Network Tools Application Design Based on C# with Intrusion Detection Methods and Simple Network Management Protocol

Rino)*, Elroy Maxenchio Teja2)

1)2)Universitas Buddhi Dharma
Jl. Imam Bonjol No 41 Karawaci Ilir-Tangerang, Indonesia

1)rino@ubd.ac.id

3)elroyteja43@gmail.com

Article history:

Received 20 Maret 2021;
Revised 27 Maret 2021;
Accepted 8 April 2021;
Available online 30 April 2021

Keywords: {use 4-6 keywords}

Academic Informatics Engineering
Networking
SNMP
Intrusion Detection

Abstract

The problem faced within this topic still encountered slow network constraints, thus disrupting work activities, the method used in writing is the SNMP (Simple Network Management Protocol) method & Intrusion Detection and by using the bee colony method to run tools designed to facilitate the retrieval. of network device information data and control the network. The solution that can be offered is to make it easier for admins to monitor and control network traffic and limit client network bandwidth, so as to get results in the form of organized and controlled network traffic. Management of network became important as prevention needed to securing the network and managing them requires the method mentioned above to make sure that network can be used without any problem.

I. INTRODUCTION

The technology that is currently developing allows many things that can be made to connect to the internet even through devices both from computers, devices, and smartphones so that the needs of the internet are important in following the development of technology. Computer networks with the convenience that are owned will be a bad impact if there is no supervision carried out and will not run properly as expected, deficiencies that can be found when an unattended computer network is a user who tries to access without permission, data flows the network will become uncontrollable and unstable, and so on.

Based on these problems, we need a way to manage unstable traffic or bandwidth traffic such as swelling or connection delays. With the development of the Internet and network coverage or networks that affect the security and speed of access, restrictions must be determined on its users.

Network Monitoring or Network is one thing that must be done to regulate and control data flow or activities in the network. The network has many loopholes such as unbalanced connectivity, inappropriate usage in general, and other constraints such as network interruptions and intrusions in the network.

Because of this, a network must have management that is capable of detecting and securing the network from intruders and other network disturbances.

II. RELATED WORKS/LITERATURE REVIEW (OPTIONAL)

Monitoring

"Network Management is the ability to monitor, control and plan a network of computers and systems. Network monitoring is part of network management. The basic concept of network management is the existence of a manager or device that performs monitoring and an agent as a monitored device [1].

"Monitoring Network is a function of network management, monitoring is useful for analyzing whether the network is still suitable for use or for additional capacity. The results of this monitoring can help us to redesign the existing network. Many things on the network can be monitored via a computer interface. With the monitoring application, it

[*] Corresponding author

ISSN 2622-2728 (online) 2622-271X (print)
doi:

gives the ability for users to monitor and control computer networks systematically remotely or in a central control only. This management is carried out by collecting data and assigning variables to the managed network elements. Network conditions can also be monitored, for example the up / down status of a network equipment. This can be done with various network features [2].

Monitoring is a periodic assessment of the function of program activities in terms of the schedule for use, input or data input by the group in relation to the expectations that have been planned.

In general, monitoring aims to get feedback or feedback for the needs of the ongoing learning process program, knowing this need, the program implementation will immediately prepare for these needs. Needs can be in the form of cost, time, personnel, and tools. Program implementation will know how much it costs, how much time is available for these activities.

Thus it can be seen how much manpower is needed, as well as the methods that must be provided to carry out the program.

In monitoring data is collected for analysis, the results of the analysis are translated and interpreted as input and suggestions for the leadership to make improvements.

According to [3] “Monitoring can be defined as the process of measuring, recording, collecting, processing and communicating information for project management decision making."

Based on the observations of the opinions expressed by experts, it can be concluded that monitoring is an analytical process for gathering information that will be reprocessed according to its purpose, both for improvement, calculation, and used as a basic point in decision making.

Network Monitoring System (NMS)

"NMS is a tool for monitoring elements in a computer network. The function of the NMS is to monitor the quality of the SLA (Service Level Agreement) of the bandwidth used” [4].

