-sniffing tool.

**Supported protocols:** Wireshark excels in the number of protocols that it supports more than 850 as of this writing. These range from common ones like IP and DHCP to more advanced proprietary protocols like AppleTalk and Bit Torrent. And because Wireshark is developed under an open-source model, new protocol support is added with each update.

**User-friendliness:** The Wireshark interface is one of the easiest to understand of any packet sniffing application. It is GUI-based, with very clearly written context menus and a straightforward layout. It also provides several features designed to enhance usability, such as protocol-based color coding and detailed graphical representations of raw data. Unlike some of the more complicated command-line-



## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

---

driven alternatives, like tcpdump, the Wireshark GUI is great for those who are just entering the world of packet analysis.

**Cost:** Since it is open source, Wireshark's pricing can't be beat: Wire-shark is released as free software under the GPL. You can download and use Wireshark for any purpose, whether personal or commercial.

**Program support:** A software package's level of support can make or break it. When dealing with freely distributed software such as Wireshark, there may not be any formal support, which is why the open-source community often relies on its user base to provide support. Luckily for us, the Wireshark community is one of the most active of any open-source project.

**Operating system support:** Wireshark supports all major modern operating systems, including Windows, Mac OS X, and Linux-based platforms. You can view a complete list of supported operating systems on the Wire-shark home page.

#### Installing Wireshark

The Wireshark installation process is surprisingly simple. However, before you install Wireshark, make sure that your system meets the following requirements:

- More than 400 MHz processor or faster
- More than 512 MB RAM
- At least 75 MB of available storage space
- NIC that supports promiscuous mode
- WinPcap capture driver The WinPcap capture driver is the Windows implementation of the pcap packet-capturing application programming interface (API). Simply put, this driver interacts with your operating system to capture raw packet data, apply filters, and switch the NIC in and out of promiscuous mode.

Although you can download WinPcap separately (from <http://www.winpcap.org/>), it is typically better to install WinPcap from the Wireshark installation package, because the included version of WinPcap has been tested to work with Wireshark.

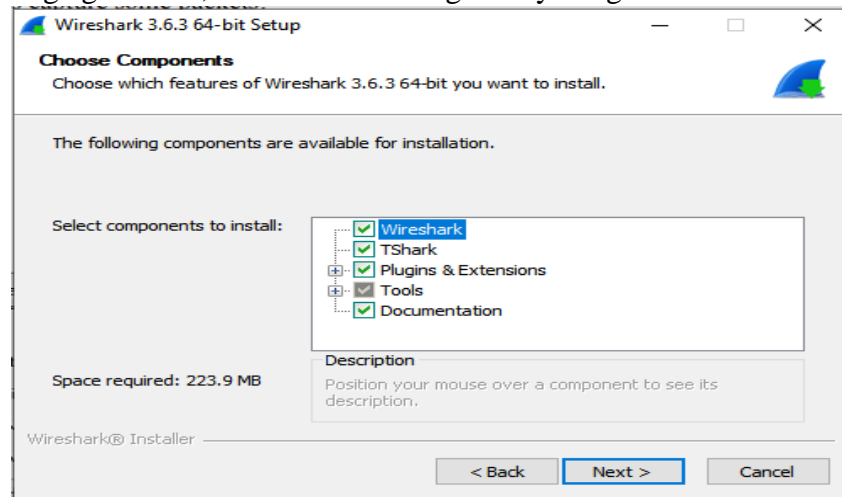
**Installing on Microsoft Windows Systems** The first step when installing Wireshark under Windows is to obtain the latest installation build from the official Wireshark web page, <http://www.wireshark.org/>. Navigate to the Downloads section on the website and choose a mirror. Once you've downloaded the package, follow these steps:



**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

---

1. Double-click the .exe file to begin installation, and then click Next in the introductory window.
2. Read the licensing agreement, and then click I Agree if you agree.



**Fig.1 Choosing Wireshark Components you wish to install**

3. Select the components of Wireshark you wish to install. For our purposes, you can accept the defaults by clicking Next.
4. Click Next in the Additional Tasks window.
5. Select the location where you wish to install Wireshark, and then click Next.
6. When the dialog asks whether you want to install WinPcap, make sure the Install WinPcap box is checked, and then click Install. The installation process should begin.
7. About halfway through the Wireshark installation, the WinPcap installation should start. When it does, click Next in the introductory window, read the licensing agreement, and then click I Agree.
8. WinPcap should install on your computer. After this installation is complete, click Finish.
9. Wireshark should complete its installation. When it's finished, click Next.
10. In the installation confirmation window, click Finish.

### **Wireshark Fundamentals**

Once you've successfully installed Wireshark on your system, you can begin to familiarize yourself with it. Now you finally get to open your fully functioning packet sniffer and see . . . absolutely nothing! Okay, so Wireshark isn't very interesting when you first open it. In order for things to really get exciting, you need to get some data.



## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

---

#### **Your First Packet Capture**

To get packet data into Wireshark, you'll perform your first packet capture. You may be thinking, "How am I going to capture packets when nothing is wrong on the network?" First, there is always something wrong on the network. If you don't believe me, then go ahead and send an email to all your network users and let them know that everything is working perfectly. Secondly, there doesn't need to be something wrong for you to perform packet analysis. In fact, most packet analysts spend more time analyzing problem free traffic than traffic that they troubleshoot network traffic. For example, if you ever hope to solve a problem with DHCP by analyzing its traffic, you must understand what the flow of working DHCP traffic looks like. More broadly, to find anomalies in daily network activity, you must know what normal daily network activity looks like. When your network is running smoothly, you can set your baseline so that you'll know what its traffic looks like in a normal state.

So, let's capture some packets!

1. Open Wireshark.
2. From the main drop-down menu, select Capture and then Interfaces. You should see a dialog listing the various interfaces that can be used to capture packets, along with their IP addresses.
3. Choose the interface you wish to use, and click Start, or simply click the interface under the Interface List section of the welcome page. Data should begin filling the window.
4. Wait about a minute or so, and when you are ready to stop the capture and view your data, click the Stop button from the Capture drop-down menu.

Once you have completed these steps and finished the capture process, the Wireshark main window should be alive with data. As a matter of fact, you might be overwhelmed by the amount of data that appears, but it will all start to make sense very quickly as we break down the main window of Wireshark one piece at a time.

