PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE - 411043

Department of Electronics & Telecommunication

CLASS : BE (E&TC) **SUBJECT: CN**
EXPT. NO : - 01 **DATE :** 18-08-2020

I. AIM : Implementation of LAN using Star topology and verify connectivity between two Computers using crossover UTP CAT-5 cable.

II. APPARATUS: Computer Systems (2 Nos.), Crossover UTP CAT-5 cable.

III. THEORY: Local area networks (LANs) can be implemented in several ways. They can be divided into several subgroups based on e.g. physical implementation or standardized technologies. Choosing the right kind of LAN solution for a particular purpose always depends on several issues, e.g. size of the network, location of the terminals, and usually also on the cost issues. This essay offers a brief overview on some of the most common LAN implementation techniques.

LANs can be divided into two quite different types: wired LANs and wireless LANs. As their names imply, wired LANs require fixed wiring whereas wireless LANs utilize radio or light waves as the transmission media. Wired LANs are much more common and usually less costly when used to e.g. interconnect all office equipment to provide shared use of printers and other resources. But if the layout of the interconnected computers is due to change often, a wireless network is worth considering, as also in the case of interconnecting handheld terminals and portable computers.

NIC(network interface card): A network interface controller (NIC, also known as a network interface card, network adapter, LAN adapter or physical network interface, and by similar terms) is a computer hardware component that connects a computer to a computer network(see Fig.1).

The network controller implements the electronic circuitry required to communicate using a specific physical layer and data link layer standard such as Ethernet, Fiber Channel, Wi-Fi or Token Ring. This provides a base for a full network protocol stack, allowing communication among small groups of computers on the same local area network (LAN) and large-scale network communications through routable protocols, such as Internet Protocol (IP).

The NIC allows computers to communicate over a computer network, either by using cables or wirelessly. The NIC is both a physical layer and data link layer device, as it provides physical access to a networking medium and, for IEEE 802 and similar networks, provides a low-level addressing system through the use of MAC addresses that are uniquely assigned to network interfaces.

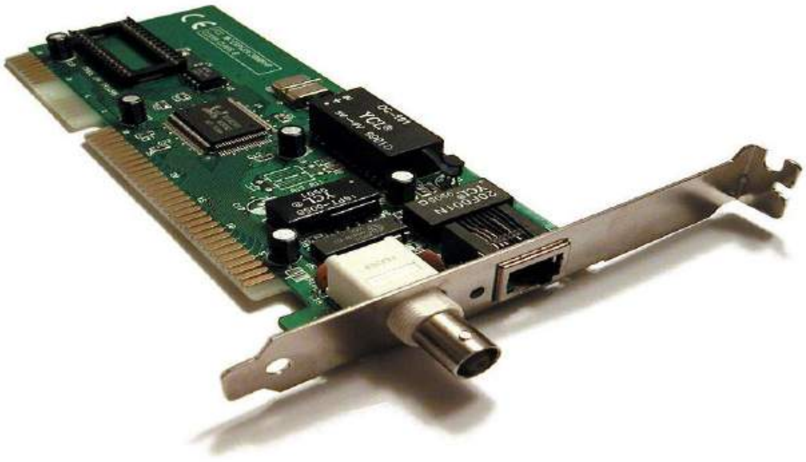


Fig.1 NIC (network interface card):

NIC (Network Interface Card) or, also called a LAN adapter, crucial and the starting point of any network communications. Network card has a unique code called a MAC (Media Access Control). This is a binary number of 48 bits, which are often presented in hexadecimal form as PP-PP-PP-SS-SS-SS. The first 24 bits (PP) marks the manufacturer and the next 24 bits(SS) belong to the serial number of the card. As directed by ISO can be no more cards with the same serial number, which means that the MAC address is unique. There is a PC, network printer, Ethernet port of routers and similar devices. It belongs to the devices of the second layer of the OSI model what it means to know what to do with a FRAME. In the following figure.2 shows the block diagram of communication two network cards.

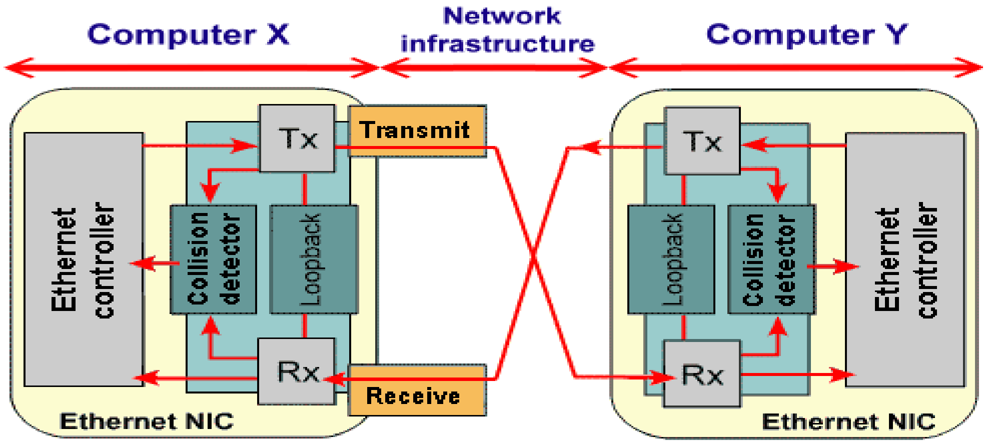


Fig.2 Block Diagram of Network Adaptor Card.

Physical Topology

The term physical topology refers to the way in which a network is laid out physically.

There is also other physical division criterion: Naturally wired and wireless LANs use different topologies. The four topologies in common use for wired LANs are bus, ring, hub and star. Bus is a linear connection between the data terminals. A single network cable is routed through those locations that have terminals, and a physical connection (tap) is made to the cable for each terminal.

Bus networks are often extended into an interconnected set of buses with special bus extenders. Ring topology is similar to bus topology except that in ring topology the two ends of the bus are connected to form a ring. Hub topology is a variation of bus and ring(See Fig.3,4,5,6). In this case wiring from terminal always goes through hub first before going to another terminal. Hub consists of a set of repeaters that retransmit all the received signals to all terminals in that direction.

Star topology means that the terminals are connected through a server or a router, which takes care of routing the signals into the right direction. Wireless LANs have two common topologies, namely fixed-wire replacement and ad hoc networks. The former is simply a LAN using wireless connection in a place where normally would be a wired LAN, but due to a high cost of installing wiring or often changing network layout. The latter is a real wireless LAN with possibly nothing else than portable-to-portable connections.

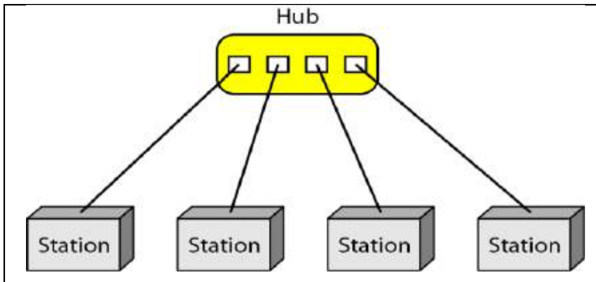


Fig 3. Star Topology

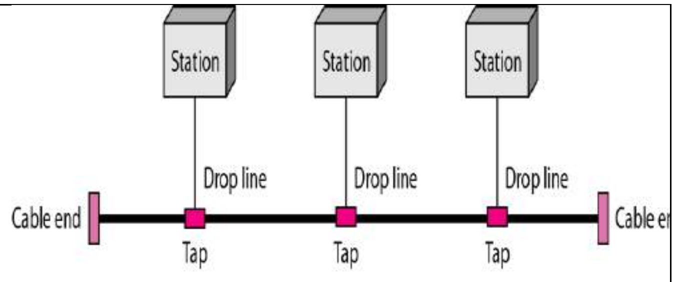


Fig 4 .Bus Topology

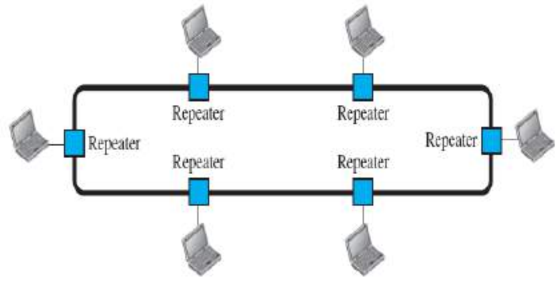


Fig 5.Ring Topology

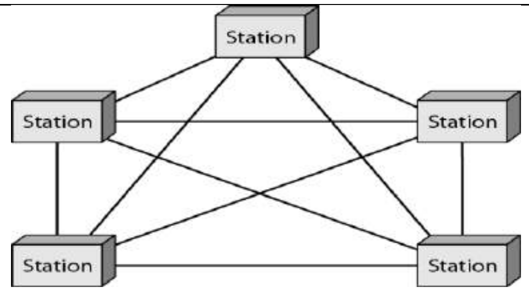


Fig 6 .Mesh Topology

A. The following table shows the different types of UTP-CAT Ethernet cables.

UTP- Categories				
UTP-Categories	**Data Rate**	**Max.Length**	**Cable Types**	**Application**
CAT-1	Up to 1Mbps	--	Twisted Pair	Old Telephone Cable
CAT-2	Up to 4Mbps	--	Twisted Pair	Token Ring Networks
CAT-3	Up to 10Mbps	100m	Twisted Pair	Token Ring & 10BASE –T Ethernet
CAT-4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT-5	Up to 100Mbps	100m	Twisted Pair	Ethernet,Fast Etherent,Tokenn Ring.
CAT-5E	Up to 1Gbps	100m	Twisted Pair	Ethernet,Fast Etherent,Gigabit Ethernet.
CAT-6	Up to 10Gbps	100m	Twisted Pair	Gigabit Ethernet,10G Etherent(55meters)
CAT-6a	Up to 10Gbps	100m	Twisted Pair	Gigabit Ethernet,10G Etherent(55meters)
CAT-7	Up to 10Gbps	100m	Twisted Pair	Gigabit Ethernet,10G Etherent(100 meters)

Table.1 Types of UTP-CAT Ethernet cables

Ethernet network cables are straight and crossover cable. This Ethernet network cable is made of 4 pair high performance cable that consists of twisted pair conductors that used for data transmission. Both end of cable is called RJ45 connector.

Straight and crossover cable can be Cat3, Cat 5, Cat 5e or Cat 6 etc UTP cable, the only difference is each type will have different wire arrangement in the cable for serving different purposes.

There are two types of network cables commonly used in PC networks - Straight-through and cross-over

Purpose of this cross cable is RX (receiving terminal) connects to TX (transmitting) of one pc to another PC and vice versa.

As we use two PCs (same devices), straight cable will connect TX to TX and RX to RX of two computers, so cross cable is required. If you use HUB or switch, then straight cable will work because it has internal arrangement like cross cable. So note that use cross cable to connect two similar devices.

A straight cable will not work to connect two computers together.

Crossover used to connect to PCs directly together, also used for connecting networking devices together like Switch to Switch etc.

Straight cables connect two DIFFERENT types of devices. Whereas crossover cables connect two of the SAME type

A. Straight Cable:

Usually use straight cable to connect different type of devices. This type of cable will be used most of the time and can be used to:

Straight-through cables connect the following devices:

- Switch to router
- Switch to workstation or server
- Hub to workstation or server

If you need to check how straight cable looks like, it's easy. Both sides (side A and side B) of cable have wire arrangement with same color.

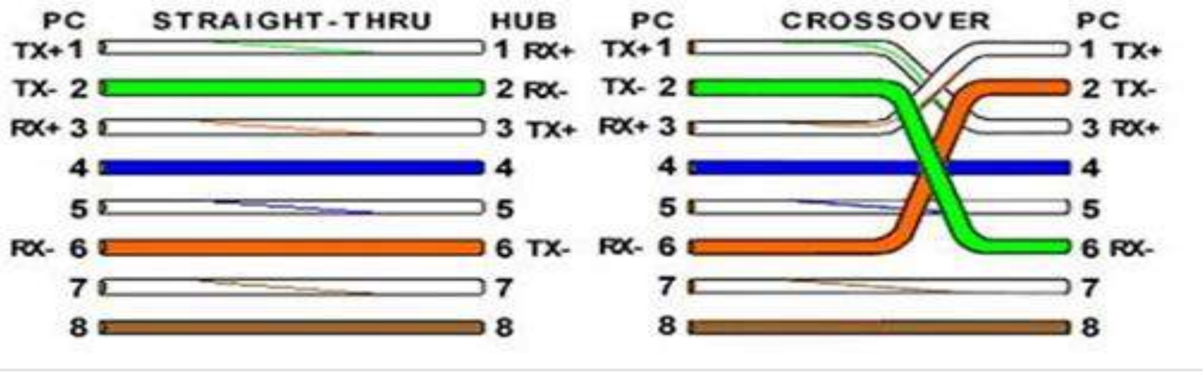
B. Crossover Cable:

Sometimes you will use crossover cable, it's usually used to connect same type of devices. A crossover cable can be used to:

When a workstation (PC) connects to a LAN, it transmits data independently of the other devices connected to the LAN media. The workstation simply transmits data frames from a NIC to the network medium.

If desired, the workstation can be attached directly to another workstation by using a crossover cable. Crossover cables connect the following devices:

- Workstation to workstation
- Switch to switch
- Switch to hub
- Hub to hub
- Router to router
- Router to PC



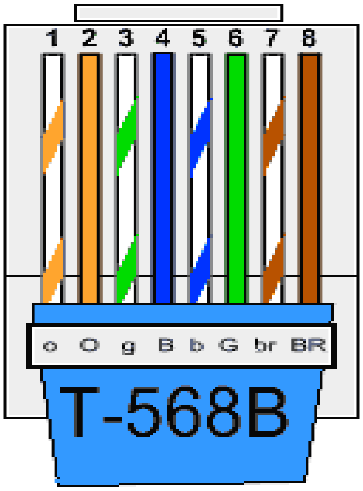
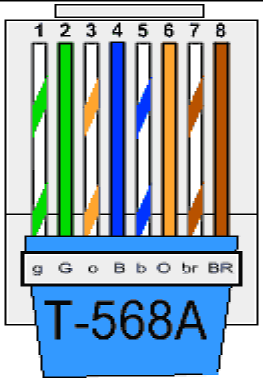
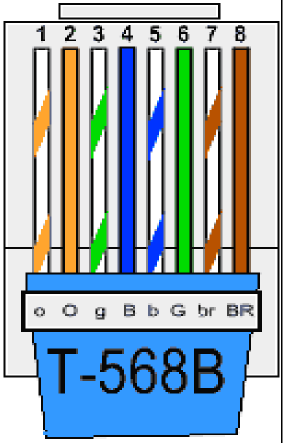
<table>
<tr><td colspan="4"><b>RJ 45 COLOR ARRANGEMENT FOR BOTH TYPES OF CABLES</b></td></tr>
<tr><td colspan="2"><b>1.Straight Cable (Both end same color)</b></td><td colspan="2"><b>Color Coding</b></td></tr>
<tr><td colspan="2">
 </td><td colspan="2">1. Orange white
2. Orange
3. Green white
4. Blue
5. Blue white
6. Green
7. Brown white
8. Brown</td></tr>
<tr><td colspan="4"><b>2.Cross Over</b></td></tr>
<tr><td colspan="2"><b>One end of cable</b></td><td colspan="2"><b>Other end of cable</b></td></tr>
<tr><td>
 </td><td>1. Green white
2. Green
3. Orange white
4. Blue
5. Blue white
6. Orange
7. Brown white
8. Brown</td><td>
 </td><td>1. Orange white
2. Orange
3. Green white
4. Blue
5. Blue white
6. Green
7. Brown white
8. Brown</td></tr>
</table>

Fig 2. Straight-through and cross-over.

B. Every user should know the purpose of different types of commands.

- Ipconfig.
- Ipconfig/all.
- Ping.
- Ping -n 10 IP-address.
- Netstat.
- Tasklist.
- Taskkill.

C. File sharing.

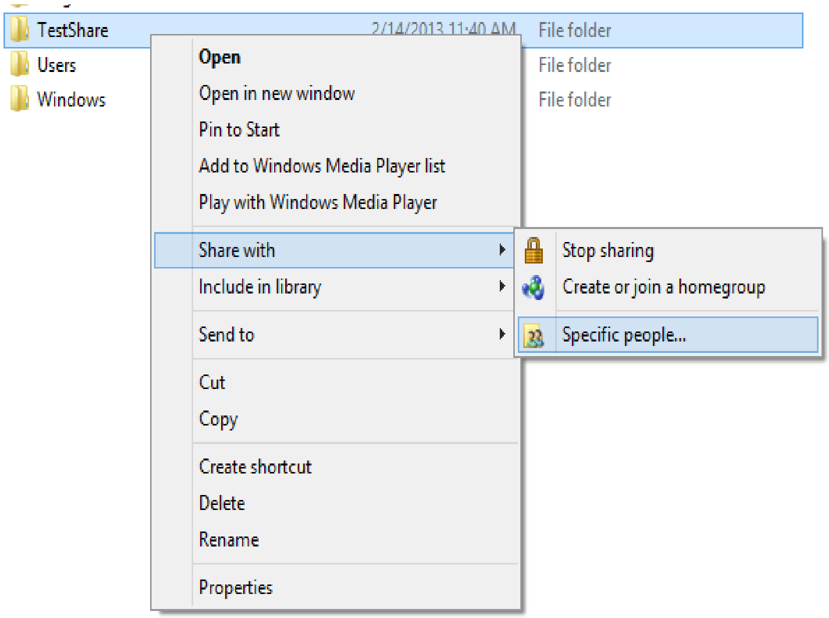
Simple Steps to share folders on Windows 7.

1. Go to Control Panel / Network and Sharing / Advanced sharing options.

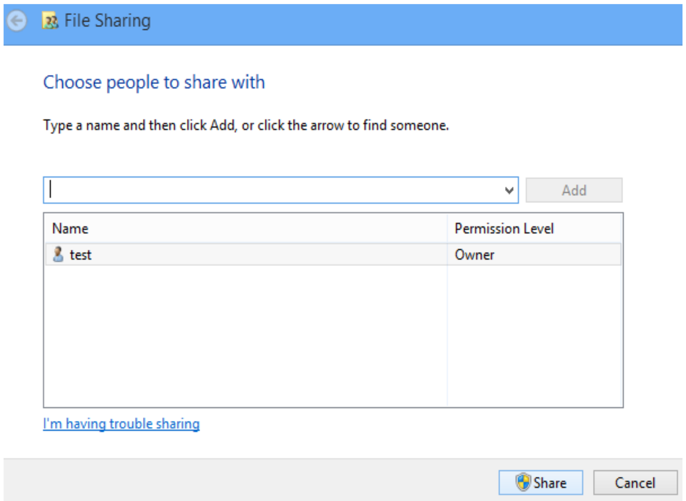
2. Turn **on** file and printer sharing in (current profile).

3. Turn **off** [Password protected sharing] in [All Networks].

4. Choose a folder to be shared.



5. To share with password enabled, add corresponding login name to the dialog, and press [Share] button.

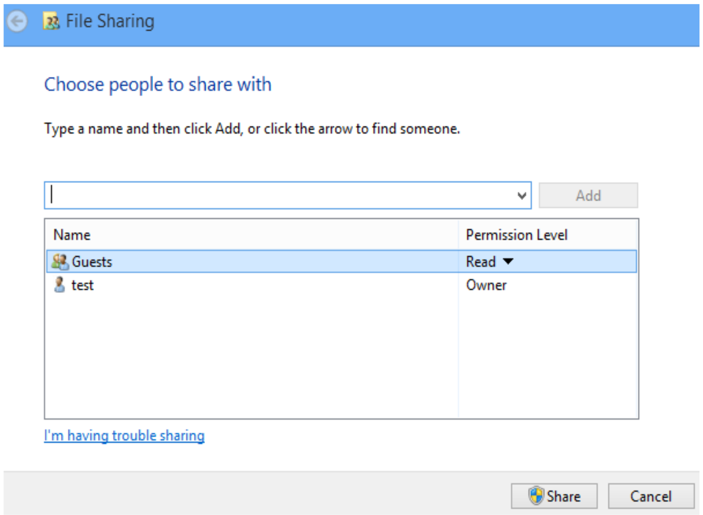


Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
test	Owner

6. To share without password, add "Guests" to the dialog, and press [Share] button



Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
Guests	Read ▾
test	Owner

- If you chose to use password, login/password dialog will appear.
- If you added "Guests", login/password dialog will not appear.

D. Connect two ends of crossover UTP CAT-5 cable to each NIC of the two computers.

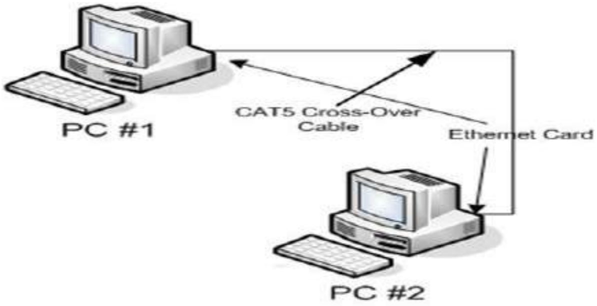


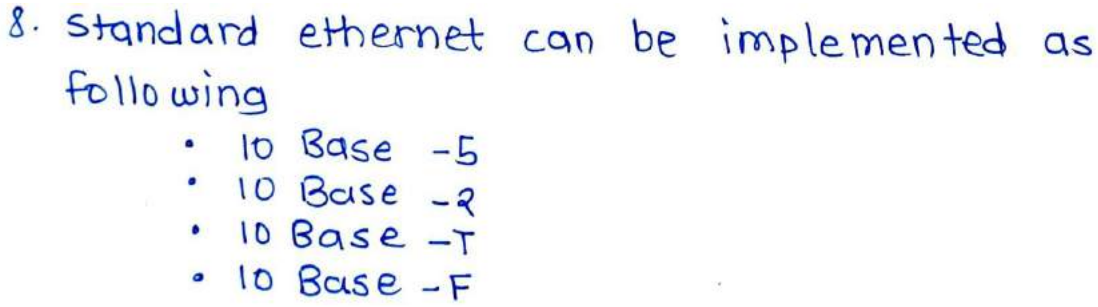
Fig.3 Implementation of LAN using UTP CAT-5 Cross over Cable.

Procedure:

1) Make sure both CPU should having Ethernet Card or NIC (Network Interface Card).
2) Connect two PC using UTP CAT-5 Cross over Cable.
3) Install the driver and configure the TCP/IP.
4) Check Connectivity between 2 PC by PING commands.

IV. CONCLUSION

1. Straight cat-5 wire is required to connect PC & switch.
2. Cross-over cat-5 cable is required between two switches for data communication.
3. Cross-over cable is required for direct PC to PC comm.
4. Function of network interface card driver can be defined by LLC layer of ISO-OSI set model.
5. Functions of LLC (logic link layer) are
   - Framing
   - flow control
   - Error detection & correction.
6. We are using full duplex switched ethernet technology for LAN communication where there is no use for CSMA/CD method. Each station is connected to the switch via separate links. Each station can send on receive independently without worrying about collision.
7. Ethernet evaluation are through Four generations
   - Standard ethernet (10Mbps)
   - Fast ethernet (100 Mbps)
   - Gigabit ethernet (1Gbps)
   - Ten Gigabit ethernet (10Gbps)



8. standard ethernet can be implemented as following
    - 10 Base -5
    - 10 Base -2
    - 10 Base -T
    - 10 Base -F

SIGNATURE

REFERENCES:

1. Data Communication. & Networking. B *Forouzan.*
2. Computer Networks' by Andrew Tannebaum.
3. https://en.wikipedia.org/wiki/Network_interface_controller.

PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE - 411043

Department of Electronics & Telecommunication

CLASS : BE (E&TC) **SUBJECT: CN**
EXPT. NO : - 02 **DATE :** 08-09-2020

I. **AIM:** Installation and configuration of the network application “FTP”.(Installation and Configuration of FTP Server).

II. **APPARATUS:** Bison FTP Server, PC connected in LAN.

III. **THEORY:** The **File Transfer Protocol** (See fig.1)is a standard network protocol used to transfer computer files between a client and server on a computer network. FTP works at the application layer of TCP/IP.

- File Transfer Protocol (FTP) powers one of the most fundamental Internet functions i.e. the transfer of files between computers.
- Today web developers use FTP protocols o upload/update their websites and download other information.
- Basic understanding about FTP process and software programs is important for every web developer.
- FTP is the prescribed method for the transfer of files between computers.
- It is also the easiest and most secure way to exchange files over internet.
- An FTP address looks a lot like an HTTP or website address but it uses the prefix “ftp://” instead of “http://”
- The most common use of FTP is to download files.
- FTP is vital to mp3 music sharing, most online auctions and game enthusiasts.
- The ability to transfer files quickly and reliably is essential for everyone creating and maintaining a web page.

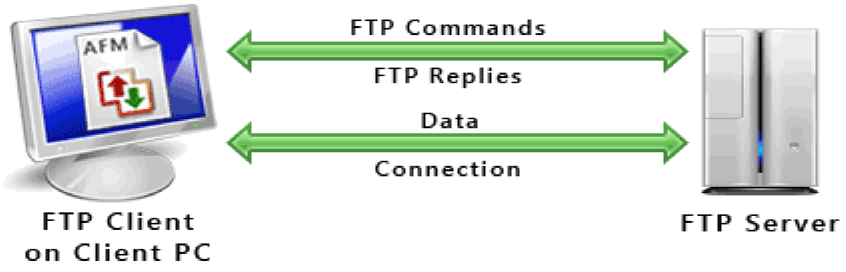


Fig.1 FTP Server.

Some basic FTP terms are:

1. Anonymous FTP:
   Transfer files from the public portion of an FTP server. Anonymous FTP is a method for giving users access to files so that they don't need to identify themselves to the server. Using an FTP program or the FTP command interface, the user enters "anonymous" as a user ID. Usually, the password is defaulted or furnished by the FTP server. Anonymous FTP is a common way to get access to a server in order to view or download files that are publicly available.

2. Archive:
   An FTP site that contains a selection of files for download.

3. Download:
   Also called ‘Get’. Copy a file from an FTP site to another computer. For merely downloading shared files, an anonymous account is usually sufficient. However, for downloading web pages for update a password and user privileges are usually required.

4. FTP site:
   A website that stores files for download. You can access the sites with a web browser by typing the address. All FTP sites begin with ftp://

5. Upload:
   Also called ‘Put’. Place files on a FTP server. Upload privileges are usually password protected to keep unauthorized users from placing files that could contain viruses or other malicious code on the server.

Practically using the ‘FTP’:

1. FTP is a core protocol in the IP world to quickly transfer files between your hard drive and a remote server.
2. Typically, a site on the internet stores a number of files (eg. Application executable, graphics, audio clips) and runs an FTP server application that waits for transfer requests.
3. To download a file to your system, you run an FTP client application that connects to the FTP server and request a file from a particular directory or folder.
4. Files can be uploaded to the FTP server, if appropriate access is granted.
5. FTP is a user level protocol for transferring files between host computers
6. An FTP sessions involves two separate connections:

Control connections:

- The server listens for client connections on port 21.

- The client opens a connection to the server port 21 on a client port above 1023
- The client uses this connection to send commands to and receive replies from the server.

This connection lasts through the FTP session.

Data connection:

- It is used for transferring data between client and server.
- A new data connection is opened for each FTP command.
- The way the connection is created depends on the type of FTP session- active or passive.

IV. BISON FTP SERVER

Some features of bison ftp server

1. This software is basically self-installing, simply move the executable to a directory of your choice. Run the application.

2. The server keeps all of its settings inside the window registry.

3. You can start and stop server directly from icon provided.

4. User groups are used to predefine the classes of users that will be allowed to sign onto this server.

5. For each group following options are allowed:

- Allow any password
- Enforce email address for password
- Manual authorization required
- Password retries allowed
- Home directory
- Uploads per session
- Downloads per session
- Maximum upload size
- Maximum download size
- Download/Upload ratio
- Ideal time out
- Permissions

6. These options specify the access that a user will have, to your file system.

7. You may set default access to all directories and then separate file access for any special directories e.g. allow read access to all of your hard drive except for a single upload directory.

8. Whenever you create a new user group, the'<default access>' entry is created automatically and cannot be deleted. To change the access permissions, use the check boxes to right of the permission of the list box.

9. To specify permissions for particular directories, add the directory path to the list box by pressing the button with the '>' symbol.

10. To remove a directory from the permissions list box, select it and press the button with the '<' symbol.

V. PROCEDURE:

1. Install and run the FTP server.
2. Set the default FTP drive.
3. Transfer files from FTP drive to client.
4. Transfer files from client to FTP drive.
5. Check the Port 21 to see if it has opened with the 'Netstar' command.
   Eg. C:> Netstar-n-a

VI. CONCLUSION:

1. FTP is the application layer protocol of TCP|IP
2. FTP is faster than HTTP but slower than NETBEUI
3. FTP is connection oriented service uses TCP as connection oriented protocol.
4. For file transfer application between two PC's TCP|IP should be available on both machines & FTP server should be ~~available~~ installed on one machine.
5. On FTP server machine TCP port 21 is opened when FTP server is running. This is verified using netstat -n-a command.

Signature

REFERENCES:

1. ‘Computer Networks’ by Andrew Tannebaum.
2. Data Communication. & Networking. B *Forouzan.*
3. ‘TCP/IP Illustrated volume’ by Stevens.
4. “Bison FTP Server” help files.

PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE - 411043

Department of Electronics & Telecommunication

CLASS : BE (E&TC) **SUBJECT: CN**
EXPT. NO : - 03 **DATE :** 15-09-2020

I. **AIM**: Installation and configuration of the network application ‘TELNET.

II. **APPARATUS:** BFTelnet software, PC connected in LAN.

III. **THEORY:** Telnet is an application layer protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

Telnet was developed in 1969 beginning with RFC 15, extended in RFC 854, and standardized as Internet Engineering Task Force (IETF) Internet Standard STD 8, one of the first Internet standards. Historically, Telnet provided access to a command-line interface (usually, of an operating system) on a remote host, including most network equipment and operating systems with a configuration utility (including systems based on Windows NT).[clarification needed] However, because of serious security concerns when using Telnet over an open network such as the Internet, its use for this purpose has waned significantly in favor of SSH.

The term telnet is also used to refer to the software that implements the client part of the protocol. Telnet client applications are available for virtually all computer platforms. Telnet is also used as a verb. To telnet means to establish a connection with the Telnet protocol, either with command line client or with a programmatic interface. For example, a common directive might be: "To change your password, telnet to the server, log in and run the passwd command." Most often, a user will be telnetting to a Unix-like server system or a network device (such as a router) and obtaining a login prompt to a command line text interface or a character-based full-screen manager.

Telnet(see fig.1) is a client-server protocol, based on a reliable connection-oriented transport. Typically, this protocol is used to establish a connection to Transmission Control Protocol (TCP) port number 23, where a Telnet server application (telnetd) is listening. Telnet, however, predates TCP/IP and was originally run over Network Control Program (NCP) protocols.

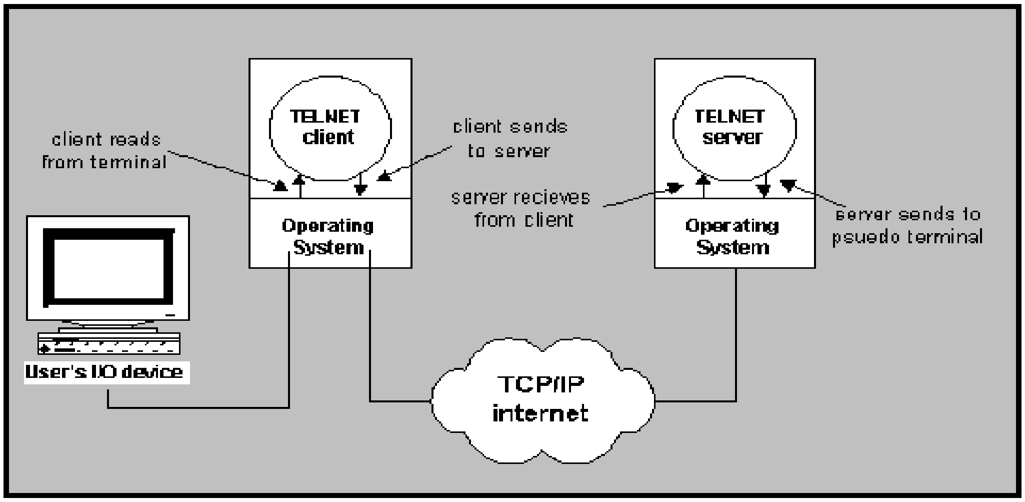


Fig.1Remote login using Telnet server

IV. BFTELNET.

BFTelnet primarily supports batch oriented program output. Full screen, interactive console applications are not supported. This limitation is due to the difference between UNIX and Windows console applications. Under UNIX, the interaction between an application and its terminal models the client/server paradigm where the application sends output as a byte stream to the terminal which in turn displays the output on behalf of the application. Hence, UNIX telnet sessions merely redirect the output to the telnet client. Under Windows, many console applications write directly to screen memory instead of the standard output device. Thus redirecting standard output fails to capture the display. Windows telnet servers that support full screen applications typically do so by continuously scanning screen memory and propagating changes to the telnet session. With this approach, screen updates may be lost if the scanning frequency is too low. However, CPU performance declines seriously with increased scanning frequency. BFTelnet has been designed to operate with a minimum impact on other applications and the operating system and therefore utilizes input / output redirection to support batch oriented program output.

The following are the feature of BFTelnet software.

- Ease of Use.
  BFTelnet accepts telnet connections from UNIX clients, Windows NT/2000/XP/2003, Windows 95/98, and others, right out of the box.
- No Connection Limits.
  Our licensing policy imposes no connection limits. You can maintain as many client connections to a single server as your hardware will support.
- Lightweight Design.
  The idle time RAM footprint of BFTelnet is approximately 100 Kilobytes. This makes BFTelnet unobtrusive and versatile. It operates with minimum impact on other applications.

