



GOVERNMENT OF PAKISTAN
MINISTRY OF COMMUNICATION
CONSTRUCTION TECHNOLOGY TRAINING INSTITUTE
ISLAMABAD



Network Scanning Tool (LAN Scanner)

In partial fulfillment of the requirement for the degree of

Diploma of Associate Engineer

Information Communication Technology

By

DAE ICT 3rd Year (A)

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

IN THE NAME OF ALLAH THE MOST MERCIFUL THE MOST
COMPASSIONATE AND THE MOST BENEFICENT

DEDICATION

PROJECT ADVISER

Madam Zeba Ghaffar

ASST ADVISOR

Mr. Hassan Anjum

Mr. Imran

GROUP LEADER

Ghulam Haider (18-ICT-14)

ASST GROUP LEADER

Daniyal Asghar (18-ICT-16)

GROUP MEMBER

Afghan Naeem (18-ICT-12)

Umair Ali(18-ICT-30)



ACKNOWLEDGEMENT

There is no success without ALLAH almighty. We are grateful to ALLAH almighty, who has given us guidance, strength and enabled us to accomplish this project. Foremost, we would like to express our sincere gratitude to our Group Advisor Madam Zeba Ghaffar for their continuous support on our project and research, for their patience, motivation, enthusiasm and immense knowledge and then we would like to thanks our HoD (ICT Dept) Col.(RETD).Mr.Iftikhar for their support and for enlightening us the first glance of research. We could not have imagined having a better HoD and advisor for our project. Last but not the least; we would like to thank our parents for supporting us spiritually and financially throughout this project.



CONSTRUCTION TECHNOLOGY TRAINING INSTITUTE

Department of Information Communication Technology

ICT 3rd YEAR “A”

SESSION 2018-2021

APPROVED BY

PROJECT ADVISOR:

Mam Zeba Ghaffar

TRAINING OFFICER:

Col(retd). Mr Altaf Bajwa

CHIEF INSTRUCTOR (ICT):

Col(retd). Mr. Iftikhar

DIRECTOR:

Col(retd). Mr. Atif Jalil

Contents

1 INTRODUCTION:	9
1.1 PROBLEM STATEMENT	9
1.2 OBJECTIVE AND GOALS	9
1.3 SCOPE	10
1.4 DEFINITIONS, ACRONYMS, AND ABBREVIATIONS.	10
2 THE OVERALL DESCRIPTION	12
2.1 PRODUCT PERSPECTIVE	12
• MANAGE DYNAMIC NETWORKS BY IP SCANNING ACROSS MULTIPLE SUBNETS IN REAL-TIME	13
• AUDIT NETWORK RESOURCE USAGE WITH GRANULAR IP SCAN REPORTS	13
2.2 INTERFACES	13
• SOFTWARE INTERFACES	13
• HARDWARE INTERFACES	13
2.3 MEMORY CONSTRAINTS	14
• REQUIREMENTS FOR A LOCAL PC	14
• RECOMMENDED HARDWARE REQUIREMENTS	14
• MINIMUM HARDWARE REQUIREMENTS	14
• REQUIREMENTS	14
• SUPPORTED PLATFORMS (x86/x64)	14
2.4 OPERATIONS	14
• PORT SCANNING:	14
• MAC ADDRESS:	14
• HOST NAME	14
• IP ADDRESS	15
• SHARED PC FOLDER	15
• PING SPECIFIC IP	15
2.5 NON-FUNCTIONAL REQUIREMENTS	15
• RELIABILITY	15
• AVAILABILITY	15
• MAINTAINABILITY	15
3 IMPLEMENTATION	17
3.1 AUTOMATICALLY IP PICKING OF OUR COMPUTER	17
3.2 TAKING 3 OCTETS OF LOCAL IP ADDRESS	17
3.3 DON'T WORK IF WE DON'T HAVE NETWORK	17
3.4 TRANSFER CONTROL TO BACKGROUND WORKER	18
3.5 MAC ADDRESS, IP ADDRESS, HOSTNAME, VENDORNAME	18
3.5.1 IP ADDRESS & HOSTNAME	18

3.5.2	ADDING IP ADDRESS AND HOSTNAME TO DATAGRID VEIW	19
3.5.3	FINDING MAC ADDRESS THROUGH IP ADDRESS	19
3.5.4	ADDING MAC ADDRESS TO DATAGridView	20
3.5.5	DATAGridView1.Rows[nRowIndex].Cells[3].Value = "DELL INC";	20
3.6	DATA GRID VIEW CODE FOR OPENING NEW WINDOW	23
3.6.1	FORM 2 PINGING	24
3.6.2	TRACE ROUTE COMMAND	24
3.6.3	SENDING DATA FOR PORT SCANNING	24
3.6.4	SHARED FOLDER	25
3.7	PORT SCANNING	26
3.8	SYSTEM DIAGRAM	29
4	SUMMARY AND CONCLUSION	30
5	FUTURE ENHANCEMENT	31
6	REFERENCES	32

1 INTRODUCTION:

Modern businesses can't function without an internal network, where data and files are kept and shared by the employees. Businesses, whether big or small, need to have experienced IT staff to protect the company's network from data theft and interference. If you think your business is too small for cybercriminals to notice, it's time to review your security measures.

Regular scanning of your network allows you to keep track of the devices on your network, view how they're performing, spot the flaws, and understand the flow of traffic between connected devices and applications. Thus, network scanning is a process helping admins gather information from all devices or endpoints on a network. During a network scan, all the active devices on the network send signals, and once the response is received, the scanner evaluates the results and checks to see if there are inconsistencies.

The Network Scanning Tool used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection. Network scanning is mainly used for security assessment, system maintenance, and also for performing attacks by hackers. The program will detect hardware addresses, vulnerabilities, and security holes. The Network Scanning Tool will have both interfaces Command Line Interface (CLI) and Graphical User Interface (GUI).