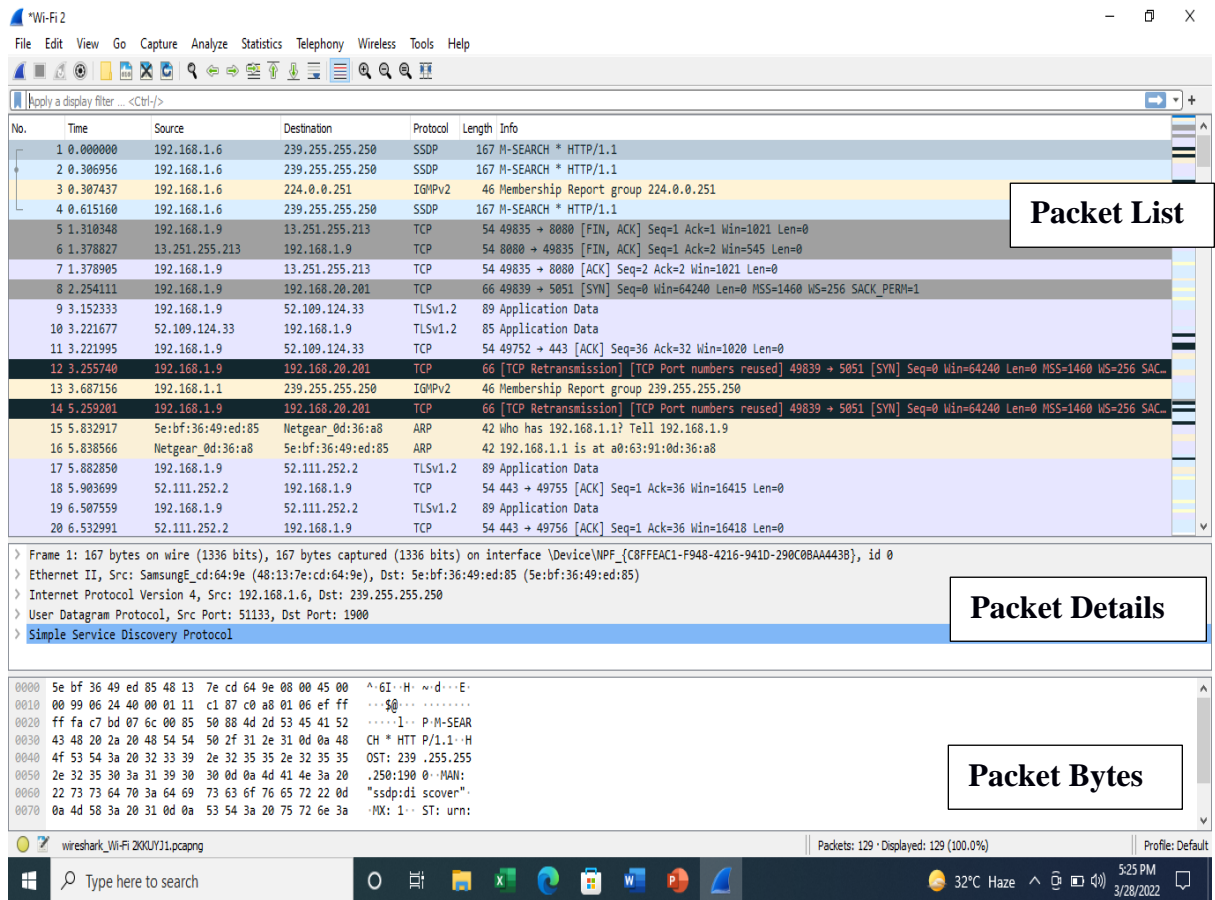
#### **Wireshark's Main Window**

You'll spend most of your time in the Wireshark main window. This is where all the packets you capture are displayed and broken down into a more understandable format. Using the packet capture you just made, let's look at Wireshark's main window, as shown in Figure-2



# Vidyavardhini's College of Engineering & Technology

## Department of Electronics and Telecommunication Engineering



**Figure-2: The Wireshark main window uses a three-pane design**

The three panes in the main window depend on one another. To view the details of an individual packet in the Packet Details pane, you must first select that packet by clicking it in the Packet List pane. Once you've selected your packet, you can see the bytes that correspond with a certain portion of the packet in the Packet Bytes pane when you click that portion of the packet in the Packet Details pane.

Here's what each pane contains:

**Packet List:** The top pane displays a table containing all packets in the current capture file. It has columns containing the packet number, the relative time the packet was captured, the source and destination of the packet, the packet's protocol, and some general information found in the packet.

**Packet Details:** The middle pane contains a hierarchical display of information about a single packet. This display can be collapsed and expanded to show all of the information collected about an individual packet.



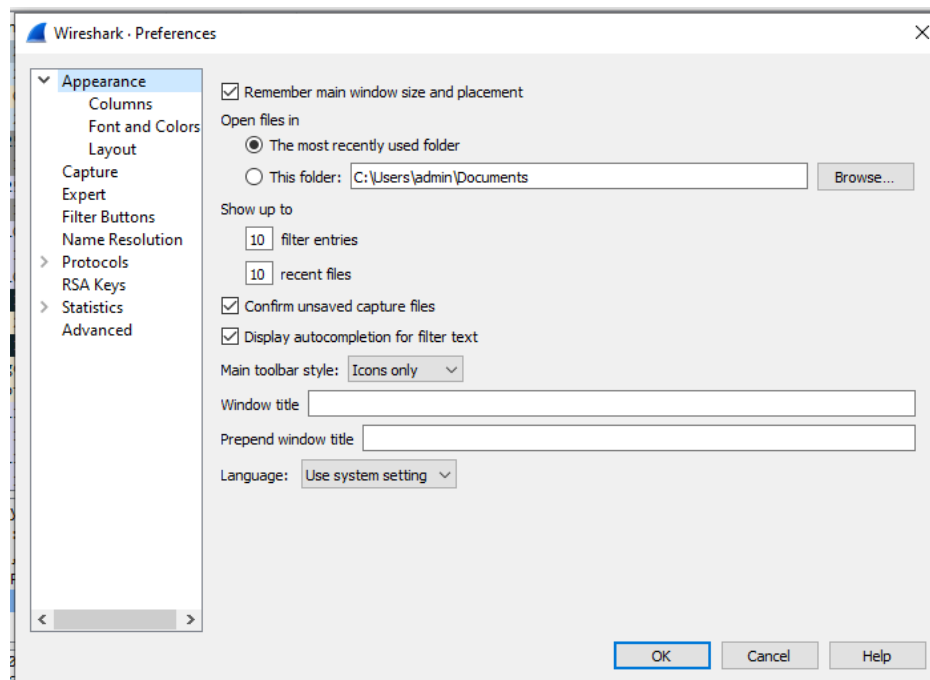
## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

**Packet Bytes:** The lower pane perhaps the most confusing displays a packet in its raw, unprocessed form; that is, it shows what the packet looks like as it travels across the wire. This is raw information with nothing warm or fuzzy to make it easier to follow.

### Wireshark Preferences

Wireshark has several preferences that can be customized to meet your needs. To access Wireshark's preferences, select Edit from the main drop-down menu and click Preferences. You'll see the Preferences dialog, which contains several customizable options, as shown in Figure-5.



**Figure-3: You can customize Wireshark using preference dialogue options**

Wireshark's preferences are divided into six major sections:

- 1. User Interface:** These preferences determine how Wireshark presents data. You can change most options here according to your personal preferences, including whether to save window positions, the layout of the three main panes, the placement of the scroll bar, the placement of the Packet List pane columns, the fonts used to display the captured data, and the background and foreground colors.
- 2. Capture** These preferences allow you to specify options related to the way packets are captured, including your default capture interface, whether to use promiscuous mode by default, and whether to update the Packet List pane in real time.



## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

**3. Printing** The preferences in this section allow you to specify various options related to the way Wireshark prints your data.

**4. Name Resolution** Through these preferences, you can activate features of Wireshark that allow it to resolve addresses into more recognizable names (including MAC, network, and transport name resolution) and specify the maximum number of concurrent name resolution requests.

**5. Statistics** This section provides a few configurable options for Wireshark's statistical features. **6. Protocols** The preferences in this section allow you to manipulate options related to the capture and display of the various packets Wireshark is capable of decoding. Not every protocol has configurable preferences, but some have several options that can be changed

These options are best left at their defaults unless you have a specific reason to change them.

**Packet Color Coding** If you are anything like me, you may enjoy shiny objects and pretty colors. If that is the case, you probably got excited when you saw all those different colors in the Packet List pane, as in the example in Figure

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.6	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
2	0.306956	192.168.1.6	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
3	0.307437	192.168.1.6	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
4	0.615160	192.168.1.6	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
5	1.310348	192.168.1.9	13.251.255.213	TCP	54	49835 → 8080 [FIN, ACK] Seq=1 Ack=1 Win=1021 Len=0
6	1.378827	13.251.255.213	192.168.1.9	TCP	54	8080 → 49835 [FIN, ACK] Seq=1 Ack=2 Win=545 Len=0
7	1.378905	192.168.1.9	13.251.255.213	TCP	54	49835 → 8080 [ACK] Seq=2 Ack=2 Win=1021 Len=0
8	2.254111	192.168.1.9	192.168.20.201	TCP	66	49839 → 5051 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
9	3.152333	192.168.1.9	52.109.124.33	TLsv1.2	89	Application Data
10	3.221677	52.109.124.33	192.168.1.9	TLsv1.2	85	Application Data
11	3.221995	192.168.1.9	52.109.124.33	TCP	54	49752 → 443 [ACK] Seq=36 Ack=32 Win=1020 Len=0
12	3.255740	192.168.1.9	192.168.20.201	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49839 → 5051 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
13	3.687156	192.168.1.1	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250

**Figure-4: Wireshark color coding allows for quick protocol identification**

Each packet is displayed as a certain color for a reason. These colors reflect the packet's protocol. For example, all DNS traffic is blue, and all HTTP traffic is green. The color coding allows you to quickly differentiate between various protocols so that you don't need to read the protocol field in the Packet List pane for each individual packet. You will find that this greatly speeds up the time it takes to browse through large capture files. Wireshark makes it easy to see which colors are assigned to each protocol through the Coloring Rules window, shown in Figure-5. To open this window, select View from the main drop-down menu and click Coloring Rules



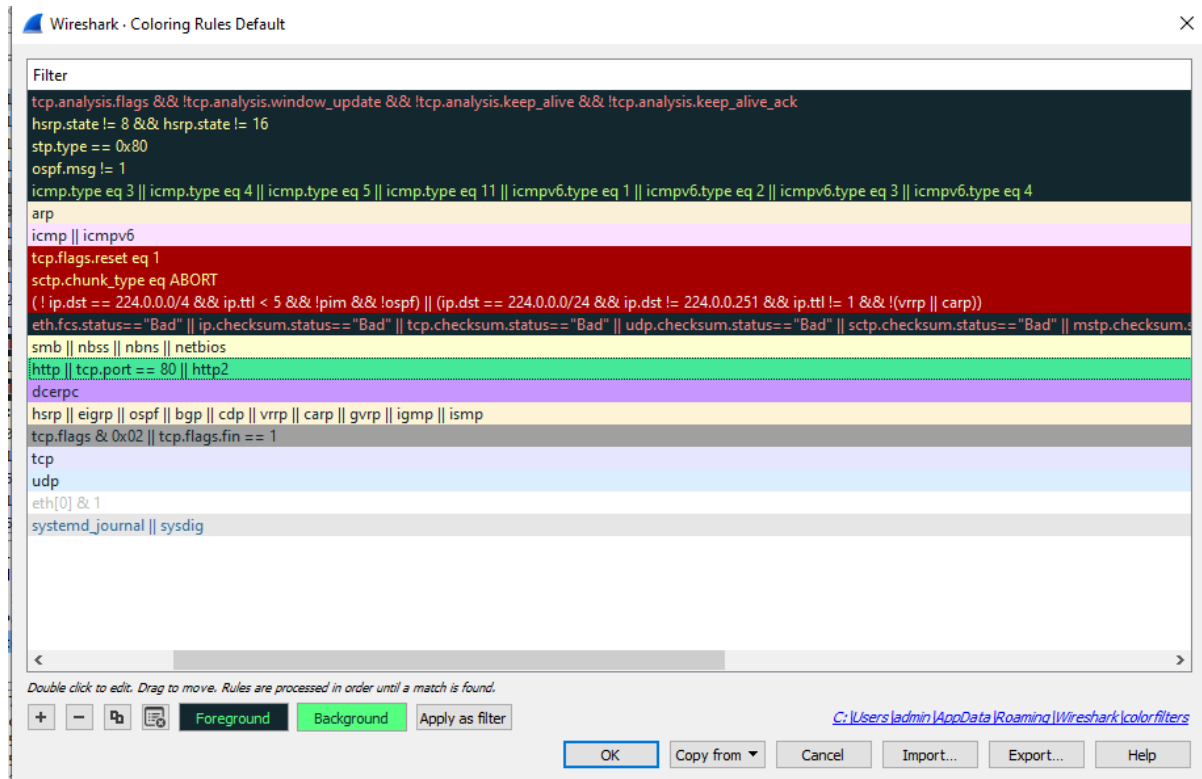






## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering



**Figure-6: When editing a color filter, you can modify both foreground and background colors**

As you work with Wireshark on your network, you will notice that you deal with certain protocols more than others. Here's where color-coded packets can make your life a lot easier. For example, if you think that there is a rogue DHCP server on your network handing out IP leases, you could simply modify the coloring rule for the DHCP protocol so that it shows up in bright yellow (or some other easily identifiable color). This would allow you to pick out all DHCP traffic much more quickly and make your packet analysis more efficient. These coloring rules can also be further extended by creating them based on your own custom filters. Now that you have Wireshark up and running, you're ready to do some packet analysis.



## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

---

#### Experiment 9B

**Aim:** Study of working with captured packets.

#### **Learning Objective:**

At the end of the session, you will be able to

- work with capture files, packets, and time-display formats
- also cover more advanced options for capturing packets and dive into the world of filters.
- save your capture files to be analyzed later. You can also merge multiple capture files.

**Working with Capture Files** As you perform packet analysis, you will find that a good portion of the analysis you do will happen after your capture. Usually, you will perform several captures at various times, save them, and analyze them all at once. Therefore, Wireshark allows you to save your capture files to be analyzed later. You can also merge multiple capture files.

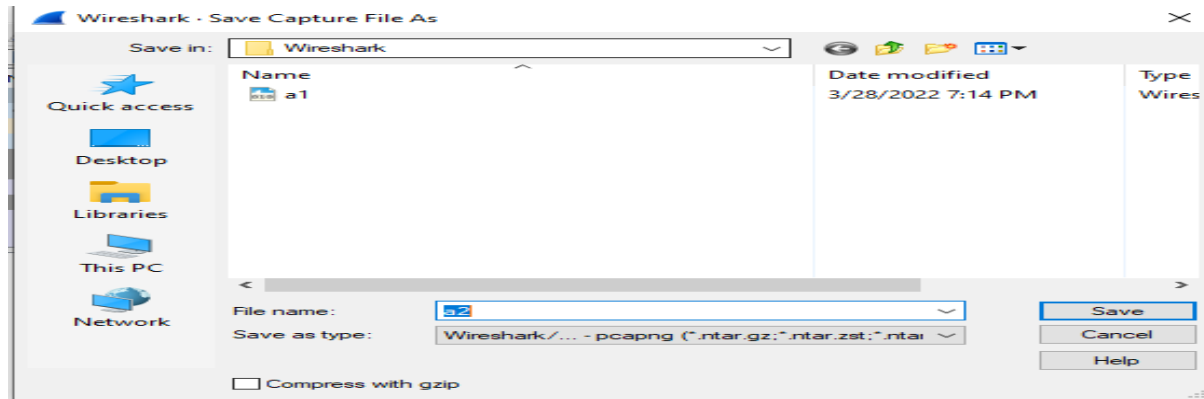
#### **Saving and Exporting Capture File**

To save a packet capture, select File - Save As. You should see the Save File As dialog, as shown in Figure-1. You're asked for a location to save your packet capture and for the file format you wish to use. If you do not specify a file format, Wireshark will use the default. pcap file format. One of the more powerful features of the Save File As dialog is the ability to save a specific packet range. This is a great way to thin bloated packet capture files. You can choose to save only packets in a specific number range, marked packets, or packets visible as the result of a display filter (marked packets and filters are discussed later in this chapter). You can export your Wireshark capture data into several different formats for viewing in other media or for importing into other packet-analysis tools. Formats, include plaintext, PostScript, comma-separated values (CSV), and XML. To export your packet capture, choose File - Export, and then select the format for the exported file. You will see a Save As dialog containing options related to that specific format



## Vidyavardhini's College of Engineering & Technology

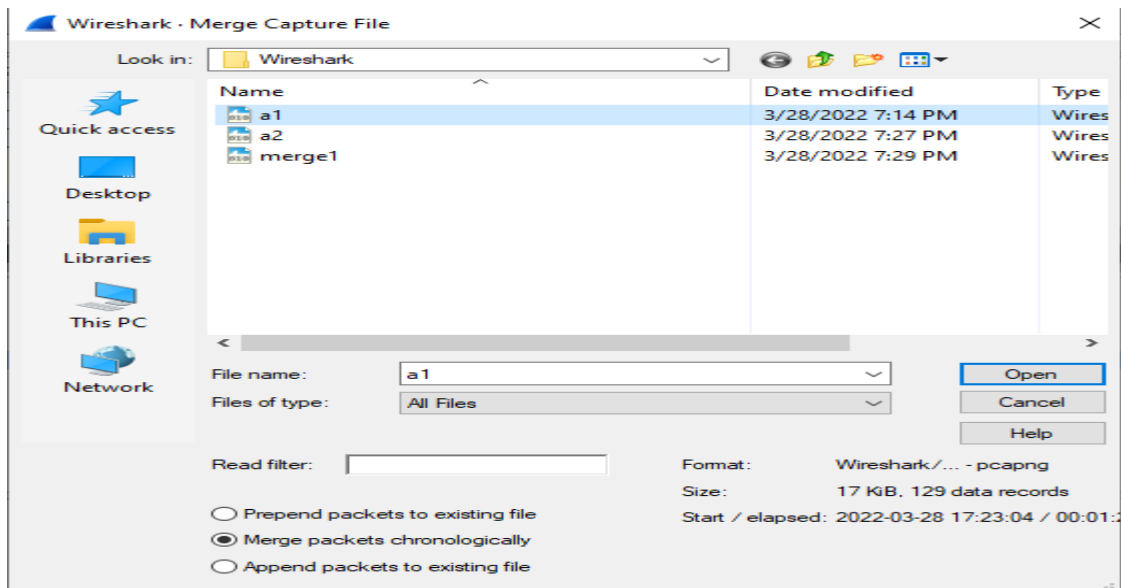
### Department of Electronics and Telecommunication Engineering



**Fig 1: Save file as dialog allows you to save your packet capture**

**Merging Capture Files** Certain types of analysis require the ability to merge multiple capture files. This is a common practice when comparing two data streams or combining streams of the same traffic that were captured separately.

To merge capture files, open one of the capture files you want to merge and choose File - Merge to bring up the Merge with Capture File dialog, shown in Figure-2. Select the new file you wish to merge into the already open file, and then select the method to use for merging the files. You can prepend the selected file to the currently open one, append it, or merge the files chronologically based on their timestamps



**Fig 2: Merge with capture file dialog allows to merge two capture files**



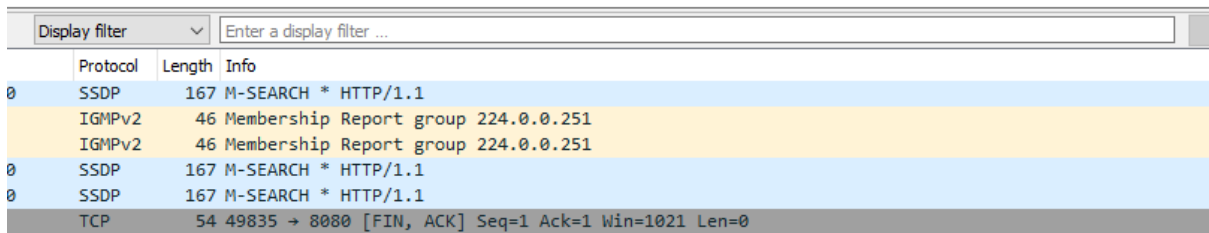
## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

#### Working with Packets

You will eventually encounter situations involving a very large number of packets. As the number of these packets grows into the thousands and even millions, you will need to be able to navigate through packets more efficiently. For this purpose, Wireshark allows you to find and mark packets that match certain criteria. You can also print packets for easy reference.

**Finding Packets** To find packets that match particular criteria, open the Find Packet dialog, shown in Figure-3, by pressing CTRL-F.



	Protocol	Length	Info
0	SSDP	167	M-SEARCH * HTTP/1.1
	IGMPv2	46	Membership Report group 224.0.0.251
	IGMPv2	46	Membership Report group 224.0.0.251
0	SSDP	167	M-SEARCH * HTTP/1.1
0	SSDP	167	M-SEARCH * HTTP/1.1
	TCP	54	49835 → 8080 [FIN, ACK] Seq=1 Ack=1 Win=1021 Len=0

**Fig 3: Finding packets in Wireshark based on specific criteria**

This dialog offers three options for finding packets:

- The Display filter option allows you to enter an expression-based filter that will find only those packets that satisfy that expression.
- The Hex value option searches for packets with a hexadecimal (with bytes separated by colons) value you specify.
- The String option searches for packets with a text string you specify.

Table-1 shows examples of these search types. Other options include the ability to select the window in which you want to search, the character set to use, and the search direction. You can extend the capability of your string searches by specifying the pane the search is per-formed in, setting the character set used, and making the search case sensitive



## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

Table-1: Search Types for Finding Packets

Search Type	Examples
Display filter	not ip ip addr--192.168.0.1 arp
Hex value	00:ff ff:ff 00:AB:B1:fo
String	Workstation1 UserB domain

Once you've made your selections, enter your search criteria in the text box, and click Find to find the first packet that meets your criteria. To find the next matching packet, press CTRL-N; find the previous matching packet by pressing CTRL-B.

**Marking Packets** After you have found the packets that match your criteria, you can mark those of particular interest. For example, you may want to mark packets to be able to save those packets separately or to find them quickly based on the coloration. Marked packets stand out with a black background and white text, as shown in Figure-4. (You can also sort out only marked packets when saving packet captures.) To mark a packet, right-click it in the Packet List pane and choose Mark Packet from the pop-up or click a packet in the Packet List pane and press CTRL-M. To unmark a packet, toggle this setting off using CTRL-M again. You can mark as many packets as you wish in a capture. To jump forward and backward between marked packets, press SHIFT-CTRL-N and SHIFT-CTRL-B, respectively.

**Marking Packets** After you have found the packets that match your criteria, you can mark those of particular interest. For example, you may want to mark packets to be able to save those packets separately or to find them quickly based on the coloration. Marked packets stand out with a black background and white text, as shown in Figure-4. (You can also sort out only marked packets when saving packet captures.) To mark a packet, right-click it in the Packet List pane and choose Mark Packet from the pop-up or click a packet in the Packet List pane and press CTRL-M.

No.	Time	Source	Destination	Protocol	Length	Info
72	14.336445	192.168.1.6	224.0.0.251	NDNS	103	Standard query 0x0004 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, _
73	14.351287	HonHaiPr_b5:10:f9	5e:bf:36:49:ed:85	ARP	42	Who has 192.168.1.9? Tell 192.168.1.2
74	14.351287	HonHaiPr_b5:10:f9	5e:bf:36:49:ed:85	ARP	42	Who has 192.168.1.9? Tell 192.168.1.2
75	14.351331	5e:bf:36:49:ed:85	HonHaiPr_b5:10:f9	ARP	42	192.168.1.9 is at 5e:bf:36:49:ed:85
76	14.351331	5e:bf:36:49:ed:85	HonHaiPr_b5:10:f9	ARP	42	192.168.1.9 is at 5e:bf:36:49:ed:85
77	15.257890	192.168.1.2	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
78	15.257890	192.168.1.2	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250

Fig 4: A marked packet is highlighted on your screen



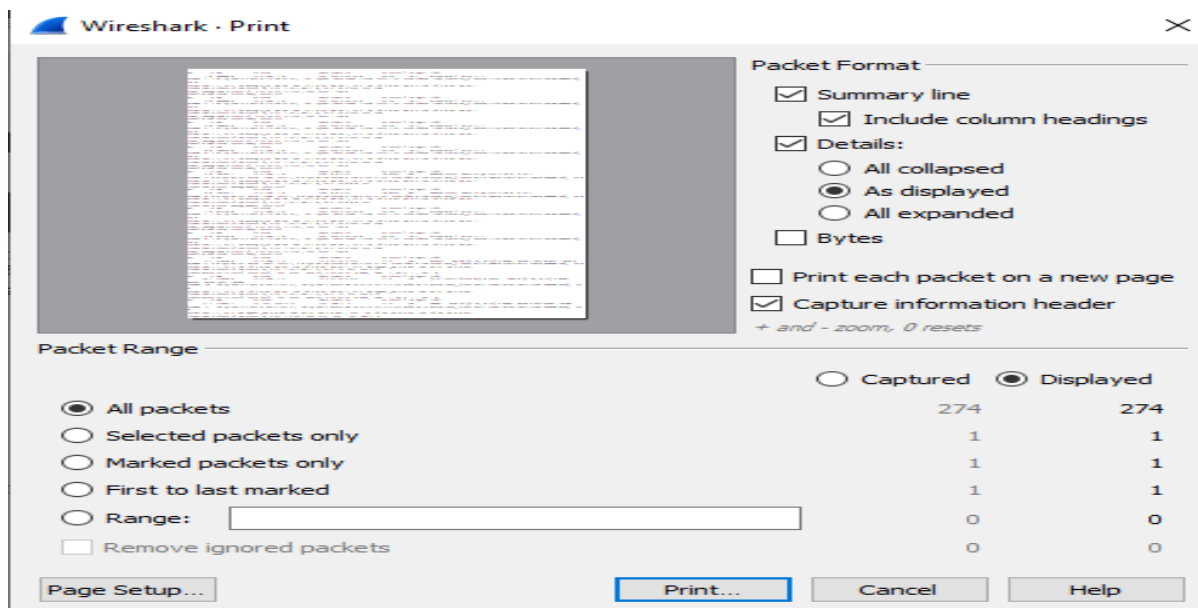
## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

To unmark a packet, toggle this setting off using CTRL-M again. You can mark as many packets as you wish in a capture. To jump forward and backward between marked packets, press SHIFT-CTRL-N and SHIFT-CTRL-B, respectively.

### Printing Packet

Although most analysis will take place on the computer screen, you may need to print captured data. Being able to print packets to a PDF file is also very convenient, especially when preparing reports. To print captured packets, open the Print dialog by choosing File - Print from the main menu. You will see the Print dialog, as shown in Figure-5



**Fig 5: Print dialog allows you to print thr packets you specify**

You can print the selected data as plaintext or PostScript, or to an output file. As with the Save File As dialog, you can print a specific packet range, marked packets only, or packets displayed as the result of a filter. You can also select which of Wireshark's three main panes to print for each packet. Once you have selected the options, click Print.

### Setting Time Display Formats and References

Time is of the essence especially in packet analysis. Everything that happens on a network is time sensitive, and you will need to examine trends and network latency in nearly every capture file. Wireshark recognizes the importance of time and supplies several configurable options relating to it. In this section, we'll look at time display formats and references.



## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

**Time Display Formats** Each packet that Wireshark captures is given a timestamp, which is applied to the packet by the operating system. Wireshark can show the absolute timestamp indicating the exact moment when the packet was captured, as well as the time in relation to the last captured packet and the beginning and end of the capture. The options related to the time display are found under the View heading on the main menu. The Time Display Format section, lets you configure the presentation format as well as the precision of the time display. The presentation format option lets you choose various options for time display. The precision options allow you to set the time display precision to automatic or to a manual setting, such as seconds, milliseconds, micro-seconds, and so on.

**Packet Time Referencing** Packet time referencing allows you to configure a certain packet so that all subsequent time calculations are done in relation to that specific packet. This feature is particularly handy when you are examining a series of sequential events that are triggered somewhere other than the start of the capture file. To set a time reference to a certain packet, select the reference packet in the Packet List pane, and then choose Edit - Set Time Reference from the main menu. To remove a time reference from a certain packet, select the packet and toggle off the Edit - Set Time Reference setting. When you enable a time reference on a particular packet, the Time column in the Packet List pane will display \*REF\*, as shown in Figure-6.

The screenshot shows the Wireshark interface with a packet capture named 'merge1.pcapng'. The packet list pane shows a list of packets. Packet 56 is selected, and its time is displayed as '\*REF\*'. The packet details pane shows the following information:

No.	Time	Source	Destination	Protocol	Length	Info
52	2022-03-28 17:23:14.855255	192.168.1.6	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
53	2022-03-28 17:23:15.251256	192.168.1.6	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
54	2022-03-28 17:23:15.251256	192.168.1.6	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
55	2022-03-28 17:23:15.558548	192.168.1.6	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
56	*REF*	192.168.1.2	192.168.1.9	UDP	455	37294 → 62749 Len=413
57	2022-03-28 17:23:15.558548	192.168.1.6	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
58	2022-03-28 17:23:15.558548	192.168.1.2	192.168.1.9	UDP	455	37294 → 62749 Len=413
59	2022-03-28 17:23:15.797651	192.168.1.9	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
60	2022-03-28 17:23:15.797651	192.168.1.9	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1

Packet details for packet 56:

- > Frame 56: 455 bytes on wire (3640 bits), 455 bytes captured (3640 bits) on interface \Device\NPF\_{C8FFEAC1-F948-4216-941D-290C08AA443B}, id 0
- > Ethernet II, Src: HonHaiPr\_b5:10:f9 (38:b1:db:b5:10:f9), Dst: 5e:bf:36:49:ed:85 (5e:bf:36:49:ed:85)
- > Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.9
- > User Datagram Protocol, Src Port: 37294, Dst Port: 62749
- > Data (413 bytes)

**Fig 6: A packet with packet time reference toggle enabled**

Setting a packet time reference is useful only when the time display for-mat of a capture is set to display the time in relation to the beginning of the capture. Any other setting will produce no usable results and will create a set of times that can be very confusing.

### Setting Capture Options



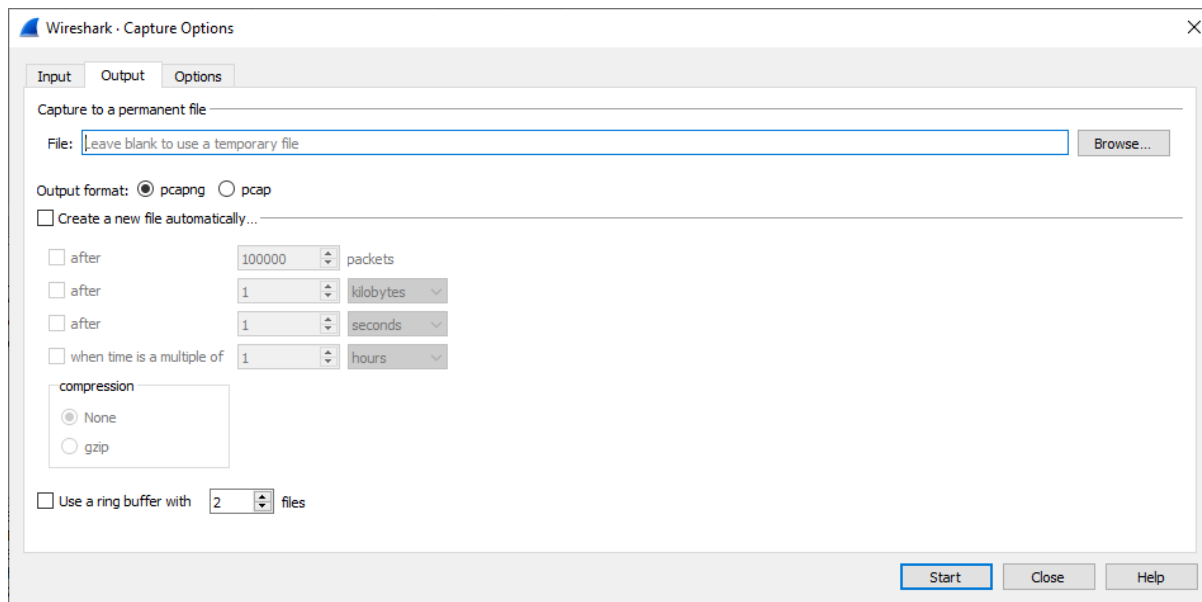
## Vidyavardhini's College of Engineering & Technology