The results of monitoring are used as material in management decision making, on the other hand it is used by the network administrator (technical person) to analyze whether there are any irregularities in network operations. According [5], there are 10 reasons for using a computer network monitoring application, namely:

a) Know what is happening on the network.
b) For planning to upgrade or change network equipment.
c) Diagnose problems in the network.
d) Materials needed for SLA (Service Level Agreement).
e) Knowing when is the right time to implement a disaster recovery system (disaster / problem recovery).
f) Ensuring system security is running well.
g) Ensuring users (clients) are connected to the server they need.
h) Get remote network status information
i) Ensuring uptime for user needs.
j) Save money by reducing the amount of network downtime and reducing the time spent analyzing problems

ARP Spoofing

"On the local area network there is a protocol called ARP (Address Resolution Protocol). The ARP protocol serves to translate IP addresses into MAC addresses” [6] ARP request packets are sent broadcast containing the IP address of the destination host. The destination host sends the ARP reply packet unicast to the sending host when the destination host receives the ARP request packet. The sending host stores the IP and MAC addresses of the destination host in the ARP Cache table. ARP Cache Table has a storage time limit. The time limit is different for each operating system.

"The ARP protocol is stateless in that every incoming ARP reply is not verified and the IP-MAC address of the ARP reply packet is stored directly into the ARP Cache table. ARP does not provide a feature to check whether the received ARP reply is sent the previous ARP request packet” [7]. "So that the ARP protocol is stateless and there is no authentication, making ARP vulnerable to several computer network attacks" [8].

“The ARP protocol is vulnerable to attacks known as ARP Spoofing or ARP Poisoning which are caused by a security flaw in the ARP protocol. Therefore, the process of detecting an attack is important to protect a host before carrying out an attack prevention process”[9]. [10] “propose active detection of ARP Spoofing attacks using ICMP echo request and ICMP echo reply packets".

"However, this method consumes large resources on the network" [11]. "Cisco switches also use the Dynamic ARP Inspection method to perform security on the switch, but the costs involved are very large to implement this method" [12].

"Likewise, a good ARP Spoofing detection system is a system that does not change the ARP protocol, does not require additional installation on every host connected to the network, uses small network resources, and is able to detect all types of ARP attacks and does not slow down the packet sending process." [11].

Address Resolution Protocol (ARP)

According to [13], "Address Resolution Protocol (ARP) is a protocol in the TCP / IP Protocol Suite which is responsible for performing IP address resolution into Media Access Control (MAC)".

"Address Resolution Protocol (ARP) is a network protocol in TCP / IP that is useful in mapping an IP Address to become a Mac Address" " [14]

Based on the opinion of experts, it can be concluded that the Address Resolution Protocol (ARP) is a rule used to map IP addresses to MAC addresses which are used as identification in sending a data packet.

Simple Network Management Protocol (SNMP)

"The use of a network monitoring system can make it easier for network managers to monitor their network from anywhere as long as they are connected to the internet" [15].

"The method used for this problem is the Intrusion Detection System and SNMP (Simple Network Management Protocol) method, the Intrusion Detection System is used as a method to detect suspicious activity in a system and network" [16].

III. Methods

Bee Colony is an optimization algorithm used in finding a path through all the destination points with the closest or lowest distance. The method used is designing or designing a software and testing the application or tool. The application or tools to be designed is a computer network monitoring application.

There are several methods such as Intrusion Detection, Packet Sniffing, Vulnerability Scanning, Firewall Monitoring, and Penetration Testing or penetration testing. However, the methods used in this project are Intrusion Detection and Vulnerability Scanning.

Bee Colony Algorithm is an algorithm that is used for path search, and its implementation for the program to be made is a detector to look for disturbances in a network.

By detecting all existing networks and devices connected to the network, it will be easier to manage, detect, and control the connection flow of the available networks.

Where there will be a division of tasks that will run in the program, namely Searchers (onlooker), Workers, and Monitoring (scouts). In the division of tasks, the Seeker will take care of whatever part or node is connected to the network, the Worker will manage the network such as managing network traffic, and have access to close the network or connection devices connected to the network, while the Monitor will monitor network traffic to detect anomalies that occur in the network.

IV. Results

Program View (Testing)

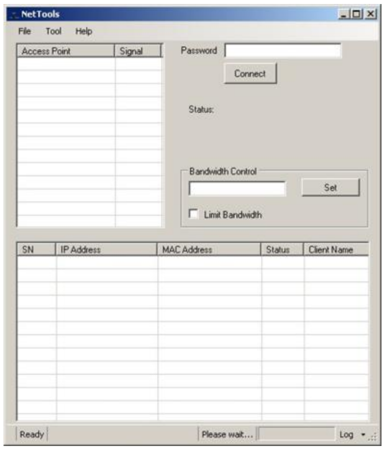


Figure 1. Program View

This section will explain the testing of the following applications, for this study using Black Box Testing with the functional testing method, the purpose of this method is to test the overall application work system such as bandwidth limit trials, network control, network detection, address reading and log storage.