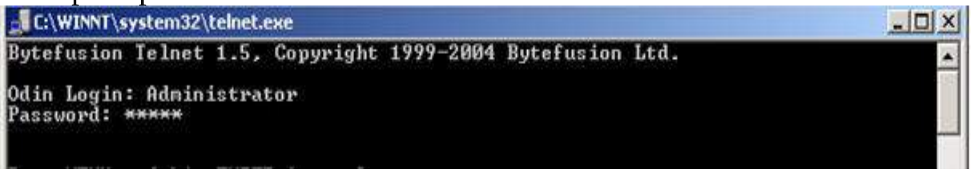
- True System Service.
  BFTelnet operates as a true NT/2000/XP system service - invisibly in the background. It is started automatically by the operating system at boot time and continues to operate after the user has logged off.
- Supports Standard Admin Tasks.
  BFTelnet features a system menu that allows administrators to carry out standard maintenance tasks conveniently and easily via a standard telnet session : start and stop system services, display active processes, reboot the system, view the application event log, and more.

V. PROCEDURE.

1. Install the Telnet server.

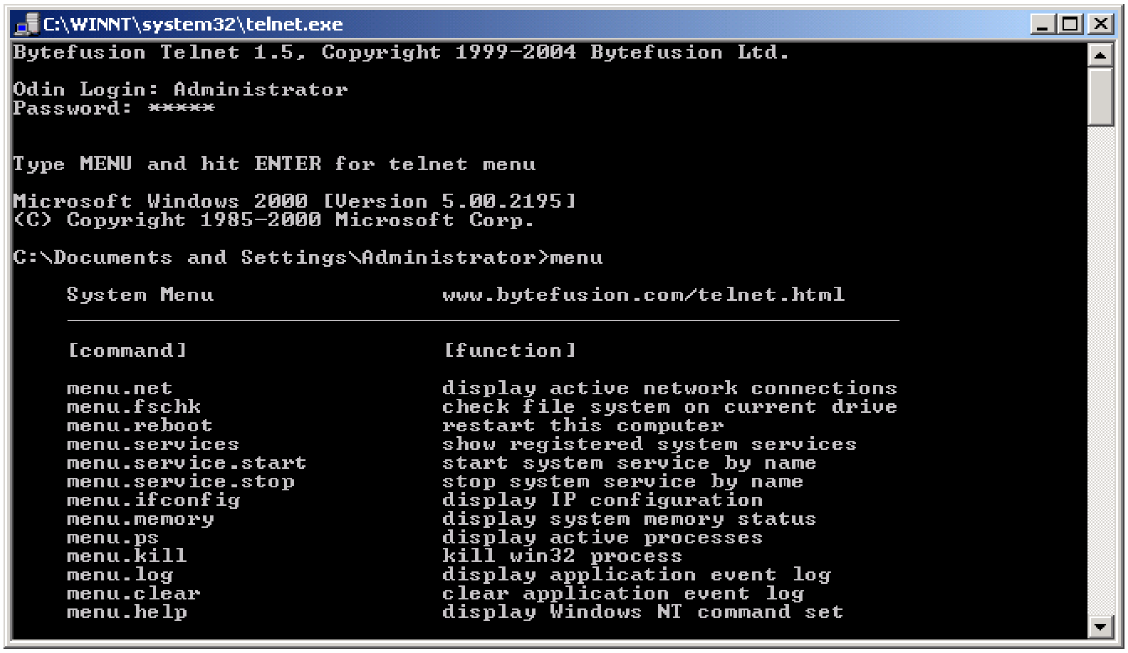
2. Check if port 23 has opened with the ‘Netstat’ command.

3. Establish telnet connection between client and Telnet server by running Telnet command at command prompt of client.



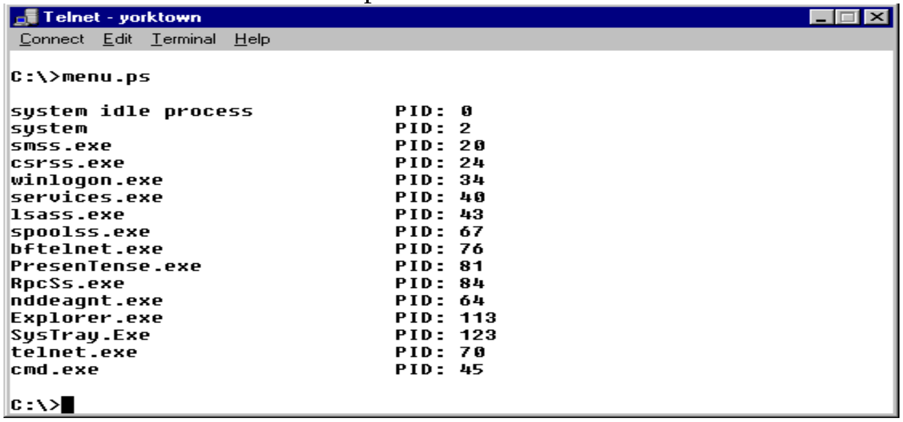
```
Bytefusion Telnet 1.5, Copyright 1999-2004 Bytefusion Ltd.

Odin Login: Administrator
Password: *****
```

4. Using menu.help, run the different DOS commands.



```
Bytefusion Telnet 1.5, Copyright 1999-2004 Bytefusion Ltd.

Odin Login: Administrator
Password: *****


Type MENU and hit ENTER for telnet menu

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>menu

    System Menu                 www.bytefusion.com/telnet.html
    ____________________________________________________________

    [command]                   [function]

    menu.net                    display active network connections
    menu.fschk                  check file system on current drive
    menu.reboot                 restart this computer
    menu.services               show registered system services
    menu.service.start          start system service by name
    menu.service.stop           stop system service by name
    menu.ifconfig               display IP configuration
    menu.memory                 display system memory status
    menu.ps                     display active processes
    menu.kill                   kill win32 process
    menu.log                    display application event log
    menu.clear                  clear application event log
    menu.help                   display Windows NT command set
```

5. Verify the different administrative tasks by entering different commands. Eg. Enter menu.reboot to reboot the remote computer.



```
C:\>menu.ps

system idle process            PID: 0
system                         PID: 2
smss.exe                       PID: 20
csrss.exe                      PID: 24
winlogon.exe                   PID: 34
services.exe                   PID: 40
lsass.exe                      PID: 43
spoolss.exe                    PID: 67
bftelnet.exe                   PID: 76
PresenTense.exe                PID: 81
RpcSs.exe                      PID: 84
nddeagnt.exe                   PID: 64
Explorer.exe                   PID: 113
SysTray.Exe                    PID: 123
telnet.exe                     PID: 70
cmd.exe                        PID: 45

C:\>█
```

6. Also, you can open different files on the remote machine like abc.doc, xyz.ppt, pqr.xls, etc.

VI. CONCLUSION

1. Telnet is application layer protocol of TCP|IP
2. Telnet is remote execution utility of TCP|IP
3. Telnet is connection oriented service uses TCP as connection oriented protocol.
4. For execution & working of telnet between two PC's TCP|IP should be available on both machines & telnet server should be installed on one machine.
5. On telnet server machine TCP port 23 is opened when Telnet server is running.
6. All menu commands are executed & verified practically.

SIGNATURE

REFERENCES

1. ‘Computer networks’ by Andrew Tannenbaum.
2. Data Communication. & Networking. B *Forouzan.*
3. ‘TCP/IP illustrated volume’ by Stevens.
4. ‘Byte fusion Telnet server help file.

CLASS : BE (E&TC) **SUBJECT: CN**
EXPT. NO : - 04 **DATE :** 01-09-2020

I. AIM : Installation and configuration of web-server.

II. APPARATUS: Abyss Web Server, PC connected in LAN.

III. THEORY: A Web service (See fig.1) is a service offered by an electronic device to another electronic device, communicating with each other via the World Wide Web. In a Web service, Web technology such as HTTP, originally designed for human-to-machine communication, is utilized for machine-to-machine communication, more specifically for transferring machine readable file formats such as XML(Extensible Markup Language) and JSON(JavaScript Object Notation). In practice, the Web service typically provides an object-oriented Web-based interface to a database server, utilized for example by another Web server, or by a mobile application, that provides a user interface to the end user. Another common application offered to the end user may be a mashup, where a Web server consumes several Web services at different machines, and compiles the content into one user interface.

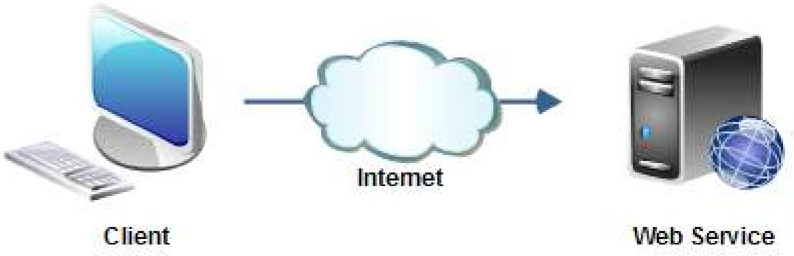


Fig.1 Web Service

A web server is a computer system that processes requests via HTTP, the basic network protocol used to distribute information on the World Wide Web. The term can refer to the entire system, or specifically to the software that accepts and supervises the HTTP requests.

Most web servers have features that allow you to do the following:

1. HTTP: every web server program operates by accepting HTTP requests from the client, and providing an HTTP response to the client. The HTTP response usually consists of an HTML document, but can also be a raw file, an image, or some other type of

document (defined by MIME-types); if some error is found in client request or while trying to serve the request, a web server has to send an error response which may include some custom HTML or text messages to better explain the problem to end users.

2. Logging: usually web servers have also the capability of logging some detailed information, about client requests and server responses, to log files; this allows the webmaster to collect statistics by running log analyzers on log files.
3. Authentication, optional authorization request (request ofuser name and password) before allowing access to some or all kind of resources.
4. Handling of not only static content (file content recorded in server's filesystem(s)) but of dynamic content too by supporting one or more related interfaces (SSI, CGI, SCGI, FastCGI, JSP, PHP, ASP, ASP .NET, Server API such as NSAPI,ISAPI, etc.).
5. HTTPS support (by SSL or TLS) to allow secure (encrypted) connections to the server on the standard port 443 instead of usual port 80.
6. Content compression (i.e. by gzip encoding) to reduce the size of the responses (to lower bandwidth usage, etc.).
7. Virtual hosting to serve many web sites using one IP address.
8. Large file support to be able to serve files whose size is greater than 2 GB on 32 bit OS.
9. Bandwidth throttling to limit the speed of responses in order to not saturate the network and to be able to serve more clients.

IV. WHAT IS ABYSS WEB SERVER?

Abyss Web Server turns your computer in a full-featured web server. People all over the Internet can view documents, download graphics, listen to music and view movies hosted on it. Abyss Web Server was designed with both novice and experimented users in mind. That’s why it is easy to use and incredibly powerful.

Abyss Web Server exists in two editions:

• Abyss Web Server X1: Free personal edition. It is fully functional software with no limitations, no nag screens, no spyware, and no advertisements.

• Abyss Web Server X2: Professional edition. It is suitable for demanding users and medium to high loaded web sites. It supports virtual hosting, dual hosts (HTTP+HTTPS), and advanced features. For more information, visit http://www.aprelium.com/abyssws/x2

1. System requirements.

Abyss Web Server is a multiplatform software designed for Microsoft Windows 95, 98, Millennium Edition (ME), as well as all editions of 2000, XP, 2003, Vista, 7, 2008, 8, 8.1, 2012, and 10; Mac OS X 10.2 and higher; and Linux (Kernel 2.4 and higher) systems. It is compatible with both 32 and 64-bit architectures and operating systems.

This guide documents the Windows version. Abyss Web Server for Windows minimum requirements are:

- An Intel 80486 processor at 33 MHz.
- 4 Mb of free RAM.
- A modern web browser with HTML 5.0 support. Legacy web browsers (graphical or text-based) can still be used but the user experience will be partially degraded.
- TCP/IP protocol stack installed. Although Abyss Web Server can run on a standalone computer, it is recommended to have a Modem or a network card and to be connected to a LAN (Local Area Network) or to the Internet.

2. What is the console?

The console is a remote web based configuration and monitoring system. With the console, you can:

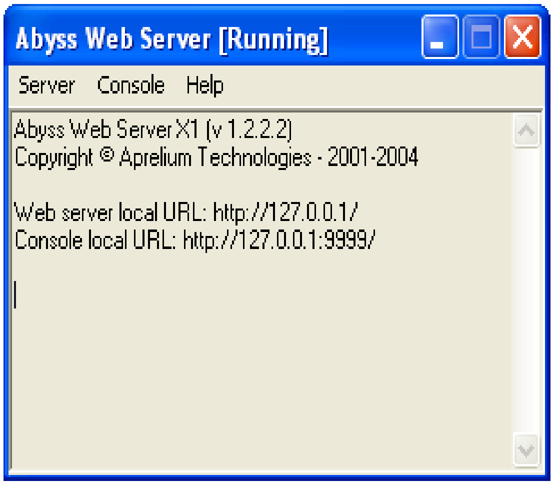
- Configure Abyss Web Server.
- Stop, run and shutdown the web server.
- View the web server's access statistics.
- Read the documentation.

3. Server Status

Open the console and select 'server status'. The console displays the current status of the server. To change it, press one of the following buttons:

: It can be Running (see fig.2), Stopped, or Error when the host cannot be started because of a configuration error; in such a case, click Error to have detailed information about the problem.

- A Start or Stop button.
- A Configure to access the host configuration dialog.



```
Abyss Web Server X1 (v 1.2.2.2)
Copyright © Aprelium Technologies - 2001-2004

Web server local URL: http://127.0.0.1/
Console local URL: http://127.0.0.1:9999/
```

Fig.2 Server Status

V. PROCEDURE:

1. Installing/Upgrading the software

To setup Abyss Web Server:

- Open the directory where you have saved the software package.
- Double-click on the software package icon.
- If an old version of Abyss Web Server is already installed on your computer, you may be asked to uninstall it. All you have to do is to follow the on-screen instructions. IMPORTANT NOTICE: When the uninstaller asks you to confirm the deletion of the installation directory, select No.
- Read carefully the license agreement. If you agree with it, press I Agree. If you do not, press Cancel and delete Abyss Web Server package from your computer.
- Deselect components you do not want to install. Auto Start enables Abyss Web Server auto starting when a Windows session starts. Start Menu Shortcuts enables adding Abyss Web Server shortcuts in the Start Menu.
- Press Next.
- Choose a directory where you want to install Abyss Web Server files. From now on, <Abyss Web Server directory> will refer to this directory.
- Press Install.

After installing, you will be asked if you want to launch Abyss Web Server. If you press No, you should press Close to close the setup program.

2. Setting up a web site

Using your favorite web pages editor (also known as HTML editor), create a web site and put its files in the directory <Abyss Web Server directory>/htdocs. The index files must be called index.html or index.htm.

Other computers on the network can access your web site if they browse http://<your host name>:<host port>. <your host name> is the host name of your computer or its IP address. Ask your network's administrator for this information. If you want to connect to the server from the computer it runs on, you can also use 127.0.0.1, ::1, or localhost.<host port> is the number of the port the server waits for connections on. It is printed on the server's window or terminal. If <host port> is 80 (which is the default), it can be omitted from the URL and the web server can be accessed with only http://<your host name>.

VI. CONCLUSION

1. Hosting of webpage or website can be done with the help of web server.
2. This web server is also called as http server
3. For doing this experiment web server & web browser are required.
4. For hosting site abbys web server is installed on one machine & browsing is done.
5. For communication between web server & web browser TCP/IP should be present on both machines.

SIGNATURE

REFERENCES:

1. The Web Server Book: Tools & Techniques for Building Your Own Internet by Douglas Matthews, Jonathan Magid, and Paul Jones
2. Data Communication. & Networking. B *Forouzan.*
3. Computer Networks' by Andrew Tannebaum.

PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE - 411043

Department of Electronics & Telecommunication

CLASS : BE (E&TC) **SUBJECT: CN**
EXPT. NO : 05 **DATE :** 22-09-2020

I. AIM : Installation and Configuration of DHCP Server

II. APPARATUS: DHCP 2.2 Software, PC connected in LAN.

III. THEORY: Dynamic Host Configuration Protocol (DHCP) is a standard protocol that allows a server to dynamically distribute IP addressing and configuration information to clients. Normally the DHCP server provides the client with at least this basic information: IP Address**,** Subnet Mask**,** and Default Gateway
Other information can be provided as well, such as Domain Name Service (DNS) server addresses and Windows Internet Name Service (WINS) server addresses. The system administrator configures the DHCP server with the options that are parsed out to the client.

Every device on a TCP/IP-based network must have a unique unicast IP address to access the network and its resources. Without DHCP, IP addresses for new computers or computers that are moved from one subnet to another must be configured manually; IP addresses for computers that are removed from the network must be manually reclaimed. With DHCP, this entire process is automated and managed centrally. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts up on the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

The network administrator establishes DHCP servers that maintain TCP/IP configuration information and provide address configuration to DHCP-enabled clients in the form of a lease offer. The DHCP server stores the configuration information in a database that includes:

- Valid TCP/IP configuration parameters for all clients on the network.
- Valid IP addresses, maintained in a pool for assignment to clients, as well as excluded addresses.
- Reserved IP addresses associated with particular DHCP clients. This allows consistent assignment of a single IP address to a single DHCP client.
- The lease duration, or the length of time for which the IP address can be used before a lease renewal is required.

A. Benefits of DHCP.

DHCP Server service provides the following benefits:

- Reliable IP address configuration. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.
- Reduced network administration. DHCP includes the following features to reduce network administration:
  - Centralized and automated TCP/IP configuration.
  - The ability to define TCP/IP configurations from a central location.
  - The ability to assign a full range of additional TCP/IP configuration values by means of DHCP options.
  - The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable computers that move to different locations on a wireless network.
  - The forwarding of initial DHCP messages by using a DHCP relay agent, which eliminates the need for a DHCP server on every subnet.

B. DHCP operations.

DHCP operations fall into four phases (See fig.1): server discovery, IP lease offer, IP lease request, and IP lease acknowledgement. These stages are often abbreviated as DORA for discovery, offer, request, and acknowledgement.

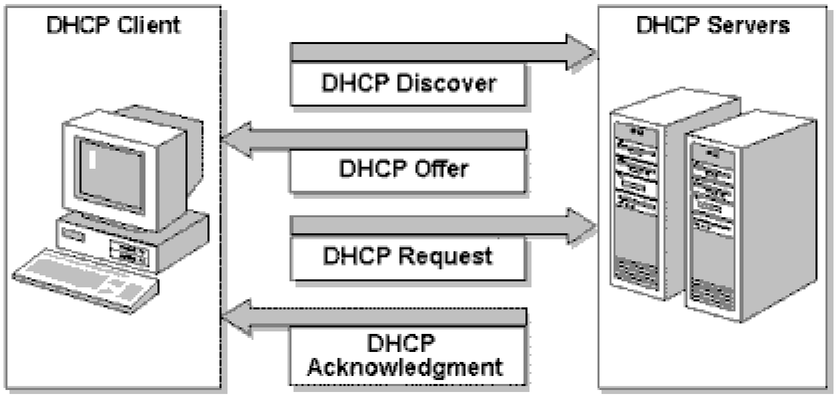


Fig.1 DHCP Operation

1. **DHCP discovery.**

The client broadcasts messages on the network subnet using the destination address 255.255.255.255 or the specific subnet broadcast address. A DHCP client may also request its last-known IP address. If the client remains connected to the same network, the server may grant the request. Otherwise, it depends whether the server is set up as authoritative or not. An authoritative server denies the request, causing the client to issue a new request. A non-authoritative server simply ignores the request, leading to an implementation-dependent timeout for the client to expire the request and ask for a new IP address.

2. **DHCP offer.**

When a DHCP server receives a DHCPDISCOVER message from a client, which is an IP address lease request, the server reserves an IP address for the client and makes a lease offer by sending a DHCPOFFER message to the client. This message contains the client's MAC address, the IP address that the server is offering, the subnet mask, the lease duration, and the IP address of the DHCP server making the offer.

3. **DHCP Request.**

In response to the DHCP offer, the client replies with a DHCP request, broadcast to the server requesting the offered address. A client can receive DHCP offers from multiple servers, but it will accept only one DHCP offer. Based on required *server identification* option in the request and broadcast messaging, servers are informed whose offer the client has accepted. When other DHCP servers receive this message, they withdraw any offers that they might have made to the client and return the offered address to the pool of available addresses.

4. **DHCP acknowledgement.**

When the DHCP server receives the DHCPREQUEST message from the client, the configuration process enters its final phase. The acknowledgement phase involves sending a DHCPACK packet to the client. This packet includes the lease duration and any other configuration information that the client might have requested. At this point, the IP configuration process is completed.

C. The DHCP Lease Process.

The first time a DHCP-enabled client starts and attempts to join the network, it automatically follows an initialization process to obtain a lease from a DHCP server. Figure .2 shows the lease process.

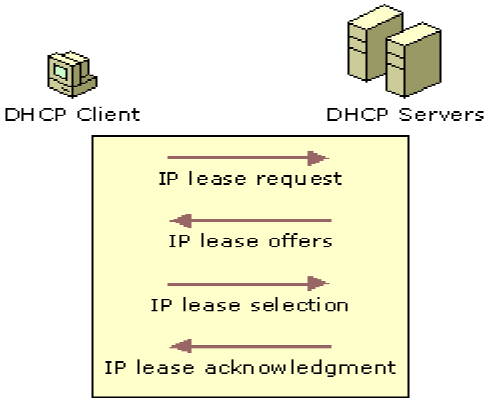


Figure .2 The DHCP Lease Process

1. The DHCP client requests an IP address by broadcasting a DHCP Discover message to the local subnet.
2. The client is offered an address when a DHCP server responds with a DHCP Offer message containing an IP address and configuration information for lease to the client. If no DHCP server responds to the client request, the client can proceed in two ways:
   - If it is a Windows 2000–based client, and IP auto-configuration has not been disabled, the client self-configures an IP address for its interface.
   - If the client is not a Windows 2000–based client, or IP auto-configuration has been disabled, the client network initialization fails. The client continues to resend DHCP Discover messages in the background (four times, every 5 minutes) until it receives a DHCP Offer message from a DHCP server.
3. The client indicates acceptance of the offer by selecting the offered address and replying to the server with a DHCP Request message.
4. The client is assigned the address and the DHCP server sends a DHCPAck message, approving the lease. Other DHCP option information might be included in the message.
5. Once the client receives acknowledgment, it configures its TCP/IP properties using any DHCP option information in the reply, and joins the network.

IV. PROCEDURE:

1) Install and configure the DHCP Server on one machine in LAN.

- DHCP extract content from zip file
  1. Dhcp.exe //dhcp server program
  2. Dhcpwiz.exe //configuration program
  3. Readme.txt //help
  4. wwwroot //Directory with basic web file
- Start DHCP wizard first (Dhcpwiz.exe) steps encountered.
  1. Welcome to DHCP configuration wizard.
  2. Network interface card

     Choose an interface from the list of all currently identify network interface on your computer.

3. Supported protocol
   Select TCP/IP to be activated, enable HTTP
4. Configuring DHCP for interface: Define the pool of IP address
5. Writing the INI file
   Which contains all the configuration options; it should be placed into same folder as dhcpsrv.
6. DHCP configuration completed.
7. Run the dhcpsrv.exe
8. Check the DHCP server work as expected.

2. Take another client; enable the following option in TCP/IP properties.

a. Click Start, click Control Panel, and then double-click Network Connections.
b. Right-click Local Area Connection and then click Properties.
c. Click Internet Protocol (TCP/IP), and then click Properties.
d. Select obtain the IP address automatically.

And reboot system.

3. Thus the IP address is automatically allocated to client by installed DHCP Server on LAN.

VI. CONCLUSION

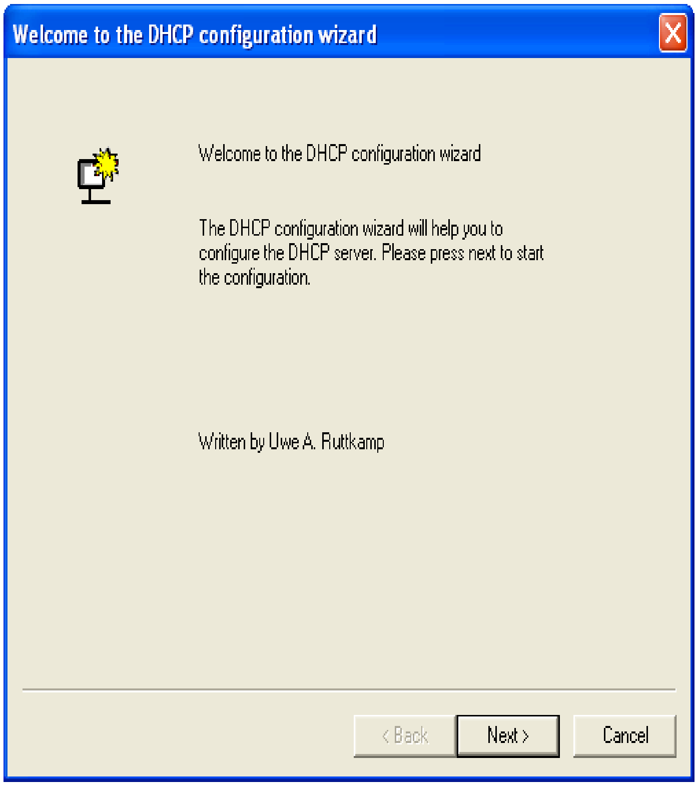
1. The IP address range specified in IP pool option of DHCP server config. is allocated to the DHCP client.
2. Default gateway & DNS setting done at the DHCP server configuration can be as it is forwarded to DHCP enabled clients.
3. IP address allocated by DHCP server to DHCP client is practically observed by entering command. IP config./ All on command prompt of client.

SIGNATURE

REFERENCES:

1. Data Communication. & Networking. B *Forouzan.*
2. Computer Networks’ by Andrew Tannebaum.
3. https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

DHCP SERVER SIDE CONFIGURATION

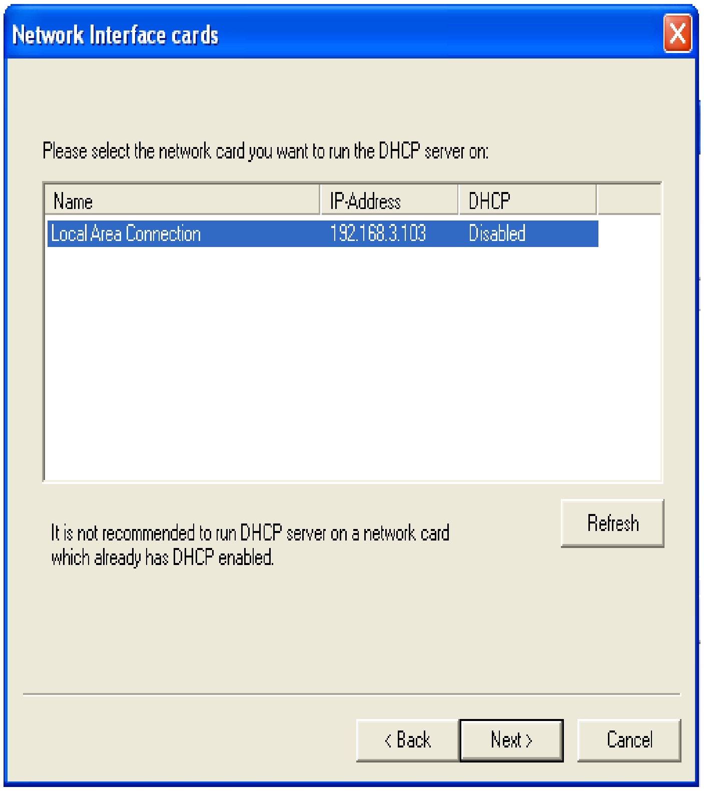


Welcome to the DHCP configuration wizard

Welcome to the DHCP configuration wizard

The DHCP configuration wizard will help you to configure the DHCP server. Please press next to start the configuration.

Written by Uwe A. Ruttkamp



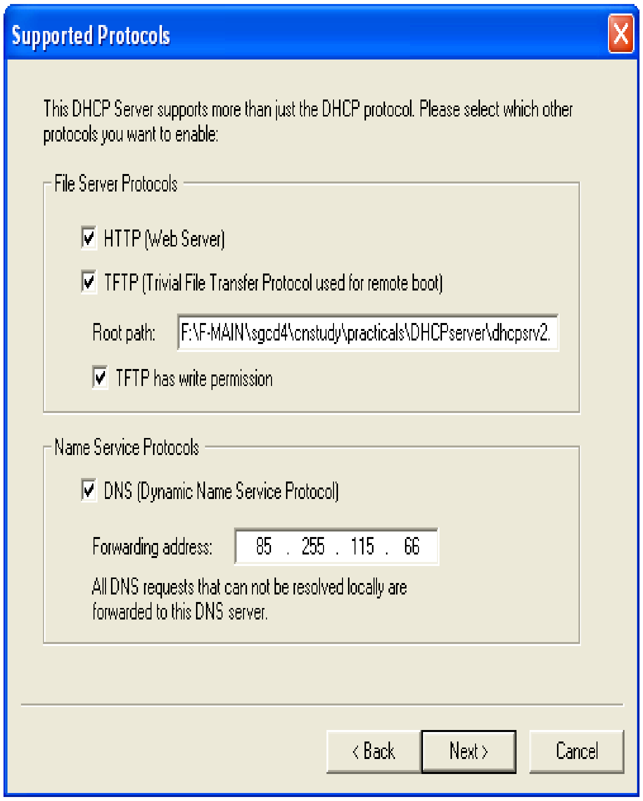
Network Interface cards

Please select the network card you want to run the DHCP server on:

Name	IP-Address	DHCP
Local Area Connection	192.168.3.103	Disabled

It is not recommended to run DHCP server on a network card which already has DHCP enabled.

DHCP SERVER SIDE CONFIGURATION



This DHCP Server supports more than just the DHCP protocol. Please select which other protocols you want to enable:

File Server Protocols

☑ HTTP (Web Server)

☑ TFTP (Trivial File Transfer Protocol used for remote boot)

Root path: F:\F-MAIN\sgcd4\cnstudy\practicals\DHCPserver\dhcpsrv2.

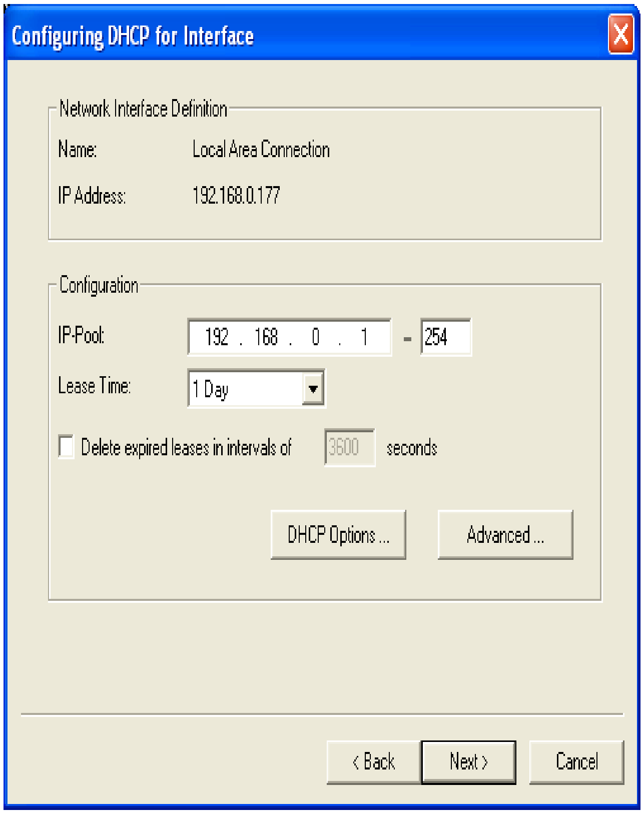
☑ TFTP has write permission

Name Service Protocols

☑ DNS (Dynamic Name Service Protocol)

Forwarding address: 85 . 255 . 115 . 66

All DNS requests that can not be resolved locally are forwarded to this DNS server.