### Department of Electronics and Telecommunication Engineering

Wireshark offers quite a few more capture options in the Capture Options dialog. To open this dialog, choose Capture - Interfaces and click the Options button next to the interface on which you want to capture packets. The Capture Options dialog has more bells and whistles than you can shake a stick at, all designed to give you more flexibility while capturing packets. It's divided into Capture, Capture Files, Stop Capture, Display Options, and Name Resolution sections, out of which only capture setting discussed here

### Capture Settings

The Interface drop-down list in the Capture section is where you can select the network interface to configure. The left drop-down list allows you to specify whether the interface is local or remote, and the right drop-down list shows all available capture interfaces. The IP address of the interface you have selected is displayed directly below this drop-down list.



checkboxes on the left side of the dialog box allow you to enable or disable promiscuous mode (always enabled by default), capture packets in the currently experimental pcap-ng format and limit the size of each capture packet by bytes. The buttons on the right side of the Capture section let you access wireless and remote settings (as applicable). Beneath those is the buffer size option, which is available only on systems running Microsoft Windows. You can specify the amount of capture packet data that is stored in the kernel buffer before it is written to disk. (This is a value you won't normally modify unless you begin noticing that you are dropping a lot of packets.)





**Vidyavardhini's College of Engineering & Technology**  
**Department of Electronics and Telecommunication Engineering**

---

**Result analysis and Conclusion:**

### **Post Experiment Quiz:**

Answer the following questions for the TCP segments:

1. What is the IP address and TCP port number used by your client computer (source) to transfer the file to `www.vcet.edu.in`?
2. What is the IP address and port number used by `www.vcet.edu.in` to receive the file?
3. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and `www.vcet.edu.in`? What is it in the segment that identifies the segment as a SYN segment?
4. What is the sequence number of the SYNACK segment sent by `gaia.cs.umass.edu` to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did `www.vcet.edu.in` determine that value? What is it in the segment that identifies the segment as a SYNACK segment?



## Experiment 10

**AIM:** To compare TCP (connection oriented) and UDP (connectionless) performance using Netsim.

**Objective:** Simulate a three-node point to point network with the links connected as follows: N0-n2, n1-n2, n2-n3. Apply TCP agent between n0-n3 & UDP between n1-n3. Apply relevant applications over TCP & UDP agents changing the parameter and determine the number of packets sent by TCP/UDP

**REQUIREMENT:** NETSIM Software

TCP recovers data that is damaged, lost duplicated or delivered out of order by the internet communication system. This is achieved by assigning a sequence number to each octet transmitted and requiring positive acknowledgement (ACK) from the receiving TCP. If the ACK is not received within a timeout interval, the data is retransmitted. At the receiver side sequence number is used to eliminate the duplicates as well as to order the segments in correct order since there is a chance of “out of order “ reception .Therefore in TCP no transmission errors will affect the correct delivery of data.

UDP:

UDP uses a simple transmission model with a minimum of protocol mechanism. It has no handshaking dialogues ,and thus exposes any unreliability of the underlying network protocol to the users program .As this is normally IP over unreliable media, there is no guarantee of delivery, ordering or duplicate protection.

**SIMULATION SCENARIO:**

**PROCEDURE:**

Create Scenario:” Simulation□New□Internetworks”

Click and drop Router, Wired Nodes and Application onto the simulation Environment from tool bar. Sample Inputs

Sample Inputs:

Sample 1:

Wired Node Properties	Wired Node B	Wired Node C
Transport Layer Properties		
TCP	Enable	Disable
UDP	Disable	Enable



Application Properties:

<b>Application Type</b>	custom	custom
<b>Source ID</b>	2(wired Node B)	3(Wired Node C)
<b>Destination ID</b>	4((wired Node D)	4(Wired Node D)
<b>Packet Size</b>		
<b>Distribution</b>	Constant	Constant
<b>Value(Bytes)</b>	1460	1460

<b>Inter arrival Time</b>		
<b>Distribution</b>	Constant	Constant
<b>Value(Bytes)</b>	10000	10000

To add an application, click add button in application property.

Router Properties:

Accept the default properties for all Wired Links.

Sample 1: Wired Node B and Wired Node C transmit data to Wired Node D with the packet Interval Arrival Time as 1000  $\mu$ s.

Likewise do the Sample 2 and Sample 3 by decreasing the Packet Inter Arrival Time as 5000  $\mu$ s and 2500  $\mu$ s respectively.

Simulation Time-100 Sec

Comparison Chart:

The number of Segments Sent, Segments Received and Datagram Sent, Datagram Received will be available in the TCP Metrics and UDP Metrics of “Performance Metrics” screen of NetSim Graph I

The Packets transmitted successfully “for TCP is Segments Received and for UDP is Datagram Received of the destination node i.e., wired Node 3

Graph II

Number of lost packets in TCP and UDP

To get the “No. of packet lost”, For TCP, get the difference between Segments Sent and Segment Received and for UDP, get the difference between Datagram Sent and Datagram Received.



Vidyavardhini's College of Engineering & Technology  
Department of Electronics and Telecommunication Engineering

---

OBSERVATION TABLE:

Sr.No	Sample	Interarrival time	Throughput		Delay		Packet loss	
			TCP	UDP	TCP	UDP	TCP	UDP
1	1	10,000	1.167	1.165	279.675	254.182	0	22
2	2	5,000	2.335	2.330	291.445	254.171	0	46
3	3	2500	4.670	4.660	318.433	254.165	996	64

**Result analysis and Conclusion:**

**Post Experiment questions:** Write applications which are based on TCP and UDP.



## **Experiment 11**

**Aim:** Study the throughputs of Slow start + Congestion avoidance (Old Tahoe) and Fast Retransmit (Tahoe) Congestion Control Algorithms.

**Learning Objectives:** Part 1: To configure 1 client and 1 server model

Compare Old Tahoe and Tahoe

Part 2: To configure 2 client and 2 server model

Compare Old Tahoe and Tahoe

**REQUIREMENT:** NetSim Software

### **Theory:**

One of the important functions of a TCP Protocol is congestion control in the network. Given below is a description of how Old Tahoe and Tahoe variants (of TCP) control congestion. Old Tahoe: Congestion can occur when data arrives on a big pipe (i.e. a fast LAN) and gets sent out through a smaller pipe (i.e. a slower WAN). Congestion can also occur when multiple input streams arrive at a router whose output capacity is less than the sum of the inputs. Congestion avoidance is a way to deal with lost packets. The assumption of the algorithm is that the packet loss caused by damaged is very small (much less than 1%), therefore the loss of a packet signals congestion somewhere in the network between the source and destination. There are two indications of packets loss: a timeout occurring, and the receipt of duplicate ACKs Congestion avoidance and slow start are independent algorithms with different objectives. But when congestion occurs TCP must slow down its transmission rate and then invoke slow start to get things going again. In practice they are implemented together. Congestion avoidance and slow start requires two variables to be maintained for each connection: a Congestion Window (i.e. cwnd) and a Slow Start Threshold Size (i.e. ssthresh). Old Tahoe algorithm is the combination of slow start and congestion avoidance. The combined algorithm operates as follows,