The first stage of this application is to detect what networks can be read. After the program successfully pulls network information, the next stage is carried out.

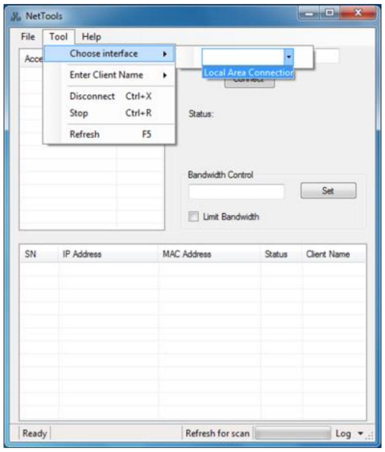


Figure 2. Option Tools

The following is a display of the tools provided in the application, the existing tools have the functions needed in a network administration application such as refreshing, scanning the network based on the interface (if the computer has a wireless adapter it can detect Wi-Fi signals and any connections in it)

In selecting an interface, it should be noted that this application detects the network in an interface that is read and on a computer, for example as shown below:

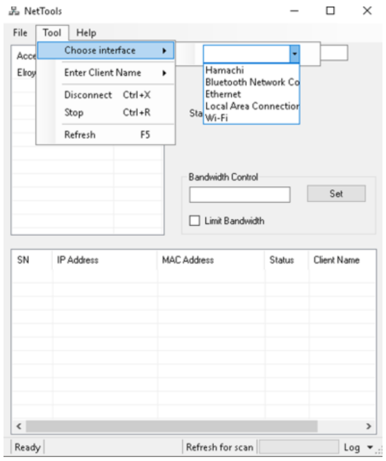


Figure 3. Interface List

The following are the types of interfaces that can be selected to be detected on the network, the interfaces listed are interfaces that already exist on the computer device itself such as a Network Interface Card that allows for Local Area Networks, built-in or external Wireless Adapters, and so on.

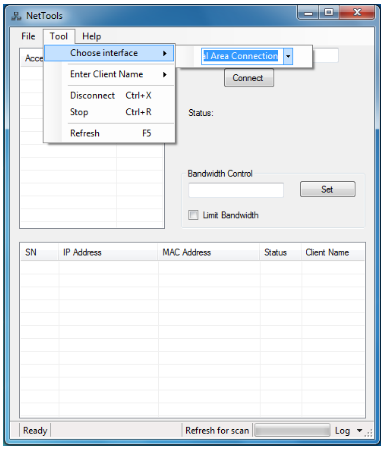


Figure 4. Choose Interface

select one *interface* and refresh by pressing F5 or clicking tools then Refresh. Interfaces that can be selected are based on the device you have, for example a Wi-Fi Interface requires a Wireless Adapter or Wireless Card (built-in or external).

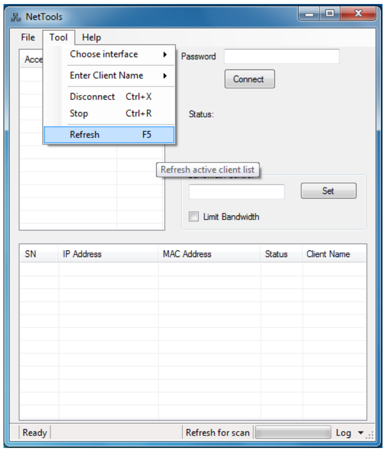
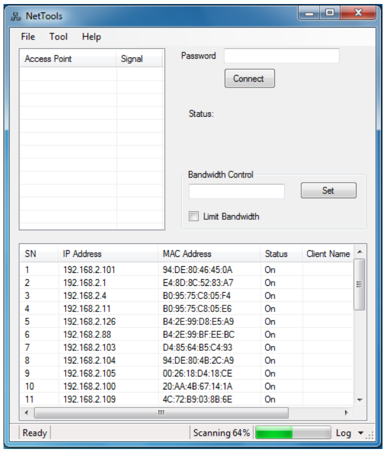


Figure 5. Refresh Option

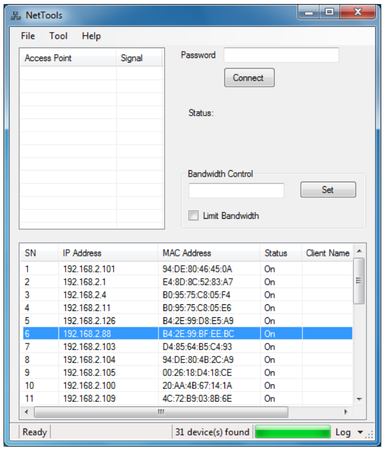
This refresh function is performed to run the program assigned to retrieve or call network information connected to an existing interface. The Refresh function is used to recall the application page and retrieve information, namely the IP Address and MAC Address that have entered the network or network.