1.1 Problem statement

LAN scanners are programs that pings all the IP addresses on a LAN. A ping is a basic network command that allows a user to verify that a particular IP address exists, and can accept requests. Using ping, a LAN scanner reports what comes back, on what IP address, including the MAC addresses and hostnames (if available).

This is powerful information as you can immediately see what is plugged into your LAN, and quickly identify errors in addressing, missing clients and so on.

Once devices on your network are identified, you can further run a port scan on IP address to check whether it is accepting requests on the ports you require. A network port is a number that identifies one side of a connection between two devices. Devices use port numbers to determine to which process should be delivered.

1.2 Objective and Goals

- Detect the live host on the network (host discovery)
- Detect the open ports on the host (port discovery or enumeration)
- Detect the IP address (IP address discovery)
- Detect the hardware address

1.3 SCOPE

This software has been manufactured by using Visual Studio. Reliable and free network scanner to analyze LAN. The program shows all network connected devices, gives you access to shared folders, trace route, gives you vendor's name, gives you Mac addresses, detect the software and the version to the respective port, detect the vulnerability and security holes. The network scanning tool can be used by the network administrator of an organization to secure their data on network from unauthorized strikes on the network.

1.4 Definitions, Acronyms, and Abbreviations.

LAN:

A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home.

LAN SCANNER:

LAN scanners are programs that pings all the IP addresses on a LAN

PING:

A ping is a basic network command that allows a user to verify that a particular IP address exists, and can accept requests.

PORTS:

Ports are virtual places within an operating system where network connections start and end.

HOSTNAME:

The **hostname** is what a device is called on a network. Alternative terms for this are **computer name** and **site name**. The hostname is used to distinguish devices within a local network.

IP ADDRESSES:

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

MAC ADDRESS:

A media access control address (MAC address) is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment.

VENDOR NAME:

This is a name used to describe a company or individual offering a product or service for reselling to the next link in the supply chain. A vendor name can be a registered business name or the vendor's name. Vendors may supply goods and services to other businesses, consumers or the government.

TRACE ROUTE:

Trace route is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination, reporting the IP addresses of all the routers it pinged in between. Trace route also records the time taken for each hop the packet makes during its route to the destination.

NETWORK SHARING:

Network sharing is a feature that allows resources to be shared over a network, be they files, documents, folders, media, etc. These are made accessible to other users/computers over a network.

COMMANDS:

In computing, a command is a directive to a computer program to perform a specific task. It may be issued via a command-line interface, such as a shell, or as input to a network service as part of a network protocol, or as an event in a graphical user interface triggered by the user selecting an option in a menu.

2 The Overall Description

Network scanning allows companies to:

- Access the operating systems in use by monitoring the IP responses
- Network scanning involves network port scanning and vulnerability scanning.
- In port scanning, the scanner sends data packets to a specified service port number over the network. This helps to identify the available network services on a particular system for troubleshooting.
- Vulnerability scanning allows the scanner to detect known vulnerabilities of computing systems available on a network. This process helps the scanner to identify specific weak spots in application software or the operating system.
- Both network port and vulnerability scanning gather relevant information from the network. This information, when used by unauthorized personnel, poses a serious threat to the company.
- Network scanning is also closely related to packet sniffing or passive scanning.
- Passive scanning captures and tracks the flow of data packets over the network. Packet-level traffic on your network can be tracked by implementing sensors on the devices and using tools to translate packet data into relevant information easily. With this approach, the scanner evaluates the traffic flow as soon as the devices start sending messages to the network, without having to ping the devices separately.
- Although passive scanning is an important part of your toolkit, it has some limitations. The passive scanner cannot detect those devices or applications not communicating.

2.1 Product Perspective

Network scanning helps to detect all the active hosts on a network and maps them to their IP addresses. Network scanners send a packet or ping to every possible IP address and wait for a response to determine the status of the applications or devices (hosts). The responding hosts are considered active, while others are considered dead or inactive. These responses are then scanned to detect inconsistencies.

To keep the networking systems up and running, companies need to rely on robust Network scanning tools. A Network scanning tool is essential for companies who have a large network with multiple subnets. The companies must always invest in those scanners providing flexibility with the changing requirements. The chosen network scanner should be able to scale up easily with time as per the network security requirements without having to incur any substantial additional costs.

- **Manage dynamic networks by IP scanning across multiple subnets in real-time**

Unlike in small-scale, static networks, where IP allocation remains constant over a period, IP allocations in dynamic networks tend to change continually. Enterprise-level networks often implement dynamic IP allocations to manage the large number of devices connecting and disconnecting from the network. This makes it important for IP scanner tools to keep track of the IP provisioning and decommissioning. Network IP scanning helps in keeping track of these allocations by continually scanning the network for IP status changes.

