Gokhale Education Society's

R. H. SAPAT COLLEGE OF ENGINEERING,

MANAGEMENT STUDIES AND RESEARCH

Prin. T. A. Kulkarni Vidyanagar, Nashik-422005.

DEPARTMENT OF

ELECTRONICS AND TELECOMMUNICATION

ENGINEERING

Computer Network

Third Year of Engineering (T.E.)

(2019 Course)

Prepared By- Mrs. G.R.Kawale

VISION AND MISSION OF THE INSTITUTE

VISION

- To Produce World class Engineers for converting global challenges into Opportunities through "Value Embedded Quality Technical Education".
- To develop this College as an Academy of Higher Learning in the field of Engineering & Technology.

MISSION

- To Impart Technical Education through effective Teaching-learning process
- To Nurture Creativity & Critical thinking in applying Engineering skills to face the fast-growing globalization
- To Develop a Holistic Personality of the learners
- To make this Institute as a Lead Centre of Research

QUALITY POLICY

We at R. H. Sapat College of Engineering, Management Studies and Research, Nashik (RHSCOEMS&R) are committed to impart "Value Embedded Quality Technical Education" to fulfill the need and expectations of students, parents, employers and society at large. This is done through the total involvement of the faculty, students, technical and supporting staff in the process of teaching and learning, complying to the quality system and continually improving the process and system.

CORE VALUES

G.E.S.R.H.S.COE, MS&R, Nashik engages in a process of self and community reflection that would lead us to recognize and heighten awareness of the core values.

1. **Leadership**: To set standards in our teaching learning process.
2. **Integrity and transparency**: To be ethical, sincere and honest.
3. **Excellence**: To strive relentlessly and constantly improving ourselves, to achieve the best.
4. **Fairness**: To use technology for achieving excellence, creativity to hold standards of integrity

VISION AND MISSION OF E & TC DEPARTMENT

VISION

- To facilitate the continuous transformation of students into competent professionals and responsible citizens who apply efforts towards betterment of the society.

MISSION

- Impart quality technical education using excellence in teaching-learning process and research, in the view of assimilation and dissemination of knowledge which will produce competent professionals to meet the needs of society.
- Develop talented entrepreneurs through conducive and creative environment which promotes novelty of ideas.
- Promote continuous interactions with alumni, industries, institutions and stakeholders.

PROGRAM SPECIFIC OUTCOME (PSO)

PSO1: To Create Electronics and Telecommunication engineering graduates with fundamentals of sciences, mathematics and technical expertise with an ability to outperform in professional career and/or higher education.

PSO2: To apply the concepts of Electronics and Telecommunication Engineering to design and solve complex problems in the field related to Analog and Digital electronics, embedded systems, communications, signal processing and VLSI systems using Electronics equipment's and EDA tools

PSO3: Inculcate multidisciplinary expertise along with leadership and problem solving skills for life-long learning and development.

PROGRAM OUTCOMES (PO'S)

The program outcomes (POs) are what knowledge skills and attitudes a graduate should have at the time of graduation.

1. **Engineering knowledge**: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. **Problem analysis**: Identify, formulate, research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
3. **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.
4. **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.
5. **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.
6. **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.
7. **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.
8. **Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. **Individual and team work**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. **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.
11. **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.

12. **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.

PROGRAM EDUCATIONAL OBJECTIVES (PEO)

PEO1: Create graduates with fundamentals of sciences, mathematics and relevant technical expertise with an ability to outperform in professional career and/or higher education.

PEO2: Develop competent, determined and self-motivated professionals with ethical and moral values.

PEO3: Develop engineers with capability to implement knowledge, explore and analyze results based on facts, tests, hands-on experimentations and research.

PEO4: Inculcate multidisciplinary expertise along with leadership and problem-solving skills for life-long learning and development.

PEO5: Communicate the ideas effectively and to manage projects in the capacity of a team member.

COURSE OUTCOMES (CO)

Subject: **Computer Network** 2019 Course

On completion of the course, student will be able to,

CO1: Apply the fundamental knowledge of project management for effectively handling the projects.

CO2: Identify and select the appropriate project based on feasibility study and undertake its effective planning.

CO3: Assimilate effectively within the organizational structure of project and handle project management related issues in an efficient manner.

CO4: Apply the project scheduling techniques to create a Project Schedule Plan and accordingly utilize the resources to meet the project deadline.

CO5: Identify and assess the project risks and manage finances in line with Project Financial Management Process.

CO6: Develop new products assessing their commercial viability and develop skillsetsfor becoming successful entrepreneurs while being fully aware of the legal issuesrelated to Product development and Entrepreneurship

INSTRUCTIONS FOR STUDENTS

Students shall read the points given below for understanding the theoretical concepts and practical applications.

1. Listen carefully to the lecture given by teacher about importance of subject, curriculum philosophy, learning structure, skills to be developed, information about equipment, instruments, procedure, method of continuous assessment, tentative plan of work in laboratory and total amount of works to be done in a semester.
2. Students shall undergo study visit of the laboratory for types of equipment, instrument and material to be used, before performing experiments.
3. Read the write up of each experiment to be performed, a day in advance.
4. Organize the work in the group and make a record of all observations.
5. Understand the purpose of experiment and its practical implications.
6. Student should not hesitate to ask any difficulty faced during conduction of practical/exercise.
7. Write the answers of the questions allotted by the teacher during practical hours if possible or after wards, but immediately.
8. The student shall study all the questions given in the laboratory manual and practice to write the answers to these questions.
9. Student should develop the habit of pear discussion/group discussion related to experiments/exercise so that exchanges of knowledge/skills could take place.
10. Student shall attempt to develop related hands-on-skills and gain confidence.
11. Student shall focus on development of skills rather than theoretical or codified knowledge.
12. Student shall visit the nearby workshops, workstation, Industries, laboratories, technical exhibitions, trade fair etc. even not included in the Lab Manual. In short, students should have exposure to the area of work right in the student hood.
13. Students shall insist for the completions of recommended Laboratory Work, industrial visits, answers to the given question etc.
14. Student shall develop the habit of evolving more ideas, innovations, skills etc. than included in the scope of the manual.
15. Student shall refer technical magazines, proceedings of the Seminars, refer website related to the scope of the subjects and update their knowledge and skills.
16. Student should develop the habit of not to depend totally on teachers but to develop self-learning techniques.
17. Student should develop the habit to interact with the teacher without hesitation with respect to the academics involved.

18. Student should develop habit to submit the practical's exercise continuously and progressively on the scheduled dates and should get the assessment done.
19. Student should be well prepared while submitting the write up of the exercise. This will develop the continuity of the studies and he will not be over loaded at the end of the term.

EXPERIMENT LIST

Name of Subject: **COMPUTER NETWORK Lab (304189)** (Elective – I)

Marking Scheme: **Oral**: 25 Marks **Credit:** 01

CLASS: T.E.- E&TC **Course In charge**: Mrs. G.R.Kawale

List of the Experiments (Minimum 8 experiments are to be performed).Group A (Any Four)

1) Implementation of LAN using suitable multiuser Windows operating System and demonstrating client-server and peer to peer mode of configuration.
2) Simulating various Networks (LAN, WAN) using relevant network devices on Simulator
   a) Ping b) ipconfig / ifconfig c) Host name d) Whois
   e) Netstat f) Route g) Tracert/Traceroute/ Tracepath
   h) NSlookup i) ARP j) Finger k) Port Scan / nmap
3) Observe and note the details of the live type of traffic (ARP, Frame analysis, ethernet) from interface using packet capture and analysis tool
4) Using a Network Simulator (e.g., packet tracer) Configure router using RIP
5) Capture and note the packet of HTTP /FTP /Telnet / DHCP Protocol using TCP-stream learnsequence of packets being sent and received.

Group B (Any Four)

1) Socket Programming in C/C++ on TCP Client, TCP Server.
2) Write a program to simulate leaky bucket/token bucket.
3) Observe and note the working of protocols using PING / TRACEROUTE / PATHPING and capturepackets in LAN using packet capture and analysis tool.
4) Configure servers like HTTP / FTP and understand packet sequence and data flowing between client-server using packet analysis tools.
5) Executing Proxy, web Server using simulator
6) Executing Telnet, DHCP Server using simulator.

R. H. Sapat COE, Management Studies & Research, Nashik

Department of Electronics and Telecommunication Engineering

CERTIFICATE

This is to certify that Mr/Ms. _____

Roll No. _____ from **Third Year Electronics and Telecommunication Engineering** has successfully completed his/her term work of **Computer Networks (Elective-1)** at **R. H. Sapat COE, Management Studies & Research, Nashik**

in the partial fulfillment of the Bachelor's Degree in Engineering under Savitribai Phule Pune University.

(Mrs. G.R. Kawale)
Subject In-charge

(Dr. Santosh P. Agnihotri)
Head of Department

R. H. Sapat COE, Management Studies & Research, Nashik

Department of Electronics and Telecommunication Engineering

INDEX

Class: TE E&TC **Sub-** Computer Networks

Academic Year: 2023-24 **2019 Course (Sem-1)**

Experiment No: 1

TITLE: Implementation of LAN using suitable multiuser Windows operating System and demonstratingclient-server and peer to peer mode of configuration.

AIM: - **Study of Networks and networking devices.**

Study of existing LAN and understand the design and various components. Set up a small network of 3 to 4 computers and Hub/Switch as directed by the instructor. Use LAN card, UTP cables and connectors. Install LAN cards and crimp the connectors. Assign unique IP addressed and share C drive on each machine. Test the network by using ping command. Use protocol analyzer software. Repeat the assignment by installing to LAN cards in one of the machines.

Requirements:-

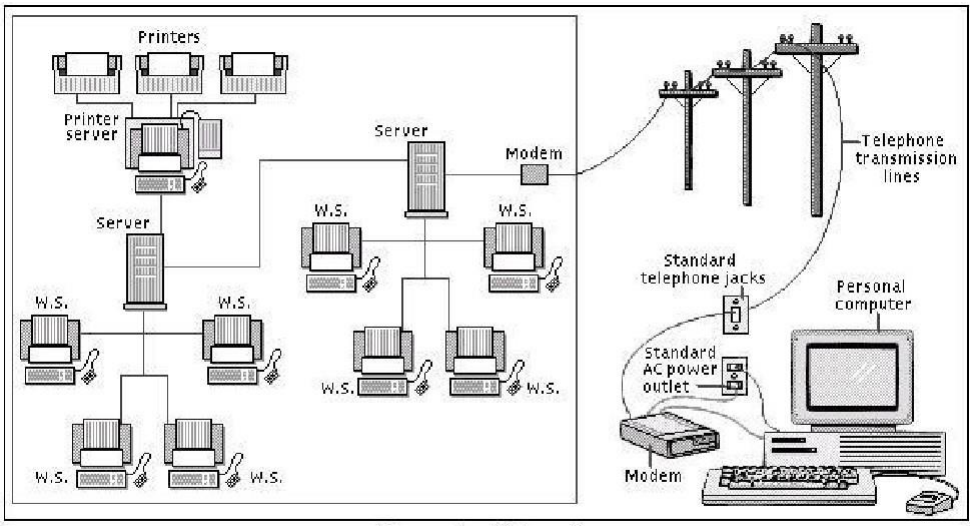
Hardware: Computer, LAN Cards, RJ-45 Connectors, Switch, CAT-5 Cable, Cable tester, Crimpingtool, etc.

Software: Operating system Windows XP, 2003 Server, etc.

Theory:-

Computer Networks, the widespread sharing of information among groups of computers and their users, a central part of the information age. The popular adoption of the personal computer (PC) and the local area network (LAN) during the 1980s has led to the capacity to access information on a distant database; download an application from overseas; send a message to a friend in a different country; and share files with a colleague—all from a personal computer.

The networks that allow all this to be done so easily are sophisticated and complex entities. They rely for their effectiveness on many cooperating components. The design and deployment of the worldwide computer network can be viewed as one of the great technological wonders of recent decades.



Computer Network

Networks are connections between groups of computers and associated devices that allow usersto transfer information electronically. The local area network shown on the left is representative of the setup used in many offices and companies. Individual computers, called work stations (WS), communicate to each other via cable or telephone line linking to servers.

Servers are computers exactly like the WS, except that they have an administrative function and are devoted entirely to monitoring and controlling WS access to part or all of the network and to any shared resources (such as printers). The red line represents the larger network connection between servers, called the backbone; the blue line shows local connections. A modem (modulator/demodulator) allows computers to transfer information across standard telephone lines. Modems convert digital signals into analogue signals and back again, making it possible for computers to communicate, or network, across thousands of miles.

STUDY OF TOPOLOGIES: -What is a Topology?

The physical topology of a network refers to the configuration of cables, computers, and other peripherals. Physical topology should not be confused with logical topology which is the method used to pass information between workstations. Some topologies are:-

Bus Topologies: -

Each node is daisy–chained (connected one right aft er the other) along the same backbone.Information sent from a node travel along the backbone until it reaches its destination node.

Network maintained by a single cable.

Cable segment must end with a terminator.

Uses thin coaxial cable (backbones will be thick coaxial

cable).Extra stations can be added in a daisy chain manner.

Standard is IEEE 802.3.

Thin Ethernet (10Base2) has a maximum segment length of 200m.

Max no. of connections is 30 devices.

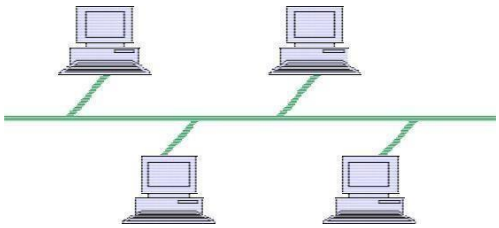
Four repeaters may be used to a total cable length of 1000m.

Max no. of nodes is 150.

Thick Ethernet (10Base5) used for backbones.

Limited to 500m.

Max of 100 nodes per segment.



Total of four repeaters, 2500m, with a total of 488 nodes.

Advantages:-

1. Inexpensive to install.
2. Easy to add stations.
3. Use less cable than other topologies.
4. Works well for small networks.

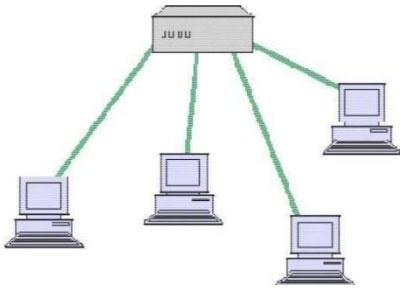
Disadvantages:-

5. Longer recommended.
6. Backbone breaks whole network down.
7. Limited no of devices can be attached.
8. Difficult to isolate problems.
9. Sharing same cable slows response rate.

a) **Star Topologies: -**

In a star network, each node is connected to a central device called a hub. The hub takes a signal that comes from any node and passes it along to all the other nodes in the network. A hub does not perform any type of filtering or routing of the data. It is simply a junction that joins all the different nodes together.

- Like the spokes of a wheel (without the symmetry).
- Centre point is a Hub.
- Segments meet at the Hub.
- Each device needs its own cable to the Hub.
- Predominant type of topology.
- Easy to maintain and expand.



Advantages:-

- Easy to add devices as the network expands.
- One cable failure does not bring down the entire network.
- Hub provides centralized management.
- Easy to find device and cable problems.
- Can be upgraded to faster speeds.
- Lots of support as it is the most used.

Disadvantages:-

1) A star network requires more cable than a ring or bus network.

2) Failure of the central hub can bring down the entire network.

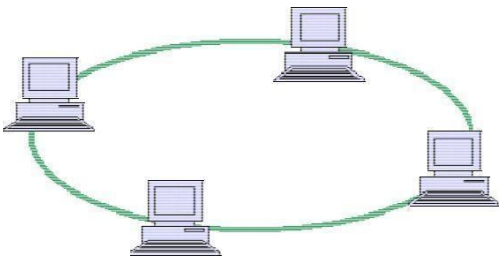
3) Costs are higher (installation and equipment) than for most bus networks.

1 **Ring Topology:-**

Like a bus network, rings have the nodes daisy-chained. The difference is that the end of the network comes back around to the first node, creating a complete circuit. In a ring network, each node takes a turn sending & receiving information through the use of a token. The token along with any data is sent from the first node to the second node, which extracts the data addressed to it and adds any data it wishes to send. Then the second node passes the token and data to the third node, and so on until it comes back around to the first node again. Only the node with the token is allowed to send data. All other nodes must wait for the token to come to them.

- No beginning or end (a ring in fact!!).
- All devices of equality of access to media.
- Single ring – data travels in one direction only, guess what a double ring allows?
- Each device has to wait its turn to transmit.

- Most common type is Token Ring (IEEE 802.5).
- A token contains the data, reaches the destination, data extracted, acknowledgement of receipt sent back to transmitting device, removed, empty token passed on for another device to use.