SN	IP Address	MAC Address	Status	Client Name
1	192.168.2.101	94:DE:80:46:45:0A	On	
2	192.168.2.1	E4:8D:8C:52:83:A7	On	
3	192.168.2.4	B0:95:75:C8:05:F4	On	
4	192.168.2.11	B0:95:75:C8:05:E6	On	
5	192.168.2.126	B4:2E:99:D8:E5:A9	On	
6	192.168.2.88	B4:2E:99:BF:EE:BC	On	
7	192.168.2.103	D4:85:64:B5:C4:93	On	
8	192.168.2.104	94:DE:80:4B:2C:A9	On	
9	192.168.2.105	00:26:18:D4:18:CE	On	
10	192.168.2.100	20:AA:4B:67:14:1A	On	
11	192.168.2.109	4C:72:B9:03:8B:6E	On	

Figure 6. Refresh & Read Network

After refreshing, the program will start scanning for network devices that are online in the selected interface, the scanning process has a time range of 5 seconds - 10 minutes depending on the number of connected devices.

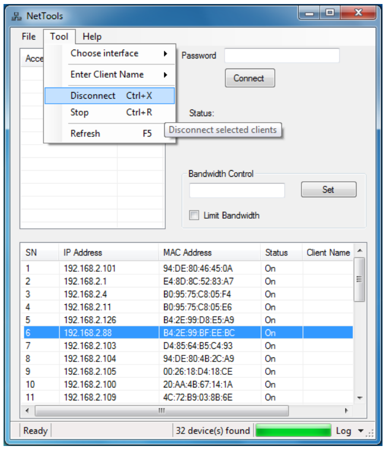


SN	IP Address	MAC Address	Status	Client Name
1	192.168.2.101	94:DE:80:46:45:0A	On	
2	192.168.2.1	E4:8D:8C:52:83:A7	On	
3	192.168.2.4	B0:95:75:C8:05:F4	On	
4	192.168.2.11	B0:95:75:C8:05:E6	On	
5	192.168.2.126	B4:2E:99:D8:E5:A9	On	
6	192.168.2.88	B4:2E:99:BF:EE:BC	On	
7	192.168.2.103	D4:85:64:B5:C4:93	On	
8	192.168.2.104	94:DE:80:4B:2C:A9	On	
9	192.168.2.105	00:26:18:D4:18:CE	On	
10	192.168.2.100	20:AA:4B:67:14:1A	On	
11	192.168.2.109	4C:72:B9:03:8B:6E	On	

Ready | 31 device(s) found | Log

Figure 7. Choose the device to be disabled

Now entering the network control stage, which is closing the connected device access so that it cannot accept internet or local connections, first select the device to be disabled.

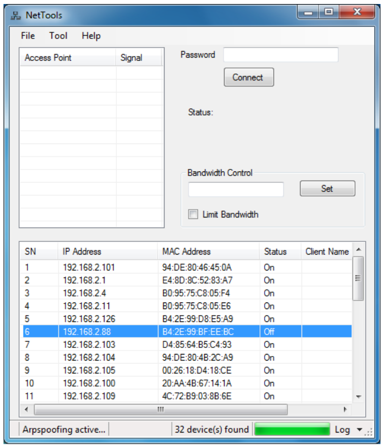


SN	IP Address	MAC Address	Status	Client Name
1	192.168.2.101	94:DE:80:46:45:0A	On	
2	192.168.2.1	E4:8D:8C:52:83:A7	On	
3	192.168.2.4	B0:95:75:C8:05:F4	On	
4	192.168.2.11	B0:95:75:C8:05:E6	On	
5	192.168.2.126	B4:2E:99:D8:E5:A9	On	
6	192.168.2.88	B4:2E:99:BF:EE:BC	On	
7	192.168.2.103	D4:85:64:B5:C4:93	On	
8	192.168.2.104	94:DE:80:4B:2C:A9	On	
9	192.168.2.105	00:26:18:D4:18:CE	On	
10	192.168.2.100	20:AA:4B:67:14:1A	On	
11	192.168.2.109	4C:72:B9:03:8B:6E	On	

Ready | 32 device(s) found | Log

Figure 8. Tools Disconnect

Then click tools and select disconnect, or you can also press Ctrl + X directly, and the next process is to do Arp spoofing or Arp poisoning. Arp Spoofing or Arp Poisoning is an attack carried out on connected and communicating devices, as in the picture above the device is connected and to disable it, communication is carried out in the form of an Arp Spoofing or Arp Poisoning attack which will send a packet with the aim of disabling the selected network connection.