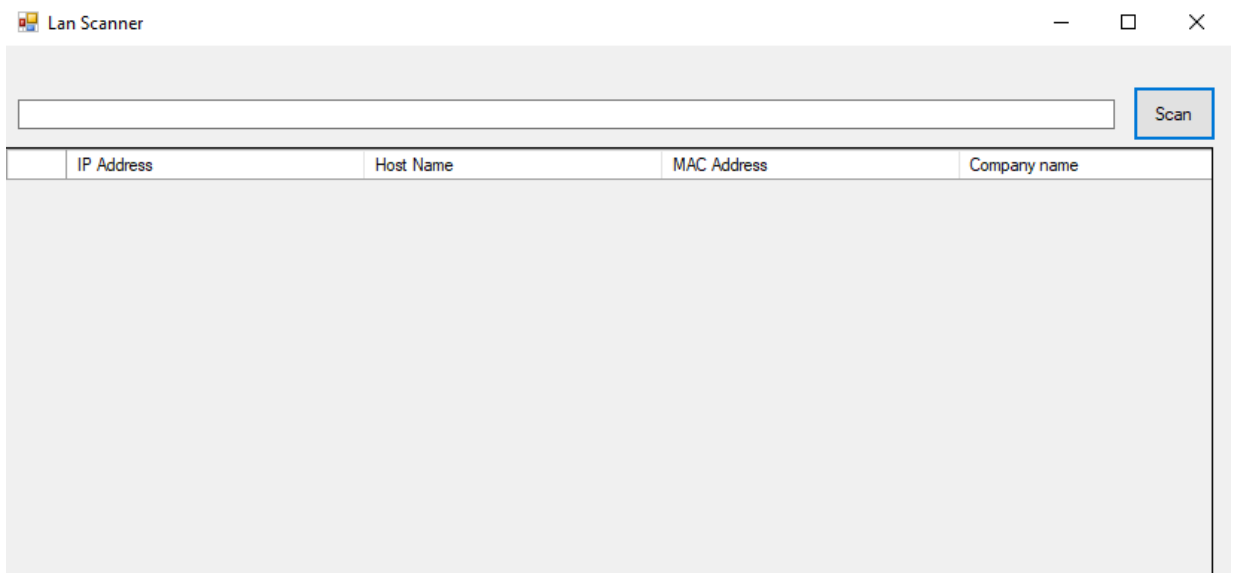
- **Audit network resource usage with granular IP scan reports**

Using network IP scanner, you can keep track of the users of a particular IP by viewing historical logs of its allocations. All network data, statistics, and performance metrics are stored to help make the auditing process easier. IP scanning generates reports on used and unused IP addresses by marking IPs that do not respond within a 10-day period as Available. The network IP scanner software reports can be exported in PDF, CSV, or XLS format and stored for future reference

2.2 Interfaces

- **Software Interfaces**

The software will use 2GB RAM and 500MB Hard drive space. A network connection will also be needed to the software to run its diagnosis. The software will be GUI (Graphical User Interface) built means it will not have any complexity for the user. It will be one click operational software which will be user friendly and easy for the user to use.



- **Hardware Interfaces**

Our project have no hardware

2.3 Memory Constraints

- **Requirements for a Local PC**

A computer where the program is installed should be configured to satisfy the following requirements.

- **Recommended Hardware Requirements**

- Intel Corei5 4th gen
- 4 GB of RAM
- 1 GB of free disk space

- **Minimum Hardware Requirements**

- Intel Core core2duo
- 1 GB of RAM
- 500 MB of free disk space

- **Requirements**

- Administrative rights on the local computer
- Microsoft .NET Framework 4.0 or above
- Enabled NetBIOS over TCP/IP

- **Supported Platforms (x86/x64)**

- Windows 10, 8.1, 8, 7, Vista, XP (with SP3 or later)
- Windows Server 2019, 2016, 2012 R2, 2012, 2008 R2, 2008, 2003 R2, 2003 (with SP2 or later)

2.4 Operations

- **Port Scanning:**

Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities.

- **MAC Address:**

A media access control address (MAC address) is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment.

- **Host Name**

The **hostname** is what a device is called on a network. Alternative terms for this are **computer name** and **site name**. The hostname is used to distinguish devices within a local network.

- **IP Address**

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

- **Shared PC Folder**

You can use the Share tab in File Explorer to share files and folders on your network (homegroup, workgroup, or domain) or on a PC that you share with other people.

- **Ping Specific IP**

A ping is a basic network command that allows a user to verify that a particular IP address exists, and can accept requests

2.5 Non-Functional Requirements

- **Reliability**

It should go without saying that a reliable wireless LAN depends on smart planning and preemptive troubleshooting on the part of the IT manager – i.e. designing the network based on the specific needs of the company. Implementing a WLAN without conducting a thorough site survey, only to find that it does not reliably serve your employees, makes about as much sense as purchasing a Volkswagen Bug on a whim, only to find that it does not reliably transport a family of eight.

- **Availability**

The software will be operational for 24/7. The user can just diagnose his/her network anytime by simply getting connection in the network. This would be helpful in a fact that if the user has left any of his/her port open for the hacker to break into his/her network.

- **Maintainability**

Software maintenance is widely accepted part of SDLC now a days. It stands for all the modifications and updating done after the delivery of software product. There are number of reasons, why modifications are required, some of them are briefly mentioned below:

- **Market Conditions –**

Policies, which changes over the time, such as taxation and newly introduced constraints like, how to maintain bookkeeping, may trigger need for modification.

- *Client Requirements –*

Over the time, customer may ask for new features or functions in the software.

In a software lifetime, type of maintenance may vary based on its nature. It may be just a routine maintenance tasks as some bug discovered by some user or it may be a large event in itself based on maintenance size or nature. Our company will conduct some information from surveillance from user experience and updates will be sent to the installed software's. the user will get update alert and will install them.

3 Implementation

3.1 Automatically Ip picking of Our computer

```
IPHostEntry host;  
  
string localIP = "?";  
  
host = Dns.GetHostEntry(Dns.GetHostName());  
  
foreach (IPAddress ip in host.AddressList)  
  
    if (ip.AddressFamily.ToString() == "InterNetwork")  
  
        {
```

3.2 Taking 3 octets of local Ip address

```
        string IPP;  
  
        IPP = localIP = ip.ToString();  
  
        string[] allocates = IPP.Split('.');  
  
  
        foreach (string str in allocates)  
  
        {  
  
            IPADD.Text = IPADD.Text + str + "\n";  
  
        }  
  
  
  
        int value1 = Int32.Parse(allocates[0]);  
  
        int value2 = Int32.Parse(allocates[1]);  
  
        int value3 = Int32.Parse(allocates[2]);  
  
        IPADD.Text = value1 + "." + value2 + "." + value3 + ".";  
  
    }
```