1. Initialization for a given connection sets cwnd to one segment and ssthresh to 65535 bytes.
2. When congestion occurs (indicated by a timeout or the reception of duplicate ACKs), one-half of the current window size (the minimum of cwnd and the receiver's advertised window, but at least two segments) is saved in ssthresh. Additionally, if the congestion is indicated by a timeout, cwnd is set to one segment (i.e. slow start).
3. When new data is acknowledged by the other end, increase cwnd, but the way it increases depends on whether TCP is performing slow start or congestion avoidance. If cwnd is less than or equal to ssthresh, TCP is in slow start. Else TCP is performing congestion avoidance. Slow start continues until TCP is halfway to where it was when congestion occurred (since it recorded half of the window size that caused the problem in step 2). Then congestion avoidance takes over. Slow start has cwnd begins at one segment and be incremented by one segment



every time an ACK is received. As mentioned earlier, this opens the window exponentially: send one segment, then two, then four, and so on. Congestion avoidance dictates that cwnd be incremented by  $1/\text{cwnd}$ , compared to slow start's exponential growth. The increase in cwnd should be at most one segment in each round-trip time (regardless of how many ACKs are received in that RTT), whereas slow start increments cwnd by the number of ACKs received in a round-trip time. Tahoe (Fast Retransmit): The Fast retransmit algorithms operating with Old Tahoe is known as the Tahoe variant. TCP may generate an immediate acknowledgement (a duplicate ACK) when an out-of-order segment is received out-of-order, and to tell it what sequence number is expected. Since TCP does not know whether a duplicate ACK is caused by a lost segment or just a re-ordering of segments, it waits for a small number of duplicate ACKs to be received. It is assumed that if there is just a reordering of the segments, there will be only one or two duplicate ACKs before the re-ordered segment is processed, which will then generate a new ACK. If three or more duplicate ACKs are received in a row, it is a strong indication that a segment has been lost. TCP then performs a retransmission of what appears to be the missing segment, without waiting for a re-transmission timer to expire.

### Procedure:

Go to Simulation ➡ New ➡ Internetworks

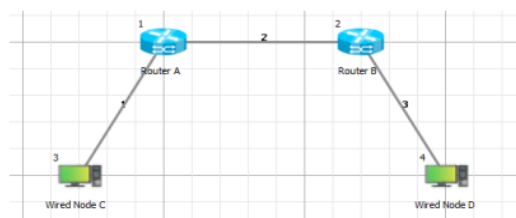
Sample 1.a:

Old Tahoe (1 client and 1 server) In this Sample,

- Total no of Node used: 2
- Total no of Routers used: 2

The devices are interconnected as given below, • Wired Node C is connected with Router A by Link 1.

- Router A and Router B are connected by Link 2.
- Wired Node D is connected with Router B by Link 3.



Set the properties for each device by following the tables,



Application Properties	
Application Type	Custom
Source_Id	4(Wired Node D)
Destination_Id	3(Wired Node C)

Packet Size	
Distribution	Constant
Value (bytes)	1460
Inter Arrival Time	
Distribution	Constant
Value (micro secs)	1300

Node Properties: In Transport Layer properties, set

TCP Properties	
MSS(bytes)	1460
Congestion Control Algorithm	Old Tahoe
Window size(MSS)	8

Router Properties: Accept default properties for Router.

Link Properties	Link 1	Link 2	Link 3
Max Uplink Speed (Mbps)	8	10	8
Max Downlink Speed(Mbps)	8	10	8
Uplink BER	0.000001	0.000001	0.000001
Downlink BER	0.000001	0.000001	0.000001

**Simulation Time** - 10 Sec Upon completion of simulation, "Save" the experiment.

#### Sample 1.b:

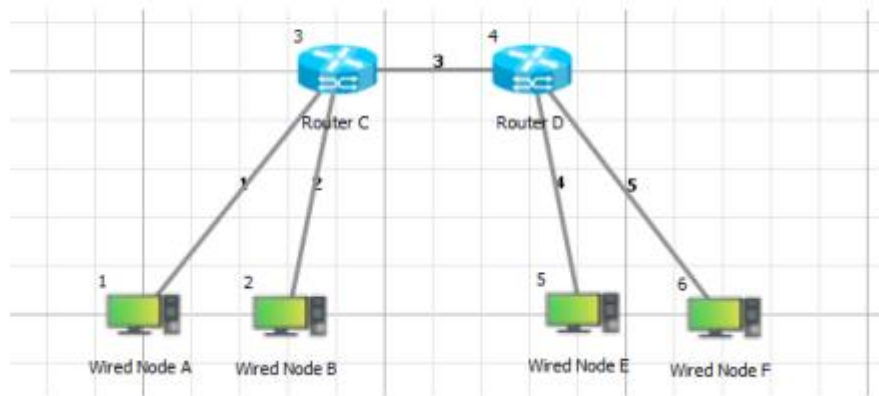
Tahoe (1 client and 1 server) Open sample 1.a, and change the TCP congestion control algorithm to Tahoe (in Node Properties). Upon completion of simulation, "Save" the experiment as sample 1.b





**Sample 2.a: Old Tahoe (2 clients and 2 servers)**

In this Sample,



Total no of Wired Nodes used: 4

- Total no of Routers used: 2 The devices are interconnected as given below,
- Wired Node A and Wired Node B are connected with Router C by Link 1 and Link 2.
- Router C and Router D are connected by Link 3.
- Wired Node E and Wired Node F are connected with Router D by Link 4 and Link 5.
- Wired Node A and Wired Node B are not transmitting data in this sample.

Simulation Time - 10 Sec

**Sample 2.b:**

Tahoe (2 clients and 2 servers) Do the experiment as sample 2.a, and change the congestion control algorithm to Tahoe. Upon completion of simulation, “Save” the experiment.

Output:

Comparison Table:

TCP Downloads	Metric	Slow Start+ Congestion Avoidance (Old Tahoe)	Fast Retransmit Tahoe
1 Client 1 Server	Throughput (MBPS)	5.926	6.12
	Segments Retransmitted +	192	231



Vidyavardhini's College of Engineering & Technology  
Department of Electronics and Telecommunication Engineering

		Seg Fast Retransmitted		
2 Clients Servers	2	Throughput (MBPS)	8.79	8.8
		Segments Retransmitted + Seg Fast Retransmitted	343	378

**Result analysis and Conclusion:**

**Post Experiment questions:** Discuss congestion control in wireless and wired networks.