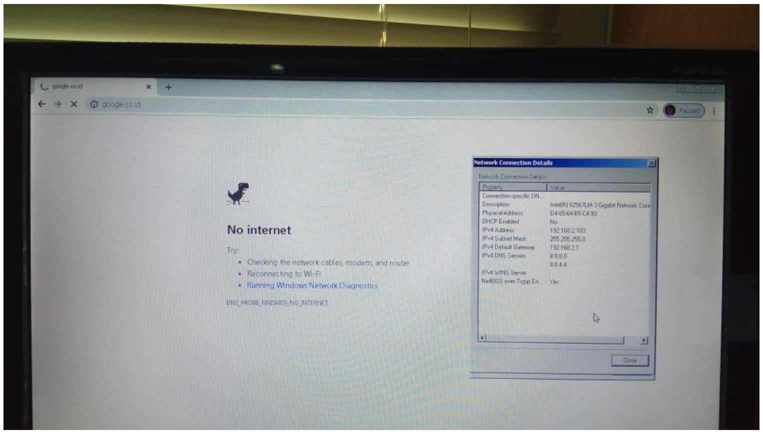


SN	IP Address	MAC Address	Status	Client Name
1	192.168.2.101	94:DE:80:46:45:0A	On	
2	192.168.2.1	E4:8D:8C:52:83:A7	On	
3	192.168.2.4	B0:95:75:C8:05:F4	On	
4	192.168.2.11	B0:95:75:C8:05:E6	On	
5	192.168.2.126	B4:2E:99:D8:E5:A9	On	
6	192.168.2.88	B4:2E:99:BF:EE:BC	Off	
7	192.168.2.103	D4:85:64:B5:C4:93	On	
8	192.168.2.104	94:DE:80:4B:2C:A9	On	
9	192.168.2.105	00:26:18:D4:18:CE	On	
10	192.168.2.100	20:AA:4B:67:14:1A	On	
11	192.168.2.109	4C:72:B9:03:8B:6E	On	

Arpspoofing active... 32 device(s) found

Figure 9. Arp spoofing Active.

After Arp spoofing is active, the selected device will be constantly and continuously sent packets whose purpose is to block internet and local connections so that they cannot enter the device whose access is closed, and the status of the device connection will be changed to off.



No internet

Try:

- Checking the network cables, modem, and router
- Reconnecting to Wi-Fi
- Running Windows Network Diagnostics

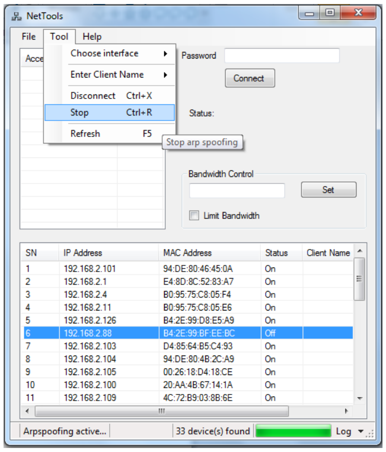
DNS_PROBE_FINISHED_NO_INTERNET

Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Intel(R) 82567LM-3 Gigabit Network Con
Physical Address	D4-85-64-B5-C4-93
DHCP Enabled	No
IPv4 Address	192.168.2.103
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	192.168.2.1
IPv4 DNS Servers	8.8.8.8
	8.8.4.4
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes

Figure 10. Network Disconnected

The image above is the result of Arp spoofing which is run by the application to close the selected network. The connection from the device that is disabled cannot communicate with the internet or locally.