3.3 Don't work if we don't have network

```
        if (IPADD.Text == "127.0.0.")  
  
        {  
  
            MessageBox.Show("No internet connection Found");  
  
        }
```

```

else
{
    textBox1.Text = IPADD.Text;

```



3.4 transfer Control to Background Worker

```

    backgroundWorker1.RunWorkerAsync();

}

string txt;

txt = IPADD.Text;

```

3.5 MAC Address, IP Address, Hostname, Vendorname

3.5.1 IP Address & Hostname

```

Thread.Sleep(500);

Ping ping;

IPAddress addr;

PingReply pingReply;

IPHostEntry host;

string name;

Parallel.For(0, 254, (i, loopstate) =>
{
    ping = new Ping();

    pingReply = ping.Send(textBox1.Text + i.ToString());

    this.BeginInvoke((Action)delegate ()
    {
        if (pingReply.Status == IPStatus.Success)
        {

```

```

try
{
    addr = IPAddress.Parse(textBox1.Text + i.ToString());
    host = Dns.GetHostEntry(addr);
    name = host.HostName;

```

3.5.2 Adding IP Address and Hostname to Datagrid view

```

dataGridView.Rows.Add();

int nRowIndex = dataGridView.Rows.Count - 1;

dataGridView.Rows[nRowIndex].Cells[0].Value = textBox1.Text +
i.ToString();

dataGridView.Rows[nRowIndex].Cells[1].Value = name;

```

3.5.3 Finding MAC address through IP Address

```

System.Diagnostics.Process pProcess = new
System.Diagnostics.Process();

string macAddress;

pProcess.StartInfo.FileName = "arp";

pProcess.StartInfo.Arguments = "-a" +
dataGridView.Rows[nRowIndex].Cells[0].Value.ToString();

pProcess.StartInfo.UseShellExecute = false;
pProcess.StartInfo.RedirectStandardOutput = true;
pProcess.StartInfo.CreateNoWindow = true;

pProcess.Start();

string strOutput = pProcess.StandardOutput.ReadToEnd();

string[] substrings = strOutput.Split('-');

if (substrings.Length >= 8)
{
    macAddress = substrings[3].Substring(Math.Max(0,
substrings[3].Length - 2))

    + "-" + substrings[4] + "-" + substrings[5] + "-" + substrings[6]

```

```
+ "-" + substrings[7] + "-"
+ substrings[8].Substring(0, 2);
```

3.5.4 Adding MAC Address to DataGridView

```
dataGridView.Rows[nRowIndex].Cells[2].Value = macAddress;

label1.Text = macAddress;

string IPP;

IPP = label1.Text;

IPP = IPP.Remove(IPP.Length - 9);

switch (IPP)
{
    case "98-E7-43":

        dataGridView1.Rows[nRowIndex].Cells[3].Value = "Dell
INC";

        break;

    case "C8-F7-50":

        dataGridView1.Rows[nRowIndex].Cells[3].Value = "Dell Inc";

        break;

    case "6C-2B-59":
```

3.5.5 dataGridView1.Rows[nRowIndex].Cells[3].Value = "Dell Inc";

```
        break;

    case "c0-b8-83":

        dataGridView1.Rows[nRowIndex].Cells[3].Value = "HP";

        break;

    case "88-3A-30":

        dataGridView1.Rows[nRowIndex].Cells[3].Value = "Hewlett
Packard Enterprise Company";

        break;

    case "D4-6B-A6":
```

```

        dataGridView1.Rows[nRowIndex].Cells[3].Value = "HUAWEI
TECHNOLOGIES CO.,LTD";

        break;
    case "D0-43-1E":
        dataGridView1.Rows[nRowIndex].Cells[3].Value = "Dell Inc";

        break;
    case "E4-54-E8":
        dataGridView1.Rows[nRowIndex].Cells[3].Value = "Dell
INC";

        break;
    case "8C-04-BA":
        dataGridView1.Rows[nRowIndex].Cells[3].Value = "Dell Inc";

        break;
    case "F0-D4-E2":
        dataGridView1.Rows[nRowIndex].Cells[3].Value = "Dell Inc";

        break;
    case "E4-43-4B":
        dataGridView1.Rows[nRowIndex].Cells[3].Value = "Dell Inc";

        break;
    case "34-e6-ad":
        dataGridView1.Rows[nRowIndex].Cells[3].Value = "Dell Inc";

        break;
    case "b0-83-fe":
        dataGridView1.Rows[nRowIndex].Cells[3].Value = "Dell inc";

        break;
    case "6c-d9-4c":
        dataGridView1.Rows[nRowIndex].Cells[3].Value = "Vivo";

        break;

```

```

        default:
            dataGridView1.Rows[nRowIndex].Cells[3].Value = "Vender
not found";

            break;
        }
    }

    // return macAddres;

}

else
{
    // return "not found";
}

}

catch (SocketException ex)
{
    name = "?";

}

}

});

});

MessageBox.Show("Scan complete");

var macAddr =

(
    from nic in NetworkInterface.GetAllNetworkInterfaces()

```

```

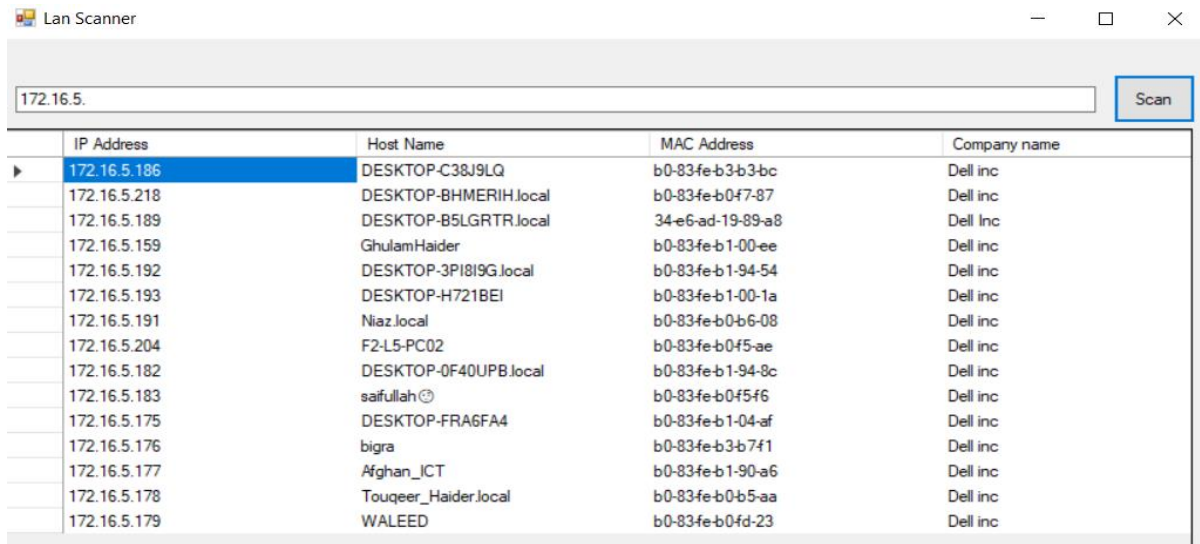
        where nic.OperationalStatus == OperationalStatus.Up

        select nic.GetPhysicalAddress().ToString()

    ).FirstOrDefault();

}

```



The screenshot shows the 'Lan Scanner' application window. At the top, there is a text input field containing '172.16.5.' and a 'Scan' button. Below this is a table with four columns: 'IP Address', 'Host Name', 'MAC Address', and 'Company name'. The table lists 18 discovered devices. The first row is highlighted in blue.

IP Address	Host Name	MAC Address	Company name
172.16.5.186	DESKTOP-C38J9LQ	b0-83-fe-b3-b3-bc	Dell inc
172.16.5.218	DESKTOP-BHMERIH.local	b0-83-fe-b0-f7-87	Dell inc
172.16.5.189	DESKTOP-B5LGRTR.local	34-e6-ad-19-89-a8	Dell inc
172.16.5.159	GhulamHaider	b0-83-fe-b1-00-ee	Dell inc
172.16.5.192	DESKTOP-3PI8I9G.local	b0-83-fe-b1-94-54	Dell inc
172.16.5.193	DESKTOP-H721BEI	b0-83-fe-b1-00-1a	Dell inc
172.16.5.191	Niaz.local	b0-83-fe-b0-b6-08	Dell inc
172.16.5.204	F2-L5-PC02	b0-83-fe-b0-f5-ae	Dell inc
172.16.5.182	DESKTOP-0F40UPB.local	b0-83-fe-b1-94-8c	Dell inc
172.16.5.183	saifullah ☺	b0-83-fe-b0-f5-f6	Dell inc
172.16.5.175	DESKTOP-FRA6FA4	b0-83-fe-b1-04-af	Dell inc
172.16.5.176	bigra	b0-83-fe-b3-b7-f1	Dell inc
172.16.5.177	Afghan_ICT	b0-83-fe-b1-90-a6	Dell inc
172.16.5.178	Touqeer_Haider.local	b0-83-fe-b0-b5-aa	Dell inc
172.16.5.179	WALEED	b0-83-fe-b0-fd-23	Dell inc

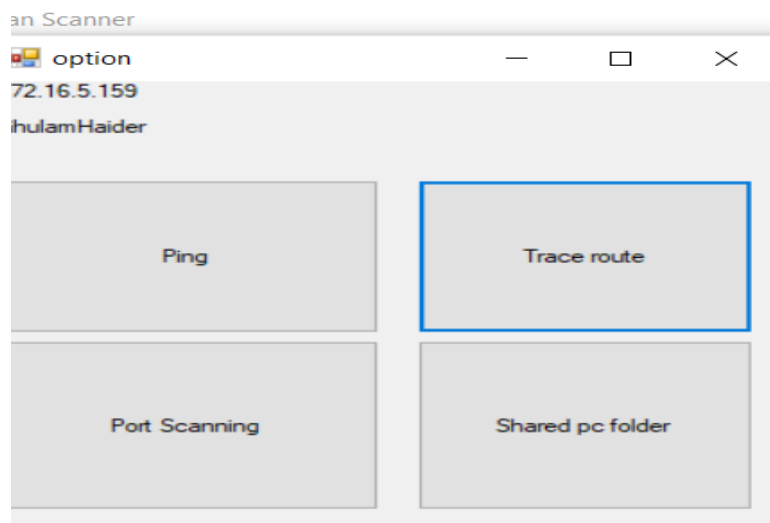
3.6 Data grid view code for opening new Window

```
Form2 f2 = new Form2();
```

```
f2.Get_ip = this.dataGridView.CurrentRow.Cells[0].Value.ToString();
```

```
f2.Get_Host = this.dataGridView.CurrentRow.Cells[1].Value.ToString();
```

```
f2.ShowDialog();
```



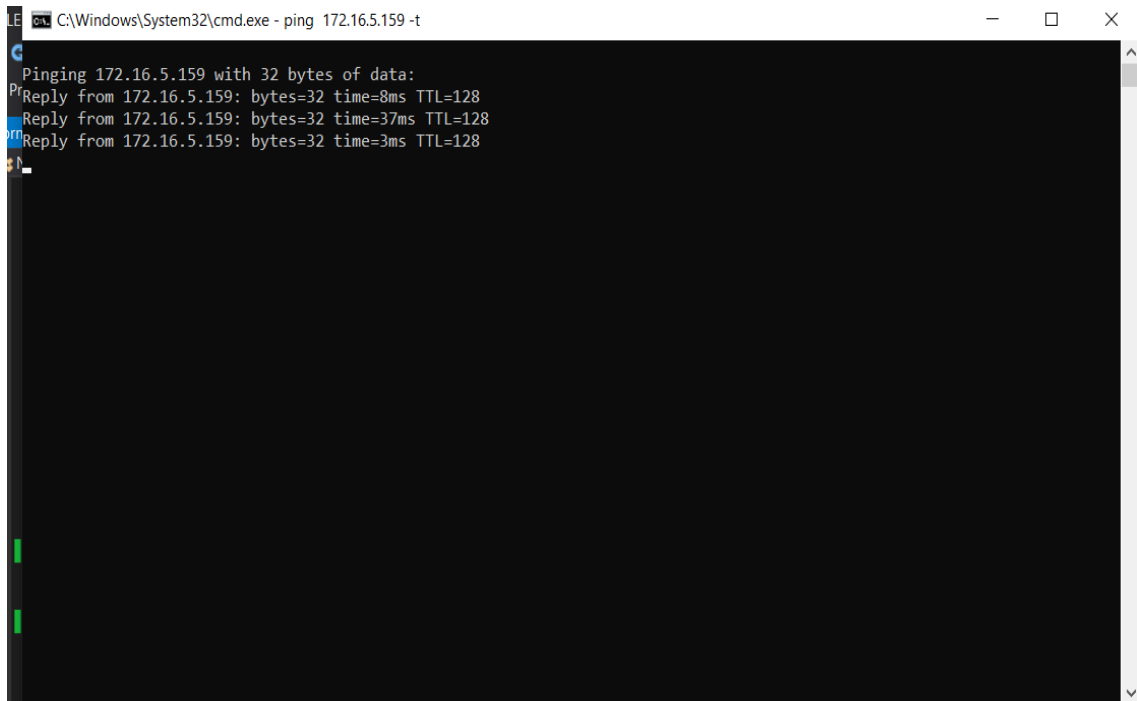
3.6.1 Form 2 ping

```
string strCmdText;
```

```
//For Testing
```

```
strCmdText = "/K ping " + label1.Text + " -t";
```

```
System.Diagnostics.Process.Start("CMD.exe", strCmdText);
```



The screenshot shows a Windows Command Prompt window titled "C:\Windows\System32\cmd.exe - ping 172.16.5.159 -t". The window has a black background with white text. The output of the command is as follows:

```
Pinging 172.16.5.159 with 32 bytes of data:
Reply from 172.16.5.159: bytes=32 time=8ms TTL=128
Reply from 172.16.5.159: bytes=32 time=37ms TTL=128
Reply from 172.16.5.159: bytes=32 time=3ms TTL=128
```

3.6.2 Trace Route Command

```
string strCmdText;
```

```
//For Testing
```

```
strCmdText = "/k tracert " + label1.Text;
```

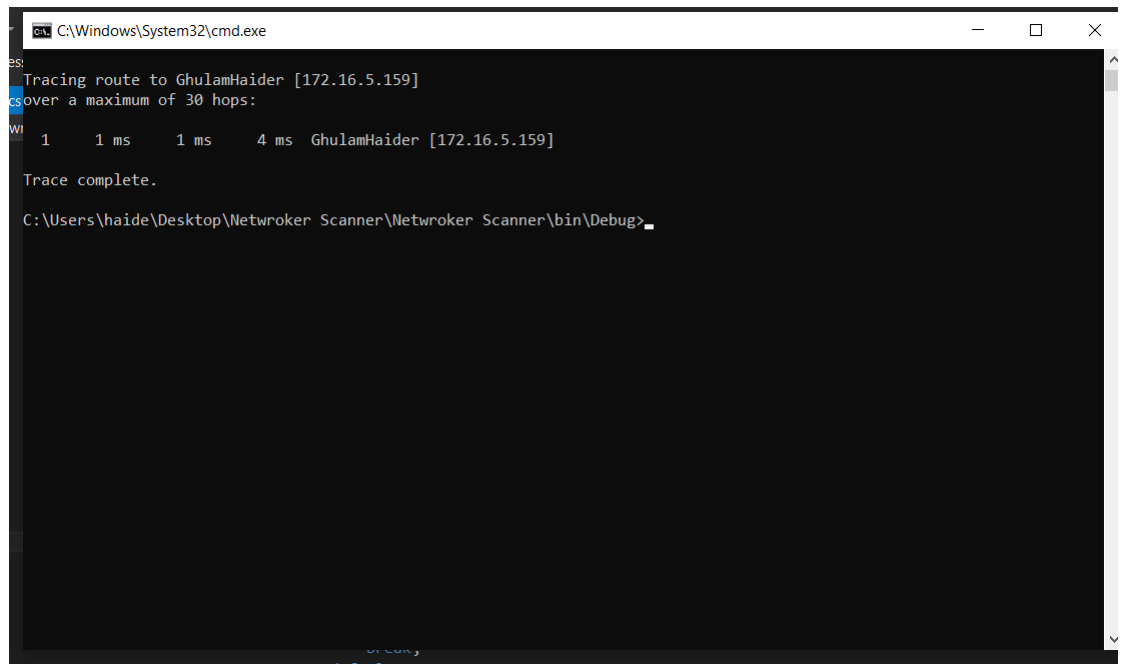
```
System.Diagnostics.Process.Start("CMD.exe", strCmdText);
```

3.6.3 Sending Data For Port Scanning

```
Form4 f3 = new Form4();
```

```
f3.Get_ip = label1.Text;
```

```
f3.ShowDialog();
```

```
C:\Windows\System32\cmd.exe
Tracing route to GhulamHaider [172.16.5.159]
over a maximum of 30 hops:
  0  1 ms  1 ms  4 ms  GhulamHaider [172.16.5.159]
Trace complete.
C:\Users\haide\Desktop\Netwroker Scanner\Netwroker Scanner\bin\Debug>
```

3.6.4 Shared Folder

```
System.Diagnostics.Process p = new System.Diagnostics.Process();
```

```
p.StartInfo.UseShellExecute = false;
```

```
p.StartInfo.RedirectStandardOutput = true;
```

```
string strCmdText;
```

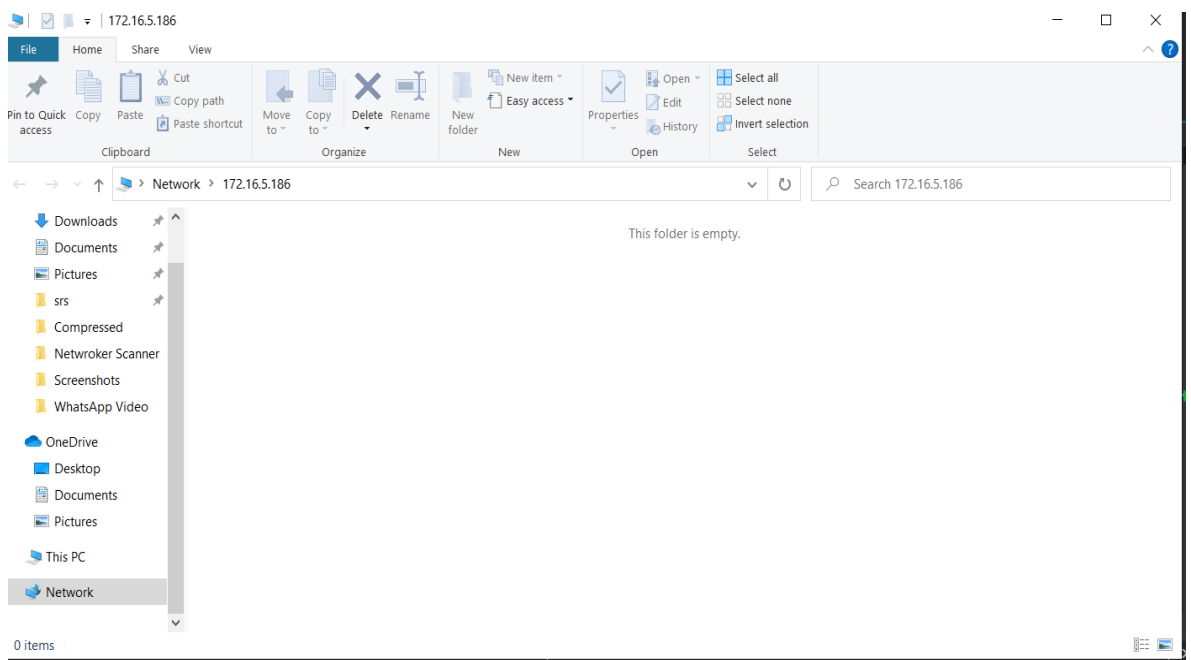
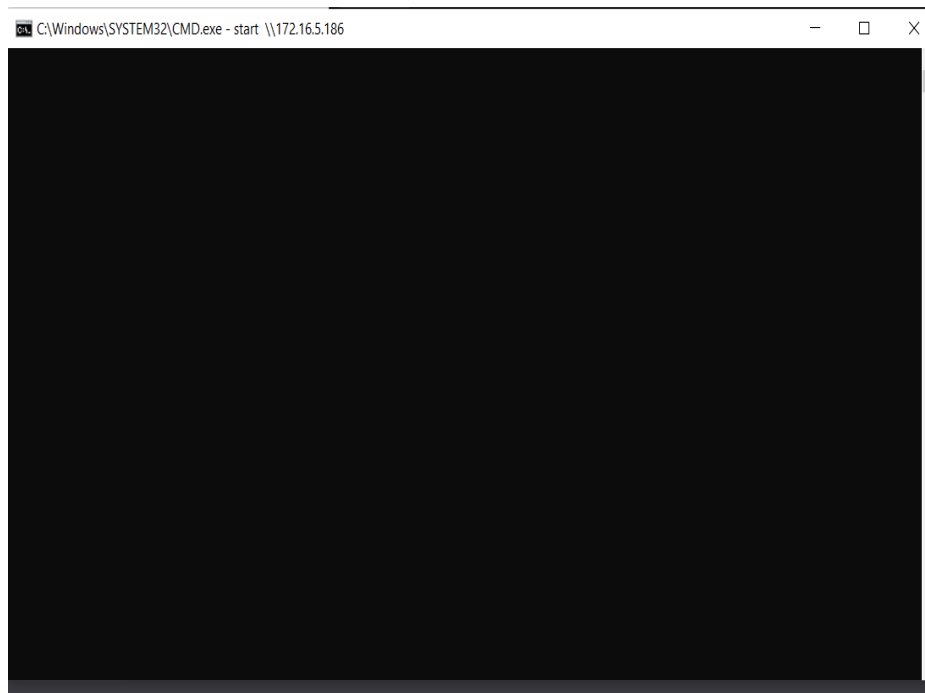
```
strCmdText = "/K start \\\\" + label1.Text;
```

```
p.StartInfo.FileName = "CMD.exe";
```

```
p.StartInfo.Arguments = strCmdText;
```

```
// p.StartInfo.UseShellExecute = false;
```

```
p.Start();
```



3.7 Port Scanning

```
string a = textBox1.Text;  
  
string b = textBox2.Text;  
  
int startPort = Convert.ToInt32(a);
```

```

int endPort = Convert.ToInt32(b);

//port scanning
for (int currport = startPort; currport <= endPort; currport++)
{
    TcpClient tcpportscan = new TcpClient();

    try
    {

        tcpportscan.Connect(label4.Text, currport);

        string portopen = "port" + currport + "open\n";

        listBox1.Items.Add(portopen);

    }

    catch
    {

        string portclosed = "port" + currport + "closed\n";

    }

}

```

Port_scanning

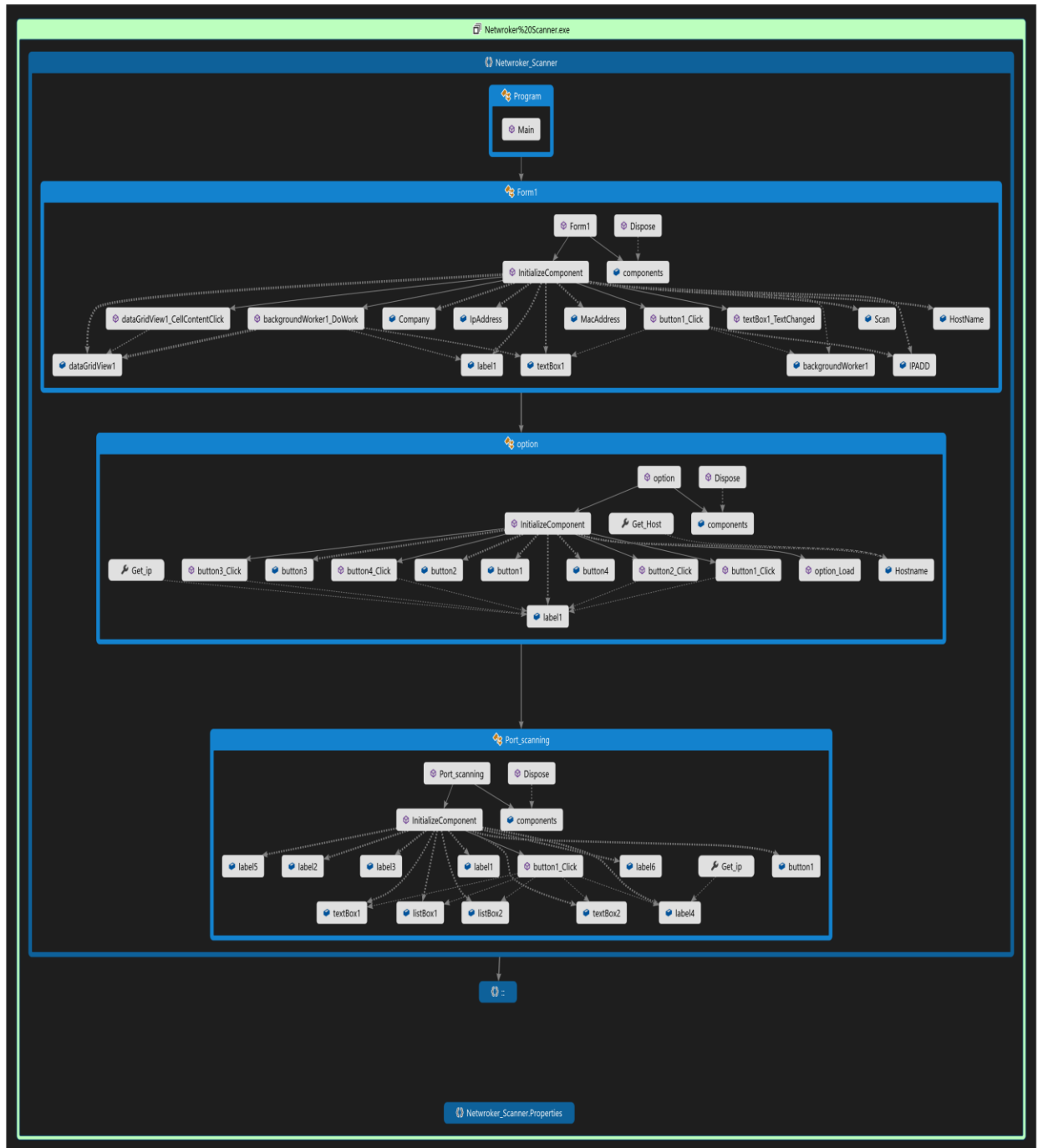
start port no Ending port no

Open Ports

Close Ports

port20closed/n
port21closed/n
port22closed/n
port23closed/n
port24closed/n
port25closed/n

3.8 System Diagram



4 Summary and Conclusion

The project (LAN scanner) involves the design of the network scanning tool, which will enable the network administrator to see all the active hosts on the network and their physical addresses (MAC addresses) Network scanning helps to detect all the active hosts on a network and maps them to their IP addresses. Network scanners send a packet or ping to every possible IP address and wait for a response to determine the status of the applications or devices (hosts) and their vendor's name. However, port scanning refers to the process of sending packets to specific ports on a host and analyzing the responses to learn details about its running services or locate potential vulnerabilities

5 Future Enhancement

Currently, we have designed LAN scanner for active devices. In future we will try to make enhancement by adding recent activity notification of devices as well can be access from office and remotely.

6 References

1. T. Killalea, "Recommended Internet Service Provider Security Services and Procedures", *RFC Editor United States*.
2. Huis Van Koc and Presse Borja, "Internet service provider selection decisions. Management of Engineering and Technology", *PICMET '01. Portland International Conference*, vol. 1, 2001.
3. Sharmin Rashid Linta and Md. Ridgewan Khan Neuton, *Today's Impact on Communication System by IP Spoofing: Some great methods for detecting and preventing IP Spoofing*, Germany:LAP Lambert Academic Publishing, 2012.
4. Andrew Buhr, Dale Lindskog, Pavol Zavarsky and Ron Ruhl, "Media access control address spoofing attacks against port security", *USENIX Association Berkeley CA USA*, 2011.
5. [online] Available: <http://www.advanced-jp-scanner.com>.
6. [online] Available: <http://www.softpedia.com/get/Tweak/Network-Tweak/MAC-Address-Changer.shtm>.