Advantages:-

i) Data packets travel at great speed.

ii) No collisions.

iii) Easier to fault find.

iv) No terminators required.

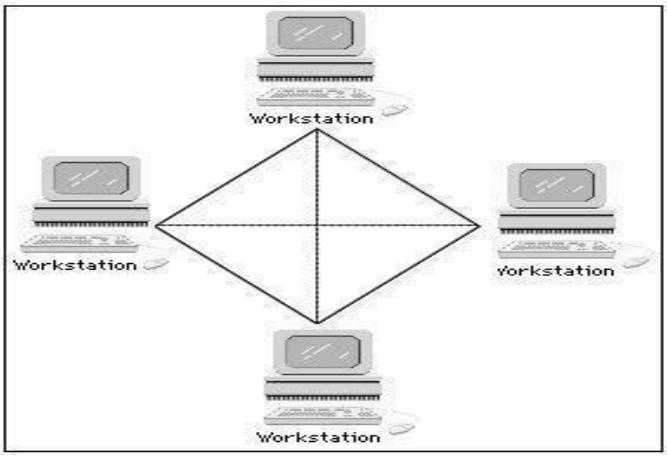
Disadvantages:-

- Requires more cable than a bus.
- A break in the ring will bring it down.
- Not as common as the bus – less devices available.

1) Mesh Topology: -

The type of network topology in which each of the nodes of the network is connected to each of the other nodes in the network with a point-to-point link – this makes it possible for data to be simultaneously transmitted from any single node to all of the other nodes.

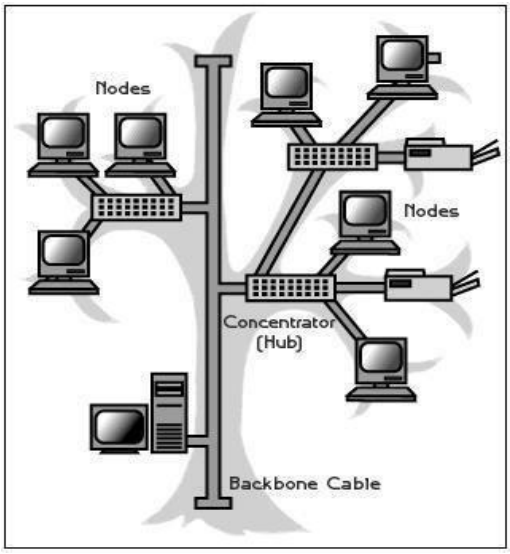
Note: The physical fully connected mesh topology is generally too costly and complex for practical networks, although the topology is used when there are only a small number of nodes to be interconnected.



5. **Hybrid/Tree Topology: -**

A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable.

These topologies can also be mixed. For example, a bus-star network consists of a high-bandwidth bus, called the ***backbone,*** which connects a collection of slower-bandwidth star segments.



TYPES OF NETWORKS: -

1. Local Area Network (LAN): -

A LAN is a network of computers that are in the same general physical location, usually within a building or a campus. If the computers are far apart (such as across town or in different cities), then a Wide Area Network (WAN) is typically used.

- LANs are designed to:
  - –Operate within a limited geographic area.
  - –All multi-access to high-bandwidth media.
  - –Control the network privately under local administration.
  - –Provide full-time connectivity to local services.
  - –Connect physically adjacent devices.
- LANs make it possible for businesses that use computer technology to locally share files and printers efficiently, and make internal communications possible.
- LANs consist of the following components:
  - –Computers.
  - –Network interface cards.
  - –Peripheral devices.
  - –Networking media.
  - –Network devices.
- Some common LAN technologies are:
  - Ethernet.
  - Token Ring.
  - FDDI.

a) Wide Area Network (WAN): -

WANs interconnect LANs, which then provide access to computers or file servers in other locations.

1. WANs are designed to:
   - Operate over a large geographical area.
   - Allow access over serial interfaces operating at lower speeds.
   - Provide full-time and part-time connectivity.
   - Connect devices separated over wide, even global areas.
2. Some common WAN technologies are:
   - Modems.
   - Integrated Services Digital Network (ISDN).
   - Digital Subscriber Line (DSL).
   - Frame Relay.
   - US (T) and Europe (E) Carrier Series – T1, E1, T3, E3.

- Synchronous Optical Network (SONET).

b) Metropolitan Area Networks (MANs): -

1. A MAN is a network that spans a metropolitan area such as a city or suburban area.
2. A MAN usually consists of two or more LANs in a common geographic area.
3. For example, a bank with multiple branches may utilize a MAN.

c) Storage-area Networks (SANs):-

1. A SAN is a dedicated, high-performance network used to move data between servers and storage resources.
2. Because it is a separate, dedicated network, it avoids any traffic conflict between clients and servers.
3. SANs offer the following features:
   - Performance
   - Availability
   - Scalability

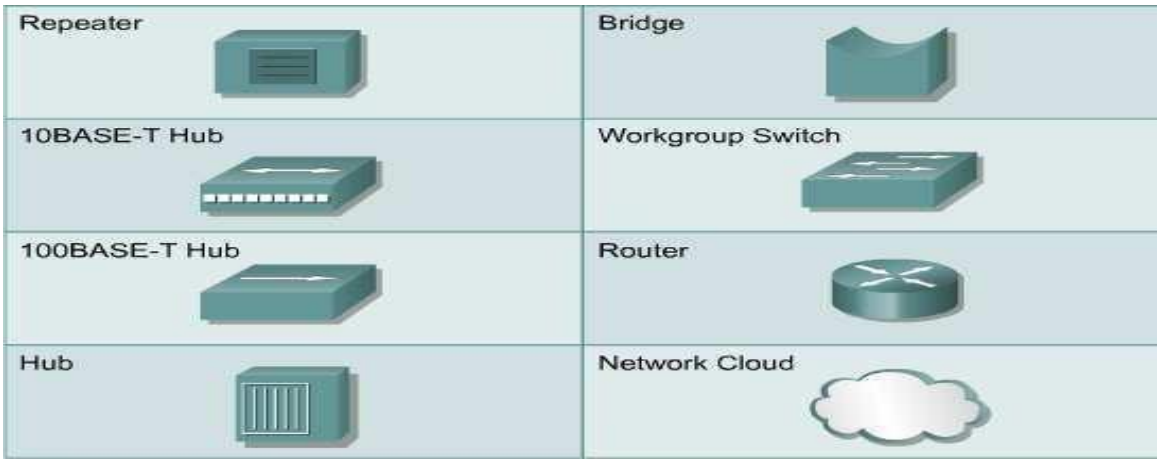
d) Virtual Private Network (VPN):-

1. A VPN is a service that offers secure, reliable connectivity over a shared public network infrastructure such as the Internet.
2. VPNs maintain the same security and management policies as a private network.
3. They are the most cost-effective method of establishing a point-to-point connection between remote users and an enterprise customer's network.
4. The three main types of VPNs are:
   - Access VPNs.
   - Intranet VPNs.
   - Extranet VPNs.

DEVICES USED IN A LAN:

- NETWORK ADAPTER: interfaces a computer board with the network medium.
- REPEATER: two-ports electronic device that just repeats what receives from one port to the other (BIT level).
- BRIDGE: intelligent repeater with *filtering* (FRAME level).

- HUB: multi-port repeater.
- SWITCH: multi-port bridge.
- ROUTER: links two or more networks (different types too), providing the appropriate routing information (routing tables) (PACKET level).
- GATEWAY: simple router that links two networks.
- CAT 5 cable.

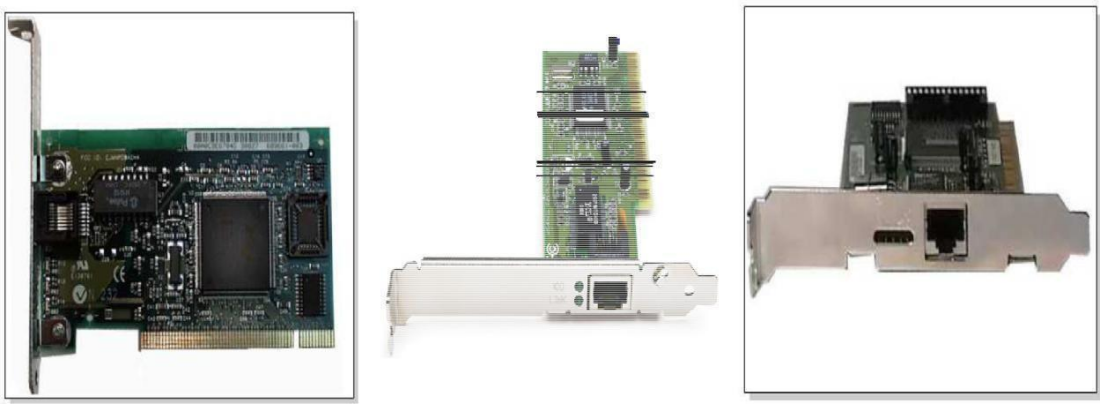


1. Network Interface Card (NIC): -

Every computer (and most other devices) is connected to a network through an NIC. In the most desktop computers, this is an Ethernet card (normally 10 or 100 Mbps) that is plugged into a slot on the computer's motherboard.

Types of Card:-

1. Arc net card (2.5 mbits/sec).
2. Ethernet card (10/100 mbps).
3. Token Ring card (4-16 mbits/sec).



NIC as a Source Device:-

- Receives the data packet from the Network Layer.
- Attaches its the MAC address to the data packet.
- Attaches the MAC address of the destination device to the data packet.
- Converts data in to packets suitable for the particular network (Ethernet, Token Ring, FDDI).
- Converts packets in to electrical, light or radio signals.

1. Provides the physical connection to the media.

NIC as a Destination Device:-

1. Provides the physical connection to the media.
2. Translates the signal in to data.
3. Reads the MAC address to see if it matches its own address.
4. If it does match, passes the data to the Network Layer.

2) Repeater:-

Repeaters are devices that operate at the physical layer based on the OSI model. The basic purpose of a repeater is to extend the distance of something. Their primary purpose is simply to regenerate a signal received from input and correct the signal to its original state for output i.e. they provide signal amplification and also retiming required connecting the connected segments.

- Allows the connection of segments.
- Extends the network beyond the maximum length of a single segment.
- Functions at the Physical Layer of the OSI model.
- A multi-port repeater is known as a Hub.

- Connects segments of the same network, even if they use different media.
- Has three basic functions.
- Receives a signal which it cleans up.
- Re-times the signal to avoid collisions.
- Transmits the signal on to the next segment.

Advantage:-

Can connect different types of media, can extend a network in terms of distance, and does not increase network traffic.

Disadvantages: -

Extends the collision domain, can not filter data, can not connect different network architectures, limited number only can be used in network.

1) **Hub: -**

All networks require a central location to bring media segment together. These central locations are called hubs. Hubs are special repeaters that overcome the electromechanical limitations of a media signal path. The hub organizes the cables and transmits incoming signals to the other media segments. There are main types of hubs:-

(A) Passive Hubs: They simply combine the signals of network segments. There is no signal regeneration.

(B) Active Hubs: They regenerate and amplify the signals so the distance between devices is increased.

(C) Intelligent Hubs: They regenerate the signal and perform some network management and intelligent path selection. Intelligent hub includes switching hubs. In switches internal paths are setup due to which overall bandwidth of the network increases.

- A central point of a star topology.
- Allows the multiple connections of devices.
- Can be more than a basic Hub – providing additional services (Managed Hubs, Switched Hubs, Intelligent Hubs).
- In reality a Hub is a Repeater with multiple ports.
- Functions in a similar manner to a Repeater.

- Works at the Physical Layer of the OSI model.
- Passes data no matter which device it is addressed to.
- This feature adds to congestion.
- Use large Hubs (24 port), or stacking them exacerbates this negative feature.

Hub Features:-

1. Type of media connection needed.
- Number of ports.
- Speed.
- Managed or Unmanaged.
- Requirement for Uplink Port? (allows two Hubs to be connected using a patch cable – crossover cable).
- Token Ring Hubs are known as MAUs – see last week's notes.

Advantages:-

Cheap, can connect different media types.

Disadvantages:-

Extends the collision domain, can not filter information, passes packets to all connected segments.

- **Bridge:-**

Bridges connect network segments. It operates on data link layer. A bridge extends the maximum distance of network by connecting separate network segments. Bridge simply passes on all the signals it receives. Bridges can divide busy network into segments and reduce network traffic. There are two types of bridges:-

1) Transparent bridge: Has a memory to store the routing table.
2) Source routing bridge: Requires the entire routing table to be included in the transmission and do not route packets intelligently.
3) Like a Repeater or Hub it connects segments.
4) Works at Data Layer – not Physical.
5) Uses Mac address to make decisions.
6) Acts as a 'filter', by determining whether or not t o forward a packet on to another segment.

7) Builds a Bridging Table, keeps track of devices on each segment.
8) Filters packets, does not forward them, by examining their MAC address.
9) It forwards packets whose destination address is on a different segment from its own.
10) It divides a network in to multiple collision domains – so reducing the number of collisions.

Advantages:-

Limits the collision domain, can extend network distances, uses MAC address to filter traffic, eases congestion, can connect different types of media, some can connect differing architectures.

Disadvantages:-

Broadcast packets can not be filtered, more expensive than a repeater, slower than a repeater due toadditional processing of packets.

1) **Switch:-**

- A multiport Bridge, functioning at the Data Link Layer.
- Each port of the bridge decides whether to forward data packets to the attached network.
- Keeps track of the Mac addresses of all attached devices (just like a bridge).
- Similarly priced to Hubs – making them popular.
- Acts like a Hub, but filters like a Bridge.
- Each port on a Switch is a collision domain.

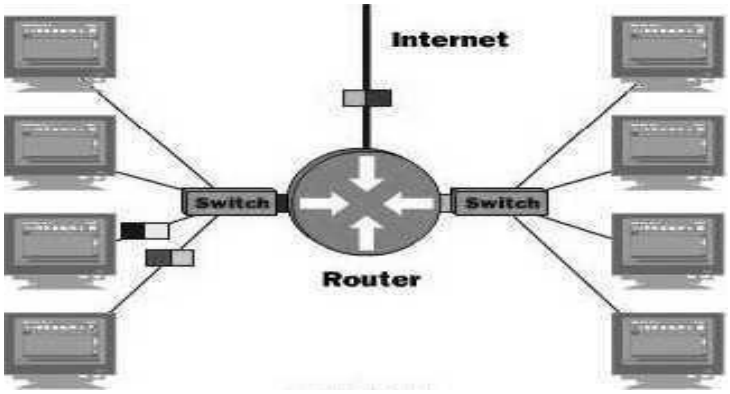
Advantages:-

Limits the collision domain, can provide bridging, can be configured to limit broadcast domain.

Disadvantages:-

More expensive than a hub or bridge, configuration of additional functions can be very complex.

6. Router:-



Routers connect two or more logically separate networks. It operates on network layer. They consist of combination of hardware and software. Hardware can be server, a separate computer. Software in the router is the operating system and routing protocols. Management software can be another router component.

- Functions both as Bridge and a Router – hence name.
- Can work on networks using different protocols.
- Can be programmed only to pass data packets using a specific protocol forward to a segment – in this case it is functioning in a similar manner to a Bridge.
- If a Router is set to route data packets to the appropriate network with a routed protocol such as IP, it is functioning as a Router.
- Works at Network Layer in an intelligent manner.
- Can connect different network segments, if they are in the same building or even on the opposite side of the globe.
- Work in LAN, MAN and WAN environments.
- Allows access to resources by selecting the best path.
- Can interconnect different networks – Ethernet with Token Ring.
- Changes packet size and format to match the requirements of the destination network.

- Two primary functions – to determine the 'best path' and to share details of routes with other routers.
- Routing Table – a database which keeps track of the routes to networks and the associated costs.
- Static Routing – routes are manually configured by a network administrator.
- Dynamic Routing – adjust automatically to changes i n network topology, and information it receives from other routers.
- Routing Protocol – uses a special algorithm to rout e data across a network.

In a slightly more complicated intranet which is composed of a number of TCP/IP-based networks, and connects to a limited number of TCP/IP-based networks, static routing will be required. In static routing, the routing table has specific ways of routing data to other networks. Only those pathways can be used. Intranet administrators can add routes to the routing table. Static routing is more flexible than minimal routing, but it can't change routes as network traffic changes, and so isn't suitable for many intranets.

In more complex intranets, dynamic routing will be required. Dynamic routing is used to permit multiple routes for a packet to reach its final destination. Dynamic routing also allows routers to change the way they route information based on the amount of network traffic on some paths and routers. In dynamic routing, the routing table is called a dynamic routing table and changes as network conditions change. The tables are built dynamically by routing protocols, and so constantly change according to network traffic and conditions.