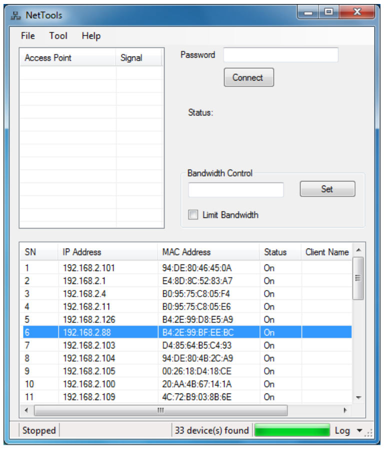


SN	IP Address	MAC Address	Status	Client Name
1	192.168.2.101	94:DE:80:46:45:0A	On	
2	192.168.2.1	E4:8D:8C:52:83:A7	On	
3	192.168.2.4	B0:95:75:C8:05:F4	On	
4	192.168.2.11	B0:95:75:C8:05:E6	On	
5	192.168.2.126	B4:2E:99:D8:E5:A9	On	
6	192.168.2.88	B4:2E:99:BF:EE:BC	Off	
7	192.168.2.103	D4:85:64:B5:C4:93	On	
8	192.168.2.104	94:DE:80:4B:2C:A9	On	
9	192.168.2.105	00:26:18:D4:18:CE	On	
10	192.168.2.100	20:AA:4B:67:14:1A	On	
11	192.168.2.109	4C:72:B9:03:8B:6E	On	

Arpspoofing active... 33 device(s) found

Figure 11. Disables ARP Spoofing / Poisoning

If you want to reactivate the network, simply disable Arp spoofing by selecting Tools, then Stop. After Arp spoofing has been disabled, you can refresh it to refresh the network status.

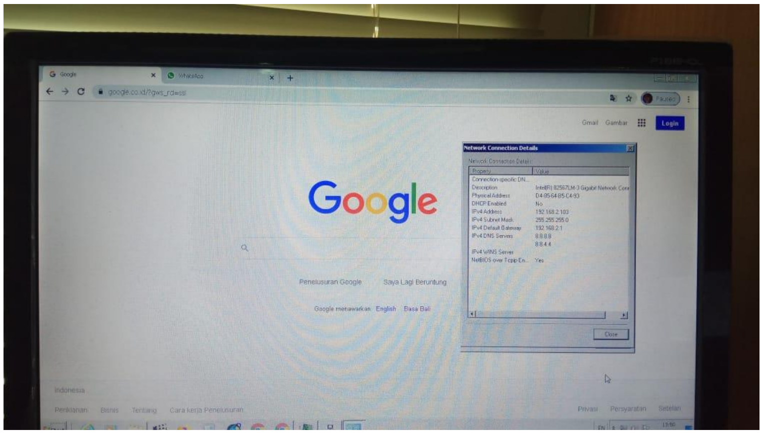


SN	IP Address	MAC Address	Status	Client Name
1	192.168.2.101	94:DE:80:46:45:0A	On	
2	192.168.2.1	E4:8D:8C:52:83:A7	On	
3	192.168.2.4	B0:95:75:C8:05:F4	On	
4	192.168.2.11	B0:95:75:C8:05:E6	On	
5	192.168.2.126	B4:2E:99:D8:E5:A9	On	
6	192.168.2.88	B4:2E:99:BF:EE:BC	On	
7	192.168.2.103	D4:85:64:B5:C4:93	On	
8	192.168.2.104	94:DE:80:4B:2C:A9	On	
9	192.168.2.105	00:26:18:D4:18:CE	On	
10	192.168.2.100	20:AA:4B:67:14:1A	On	
11	192.168.2.109	4C:72:B9:03:8B:6E	On	

Stopped | 33 device(s) found | Log

Figure 12. Turn on the network connection again

After stopping, the command from Arp Spoofing or Arp poisoning will be stopped and the selected device can receive back internet connections and local connections, because this stop command is intended to stop Arp Spoofing or Arp Poisoning packets so that devices that were blocked from connection can be returned as up and running normally, then do a Refresh.

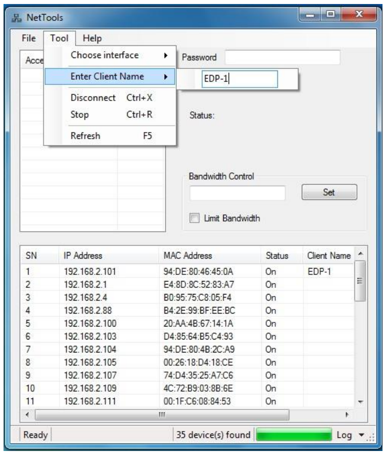


Network Connection Details

Property	Value
Connection-specific DN...	
Description	Intel(R) 82567LM-3 Gigabit Network Conr
Physical Address	D4-85-64-B5-C4-93
DHCP Enabled	No
IPv4 Address	192.168.2.103
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	192.168.2.1
IPv4 DNS Servers	8.8.8.8 8.8.4.4
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes

Figure 13. Network On

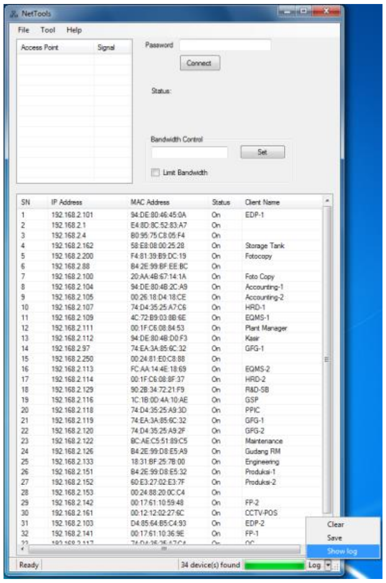
And the image above shows that the connection has been running smoothly after previously being deactivated. The implementation of this program can be used as a control or network center control to regulate the number of networks as well as network control to close access, and with the use of this program it can make it easier for administrators to disable networks that are improper or unregistered.



SN	IP Address	MAC Address	Status	Client Name
1	192.168.2.101	94:DE:80:46:45:0A	On	EDP-1
2	192.168.2.1	E4:8D:8C:52:83:A7	On	
3	192.168.2.4	B0:95:75:C8:05:F4	On	
4	192.168.2.88	B4:2E:99:BF:EE:BC	On	
5	192.168.2.100	20:AA:4B:67:14:1A	On	
6	192.168.2.103	D4:85:64:B5:C4:93	On	
7	192.168.2.104	94:DE:80:4B:2C:A9	On	
8	192.168.2.105	00:26:18:D4:18:CE	On	
9	192.168.2.107	74:D4:35:25:A7:C6	On	
10	192.168.2.109	4C:72:B9:03:8B:6E	On	
11	192.168.2.111	00:1F:C6:08:84:53	On	

Figure 14. Input Client Name

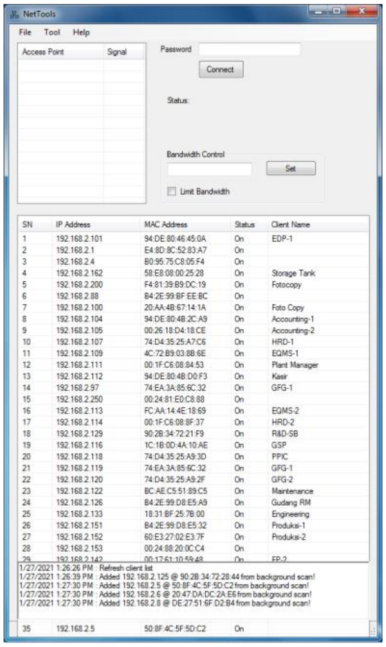
In this program the administrator can manually provide the client name by selecting the connected device then selecting the Tools menu, then Entering Client Name. Press enter to enter the client's identity. Client names can be tailored to suit individual needs, for example Computer 1-A, IT Room - A, and so on. This naming is also done for documentation and differentiating between new devices and devices that have been recorded.



SN	IP Address	MAC Address	Status	Client Name
1	192.168.2.101	94:DE:80:46:45:0A	On	EDP-1
2	192.168.2.1	E4:8D:8C:52:83:A7	On	
3	192.168.2.4	B0:95:75:C8:05:F4	On	
4	192.168.2.162	58:E8:08:00:25:28	On	Storage Tank
5	192.168.2.200	F4:81:39:B9:DC:19	On	Fotocopy
6	192.168.2.88	B4:2E:99:BF:EE:BC	On	
7	192.168.2.100	20:AA:4B:67:14:1A	On	Foto Copy
8	192.168.2.104	94:DE:80:4B:2C:A9	On	Accounting-1
9	192.168.2.105	00:26:18:D4:18:CE	On	Accounting-2
10	192.168.2.107	74:D4:35:25:A7:C6	On	HRD-1
11	192.168.2.109	4C:72:B9:03:8B:6E	On	EQMS-1
12	192.168.2.111	00:1F:C6:08:84:53	On	Plant Manager
13	192.168.2.112	94:DE:80:4B:D0:F3	On	Kasir
14	192.168.2.97	74:EA:3A:85:6C:32	On	GFG-1
15	192.168.2.250	00:24:81:E0:C8:88	On	
16	192.168.2.113	FC:AA:14:4E:18:69	On	EQMS-2
17	192.168.2.114	00:1F:C6:08:8F:37	On	HRD-2
18	192.168.2.129	90:2B:34:72:21:F9	On	R&D-SB
19	192.168.2.116	1C:1B:0D:4A:10:AE	On	GSP
20	192.168.2.118	74:D4:35:25:A9:3D	On	PPIC
21	192.168.2.119	74:EA:3A:85:6C:32	On	GFG-1
22	192.168.2.120	74:D4:35:25:A9:2F	On	GFG-2
23	192.168.2.122	BC:AE:C5:51:89:C5	On	Maintenance
24	192.168.2.126	B4:2E:99:D8:E5:A9	On	Gudang RM
25	192.168.2.133	18:31:BF:25:7B:00	On	Engineering
26	192.168.2.151	B4:2E:99:D8:E5:32	On	Produksi-1
27	192.168.2.152	60:E3:27:02:E3:7F	On	Produksi-2
28	192.168.2.153	00:24:88:20:0C:C4	On	
29	192.168.2.142	00:17:61:10:59:48	On	FP-2
30	192.168.2.161	00:12:12:02:27:6C	On	CCTV-POS
31	192.168.2.103	D4:85:64:B5:C4:93	On	EDP-2
32	192.168.2.141	00:17:61:10:36:9E	On	FP-1
33	192.168.2.117	74:D4:35:25:A7:C4	On	QC