Network Interface Definition

Name: Local Area Connection

IP Address: 192.168.0.177

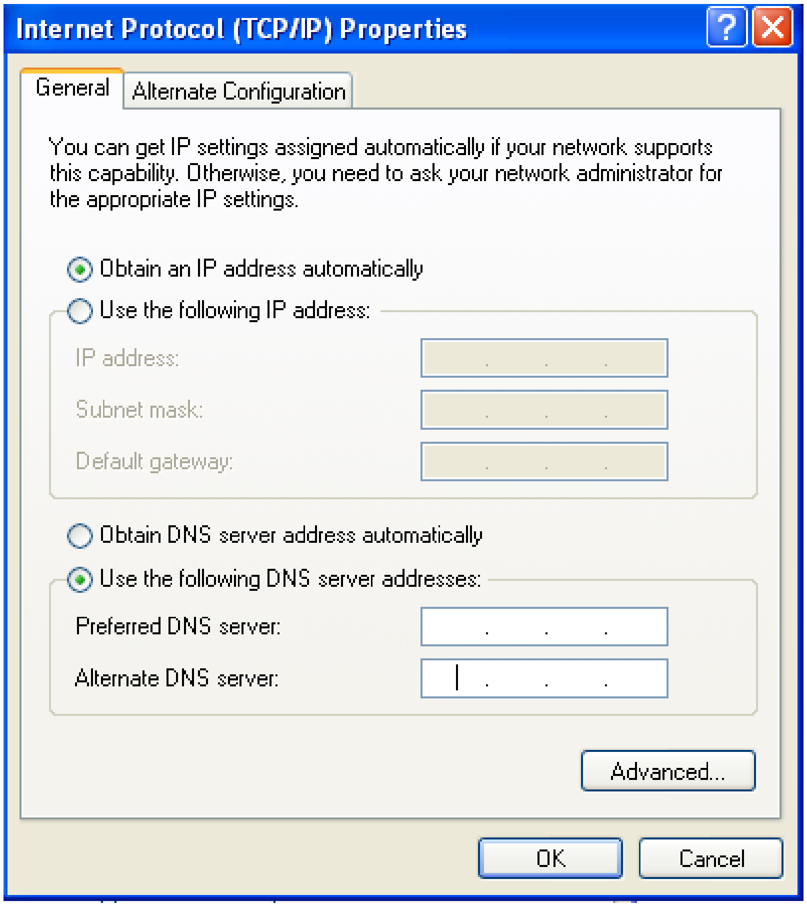
Configuration

IP-Pool: 192 . 168 . 0 . 1 - 254

Lease Time: 1 Day

☐ Delete expired leases in intervals of 3600 seconds

Client side enable the first option, Obtained an IP address automatically. Thus, reboot the system and IP address will be allocated to required client automatically in range specified in IP-Pool option of DHCP server configuration.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

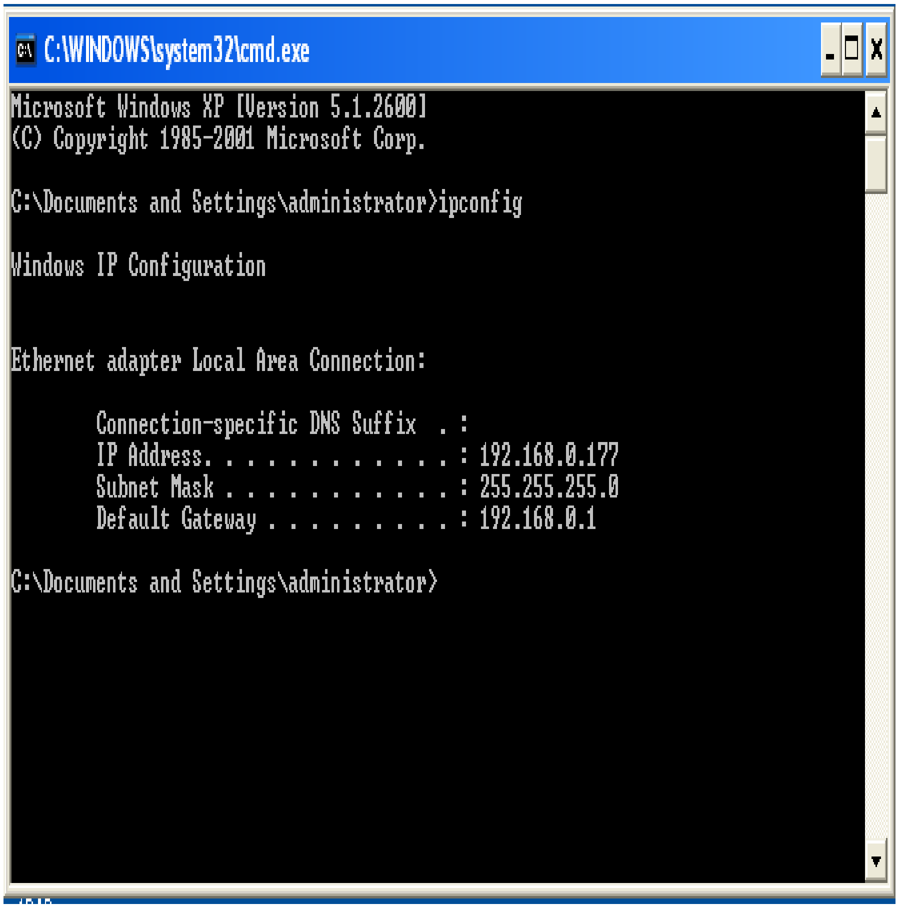
Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.0.177
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1

C:\Documents and Settings\administrator>
```

PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE - 411043

Department of Electronics & Telecommunication

CLASS : BE (E&TC) **SUBJECT: CN**
EXPT. NO : 06 **DATE :** 10-11-2020

I. AIM: Study of Network Protocol Analyzer

II. APPARATUS: Wireshark and Telnet Software, PC connected in LAN.

III. Theory:

A network protocol analyzer is a vital part of network administrator’s toolkit. Network protocol analysis is the truth serum of network communications. If you want to find out why a network device is functioning in a certain way, use a protocol analyser to sniff the traffic and expose the data and protocols that pass along the wire. You can use a network protocol analyser to

- Troubleshoot hard-to-solve problems.
- Detect and identify malicious software(malware).
- Gather information, such as baseline traffic patterns and network-utilization metrics.
- Identify unused protocols so that you can remove them from the network.
- Generate traffic for penetration testing.
- Work with an Intrusion Detection System(IDS) or a honeypot.
- Eavesdrop on traffic(e.g., locate unauthorized Instant Messaging--IM—traffic or wireless Access Points—APs).
- Learn about networking.

If you manage a network and don’t yet have a protocol analyser, you need one.

Detect network protocols

Network Protocol analyser will let you see all the network protocols being used on your network. It will show you the protocol names, ports, and descriptions, the amount of traffic seen, as well as the bandwidth used by each protocol.

You can drill down further into each and every protocol entry found to see which hosts and conversations are using them and how much.

See who is using your network

See detailed statistics of where each host is sending and receiving traffic on your network. Network Protocol Analyzer will show you host names, IP addresses, packets and bytes transmitted and received, the number of protocol used by each host, the number of conversation each host has participated in, and the bandwidth usage foe each one.

You can drill down further into each host entry found to see which protocols they have used and which conversations they have participated in.

See conversations on your network

You can see statistics of where each host is receiving data from or transmitting data to. Network Protocol analyser will collect source and destination host names and IP addresses for each conversation taking place on your network, as well as the number of packets and bytes transmitted, and the bandwidth usage for each conversation. You can drill down further into each conversation entry to see which protocols they have used.

Network card statistics

See detailed statistics for each network interface on your network segment. Network Probe will display the MAC address, IP address, host name, and vendor for each card, ad well as the amount of traffic received or transmitted, unicast, multicast, and broadcast. You can drill down further to see each network card conversation taking place.

Network segment overview

See the throughput for the entire network and the amount of traffic sent with different packet sizes.

Technical features of Network Protocol Analyzer

Wireshark is used by network professionals around the world for troubleshooting, analysis, software and protocol development, and education. It has all of the standard features you would expect in a protocol analyser, and several features not seen in any other product. Its open source license allows talented experts in the networking community to add enhancements. It runs on all popular computing platforms, including Unix, Linux, and Windows.

Wireshark is still technically beta software, but it has a comprehensive feature set and is suitable for production use. Here is a list of features, current as of version 0.9.14, in no particular order

- Data can be captured “off the wire” from a live network connection, or read from a capture file.
- Wireshark can read capture files from tcpdump (libpcap), NAI’s Sniffer(compressed and uncompressed),Sniffer Pro, NetXray, Sun snoop and atmsnoop, Shomiti/Finisar Surveyor, AIX’s iptrace, Microsoft’s Network Monitor, Novell’s LANalyzer, RADCOM’s WAN/LAN Analyzer, HP-UX nettl, i4btrace from the ISDN4BSD project,

Cisco Secure IDS iplog, the pppd log(pppdump-format), the AG Group's/WildPacket's, EtherPeek/TokenPeek/AiroPeek, or Visual Network Visual UpTime. It can also read traces made from Lucent/Ascend WAN routes and Toshiba ISDN routers, as well as the text output from VMS's TCPIPtrace utility and the DBS Etherwatch utility for VMS. Any of these files can be compressed with gzip and Wireshark will decompress them on the fly.

- Live data can be read from Ethernet, FDDI, PPP, Token-Ring, IEEE 802.11, Classical IP over ATM, and loopback interfaces(at least on some platforms; not all of those types are supported on all platforms).
- Captured network data can be browsed via a GUI, or via the TTY-mode "tethereal" program.
- Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.
- 759 protocols can currently be dissected in Wireshark protocol Analyzer.
- Output can be saved or printed as plain text or PostScript.
- Data display can be refined using a display filter.
- summary information.
- All or part of each captured network trace can be saved to disk.

Display filters can also be used to selectively highlight and colour packet

Some intended purposes:

Here are some examples people use Wireshark for:

- Network administrators use it to troubleshoot network problems.
- Network security engineers use it to examine security problems.
- Developers use it to debug protocol implementations.
- People use it to learn network protocol internals.

Besides these examples, Wireshark can be helpful in many other situations too.

The following are some of the many features Wireshark provides:

- Available for UNIX and Windows.
- Capture live data packets from a network interface.
- Display packets with very detailed protocol information.
- Open and save packet data captured.
- Import and Export packet data from and to a lot of other capture programs.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Colorize packet display based on filters.

- Create various statistics.

However, to really appreciate its power, you have to start using it. “Wireshark captures packets and allows you to examine their content.” Shows Wireshark having captured some packets and waiting for you to examine them.

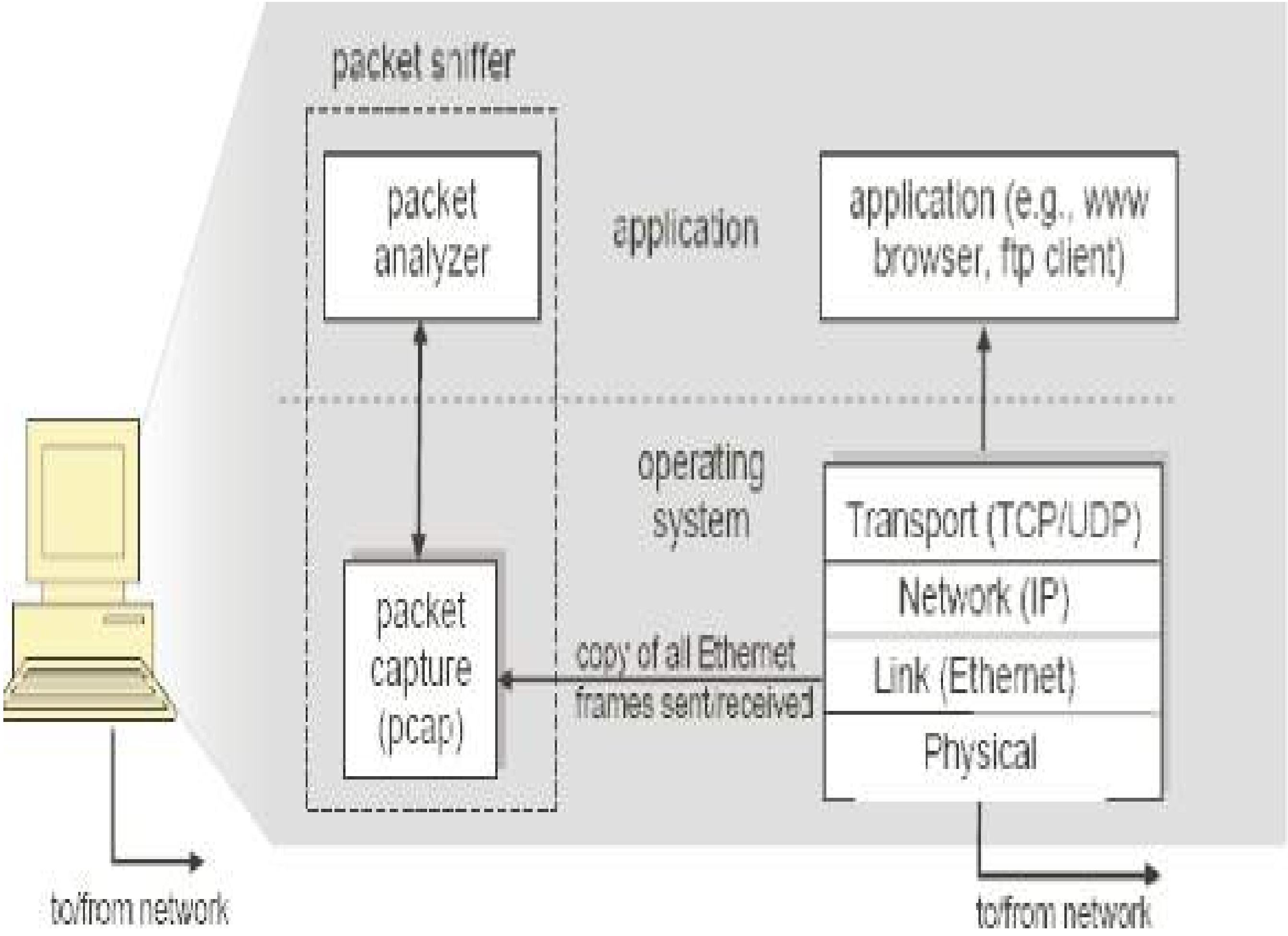


Figure 1. Network Protocol Analyzer Structure

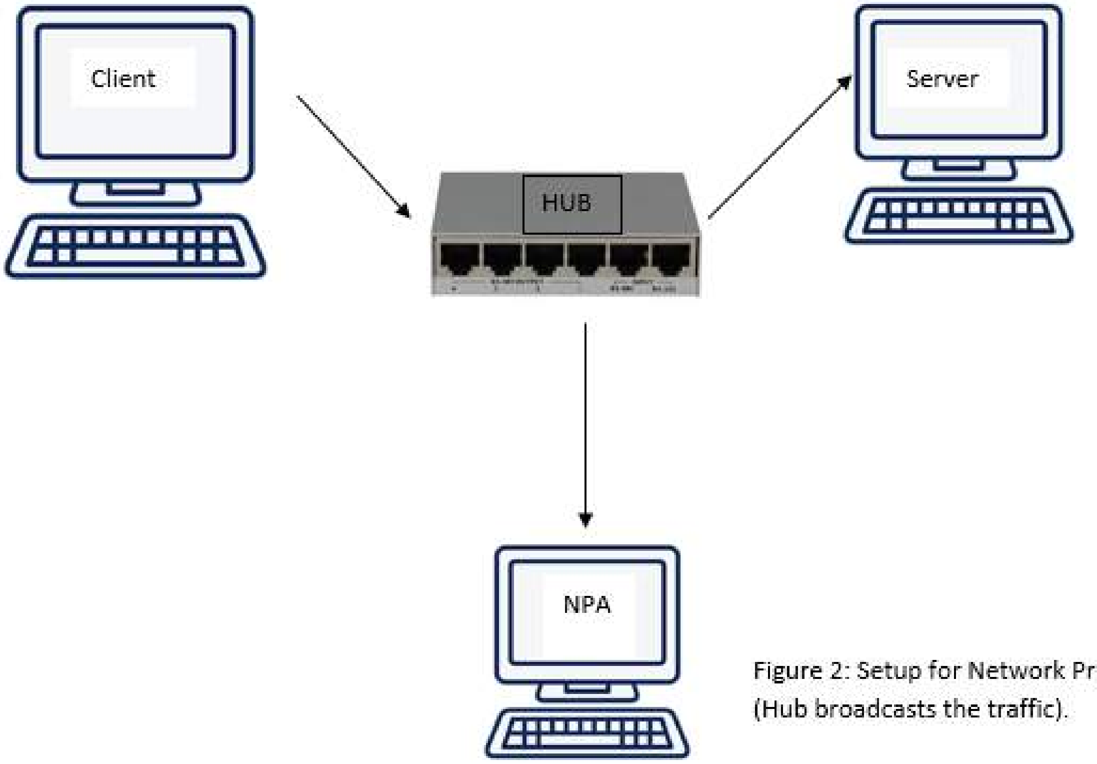


Figure 2: Setup for Network Protocol Analysis. (Hub broadcasts the traffic).

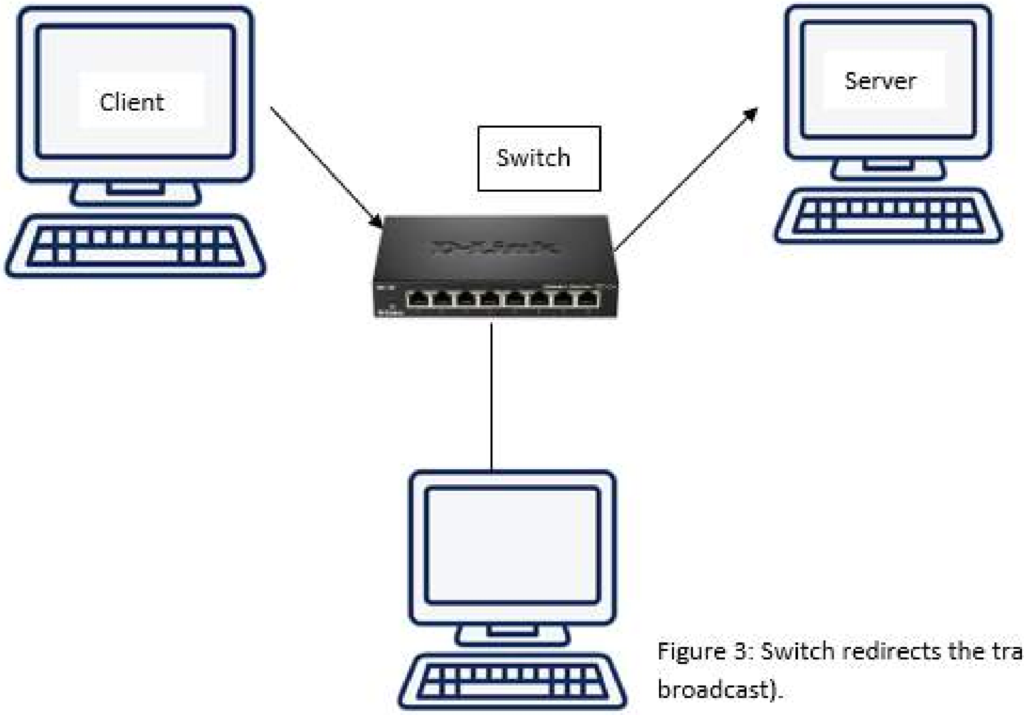


Figure 3: Switch redirects the traffic (Doesn't broadcast).

IV. Procedure:

1. Install the Wireshark Network Protocol analyser on the machine
2. Run the Wireshark program, so that Menu Bar, Button Bar, Pane 1, Pane 2, Pane 3 and status bar will be observed.
3. Click the capture option and capture the data on required interface in promiscuous mode.
4. From another machine generate the Telnet traffic as shown in the figure and capture it using Wireshark protocol analyser.The captured frame gives the details of the password captured.
5. Also from another machine generate the ping traffic as shown in the figure and capture it using Wireshark protocol analyser.The captured frame gives the ICMP protocol details.
6. Flow graph option can be used by clicking the statistics option on Menu bar. This option gives the details of communication(IP address, Port address details) signals in graphical form.

V. CONCLUSION:

1. It is passive tool & does not generate network traffic.
2. It is not a network mentoring software.
3. It shows details in Foundation about protocols.
4. Shifting process of password using wire shark protocol analyzer is practically verified.
5. Statistically properties of traffic is shown by clicking summary sub option of statistics option available on menu bar.
6. Flow graphs option gives the details of communication s/w different nodes in graphical form.

7. Filter are essential option which is used & practically verified during telnet & ping application traffic.

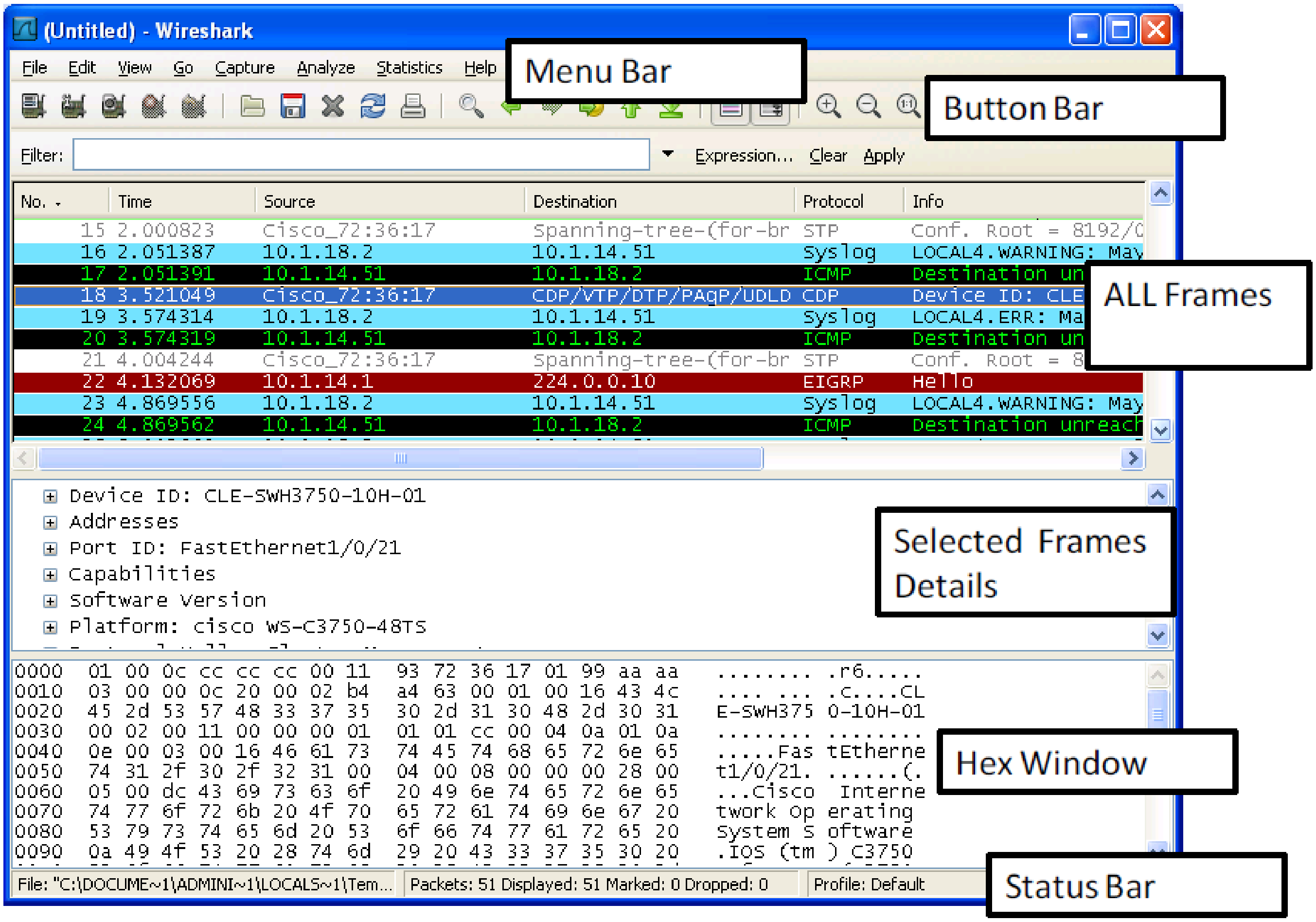
8. Thus detail traffic analysis can be done using this wire shark protocol analyzer.

SIGNATURE

REFERENCES:

1. Data Communication. & Networking. B *Forouzan.*
2. Computer Networks' by Andrew Tannebaum.
3. https://en.wikipedia.org/wiki/Network_interface_controller.

With traffic…

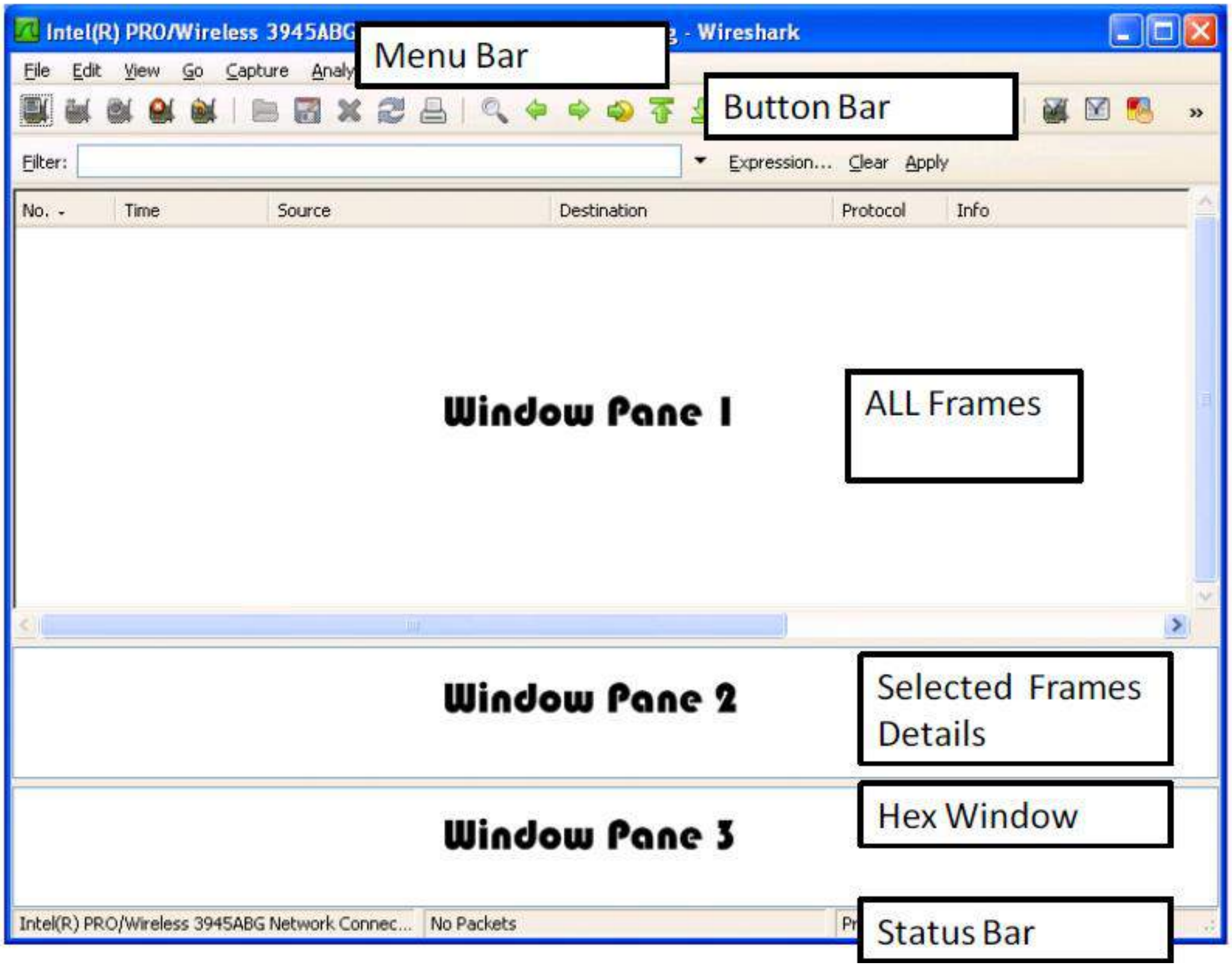


```
No. .  Time      Source             Destination            Protocol  Info
   15 2.000823  Cisco_72:36:17     Spanning-tree-(for-br  STP       Conf. Root = 8192/C
   16 2.051387  10.1.18.2          10.1.14.51             Syslog    LOCAL4.WARNING: May
   17 2.051391  10.1.14.51         10.1.18.2              ICMP      Destination un
   18 3.521049  Cisco_72:36:17     CDP/VTP/DTP/PAgP/UDLD  CDP       Device ID: CLE
   19 3.574314  10.1.18.2          10.1.14.51             Syslog    LOCAL4.ERR: Ma
   20 3.574319  10.1.14.51         10.1.18.2              ICMP      Destination un
   21 4.004244  Cisco_72:36:17     Spanning-tree-(for-br  STP       Conf. Root = 8
   22 4.132069  10.1.14.1          224.0.0.10             EIGRP     Hello
   23 4.869556  10.1.18.2          10.1.14.51             Syslog    LOCAL4.WARNING: May
   24 4.869562  10.1.14.51         10.1.18.2              ICMP      Destination unreach
```

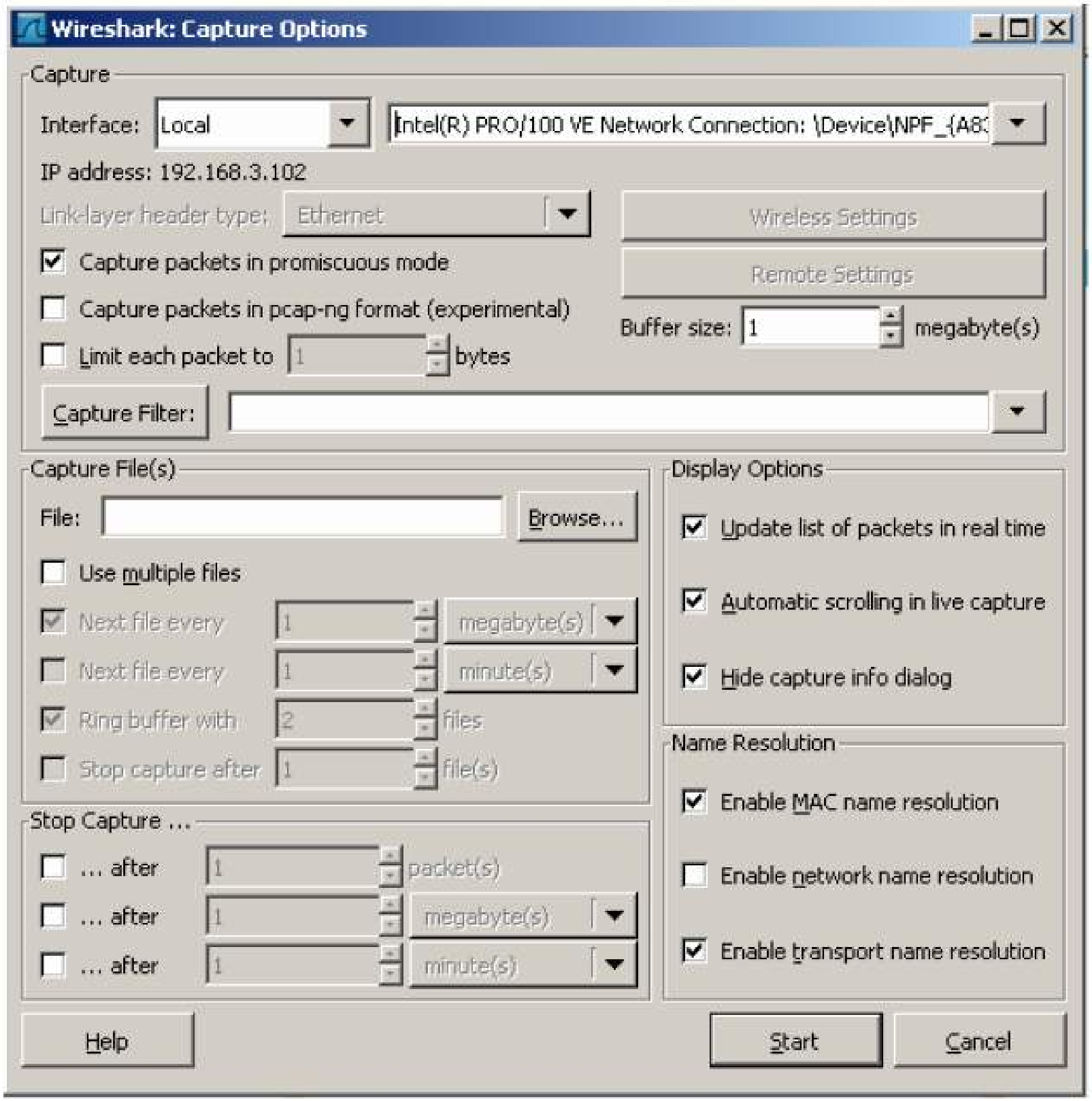
```
⊞ Device ID: CLE-SWH3750-10H-01
⊞ Addresses
⊞ Port ID: FastEthernet1/0/21
⊞ Capabilities
⊞ Software Version
⊞ Platform: cisco WS-C3750-48TS
```

```
0000  01 00 0c cc cc cc 00 11  93 72 36 17 01 99 aa aa   ........ .r6.....
0010  03 00 00 0c 20 00 02 b4  a4 63 00 01 00 16 43 4c   .... ... .c....CL
0020  45 2d 53 57 48 33 37 35  30 2d 31 30 48 2d 30 31   E-SWH375 0-10H-01
0030  00 02 00 11 00 00 00 01  01 01 cc 00 04 0a 01 0a   ........ ........
0040  0e 00 03 00 16 46 61 73  74 45 74 68 65 72 6e 65   .....Fas tEtherne
0050  74 31 2f 30 2f 32 31 00  04 00 08 00 00 00 28 00   t1/0/21. ......(.
0060  05 00 dc 43 69 73 63 6f  20 49 6e 74 65 72 6e 65   ...Cisco  Interne
0070  74 77 6f 72 6b 20 4f 70  65 72 61 74 69 6e 67 20   twork Op erating
0080  53 79 73 74 65 6d 20 53  6f 66 74 77 61 72 65 20   System S oftware
0090  0a 49 4f 53 20 28 74 6d  29 20 43 33 37 35 30 20   .IOS (tm ) C3750
```

File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Tem... Packets: 51 Displayed: 51 Marked: 0 Dropped: 0 Profile: Default


Intel(R) PRO/Wireless 3945ABG
- Wireshark
Menu Bar
File Edit View Go Capture Analy
Button Bar
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
Window Pane 1
ALL Frames
Window Pane 2
Selected Frames Details
Window Pane 3
Hex Window
Intel(R) PRO/Wireless 3945ABG Network Connec...
No Packets
Status Bar

After running the Wireshark application, Capture option Window in available



Wireshark: Capture Options

Capture

Interface: Local | Intel(R) PRO/100 VE Network Connection: \Device\NPF_{A8:

IP address: 192.168.3.102

Link-layer header type: Ethernet

☑ Capture packets in promiscuous mode

☐ Capture packets in pcap-ng format (experimental)

☐ Limit each packet to 1 bytes

Buffer size: 1 megabyte(s)

Capture Filter:

Capture File(s)

File:

☐ Use multiple files

☑ Next file every 1 megabyte(s)

☐ Next file every 1 minute(s)

☑ Ring buffer with 2 files

☐ Stop capture after 1 file(s)

Stop Capture ...

☐ ... after 1 packet(s)

☐ ... after 1 megabyte(s)

☐ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

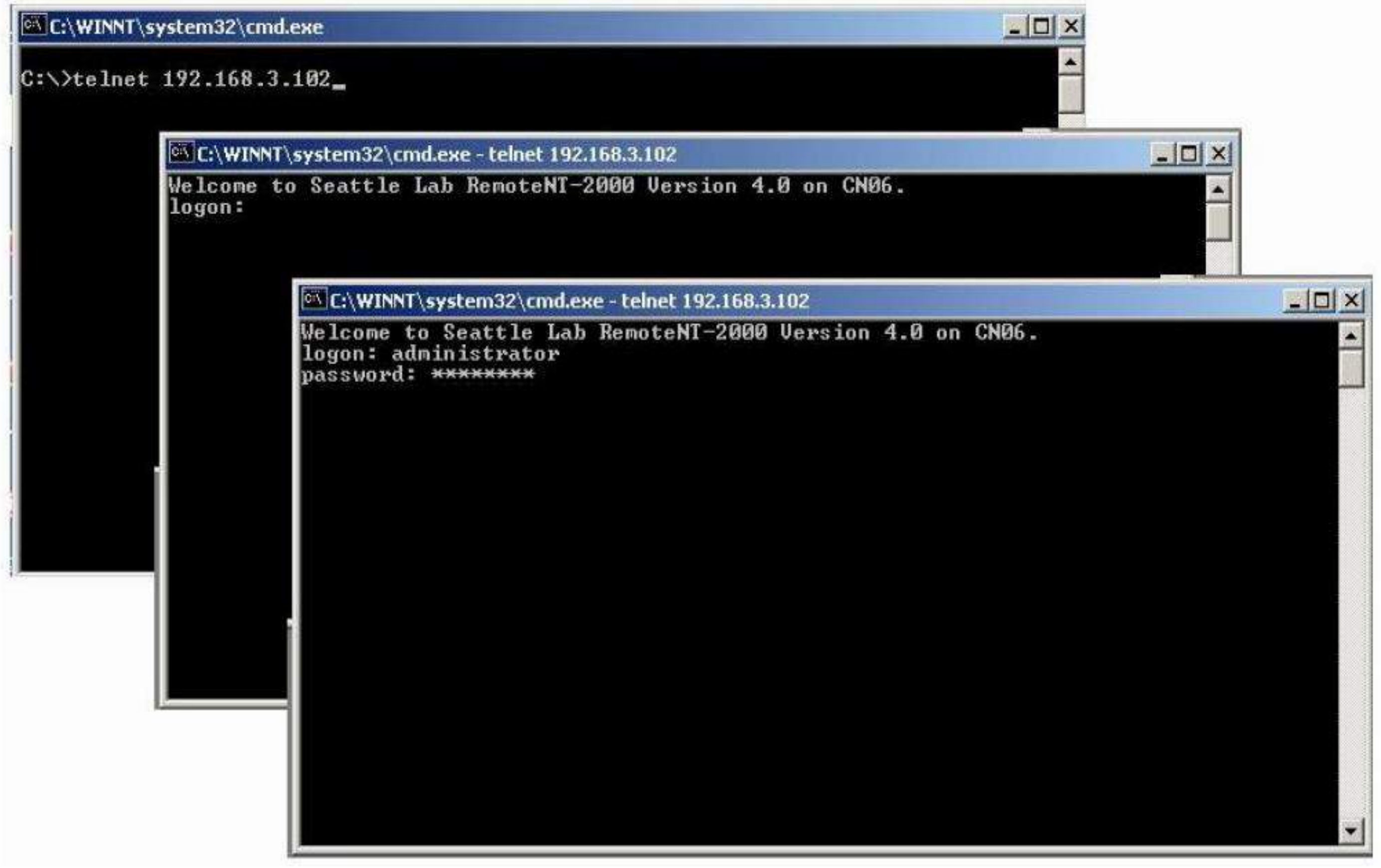
Name Resolution

☑ Enable MAC name resolution

☐ Enable network name resolution

☑ Enable transport name resolution

Telnet traffic is generated from 192.168.3.103 and Telnet server is available on 192.168.3.102



C:\WINNT\system32\cmd.exe

```
C:\>telnet 192.168.3.102_
```

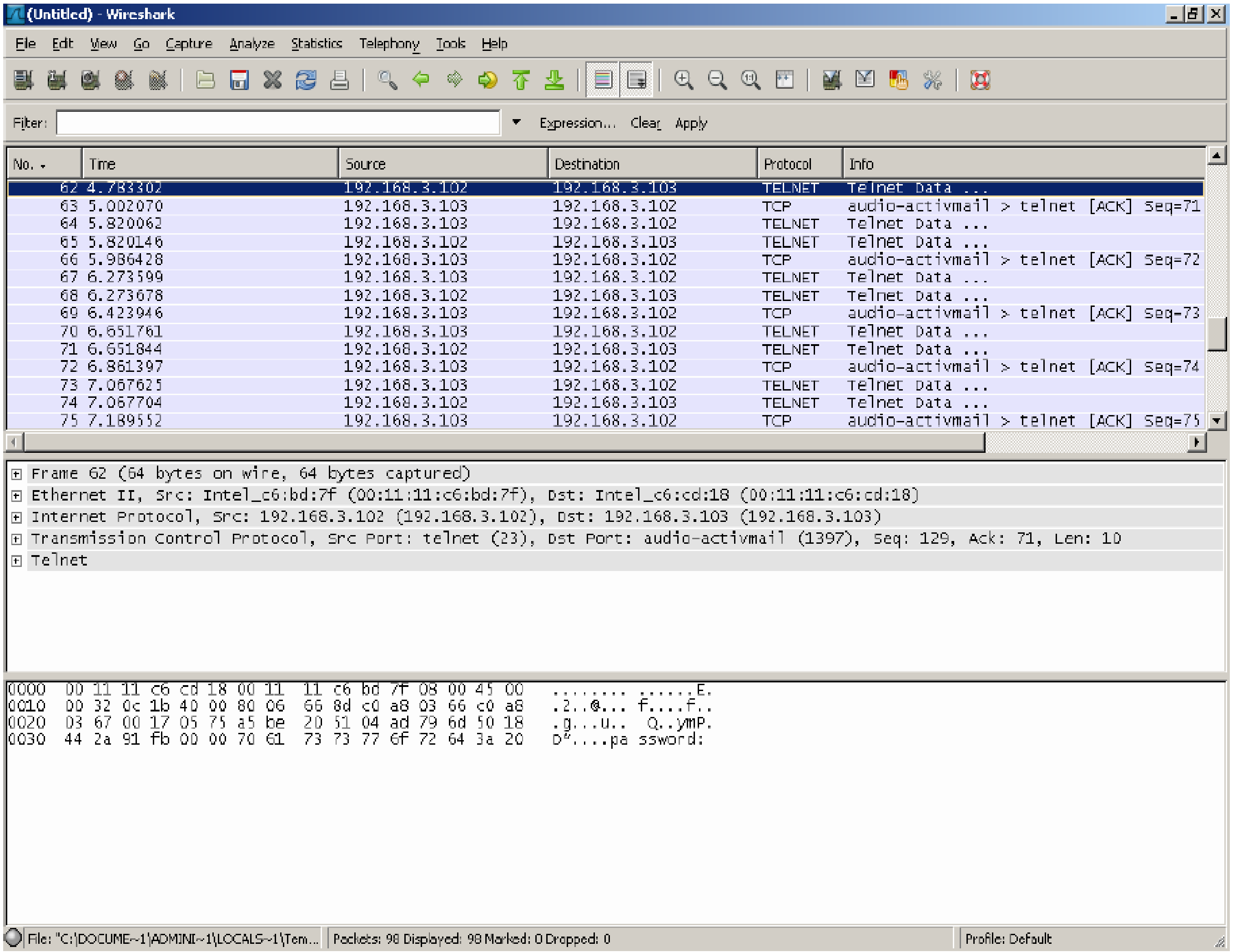
C:\WINNT\system32\cmd.exe - telnet 192.168.3.102

```
Welcome to Seattle Lab RemoteNT-2000 Version 4.0 on CN06.
logon:
```

C:\WINNT\system32\cmd.exe - telnet 192.168.3.102

```
Welcome to Seattle Lab RemoteNT-2000 Version 4.0 on CN06.
logon: administrator
password: ********
```

Wireshark captures the Frames and TELNET protocol traffic is analyzed.(and Password is sniffed)


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

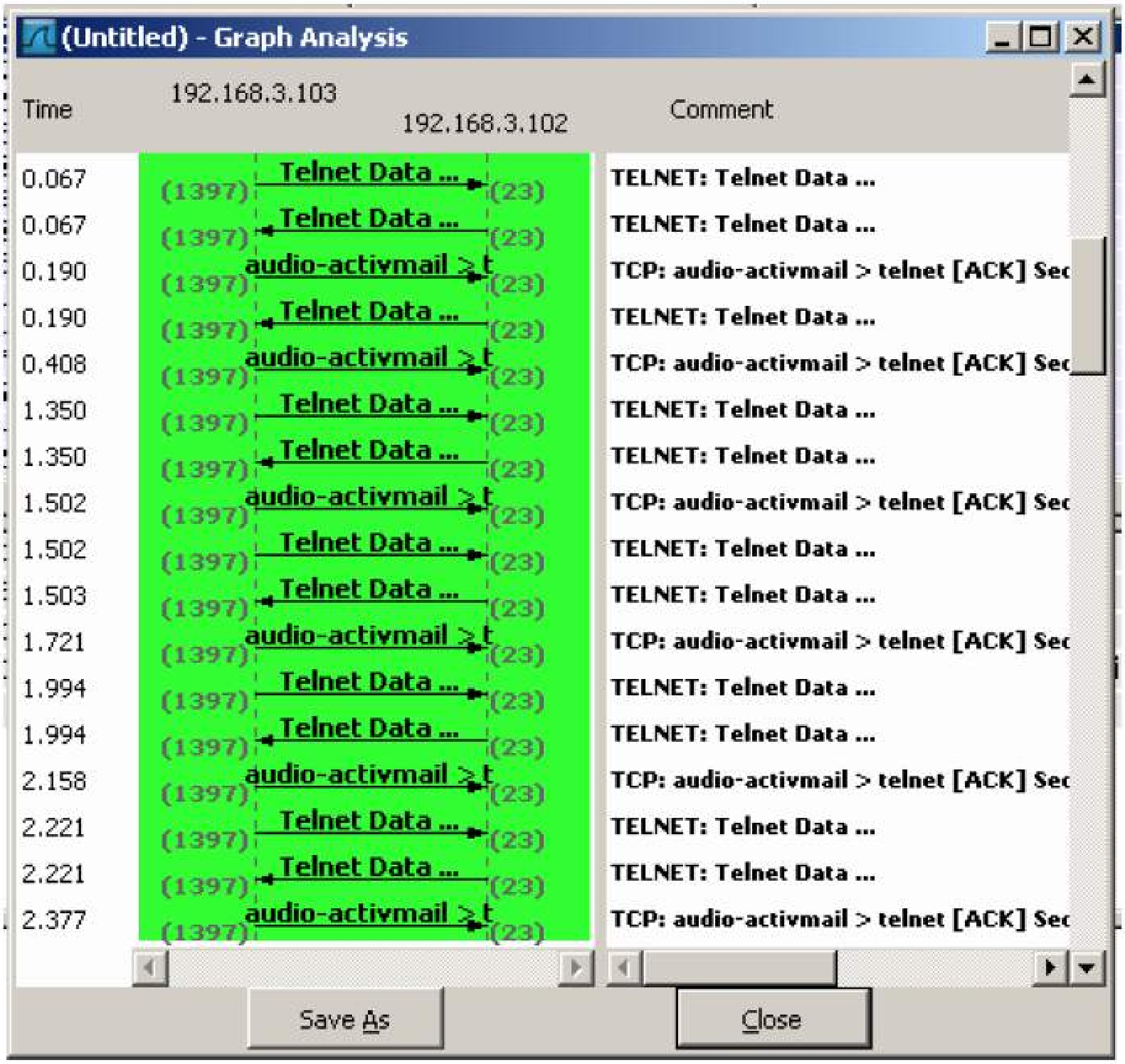
```
No. -  Time          Source          Destination     Protocol  Info
  62 4.783302        192.168.3.102   192.168.3.103   TELNET    Telnet Data ...
  63 5.002070        192.168.3.103   192.168.3.102   TCP       audio-activmail > telnet [ACK] Seq=71
  64 5.820062        192.168.3.103   192.168.3.102   TELNET    Telnet Data ...
  65 5.820146        192.168.3.102   192.168.3.103   TELNET    Telnet Data ...
  66 5.986428        192.168.3.103   192.168.3.102   TCP       audio-activmail > telnet [ACK] Seq=72
  67 6.273599        192.168.3.103   192.168.3.102   TELNET    Telnet Data ...
  68 6.273678        192.168.3.102   192.168.3.103   TELNET    Telnet Data ...
  69 6.423946        192.168.3.103   192.168.3.102   TCP       audio-activmail > telnet [ACK] Seq-73
  70 6.651761        192.168.3.103   192.168.3.102   TELNET    Telnet Data ...
  71 6.651844        192.168.3.102   192.168.3.103   TELNET    Telnet Data ...
  72 6.861397        192.168.3.103   192.168.3.102   TCP       audio-activmail > telnet [ACK] Seq=74
  73 7.067625        192.168.3.103   192.168.3.102   TELNET    Telnet Data ...
  74 7.067704        192.168.3.102   192.168.3.103   TELNET    Telnet Data ...
  75 7.189552        192.168.3.103   192.168.3.102   TCP       audio-activmail > telnet [ACK] Seq=75
```

```
⊞ Frame 62 (64 bytes on wire, 64 bytes captured)
⊞ Ethernet II, Src: Intel_c6:bd:7f (00:11:11:c6:bd:7f), Dst: Intel_c6:cd:18 (00:11:11:c6:cd:18)
⊞ Internet Protocol, Src: 192.168.3.102 (192.168.3.102), Dst: 192.168.3.103 (192.168.3.103)
⊞ Transmission Control Protocol, Src Port: telnet (23), Dst Port: audio-activmail (1397), Seq: 129, Ack: 71, Len: 10
⊞ Telnet
```

```
0000  00 11 11 c6 cd 18 00 11  11 c6 bd 7f 08 00 45 00   ........ ......E.
0010  00 32 0c 1b 40 00 80 06  66 8d c0 a8 03 66 c0 a8   .2..@... f....f..
0020  03 67 00 17 05 75 a5 be  20 51 04 ad 79 6d 50 18   .g...u..  Q..ymP.
0030  44 2a 91 fb 00 00 70 61  73 73 77 6f 72 64 3a 20   D*....pa ssword:
```

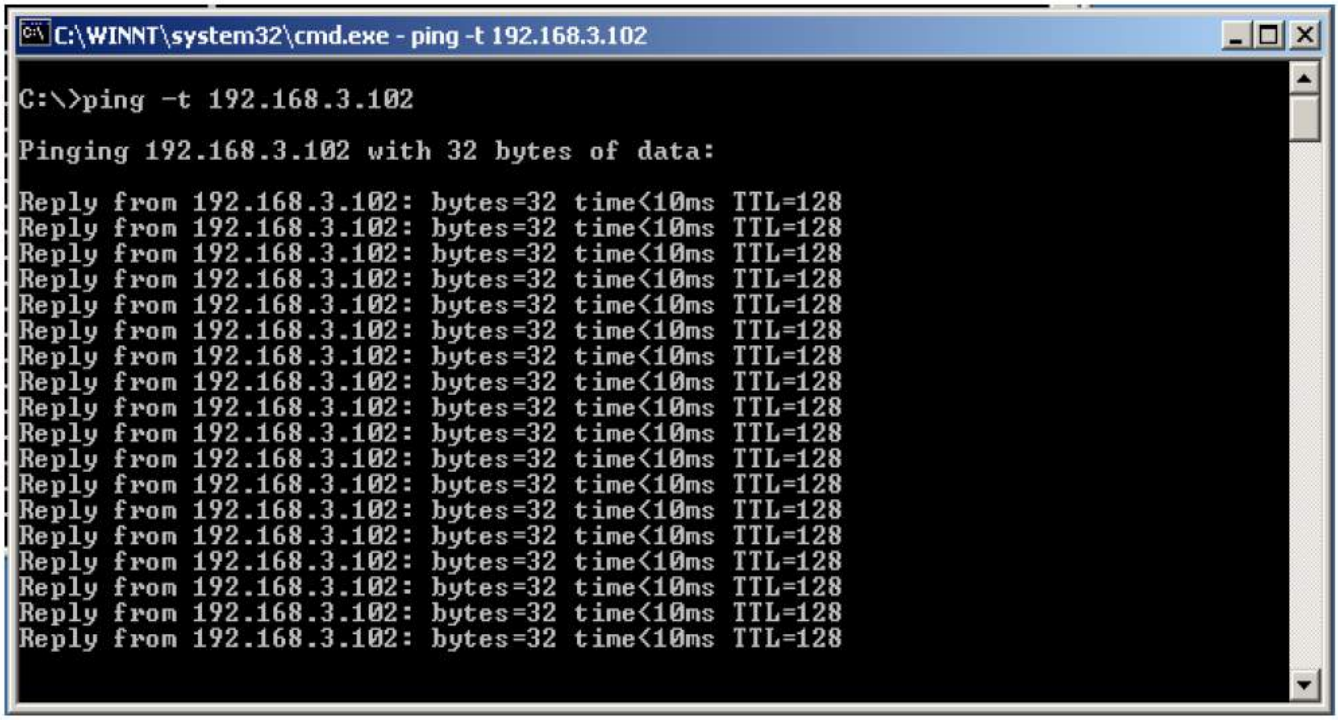
File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Tem... | Packets: 98 Displayed: 98 Marked: 0 Dropped: 0 | Profile: Default

Wireshark captures the Frames and Flow graphs option gives the detail graphical analysis.



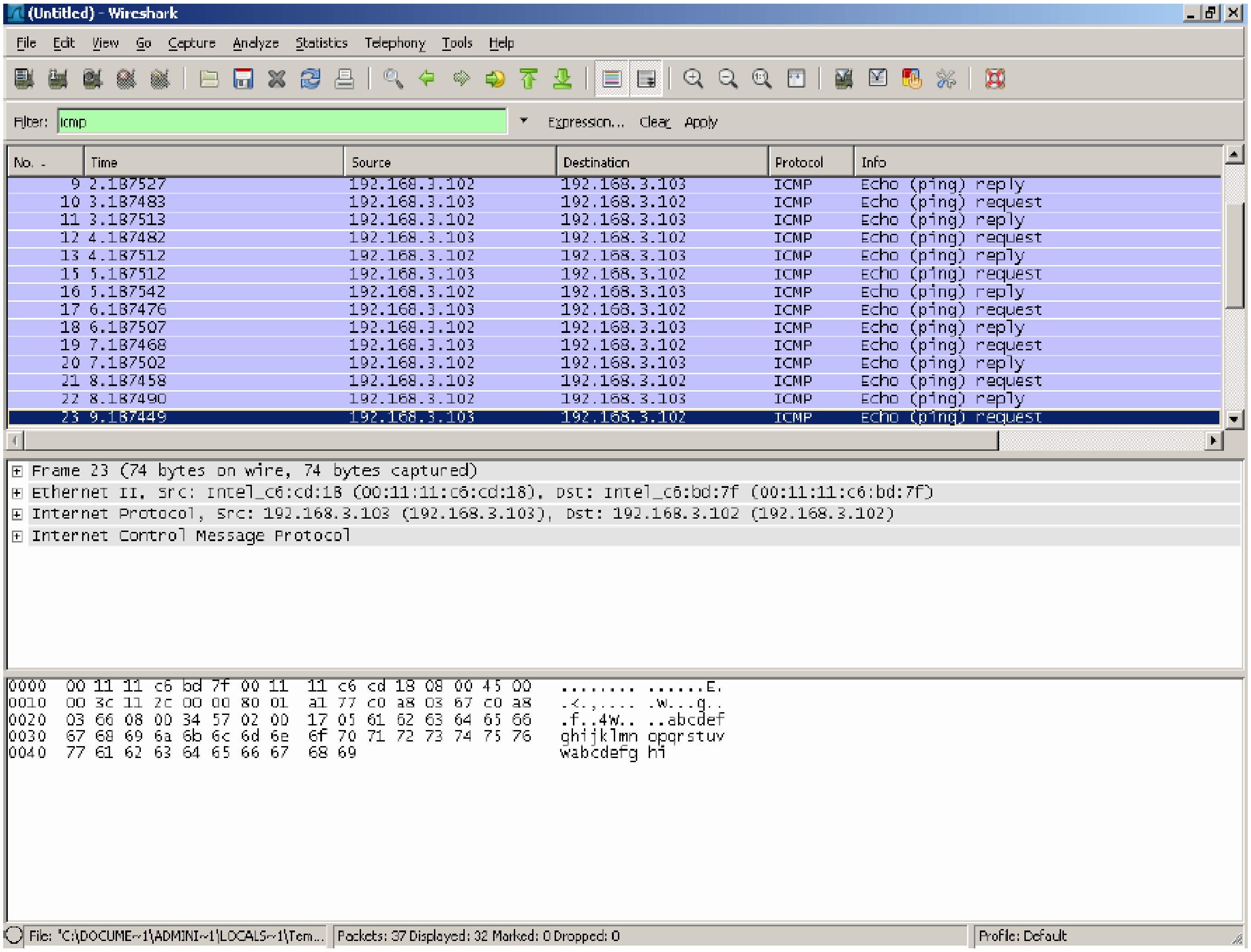
Time	192.168.3.103		192.168.3.102	Comment
0.067	(1397)	Telnet Data ... →	(23)	TELNET: Telnet Data ...
0.067	(1397)	← Telnet Data ...	(23)	TELNET: Telnet Data ...
0.190	(1397)	audio-activmail > t →	(23)	TCP: audio-activmail > telnet [ACK] Sec
0.190	(1397)	← Telnet Data ...	(23)	TELNET: Telnet Data ...
0.408	(1397)	audio-activmail > t →	(23)	TCP: audio-activmail > telnet [ACK] Sec
1.350	(1397)	Telnet Data ... →	(23)	TELNET: Telnet Data ...
1.350	(1397)	← Telnet Data ...	(23)	TELNET: Telnet Data ...
1.502	(1397)	audio-activmail > t →	(23)	TCP: audio-activmail > telnet [ACK] Sec
1.502	(1397)	Telnet Data ... →	(23)	TELNET: Telnet Data ...
1.503	(1397)	← Telnet Data ...	(23)	TELNET: Telnet Data ...
1.721	(1397)	audio-activmail > t →	(23)	TCP: audio-activmail > telnet [ACK] Sec
1.994	(1397)	Telnet Data ... →	(23)	TELNET: Telnet Data ...
1.994	(1397)	← Telnet Data ...	(23)	TELNET: Telnet Data ...
2.158	(1397)	audio-activmail > t →	(23)	TCP: audio-activmail > telnet [ACK] Sec
2.221	(1397)	Telnet Data ... →	(23)	TELNET: Telnet Data ...
2.221	(1397)	← Telnet Data ...	(23)	TELNET: Telnet Data ...
2.377	(1397)	audio-activmail > t →	(23)	TCP: audio-activmail > telnet [ACK] Sec

Ping traffic is generated from 192.168.3.103 and reply is received from 192.168.3.102



```
C:\>ping -t 192.168.3.102

Pinging 192.168.3.102 with 32 bytes of data:

Reply from 192.168.3.102: bytes=32 time<10ms TTL=128
Reply from 192.168.3.102: bytes=32 time<10ms TTL=128
Reply from 192.168.3.102: bytes=32 time<10ms TTL=128
Reply from 192.168.3.102: bytes=32 time<10ms TTL=128
Reply from 192.168.3.102: bytes=32 time<10ms TTL=128
Reply from 192.168.3.102: bytes=32 time<10ms TTL=128
Reply from 192.168.3.102: bytes=32 time<10ms TTL=128
Reply from 192.168.3.102: bytes=32 time<10ms TTL=128
Reply from 192.168.3.102: bytes=32 time<10ms TTL=128
Reply from 192.168.3.102: bytes=32 time<10ms TTL=128
Reply from 192.168.3.102: bytes=32 time<10ms TTL=128
Reply from 192.168.3.102: bytes=32 time<10ms TTL=128
Reply from 192.168.3.102: bytes=32 time<10ms TTL=128
Reply from 192.168.3.102: bytes=32 time<10ms TTL=128
Reply from 192.168.3.102: bytes=32 time<10ms TTL=128
Reply from 192.168.3.102: bytes=32 time<10ms TTL=128
Reply from 192.168.3.102: bytes=32 time<10ms TTL=128
Reply from 192.168.3.102: bytes=32 time<10ms TTL=128
```

Wireshark captures the Frames and ICMP protocol traffic is analyzed.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

Filter: icmp

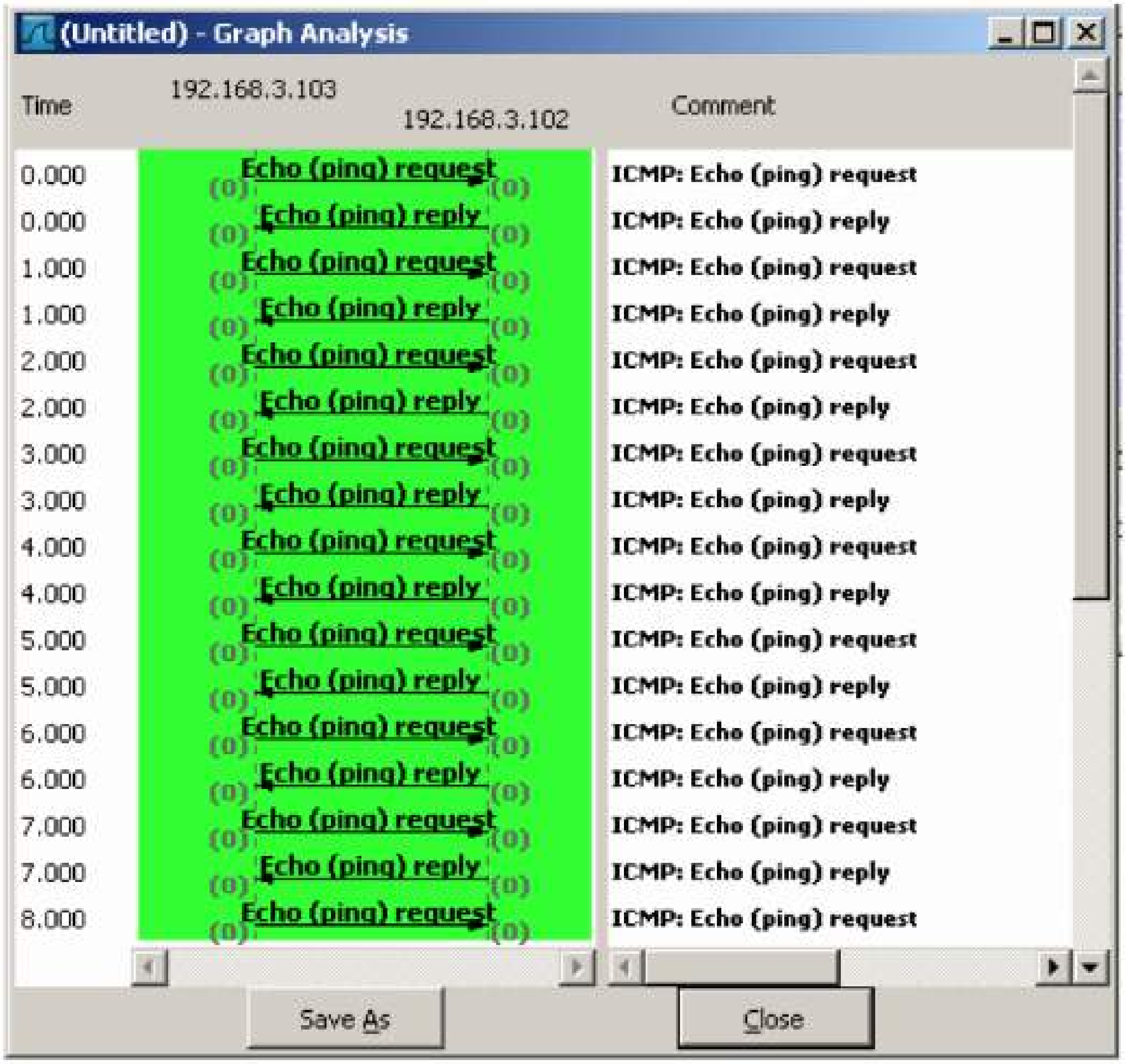
```
No. -  Time        Source          Destination     Protocol  Info
    9  2.187527    192.168.3.102   192.168.3.103   ICMP      Echo (ping) reply
   10  3.187483    192.168.3.103   192.168.3.102   ICMP      Echo (ping) request
   11  3.187513    192.168.3.102   192.168.3.103   ICMP      Echo (ping) reply
   12  4.187482    192.168.3.103   192.168.3.102   ICMP      Echo (ping) request
   13  4.187512    192.168.3.102   192.168.3.103   ICMP      Echo (ping) reply
   15  5.187512    192.168.3.103   192.168.3.102   ICMP      Echo (ping) request
   16  5.187542    192.168.3.102   192.168.3.103   ICMP      Echo (ping) reply
   17  6.187476    192.168.3.103   192.168.3.102   ICMP      Echo (ping) request
   18  6.187507    192.168.3.102   192.168.3.103   ICMP      Echo (ping) reply
   19  7.187468    192.168.3.103   192.168.3.102   ICMP      Echo (ping) request
   20  7.187502    192.168.3.102   192.168.3.103   ICMP      Echo (ping) reply
   21  8.187458    192.168.3.103   192.168.3.102   ICMP      Echo (ping) request
   22  8.187490    192.168.3.102   192.168.3.103   ICMP      Echo (ping) reply
   23  9.187449    192.168.3.103   192.168.3.102   ICMP      Echo (ping) request
```

```
⊞ Frame 23 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: Intel_c6:cd:18 (00:11:11:c6:cd:18), Dst: Intel_c6:bd:7f (00:11:11:c6:bd:7f)
⊞ Internet Protocol, Src: 192.168.3.103 (192.168.3.103), Dst: 192.168.3.102 (192.168.3.102)
⊞ Internet Control Message Protocol
```

```
0000  00 11 11 c6 bd 7f 00 11  11 c6 cd 18 08 00 45 00   ........ ......E.
0010  00 3c 11 2c 00 00 80 01  a1 77 c0 a8 03 67 c0 a8   .<.,.... .w...g..
0020  03 66 08 00 34 57 02 00  17 05 61 62 63 64 65 66   .f..4W.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Tem... | Packets: 37 Displayed: 32 Marked: 0 Dropped: 0 | Profile: Default

Wireshark captures the Frames and Flow graphs option gives the detail graphical analysis.



Time	192.168.3.103 192.168.3.102	Comment
0.000	(0) Echo (ping) request (0)	ICMP: Echo (ping) request
0.000	(0) Echo (ping) reply (0)	ICMP: Echo (ping) reply
1.000	(0) Echo (ping) request (0)	ICMP: Echo (ping) request
1.000	(0) Echo (ping) reply (0)	ICMP: Echo (ping) reply
2.000	(0) Echo (ping) request (0)	ICMP: Echo (ping) request
2.000	(0) Echo (ping) reply (0)	ICMP: Echo (ping) reply
3.000	(0) Echo (ping) request (0)	ICMP: Echo (ping) request
3.000	(0) Echo (ping) reply (0)	ICMP: Echo (ping) reply
4.000	(0) Echo (ping) request (0)	ICMP: Echo (ping) request
4.000	(0) Echo (ping) reply (0)	ICMP: Echo (ping) reply
5.000	(0) Echo (ping) request (0)	ICMP: Echo (ping) request
5.000	(0) Echo (ping) reply (0)	ICMP: Echo (ping) reply
6.000	(0) Echo (ping) request (0)	ICMP: Echo (ping) request
6.000	(0) Echo (ping) reply (0)	ICMP: Echo (ping) reply
7.000	(0) Echo (ping) request (0)	ICMP: Echo (ping) request
7.000	(0) Echo (ping) reply (0)	ICMP: Echo (ping) reply
8.000	(0) Echo (ping) request (0)	ICMP: Echo (ping) request

CLASS : BE (E&TC) **SUBJECT: CN**
EXPT. NO : - 07 **DATE :** 24-11-2020

I.AIM : Study of wireless networking

II.APPARATUS:

III.THEORY: Wireless communication is one of the fastest-growing technologies. The demand for connecting devices without the use of cables is increasing everywhere. Wireless LANs can be found on college campuses, in office buildings, and in many public areas.

In this chapter, we concentrate on two promising wireless technologies for LANs: IEEE 802.11 wireless LANs, sometimes called wireless Ethernet, and Bluetooth, a technology for small wireless LANs.

Architecture:

The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

Basic Service Set:

IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP). Figure 3 shows two sets in this standard.

The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture. In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an infrastructure network.

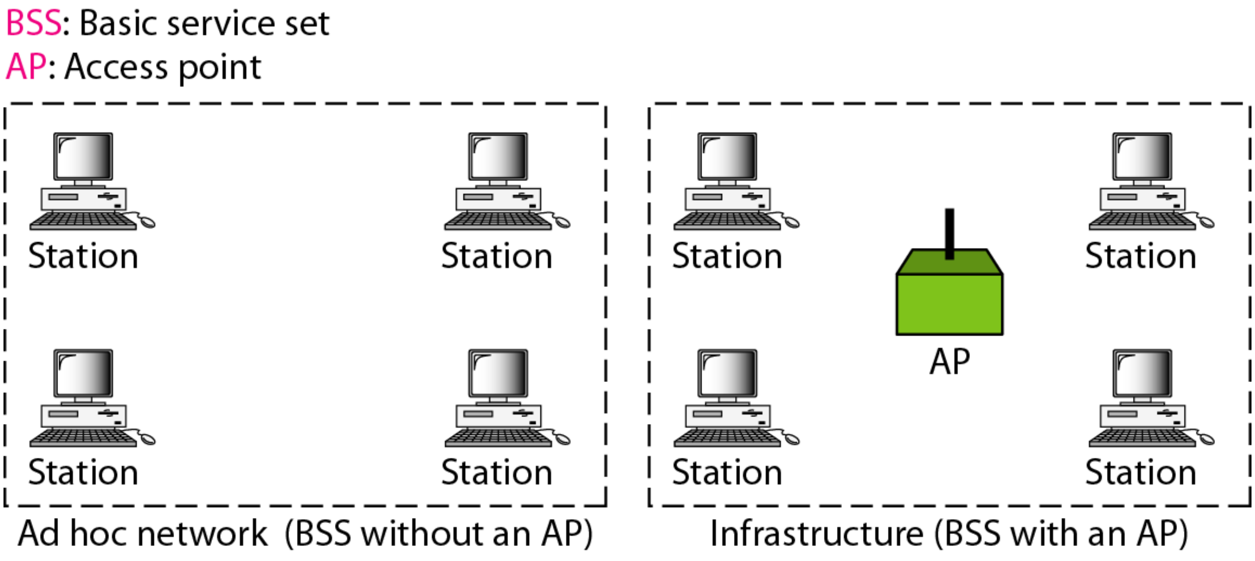


Figure 1 Basic service set (BSSs)

Extended Service Set:

An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a distribution system, which is usually a wired LAN. The distribution system connects the APs in the BSSs. IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet. Note that the extended service set uses two types of stations: mobile and stationary. The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN. Figure 4 shows an ESS.

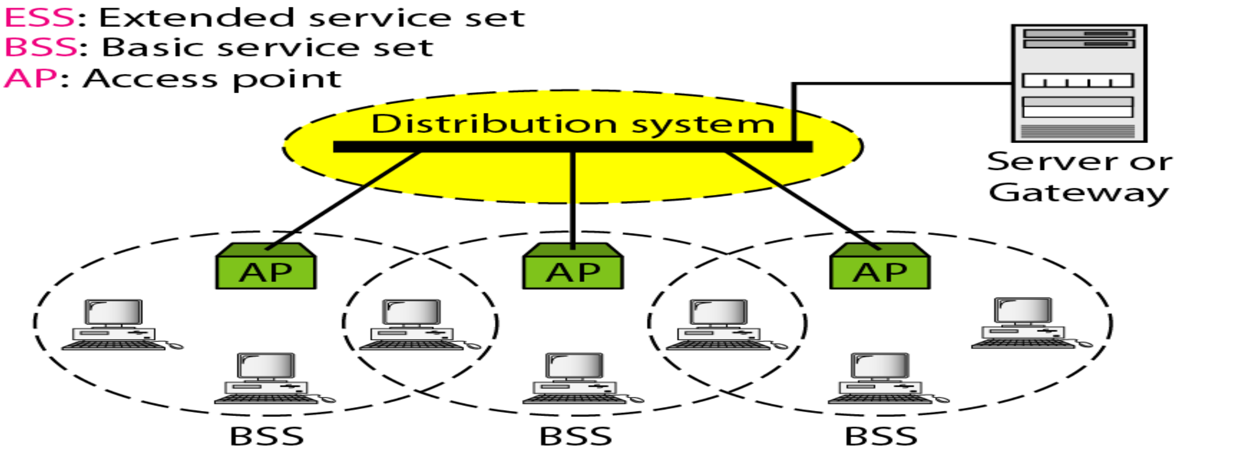


Figure 2 Extended service set (ESSs)

When BSSs are connected, the stations within reach of one another can communicate without the use of an AP. However, communication between two stations in two different BSSs usually occurs via two APs. The idea is similar to communication in a cellular network if we Consider each BSS to be a cell and each AP to be a base station. Note that a mobile station can belong to more than one BSSs at the same time.

MAC Sublayer :

IEEE 802.11 defines two MAC sublayers: the distributed coordination function (DCF) and point coordination function (PCF). Figure 5 shows the relationship between the two MAC sublayers, the LLC sublayer, and the physical layer. We discuss the physical layer implementations later in the chapter and will now concentrate on the MAC sublayer.

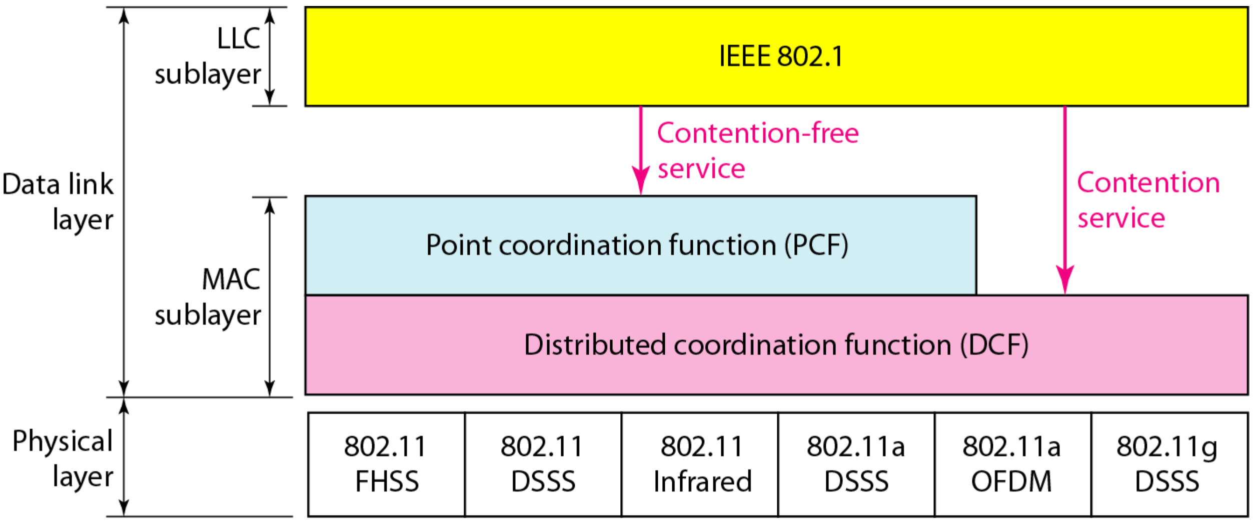


Figure 3 MAC layers in IEEE 802.11 standard

Distributed Coordination Function :

One of the two protocols defined by IEEE at the MAC sublayer is called the distributed coordination function (DCF). DCF uses CSMA/CA as the access method. Wireless LANs cannot implement CSMA/CD for three reasons:

1. For collision detection a station must be able to send data and receive collision signals at the same time. This can mean costly stations and increased bandwidth requirements.

2. Collision may not be detected because of the hidden station problem. We will discuss this problem later in the chapter.

3. The distance between stations can be great. Signal fading could prevent a station at one end from hearing a collision at the other end.

Point Coordination Function (PCF) :

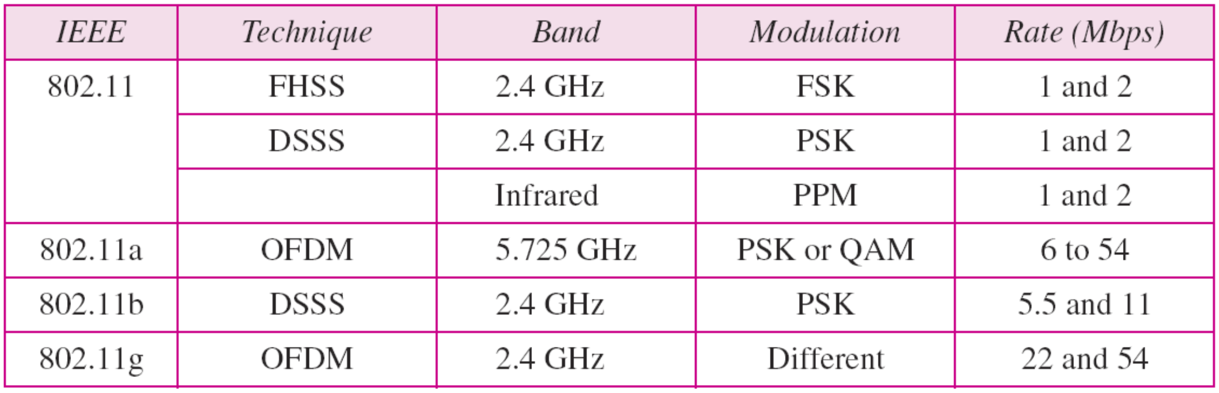
The point coordination function (PCF) is an optional access method that can be implemented in an infrastructure network (not in an ad hoc network). It is implemented on top of the DCF and is used mostly for time-sensitive transmission.

PCF has a centralized, contention-free polling access method. The AP performs polling for stations that are capable of being polled. The stations are polled one after another, sending any data they have to the AP.

To give priority to PCF over DCF, another set of interframe spaces has been defined: PIFS and SIFS. The SIFS is the same as that in DCF, but the PIFS (PCF IFS) is shorter than the DIFS. This means that if, at the same time, a station wants to use only DCF and an AP wants to use PCF, the AP has priority.

Physical Layer :

We discuss six specification, as shown in table.

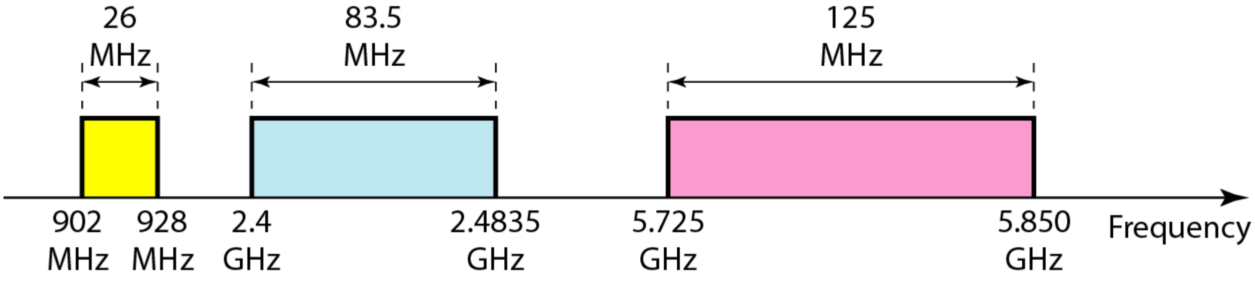


IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.4 GHz	FSK	1 and 2
	DSSS	2.4 GHz	PSK	1 and 2
		Infrared	PPM	1 and 2
802.11a	OFDM	5.725 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.4 GHz	PSK	5.5 and 11
802.11g	OFDM	2.4 GHz	Different	22 and 54

Table 1 Physical layers

All implementations, except the infrared, operate in the industrial, scientific. and medical (ISM) band, which defines three unlicensed bands in the three ranges 902-928 MHz, 2.400-4.835 GHz, and 5.725-5.850 GHz, as shown in Figure 6.

Figure 4 Industriyal,scientific, and medical (ISM) band



Association Process :

Association is the process of registering with a system to allow information to be transmitted and received with a device or system. Association in a WLAN systems the process of registering a wireless data device (station) with a Specific access point (AP) that is part of a wireless local area network (WLAN) system.

Roaming :

There are 2 definitions for wireless LAN roaming:

Internal Roaming (l): The Mobile Station (MS) moves from one access point (AP) to another AP within a home network because the signal strength is too weak.

External Roaming (2): The MS (client) moves into a WLAN of another Wireless Internet Service Provider (WISP) and takes their services (Hotspot). The user can independently of his home network use another foreign network, if this is open for visitors. There must be special authentication and billing systems for mobile services in a foreign network.

Wireless Channels :

IEEE 802.11g/b wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4 GHz and 2.5 GHz. Neighboring channels are 5 MHz apart. However, due to the spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum 12.5 MHz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channel 1 and channel 2) in the same general vicinity will interfere with each other. Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk and provide a noticeable performance increase over networks with minimal channel separation. Both wireless protocols operate in the 2.40 to 2.48-GHz ISM (industrial, scientific, and medical) RF band. WiFi uses one of 12 overlapping channels of 22-MHz bandwidth each, and Bluetooth frequency-hops among 79 channels. These channels are l-MHZ evenly spaced across the band. As a result, no matter which channel of WiFi is in use, a risk exists of interference between the two that will result in lowered data throughput for both.

The radio frequency channels used are listed in Table :

Table 2 802.11g Radio Frequency Channels

Channel	Center Frequency (MHz)	Frequency Spread (MHz)
1	2412	2399.5 – 2424.5
2	2417	2404.5 – 2429.5
3	2422	2409.5 – 2434.5
4	2427	2414.5 – 2439.5
5	2432	2419.5 – 2444.5
6	2437	2424.5 – 2449.5
7	2442	2429.5 – 2454.5

8	2447	2434.5 – 2459.5
9	2452	2439.5 – 2464.5
10	2457	2444.5 – 2469.5
11	2462	2449.5 – 2474.5
12	2467	2454.5 – 2479.5
13	2472	2459.5 – 2484.5

The benefits of wireless LANs include :

- ***Convenience***: The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking environment (home or office). With the increasing saturation of laptop-style computers, this is particularly relevant.
- ***Mobility***: With the emergence of public wireless networks, users can access the internet even outside their normal work environment. Most chain coffee shops, for example, offer their customers a wireless connection to the internet at little or no cost.
- ***Productivity***: Users connected to a wireless network can maintain a nearly constant affiliation with their desired network as they move from place to place. For a business, this implies that an employee can potentially be more productive as his or her work can be accomplished from any convenient location.
- ***Deployment***: Initial setup of an infrastructure-based wireless network requires little more than a single access point. Wired networks, on the other hand, have the additional cost and complexity of actual physical cables being run to numerous locations (which can even be impossible for hard-to-reach locations within a building).
- ***Expandability***: Wireless networks can serve a suddenly-increased number of clients with the existing equipment. In a wired network, additional clients would require additional wiring.
- ***Cost***: Wireless networking hardware is at worst a modest increase from wired counterparts. This potentially increased cost is almost always more than outweighed by the savings in cost and labor associated to running physical cables.

Disadvantages of Wireless LAN :

Wireless LAN technology, while replete with the conveniences and advantages described above has its share of downfalls. For a given networking situation, wireless LANs may not be desirable for a number of reasons. Most of these have to do with the inherent limitations of the technology.

- ***Security***: Wireless LAN transceivers are designed to serve computers throughout a structure with un-interrupted service using radio frequencies. Because of Space and cost, the antennas typically present on wireless networking cards in the end computers are generally relatively poor. In order to properly receive signals using such limited antennas throughout even a modest area, the wireless LAN transceiver utilizes a fairly considerable amount of power. What this means is that not only can the wireless packets be intercepted by a nearby adversary's poorly-equipped computer, but more importantly, a user willing to spend a small amount of money on a good quality antenna can pick up packets at a remarkable distance; perhaps hundreds of times the radius as the typical user. In fact, there are even computer users dedicated to locating and sometimes even hacking into wireless networks, known as wardrivers. On a wired network, any adversary would first have to overcome the physical limitation of tapping into the actual wires, but this is not an issue with wireless packets. To combat this consideration, wireless networks users usually choose to utilize various encryption technologies available such as Wi-Fi Protected Access (WPA). Some of the older encryption methods, such as WEP are known to have weaknesses that a dedicated adversary can compromise.

- ***Range***: The typical range of a common 802.11g network with standard equipment is on the order of tens of meters. While sufficient for a typical home, it will be insufficient in a larger structure. To obtain additional range, repeaters or additional access points will have to be purchased. Costs for these items can add up quickly. Other technologies are in the development phase, however, which feature increased range, hoping to render this disadvantage irrelevant.
- ***Reliability***: Like any radio frequency transmission, wireless networking signals are subject to a wide variety of interference, as well as complex propagation effects (such as multipath or especially in this case Rician fading) that are beyond the control of the network administrator. In the case of typical networks, modulation is achieved by complicated forms of phase-shift keying (PSK) or quadrature amplitude modulation (QAM), making interference and propagation effects all the more disturbing. As a result, important network resources such as servers are rarely connected wirelessly.
- ***Speed***: The speed on most wireless networks (typically 1-108Mbit/s) is reasonably slow compared to the slowest common wired networks (100 Mbit/s up to several Gbit/s). There are also performance issues caused by TCP and its built-in congestion avoidance for most users, however, this observation is irrelevant since the speed bottleneck is not in the wireless routing but rather in the outside network connectivity itself. For example, the maximum ADSL throughput (usually 8 Mbit/s or less) offered by telecommunications companies to general-purpose customers is already far slower than the slowest wireless network to which it is typically connected. That is to say, in most environments, a wireless network running at its slowest speed is still faster than the internet connection serving it in the first place. However, in specialized environments, the throughput of a wired network might be necessary. Newer standards such as 802.11n are addressing this limitation and will support peak throughputs in the range of 100-200 Mbit/s.

14.2 BLUETOOTH :

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, and so on. A Bluetooth LAN is an ad hoc network, which means that the, network is formed Spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet. A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability. A Bluetooth LAN, by nature can not be large. If there are many gadgets that try to connect, there is chaos.

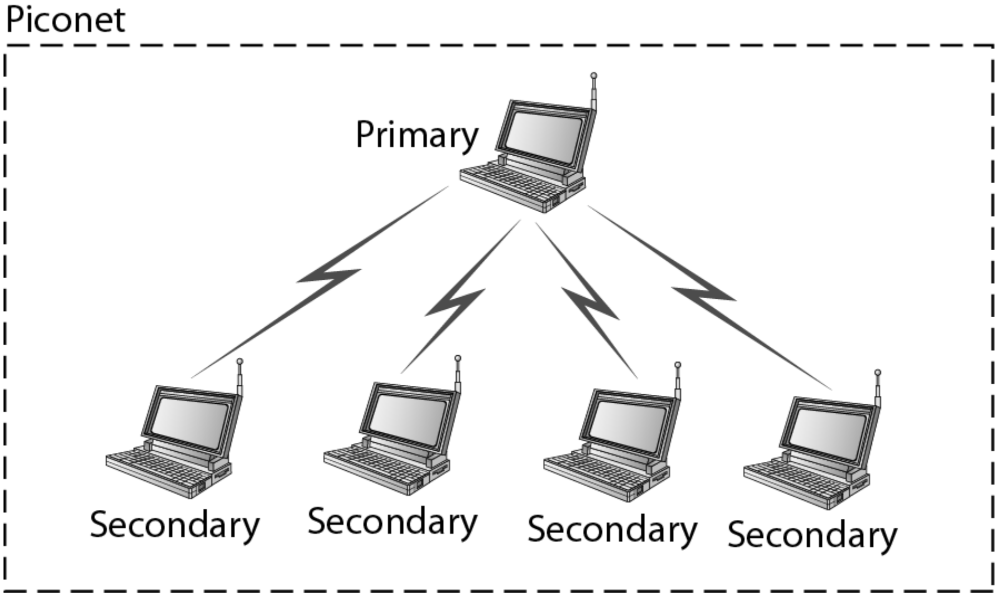
Architecture :

Bluetooth defines.two types of networks: piconet and scatternet.

Piconets :

A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries. All the secondary stations synchronize their clocks and hopping sequence with the primary. Note that a piconet can have only one primary station. The communication between the primary and the secondary can be one-to-one or one-to-many. Figure 7 shows a piconet.

Figure 5 Piconet



Although a piconet can have a maximum of seven secondaries, an additional eight secondaries can be in the parked state. A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state. Because only eight stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

Scattenet :

Piconets can be combined to form what is called a scatternet. A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets. Figure 8 illustrates a scatternet.

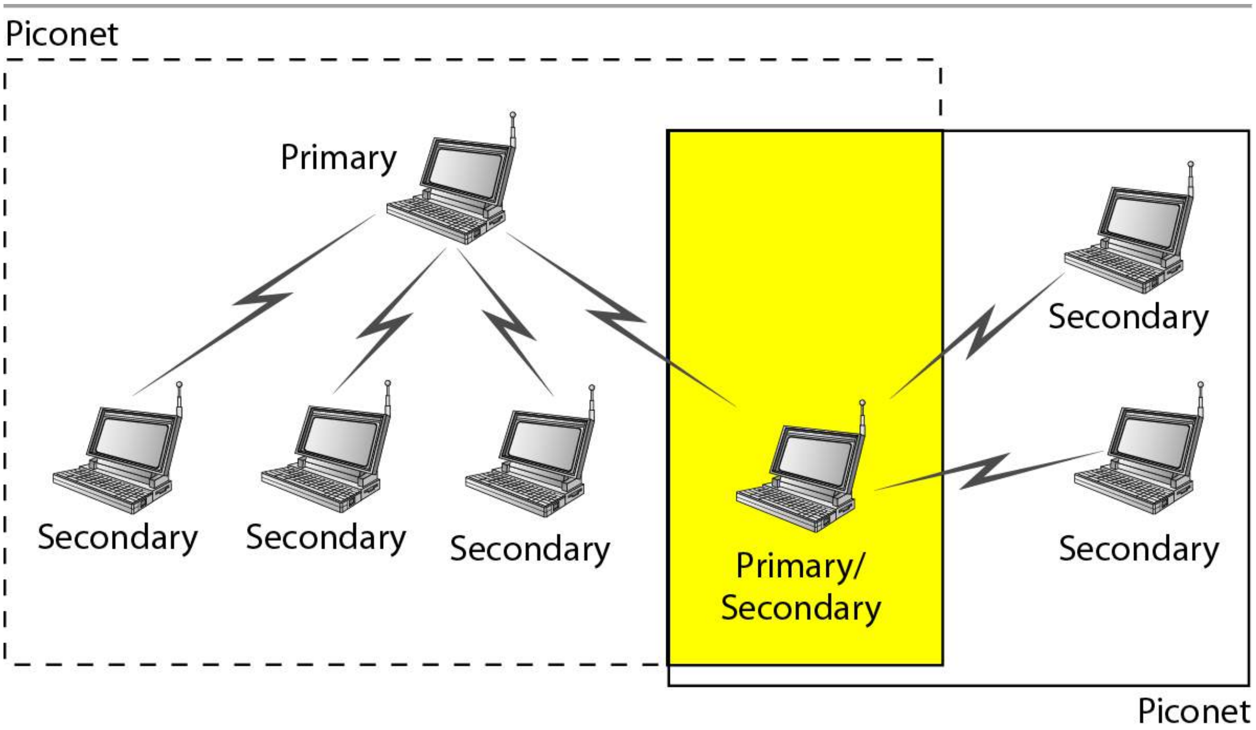


Figure 6 Scatternet

Bluetooth Devices:

A Bluetooth device has a built-in short-range radio transmitter. The current data rate is 1 Mbps with a 2.4GHz bandwidth. This means that there is a possibility of interference between the IEEE 802.11b wireless LANs and Bluetooth LANs.

Bluetooth Layers:

Bluetooth uses several layers that do not exactly match those of the Internet model we have delined in this book. Figure 9 shows these layers.

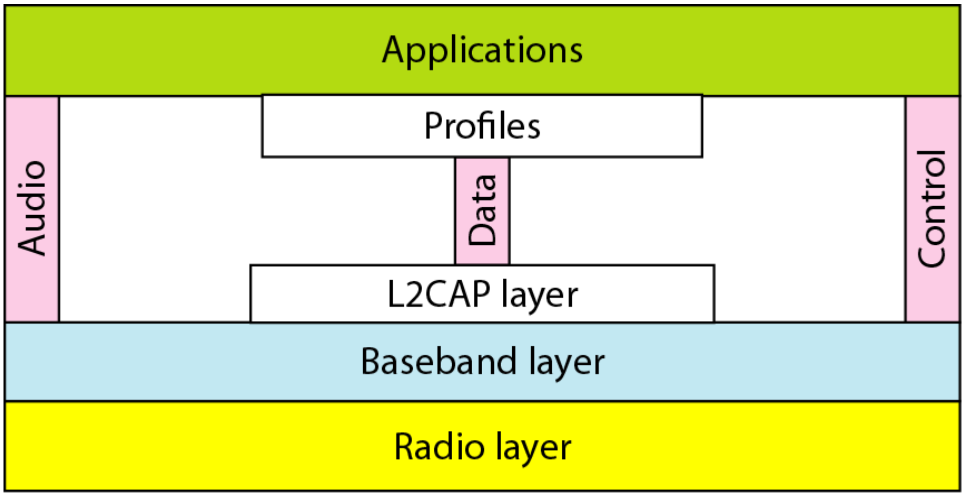


Figure 7 Bluetooth layers

Radio Layer :

1. BAND used is :2.4 GHz ISM band
2. Technique used is : FHSS.
3. Modulation used is : GFSK (Gaussian FSK)

Baseband layer :

1. Equivalent to MAC sublayer
2. TDD-TDMA: Time division Duplex TDMA

L2CAP layer :

1. The logical Link control and Adaptation Protocol
2. The functions are Multiplexing, Segmentation and Reassembly, QoS handling & Group Management.

Classes and Versions of Bluetooth

Bluetooth is a standard wire-replacement communications protocol primarily designed for low power consumption, with a short range (power-class-dependent, but effective ranges vary in practice; see table below) based on low-cost transceiver microchips in each device. Because the devices use a radio (broadcast) communications system, they do not have to be in visual line of sight of each other, however a quasi optical wireless path must be viable.

Class	Maximum permitted power		Range(m)
	(mW)	(dBm)	
Class1	100	20	~100
Class2	2.5	4	~10
Class3	1	0	~5

The effective range varies due to propagation conditions, material coverage, production sample variations. Antenna configurations and battery conditions. In most cases the effective range of class 2 devices is extended if they connect to a class 1 transceiver, compared to a pure class 2 network. This is accomplished by the higher sensitivity and transmission power of Class 1 devices.

Version	Data rate	Maximum application throughput
Version 1.2	1 Mbit/sec	0.7 Mbit/sec
Version 2.0 + EDR	3 Mbit/sec	2.1 Mbit/sec
Version 3.0 + HS	24 Mbit/sec approx.	2.1 Mbit/sec max
Version 4.0	24 Mbit/sec approx.	2.1 Mbit/sec max

While the Bluetooth Core Specification does mandate minimums for range, the range of the technology is application specific and is not limited. Manufacturer may tune their implementations to the range needed to support individual use cases.

Advantages of Bluetooth:

Bluetooth has a lot to offer with an increasingly difficult market place. Bluetooth helps to bring with it the promise of freedom from the cables and simplicity in networking that has yet to be matched by LAN (Local Area Network). in the key marketplace, of wireless and handheld devices, the closest competitor to Bluetooth is infrared. Infrared holds many key features, although the line of sight it provides doesn't go through walls or through obstacles like that of the Bluetooth technology. Unlike infrared, Bluetooth isn't a line of sight and it provides ranges of up to 100 meters. Bluetooth is also low power and low processing with an overhead protocol. What this means, is that it's ideal for integration into small battery powered devices. To put it short, the applications with Bluetooth are virtually endless.

Disadvantages of Bluetooth:

Bluetooth has several positive features and one would be extremely hard pressed to find downsides when given the current competition. The only real downsides are the data rate and security. Infrared car have data rates of up to 4 Mbps, which provides very fast rates for data transfer, while Bluetooth only offers 1 Mbps. For this very reason, infrared has yet to be dispensed with completely and is considered by many to be the complimentary technology to that of Bluetooth. Infrared has inherent security due to its line of sight. The greater range and radio frequency (RF) of Bluetooth make it much more open to interception and attack. For this reason, security is a very key aspect to the Bluetooth specification. Although there are very few disadvantages. Bluetooth still remains the best for short range wireless technology. Those who have tried it love it and they know for a fact that Bluetooth will be around for years to come.

NETGEAR 54 Mbps Wireless PCI Adapter WG311 v3 :

Default Wireless Settings :

If this is a new wireless network installation, use the factory default settings to set up the network and verify wireless connectivity. If this is an addition to an existing wireless network, you will need to identify the wireless network and wireless security settings that are already defined.

Your WG311 v3 Wireless PCI Adapter factory default basic settings are:

1. Network Name Service Set Identification (SSID): Any (First available network)
2. In order for the WG311 v3 Wireless PCI Adapter to communicate with a wireless access point or wireless adapter. all devices must be set up to use the same wireless network name (SSID).
3. Network Mode (Infrastructure or Ad-hoc): Infrastructure
4. Data security WEP, WPA2-PSK, or WPA-PSK encryption: Disabled

Main options available in Smart Wizard :

1. Settings -Profiles, network type (Infrastructure or ad hoc mode selection and security options like WEP and WPA options are available.

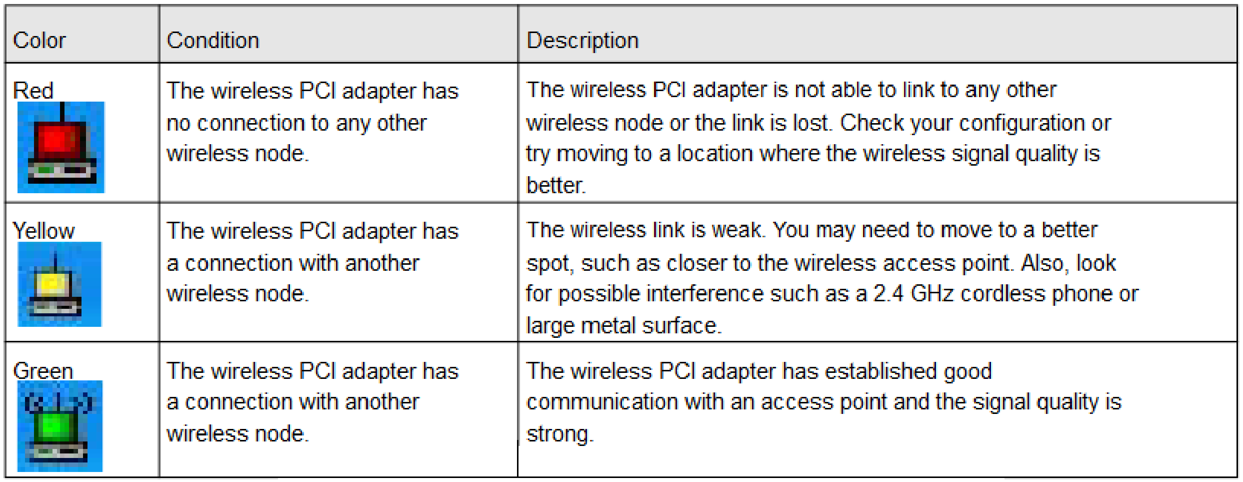
2. Networks-Available network name (SSID) is displayed and % signal strength is shown.

3. Statistics-TX and Rx statistics like Mbps & Packets/Sec is displayed

4. About: regional domain, driver version, firmware version, MAC address, IP address is indicated.

WG311 v3 Icon colors:

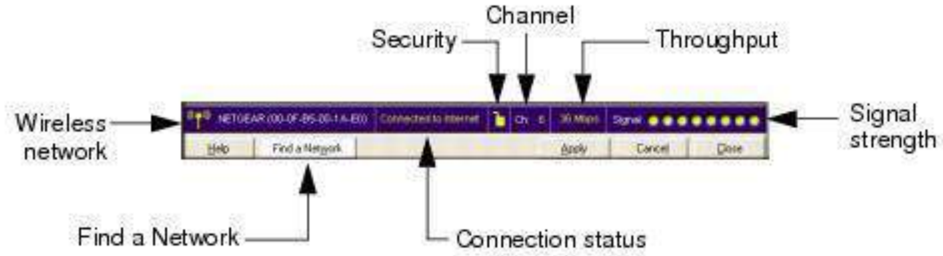
The WG311 v3 icon is on the desktop and in the Windows System Tray. The System Tray is located on one end of the taskbar in the Microsoft Windows desktop.



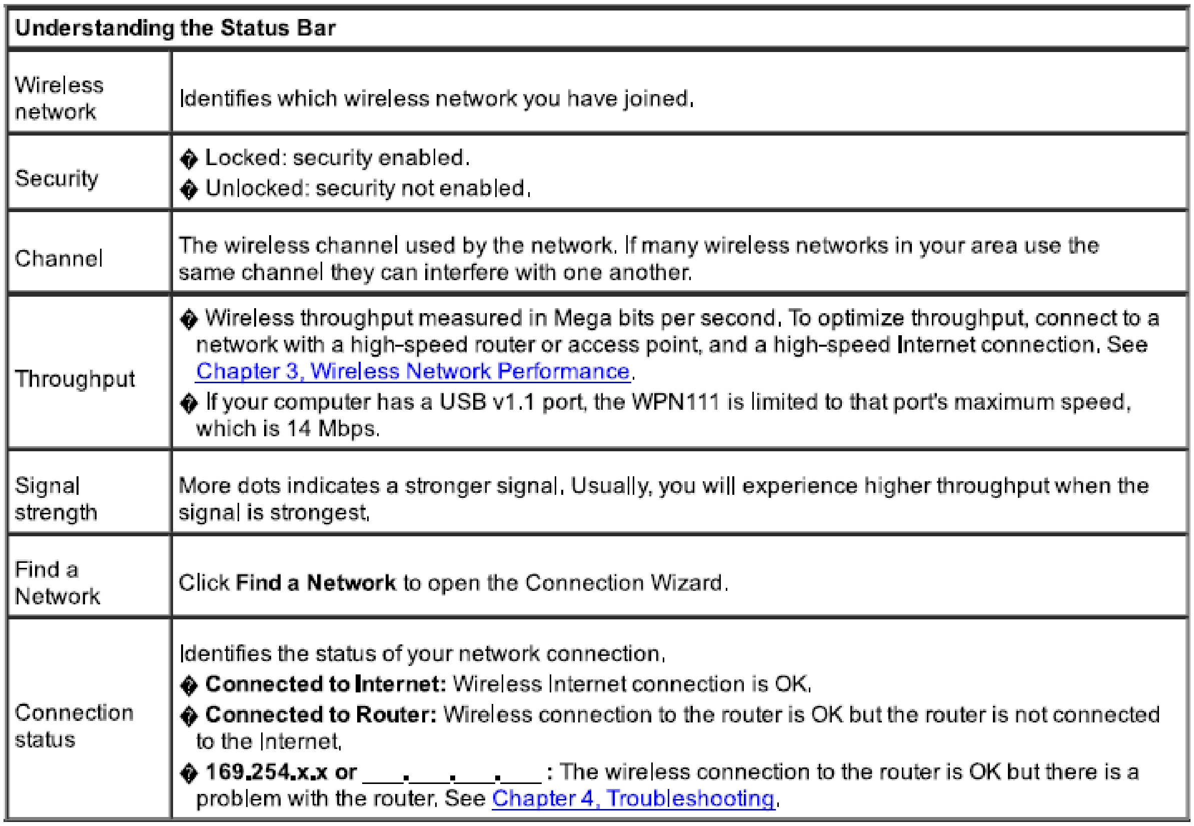
Color	Condition	Description
Red	The wireless PCI adapter has no connection to any other wireless node.	The wireless PCI adapter is not able to link to any other wireless node or the link is lost. Check your configuration or try moving to a location where the wireless signal quality is better.
Yellow	The wireless PCI adapter has a connection with another wireless node.	The wireless link is weak. You may need to move to a better spot, such as closer to the wireless access point. Also, look for possible interference such as a 2.4 GHz cordless phone or large metal surface.
Green	The wireless PCI adapter has a connection with another wireless node.	The wireless PCI adapter has established good communication with an access point and the signal quality is strong.

The Smart Wizard Status Bar :

Click the WG311 v3 icon to open the Smart Wizard so you can view the status bar. The Smart Wizard Settings page opens. The status bar is located at the bottom of the settings page.



The following table describes how to interpret the Smart Wizard status bar



Understanding the Status Bar	
Wireless network	Identifies which wireless network you have joined.
Security	� Locked: security enabled. � Unlocked: security not enabled.
Channel	The wireless channel used by the network. If many wireless networks in your area use the same channel they can interfere with one another.
Throughput	� Wireless throughput measured in Mega bits per second. To optimize throughput, connect to a network with a high-speed router or access point, and a high-speed Internet connection. See Chapter 3, Wireless Network Performance. � If your computer has a USB v1.1 port, the WPN111 is limited to that port's maximum speed, which is 14 Mbps.
Signal strength	More dots indicates a stronger signal. Usually, you will experience higher throughput when the signal is strongest.
Find a Network	Click **Find a Network** to open the Connection Wizard.
Connection status	Identifies the status of your network connection. � **Connected to Internet:** Wireless Internet connection is OK. � **Connected to Router:** Wireless connection to the router is OK but the router is not connected to the Internet. � **169.254.x.x or ___.___.___.___ :** The wireless connection to the router is OK but there is a problem with the router. See Chapter 4, Troubleshooting.

Technical Specifications of NETGEAR 54 Mbps Wireless PCI Adapter WG311 v3

Antenna	1 Integrated internal antenna
Antenna	External antenna
Radio data rate	1,2,5.5,11,6,9,12,18,24,36,48 and 54 Mbps(Auto Rate Sensing)
Frequency	2.4 GHz-2.5GHz (CCK and OFDM modulation)

Emissions	FCC, CE, TELEC
Bus interface	PCI
Provided drivers	Microsoft Vista, Windows XP,2000,98, and Me
Weight	40 gram
LED	Link
Operating Environment	Operating temperature: 0-55 degree C,32-131 degree F
Encryption	WPA2-PSK, WPA-PSK, and 40-bit and 128-bit WEP data encryption
Warranty	Limited 1 year warranty

Observe Wireless Location and Range Guidelines

Computers can connect over wireless networks indoors at a range which vary significantly based on the physical location of the computer with the NETGEAR 54 Mbps Wireless PCI Adapter WG311 v3. For best results. avoid potential sources of interference. such as:

1. Large metal surfaces
2. M1crowaves
3. 2.4 GHZ Cordless phones

In general, wireless devices can communicate through walls. However, if the walls are constructed with concrete, or have metal, or metal mesh, the effective range will decrease if such materials are between the devices.

Procedure for W-LAN networking :

1. For wLAN communication, insert the wireless PCI adapter in PCI slot.
2. Install the driver for same using installation driver CD. (Do this for other system also.)
3. Turn on the wireless access point (AP) for infrastructure mode of communication.
4. DHCP server from access point allocates IP address to the system1 and system2 (or end station1 and end station2.)
5. IP address for end station1 = 192.168.1.101
   IP address for end station2 = 192.168.1.102

   Verify the above IP addresses using command ipconfig/ all.
6. Thus transfer the data from end station1 to end station2, with wireless connectivity.

Procedure for Bluetooth Networking :

1. Connect the USB-Bluetooth devices on two different machines.

2. If windows XP operating system is used then it automatically installs the driver for it(otherwise for old operating system like windows-98, the driver installation is done by provided driver installation is done by provided driver installation CD).

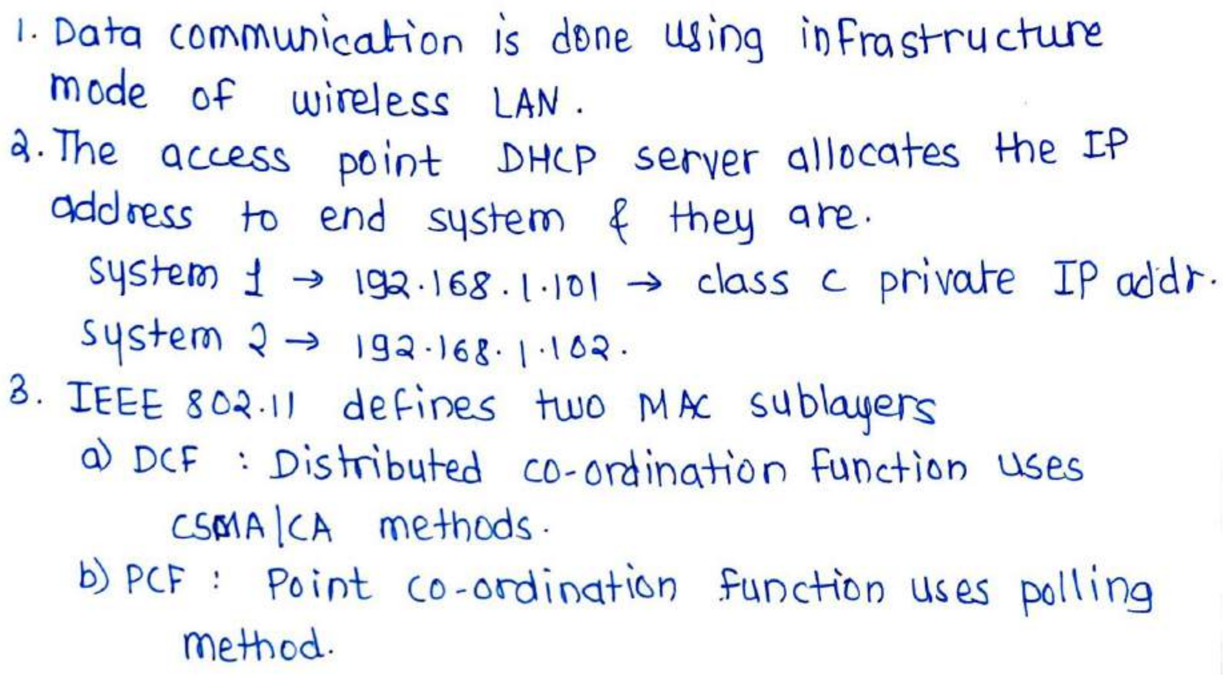
3. As soon as USB-Bluetooth device driver is installed, the Bluetooth icon is displayed in the system tray. If right click this option, then it gives following options

a) Add a Bluetooth device.
b) Show Bluetooth devices.
c) Send a file.
d) Receive a file.
e) Join a personal area network.
f) Open Bluetooth settings.
g) Remove Bluetooth icons.

4. Select "Show Bluetooth devices" and search for the system2 bluetooth device from system1 bluetooth device.

5. Thus after joining both the devices can act as sender and other device acts as receiver thus send file using device1 and receive a file using bluetooth device2 using system1 and system2 respectively.

IV. CONCLUSION:



1. Data communication is done using infrastructure mode of wireless LAN.

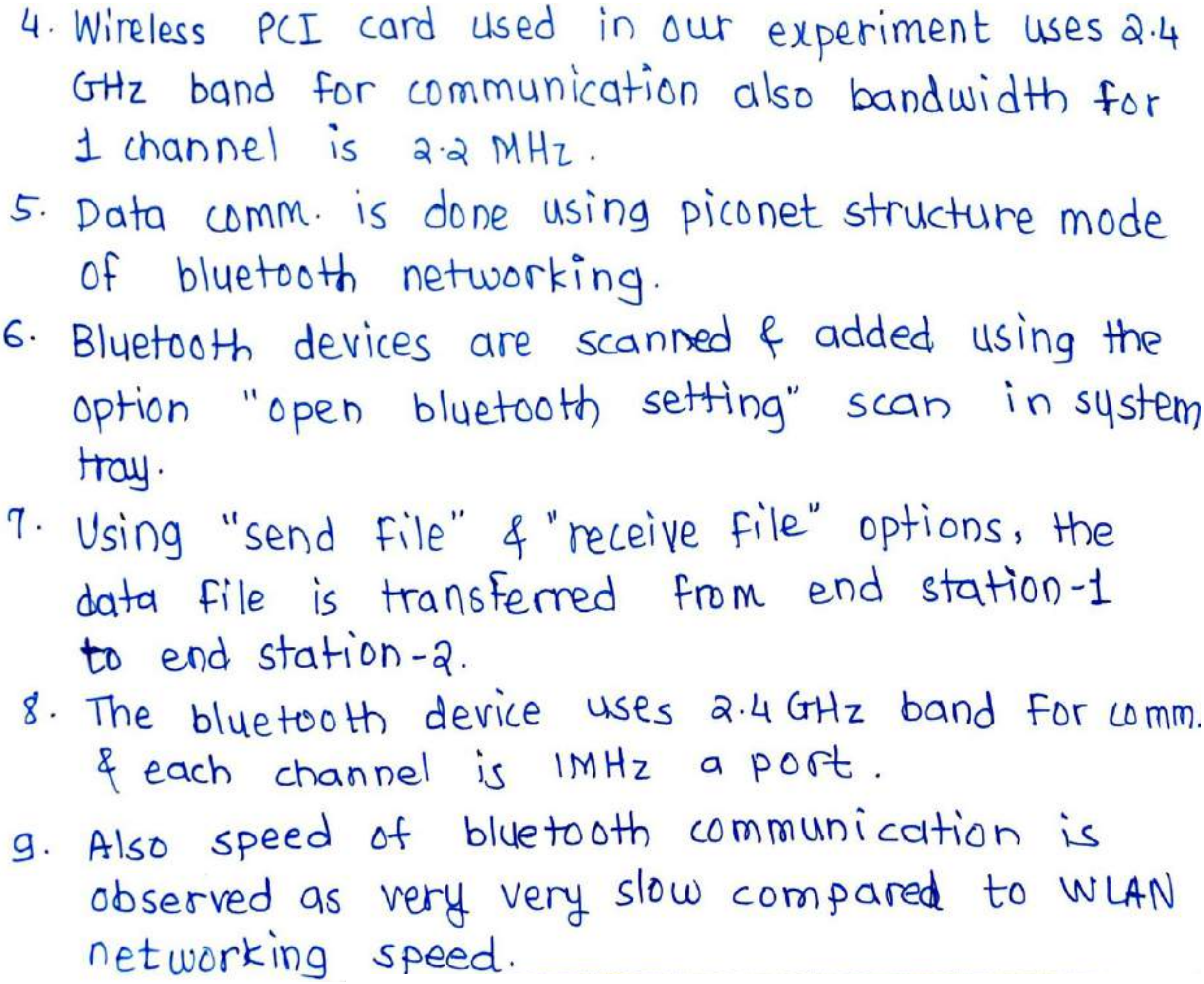
2. The access point DHCP server allocates the IP address to end system & they are.

system 1 → 192.168.1.101 → class C private IP addr.
system 2 → 192.168.1.102.

3. IEEE 802.11 defines two MAC sublayers

a) DCF : Distributed co-ordination function uses CSMA|CA methods.

b) PCF : Point co-ordination function uses polling method.

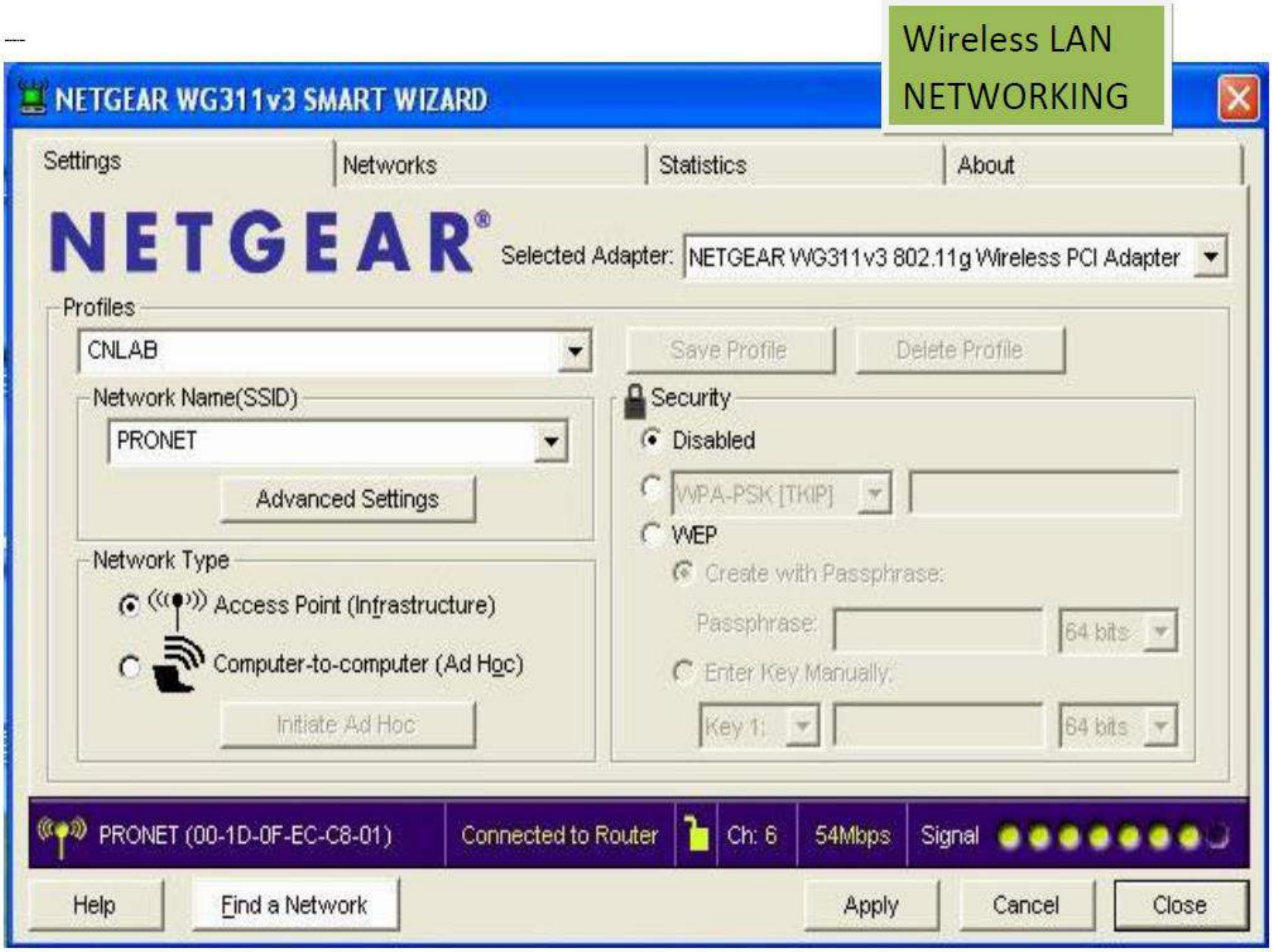


4. Wireless PCI card used in our experiment uses 2.4 GHz band for communication also bandwidth for 1 channel is 2.2 MHz.
5. Data comm. is done using piconet structure mode of bluetooth networking.
6. Bluetooth devices are scanned & added using the option "open bluetooth setting" scan in system tray.
7. Using "send file" & "receive file" options, the data file is transferred from end station-1 to end station-2.
8. The bluetooth device uses 2.4 GHz band for comm. & each channel is 1MHz a port.
9. Also speed of bluetooth communication is observed as very very slow compared to WLAN networking speed.

SIGNATURE

REFERENCES:

1. Data Communication. & Networking. B *Forouzan.*
2. "NETGEAR 54 Mbps wireless PCI adapter WG311v3 user manual"
3. "IVT Bluesoil standard edition user manual version 3.0"



Selected Adapter: NETGEAR WG311v3 802.11g Wireless PCI Adapter

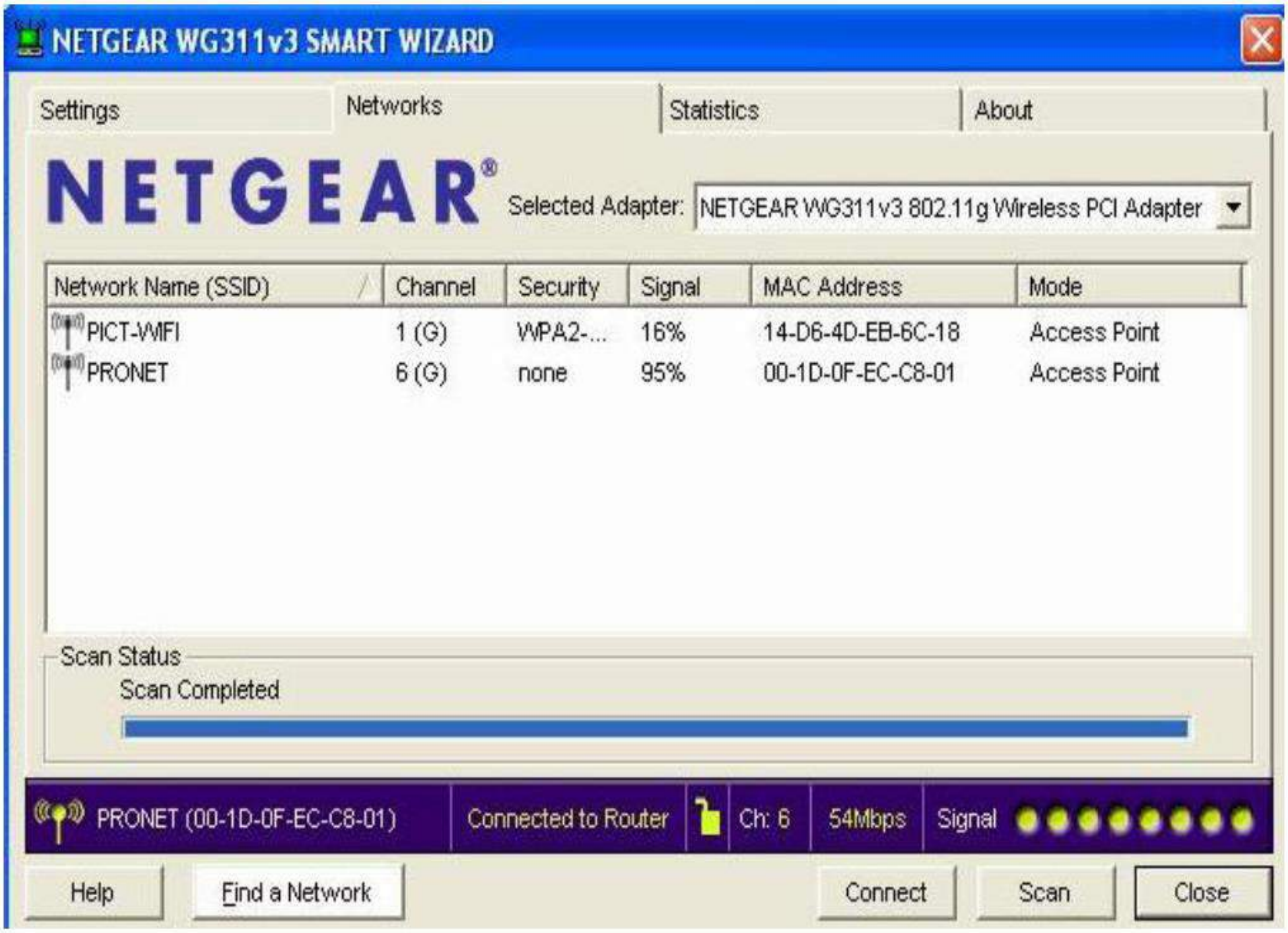
Profiles: CNLAB

Network Name(SSID): PRONET

Network Type
● Access Point (Infrastructure)
○ Computer-to-computer (Ad Hoc)

Security
● Disabled
○ WPA-PSK [TKIP]
○ WEP
● Create with Passphrase:
Passphrase: 64 bits
○ Enter Key Manually:
Key 1: 64 bits

PRONET (00-1D-0F-EC-C8-01) | Connected to Router | Ch: 6 | 54Mbps | Signal



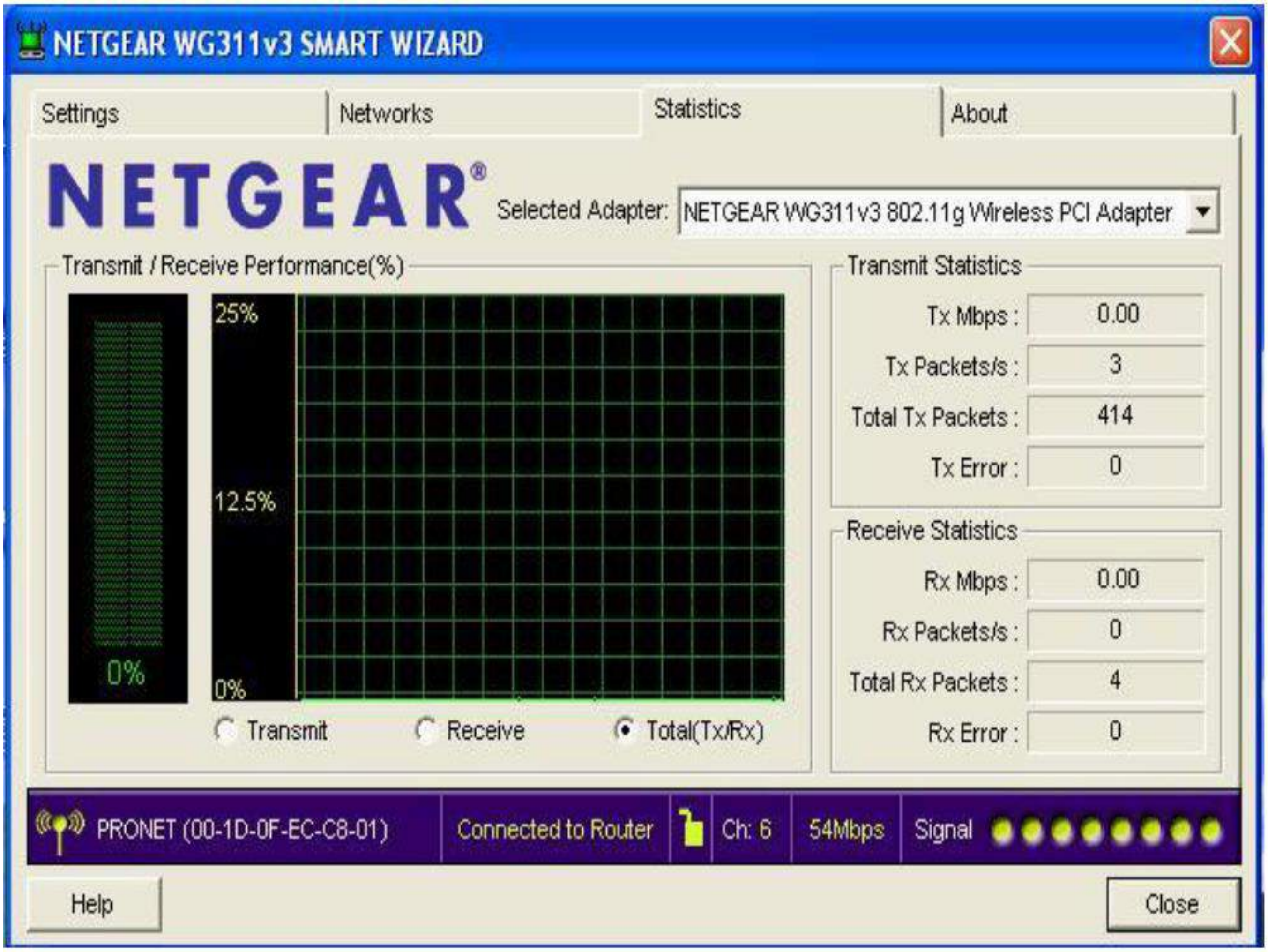
Selected Adapter: NETGEAR WG311v3 802.11g Wireless PCI Adapter

Network Name (SSID)	Channel	Security	Signal	MAC Address	Mode
PICT-WIFI	1 (G)	WPA2-...	16%	14-D6-4D-EB-6C-18	Access Point
PRONET	6 (G)	none	95%	00-1D-0F-EC-C8-01	Access Point

Scan Status

Scan Completed

PRONET (00-1D-0F-EC-C8-01) | Connected to Router | Ch: 6 | 54Mbps | Signal ●●●●●●●●



NETGEAR WG311v3 SMART WIZARD

Selected Adapter: NETGEAR WG311v3 802.11g Wireless PCI Adapter

○ Transmit ○ Receive ● Total(Tx/Rx)

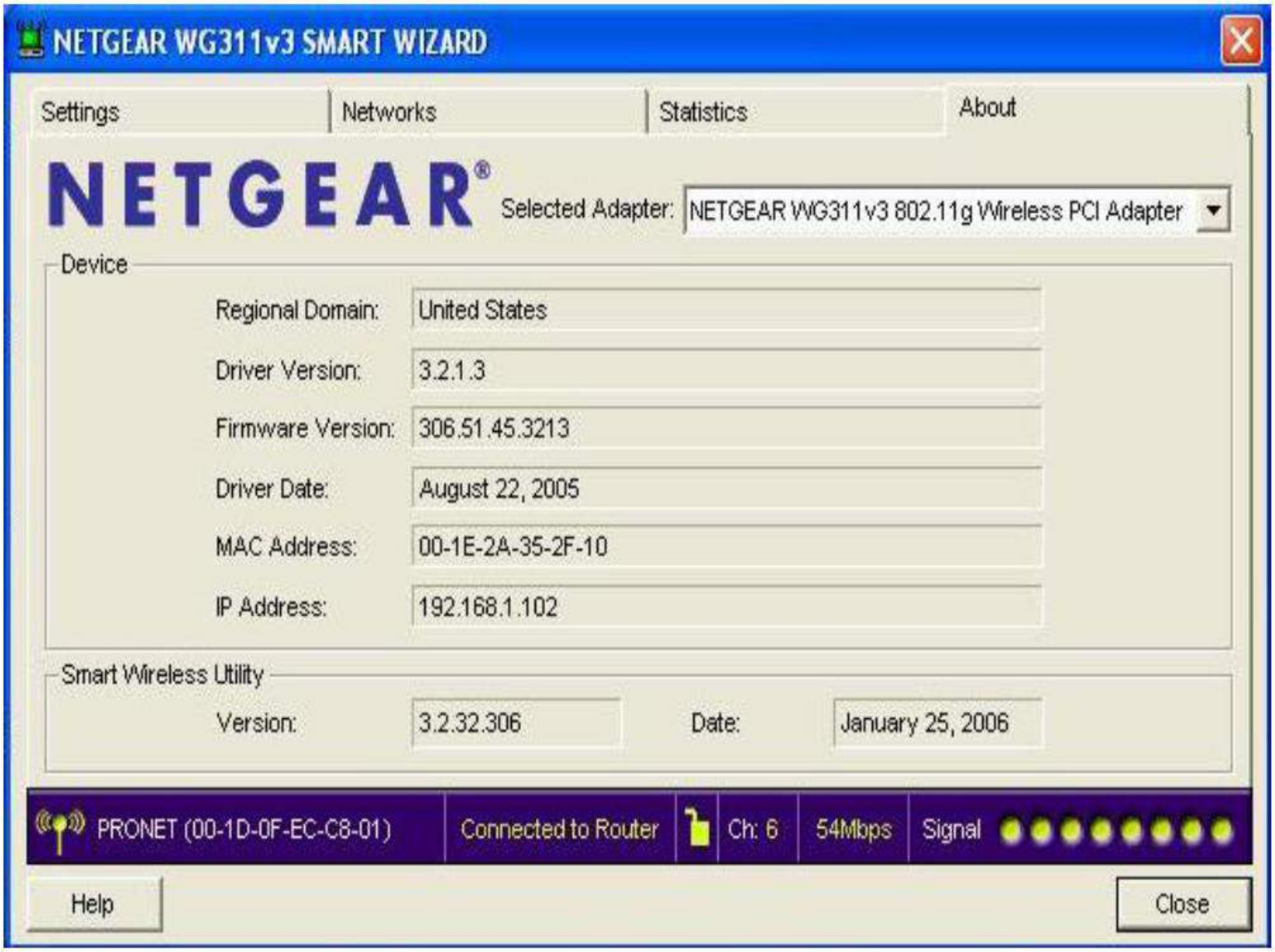
Transmit Statistics

Tx Mbps :	0.00
Tx Packets/s :	3
Total Tx Packets :	414
Tx Error :	0

Receive Statistics

Rx Mbps :	0.00
Rx Packets/s :	0
Total Rx Packets :	4
Rx Error :	0

PRONET (00-1D-0F-EC-C8-01) | Connected to Router | Ch: 6 | 54Mbps | Signal ●●●●●●●●



NETGEAR WG311v3 SMART WIZARD

Selected Adapter: NETGEAR WG311v3 802.11g Wireless PCI Adapter

Device

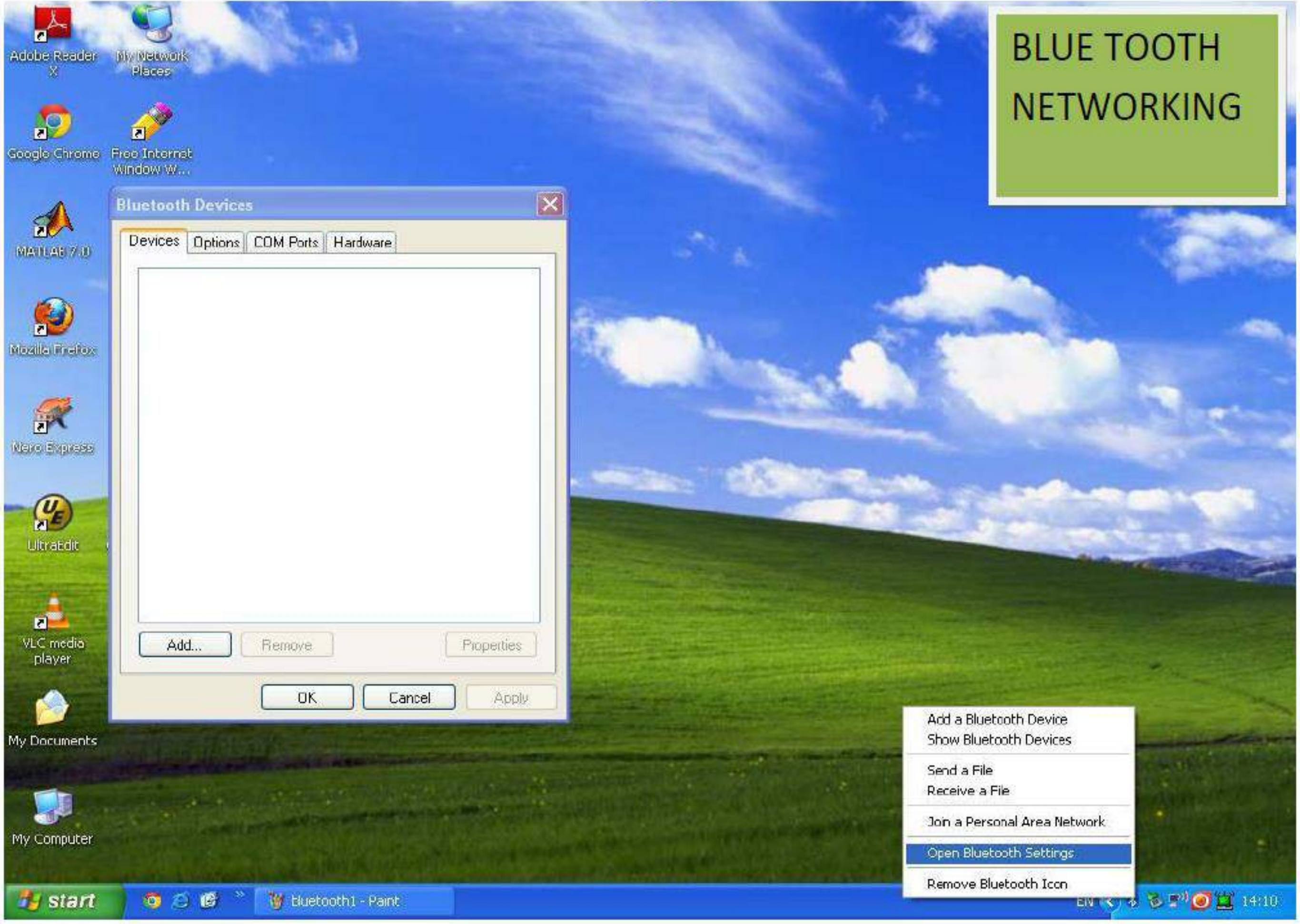
Regional Domain:	United States
Driver Version:	3.2.1.3
Firmware Version:	306.51.45.3213
Driver Date:	August 22, 2005
MAC Address:	00-1E-2A-35-2F-10
IP Address:	192.168.1.102

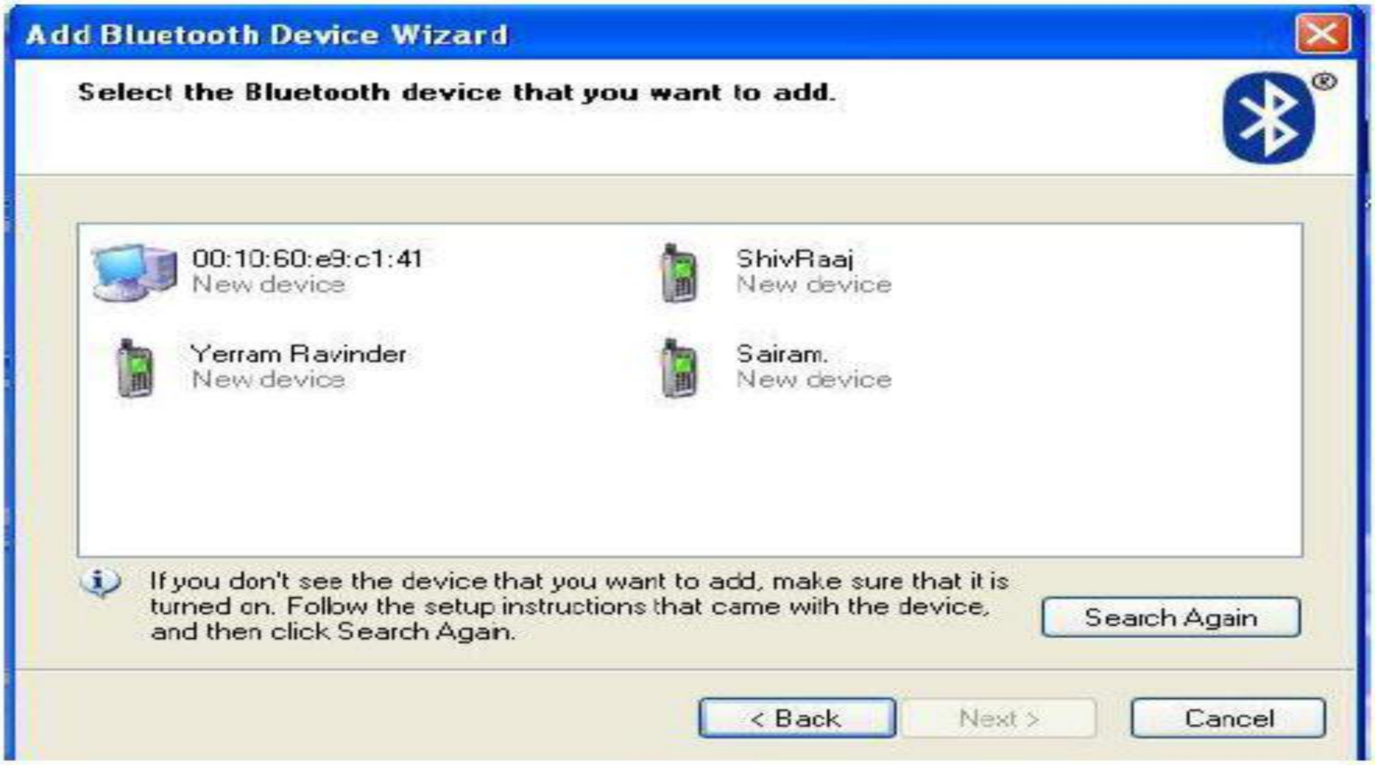
Smart Wireless Utility

Version:	3.2.32.306	Date:	January 25, 2006

PRONET (00-1D-0F-EC-C8-01) | Connected to Router | Ch: 6 | 54Mbps | Signal ●●●●●●●●

In system Tray of SYSTEM-1, the Bluetooth ICON is displayed like this .. Thus related options are as shown in figure.





Add Bluetooth Device Wizard

Select the Bluetooth device that you want to add.

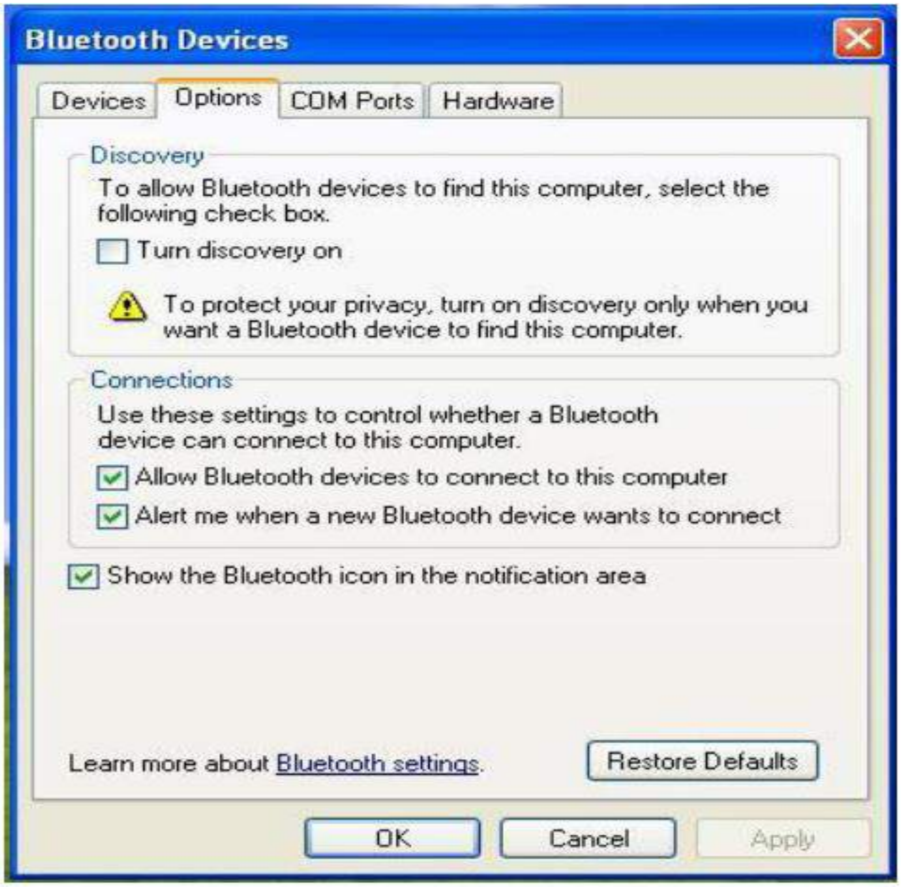
00:10:60:e9:c1:41
New device

ShivRaaj
New device

Yerram Ravinder
New device

Sairam.
New device

If you don't see the device that you want to add, make sure that it is turned on. Follow the setup instructions that came with the device, and then click Search Again.



Bluetooth Devices

Discovery

To allow Bluetooth devices to find this computer, select the following check box.

□ Turn discovery on

To protect your privacy, turn on discovery only when you want a Bluetooth device to find this computer.

Connections

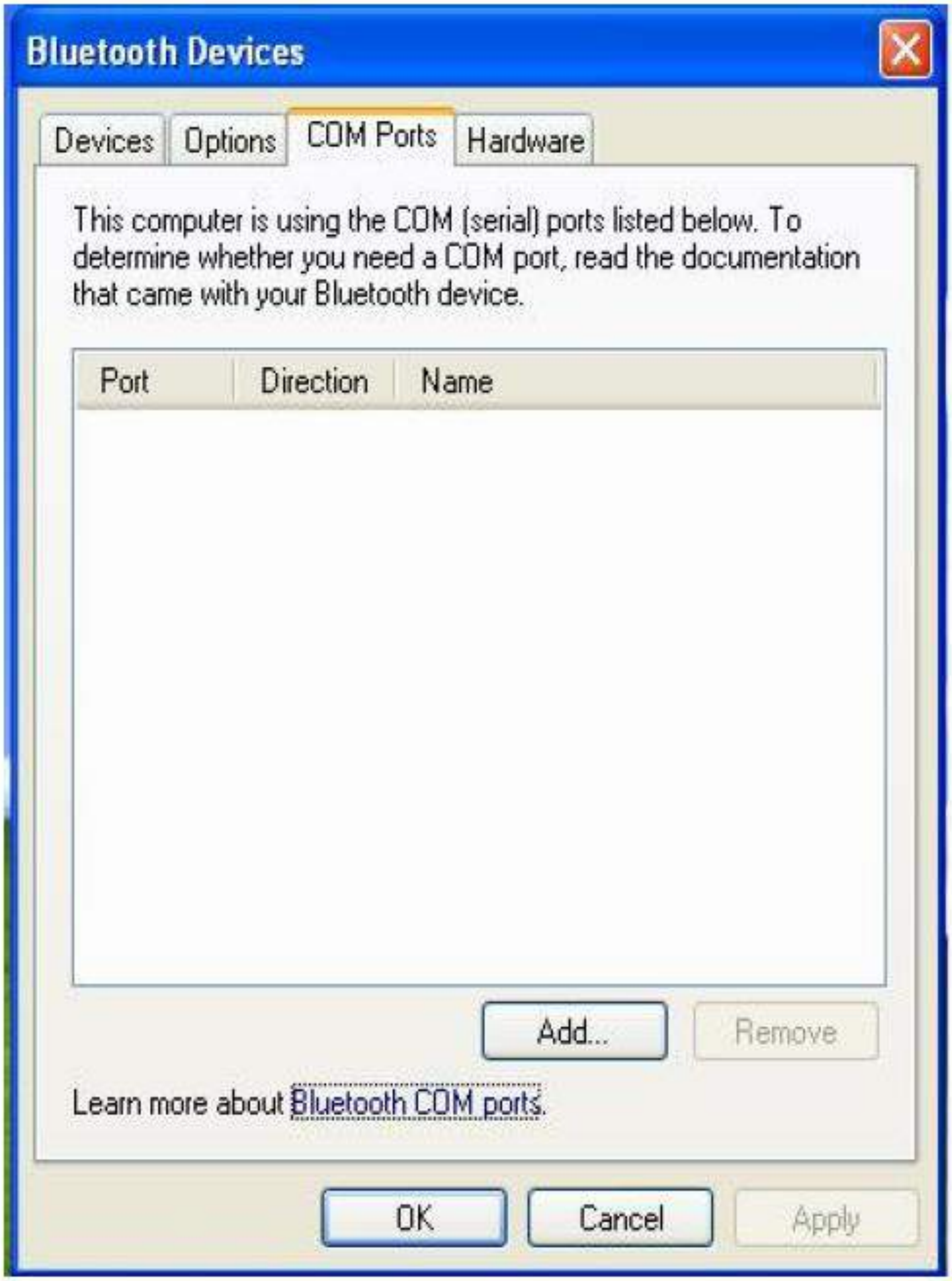
Use these settings to control whether a Bluetooth device can connect to this computer.

☑ Allow Bluetooth devices to connect to this computer

☑ Alert me when a new Bluetooth device wants to connect

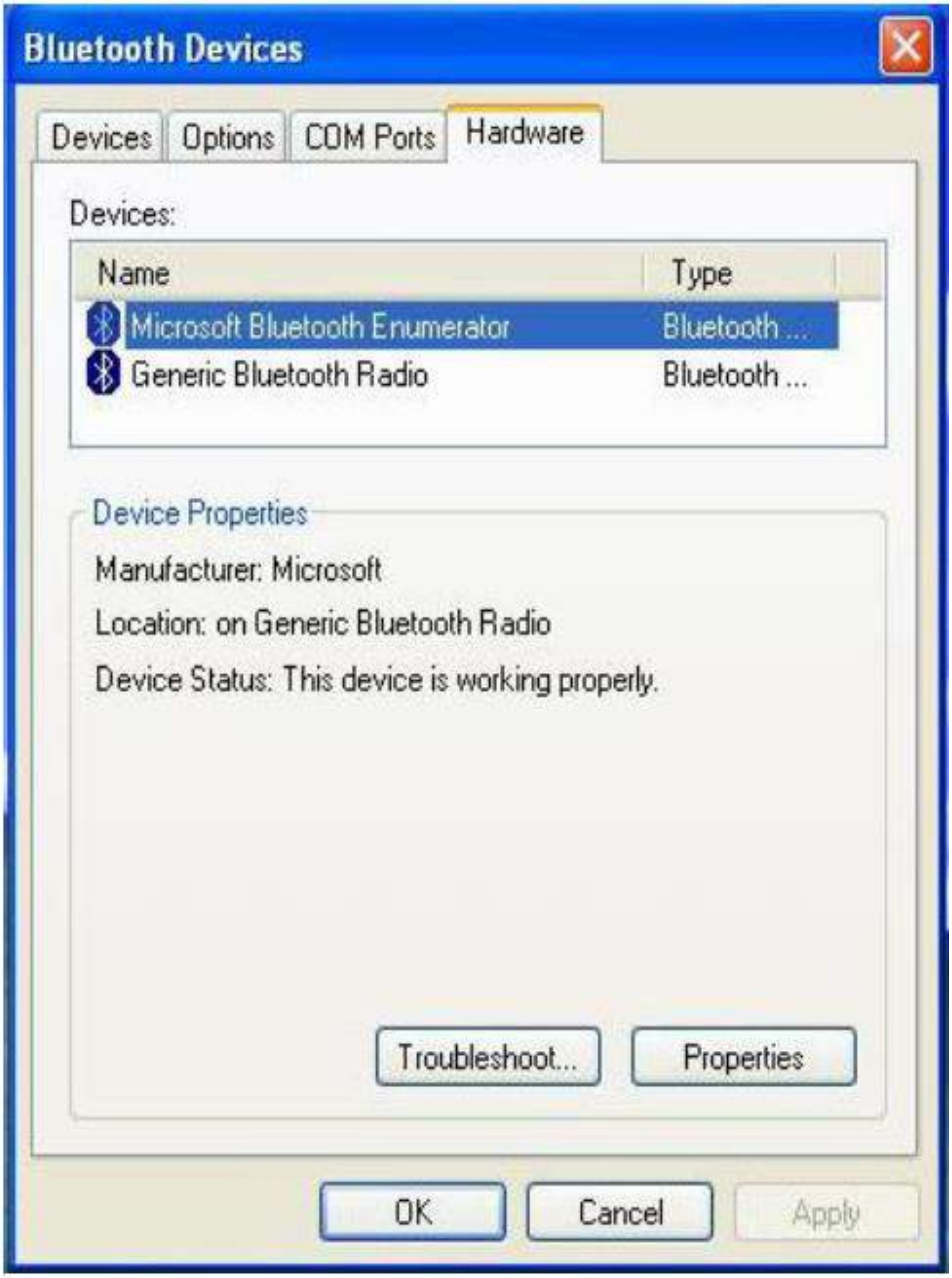
☑ Show the Bluetooth icon in the notification area

Learn more about Bluetooth settings.



This computer is using the COM (serial) ports listed below. To determine whether you need a COM port, read the documentation that came with your Bluetooth device.

Learn more about Bluetooth COM ports.



Devices:

Name	Type
Microsoft Bluetooth Enumerator	Bluetooth ...
Generic Bluetooth Radio	Bluetooth ...

Device Properties

Manufacturer: Microsoft

Location: on Generic Bluetooth Radio

Device Status: This device is working properly.

PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE - 411043

Department of Electronics & Telecommunication

CLASS : BE (E&TC)	**SUBJECT: CNS**
EXPT. NO : - 08	**DATE :** 03-11-2020

I. AIM : Study of Network Monitoring Tool/Software.

II. APPARATUS: Computer Systems

III. THEORY:

NETWORK MONITORING:

Network monitoring is the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via email, SMS or other alarms) in case of outages or other trouble. Network monitoring is part of network management.

Commonly measured metrics are response time, availability and uptime, although both consistency and reliability metrics are starting to gain popularity. The widespread addition of WAN optimization devices is having an adverse effect on most network monitoring tools, especially when it comes to measuring accurate end-to-end delay because they limit round-trip delay time visibility.

Status request failures, such as when a connection cannot be established, it times-out, or the document or message cannot be retrieved, usually produce an action from the monitoring system. These actions vary; An alarm may be sent (via SMS, email, etc.) to the resident sysadmin, automatic failover systems may be activated to remove the troubled server from duty until it can be repaired, etc.

SNMP PROTOCOL:

Simple Network Management Protocol (SNMP) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and more.

SNMP is widely used in network management for network monitoring. SNMP exposes management data in the form of variables on the managed systems organized in a management information base (MIB) which describe the system status and configuration. These variables can then be remotely queried (and, in some circumstances, manipulated) by managing applications.

Three significant versions of SNMP have been developed and deployed. SNMPv1 is the original version of the protocol. More recent versions, SNMPv2c and SNMPv3, feature improvements in performance, flexibility and security.

SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

Understand SNMP

SNMP consists of 3 items:

- SNMP Manager
- SNMP agent
- Management Information Database Otherwise called as Management Information Base (MIB)

SNMP Manager (sometimes called Network Management System – NMS): a software runs on the device of the network administrator (in most case, a computer) to monitor the network. A manager or management system is a separate entity that is responsible to communicate with the SNMP agent implemented network devices. This is typically a computer that is used to run one or more network management systems.

SNMP Manager’s key functions

- Queries agents
- Gets responses from agents
- Sets variables in agents
- Acknowledges asynchronous events from agents

SNMP Agent: A Software runs on network devices that we want to monitor (router, switch, server…)

The agent is a program that is packaged within the network element. Enabling the agent allows it to collect the management information database from the device locally and makes it available to the SNMP manager, when it is queried for. These agents could be standard (e.g. Net-SNMP) or specific to a vendor (e.g. HP insight agent)

SNMP agent’s key functions

- Collects management information about its local environment
- Stores and retrieves management information as defined in the MIB.
- Signals an event to the manager.
- Acts as a proxy for some non–SNMP manageable network node.

Management Information Base (MIB): is the collection of managed objects. This component makes sure that the data exchange between the manager and the agent remains structured. In other words, MIB contains a set of questions that the SNMP Manager can ask the Agent (and the Agent can understand them). MIB is commonly shared between the Agent and Manager. Every

SNMP agent maintains an information database describing the managed device parameters. The SNMP manager uses this database to request the agent for specific information and further translates the information as needed for the Network Management System (NMS). This commonly shared database between the Agent and the Manager is called Management Information Base (MIB).

Typically these MIB contains standard set of statistical and control values defined for hardware nodes on a network. SNMP also allows the extension of these standard values with values specific to a particular agent through the use of private MIBs.

In short, MIB files are the set of questions that a SNMP Manager can ask the agent. Agent collects these data locally and stores it, as defined in the MIB. So, the SNMP Manager should be aware of these standard and private questions for every type of agent.

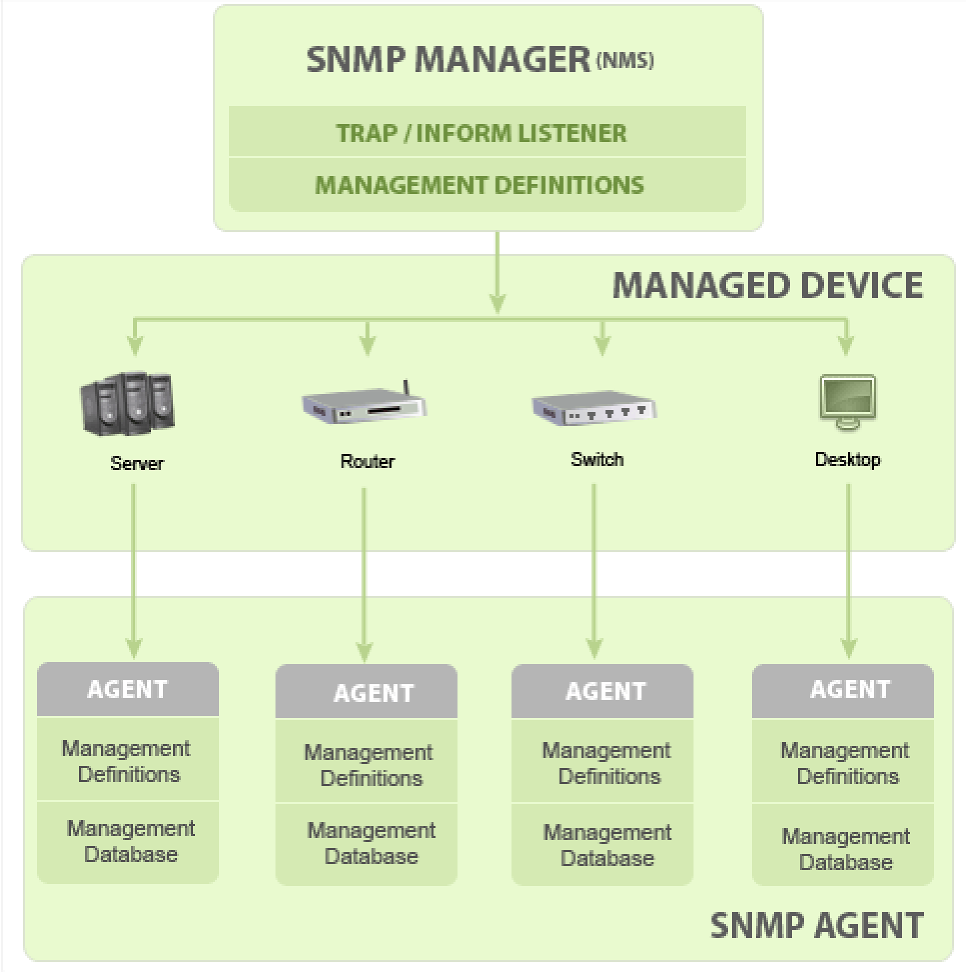


Fig1. Basic SNMP Communication Diagram

For example, in the topology above you want to monitor a router, a server and a Multilayer Switch. You can run SNMP Agent on all of them. Then on a PC you install a SNMP Manager software to receive monitoring information. SNMP is the protocol running between the Manager and Agent. SNMP communication between Manager and Agent takes place in form of messages. The monitoring process must be done via a MIB which is a standardized database and it contains parameters/objects to describe these networking devices (like IP addresses, interfaces, CPU utilization,..). Therefore the monitoring process now becomes the process of GET and SET the information from the MIB. A managed device or the network element is a part of the network that requires some form of monitoring and management e.g. routers, switches, servers, workstations, printers, UPSs, etc...

Look@Lan is an advanced network monitor that allows you to monitor your net in few clicks. Extremely easy to use and very fast in discovering your network's active nodes. Full of relevant features such as: auto-detect of network configuration, monitoring, reporting, trapping, statistics and graphs, network tree view, network log, proof single node scan, os detection.

Main Features:

- Auto-Detect of Network Settings
- Scanning of one or more Scan-Ranges
- Complete Management of Network Profiles
- World's Faster Node Discovery Scan
- Automatic and Manual Network Configuration
- Network Statistics and Graphs
- Profile Export (text and HTML)
- Advanced Trapping
- Network Log
- Network Tree View
- Proof Single Node Scan
- Reporting

Procedure:

1. Install the Look@Lan Network Monitoring tool on the machine.
2. Run the Look@Lan Network Monitoring program, so that Create new profile, Open Profile, Open Last Profile, Quick host scan and exit options will be observed.
3. Click on the Create new profile option and click on the interface list, select the IP address and proceed further directly or manually specifying the IP address range. Accordingly it starts the monitoring process and monitored data will be observed in the new window.
4. Network Monitored details are shown like IP address, Status(Online/Offline), Distance, OS(Win/ Not Win), Host name, NetBIOS name, NetBIOS User are shown for every PC available on LAN.
5. Select any one PC with specified IP address and right click on the same for “Do Proof Scan” option and proceed further for detailed monitoring.
6. After doing “Do Proof Scan”, the various data options are shown like Round trip time, Hostname Traceroute, NetBios details and Active services installed and running on the same PC.
7. Also, Graphical ping option is there for network debugging and testing.

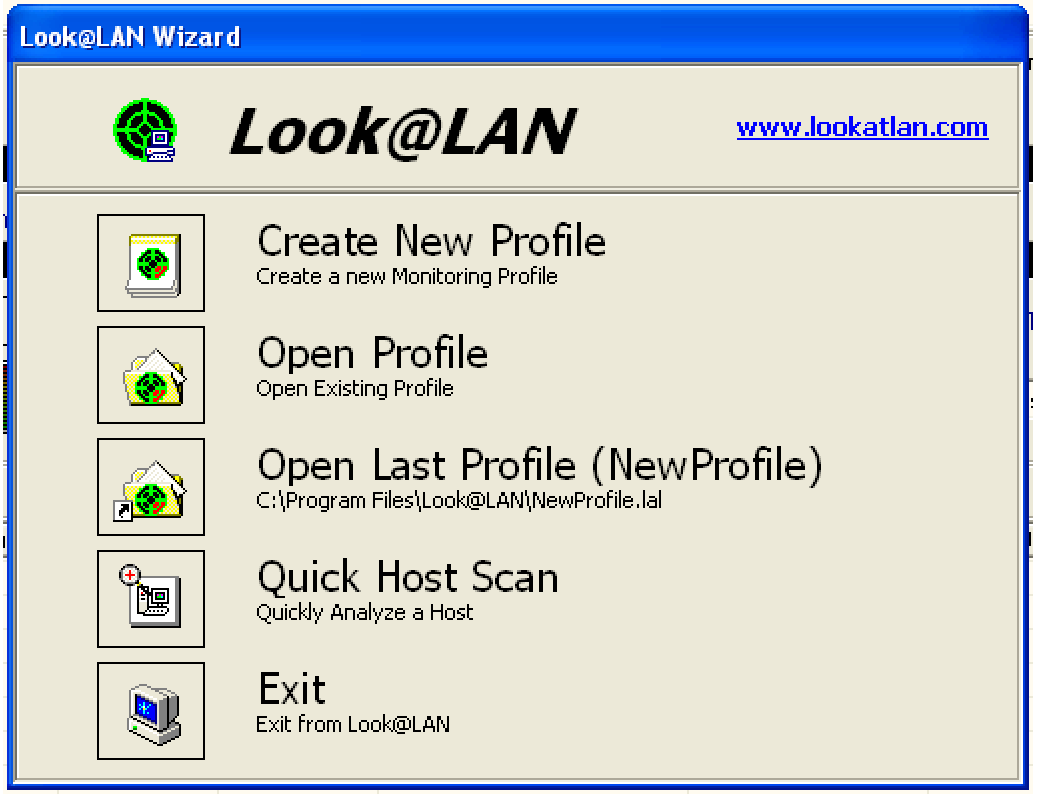
IV. **CONCLUSION:**

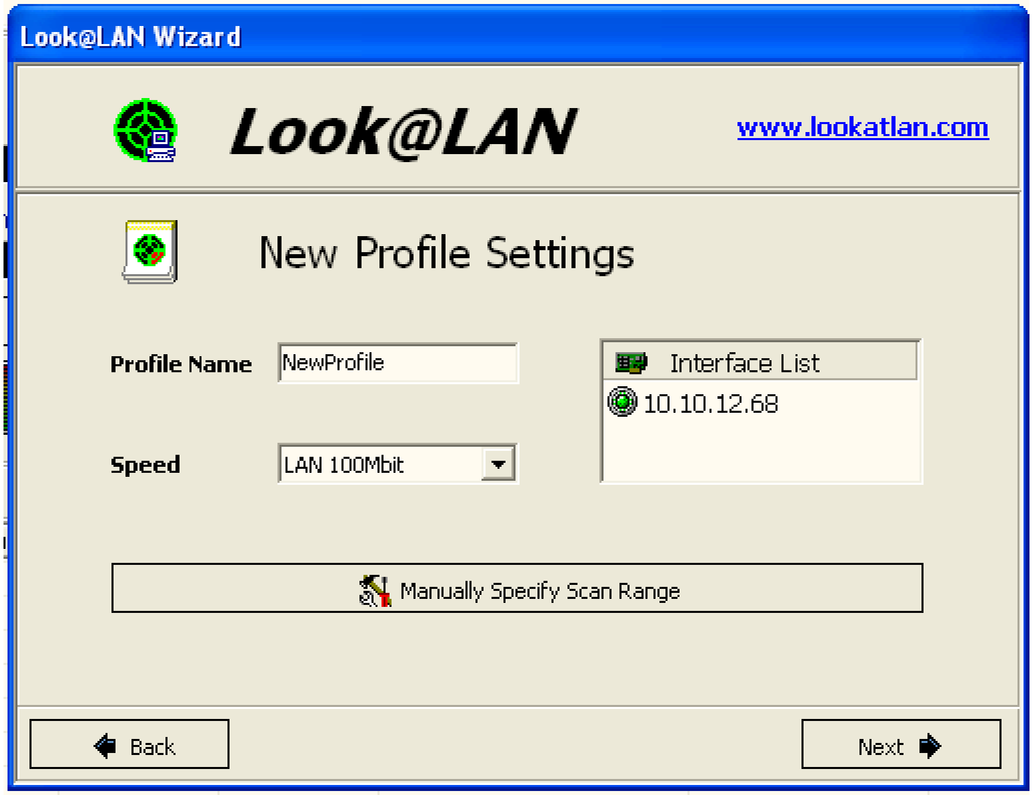
1. Network monitoring is basically a part of network management system & mainly used by network administrator to monitor entire campus network activities on single system.
2. All classes of IP address range is supported by the look @ LAN monitoring tool.
3. Details of hosts on the existing network is monitored with features like IP address, status (offline|online) operating system (windows) , Net Bios name, Net Bios username, etc
4. "Do proof Scan" option gives the details of all application layer services installed & running on the specific host like (Web, FTP & telnet, etc.)
5. SNMP is application layer protocol of TCP|IP
6. SNMP consists of three components & they are SNMP manager, SNMP agent & MIB (Management information Database).
7. Devices that supports SNMP protocol are servers, client, router, switches & modems, etc.

SIGNATURE

REFERENCES:

1. Data Communication. & Networking. B *Forouzan.*
2. Computer Networks' by Andrew Tannebaum.
3. "Data and Computer Communication" by William Stallings

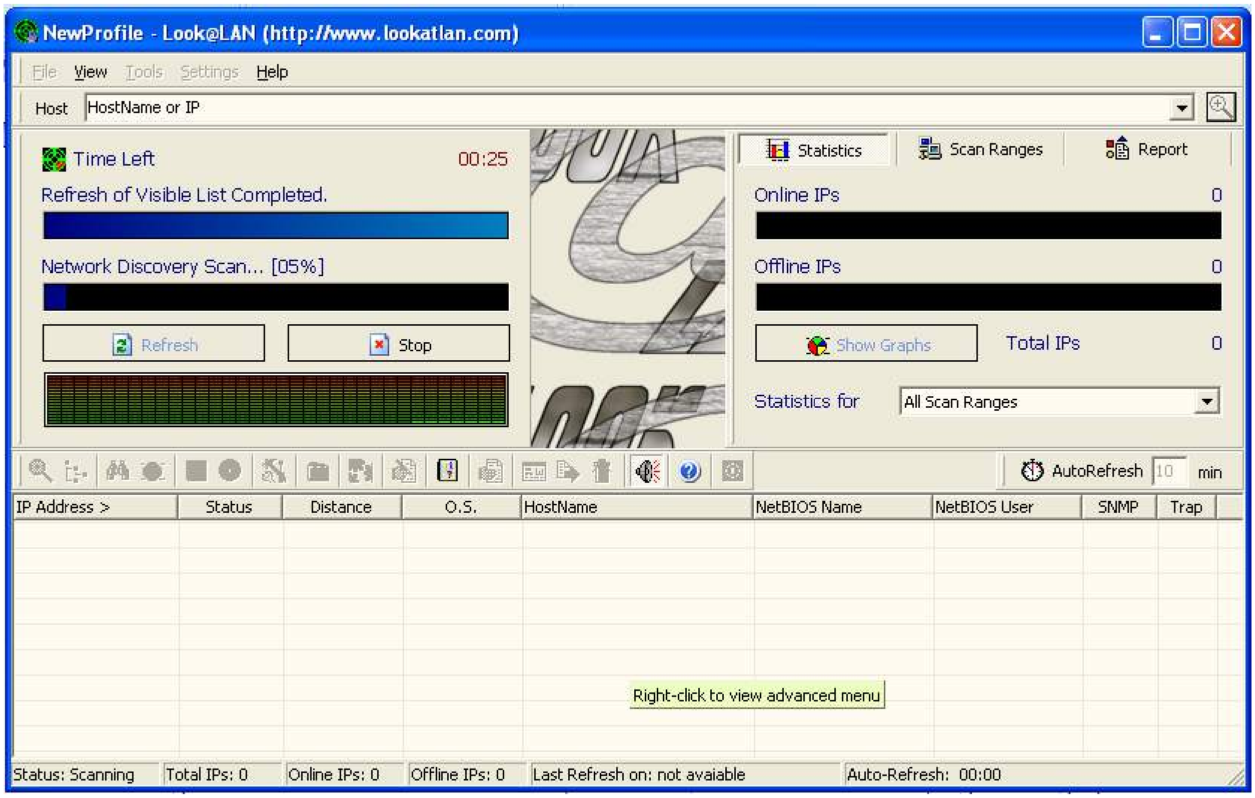




Profile Name NewProfile

Speed LAN 100Mbit

Interface List: 10.10.12.68



NewProfile - Look@LAN (http://www.lookatlan.com)

HostName or IP

Time Left 00:25

Refresh of Visible List Completed.

Network Discovery Scan... [05%]

Online IPs 0

Offline IPs 0

Total IPs 0

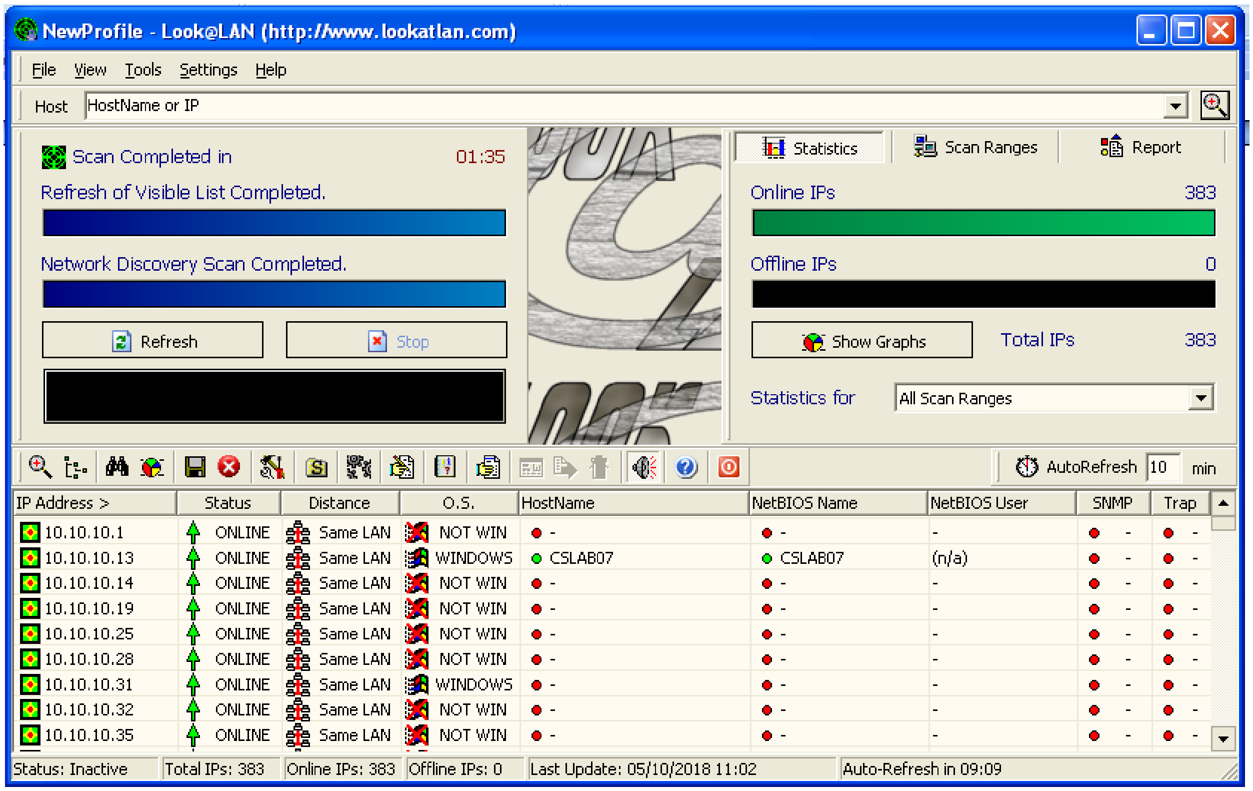
Statistics for: All Scan Ranges

AutoRefresh 10 min

IP Address >	Status	Distance	O.S.	HostName	NetBIOS Name	NetBIOS User	SNMP	Trap

Right-click to view advanced menu

Status: Scanning | Total IPs: 0 | Online IPs: 0 | Offline IPs: 0 | Last Refresh on: not avaiable | Auto-Refresh: 00:00



NewProfile - Look@LAN (http://www.lookatlan.com)

HostName or IP

Scan Completed in 01:35

Refresh of Visible List Completed.

Network Discovery Scan Completed.

Online IPs 383

Offline IPs 0

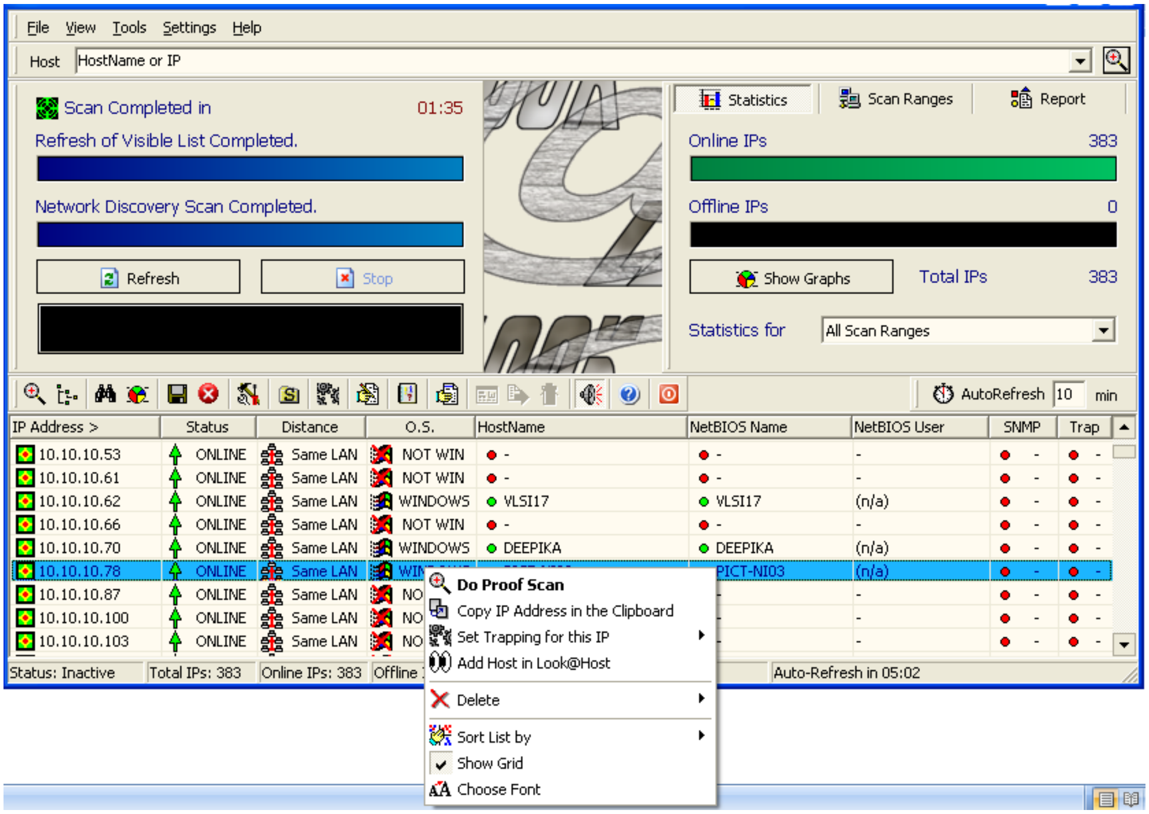
Total IPs 383

Statistics for: All Scan Ranges

AutoRefresh 10 min

IP Address >	Status	Distance	O.S.	HostName	NetBIOS Name	NetBIOS User	SNMP	Trap
10.10.10.1	ONLINE	Same LAN	NOT WIN	● -	● -	-	● -	● -
10.10.10.13	ONLINE	Same LAN	WINDOWS	● CSLAB07	● CSLAB07	(n/a)	● -	● -
10.10.10.14	ONLINE	Same LAN	NOT WIN	● -	● -	-	● -	● -
10.10.10.19	ONLINE	Same LAN	NOT WIN	● -	● -	-	● -	● -
10.10.10.25	ONLINE	Same LAN	NOT WIN	● -	● -	-	● -	● -
10.10.10.28	ONLINE	Same LAN	NOT WIN	● -	● -	-	● -	● -
10.10.10.31	ONLINE	Same LAN	WINDOWS	● -	● -	-	● -	● -
10.10.10.32	ONLINE	Same LAN	NOT WIN	● -	● -	-	● -	● -
10.10.10.35	ONLINE	Same LAN	NOT WIN	● -	● -	-	● -	● -

Status: Inactive | Total IPs: 383 | Online IPs: 383 | Offline IPs: 0 | Last Update: 05/10/2018 11:02 | Auto-Refresh in 09:09



Scan Completed in 01:35

Refresh of Visible List Completed.

Network Discovery Scan Completed.

Online IPs 383

Offline IPs 0

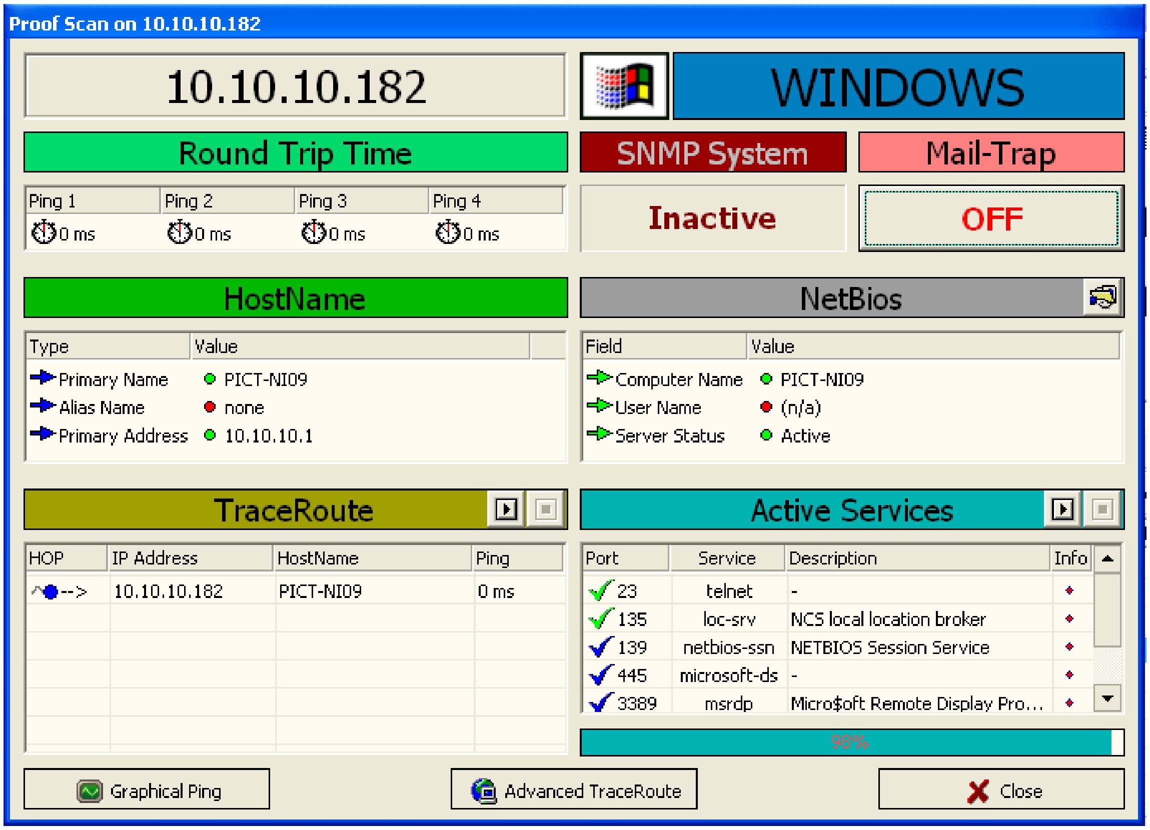
Total IPs 383

Statistics for: All Scan Ranges

AutoRefresh 10 min

IP Address >	Status	Distance	O.S.	HostName	NetBIOS Name	NetBIOS User	SNMP	Trap
10.10.10.53	ONLINE	Same LAN	NOT WIN	● -	● -	-	● -	● -
10.10.10.61	ONLINE	Same LAN	NOT WIN	● -	● -	-	● -	● -
10.10.10.62	ONLINE	Same LAN	WINDOWS	● VLSI17	● VLSI17	(n/a)	● -	● -
10.10.10.66	ONLINE	Same LAN	NOT WIN	● -	● -	-	● -	● -
10.10.10.70	ONLINE	Same LAN	WINDOWS	● DEEPIKA	● DEEPIKA	(n/a)	● -	● -
10.10.10.78	ONLINE	Same LAN	WIN		PICT-NI03	(n/a)	● -	● -
10.10.10.87	ONLINE	Same LAN	NO			-	● -	● -
10.10.10.100	ONLINE	Same LAN	NO			-	● -	● -
10.10.10.103	ONLINE	Same LAN	NO			-	● -	● -

Status: Inactive | Total IPs: 383 | Online IPs: 383 | Offline | Auto-Refresh in 05:02



Proof Scan on 10.10.10.182

10.10.10.182 | WINDOWS

Round Trip Time

Ping 1	Ping 2	Ping 3	Ping 4
0 ms	0 ms	0 ms	0 ms

SNMP System: Inactive

Mail-Trap: OFF

HostName

Type	Value
Primary Name	● PICT-NI09
Alias Name	● none
Primary Address	● 10.10.10.1

NetBios

Field	Value
Computer Name	● PICT-NI09
User Name	● (n/a)
Server Status	● Active

TraceRoute

HOP	IP Address	HostName	Ping
-->	10.10.10.182	PICT-NI09	0 ms

Active Services

Port	Service	Description	Info
✓ 23	telnet	-	◆
✓ 135	loc-srv	NCS local location broker	◆
✓ 139	netbios-ssn	NETBIOS Session Service	◆
✓ 445	microsoft-ds	-	◆
✓ 3389	msrdp	Micro$oft Remote Display Pro…	◆

98%

PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE - 411043

Department of Electronics & Telecommunication

CLASS : BE (E&TC) **SUBJECT: CN**
EXPT. NO : - 09 **DATE :** 27-10-2020

I. AIM : Write a program in 'c' for encryption and decryption. (For substitution cipher/and transposition cipher)

II. APPARATUS: Computer Systems (2 Nos.)

III. THEORY:

Introduction to Cryptography

Historically, four groups of people have used and contributed to the art of cryptography: the military, the diplomatic corps, diarists, and lovers. Of these, the military has had the most important role and has shaped the field over the centuries. Within military organizations, the messages to be encrypted have traditionally been given to poorly-paid, low level code clerks for encryption and transmission. The sheer volume of message prevented this work from being done by a few elite specialists.

Until; the advent of computers, one of the main constraints on cryptography had been the ability of the code clerk to perform the necessary transformation, often on battlefield with little equipment. An additional constraint has been the difficulty in switching over quickly from one cryptographic method to another one, since this entails retraining a large number of people. However, the danger of a code clerk being captured by the enemy has made it essential to be able to change the cryptographic method instantly if need be.

These conflicting requirements have given rise to the model Fig.1

The messages to be encrypted, known as the plain text, are transformed by a function that is parameterized by a key. The output of the encryption the output of the encryption process, known as the cipher text is then transmitted, often by messenger or radio. We assume the enemy, or intruder, hears and accurately copies down the complete cipher text. However, unlike the intended recipient, he does not know what the decryption key is and so cannot decrypt the cipher text easily. Sometimes the intruder can not only listen to the communication channel (passive intruder) but can also record messages and play them back later, inject in his own message, or modify legitimate message before they get to receiver (active intruder). The art of breaking ciphers, called cryptanalysis, and the art devising them (cryptography) is collectively known as cryptology.

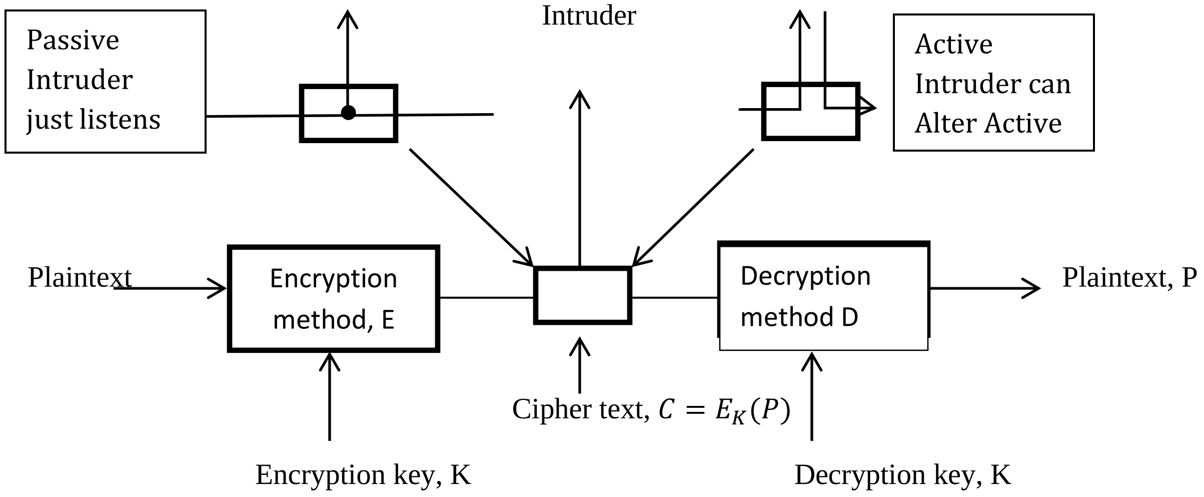


Fig 1.The encryption model (For a symmetric-key cipher)

It will often be useful to have notation for relating plaintext, cipher text, and keys. We will use $C = E_k(P)$ to mean that the encryption of the plaintext P using key K gives the ciphertext C. similarly$P = D_k(C)$ represents the decryption of the C to get the plaintext again. It then follows that

$$D_K\big(E_K(P)\big) = P$$

This notation suggests that E and D are just mathematical functions, which they are. The only tricky part is that both are functions of two parameters, and we have written one of the parameter (the key) as a subscript, rather than as an argument, to distinguish it from the message.

A fundamental rule of cryptography is that one must assume that the cryptanalyst knows the methods used for encryption and decryption. In other words, cryptanalyst knows how the encryption method, E, and decryption, D. of the fig. 1 work in detail. The amount of effort necessary to invent, test and install a new algorithm every time the old method is compromised (or thought to be compromised) has always made it in practical to keep the encryption algorithm secret. Thinking it is secret when it is not does more harm than good.

This is where the key enters. The key consists of short string that selects one of many potential encryption in contrast to general method which may only be change every few years, the key can be changed as often as required. Thus, our basic model is stable and publically known general method parameterized by secret and easily change key.

Encryption methods have historically been divided in two categories: substitution ciphers and transposition ciphers. We will now deal with each of these briefly as background for modern cryptography.

Substitution Ciphers:

In a substitution cipher each letter or group of letters is replaced by another letter or group of letters to disguise it. One of the oldest known ciphers is the Caesar cipher, attributed to Julius Caesar. In this method, a becomes D, b becomes E, c becomes F,..., and z becomes C. For example, attack becomes DWWDFN.

In examples, plaintext will be given in lower case letters, and cipher text in upper case letters.

A slight generalization of the Caesar cipher allows the cipher text alphabet to be shifted by k letters, instead of always 3. In this case k becomes a key to the general method of circularly shifted alphabets. The Caesar cipher may have fooled Pompey, but it has not fooled anyone since.

The next improvement is to have each of the symbols in the plaintext, say, the 26 letters for simplicity, and map onto some other letter.

For example,

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cipher text	Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

The general system of symbol-for-symbol substitution is called a **monoalphabetic s**ubstitution, with the key being the 26-letter string corresponding to the full alphabet. For the key above, the plaintext attack would be transformed into the cipher text QZZQEA.

At first glance this might appear to be a safe system because although the cryptanalyst knows the general system (letter-for-letter substitution), he does not know which of the 26! 4 x 1026 possible keys are in use. In contrast with the Caesar cipher, trying all of them is not a promising approach. Even at 1nsec per solution, a computer would take 1010 years to try all the keys. Nevertheless, given a surprisingly small amount of cipher text, the cipher can be broken easily. The basic attack takes advantage of the statistical properties of natural languages. In English, for example, e is the most common letter, followed by t, o, a, n, i, etc. The most common two-letter combinations, or diagrams, are th, in, er, re, and an. The most common three-letter combinations, or trigrams, are the, ing, and, and ion.

A cryptanalyst trying to break a mono alphabetic cipher would start out by counting the relative frequencies of all letters in the cipher text. Then he might tentatively assign the most common one to e and the next most common one to t. He would then look at trigrams to find a common one of the form tXe, which strongly suggests that X is h. Similarly, if the pattern thYt occurs frequently, the Y probably stands for a. With this information, he can look for a frequently occurring trigram of the form aZW, which is most likely and. By making guesses at common letters, diagrams, and trigrams and knowing about likely patterns of vowels and consonants, the cryptanalyst builds up a tentative plaintext, letter by letter.

Transposition cipher:

Substitution ciphers preserve the order of the plaintext symbols but disguise them. Transposition ciphers, in contrast, reorder the letters but do not disguise them. Figure 2 depicts a common transposition cipher, the columnar transposition.

The cipher is keyed by a word or phrase not containing any repeated letters. In this e.g. MEGABUCK is the key. The purpose of the key is to number the columns, column1 being under the key letter closest to the start of the alphabet and so on. The plaintext is written horizontally, in rows, padded to fill the matrix if need be. The cipher text is read out by columns, starting with the column1 whose key letter is the lowest.

To break a transposition cipher, the cryptanalyst must first be aware that he is dealing with a transposition cipher. By looking at the frequency of E , T, A , O , I , N , etc. ,it is easy to see if they fit the normal pattern for plain text. If so, the cipher is clearly a transposition cipher, because in such a cipher every letter represents itself, keeping the frequency distribution intact.

The next step is to make a guess at the number of columns. In many cases a probable word or phrase may be guessed at from the context.

For e.g. suppose that our cryptanalyst suspects that plaintext phrase million dollars occurs somewhere in the message. Observe that diagrams MO, IL , LL , LA , IR , AND OS occur in the cipher text as a result of this phrase wrapping around. The cipher text letter O follows the cipher text letter M (i.e. they are vertically adjacent in column 4) because they are separated in the probable phrase by a distance = the key length. If a key of length seven had been used, the diagrams MD.IO, LL , LL ,IA,OR,NS would have occurred instead. In fact, for each key length, a different set of diagrams is produced in the cipher text. By hunting for the various possibilities, the cryptanalyst can often easily determine the key length.

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Figure 2 A Transposition Cipher

Plaintext:

PleasetransferonemilliondollarstoMyswissbankaccountsixtwotwo

Ciphertext:
AFLLSKSOSELAWAIATOOSSCTCLNMOMANTESILYNTWRNNTSOWDPAEDOBUOERIRICXB

The remaining step is to order the columns. When the number of columns, k, is small, each of the k(k-1) column pairs can be examined to see if its diagram frequencies match those for English plaintext . The pair with the best match is assumed to be correctly positioned. Now each remaining is tentatively tried as the successor to this pair. The column whose trigram and diagram frequencies give the best match is tentatively assumed to be correct. The predecessor column is found in the same way. The entire process is continued until a potential ordering is found. Chances are that the plaintext will be recognizable at this point (e.g., if million occurs, it is clear what the error is).

Some transposition ciphers accept a fixed-length block of input and produce a fixed – length block of output .These ciphers can be completely described by giving a list telling the order in which the characters are to be output. For example, the cipher of fig.8-3 can be seen as a 64 character block cipher. Its output is 4,12,20,28,36,44,52,60,5,13,…,62.In other words, the fourth input character ,a, is the first to be output, followed by the twelfth, f , and so on.

Procedure:

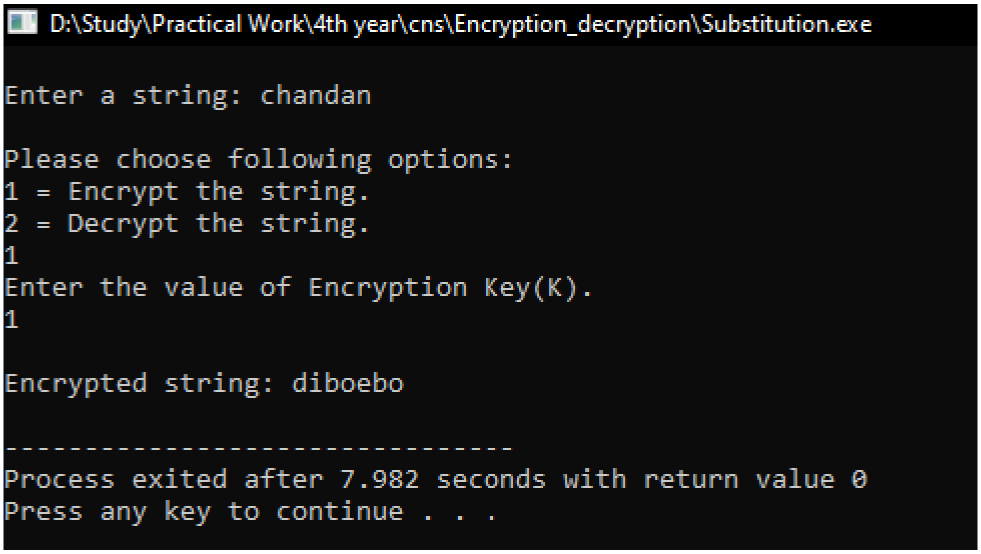
1) Write a ‘C’ program for encryption/decryption of substitution cipher and verify the result.
2) Write a ‘C’ program for encryption/decryption of transposition cipher and verify the result.
3) ADD Flowchart +Algorithm + program print + result o/p

IV. CODE:

```
/*Encryption and Decryption using Substitution Cipher*/

#include <stdio.h>

int main()
{
  int i, x, k;
  char str[100];

  printf("\nEnter a string:\t");
  gets(str);

  printf("\nPlease choose following options:\n");
  printf("1 = Encrypt the string.\n");
  printf("2 = Decrypt the string.\n");
  scanf("%d", &x);
  switch(x)
  {
        case 1:
                printf("Enter the value of Encryption Key(K).\n");
                scanf("%d", &k);
                for(i = 0; (i < 100 && str[i] != '\0'); i++)
                str[i] = str[i] + k;                    //the key for encryption is k that is
added to ASCII value

                printf("\nEncrypted string: %s\n", str);
                break;

        case 2:
                printf("Enter the value of Encryption Key(K).\n");
                scanf("%d", &k);
                for(i = 0; (i < 100 && str[i] != '\0'); i++)
                str[i] = str[i] - k;                    //the key for encryption is k that is
subtracted to ASCII value

                printf("\nDecrypted string: %s\n", str);
                break;

        default:
                printf("\nError\n");
  }
  return 0;
}
```

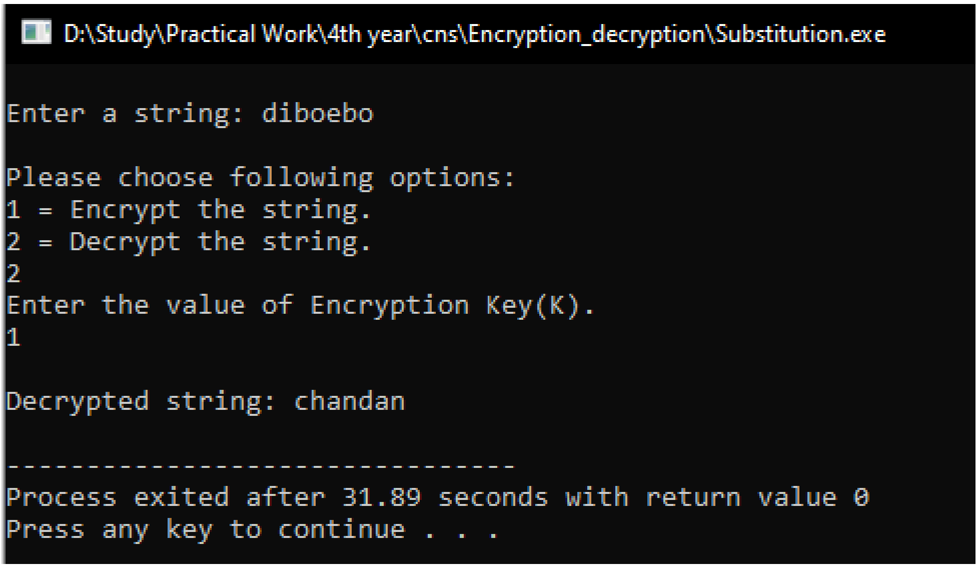
OUTPUT:

Encryption:


D:\Study\Practical Work\4th year\cns\Encryption_decryption\Substitution.exe

```
Enter a string: chandan

Please choose following options:
1 = Encrypt the string.
2 = Decrypt the string.
1
Enter the value of Encryption Key(K).
1

Encrypted string: diboebo

--------------------------------
Process exited after 7.982 seconds with return value 0
Press any key to continue . . .
```

Decryption:


D:\Study\Practical Work\4th year\cns\Encryption_decryption\Substitution.exe

```
Enter a string: diboebo

Please choose following options:
1 = Encrypt the string.
2 = Decrypt the string.
2
Enter the value of Encryption Key(K).
1

Decrypted string: chandan

--------------------------------
Process exited after 31.89 seconds with return value 0
Press any key to continue . . .
```

```
/*Encryption and Decryption using Transposition Cipher*/

#include<stdio.h>
#include<string.h>
#include<math.h>

void cipher(int i,int c);
int findMin();
void makeArray(int,int);
```

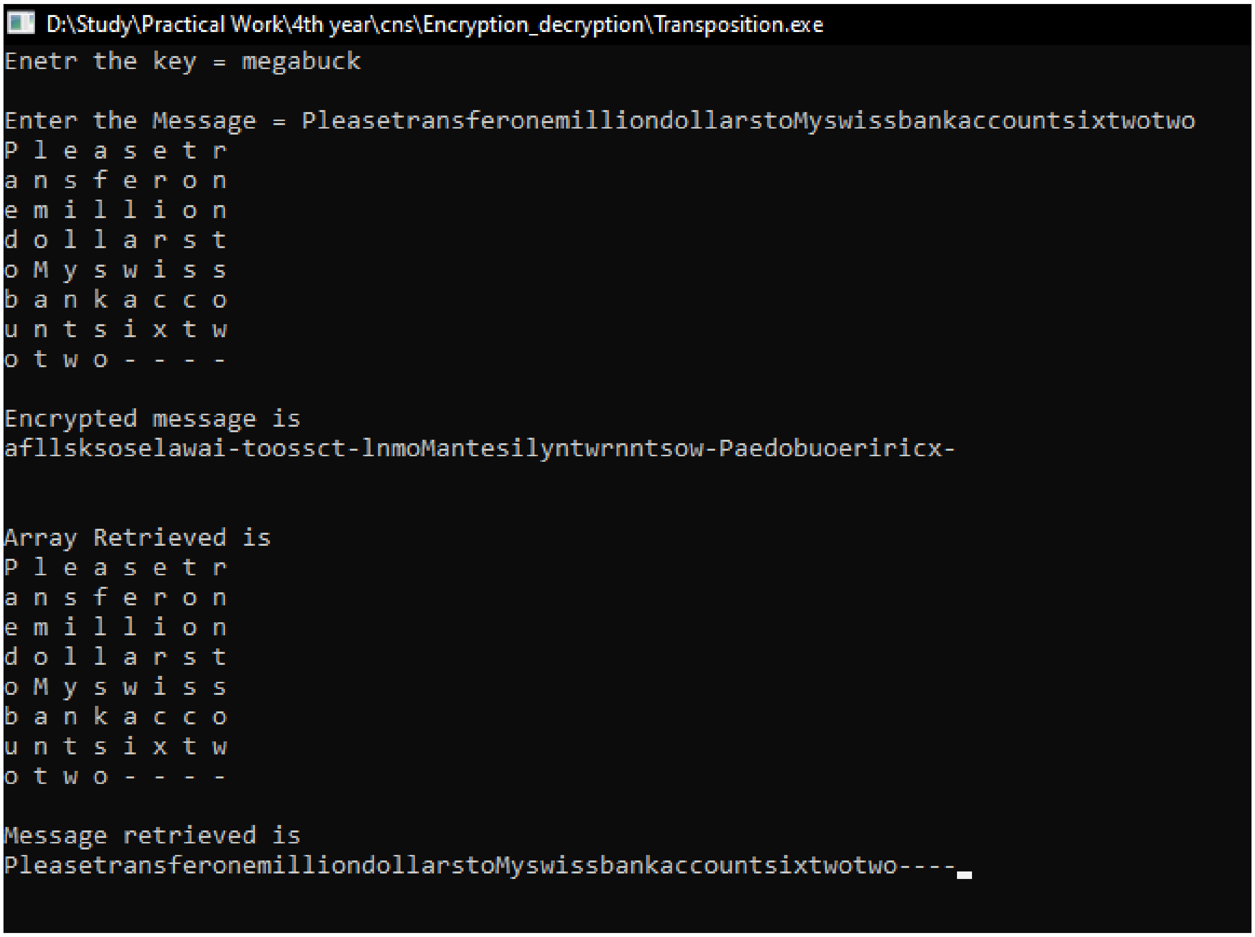
```
char arr[22][22],darr[22][22],emessage[111],retmessage[111],key[55];
char temp[55],temp2[55];
int k=0;
int main()
{
	char message[111],dmessage[111];
	int i,j,klen,emlen,flag=0;
	int r,c,index,min,rows;
	printf("Enetr the key = ");
	gets(key);
	printf("\nEnter the Message = ");
	gets(message);
	strcpy(temp,key);
	klen=strlen(key);
	c=klen;
	r=ceil(strlen(message)/(double)c);
	k=0;
	for (i=0;i<r;i++)
	{
		for (j=0;j<c;j++)
		{
			if(message[k]=='\0')
			{
				flag=1;
				arr[i][j]='-';
			}else
			{
				arr[i][j]=message[k++];
			}
		}
	}
	for (i=0;i<r;i++)
	{
		for (j=0;j<c;j++)
		{
			printf("%c ",arr[i][j]);
		}
		printf("\n");
	}
	k=0;
```

```
for (i=0;i<klen;i++)
{
	index=findMin();
	cipher(index,r);
}
emessage[k]='\0';
printf("\nEncrypted message is\n");
for (i=0;emessage[i]!='\0';i++)
   printf("%c",emessage[i]);
printf("\n\n");
//deciphering
emlen=strlen(emessage);
//emlen is length of encrypted message
strcpy(temp,key);
rows=emlen/klen;
//rows is no of row of the array to made from ciphered message
rows;
j=0;
for (i=0,k=1;emessage[i]!='\0';i++,k++)
{
	//printf("\nEmlen=%d",emlen);
	temp2[j++]=emessage[i];
	if((k%rows)==0)
	{
		temp2[j]='\0';
		index=findMin();
		makeArray(index,rows);
		j=0;
	}
}
printf("\nArray Retrieved is\n");
k=0;
for (i=0;i<r;i++)
{
	for (j=0;j<c;j++)
	{
		printf("%c ",darr[i][j]);
		//retrieving message
		retmessage[k++]=darr[i][j];
	}
```

```
        printf("\n");
    }
    retmessage[k]='\0';
    printf("\nMessage retrieved is\n");
    for (i=0;retmessage[i]!='\0';i++)
      printf("%c",retmessage[i]);
    getch();
    return(0);
}
void cipher(int i,int r)
{
    int j;
    for (j=0;j<r;j++)
    {
        emessage[k++]=arr[j][i];
    }
    // emessage[k]='\0';
}
void makeArray(int col,int row)
{
    int i,j;
    for (i=0;i<row;i++)
    {
        darr[i][col]=temp2[i];
    }
}
int findMin()
{
    int i,j,min,index;
    min=temp[0];
    index=0;
    for (j=0;temp[j]!='\0';j++)
    {
        if(temp[j]<min)
        {
            min=temp[j];
            index=j;
        }
    }
    temp[index]=123;
```

```
        return(index);
}
```

OUTPUT:



D:\Study\Practical Work\4th year\cns\Encryption_decryption\Transposition.exe

```
Enetr the key = megabuck

Enter the Message = PleasetransferonemilliondollarstoMyswissbankaccountsixtwotwo
P l e a s e t r
a n s f e r o n
e m i l l i o n
d o l l a r s t
o M y s w i s s
b a n k a c c o
u n t s i x t w
o t w o - - - -

Encrypted message is
afllsksoselawai-toossct-lnmoMantesilyntwrnntsow-Paedobuoeriricx-


Array Retrieved is
P l e a s e t r
a n s f e r o n
e m i l l i o n
d o l l a r s t
o M y s w i s s
b a n k a c c o
u n t s i x t w
o t w o - - - -

Message retrieved is
PleasetransferonemilliondollarstoMyswissbankaccountsixtwotwo----
```

V. CONCLUSION:

1. Substitution cipher & tranportation cipher encryption/decryption technique is verified practically.
2. There are three types of encryption decryption techniques that are being used commercially.
   a) symmetric key algorithm.
   b) Asymmetric key algorithm.
   c) Wash function.

3. If proper decryption key is entered in c program then only original plain text is recovered, otherwise text file gives garbage values.

SIGNATURE

REFERENCES:

1. Data Communication. & Networking. B *Forouzan.*
2. Computer Networks' by Andrew Tanenbaum.
3. "Data and Computer Communications " by William Stallings