There are two broad types of routing protocols: interior and exterior. Interior routing protocols are typically used on internal routers inside an intranet that routes traffic bound only for inside the intranet. A common interior routing protocol is the Routing Information Protocol (RIP). Exterior protocols are typically used for external routers on the Internet. A common exterior protocol is the Exterior Gateway Protocol (EGP).

Advantages:-

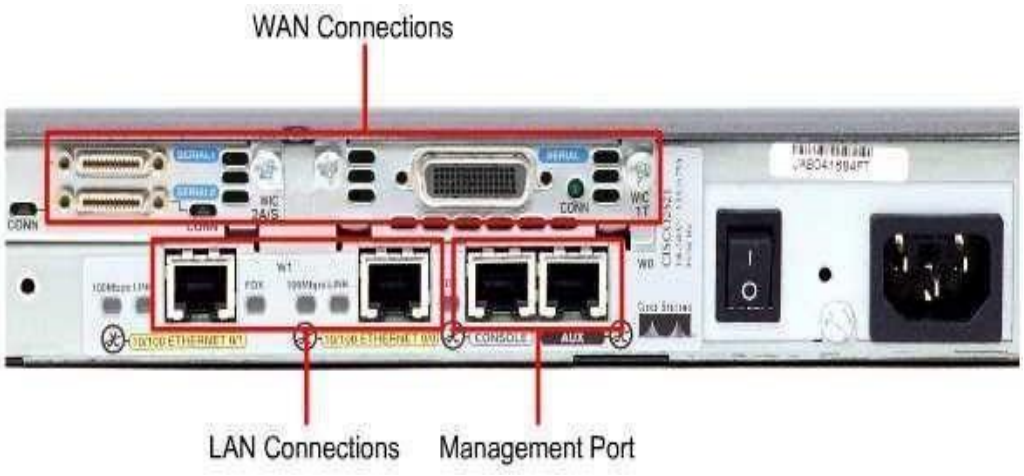
Limits the collision domain, can function in LAN or WAN, connects differing media and architectures, can determine best path/route, can filter broadcasts.

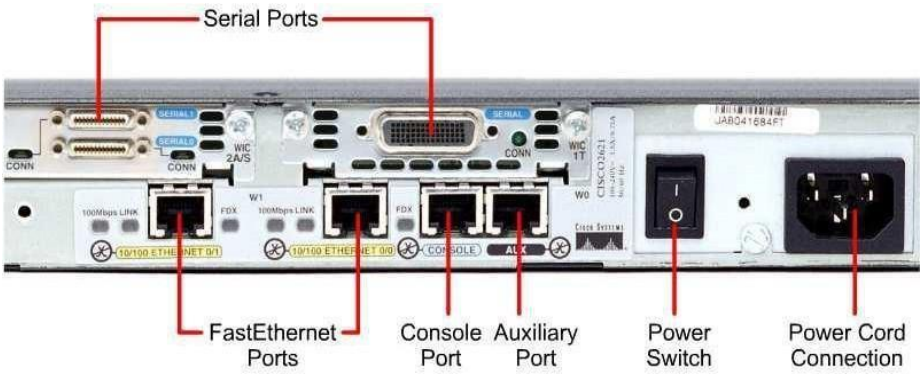
Disadvantages:-

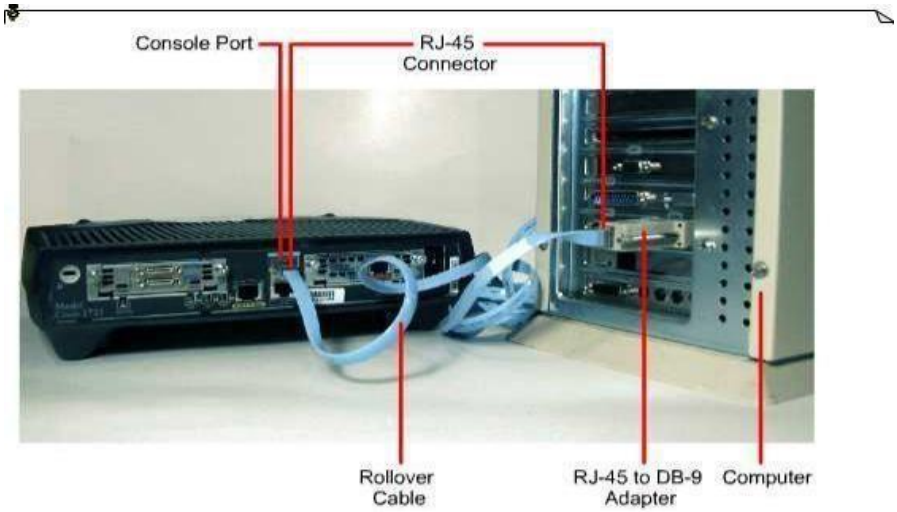
Expensive, must use routable protocols, can be difficult to configure (static routing), slower than a bridge.

Router Interfaces:-

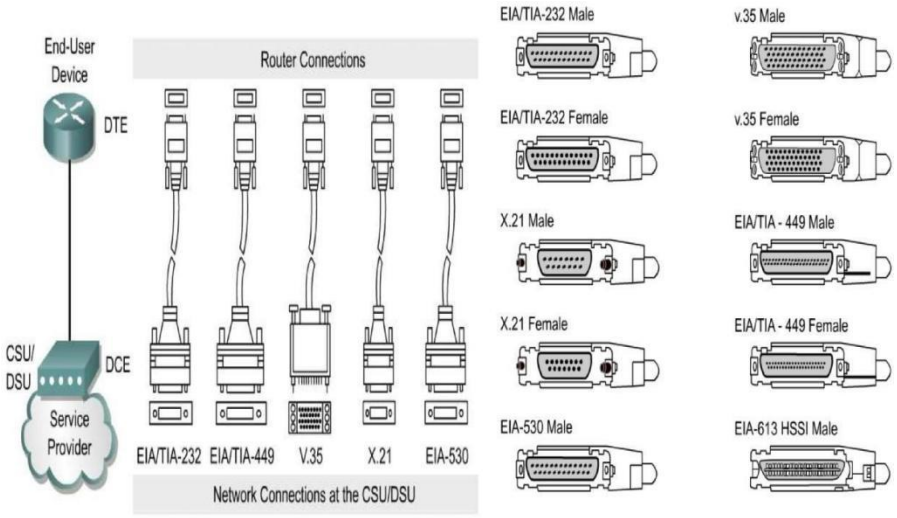
- LAN interfaces allow routers to connect to the LAN media. This is usually some form of Ethernet.
- WANs provide connections through a service provider to a distant site or to the Internet.



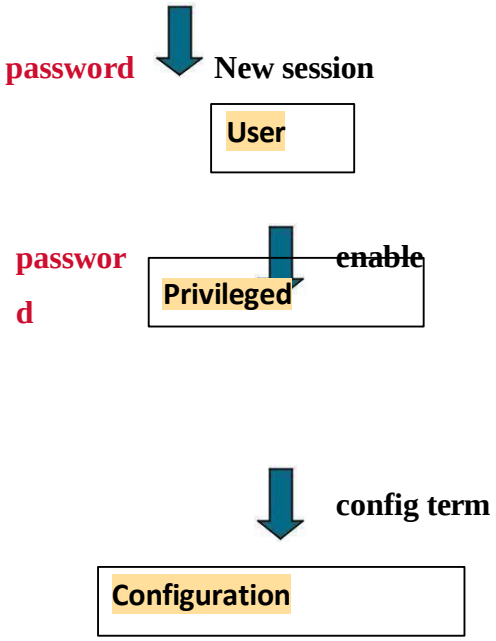




Connecting WAN Interface



Router modes: -



User mode: -

User can examine router status and operation. Configuration cannot be viewed or altered from user mode prompt router>

Privileged mode ("root"):-

Complete control over the router (anything can be set or reset) configuration cannot be altered promptrouter#

Configuration mode: -

- Used only for change of configuration.
- Not password protected from privileged mode.
- Privileged mode commands don't have meaning in configuration mode.
- Most statements can be removed from the configuration with the prefix no (ex. no shutdown).
- **Prompt router (config) #.**

7. Gateway: -

Gateway connects two independent networks. A gateway is basically a protocol converter, so it has to operate on all the layers of the OSI model. But generally it is in form of software so it is said to operate on application layer only.

- Allows different networks to communicate by offering a translation service from one protocol stack to another.
- They work at all levels of the OSI model – due to t he type of translation service they are providing.

- Address Gateway – connects networks using the same protocol, but using different directory spaces such as Message Handling Service.
- Protocol Gateway – connects network using different protocols. Translates source protocol so destination can understand it.
- Application Gateway – translates between applicatio ns such as from an Internet email server to a messaging server.

8. CAT 5 CABLE:-

The CAT 5 Cable consist of 8 wires which comes pares of White/Blue, Blue, White/Orange, Orange, White/Green, Green, White/Brown, Brown and they are coded for **Straight** and **Cross** combinations respectively.

Straight:-

Cross:-

Pair #	Wire	Pin #
1-White/Blue	White/Blue	5
	Blue	4
2-Wht. /Orange	White/Orange	1
	Orange	2
3-White/Green	White/Green	3
	Green	6
4-White/Brown	White/Brown	7
	Brown	8

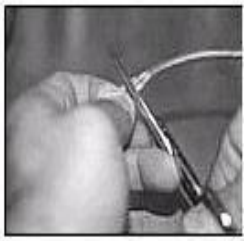
Pair #	Wire	Pin #
1-White/Blue	White/Blue	5
	Blue	4
2-White/Green	White/Green	1
	Green	2
3-White/Orange	White/Orange	3
	Orange	6

4-White/Brown	White/Brown	7
	Brown	8

How to Crimp a Cat 5 cable with RJ 45 Connector:-

1. Skin off the cable jacket approximately 1" or slightly more.

2. Un-twist each pair, and straighten each wire between the fingers.



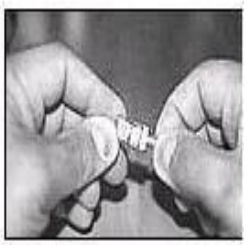
3. Place the wires in the order of one of the two diagrams shown above .Bring all of the wires together, until they touch.

4. At this point, recheck the wiring sequence with the diagram.

5. Optional: Make a mark on the wires at 1/2" from the end of the cable jacket.

6. Hold the grouped (and sorted) wires together tightly, between the thumb, and the forefinger.

7. Cut all of the wires at a perfect 90 degree angle from the cable at 1/2" from the end of the cable jacket. This is a very critical step. If the wires are not cut straight, they may not all make contact. We suggest using a pair of scissors for this purpose.



8. Conductors should be at a straight 90 degree angle, and be 1/2" long, prior to insertion into the connector.

9. Insert the wires into the connector (pins facing up).

10. Push moderately hard to assure that all of the wires have reached the end of the connector. Be sure that the cable jacket goes into the back of the connector by about 3/16".

11. Place the connector into a crimp tool, and squeeze hard so that the handle reaches its full swing.

12. Repeat the process on the other end. For a straight through cable, use the same

wiring.

13. Use a cable tester to test for proper continuity.

Cable Testing Tool:-

It is a tool used for testing weather there is no cut in between two terminals andto identify the type of pair crimp with.

CONCLUSION:-

Checked By:

Name of Subject Teacher	Sign with Date

EXPERIMENT NO. 2

TITLE – Simulating various Networks (LAN, WAN) using relevant network devices on Simulator

a) Ping b) ipconfig / ifconfig c) Host name d) Whois

e) Netstat f) Route g) Tracert/Traceroute/ Tracepath

h) NSlookup i) ARP j) Finger k) Port Scan / nmap

1. Ping command:

The ping command is a Command Prompt command used to test the ability of the source computer to reach a specified destination computer. The ping command is usually used as a simple way to verify that a computer can communicate over the network with another computer or network device. The ping command operates by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination computer and waiting for a response. How many of those responses are returned, and how long it takes for them to return, are the two major pieces of information that the ping command provides. For example, you might find that there are no responses when pinging a network printer, only to find out that the printer is offline and its cable needs replaced. Or maybe you need to ping a router toverify that your computer can connect to it, to eliminate it as a possible cause for a networking issue.

Ping Command Syntax ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [-wtimeout] [-R] [-S srcaddr] [-p] [-4] [-6] target [/?]

-t	Using this option will ping the target until you force it to stop by using Ctrl-C.
-a	This ping command option will resolve, if possible, the hostnameof an IP address target.
-n count	This option sets the number of ICMP Echo Requests to send, from 1 to 4294967295. The ping command will send 4 by default if -n isn't used.
-l size	Use this option to set the size, in bytes, of the echo request packetfrom 32 to 65,527. The ping command will send a 32-byte echo request if you don't use the -l option.

-f	Use this ping command option to prevent ICMP Echo Requests from being fragmented by routers between you and the target. The -f option is most often used to troubleshoot Path Maximum Transmission Unit (PMTU) issues.
-i TTL	This option sets the Time to Live (TTL) value, the maximum of which is 255.
-v TOS	This option allows you to set a Type of Service (TOS) value. Beginningin Windows 7, this option no longer functions but still exists for
	compatibility reasons.
-r count	Use this ping command option to specify the number of hopsbetween your computer and the target computer or device that you'd like to be recorded and displayed. The maximum value for count is 9, so use the tracert command instead if you're interested in viewing all the hops between two devices.
-s count	Use this option to report the time, in Internet Timestamp format, that each echo request is received and echo reply is sent. The maximum value for count is 4, meaning that only the first four hops can be time stamped.
-w timeout	Specifying a timeout value when executing the ping command adjusts the amount of time, in milliseconds, that ping waits for each reply. If you don't use the -w option, the default timeout value of 4000 is used, which is 4 seconds.
-R	This option tells the ping command to trace the round trip path.
-S srcaddr	Use this option to specify the source address.
-p	Use this switch to ping a Hyper-V Network Virtualization provider address.
-4	This forces the ping command to use IPv4 only but is only necessary if target is a hostname and not an IP address.
-6	This forces the ping command to use IPv6 only but as with the -4option, is only necessary when pinging a hostname.
target	This is the destination you wish to ping, either an IP address or a

	hostname.
/?	Use the help switch with the ping command to show detailed help about the command's several options.

2. ifconfig - configure a network interface

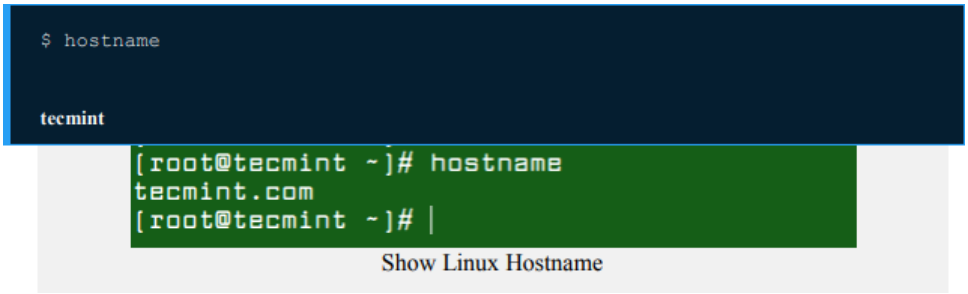
Ifconfig is used to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary. After that, it is usually only needed when debugging or when system tuning is needed. If no arguments are given, ifconfig displays the status of the currently active interfaces. If a single interface argument is given, it displays the status of the given interface only; if a single -a argument is given, it displays the status of all interfaces, even those that are down. Otherwise, it configures an interface.

3. HOSTNAME

A hostname command is used to view a computer's hostname and domain name (DNS) (Domain Name Service), and to display or set a computer's hostname or domain name. A hostname is a name that is given to a computer that attached to the network that uniquely identifies over a network and thus allows it to be accessed without using its IP address. The basic syntax for the hostname command is:

hostname [options] [new_host_name]

If you run hostname command without any options, it will displays the current host name and domain name of your Linux system.



Show Linux Hostname

If the host name can be resolved, you can display the network address(es) (IP address) of the host name with the -i flag and the -I option establishes all configured network interfaces and shows all network addresses of the host.

```
$ hostname -i

$ hostname -I
```

```
[root@tecmint ~]# hostname -i
192.168.0.1
[root@tecmint ~]# hostname -I
192.168.0.1 3a03:7b00::f13c:91ff:fedb:134560
[root@tecmint ~]#
```

4. WHOIS

whois is a client for the WHOIS directory service. whois searches for an object in a WHOIS database. WHOIS is a query and response protocol that is widely used for querying databases that store the registered users of an Internet resource, such as a domain name or an IP address block, but is also used for a wider range of other information. Most modern versions of whois try to guess the right server to ask for the specified object. If no guess can be made, whois will connect to whois.networksolutions.comfor NIC handles or whois.arin.net for IPv4 addresses and network names.

whois syntax

```
whois [ -h HOST ] [ -p PORT ] [ -aCFHILMmrRSVx ] [ -g SOURCE:FIRST-LAST ]
    [ -i ATTR ] [ -S SOURCE ] [ -T TYPE ] object
whois -t TYPE
```

```
whois -v TYPE
whois -q keyword
```

Options

-h HOST	Connect to WHOIS database host HOST.
-H	Suppress the display of legal disclaimers.
-p PORT	When connecting, connect to network port PORT.
--verbose	Operate verbosely.
--help	Display a help message, and exit.

5. **Netstate :**

netstat (network statistics) is a command line tool for monitoring network connections both

incoming and outgoing as well as viewing routing tables, interface statistics etc. netstat is available on all Unix-like Operating Systems and also available on Windows OS as well. It is very useful in terms of network troubleshooting and performance measurement. netstat is one of themost basic network service debugging tools, telling you what ports are open and whether any programs are listening on ports. This tool is very important and much useful for Linux network administrators as well as system administrators to monitor and troubleshoot their network related problems and determine network traffic performance.

6. Route :

Show or manipulate the IP routing table.

In computer networking, a router is a device responsible for forwarding network traffic. When datagrams arrive at a router, the router must determine the best way to route them to their destination. On Linux, BSD, and other Unix-like systems, the route command is used to view and make changes to the kernel routing table. The command syntax is different on different systems; here, when itcomes to specific command syntax, we'll be discussing the Linux version.

```
route
```

```
Kernel IP routing table

Destination     Gateway         Genmask         Flags Metric Ref    Use Iface

default         192.168.1.2     0.0.0.0         UG    1024   0        0 eth0

192.168.1.0     *               255.255.255.0   U     0      0        0 eth0
```

This shows us how the system is currently configured. If a packet comes into the system and has a destination in the range 192.168.1.0 through 192.168.1.255, then it is forwarded to the gateway *, which is 0.0.0.0 — a special address which represents an invalid or nonexistant destination. So, in this case, our system will not route these packets.

7. Traceroute

The traceroute command is used in Linux to map the journey that a packet of information undertakes from its source to its destination. One use for traceroute is to locate when data loss occurs throughout a network, which could signify a node that's down. Because each hop in the record reflects a new server or router between the originating PC and the intended target, reviewing the results of a traceroute scanalso lets you identify slow points that may adversely affect your network traffic.

How It Works?

Evaluating the specific route that network traffic follows (or finding the miscreant gateway that's discarding your packets) presents several troubleshooting challenges. Traceroute uses the IP protocol time to live field to solicit an ICMP TIME_EXCEEDED response from each gateway along the path to a destination host. The only parameter you must include when you execute the traceroute command is the host name or IP address of the destination.

Traceroute Syntax and Switches

Traceroute Syntax in Ubuntu.

traceroute [-dFInrvx] [-f first_ttl] [-g gateway] [-i iface] [-m max_ttl] [-p port] [- q nqueries] [-s src_addr] [-t tos] [-w waittime] [-z pausemsecs] host [packetlen]

While the above is how the traceroute command has to be written out in order to work in the command line, the performance or output of the command can be changed by specifying one or more optional switches

- -f: Set the initial time-to-live used in the first outgoing probe packet.
- -F: Set the "don't fragment" bit.
- -d: Enable socket level debugging.
- -g: Specify a loose source route gateway (8 maximum).
- -i: Specify a network interface to obtain the source IP address for outgoing probe packets. This is normally only useful on a multi-homed host. (See the -s flag for another way to do this.)
- -I: Use ICMP ECHO instead of UDP datagrams.
- -m: Set the max time-to-live (max number of hops) used in outgoing probe packets. The default is 30 hops (the same default used for TCP connections).
- -n: Print hop addresses numerically rather than symbolically and numerically (saves a nameserver address-to-name lookup for each gateway found on the path).

- -p: Set the base UDP port number used in probes (default is 33434). Traceroute hopes that nothing is listening on UDP ports base to base + nhops - 1 at the destination host (so an ICMP PORT_UNREACHABLE message will be returned to terminate the route tracing). If something islistening on a port in the default range, this option can be used to pick an unused port range.
- -r: Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly attached network, an error is returned. This option can be used to ping alocal host through an interface that has no route through it (e.g., after the interface was droppedby routed(8C)).
- -s: Use the following IP address (which usually is given as an IP number, not a hostname) as the source address in outgoing probe packets. On multi-homed hosts (those with more than one IP address), this option can be used to force the source address to be something other than the IP address of the interface the probe packet is sent on. If the IP address is not one of this machine's interface addresses, an error is returned and nothing is sent. (See the -i flag for another way to do this.)
- -t: Set the type-of-service in probe packets to the following value (default zero). The value must be a decimal integer in the range 0 to 255. This option can be used to see if different types-of-service result in different paths. (If you are not running 4.4bsd, this may be academic, since the normal network services like telnet and ftp don't let you control the TOS.) Not all values of TOS are legal or meaningful—see the IP spec for definitions. Useful values are probably `-t 16' (low delay) and `-t 8' (high throughput).
- -v: Verbose output. Received ICMP packets other than TIME_EXCEEDED and UNREACHABLEs arelisted.
- -w: Set the time (in seconds) to wait for a response to a probe (default 5 sec.).
- -x: Toggle IP checksums. Normally, this prevents traceroute from calculating IP checksums. In some cases, the operating system can overwrite parts of the outgoing packet but not recalculatethe checksum; thus, in some cases the default is to not calculate checksums and using -x causes them to be calculated. Note that checksums are usually required for the last hop when using ICMP ECHO probes (-I), so they are always calculated when using ICMP.
- -z: Set the time (in milliseconds) to pause between probes (default 0). Some systems such as Solaris and routers from Cisco, rate limit icmp messages. A good value to use with this is 500 (e.g., 1/2 second).

8. NSLOOKUP

The nslookup command is used to query Internet name servers interactively for information. nslookup,

which stands for "name server lookup", is a useful tool for finding out information about a named domain. By default, nslookup will translate a domain name to an IP address (or vice versa). For instance, to find out what the IP address of microsoft.com is, you could run the command**: nslookup microsoft.com**

...and you would receive a response like this:
Server: 8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
Name: microsoft.com
Address: 134.170.185.46
Name: microsoft.com
Address: 134.170.188.221

Here, 8.8.8.8 is the address of our system's Domain Name Server. This is the server our system is configured to use to translate domain names into IP addresses. "#53" indicates that we are communicating with it on port 53, which is the standard port number domain name servers use to accept queries. Below this, we have our lookup information for microsoft.com. Our name server returned two entries, 134.170.185.46 and 134.170.188.221. This indicates that microsoft.com uses a round robin setup to distribute server load. When you access micrsoft.com, you may be directed to either of these servers and your packets will be routed to the correct destination.

9. ARP

arp manipulates or displays the kernel's IPv4network neighbour cache.
It can add entries to the table, delete one, or display the current content.

ARP stands for Address Resolution Protocol, which is used to find the address of a network neighbor for a given IPv4 address.

arp syntax

arp [-vn] [-H type] [-i if] -a [hostname]
arp [-v] [-i if] -d hostname [pub]

arp [-v] [-H type] [-i if] -s hostname hw_addr [temp]

arp [-v] [-H type] [-i if] -s hostname hw_addr [netmask nm] pub

arp [-v] [-H type] [-i if] -Ds hostname ifa [netmask nm] pub

arp [-vnD] [-H type] [-i if] -f [filename]

11. PORT SCAN / NMAP : Scanning network for open ports with nmap command

You can use nmap tool for this job. It is flexible in specifying targets. User can scan entire network or selected host or single server. Nmap is also useful to test your firewall rules. namp is metwork exploration tool and security / port scanner. According to nmap man page: It is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime

map port scanning

TCP Connect scanning for localhost and network 192.168.0.0/24

nmap -v -sT localhost

nmap -v -sT 192.168.0.0/24

nmap TCP SYN (half-open)

scanning# nmap -v -sS localhost

nmap -v -sS 192.168.0.0/24

nmap TCP SYN (half-open)

scanning# nmap -v -sS localhost

nmap -v -sS 192.168.0.0/24

nmap TCP Xmas tree scanning

Useful to see if firewall protecting against this kind of attack or not:#

nmap -v -sX localhost

nmap -v -sX 192.168.0.0/24

nmap TCP Null scanning

Useful to see if firewall protecting against this kind attack or not:

nmap -v -sN localhost

nmap -v -sN 192.168.0.0/24

CONCLUSION -

Checked By:

Name of Subject Teacher	Sign with Date

EXPERIMENT NO. 3

TITLE – Observe and note the details of the live type of traffic (ARP, Frame analysis, ethernet) from interface using packet capture and analysis tool

Introduction: The first part of the lab introduces packet sniffer, Wireshark. Wireshark is a free opensource network protocol analyzer. It is used for network troubleshooting and communication protocol analysis. Wireshark captures network packets in real time and display them in human-readable format. It provides many advanced features including live capture and offline analysis, three-pane packet browser, coloring rules for analysis. This document uses Wireshark for the experiments, and it covers Wireshark installation, packet capturing, and protocol analysis.

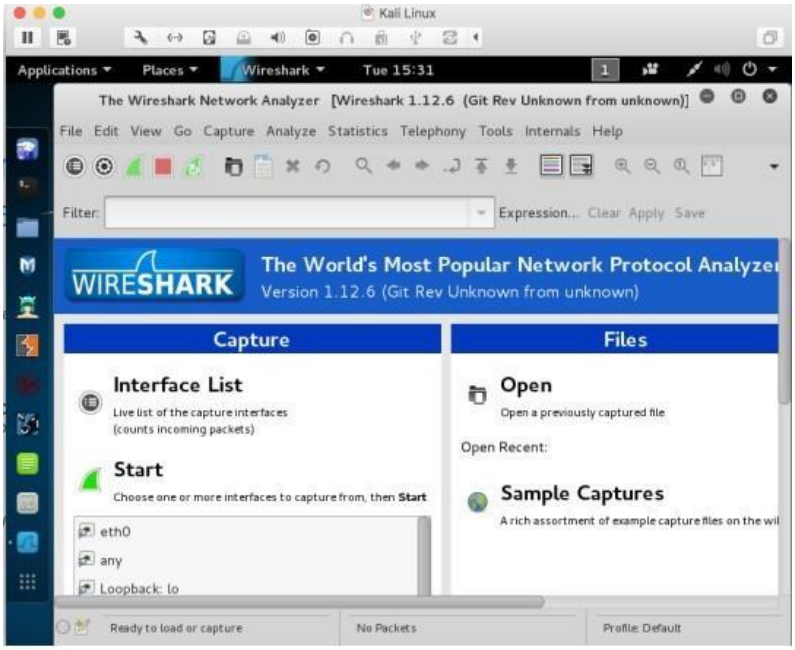


Figure 1: Wireshark in Kali Linux

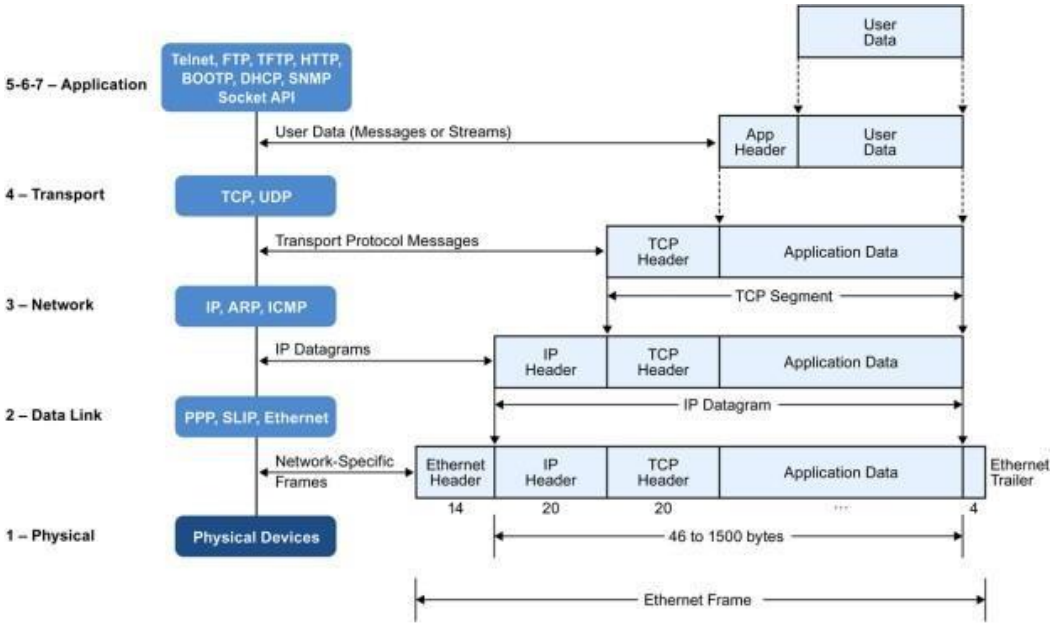


Figure 2: Encapsulation of Data in the TCP/IP Network Stack

In the CSC 4190 Introduction to Computer Networking, TCP/IP network stack is introduced and studied. This background section briefly explains the concept of TCP/IP network stack to help you better understand the experiments. TCP/IP is the most commonly used network model for Internet services. Because its most important protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP) were the first networking protocols defined in this standard, it is named as TCP/IP. However, it contains multiple layers including application layer, transport layer, network layer, and data link layer.

- Application Layer: The application layer includes the protocols used by most applications for providing user services. Examples of application layer protocols are Hypertext Transfer Protocol (HTTP), Secure Shell (SSH), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP).
- Transport Layer: The transport layer establishes process-to-process connectivity, and it provides end-to-end services that are independent of underlying user data. To implement the process-to-process communication, the protocol introduces a concept of port. The examples of transport layer protocols are Transport Control Protocol (TCP) and User Datagram Protocol (UDP). The TCP provides flowcontrol, connection establishment, and reliable transmission of data, while the UDP is a connectionless transmission model.
- Internet Layer: The Internet layer is responsible for sending packets to across networks. It has two functions: 1) Host identification by using IP addressing system (IPv4 and IPv6); and 2) packets routing from source to destination. The examples of Internet layer protocols are Internet Protocol

(IP), Internet Control Message Protocol (ICMP), and Address Resolution Protocol (ARP).

- Link Layer: The link layer defines the networking methods within the scope of the local network link. It is used to move the packets between two hosts on the same link. An common example of link layer protocols is Ethernet.

Packet Sniffer

Packet sniffer is a basic tool for observing network packet exchanges in a computer. As the name suggests, a packet sniffer captures ("sniffs") packets being sent/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured packets. A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself.

Figure 3 shows the structure of a packet sniffer. At the right of Figure 3 are the protocols (in this case, Internet protocols) and applications (such as a web browser or ftp client) that normally run on your computer. The packet sniffer, shown within the dashed rectangle in Figure 3 is an addition to the usual software in your computer, and consists of two parts. The packet capture library receives a copy of every link-layer frame that is sent from or received by your computer. Messages exchanged by higher layer protocols such as HTTP, FTP, TCP, UDP, DNS, or IP all are eventually encapsulated in link-layer frames that are transmitted over physical media such as an Ethernet cable. In Figure 1, the assumed physical media is an Ethernet, and so all upper-layer protocols are eventually encapsulated within an Ethernet frame. Capturing all link-layer frames thus gives you access to all messages sent/received from/by all protocols and applications executing in your computer.

The second component of a packet sniffer is the packet analyzer, which displays the contents of all fields within a protocol message. In order to do so, the packet analyzer must "understand" the structure of all messages exchanged by protocols. For example, suppose we are interested in displaying the various fields in messages exchanged by the HTTP protocol in Figure 3. The packet analyzer understands the format of Ethernet frames, and so can identify the IP datagram within an Ethernet frame. It also understands the IP datagram format, so that it can extract the TCP segment within the IP datagram. Finally, it understands the TCP segment structure, so it can extract the HTTP message contained in the TCP segment. Finally, it understands the HTTP protocol and so, for example, knows that the first bytes ofan HTTP message will contain the string "GET," "POST," or "HEAD". We will be using the Wireshark packet sniffer [http://www.wireshark.org/] for these labs, allowing us to display the contents of messages being sent/received from/by protocols at different levels of the protocol stack. (Technically speaking, Wireshark is a packet analyzer that uses a packet capture library in your computer). Wireshark is a free network protocol analyzer that runs on Windows, Linux/Unix, and Mac computers.

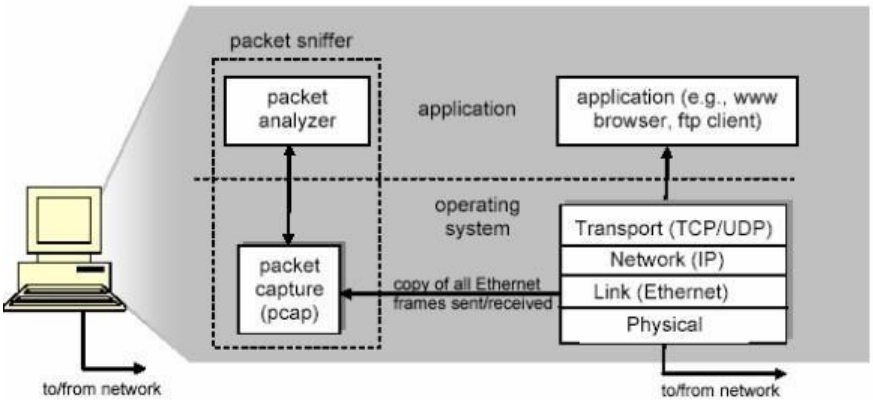


Figure 3: Packet Sniffer Structure

Getting Wireshark

The Kai Linux has Wireshark installed. You can just launch the Kali Linux VM and open Wireshark there. Wireshark can also be downloaded from here: https://www.wireshark.org/download.html

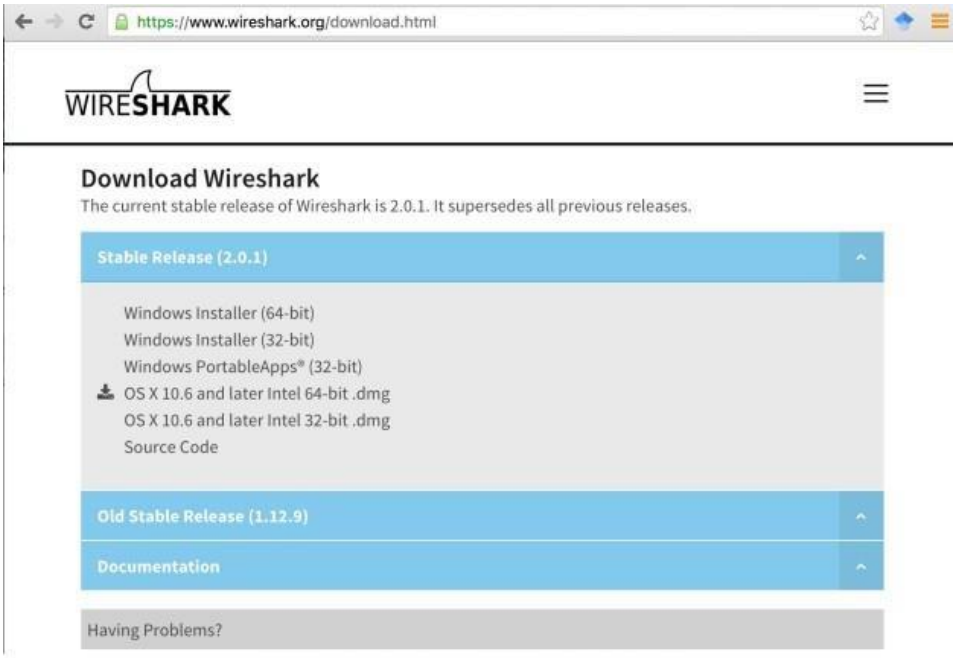


Figure 4: Download Page of Wireshark

Starting Wireshark

When you run the Wireshark program, the Wireshark graphic user interface will be shown as Figure 5.

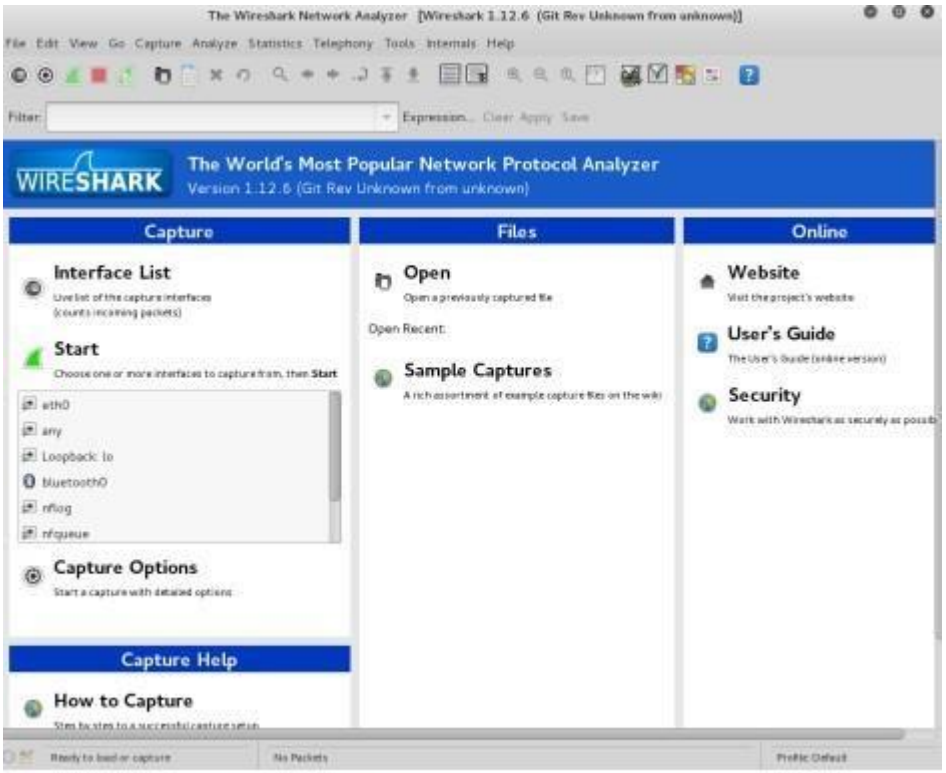


Figure 5: Initial Graphic User Interface of Wireshark

Currently, the program is not capturing the packets.

Then, you need to choose an interface. If you are running the Wireshark on your laptop, you need toselect WiFi interface. If you are at a desktop, you need to select the Ethernet interface being used. Note

that there could be multiple interfaces. In general, you can select any interface but that does not mean that traffic will flow through that interface. The network interfaces (i.e., the physical connections) that your computer has to the network are shown.

The attached Figure 6 was taken from my computer. After you select the interface, you can click start to capture the packets as shown in Figure 7.

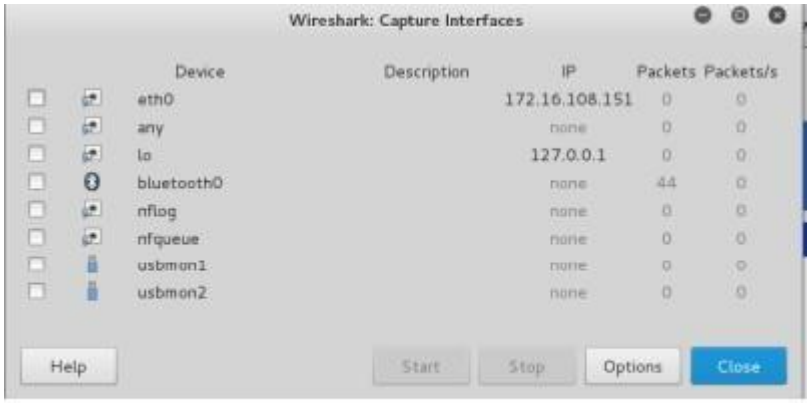


Figure 6: Capture Interfaces in Wireshark

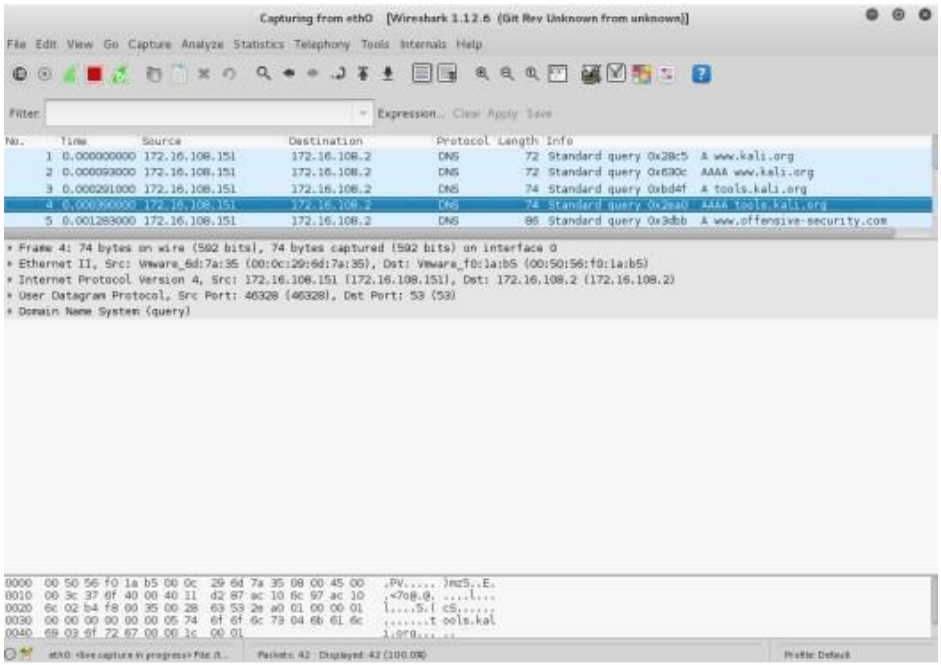


Figure 7: Capturing Packets in Wireshark

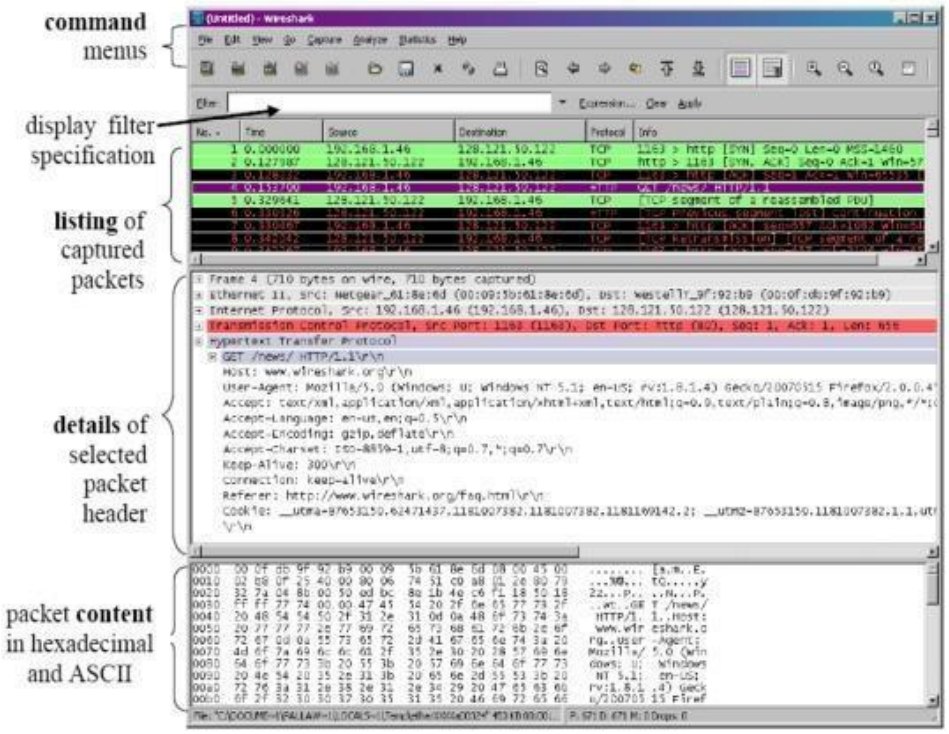


Figure 8: Wireshark Graphical User Interface on Microsoft Windows

The Wireshark interface has five major components:

- **The command menus** are standard pulldown menus located at the top of the window. Of interest to us now is the File and Capture menus. The File menu allows you to save captured packet data or open a file containing previously captured packet data, and exit the Wireshark application. The Capture menu allows you to begin packet capture.
- **The packet-listing window** displays a one-line summary for each packet captured, including the packet number (assigned by Wireshark; this is not a packet number contained in any protocol's header), the time at which the packet was captured, the packet's source and destination addresses, the protocol type, and protocol-specific information contained in the packet. The packet listing can be sorted according to any of these categories by clicking on a column name. The protocol type field lists the highestlevel protocol that sent or received this packet, i.e., the protocol that is the source or ultimate sink for this packet.
- **The packet-header** details window provides details about the packet selected (highlighted) in the packet-listing window. (To select a packet in the packet-listing window, place the cursor over the packet's one-line summary in the packet-listing window and click with the left mouse button.). These details include information about the Ethernet frame and IP datagram that contains this

packet. The amount of Ethernet and IP-layer detail displayed can be expanded or minimized by clicking on the rightpointing or down-pointing arrowhead to the left of the Ethernet frame or IP datagram line in the packet details window. If the packet has been carried over TCP or UDP, TCP or UDP details will also be displayed, which can similarly be expanded or minimized. Finally, details about the highest-level protocol that sent or received this packet are also provided.

- **The packet-contents** window displays the entire contents of the captured frame, in both ASCII and hexadecimal format.
- Towards the top of the Wireshark graphical user interface, is the packet display filter field, into which a protocol name or other information can be entered in order to filter the information displayed in the **packet-listing window** (and hence the packet-header and packet-contents windows). In the example below, we'll use the packet-display filter field to have Wireshark hide (not display) packets except those that correspond to HTTP messages.

Capturing Packets

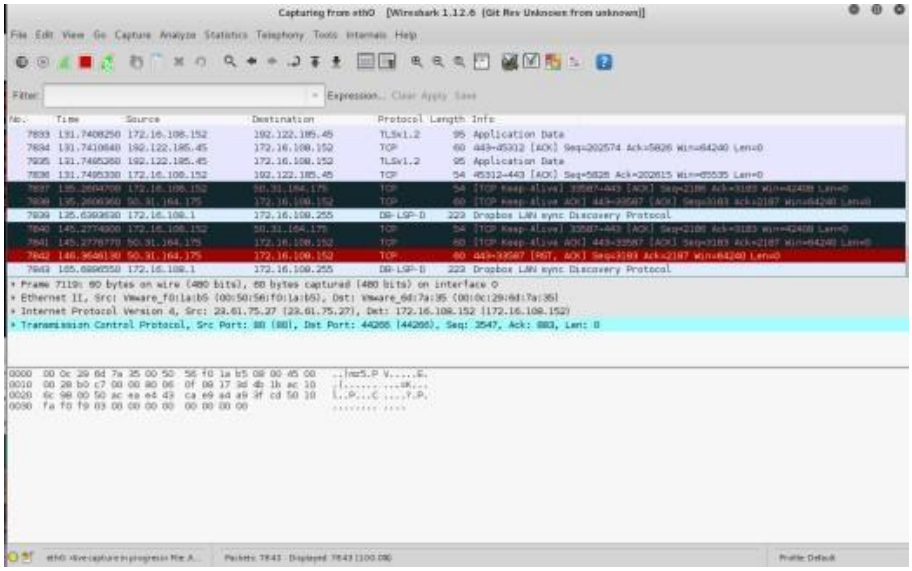
After downloading and installing Wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface.

Test Run

Do the following steps:

1. Start up the Wireshark program (select an interface and press start to capture packets).
2. Start up your favorite browser (ceweasel in Kali Linux).
3. In your browser, go to Wayne State homepage by typing www.wayne.edu.
4. After your browser has displayed the http://www.wayne.edu page, stop Wireshark packet captureby selecting stop in the Wireshark capture window. This will cause the Wireshark capture window to disappear and the main Wireshark window to display all packets captured since you began packet capture see image below:

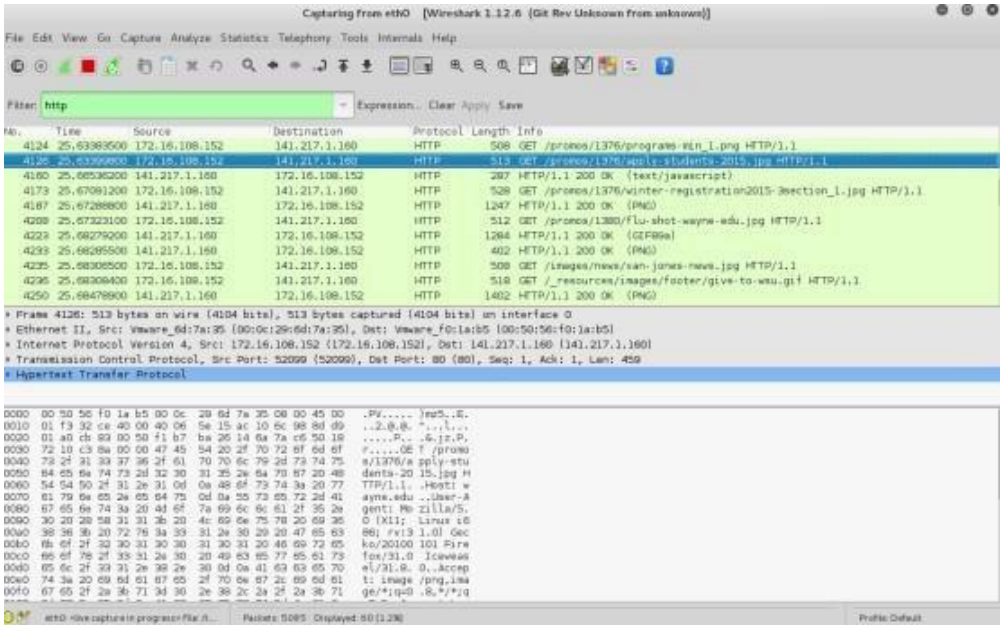
5. Color Coding: You'll probably see packets highlighted in green, blue, and black. Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is



DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems — for example, they could have been delivered out-of-order.

6. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! However, as you will notice the HTTP messages are not clearly shown because there are many other packets included in the packet capture. Even though the only action you took was to open your browser, there are many other programs in your computer that communicate via the network in the background. To filter the connections to the ones we want to

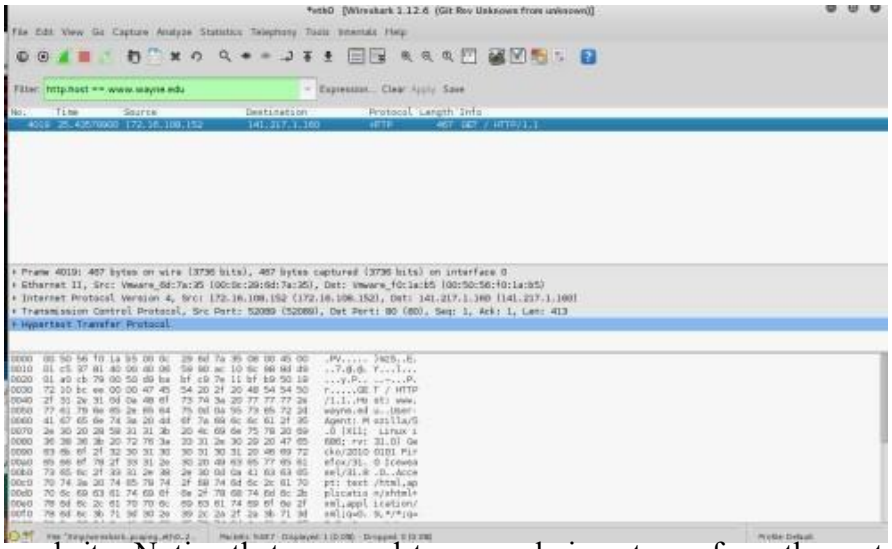
focus on, we have to use the filtering functionality of Wireshark by typing "http" in the filtering field



as shown below:

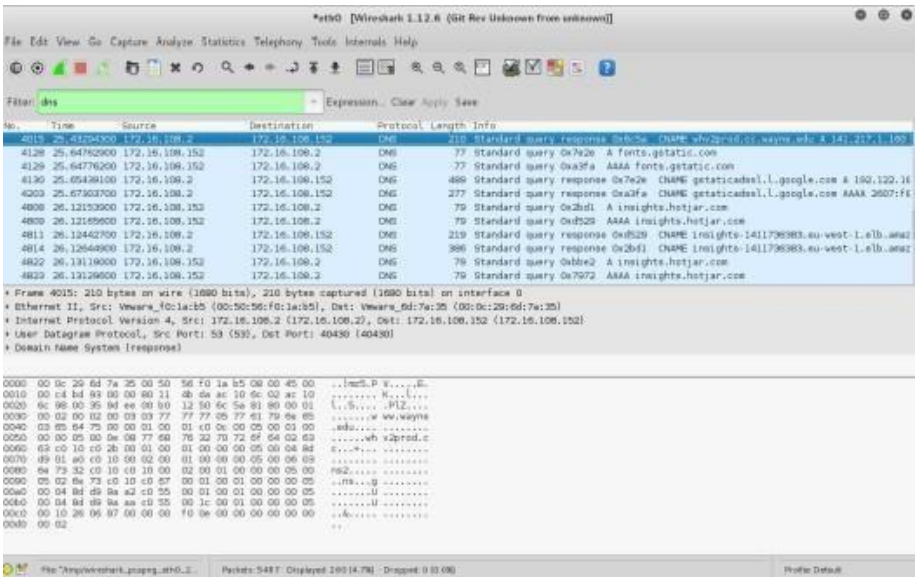
Notice that we now view only the packets that are of protocol HTTP. However, we also still do not have the exact communication we want to focus on because using HTTP as a filter is not descriptive enough to allow us to find our connection to http://www.wayne.edu. We need to be more precise if we want to capture the correct set of packets.

7. To further filter packets in Wireshark, we need to use a more precise filter. By setting the http.host==www.wayne.edu, we are restricting the view to packets that have as an http host the

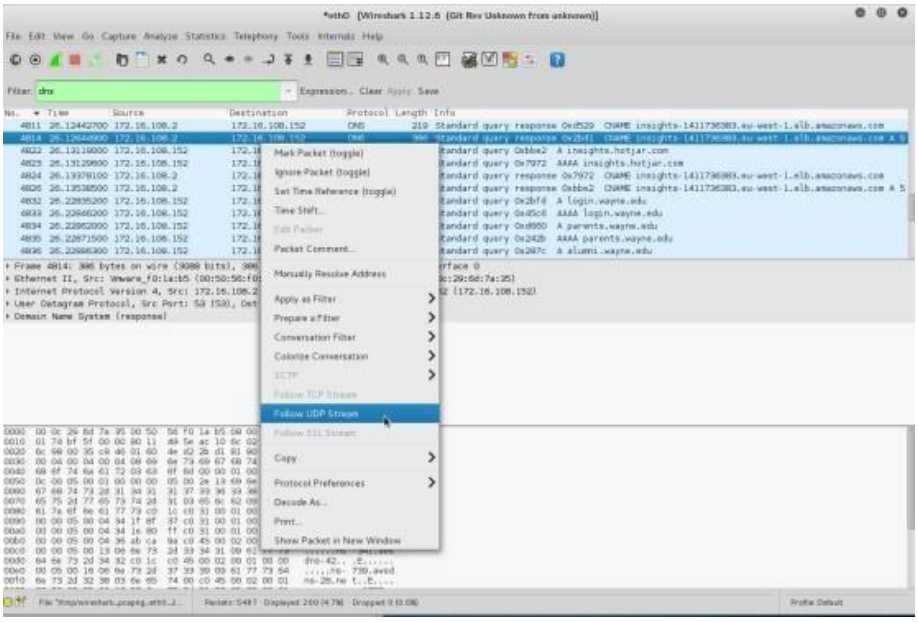


www.wayne.edu website. Notice that we need two equal signs to perform the match "==" not just one. See the screenshot below:

8. Now, we can try another protocol. Let's use Domain Name System (DNS) protocol as an example here.



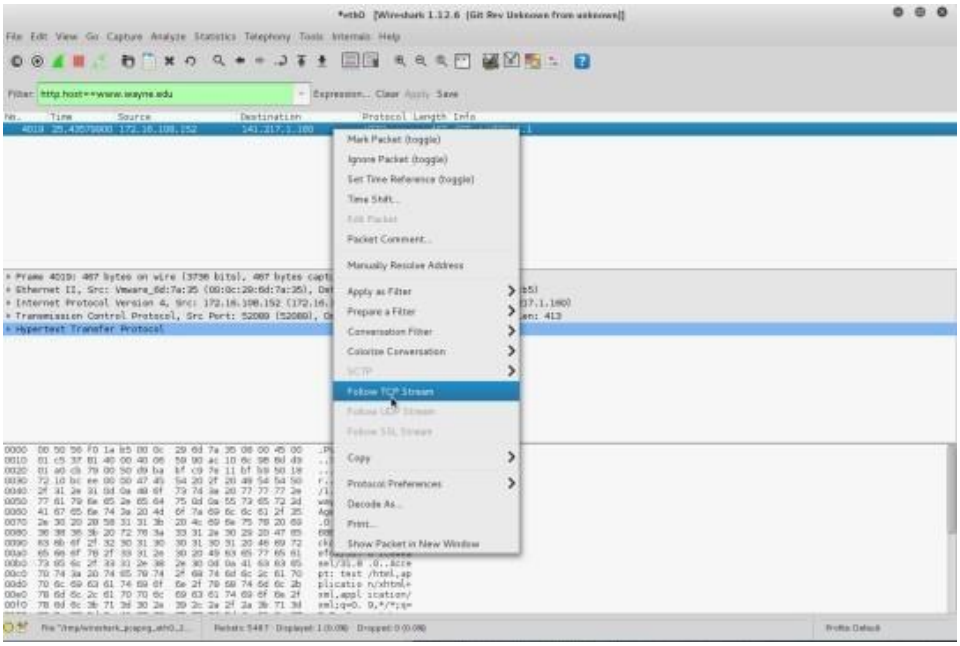
9. Let's try now to find out what are those packets contain by following one of the conversations (also called network flows), select one of the packets and press the right mouse button (if you are ona Mac



use the command button and click), you should see something similar to the screen below:

Click on Follow UDP Stream, and then you will see following screen

10. If we close this window and change the filter back to “http.host==www.wayne.edu” and then follow a packet from the list of packets that match that filter, we should get the something similar to



the following screens. Note that we click on Follow TCP Stream this time.

CONCLUSION –

Checked By:

Name of Subject Teacher	Sign with Date

EXPERIMENT NO. 4

TITLE – Using Network Simulator (e.g., packet tracer) Configure router using RIP

RIP protocol is an open standard, distance-vector, Interior Gateway Routing (IGP) routing protocol. Since it is an IGP protocol, it can only be used to perform routing between networks within the same autonomous system. Typically, it is suitable for a small-sized network.

Features of RIP Routing Protocol

Some of the of key features of RIP protocol are:

- It supports maximum 15 hops in a path.
- It uses hops count metric to calculate the best path from a source to a destination network.
- It sends routing updates (entire routing table) after every 30 seconds and when the network changes.
- It uses UDP broadcast packets to exchange routing information.
- The Administrative Distance (AD) value of the RIP protocol is 120.
- It has two versions: RIPv1 and RIPv2.

Routing Loops

If you want to configure RIP protocol on your network, you have to be familiar with the routing loops. Sometimes routing loops create a big issue on an RIP-based network. However, RIP protocol has some mechanisms that can be used to prevent the routing loops and maintain the network stability. These mechanisms are:

- **Split horizon:** In the split horizon, route information is not sent back out through the interface from which it was received. Thus, allowing to prevent routing loops.
- **Hop-count limit:** Limiting the hop-count prevents routing loops from continuing indefinitely.
- **Poison reverse:** In this mechanism, a router marks a route (that is not accessible) as unreachable and set the hop count to 16. The router then passes this route out to the neighbor router, and the neighbor router

removes the unreachable route from its routing table.

• **Hold-down timers:** When the hold-down timers are set, routers ignore the routing update information for the set period of time.

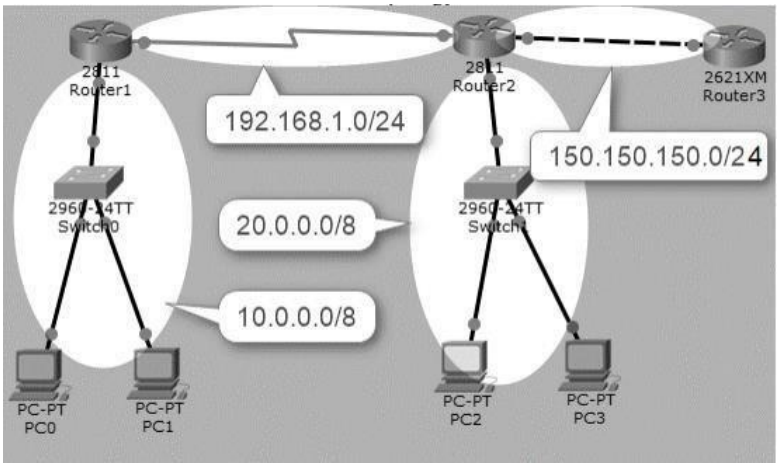
RIP Timers

Routing protocols use timers to optimize the network performance. The following table lists the various types of timers used by the RIP protocol to optimize the network performance.

Timers	Default Value	Uses
Hold down timer	180 seconds	Used to hold the routing information for the specified time.
Invalid route timer	180 seconds	Used to keep track of discovered routes
Route update timer	30 seconds	Used to update routing information
Route flush timer	240 seconds	Used to set time interval for any route that becomes invalid and its deletion from the routing table.

RIP Configuration

To demonstrate how to configure RIP in Cisco Packet Tracer, we will use the following network topology. If you are using a simulator, such as Cisco Packet Tracer or GNS3, create the following topology and configure the IP addresses as mentioned in the topology.



If you are using a simulator, such as Cisco Packet Tracer or GNS3, create the preceding topology and configure the devices as per the values mentioned in the following table.

Sr. No.	Device	Interface	IP Address
1	Router1	Fa0/1	10.0.0.1/8
		S1/0	192.168.1.1/24
2	Router2	S1/0	192.168.1.2/24
		Fa0/0	20.0.0.1/8
		Fa0/1	150.150.150.1/24
3	Router3	Fa0/1	150.150.150.2/24
4	Switch1	N/A	N/A
5	Switch2	N/A	N/A
6	PC0	Fa0	10.0.0.2/8
7	PC1	Fa0	10.0.0.3/8
8	PC2	Fa0	20.0.0.2/8
9	PC3	Fa0	20.0.0.3/8

First of all, configure the IP addresses on each device. We assume that you know how to configure IP addresses. If you stuck in configuring IP addresses, click here to know how to configure IP address or you can refer the following example

For example, to configure TCP/IP addresses on Router1, execute the following commands:

Router1(config)#interface fa0/1

Router1(config-if)#ip add 10.0.0.1

255.0.0.0Router(config-if)#no shut

Router1(config-if)#exit

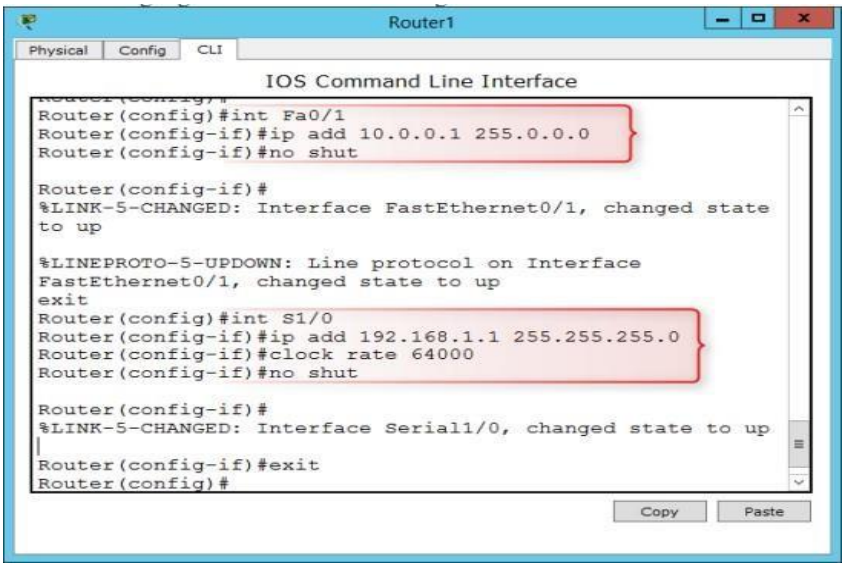
Router1(config)#interface S1/0

Router1(config-if)#ip add 192.168.1.1 255.255.255.0

Router1(config-if)#clock rate

64000Router(config-if)#no shut

The following figure shows the IP configuration of Router1



Steps to Configure RIP Routing

Once you have configured the appropriate IP addresses on each device, perform the following steps to configure RIP routing. The default version of RIP is RIPv1. In the later section, we will also configure RIPv2 routing.

1. On Router1, execute the following commands to configure RIP routing

Router1(config)#router rip

Router1(config-router)#network 10.0.0.0

Router1(config-router)#network 192.168.1.0

Router1(config-router)#exit

2. On Router2, execute the following commands to configure RIP routing

Router2(config)#router rip

Router2(config-router)#network 20.0.0.0

Router2(config-router)#network 192.168.1.0

Router2(config-router)#network 150.150.150.0

Router2(config-router)#exit

Router2(config)#

3. On Router3, execute the following commands to configure RIP routing.

Router3(config)#router rip

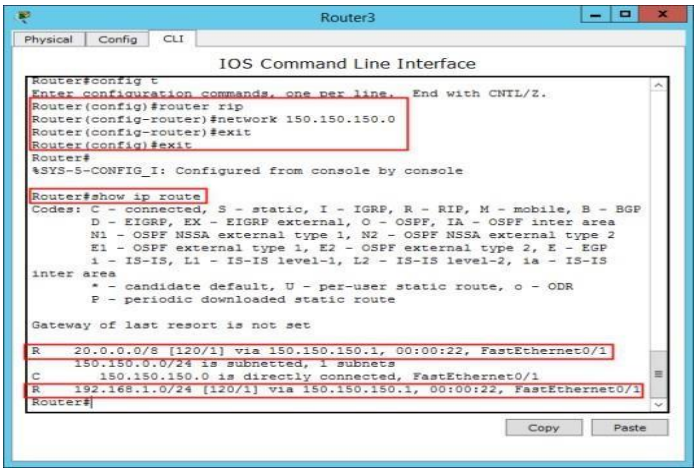
Router3(config-router)#network 150.150.150.0

Router3(config-if)#exit

Once you have configured RIP routing protocol on each router, wait for a few seconds (let complete the convergence process), and then execute the show ip route command on any router to show the routing information.

Router(config)#do show ip route

In the following figure, you can see the routes learned by the RIP protocol on Router3.



Verifying RIP Configuration

To verify and test the RIP configuration, perform the following steps:

1. To verify which routing protocol is configured, use the show ip protocols command.

    Router#show ip protocols

2. To view the RIP messages being sent and received, use the debug ip rip command.

    Router#debug ip rip

3. To stop the debugging process, use the undebug all command.

    Router#undebug all

Removing RIP Routing Configuration

If you have added a wrong network or route, you can remove that network from the routing table. In this section, we will learn how to remove the routes learned by the RIP protocol. To do this, perform the following tasks.

• **On Router1, execute the following commands.**

Router1(config)#router rip
Router1(config-router)#no network 10.0.0.0
Router1(config-router)#no network 192.168.1.0
Router1(config-router)#exit

• **On Router2, execute the following commands.**

Router2(config)#router rip

Router2(config-router)#no network 20.0.0.0

Router2(config-router)#no network 192.168.1.0

Router2(config-router)#no network 150.150.150.0

Router2(config-router)#exit

• **On Router3, execute the following commands.**

Router3(config)#router rip

Router3(config-router)#no network 150.150.150.0

Router3(config-router)#exit

Now, execute the **show ip route** command and verify that the routes learned by the RIP routing protocol are deleted. If the routes are still available in the routing table, execute the **clear ip route** * command.

Conclusion:

Checked By:

Name of Subject Teacher	Sign with Date

EXPERIMENT NO. 5

TITLE – Write a program to simulate leaky bucket/token bucket.

Requirement: Computer loaded with 'C'

Theory:

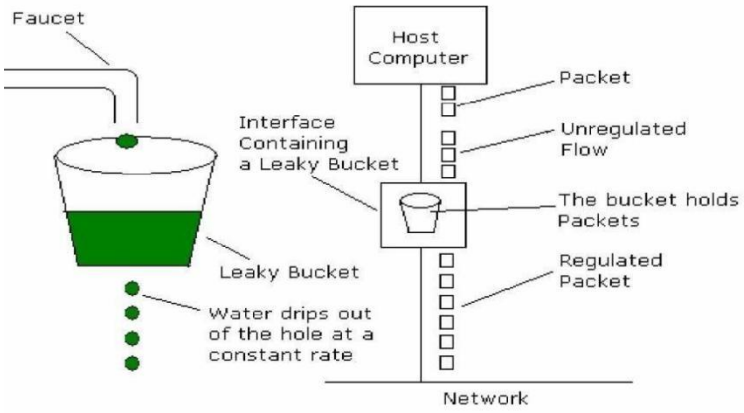
The congesting control algorithms are basically divided into two groups: open loop and closed loop. Open loop solutions attempt to solve the problem by good design, in essence, to make sure it does not occur in the first place. Once the system is up and running, midcourse corrections are not made. Open loop algorithms are further divided into ones that act at source versus ones that act at the destination.

In contrast, closed loop solutions are based on the concept of a feedback loop if there is any congestion. Closed loop algorithms are also divided into two sub categories: explicit feedback and implicit feedback. In explicit feedback algorithms, packets are sent back from the point of congestion to warn the source. In implicit algorithm, the source deduces the existence of congestion by making local observation, such as the time needed for acknowledgment to come back.

The presence of congestion means that the load is (temporarily) greater than the resources (in part of the system) can handle. For subnets that use virtual circuits internally, these methods can be used at the network layer.

Another open loop method to help manage congestion is forcing the packet to be transmitted at a more predictable rate. This approach to congestion management is widely used in ATM networks and is called traffic shaping.

The other method is the leaky bucket algorithm. Each host is connected to the network by an interface containing a leaky bucket, that is, a finite internal queue. If a packet arrives at the queue when it is full, the packet is discarded. In other words, if one or more process are already queued, the new packet is unceremoniously discarded. This arrangement can be built into the hardware interface or simulate d by the host operating system. In fact it is nothing other than a single server queuing system with constant service time. The host is allowed to put one packet per clock tick onto the network. This mechanism turns an uneven flow of packet from the user process inside the host into an even flow of packet onto the network, smoothing out bursts and greatly reducing the chances of congestion.



ALGORITHM

1. Start
2. Set the bucket size or the buffer size.
3. Set the output rate.

PROGRAM CODE

```
1.  #include<stdio.h>
2.  #include<stdlib.h>
3.  #include<unistd.h>
4.
5.  #define NOF_PACKETS 10
6.
7. int rand(int a)
8. {
9.      int rn = (random() % 10) % a;
10.     return rn == 0 ? 1 : rn;
11.
}12.
13. int main()
14. {
```

```
15.  int packet_sz[NOF_PACKETS], i, clk, b_size, o_rate, p_sz_rm=0, p_sz, p_time, op;
16.  for(i = 0; i<NOF_PACKETS; ++i)
17.     packet_sz[i] = rand(6) * 10;
18.  for(i = 0; i<NOF_PACKETS; ++i)
19.     printf("\npacket[%d]:%d bytes\t", i, packet_sz[i]);
20.  printf("\nEnter the Output rate:");
21.  scanf("%d", &o_rate);
22.  printf("Enter the Bucket Size:");
23.  scanf("%d", &b_size);
24.  for(i = 0; i<NOF_PACKETS; ++i)
25.  {
26.     if( (packet_sz[i] + p_sz_rm) > b_size)
27.        if(packet_sz[i] > b_size)/*compare the packet siz with bucket size*/
28.           printf("\n\nIncoming packet size (%dbytes) is Greater than bucket capacity (%dbytes)-
   PACKET REJECTED", packet_sz[i], b_size);
29.        else
30.           printf("\n\nBucket capacity exceeded-PACKETS REJECTED!!");
31.     else
32.     {
33.        p_sz_rm += packet_sz[i];
34.        printf("\n\nIncoming Packet size: %d", packet_sz[i]);
35.        printf("\nBytes remaining to Transmit: %d", p_sz_rm);
36.        p_time = rand(4) * 10;
37.        printf("\nTime left for transmission: %d units", p_time);
38.        for(clk = 10; clk <= p_time; clk += 10)
39.        {
40.           sleep(1);
41.           if(p_sz_rm)
42.           {
43.              if(p_sz_rm <= o_rate)/*packet size remaining comparing with output rate*/
44.                 op = p_sz_rm, p_sz_rm = 0;
45.              else
```

```
                op = o_rate, p_sz_rm -= o_rate;
            printf("\nPacket of size %d Transmitted", op);
            printf("--- Bytes Remaining to Transmit: %d", p_sz_rm);
        }
        else
        {
            printf("\nTime left for transmission: %d units", p_time-clk);
            printf("\nNo packets to transmit!!");
        }
    }
  }
}
```

ALTERNATE CODE

```
#include<iostream.h>
#include<dos.h>
#include<stdlib.h>
#define bucketSize
512
        void bktInput(int a,int b)
                {if(a>bucketSize)
                        cout<<"\n\t\tBucket overflow";
                else {
                    }
                }
        void main() {

delay(500);while(a>b){
cout<<"\n\t\t"<<b<<"
bytes outputted.";a-=b;
delay(500);
}
if (a>0) cout<<"\n\t\tLast
"<<a<<"  bytes  sent\t";
cout<<"\n\t\tBucket
output successful";
```

}

Output

Enter output rate : 100

Packet no 0 Packet size = 3
Bucket output successful Last 3
bytes sent
Packet no 1 Packet size = 33
Bucket output successful Last
33 bytes sent
Packet no 2 Packet size = 117
Bucket output successful
100 bytes outputted. Last
17 bytes sent
Packet no 3 Packet size = 95
Bucket output successful Last
95 bytes sent
Packet no 4 Packet size = 949
Bucket overflow

CONCLUSION -

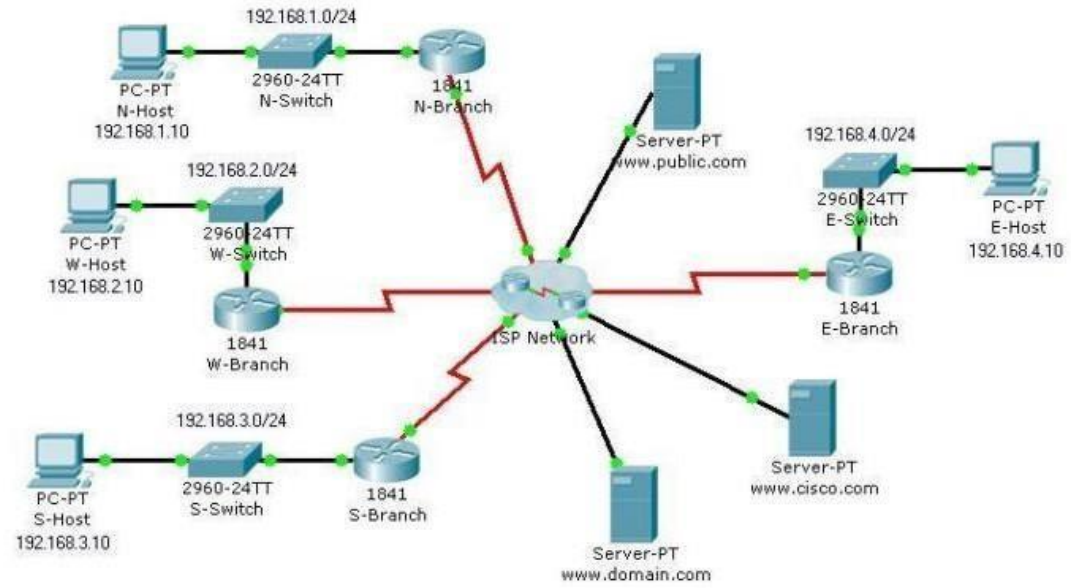
Checked By:

Name of Subject Teacher	Sign with Date

EXPERIMENT NO. 6

TITLE – Observe and note the working of protocols using PING / TRACEROUTE / PATHPING andcapture packets in LAN using packet capture and analysis tool.

Topology Diagram



Objectives

- Distinguish the difference between successful and unsuccessful ping attempts
- Distinguish the difference between successful and unsuccessful traceroute attempts.

Background / Preparation

In this activity, you will test end-to-end connectivity using ping and traceroute. At the end of this activity, you will be able to distinguish the difference between successful and unsuccessful ping and traceroute attempts. Note: Before beginning this activity, make sure that the network is converged. To converge the network quickly, switch between Simulation mode and Realtime mode until all the link lights turn green.

Step 1: Test connectivity using ping from a host computer and a router.

Click N-Host, click the Desktop tab, and then click Command Prompt. From the Command Prompt

window, ping the Cisco server at www.cisco.com.

Packet Tracer PC Command Line

1.0PC>ping www.cisco.com

Pinging 64.100.1.185 with 32 bytes of data:

Request timed out

Reply from 64.100.1.185: bytes=32 time=185ms TTL=123 Reply from 64.100.1.185: bytes=32 time=281ms TTL=123 Reply from 64.100.1.185: bytes=32 time=287ms TTL=123

Ping statistics for 64.100.1.185:

Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),Approximate round trip times in milli-seconds:

Minimum = 185ms, Maximum = 287ms, Average = 251msPC>

From the output, you can see that N-Host was able to obtain an IP address for the Cisco server. The IP address was obtained using (DNS). Also notice that the first ping failed. This failure is most likely due to lack of ARP convergence between the source and destination. If you repeat the ping, you will notice that all pings succeed.

From the Command Prompt window on N-Host, ping E-Host at 192.168.4.10. The pings fail. If you do notwant to wait for all four unsuccessful ping attempts, press Ctrl+C to abort the command, as shown below

PC>ping 192.168.4.10

PC>ping 192.168.4.10 with 32 bytes of data:

Request timed out.

Request timed out

Ping statistics for 192.168.4.10:

Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),Control-C

```
^C
PC
>
```

Click the N-Branch router, and then click the CLI tab. Press Enter to get the router prompt. From the router prompt, ping the Cisco server at ~~www.cisco.com~~.

```
N-Branch>ping www.cisco.com
Translating "www.cisco.com"...domain server (64.100.1.242)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 64.100.1.185, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 210/211/213 ms
N-Branch>
```

As you can see, the ping output on a router is different from a PC host. Notice that the N-Branch router resolved the domain name to the same IP address that N-Host used to send its pings. Also notice that the first ping fails, which is indicated by a period (.), and that the next four pings succeed, as shown with an exclamation point (!).

From the CLI tab on N-Branch, ping E-Host at 192.168.4.10. Again, the pings fail. To not wait for all thefailures, press Ctrl+C.

```
N-Branch>ping 192.168.4.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.10, timeout is 2 seconds:
...
Success rate is 0 percent (0/4)
N-Branch>
```

Step 2: Test connectivity using traceroute from a host computer and a router.

Click N-Host, click the Desktop tab, and then click Command Prompt. From the CommandPrompt window, trace the route to the Cisco server at www.cisco.com.

PC>tracert www.cisco.com

Tracing route to 64.100.1.185 over a maximum of 30 hops:

1 92 ms 77 ms 86 ms 192.168.1.1

2 91 ms 164 ms 84 ms 64.100.1.101

3 135 ms 168 ms 151 ms 64.100.1.6

4 185 ms 261 ms 161 ms 64.100.1.34

5 257 ms 280 ms 224 ms 64.100.1.62

6 310 ms 375 ms 298 ms 64.100.1.185

Trace complete.

PC>

The above output shows that you can successfully trace a route all the way to the Cisco server at 64.100.1.185. Each hop in the path is a router responding three times to trace messages from N-Host. The trace continues until the destination for the trace (64.100.1.185) responds three times.

From the Command Prompt window on N-Host, trace a route to E-Host at 192.168.4.10. The trace fails, but notice that the tracert command traces up to 30 hops. If you do not want to wait for all 30 attemptsto time out, press Ctrl+C.

```
PC>tracert 192.168.4.10

Tracing route to 192.168.4.10 over a maximum of 30 hops:

  1 103 ms     45 ms     91 ms     192.168.1.1
  2 56 ms      110 ms    125 ms    64.100.1.101
  3 174 ms     195 ms    134 ms    64.100.1.6
  4 246 ms     183 ms    179 ms    64.100.1.34
  5 217 ms     285 ms    226 ms    64.100.1.62
  6 246 ms     276 ms    245 ms    64.100.1.154
  7   *        *         *         Request timed out.
  8   *        *         *         Request timed out.
  9   *        *         *         Request timed out.
 10
Control-C
^C
PC>
```

The tracert command can be helpful in finding the potential source of a problem. The last device to respond was 64.100.1.154, so you would start troubleshooting by determining which device is configured with the IP address 64.100.1.154. The source of the problem might not be that device, but the trace has given you a starting point, whereas a ping simply tells you that the destination is either reachable or unreachable.

Click the N-Branch router, and then click the CLI tab. Press Enter to get the router prompt. From the

router prompt, trace the route to the Cisco server at www.cisco.com.

```
N-Branch>traceroute www.cisco.com
Translating "www.cisco.com"...domain server (64.100.1.242)
Type escape sequence to abort.
Tracing the route to 64.100.1.185

 1 64.100.1.101    60 msec 32 msec 59 msec
 2 64.100.1.6      98 msec 65 msec 65 msec
 3 64.100.1.34     138 msec 147 msec 147 msec
 4 64.100.1.62     189 msec 148 msec 145 msec
 5 64.100.1.185    219 msec 229 msec 293 msec
N-Branch>
```

As you can see, traceroute output on a router is very similar to the output on a PC host. The only difference is that on a PC host, the IP address is listed after the three millisecond outputs.

From the CLI tab on N-Branch, trace the route to E-Host at 192.168.4.10. The trace fails at the same IP address as it failed when tracing from N-Host. Again, you can use Ctrl+C to abort the command.

```
N-Branch>traceroute 192.168.4.10
Type escape sequence to abort.
Tracing the route to 192.168.4.10

 1  64.100.1.101   41 msec   19 msec   32 msec
 2  64.100.1.6     33 msec   92 msec   117 msec
 3  64.100.1.34    98 msec 102 msec 102 msec
 4  64.100.1.62    166 msec 172 msec 156 msec
 5  64.100.1.154   157 msec 223 msec 240 msec
 6  *    *    *
 7  *    *    *
 8  *    *    *
 9
N-Branch>
```

CONCLUSION -

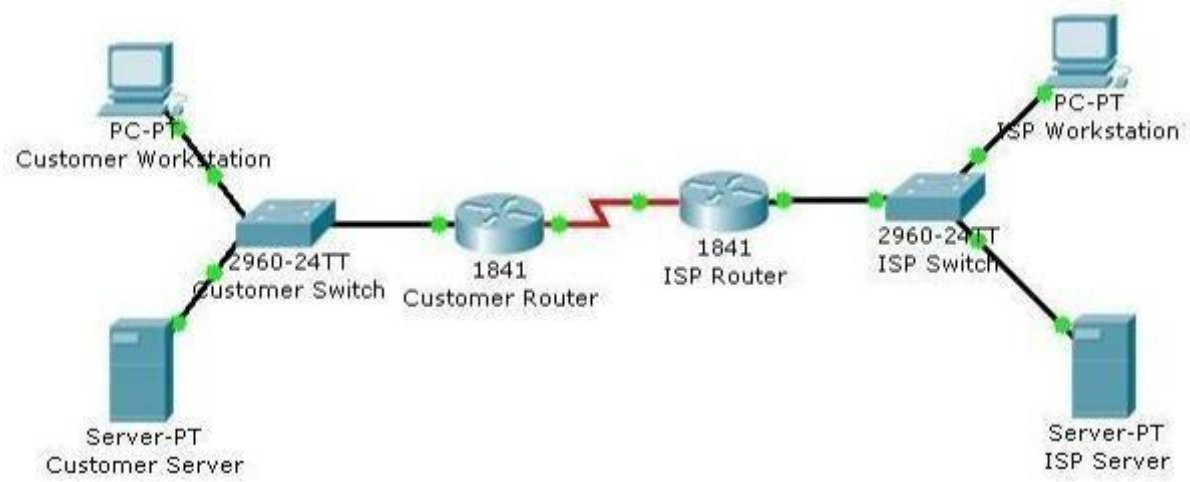
Checked By:

Name of Subject Teacher	Sign with Date

EXPERIMENT NO. 7

TITLE – Executing Telnet, DHCP Server using simulator.

Topology Diagram



Background / Preparation

In this activity, you will continue to configure the Cisco 1841 ISR router for the customer network by configuring the DHCP service. The customer has several workstations that need to be automatically configured with IP addresses on the local subnet and appropriate DHCP options to allow access to the Internet.

The DHCP pool will use the 192.168.1.0/24 network but the first 49 addresses are excluded. The default gateway and DNS server also need to be configured as 192.168.1.1 and 192.168.1.10. For this activity, both the user and privileged EXEC passwords are cisco.

Note: Packet Tracer does not currently support the domain name and lease period options. These options are not used in this activity.

Step 1: Configure the DHCP service.

a. From the customer workstation, use a console cable and terminal emulation software to connect to the console of the customer Cisco1841 ISR.

b. Log in to the console of the Cisco 1841 ISR and enter global configuration mode.

c. Before creating a DHCP pool, configure the addresses that are excluded. The range is from 192.168.1.1 to 192.168.1.49

CustomerRouter(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.49

d. Create a DHCP pool called pool1.

CustomerRouter(config)#ip dhcp pool pool1

e. Define the network address range for the DHCP pool

CustomerRouter(dhcp-config)#network 192.168.1.0 255.255.255.0

f. Define the DNS server as 192.168.1.10.

CustomerRouter(dhcp-config)#dns-server 192.168.1.10

g. Define the default gateway as 192.168.1.1

CustomerRouter(dhcp-config)#default-router 192.168.1.1

h. Add an exclusion range of 192.168.1.1 to 192.168.1.49 to the DHCP pool.CustomerRouter(dhcp-config)#exit

CustomerRouter(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.49

i. Exit the terminal.

Step 2: Verify the DHCP configuration.

a. From the customer workstation, open the Command Prompt window.

b. Type ipconfig /release to release the current IP address.

c. Type ipconfig /renew to request a new IP address on the local network.

d. Verify that the IP address has been correctly assigned by pinging the LAN IP address of the Cisco 1841 ISR.

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

CONCLUSION-

Checked By:

Name of Subject Teacher	Sign with Date

EXPERIMENT NO : - 8

TITLE : Installation and configuration of Web server, FTP Server.

Objectives

Connect to a Web server.

Assign multiple IP addresses to the web server.

Install virtual web servers using IP addresses and port numbers.

Use FTP service to transfer files.

Use netstat to check the status of the TCP ports.

Install virtual FTP servers using IP addresses and port numbers.

Network performance study using FTP.

Requirement

Personal computers with Network Interface Cards connected through category 5 UTP cables.

Windows 2000/2003 server Network Operating Systems installed in each computer.

TCP/IP protocol installed in each computer.

Switches to connect all peer computers.

Students are provided with local administrator account.

A web page should be available on LABSERVER (192.168.101.15) which is acting as a web server for thelab.

A FTP server should be running on the lab server (192.168.101.15) and populated with files.

Introduction to Web server:

Web servers are computers that deliver Web pages. Every Web server has an IP address and possibly a domain name.

For example, if you enter the URL http://www.pcweb.com/index.html in your browser, this sends a request to the Web server whose domain name is pcweb.com.

The server then fetches the page named index.html and sends it to your browser. Any computer can be turned into a Web server by installing server software and connecting the machine to the Internet.

There are many Web server software applications, including public domain software from NCSA and Apache, and commercial packages from Microsoft, Netscape and others.

Default Port number for Web Server is 80

Introduction to FTP server:

In FTP, the protocol for exchanging files over the Internet. FTP works in the same way as HTTP for transferring Web pages from a server to a user's browser and SMTP for transferring electronic mail across the Internet in that, like these technologies, FTP uses the Internet's TCP/IP protocols to enable data transfer.FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server (e.g., uploading a Web page file to a server).

An FTP server is a software.html application running the *File Transfer Protocol* (FTP), which is the protocol for exchanging files over the Internet.

Port number for FTP – Data is 20

Port number for FTP – Control is 21

Introduction to IIS:

Internet Information Services (IIS) – formerly called Internet Information Server – is a web server application and set of feature extension modules created by Microsoft for use with Microsoft Windows. It is the most used web server after Apache HTTP Server. IIS 7.5 supports HTTP, HTTPS, FTP,FTPS, SMTP and NNTP. It is an integral part of Windows Server family of products, as well as certain editions of Windows XP, Windows Vista and Windows 7. IIS is not turned on by default when Windows is installed.

Default Port number for IIS is

80IIS Versions:

- **IIS 1.0, Windows NT 3.51 available as a free add-on**
- **IIS 2.0, Windows NT 4.0**
- **IIS 3.0, Windows NT 4.0 Service Pack 2[10]**
- **IIS 4.0, Windows NT 4.0 Option Pack**
- **IIS 5.0, Windows 2003**
- **IIS 5.1, Windows XP Professional and Windows XP Media Center Edition (requires retail CD)**
- **IIS 6.0, Windows Server 2003 and Windows XP Professional x64 Edition**

IIS 7.0, Windows Server 2008 and Windows Vista (Home Premium, Business, Enterprise and

- **Ultimate editions)**
- **IIS 7.5, Windows Server 2008 R2 and Windows 7 (Home Premium, Professional, Enterprise andUltimate editions**

Test a Web server using an Internet browser and HTTP commands:

1. Switch to **Windows 2003 Server** and then Start **Internet Explorer**.
2. The URL will be **http://** followed by the IP address of your web server (Note the forward slash marks). In the **Address** box you would type:m, **http://196.15.60.220**

then press the Enter key. The home page should appear on the screen.

3. In the address box, type and watch: **http://196.15.60.220/default.htm**
4. Count the number of objects in the **default.htm** web page
5. At the command prompt, type:

And then, D:\> **netstat**

D:\> **netstat -n**

6. Telnet to the lab web server and use the HTTP commands to download HTTP objects:

D:\> **telnet**

Telnet > **set local_echo**

Telnet > **open 196.15.60.220 80**

client: GET /

* Each time you issue a HTTP command; don't forget to open a telnet connection with 196.15.60.220 at port 80.

client: GET /default.htm HTTP/1.0

Configuring IIS5 to host your default web site (Windows 2003 server):

Microsoft Internet Information Services allows the developer to efficiently deploy a web-based solution.

1. Install the IIS5 service components if not already installed (**Control Panel**, **Add/Remove Programs**, and **Add/Remove Windows Components**). Click the checkbox next to **Internet Information Service (IIS)** to be installed. Click **Next** to start the installation process (All files needed for the installation processes are in D:\I386).
2. The installation of IIS5 creates a folder **Inetpub** in the D drive. This folder contains a number of subfolders such as **wwwroot** and **ftproot**. All materials for the default web site should be saved under **D:\inetpub\wwwroot** directory.

3. Create a web page using the HTML code given in the last page of the worksheet. Save it as

default.htm to your default www service directory, i.e., **D:\Inetpub\wwwroot**

4. In the Address box of your internet browser type: **127.0.0.1**

5. Keep the HTML page you constructed. Your instructor will check your work at the end of the lab.
6. Try to access the web servers of your classmates by typing the IP address of the servers in the Address box of your Internet browser.
   Do you read their HTML pages? Try to check with them.

7. Where to find the IIS Console: click on **Start**, **Programs**, **Administrative Tools** and then **InternetServices Manager**.

8. Under the server name (NetpcX), select the **Default Web Site** service and right-click on it.
9. Select **Properties** and note the TCP port at which the web server is listening.
10. By selecting **Start**, **Stop**, or **Pause** (when right-clicking on **Default Web Site** service), you can controlthe default web service process.
    What happens when the WWW service is Stopped, Started and Paused? Check your web server in these situations using the Internet browser.

Setting up multiple IP addresses (Windows 2003 server):

Multiple IP addresses are one of the methods of hosting a number of web sites on a single IIS Server. In this part, you will add another IP address to your computer.

1. Right-click on **My Network Places** and select **Properties**.
2. Opening your local area connection properties: to open the **Network Properties** dialogue box, right-click on **Local Area Connection** and select **Properties**.

3. Internet Protocol (TCP/IP): ignore everything else and select **Internet Protocol (TCP/IP)** and click **Properties**.

4. Click **Advanced**.

4. Adding extra IP addresses is simple, just click **Add** under the **IP Addresses** box, and enter the IP address (196.15.60.x+40) and corresponding Subnet mask (255.255.255.0).

Create a virtual web server to be accessed using IP addresses:

1. Start the IIS console to create a New Site: right-click on the name of your server (in this case Netpc**X** where X is your computer number), and then select **New**, and then **Web Site**. Follow the **Web Site Creation Wizard.**

2. A second IP address is already assigned to the Web Server to identify the second web site to be hosted on your web server. All you need to do is select the second IP from the list and leave the port settings on 80.

3. You need to point IIS at the home directory of the second web site to be hosted. This is pretty self-explanatory and in this case is **D:\Inetpub\intranet** which is the sub-directory **intranet** located in the **Inetpub** directory with the D: drive on the web server (NetpcX).

4. Create the **intranet** folder, if it does not exist, under **Inetpub** and populate it with a web page that you create using HTML code.

5. To make sure your new site is operational, make sure you have a valid default.htm file in the home directory (D:\Inetpub\intranet) and enter the address, http://196.15.60.x+40, in the address box of the browser.

Create a virtual web server to be accessed using port numbers:

1. Start the IIS console to create a New Site: right-click on the name of your server (in this case Netpc**X** where X is your computer number), and then select **New**, and then **Web Site**. Follow the **Web Site Creation Wizard.**

2. All you have to work with is your IP address **196.15.60.x** (where x is your machine number). Unfortunately, this is already being used by another site (Default web site) so you are going to host this particular Web Service from Port 81 instead of 80. To view the site, users will have to enter **http://196.15.60.0.x:81** (the colon denotes the port number).

3. You need to point IIS at the home directory of the third web site to be hosted. This is pretty self-explanatory and in this case is **D:\Inetpub\extranet,** which is the sub-directory **extranet** located in the **Inetpub** directory with the D: drive on the web server (NetpcX).

4. Create the **extranet** folder, if it does not exist, under **Inetpub** and populate it with a web page that you create using HTML code.

b) To make sure your new site is operational, make sure you have a valid **default.htm** file in the home directory (D:\Inetpub\extranet) and enter the address, **196.15.60.x:81**, in the address box of the browser

Configuring and testing FTP Server using Windows 2003 server**:**

1. Start the IIS5 console, and then under the server name select the **Default FTP Site**.
2. Right-click on **Default FTP Site** and then on **Properties** and report the default TCP port and the defaultHome directory used by the default FTP service.
3. Open a command prompt and type:

D:\> Copy D:\Winnt*.bmp D:\Inetpub\ftproot

4. Create a temporary directory on your computer called **D:\ftptemp**

D:\> mkdir ftptemp.

5. Change to the **ftptemp** directory (D:\> **cd** ftptemp).
6. Start an **FTP** session with your computer by typing the following command (**debug mode**):D:\> ftp –d 127.0.0.1
7. Log on as **Anonymous** (**user:** anonymous).
8. When prompted for a password, press ENTER. An **ftp>** prompt will appear.
9. Type the following command at the **ftp>** prompt:

ftp> **dir**

A listing of all of the files available at the FTP site appears.

10. Use the **get** command to retrieve a single file. Type:

ftp> **get** zapotec.bmp

11. To view the transferred file on your computer, type the following:

ftp> **!dir**

and then press ENTER.

12. Use the **mget** command to retrieve the rest of the files. Type:

ftp> **mget ***

13. Can you download files when the FTP server is paused.
14. You can download files when the FTP server is stopped.
15. To exit the FTP session, type:

ftp> **bye**

and then press ENTER.

Use netstat to observe TCP port activity during an FTP session:

1. Open a command prompt.
2. Start an FTP session with the lab FTP server by typing the following command:

D:\> cd ftptemp

D:\ftptemp> **ftp 196.15.60.220**

3. Log on as **Anonymous**.
4. When prompted for a password, press ENTER. An **ftp>** prompt will appear.
5. Type the following command at the **ftp>** prompt:

!netstat

This will display the current TCP network connections.

6. Type the following command at the **ftp>** prompt:

!netstat –n

This will display the current TCP network connections and the current TCP port connections.

7. To exit the FTP session, type:

Bye

And then press ENTER.

11. Create a virtual FTP server to be accessed using IP addresses and populate it with some materials.
12. Create a virtual FTP server to be accessed using port numbers and populate it with some materials.
13. Let your lab instructor check your work (all your Web sites and your FTP sites)

Network Performance Study using the FTP tool:

1. Download the following files from the lab FTP server; record their size, and the download time.

2. Fill the table below.

3. Use the data to implement your lab report. Check the lab instructor web site for instruction concerning your lab report.

File Name	Size (bytes)	Download Time (sec)
File1.lab		
File2.lab		
File3.lab		
File4.lab		
File5.lab		
File6.lab		
File7.lab		
File8.lab		
File9.lab		
File10.lab		

Delete your work

1. Remove the second IP address you assigned to your machine.
2. Remove the Ftptemp folder with all its content (D:\ftptemp).
3. Remove the Internet Information Server with all services (IIS5).
4. Remove the folder Inetpub with all subfolders.

Conclusion

Checked By:

Name of Subject Teacher	Sign with Date