Figure 15. Log Option

To Show Log, point the cursor to the lower right corner then click on the log, after that the option will appear, select Show log to display the log of running applications. This log will report the new IP that entered the network along with the time it was entered.



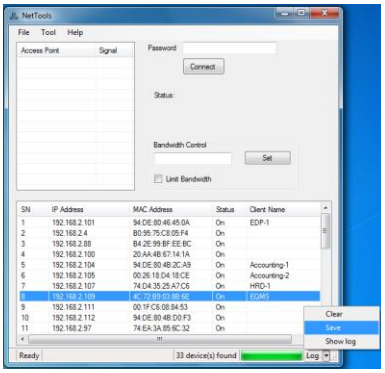
SN	IP Address	MAC Address	Status	Client Name
1	192.168.2.101	94:DE:80:46:45:0A	On	EDP-1
2	192.168.2.1	E4:8D:8C:52:83:A7	On	
3	192.168.2.4	B0:95:75:C8:05:F4	On	
4	192.168.2.162	58:E8:08:00:25:28	On	Storage Tank
5	192.168.2.200	F4:81:39:B9:DC:19	On	Fotocopy
6	192.168.2.88	B4:2E:99:BF:EE:BC	On	
7	192.168.2.100	20:AA:4B:67:14:1A	On	Foto Copy
8	192.168.2.104	94:DE:80:4B:2C:A9	On	Accounting-1
9	192.168.2.105	00:26:18:D4:18:CE	On	Accounting-2
10	192.168.2.107	74:D4:35:25:A7:C6	On	HRD-1
11	192.168.2.109	4C:72:B9:03:8B:6E	On	EQMS-1
12	192.168.2.111	00:1F:C6:08:84:53	On	Plant Manager
13	192.168.2.112	94:DE:80:4B:D0:F3	On	Kasir
14	192.168.2.97	74:EA:3A:85:6C:32	On	GFG-1
15	192.168.2.250	00:24:81:E0:C8:88	On	
16	192.168.2.113	FC:AA:14:4E:18:69	On	EQMS-2
17	192.168.2.114	00:1F:C6:08:8F:37	On	HRD-2
18	192.168.2.129	90:2B:34:72:21:F9	On	R&D-SB
19	192.168.2.116	1C:1B:0D:4A:10:AE	On	GSP
20	192.168.2.118	74:D4:35:25:A9:3D	On	PPIC
21	192.168.2.119	74:EA:3A:85:6C:32	On	GFG-1
22	192.168.2.120	74:D4:35:25:A9:2F	On	GFG-2
23	192.168.2.122	BC:AE:C5:51:89:C5	On	Maintenance
24	192.168.2.126	B4:2E:99:D8:E5:A9	On	Gudang RM
25	192.168.2.133	18:31:BF:25:7B:00	On	Engineering
26	192.168.2.151	B4:2E:99:D8:E5:32	On	Produksi-1
27	192.168.2.152	60:E3:27:02:E3:7F	On	Produksi-2
28	192.168.2.153	00:24:88:20:0C:C4	On	
29	192.168.2.142	00:17:61:10:59:48	On	EP-2

```
1/27/2021 1:26:26 PM : