Department of Electronics Engineering

LAB MANUAL

Semester-VIII

Advanced Networking Technology Laboratory

Institute Vision, Mission & Quality Policy

Vision

To foster and permeate higher and quality education with value added engineering, technology programs, providing all facilities in terms of technology and platforms for all round development with societal awareness and nurture the youth with international competencies and exemplary level of employability even under highly competitive environment so that they are innovative adaptable and capable of handling problems faced by our country and world at large.

Mission

The Institution is committed to mobilize the resources and equip itself with men and materials of excellence thereby ensuring that the Institution becomes pivotal center of service to Industry, academia, and society with the latest technology. RAIT engages different platforms such as technology enhancing Student Technical Societies, Cultural platforms, Sports excellence centers, Entrepreneurial Development Center and Societal Interaction Cell. To develop the college to become an autonomous Institution & deemed university at the earliest with facilities for advanced research and development programs on par with international standards. To invite international and reputed national Institutions and Universities to collaborate with our institution on the issues of common interest of teaching and learning sophistication.

Quality Policy

ज्ञानधीनं जगत् सर्वम।

Knowledge is supreme.

Our Quality Policy

It is our earnest endeavour to produce high quality engineering professionals who are innovative and inspiring, thought and action leaders, competent to solve problems faced by society, nation and world at large by striving towards very high standards in learning, teaching and training methodologies.

Our Motto: If it is not of quality, it is NOT RAIT!

Dr. Vijay D. Patil
President, RAES

Department Vision & Mission

Vision

The department envisions that the students of the branch become engineers of professional character equipped with a strong theoretical and experimental foundation required for critical thinking, practical engineering skills to face the recent research and industrial challenges in the field, the ability to work in a team dignity, and all the qualities that help them accomplish their goals with a zeal for social awareness.

Mission

- Our mission is to facilitate the development of well rounded, educated, productive, society–focused, creative, adaptive, motivated and ethical individuals who are well versed in technology and in social and environmental issues.
- To create an academic environment of high quality through an outcome based interactive learning teaching model.
- Provide outstanding education & research training to students to enable them to have productive careers in industry and academia.
- To inculcate leadership and entrepreneurship qualities in the students and to make them ready for the challenges of competitive professional life.
- To foster and encourage collaborative research activities and to develop the excitement of research with intellectual stimulation of diverse campus community and with other various leading industries and research institutions.

Index

List of Experiments

Sr. No.	Name of the Experiments
1	To study the features of Wireless LANs and implement
2	To simulate WIRELESS NETWORK using CISCO PACKET TRACER
3	To study and implement Bluetooth network
4	To study Remote Login Service: SSH
5	Study of **nmap** as a security audit / hacking tool
6	To Configure Firewalls using ufw and IPtables
7	To determine the network statistics using **ntop**
8	To study and implement graphical network monitor : **etherape**
9	To study System utilities for network management
10	To install and configure an SNMP Daemon/ Client and use basic SNMP commands

Experiment Plan & Course Outcomes

Course Outcomes:

CO1	Students will be able to understand the concept of Wireless network technologies and simulate or implement WLANs
CO2	Students will be able to understand the various emerging wireless technologies such as Bluetooth , ZigBee , RFID
CO3	Students will be able to analyze and determine the security of Networks using “nmap” & " ufw or iptables
CO4	Students will able to determine the performance using Network Monitoring tools such as "etherape"
CO5	Students will be able to understand network management protocol ,SNMP

Module No.	Week No.	Experiments Name	Course Outcome
1	W1	To study the features of Wireless LANs and implement	CO1
2	W2	To simulate WIRELESS NETWORK using CISCO PACKET TRACER	CO1
3	W3	To study and implement Bluetooth network	CO2
4	W4	To study Remote Login Service: SSH	CO2
5	W5	Study of ***nmap*** as a security audit / hacking tool	CO3
6	W6	To Configure Firewalls using ufw and IPtables	CO3
7	W7	To determine the network statistics using ***ntop***	CO4
8	W8	To study and implement graphical network monitor : ***etherape***	CO4
9	W9	To study System utilities for network management	CO5
10	W10	To install and configure an SNMP Daemon/ Client and use basic SNMP commands	CO5

Study and Evaluation Scheme

Course Code	Course Name	Teaching Scheme			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Practical	Tutorial	Total
EXL 802	Advanced Networking Technologies laboratory		02	--	--	01	--	01

Course Code	Course Name	Examination Scheme		
		Term Work	Oral	Total
EXL 802	Advanced Networking Technologies laboratory	25	25	50

Term Work:

1. Term work assessment must be based on the overall performance of the student with every experiment graded from time to time. The grades should be converted into marks as per the Credit and Grading System manual and should be added and averaged.
2. The final certification and acceptance of term work ensures satisfactory performance of laboratory work and minimum passing marks in term work.

Oral:

1. Oral exam will be based on the entire syllabus.

Advanced Networking Technologies

Experiment No: 1

To Study the features of Wireless LANs

Experiment No. 1

1. **Aim :** To study and Implement Wireless LAN using ESP8266 Wi-Fi Module

2. **What you will learn by performing this experiment?**

   - To understand the features of Wireless LANs.
   - To understand the advantages, disadvantages and applications of Wireless networks.
   - How to implement WLAN using ESP 8266 Wi-Fi Module.

3. **Apparatus Required:**

   Flash Magic Software, ESP8266 Wi-Fi Module, RS-232-USB converter

4. **Theory:**

Wireless Networks: A Wireless Local Area Network (WLAN) implements a flexible data communication system frequently augmenting rather than replacing a wired LAN within a building or campus. WLANs use radio frequency to transmit and receive data over the air, minimizing the need for wired connections.

The IEEE 802.11 group of standards specify the technologies for wireless LANs. 802.11 standards use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing and include an encryption method, the Wired Equivalent Privacy algorithm.

Fig.1: Access Point

A communications network that provides connectivity to wireless devices within a limited geographic area. "Wi-Fi" is the universal standard for wireless networks and is the wireless equivalent of wired Ethernet networks. In the office, Wi-Fi networks are adjuncts to the wired networks. At home, a Wi-Fi network can serve as the only network since all laptops and many printers come with Wi-Fi built in, and Wi-Fi can be added to desktop computers via USB.

Wi-Fi is achieved with a wireless base station, called an "access point." Its antennas transmit and receive a radio frequency within a range of 30 to 150 feet through walls and other non-metal barriers.

Implementing a WLAN

Implementing a WLAN involves more than selecting the desired standard and selecting a security mechanism. Access point placement can have more effect on throughput than standards. You need to understand how the efficiency of a WLAN is affected by such issues as topology, distance, and access point location.

Upon completing this lesson, you will be able to describe the factors affecting the implementation of a WLAN.

802.11 Topology Building Blocks

The following list describes these different building blocks.

- **Ad hoc mode**: Independent Basic Service Set (IBSS) is the ad hoc topology mode. Mobile clients connect directly without an intermediate access point. Operating systems such as Windows have made this peer-to-peer network easy to set up. This setup can be used for a small office (or home office) to allow a laptop to be connected to the main PC or for several people to simply share files. The coverage is limited. Everyone must be able to hear everyone else. An access point is not required. A drawback of peer-to-peer networks is that they are difficult to secure.

- **Infrastructure mode**: In infrastructure mode, clients connect through an access point. There are two infrastructure modes:

- **Basic Service Set (BSS):** The communication devices that create a BSS are mobile clients using a single access point to connect to each other or to wired network resources. The Basic Service Set Identifier (BSSID) is the Layer 2 MAC address of

the BSS access point's radio card. While the BSS is the single building block for wireless topology and the BSS access point is uniquely identified through a BSSID, the wireless network itself is advertised through a SSID, which announces the availability of the wireless network to mobile clients. The SSID is a wireless network name that is user configurable and can be made up of as many as 32 case-sensitive characters.

- **Extended Services Set (ESS):** The wireless topology is extended with two or more BSSs connected by a distribution system (DS) or a wired infrastructure. An ESS generally includes a common SSID to allow roaming from access point to access point without requiring client configuration.

ESP8266 Wi-Fi Module

The ESP8266 WiFi Module is a self-contained SOC with integrated TCP/IP protocol stack that can give any microcontroller access to your WiFi network. The ESP8266 is capable of either hosting an application or offloading all Wi-Fi networking functions from another application processor.

Each ESP8266 module comes pre-programmed with an AT command set firmware, meaning, you can simply hook this up to a Arduino device and get about as much WiFi-ability as a WiFi Shield offers .

The ESP8266 module is an extremely cost effective board with a huge, and ever growing, community. ESP8266 WiFi Module has increased the flash disk size from 512k to 1MB.

Specifications of ESP8266:

- 802.11 b/g/n
- Wi-Fi Direct (P2P), soft-AP
- Integrated TCP/IP protocol stack
- Integrated TR switch, balun, LNA, power amplifier and matching network
- Integrated PLLs, regulators, DCXO and power management units
- +19.5dBm output power in 802.11b mode
- Power down leakage current of <10uA
- 1MB Flash Memory
- Integrated low power 32-bit CPU could be used as application processor
- SDIO 1.1 / 2.0, SPI, UART
- STBC, 1×1 MIMO, 2×1 MIMO
- A-MPDU & A-MSDU aggregation & 0.4ms guard interval
- Wake up and transmit packets in < 2ms

5. Implementation Procedure:

1. Set the baud rate to 9600 for serial communication.
2. Send the AT command to check if module is responding. The module will send Ok response to AT command.
3. Get all access points available near ESP module.
4. Set the module for multiple connection by AT+CIPMUX=1.
5. Start Connection with HTTP port by AT+CIPSERVER=1, 80.
6. Get the station address and paste it in new line. In response to this we will get the input packet from station with channel no.
7. To send data, we use the command, AT+CIPSEND=0, 30 and then we type the line to be sent to chosen station.
8. Close the connection by command AT+CIPCLOSE=0 and AT+RST.

7. Results:

8. Conclusions:

9. QUIZ / Viva Questions:

- What is the difference between wireless networks and wired networks?
- Which are the modulation schemes defined in PHY layer of 802.11?
- What is CSMA/CA? Explain briefly.
- What is DHCP? Explain.
- Which are the MAC Layer Protocols as defined by 802.11?

10. References:

1. Vijay Garg , "*Wireless Communication and Networking"* ,
2. William Stallings , ""*Wireless Communication and Networking"*, Mcgrew Hill Publications ,2ed Ed
3. Behroz Furozan , "Data Communication and Networking", 4th Ed, Mcgrew Hill Publications

Advanced Networking Technologies

Experiment No: 2

To Study and Simulate Wireless Network using CISCO PACKET TRACER

Experiment No. 2

1. **Aim:** To Study and simulate wireless network using CISCO PACKET TRACER

2. **What you will learn by performing this experiment?**

   - To understand the features of Wireless Networks.
   - To understand the advantages, disadvantages and applications of Wireless networks.
   - How to simulate the wireless network using CISCO PACKET TRACER.

3. **Software Required:** CISCO PACKET TRACER

4. **Theory:**

Cisco Packet Tracer is a powerful network simulator that can be utilized to create networks with an almost unlimited number of devices and to experience troubleshooting without having to buy real Cisco TM routers or switches.
Packet Tracer is a cross-platform visual simulation program designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit.
Cisco Packet Tracer features an array of simulated Application layer protocols (HTTP, DNS,) as well as basic routing with RIP, OSPF, and EIGRP.

Key Features:
Packet Tracer Workspaces: Cisco Packet Tracer has two workspaces—logical and physical.

The logical workspace allows users to build logical network topologies by placing, connecting, and clustering virtual network devices.

The physical workspace provides a graphical physical dimension of the logical network, giving a sense of scale and placement in how network devices such as routers, switches, and hosts would look in a real environment. The physical view also provides geographic representations of networks, including multiple cities, buildings, and wiring closets.

5. Simulation Procedure:

Steps required to create a simple network in Cisco Packet Tracer:

1. Open Packet Tracer
2. Go to Start. Type "Cisco Packet Tracer" and click the application to open it.
3. Physical Setup: To make a network, we first need a source such as a network hub. For this example, we will use a router.

- Go ahead and click the Router section and choose the 1841 Router.
- Move your mouse to the white space, and click to place the router on the workspace.
- Click End Devices and click Generic PC.
- Move your mouse to the white space, and click once to place the PC on the workspace.
- Repeat, and add a second Generic PC.
- Now we are going to connect them together. Click Connections.
- Choose the Copper Cross-Over cable.
- Click on PC-0 and select FastEthernet.
- Click on the other side to Router and select the FastEthernet0/0.
- Repeat and connect PC-1 to the FastEthernet interface.
- Connect PC-1 to the Router and select FastEthernet0/1.

Router Configuration

- Click Router0. A window will come up. Go to the CLI tab.
- Type no when asked to continue with configuration dialog.
- Type enable to go to "privileged execution mode"
- Type config t, to enter "global configuration mode".
- Type hostname Router0, to name the router.
- Type enable secret class, to password protects the "privileged execution mode".
- We are going to configure the password for the console line Type line con 0. Then type password cisco, to set the password as cisco.
- Type login to enable password prompting.
- Type exit to return to "global configuration mode".
- We are going to configure the password for the "virtual terminal lines".
- Type in line vty 0 4. Type in password cisco.
- We are going to enable the password requirement. Type in "login"

- Type exit to return to "global configuration mode".
- Earlier, we connected the computers to the router using the FastEthernet interface. .We are going to set up the router to work with those interfaces. Type in interface FastEthernet0/0.
- Type in ip address 192.168.1.1 255.255.255.0 (This will set the IP address and Subnet mask of the first Fast Ethernet Interface)
- We are going to set a description on the router for later reference. To do this, we will type in description Router0 FastEthernet0/0
- To start the interface, we are going to type "no shutdown"
- Type exit to return to "global configuration mode".

We are going to repeat this process with FastEthernet0/1.

- Type in "interface FastEthernet0/1"
- This time, type ip address 192.168.2.1 255.255.255.0
- Type in "description Router0 FastEthernet0/1"
- To start the interface, we are going to type no shutdown
- Type exit to exit from "interface configuration mode".
- Type exit to return to "global configuration mode". Hit the Enter key, and we will be back at the "privileged execution mode" when we first started the command line. We are now going to check the information that we entered into the system.
- To do this, type "show running-config''Continuously hit Enter to scroll down the list. You will see all the configurations, you just set.
- We want the router to run these configurations when it starts up. To do this, we need to copy the configuration files into the Router's NV RAM. To do this, we type in "copy running-config startup-config" Hit Enter to confirm. The router configuration is now complete.

PC configuration

We are now going to configure the computers to connect to the network.

1. First, click on PC-0. A configuration window will come up.
2. Go to the Desktop tab and click IP Configuration.
3. We will set a Static IP.
4. Set the IP Address to 192.168.1.2
5. Set the Subnet Mask to 255.255.255.0
6. Set the Default Gateway to 192.168.1.1
7. Close the PC-0 configuration window.

8. Repeat with PC-1, except use 192.168.2.2 for the IP Address.
9. Set the Subnet Mask to 255.255.255.0
10. Set the Default Gateway to 192.168.2.1
11. Close the PC-1 configuration window

By now, you should see green dots on the cables connected to the devices.

Testing Connectivity

We are going to test for a valid connection by pinging PC-1 from PC-0.

1. To do this, click PC-0. Go to the Desktop tab and click Command Prompt.
2. To see the details of the computer's local network, we can type in ipconfig.
3. We are going to ping PC-1 by typing in "ping 192.168.2.2 "
   At first, the request might time-out, but you should get a reply after that.

Testing for Connectivity using Simulation Mode:

1. At the bottom right corner, click the "stopwatch" icon to activate Simulation Mode.
2. Click Edit Filters. Clear the selections. Select only ICMP.
3. Click anywhere to get out.
4. Look at the bar of items on the right hand side. Click the Closed Envelope + button. This will allow us to choose a source to test our network.
5. Click PC-0 and then click PC-1.
6. Click Auto Capture/Play to begin simulation. You should now see an envelope going from PC-0 to the Router to PC-1 and back. After that, you have successfully completed your network setup

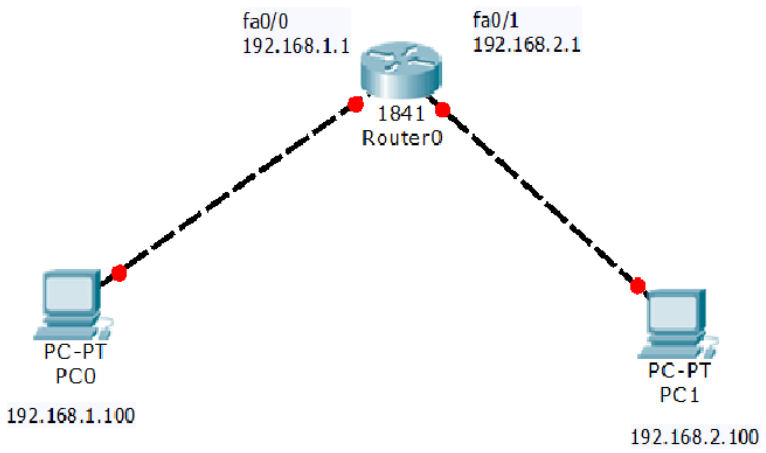


Fig.1: Routing

6. Simulation Results:

7. Conclusions:

8. QUIZ / Viva Questions:

- Bring out the advantages of using CISCO PACKET TRACER simulator.
- Which are the different interconnecting devices in a network?
- What is the role of a router as compared with the switch?
- Which are the Router configuration commands to be implemented ?
- Bring out the difference between wired and wireless networks.

9. References:

1. Vijay Garg, "*Wireless Communication and Networking".*
2. William Stallings , "*Wireless Communication and Networking"*, McGraw Hill Publications ,2ed Ed
3. Behroz Furozan , "Data Communication and Networking", 4th Ed, Mcgrew Hill Publications
4. www.**cisco**.com/web/learning/netacad/course_catalog/**PacketTracer**.html
5. https://www.youtube.com/watch?v=q-UUbPk6fYo

Advanced Networking Technologies

Experiment No: 3

To Study and Implement Bluetooth Network

Experiment No. 3

1. **Aim:** To study and implement Bluetooth network

2. **What you will learn by performing this experiment?**

   - Get familiar with Piconet and Scatternet formation.
   - Understand the functioning of Bluetooth networks.
   - Understand about Bluetooth networks and how it is differentiate from WiFi networks.

3. **Theory:**

Bluetooth Network

The name Bluetooth was named after 10th century Viking king in Denmark Harald Bluetooth who united and controlled Denmark and Norway. Bluetooth is a low power, low cost, and short range radio network standard. It supports unlicensed Industrial, Scientific and Medical (ISM) 2.4 GHz short-range radio frequency band. It is complementary to the Wi-Fi network specified by IEEE 802.11b/g/a standard. Bluetooth uses a frequency hopping scheme to provide robust wireless communication. As a cable replacement, Bluetooth is widely used in cell phone, PDA, laptop, headset, and printer, etc. to form a Personal Area Network (PAN) and provide universal access. Bluetooth uses a radio technology called frequency-hopping spread spectrum

- Bluetooth wireless technology was accepted by engineers at Swedish telecommunications manufacturer Telefonaktiebolaget LM Ericsson
- In 1994 Ericsson had started a project to study the feasibility of a low-cost and low-power radio interface to replace cables between mobile accessories and mobile phones
- In 1998, Bluetooth technology was starting to take shape and led to the development of the Bluetooth Special Interest Group (SIG); with the founding members being:IBM, Intel, Nokia, Toshiba and Ericsson.
- **Bluetooth – Power Classes**

Class	Maximum Permitted Power	Operating Range
Class 1	100mW (20dBm)	100 meters
Class 2	2.5mW (4dBm)	10 meters
Class 3	1mW (0dBm)	1 meter

- In this case, if you wish to communicate over the 100m range, you will need a class 1 Bluetooth device at both ends. But if you wish to communicate over the 10m range, you can have a class 1 or class 2 device at both ends.

Bluetooth - Versions

Many Bluetooth specification versions have been released since Bluetooth technology was finally introduced in 1998. **Versions 1.0** and 1.0B had too many problems and restraints for manufacturers to successfully develop Bluetooth devices. The main issue was the lack of interoperability among devices.

- **Bluetooth 1.1**: The Bluetooth Core Specification version 1.1 is the most successful operating version of Bluetooth technology. Bluetooth 1.1 corrected many of the problems found in the earlier versions. As a result, the devices using Bluetooth 1.1 have much more interoperability.
- **Bluetooth 1.2**: Many new Bluetooth devices, like the latest cell phones, are being sold with the newer Bluetooth specification version 1.2. It has backward compatible with Bluetooth 1.1, adaptive Frequency Hopping - helps reduce radio interference by eliminating the use of crowded frequencies in the hopping sequence, faster transmission speeds (1 Mbps) etc.
- **Bluetooth 2.0**: Version 2.0 + EDR (Enhanced Data Rate) was announced by the Bluetooth SIG in June 2004 and began appearing in Bluetooth devices in late 2005. It delivers data transfer rates up to three times faster than the original Bluetooth specification.
- **Bluetooth 2.1**: Bluetooth Core Specification Version 2.1 is fully backward compatible with 1.2, and was adopted by the Bluetooth SIG on July 26, 2007. It supports theoretical data transfer speeds of up to 3 Mb/s. This specification includes two features, such as, Extended inquiry response (EIR) and Sniff subrating
- **Bluetooth 3.0:** The 3.0 specification was adopted by the Bluetooth SIG on April 21, 2009. It supports theoretical data transfer speeds of up to 24 Mb/s. Its main new feature is AMP (Alternate MAC/PHY), the addition of 802.11 as a high speed transport.

How does Bluetooth work?

- Bluetooth is a standard for tiny, radio frequency chips that can be plugged into your devices
- These chips were designed to take all of the information that your wires normally send, and transmit it at a special frequency to something called a receiver Bluetooth chip
- Bluetooth chip is designed to replace cables. Information normally carried by the cable, is transmitted at a special frequency to a receiver Bluetooth chip

- These devices can form a quick ad-hoc secure "piconet" and start communication
- A piconet starts with two connected devices, and may grow to eight connected devices
- All Bluetooth devices are peer units and have identical implementations. However, when establishing a piconet, one unit will act as a Master and the other(s) as slave(s) for the duration of the piconet connection

Networking of Bluetooth

Bluetooth technology provides both **point-to-point** and **point-to-multipoint** connection. In point-to-multipoint connections, the channel is shared among several Bluetooth units. In point-to-point connections, only two units share the connection. Bluetooth protocols assume that a small number of units will participate in communications at any given time. These small groups are called **piconets** , and they consist of one master unit and up to seven active slave units. The master is the unit that initiates transmissions, and the slaves are responding units. This type of Bluetooth network can have only one master unit. If several piconets overlap a physical area, and members of the various piconets communicate with each other, this new, larger network is known as a **scatternet** . Any unit in one piconet can communicate in a second piconet as long as it serves as master for only one piconet at a time.

The following figure illustrated the Bluetooth Scatternet scenario with slave/slave node.

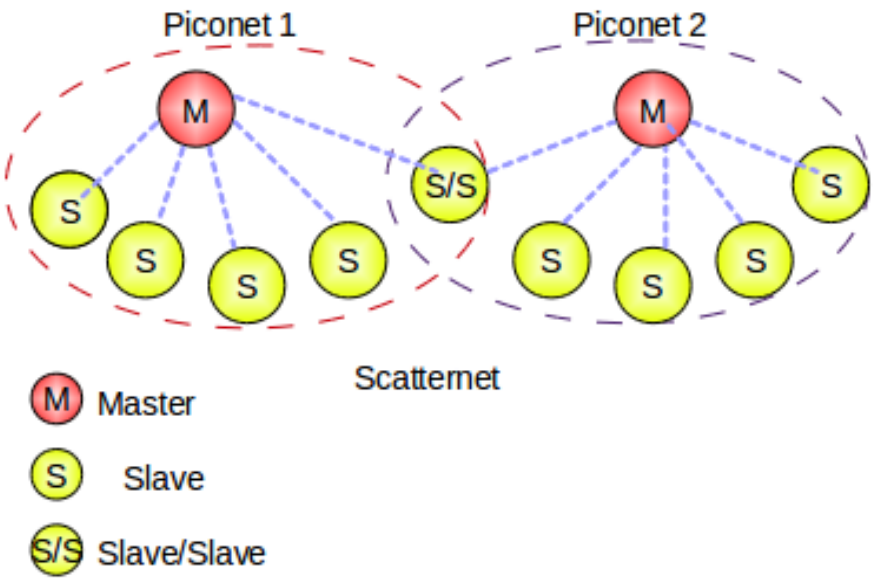


Fig.1: Illustration of Bluetooth Piconets & Scatternet with Slave/Slave node

When the no. of piconet connect with each other with the slave nodes, then the slave nodes, which are connected with both the Master nodes of Piconets are known as **Slave/Slave** nodes. But when the no. of piconets are connected with each other with another master nodes, then the master nodes, which are Slave to one Piconet and Master for other Piconets are known as **Master/Slave** nodes.The following figure-02 illustrated the Bluetooth Scatternet with master/slave scenario.

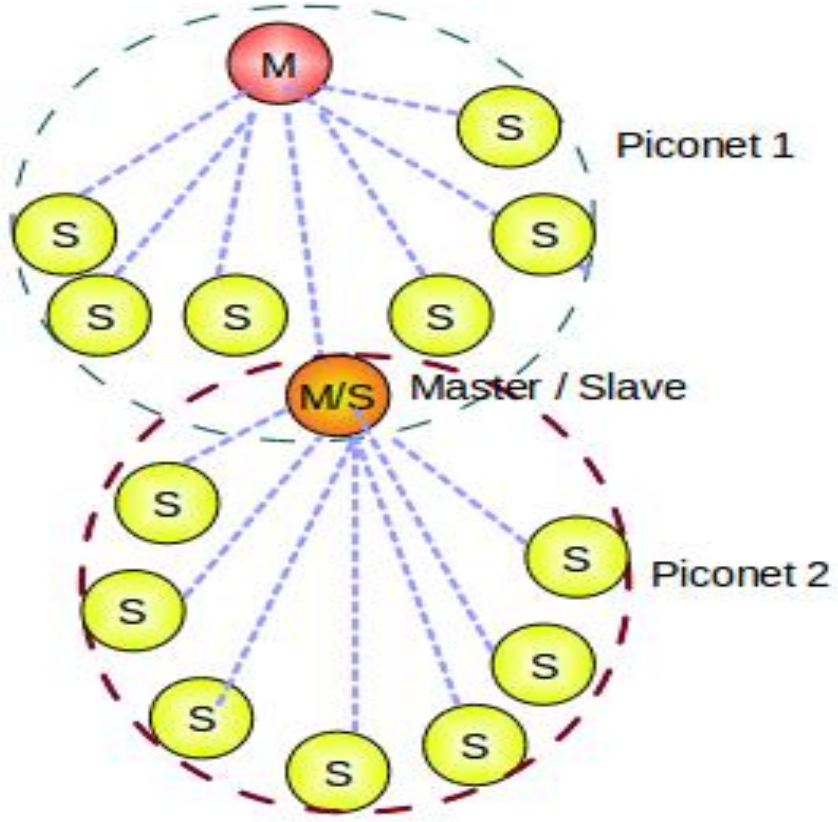


Fig.2: Illustration of Bluetooth Scatternet with Master/Slave node

How to connect Bluetooth?

Bluetooth enables ad hoc networking. Rather than depending on a broadband system, which relies on terminals and base stations for maintaining connections to the network via radio links, Bluetooth implements peer-to-peer connectivity. No base stations or terminals are involved. Using peer-to-peer connectivity, Bluetooth technology simplifies personal area wireless connections, enabling all digital devices to communicate spontaneously.

Bluetooth technology also provides fast, secure voice and data transmissions. The range for connectivity is up to 10 meters, and line of sight is not required.

The Bluetooth radio unit:

- Functions even in noisy radio environments, ensuring audible voice transmissions in severe conditions
- Protects data by using error-correction methods
- Provides a high transmission rate
- Encrypts and authenticates for privacy

4. Comparison: Bluetooth v/s Wi-Fi

Bluetooth and Wi-Fi technologies have some similarities because both are wireless technologies and used to communicate with other devices.

Parameters	Bluetooth	WiFi
Year of development	1994	1991
IEEE Standard	802.15	802.11
Power Consumption	Low	High
Cost	Low	High
Bandwidth	Low (800 Kbps)	High (11 Mbps)
Range	10 meters	100 meters
Frequency	2.4 GHz	2.4 GHz
Network	Personal Area Network (PAN)	Wireless Local Area Networks (WLAN)
Hardware requirement	Bluetooth adaptor on all the devices connecting with each other	Wireless adaptors on all the devices of the network, a wireless router and/or wireless access points
Specifications authority	Bluetooth SIG	IEEE, WECA
Primary Devices	Mobile phones, mouse, keyboards, office and industrial automation devices	Notebook computers, desktop computers, servers

Ease of Use	Fairly simple to use. Can be used to connect up to seven devices at a time. It is easy to switch between devices or find and connect to any device.	It is more complex and requires configuration of hardware and software.

5. Conclusions:

6. QUIZ / Viva Questions:

- What is meant by Scatternet?
- Which are the versions of BLUETOOTH?
- Which are the Power classes of Bluetooth?
- Compare Bluetooth with WI-FI.
- What are the functions of Bluetooth Radio unit?
- Explain Bluetooth Protocol stack.

7. References:

1. Vijay Garg , "*Wireless Communication and Networking"* ,
2. William Stallings , ""*Wireless Communication and Networking"*, Mcgrew Hill Publications ,2ed Ed
3. Behroz Furozan , "Data Communication and Networking", 4th Ed, Mcgrew Hill Publications
4. https://www.**bluetooth**.com/
5. www.rfwireless-world.com/Tutorials/**Bluetooth-protocol-stack**.html

Advanced Networking Technologies

Experiment No: 4

To study Remote Login Service: SSH

Experiment No. 4

1. **Aim:** To study Remote Login Service: SSH

2. **What you will learn by performing this experiment?**

   - To understand the concept of remote Login
   - To understand the SSH service of Linux
   - How to configure and use the Client- Server commands in SSH.

3. **Apparatus Required:**
   2 work stations installed with "open-ssh server" Package in Linux (Ubuntu) and one workstation, with Windows installed with Admin privileges.

4. **Theory:**

SSH is an acronym for secure shell, designed and created to produce the best security when accessing another computer remotely. Not only does it encrypt the session, it also provides better authentication facilities as well , like X Session.

Forwarding port security of other protocols shows how a **telnet session** can be viewed by anyone on the network by using a sniffing program like: **ethereal or** "**sniff it".** It is rather critical to do this ,since anyone on the network can steal the confidential information , like passwords etc.

SSH shows how an encrypted connection like SSH, is not viewable on the network. The Server still, can read the information, but only after negotiation with the Client.

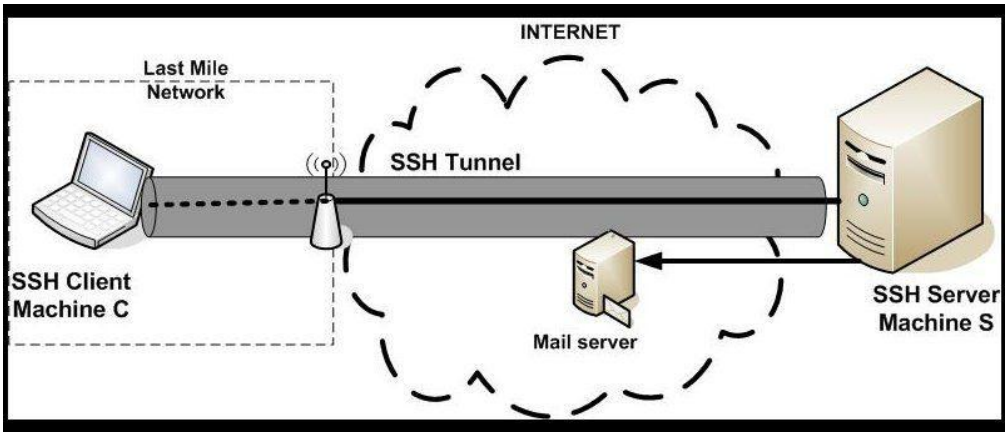


Fig.1: SSH

OpenSSH :

Ubuntu provides a powerful collection of tools for the remote control of, and transfer of data between, networked computers called OpenSSH.

OpenSSH is a freely available version of the Secure Shell (SSH) protocol family of tools for remotely controlling, or transferring files between, computers. Traditional tools used to accomplish these functions, such as telnet or rcp, are insecure and transmit the user's password in cleartext when used.

OpenSSH provides a server daemon and client tools to facilitate secure, encrypted remote control and file transfer operations, effectively replacing the legacy tools.

The OpenSSH server component, *sshd*, listens continuously for client connections from any of the client tools. When a connection request occurs, sshd sets up the correct connection depending on the type of client tool connecting.
For example, if the remote computer is connecting with the ssh client application, the OpenSSH server sets up a remote control session after authentication. If a remote user connects to an OpenSSH server with scp, the OpenSSH server daemon initiates a secure copy of files between the server and client after authentication.

OpenSSH can use many authentication methods, including plain password, public key, and Kerberos tickets.

Installation

Installation of the OpenSSH client and server applications is simple. To install the OpenSSH client applications on your Ubuntu system, use this command at a terminal prompt:

sudo apt-get install openssh-client

To install the OpenSSH server application, and related support files, use this command at a terminal prompt:

sudo apt-get install openssh-server

The openSSH-server package can also be selected to install during the Server Edition installation process.

Configuration

You may configure the default behavior of the OpenSSH server application, sshd, by editing the file /etc/ssh/sshd_config.

Prior to editing the configuration file, you should make a copy of the original file and protect it from writing so you will have the original settings as a reference and to reuse as necessary.

Copy the /etc/ssh/sshd_config file and protect it from writing with the following commands, issued at a terminal prompt:

sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.original
sudo chmod a-w /etc/ssh/sshd_config.original

The following are examples of configuration directives you may change:

- To set your OpenSSH to listen on TCP port 2222 instead of the default TCP port 22, change the Port directive as such:
  Port 2222
- To have sshd allow public key-based login credentials, simply add or modify the line:
  PubkeyAuthentication yes

  If the line is already present, then ensure it is not commented out.

SSH Keys

- SSH keys allow authentication between two hosts without the need of a password. SSH key authentication uses two keys, a private key and a public key.
- To generate the keys, from a terminal prompt enter:

  ssh -keygen -t rsa

  This will generate the keys using the RSA Algorithm. During the process you will be prompted for a password. Simply hit Enter when prompted to create the key.

- By default the public key is **saved in the file ~/.ssh/id_rsa.pub,**

  while ~/.ssh/id_rsa is the private key.

- Now copy the id_rsa.pub file to the remote host and append it to ~/.ssh/authorized_keys by entering:

  ssh-copy-id username@remotehost

- Finally, double check the permissions on the authorized_keys file, only the authenticated user should have read and write permissions. If the permissions are not correct change them by:

  chmod 600 .ssh/authorized_keys

  You should now be able to SSH to the host without being prompted for a Password.

5. Procedure:

To connect to a Remote machine:

To make SSH useful, we need a shell account on the remote machine.

1. Get the IP address of both the work stations (use ifconfig command)
2. Configure one as Server and the other as Client.
3. Create a user "user1" and give the privileges as admin.
4. Install OpenSSH client and server applications

   sudo apt-get update

   sudo apt-get install openssh-server

   To install SSH client on the client machine, run the following command:

   sudo apt-get install openssh-client

5. Configure SSH for Password-less login.
6. Generate SSH keys (public and private) for authentication.

   - On your client machine, generate SSH keys with the following command**:**

     cd ~/.ssh

     ssh-keygen -t rsa

     Simply press the Enter key at every prompt.

   - This produces two files: id_rsa.pub (public key) and id_rsa (private key).

     This will output something that looks like the following:

     ssh-keygen

- On your server, create the following folder (if it doesn't exist):

  mkdir -p ~/.ssh/

- Back to your client machine, copy the "id_rsa.pub" file to your server using the following command:

  scp -P "yourport" ~/.ssh/id_rsa.pub username@serverip:~/.ssh

- **change "your port" = port no. of server (22)**

  serverip = server IP address

- On your server machine, change the filename and setup permissions.

  cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
  chmod 700 .ssh
  chmod 600 .ssh/authorized_keys
  rm .ssh/id_rsa.pub

- To test if the key-based authentication method works, try connecting to your SSH server from the client machine:

  ssh -P "yourport" username@serverip

If you are able to connect without entering a password, then the key-based authentication method works. once authenticated , server can login to remote client machine.

- Create user1 and user 2 using the commands
  $ sudo adduser user1

7. To edit SSH Configuration file

The "/etc/ssh/sshd_config" file is the system-wide configuration file for SSH which allows you to set different options to improve the security of an SSH server.

- To edit the "/etc/ssh/sshd_config" file, run

  sudo nano /etc/ssh/sshd_config

- By default, SSH listens on port 22. To change the default port to 2200

  secure-ssh-change-port-number

- **Use protocol 2 version on Ubuntu**

- To allow "user1" and "user2," add the following line:
  AllowUsers user1 user2

- To deny "baduser1" and "baduser2," add the following line:
  DenyUsers baduser1 baduser2
- To disable root login, change the line
  PermitRoot Login without-password
  to
  PermitRootLogin no

- **secure-ssh-permit-root**

- To Disable password authentication **,** change the line

  # PasswordAuthentication yes
  to
  PasswordAuthentication no
  # secure-ssh-password-authentication

After making changes to the /etc/ssh/sshd_config file, save the file, and restart the sshd server application to effect the changes using the following command at a terminal prompt:

sudo service ssh restart

Follow the steps:

- Login to "user1 " account in SERVER machine (with the IP address :192.168.2.134 and named as "Master" in the /etc/hosts file)

- Connect remotely with the Client Machine with the IP address :192.168.2.132 client by typing the following:

  $ ssh client # connected to client machine
  $ ls # run the ls command
  --- directory listing of all files in client machine will be displayed.

6. Conclusions:

7. QUIZ / Viva Questions:

- What is meant by remote login?
- Which are the applications of "SSH"?
- How do you transfer the file?
- How do you configure for ssh?

8. References:

1. https://support.suso.com/supki/SSH_Tutorial_for_Linux
2. https://en.wikipedia.org/wiki/Secure_Shell

Advanced Networking Technologies

Experiment No: 5

To Study nmap as a security audit / hacking tool

Experiment No. 5

1. **Aim:** To Study *nmap* as a security audit / hacking tool

2. **What you will learn by performing this experiment?**

   - To study Network Audit tool.
   - To understand the usefulness of nmap tool.
   - To understand the usefulness of Zenmap tool.

3. **System Requirements:**

   - 3 workstations installed with Unix/Linux Fedora Core/Ubuntu and Windows XP.
   - Nmap latest version.
   - NmapFE latest version.
   - Zenmap latest version.

4. **Theory:**

Network administrators have many tasks, and auditing the network is at the top of the heap. This isn't a problem if you have a small network. But what happens when that network outgrows your ability to simply walk around and manually make note of what is up/down, what OS a device is running, or what ports are open? When this happens you need to make use of one of the de facto standard open source network auditing tools - Zenmap.

The Zenmap tool is actually a graphical front end for the very popular Nmap command line tool. Nmap is an open source tool for network security and auditing. Although Nmap is incredibly powerful, when working with larger networks most administrators do not want to work with command line only tools. And besides, as they say "A picture is worth a thousand words".

In this case that is very much true because Zenmap will give you an interactive graphical map of your network.

5. **Procedure:**

1. Installation

Installation of Zenmap is simple (you will need to also have Nmap installed).

- Go to command line interface (CLI)- Ctl+Alt+ T and use these commands

  student@localhost$ sudo apt-get update
  student@localhost$ sudo apt-get install nmap
  student@localhost$ sudo apt-get install zenmap
  student@localhost$ sudo zenmap

.

  Once installed you will find the tool in **Applications > Network**.

- launch Zenmap from the command line
  student@localhost$ sudo zenmap
  When the graphical window opens you are ready to start your audit.

2. Usage:

When the Zenmap window opens (see Figure 1) you will see a fairly straight-Forward user interface.

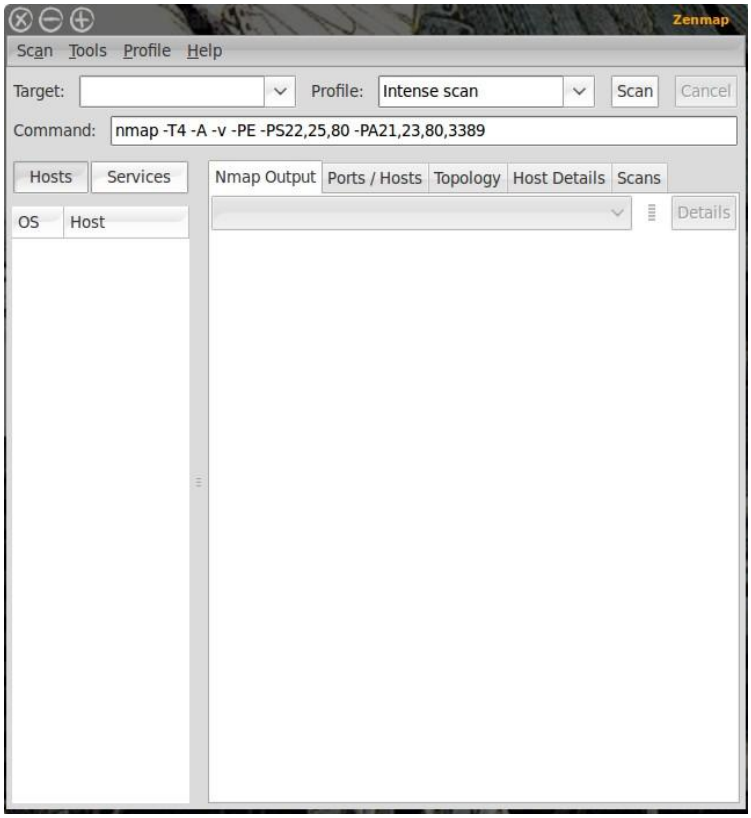


Fig.1: Interface

3. Steps to start an audit of your network:

- **Select the Target.**
  Let's say, for example, you want to audit a network that is on the 172.16.20.10 IP address scheme. If you want to scan your entire network you can enter172.16.20.* in the Target section.
  That will scan every possible address on that network.

- **Select a profile**.
  The Profile drop down is filled with pre-configured scan types that range from simple ping scans to intense scans.
  When you select the profile you want you will notice the Command section changes to reflect your choices. You could also enter this same command at a bash prompt and get results.

- **Click the Scan button** and the scan will begin.
  What happens then is all discovered addresses will begin filling up the left pane and the output of the scan will fill up the right pane.

Note: Let the scan complete before you click on a different tab.

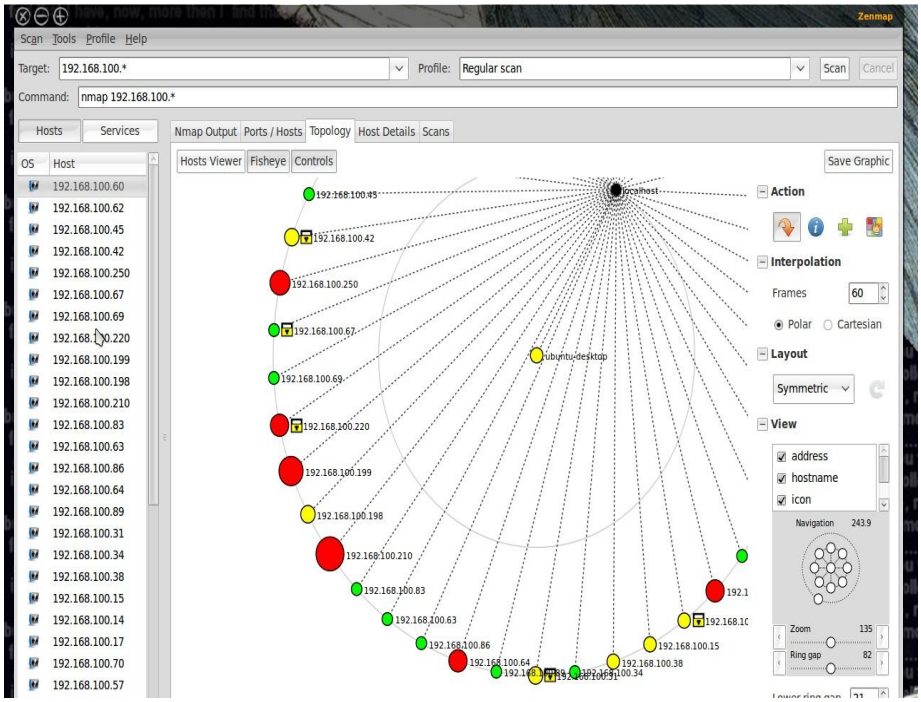


Fig.2: Topology

You will also notice there are other tabs in the right pane (Fig. 1). Each of these tabs serves a very distinct purpose:

Nmap Output: This is the default tab and shows the output of the command.

Ports/Hosts: This tab shows you what ports are open on what hosts.

Topology: This tab is a must-use for audits as it shows the actual topology of your network.
As you can see (in Figure 2) the layout of your network will be displayed in graphical form.

Host details: This tab will give you specific information about a selected host. To select a host you simply select the desired target from the left pane where all of the IP addresses or host names are listed.

Scans: This tab lists all of the scans you have executed. Most of these will be unsaved scans. You can, of course, select one of your past scans and re-run it by selecting said scan and clicking the Scan button.

Topology Tab

The Topology tab is going to be one of the more important tools in your audit. When you click on this tab you will see, depending upon the size of your network, a blob of red circles and IP addresses. If your network is large enough this blob will, at first, be worthless. What you have to do is use the Zoom and Ring Gap sliders to zoom in on your network and enlarge the ring gap. By enlarging these numbers the devices on the topology map will expand and the details will begin to show. Of course you can get a much deeper look at a particular host in the Details tab. But for the overall look at your network, this is ideal.

As mentioned earlier, this map is interactive. What you can do (other than add/remove details and zoom in and out) is select a particular host and make it the focal point of your map. You can also select a point in the Navigation section and move the map around.

6. Conclusions:

7. QUIZ/ Viva Questions:

- What is meant by network security?
- What is the concept of network audit?
- How is ‘nmap’ useful?
- How is ‘zenmap’ useful?
- What analysis can be made by using nmap tool?

8. References:

1. https://nmap.org/
2. https://hackertarget.com/nmap-tutorial/
3. https://www.youtube.com/watch?v=3Ab1gw8vQjg
4. https://www.linux.com/learn/beginners-guide-nmap

Advanced Networking Technologies

Experiment No: 6

To configure Firewalls using ufw and IPtables

Experiment No. 6

1. **Aim:** To Configure firewall using UFW and IPtables

2. **What you will learn by performing this experiment?**

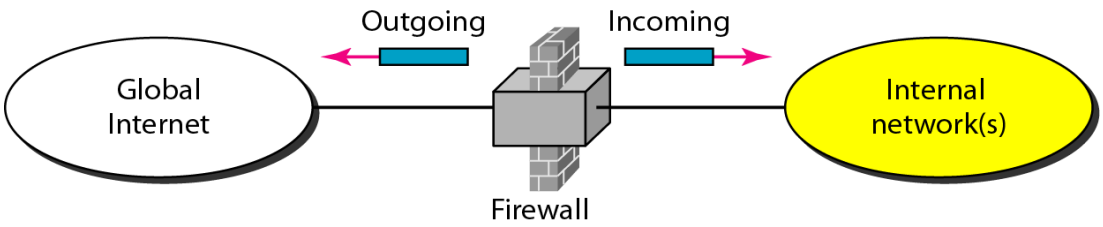
   - To understand the advantages of Firewalls
   - To understand the different implementation of firewall
   - How to configure firewall in UBUNTU.

3. **Software Required: Linux OS(Ubuntu):**

4. **Theory:**

To control access to a system, we need firewalls. A firewall is a device installed between the internal network of an organization and the rest of the Internet. It is designed to forward some packets and filter (not forward) others. A firewall is hardware, software, or a combination of both.

- Hardware Firewalls
  - Protect an entire network
  - Implemented on the router level
  - Usually more expensive, harder to configure
- Software Firewalls
  - Protect a single computer
  - Usually less expensive, easier to configure



A Firewall disrupts free communication between trusted and un-truste networks,attempting to manage the information flow and restrict dangerous free access.

Packet Filtering Firewall:

The network level operations corresponding to the security policy above were actually an example of a simple packet filter.A Firewall implementing a packet filter looks at one packet at a time, and considers it in isolation in order to make a forwarding decision. Because of the way that a packet filtering Firewall works, it can implement a restricted range of filtering decisions.

The principal limitations of packet filtering are:

- TCP connections can be filtered on port and direction in order to implement simple directional traffic rules keyed on port number only.
- It is not possible to completely filter TCP packets which aren't valid, or don't form part of an active connection.
- It is not possible to fully filter UDP connections to ensure that they are part of a valid conversation. the only safe option is to block external to internal UDP transactions when using a packet filtering Firewall.

Although the above drawbacks may seem significant, there are also some quite strong advantages to a basic packet filtering Firewall:

- It is simple to implement, which means that it is much more unlikely that exploitable bugs exist in the Firewall code. The same simplicity means that rule sets tend to be less complex, and again are less likely to contain unintentional access routes.
- It can be implemented on relatively inexpensive hardware, meaning that simple, cheap boxes can do packet filtering for very large numbers of user connections.

5. Implementation Details:

UFW - Uncomplicated Firewall

The default firewall configuration tool for Ubuntu is ufw.

Developed to ease IPtables firewall configuration, *ufw* provides a user friendly way to create an IPv4 or IPv6 host-based firewall.

By default, UFW is enabled but all ports are left open .

GUFW is a GUI that is available as a frontend.

Set Default Rule

Setting the default mode of ufw is recommended before turning it on **Set Default Deny:**

sudo ufw default deny

Set Default Allow:
sudo ufw default allow

Enable and Disable

Enable ufw

To turn UFW on:
sudo ufw enable

Unless you have used set the default to deny when you initially enable ufw ,it is in ALLOW mode, and will allow everything incoming and outgoing until you make rule sets.

Disable ufw

To disable ufw use:
sudo ufw disable

Allow and Deny

Allow

sudo ufw allow <port>/<optional: protocol>

(a) example: To allow incoming tcp and udp packet on port 53
sudo ufw allow 53
(b) example: To allow incoming tcp packets on port 53
sudo ufw allow 53/tcp

(c) example: To allow incoming udp packes on port 53
sudo ufw allow 53/udp

Deny

sudo ufw deny <port>/<optional: protocol>

(a) example: To deny tcp and udp packets on port 53
sudo ufw deny 53
(b) example: To deny incoming tcp packets on port 53
sudo ufw deny 53/tcp
sudo ufw deny 53/udp

Delete Existing Rule

To delete a rule, simply prefix the original rule with delete. For example, if the original rule was:
ufw deny 80/tcp

Use this to delete it:
sudo ufw delete deny 80/tcp

Services

You can also allow or deny by service name since ufw reads from /etc/services. To see get a list of services:

less /etc/services

Allow by Service Name

sudo ufw allow <service name>
example: to allow ssh by name
sudo ufw allow ssh

Deny by Service Name

sudo ufw deny <service name>
example: to deny ssh by name
sudo ufw deny ssh

Status

Checking the status of ufw will tell you, if ufw is enabled or disabled and also list
the current ufw rules that are applied to your iptables.

To check the status of ufw:
sudo ufw status

Status active

To	Action	From
--	------	----
22	DENY	192.168.0.1
22:	DENY	192.168.0.7
22:	ALLOW	192.168.0.0/24

if ufw was not enabled the output would be:
sudo ufw status
Status: inactive

Logging

To enable logging use:
ufw logging on

To disable logging use:
ufw logging off

Advanced Syntax

You can also use a fuller syntax, specifying the source and destination addresses
and ports.

Allow Access

This section shows how to allow specific access.

- **Allow by Specific IP**
  sudo ufw allow <ip address>
  example:To allow packets from 207.46.232.182:
  sudo ufw allow from 207.46.232.182

- **Allow by Subnet**
  You may use a net mask :
  sudo ufw allow from 192.168.1.0/24

- **Allow by specific port and IP address**
  sudo ufw allow from <ip address> to <protocol> port <port number>
  xample: allow ip address 192.168.0.4 access to port 22 for all protocols
  sudo ufw allow from 192.168.0.4 to any port 22

Deny Access

- **Deny by specific IP**
  sudo ufw deny from <ip address>
  example:To block packets from 207.46.232.182:
  sudo ufw deny from 207.46.232.182

- **Deny by specific port and IP address**
  sudo ufw deny from <ip address> to <protocol> port <port number>
  example: deny ip address 192.168.0.1 access to port 22 for all protocols
  sudo ufw deny from 192.168.0.1 to any port 22

Advanced Blocking Rules

Blocking IP addresses is not so straight forward if you have an existing set of rules as IPTABLES matches in order.
So if you started with default' deny' and added in port 80 for a public server :
sudo ufw allow 80
But then find IP address 111.222.3.44 is hacking your server :
sudo ufw deny 111.222.3.44
will do nothing (you allowed access with your first rule).

You need to edit /etc/ufw/before.rules and add a section "Block IP" after "Drop INVALID packets" :

-A ufw-before-input -s 111.222.3.44 -j DROP

Example:

Scenario: You want to block access to port 22 from 192.168.0.1 and 192.168.0.7 but allow all other 192.168.0.x IPs to have access to port 22.
To check your rules you can check the status; for the scenario the output below is the desired output for the rules to work properly

sudo ufw deny from 192.168.0.1 to any port 22
sudo ufw deny from 192.168.0.7 to any port 22
sudo ufw allow from 192.168.0.0/24 to any port 22
sudo ufw status

Status active

To	Action	From
--	------	----
22	DENY	192.168.0.1
22	DENY	192.168.0.7
22	ALLOW	192.168.0.0/24

Scenario change:
You want to block access to port 22 to 192.168.0.3 as well as 192.168.0.1 and 192.168.0.7.

sudo ufw delete allow from 192.168.0.0/24 to any port 22
sudo ufw status

Status active

To	Action	From
--	------	----
22	DENY	192.168.0.1
22	DENY	192.168.0.7

sudo ufw deny 192.168.0.3 to any port 22
sudo ufw allow 192.168.0.0/24 to any port 22
sudo ufw status

Status active

To	Action	From
22	DENY	192.168.0.1
22	DENY	192.168.0.7
22	DENY	192.168.0.3
22	ALLOW	192.168.0.0/24

6. Conclusions:

7. QUIZ / Viva Questions:

- What is a firewall?
- Which are the various types of Firewall configurations?
- What are the advantages and disadvantages of Firewalls?
- What is meant by packet filtering firewall? Bring out its merits and demerits.
- What is meant by "stateful inspection"? Explain.

8. References:

1. www.firewallinformation.com/
2. https://www.microsoft.com/en-us/safety/pc-security/firewalls-whatis.aspx
3. *rlworkman.net/howtos/iptables/iptables-tutorial.html*
4. www.linuxhowtos.org/Security/iptables.htm

Advanced Networking Technologies

Experiment No: 7

To Determine the Network Statistics using ntop

Experiment No. 7

1. **Aim:** To determine the network statistics using ntop

2. **What you will learn by performing this experiment?**

   - To learn the basics of network traffic management.
   - To understand concept of traffic load monitoring and protocol statistics.
   - To install and configure network traffic tool ntop.

3. **System Requirements:**
   - 3 workstations installed with Unix/Linux Fedora Core/Ubuntu and Windows XP
   - NTOP latest version

4. **Theory:**

ntop is the best tool to see network usage in a way similar to what top command does for processes i.e. it is network traffic monitoring software. You can see network status, protocol wise distribution of traffic for UDP, TCP, DNS, HTTP and other protocols.

ntop is a hybrid layer 2 / layer 3 network monitor, that is by default it uses the layer 2 Media Access Control (MAC) addresses AND the layer 3 tcp/ip addresses. ntop is capable of associating the two, so that ip and non-ip traffic (e.g. arp, rarp) are combined for a complete picture of network activity.

ntop is a network probe that shows interactive mode, it displays the network status on the user's terminal. In Web mode, it acts as a Web server, creating a HTML dump of the network status. It sports a NetFlow/sFlow emitter/collector, a HTTP-based client interface for creating ntop-centric monitoring applications, and RRD for persistently storing traffic statistics. Network Load Statistics.

5. **Procedure:**

1. Install ntop under Linux (Ubuntu):
   Type the following commands, enter:
   $ sudo apt-get update
   $ sudo apt-get install ntop

2. Set ntop admin user password

Type the following command to set password, enter:

#

OR

$ sudo /usr/sbin/ntop -A

3. Restart ntop service

- Type the following command, enter:

  # /etc/init.d/ntop restart

- Verify ntop is working, enter:

  # netstat -tulpn | grep :3000

ntop by default use 3000 port to display network usage via webbrowser.

4. View network usage stats:

- Type the url:

  # netstat http://localhost:3000/

  OR

  # netstat 10.0.0.4: 3309

  # netstat 10.0.0.6 : 8800

6. Conclusions:

7. Quiz / Viva Questions:

- What is meant by network management?
- What is meant by traffic load monitoring?
- What is the usage of ntop?

8. References:

1. www.**ntop**.org/support/documentation/documentation/
2. https://www.maketecheasier.com/install-configure-**ntop**/
3. https://www.youtube.com/watch?v=EQQXnQkjFCs

Advanced Networking Technologies

Experiment No: 8

To study and Implement Graphical Network Monitor: etherape

Experiment No. 8

1. **Aim:** To study and implement graphical network monitor : etherape

2. **What you will learn by performing this experiment?**

   - To understand the features of network monitoring tool , "etherape"
   - To understand the "capture " feature of this software.
   - How to run the commands in 'etherape"

3. **Software Required: "etherape" Package in Linux (Ubuntu)**

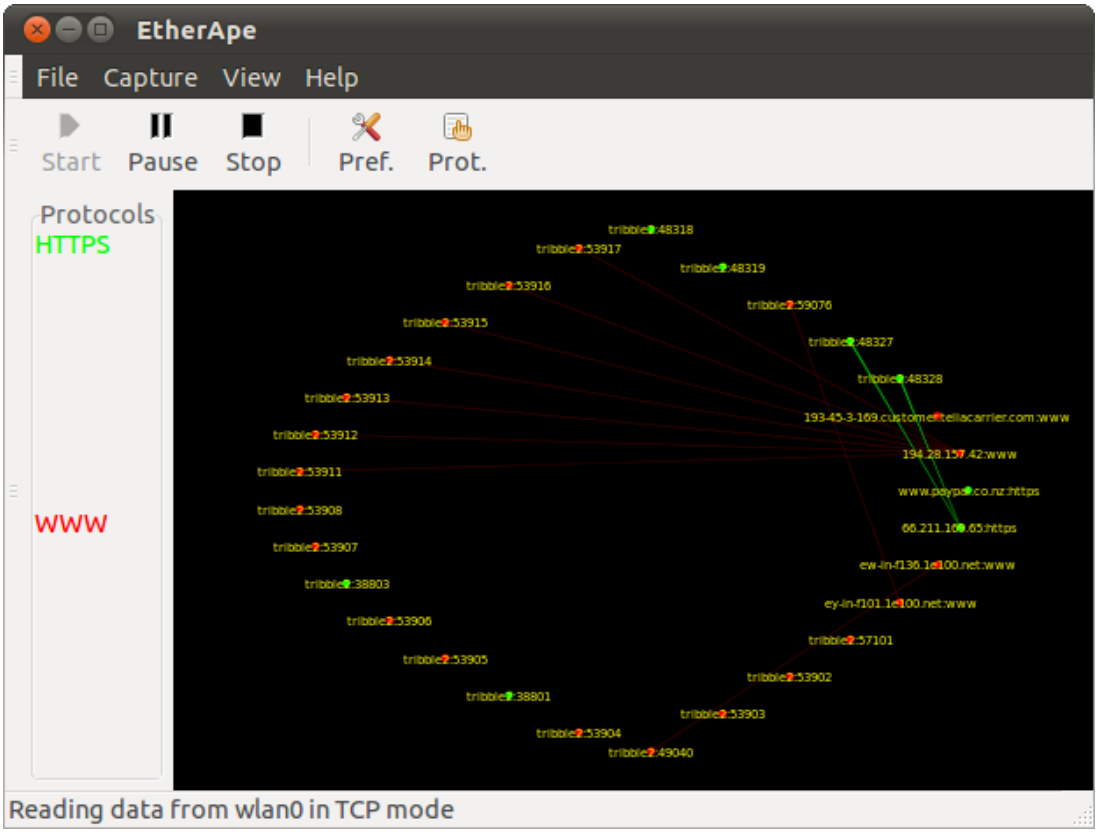
4. **Theory:**

EtherApe is a graphical network monitor modeled after etherman. it displays network activity graphically, showing active hosts as circles of varying size, and traffic among them as lines of varying width.

Etherape listens to your network (locally) and shows you the traffic.

The EtherApe network monitor is a midrange option for monitoring your network's data traffic. As an open source network monitor, EtherApe offers a dynamic graphical interface; features IP and TCP modes , color-color coded protocols display; supports Ethernet, FDDI, PPP, and slip devices; filters traffic; and reads traffic from both a tcpdump file and as well as live from the network.

EtherApe can track many types of network traffic. When you start EtherApe, you may or may not see traffic depending on whether there is traffic actively passing through your network. you'll notice that the display immediately becomes dynamic. As traffic comes in, the amount of traffic is represented by the size of the lines representing the connection.If you need to know more about the traffic passing on your network, you should open the Protocols window.



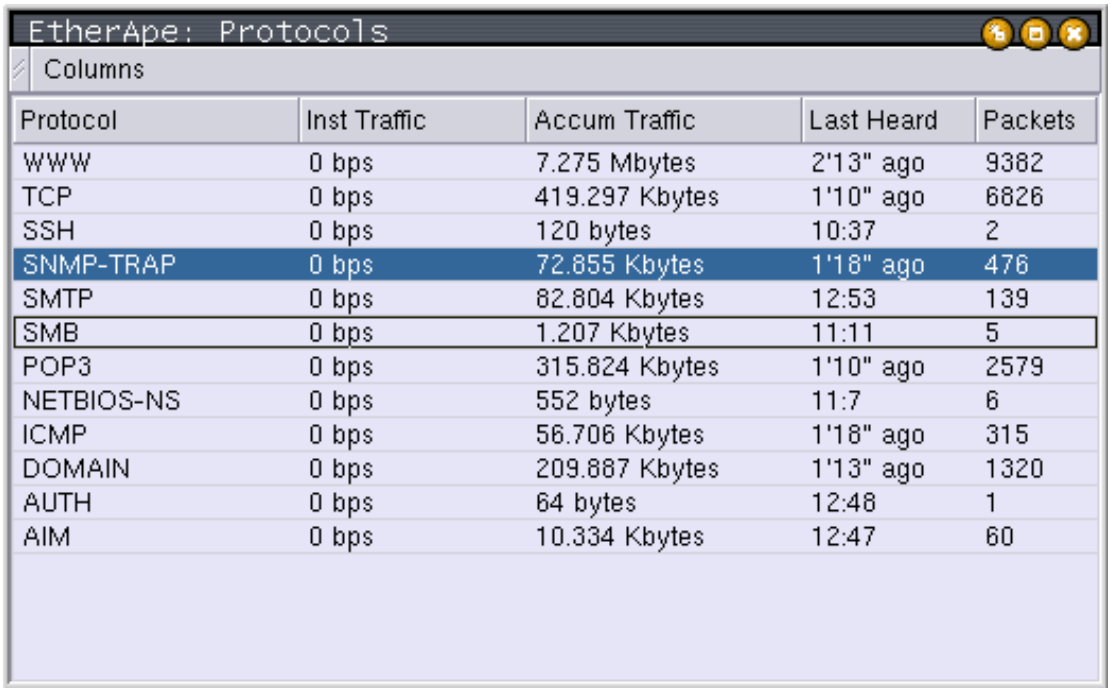
From the View drop-down menu, select Protocols to open the Protocols window.

The Protocol window keeps a running total of each type of packet that traverses your network.

Protocols window

The Protocols window is a great tool to use for troubleshooting your network. Suppose your network becomes extremely slow, and you have no idea why. You can use EtherApe to check on the traffic that's moving through your network. When you fire up EtherApe, you see a Web of traffic. You open the Protocols window and confirm that WWW is racking up an enormous amount of traffic. You can end this problem by blocking the domain from entering your internal network.

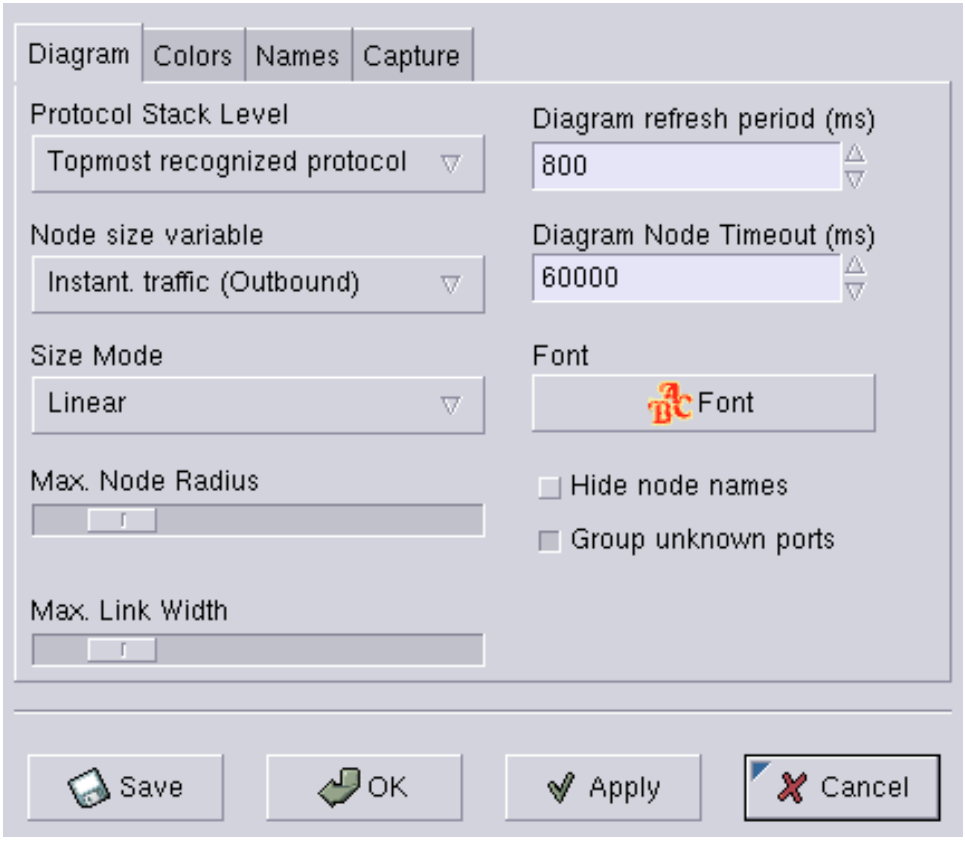
The top protocol listed is the one with the most accumulated traffic.



Protocol	Inst Traffic	Accum Traffic	Last Heard	Packets
WWW	0 bps	7.275 Mbytes	2'13" ago	9382
TCP	0 bps	419.297 Kbytes	1'10" ago	6826
SSH	0 bps	120 bytes	10:37	2
SNMP-TRAP	0 bps	72.855 Kbytes	1'18" ago	476
SMTP	0 bps	82.804 Kbytes	12:53	139
SMB	0 bps	1.207 Kbytes	11:11	5
POP3	0 bps	315.824 Kbytes	1'10" ago	2579
NETBIOS-NS	0 bps	552 bytes	11:7	6
ICMP	0 bps	56.706 Kbytes	1'18" ago	315
DOMAIN	0 bps	209.887 Kbytes	1'13" ago	1320
AUTH	0 bps	64 bytes	12:48	1
AIM	0 bps	10.334 Kbytes	12:47	60

Configuration of EtherApe

To configure EtherApe, click the Stop button on the main window and then **click the Pref** (preferences) button (on the main window) to open the Configuration window as shown in Figure below:



The first tab on the EtherApe Configuration window, **the Diagram tab**, can be used to configure some of the monitor's protocol specifics.

With the **Protocol Stack Level configuration**, you can specify the level of packet you want to monitor. **Using the Topmost Recognized Protocol** level gives you more specific information about the packets traversing your network the Topmost Recognized Protocol (Level 1, physical medium),

Level 2 (eth_II),…ARP
Level 3 (IP),
Level 4 (TCP and UDP), and
Level 5 (HTTP).

Node Size Variable is another handy configuration. Node Size allows you to dictate the direction in which EtherApe is monitoring. **There are two types of traffic, instant and accumulative,** and each type has three different directional patterns (inout, inbound, and outbound).

On this same tab, you can alter the **Diagram Refresh Rate**. This rate count is in milliseconds, Default is 800. (,but it is easier to work somewhere between 500 and 700 milliseconds.)

Also on the Diagram tab is the **Diagram Node Timeout option**, which dictates how long a node will remain in the Diagram without activity. **The default setting is 6,000 milliseconds.** With a multinode network, it would be wise to set this number to a lower number to make the Diagram more easily readable.

Filters

As with all network monitors, the most important aspect of EtherApe is the filters. In a network monitor, a filter utility allows you to monitor the traffic patterns at a granular level.

You first open the Preferences window and select the Capture tab. The top left drop-down list (labeled Capture Filter) is where you will enter the filter syntax, which for EtherApe is *src net IP_ADDRESS dst net IP_ADDRESS* (where *IP_ADDRESS* is the actual IP address of the machine, or machines, you wish to monitor).

So if you want to monitor the data processing department whose IP addresses use the range 192.168.1, you would enter *src net 192.168.1 dst net 192.168.1* to create this filter.

Once you enter the filter, you will save and then click OK. The filter will then begin running.

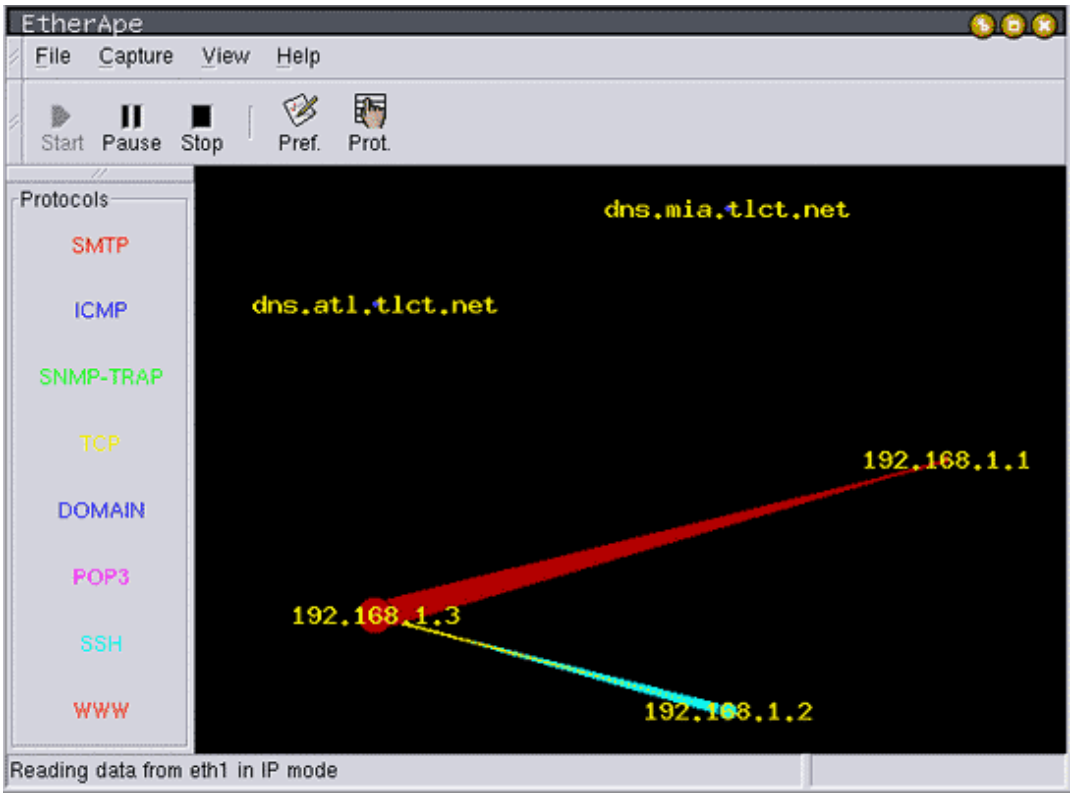
Reading from files and remote networks EtherApe's ability to read from a tcpdump file is good, because it allows an administrator to capture network traffic to a file and analyze that traffic either off-line or at a more convenient time

5. **Procedure :**

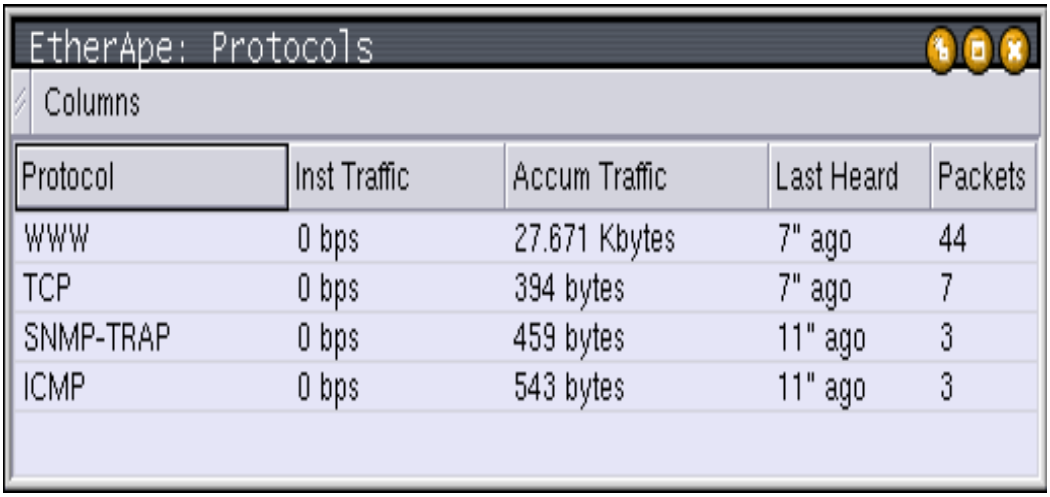
1. Install etherape under Linux (Ubuntu):
   Type the following commands, enter:
   sudo apt-get install etherape
   sudo apt-get update
2. Open the Google application and run a search for any word..(say etherape)

3. Once you've installed the application, run EtherApe by typing at the command Prompt :
   sudo etherape &
   you will see the graphical display on the screen

4. Running EtherApe
   When you open EtherApe, you'll see a window much like the one shown in



5. Now click on the 'Capture tab" and choose "interface Tab" in drop down Menu.and then choose the interface "eth0"
6. Click on "Start" to capture the packets and observe the display .
7. Click on "Protocols" Tab and note down the Protocols , whose packets are being Monitored.



Protocol	Inst Traffic	Accum Traffic	Last Heard	Packets
WWW	0 bps	27.671 Kbytes	7" ago	44
TCP	0 bps	394 bytes	7" ago	7
SNMP-TRAP	0 bps	459 bytes	11" ago	3
ICMP	0 bps	543 bytes	11" ago	3

8. Use the Tab "Pause" and observe the display.
9. Configure the Display.

6. Conclusions:

7. Quiz/ Viva questions:

- What is meant by network monitoring?
- How etherape is useful in monitoring the network?

8. References:

1. ***etherape***.*sourceforge.net/*
2. https://en.wikipedia.org/wiki/**EtherApe**
3. https://www.youtube.com/watch?v=oPlnB-Lu3v
4. https://apps.ubuntu.com/cat/applications/**etherape**/

Advanced Networking Technologies

Experiment No: 9

To Study various Network Management tools

Experiment No. 9

1. **Aim:** To study various network management tools.

2. **What you will learn by performing this experiment?**

   - To learn the basics of network management tools and utilities.
   - To use status-monitoring, route-monitoring and traffic-monitoring tools.
   - To use different network tools that are available in the Linux and Windows (XP and other) environments to obtain network parameters or the diagnosis of network problems.

3. **System Requirements:**

   - 3 workstations installed with Unix/Linux Fedora Core/Ubuntu and Windows XP
   - Nmap latest version
   - NmapFE latest version
   - Iptables latest version
   - Tcpdump latest version
   - Wireshark latest version

4. **Theory:**

System Utilities for Network Management

A significant amount of network management can be done using operating system (OS) utilities and some freely downloadable tools. Numerous basic tools are either a part of the OS or are available as add-on applications that aid in obtaining network parameters or in diagnosis of network problems. We describe some of the more popular ones here under the three categories of status-monitoring, route-monitoring and traffic-monitoring.

5. **Procedure:**

1. Under Linux:

   Go to command line interface (CLI)- Ctl+Alt+ T and use these commands
   student@localhost$

2. Under Microsoft Windows:

   Go to Start --> run --> cmd C:\

Table-1: Status Monitoring Tools:

Name	Operating Systems	Description
mii-tool	Unix/Linux	View, manipulate media-independent interface status
ifconfig/ ipconfig	Unix/Linux/ Windows	Obtains and configures a network interface parameter and status
ping	Unix/Linux/Windows	Send ICMP ECHO_REQUEST to network hosts and check the status.
nslookup	Unix/Linux/Windows	Query Internet name servers (DNS) interactively
dig	Unix/Linux	DNS lookup utility (supersedes nslookup)
host	Unix/Linux	DNS lookup utility
dmesg	Linux/Unix	Control the kernel ring buffer/log records
nmap	Linux/Unix	Network exploration tool and security / port scanner

Table-2: Route-Monitoring Tools:

Name	Operating Systems	Description
route/netstat	Unix/Linux Windows	Displays the contents of various network-related data structures
ss	Unix/Linux	Utility to investigate sockets
arp	Linux/Windows	ARP stands for Address Resolution Protocol, which is used to find the media access control address of a network neighbour for a given IPv4 Address.
traceroute	Linux	Traces the route to a destination with routing delays
tracert	Unix/Windows	Traces the route to a destination with routing delays

Table-3: Traffic-Monitoring Tools:

Name	Operating Systems	Description
ping	Linux/Windows	Used Interactively dump and analyze network traffic for measuring round-trip packet loss
bing	Unix/Linux	Measures point-to-point bandwidth of a link
tcpdump	Linux/Unix	Dump traffic on a network
Ethereal/ Wireshark	Linux/Windows	Interactively dump and analyze network traffic
iptraf	Unix/Linux	Interactive Colorful IP LAN Monitor

6. Conclusions:

7. QUIZ / Viva Questions:

- Which are the network management tools and utilities?
- Which are the different traffic monitoring tools?
- Which are the different route monitoring tools?
- Which are the different status monitoring tools?

8. References:

1. www.slac.stanford.edu/xorg/nmtf/nmtf-**tools**.html
2. *web.swcdn.net/creative/pdf/Whitepapers/npm_**routemonitoring**_130502.pdf*
3. https://en.wikipedia.org/wiki/**Route**_analytics

Advanced Networking Technologies

Experiment No: 10

To install and configure an SNMP Daemon/ Client and use basic SNMP

Experiment No. 10

1. **Aim:** To install and configure an SNMP Daemon/ Client and use basic SNMP commands.

2. **What you will learn by performing this experiment?**

   - To to explore how SNMP can be implemented on a system by installing the daemon and tools on Linux systems.
   - To learn the contents of a MIB (Management Information Base).
   - How to use an SNMP manager to query an SNMP agent.
   - How to use SNMP to learn about the network configuration.

3. **System Requirements:**

   - 3 workstations installed with Unix/Linux Fedora Core/Ubuntu and Windows XP
   - SNMP tools latest version

4. **Theory:**

SNMP stands for simple network management protocol. It is a way that servers can share information about their current state, and also a channel through which an administer can modify pre-defined values. While the protocol itself is very simple, the structure of programs that implement SNMP can be very complex.

In this lab, you will learn how to use the SNMP tool net-snmp. Information about this tool can be found in http://www.net-snmp.org/. This tool has been installed at most of the machines in the lab, but you can easily install it on any other machine you use – both Windows and Linux versions are available. The machine you are going to use will act as SNMP manager. The host runs snmpd, which is an SNMP agent. This agent can be used to access managed objects of that host.

The version of SNMP used is SNMPv2c (use option –v 2c in your commands). Also, the read-only community name public has been configured (and can be used in your commands). Most of the questions in this lab exercise are related to finding MIB objects.

5. Procedure:

1. Install the SNMP Daemon and Utilities

On the first server, update the apt database and install the manager component. Along with this, we will also download another package called snmp-mibs-downloader which contains some proprietary information about standard MIBs that allow us to access most of the MIB tree by name:

sudo apt-get update
sudo apt-get install snmp snmp-mibs-downloader

On our second server, the one that we will be interacting with that will run the daemon, we can install the necessary components by typing:

sudo apt-get update
sudo apt-get install snmpd

Now that you have installed these components, we need to configure our setup.

2. Configuring the SNMP Manager

We just need to modify one file to make sure that our client can use the extra MIB data we installed.

Open the /etc/snmp/snmp.conf file in your text editor with sudo privileges:

sudo nano /etc/snmp/snmp.conf

In this file, there are a few comments and a single un-commented line.
To allow the manager to import the MIB files, we simply need to comment out the mibs : line:
#mibs :
Save and close the file when you are finished.

We are now finished configuring the manager portion, but we will still need to use this server to help us configure our agent computer.

3. Configuring the SNMP Agent Machine

As a true client-server system, the agent computer does not have any of the external tools needed to configure its own SNMP setup. We can modify some configuration files to make some changes, but most of the changes we need to make will be done by connecting to our agent server from our management server.

To get started, on our agent computer, we need to open the daemon's configuration file with sudo privileges:

sudo nano /etc/snmp/snmpd.conf

First, we need to change the agentAddress directive. Currently, it is set to only allow connections originating from the local computer.

We need to comment out the current line, and uncomment the line underneath, which allows all connections**:**

 # Listen for connections from the local system only
#agentAddress udp:127.0.0.1:161
 # Listen for connections on all interfaces (both IPv4 *and* IPv6)
agentAddress udp:161,udp6:[::1]:161

When you are finished making these changes, save and close the file. To implement these changes, restart the snmpd service:

sudo service snmpd restart

4. SNMP commands:

Example:

snmpwalk -v 1 -c public localhost .1.3.6.1.2.1.1

Or

snmpwalk -v 1 -c public 172.16.20.11 .1.3.6.1.2.1.1

The General Structure of SNMP Commands:

When using the suite of tools included in the snmp package (the net-snmp software suite), you will notice a few patterns in the way you must call the commands.
The first thing you must do is authenticate with the SNMP daemon that you wish to communicate with. This usually involves supplying quite a few pieces of information.

The common ones are below:

-v VERSION: This flag is used to specify the version of the SNMP protocol that you would like to use. We will be using v3 in this guide.

-c COMMUNITY: This flag is used if you are using SNMP v1 or v2-style community strings for authentication. Since we are using v3-style user-based authentication, we will not be needing this.

-u USER-NAME: This parameter is used to specify the username that you wish to authenticate as. To read or modify anything using SNMP, you must authenticate with a known username.

-l LEVEL: This is used to specify the security level that you are connecting with. The possible values are noAuthNoPriv for no authentication and no encryption, authNoPriv for authentication but no encryption, and authPriv for authentication and encryption. The username that you are using must be configured to operate at the security level you specify, or else the authentication will not succeed.
-a PROTOCOL: This parameter is used to specify the authentication protocol that is used. The possible values are MD5 or SHA. This must match the information that was specified when the user was created.

-x PROTOCOL: This parameter is used to specify the encryption protocol that is used. The possible values are DES or AES. This must match the information that was specified when the user was created. This is necessary whenever the user's privilege specification has priv after it, making encryption mandatory.

-A PASSPHRASE: This is used to give the authentication passphrase that was specified when the user was created**.**

-X PASSPHRASE: This is the encryption passphrase that was specified when the user was created. If none was specified but an encryption algorithm was given, the authentication passphrase will be used. This is required when the -x parameter is given or whenever a user's privilege specification has a priv after it, requiring encryption.

Using this information, we can begin to construct our commands.

Given how we set up our bootstrap user, the commands we will be using with that account will look like this:
E.g.
$snmpget -u bootstrap -l authPriv -a MD5 -x DES -A temp_password -X temp_password remote_host 1.3.6.1.2.1.1.1.0

6. Conclusions:

7. QUIZ / Viva Questions:

- What is SNMP?
- How it is useful?
- What Is Meant By Snmp Manager?
- What Is Meant By SNMP Agent?

8. References:

1. https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
2. https://www.manageengine.com/network-monitoring/what-is-**snmp**.html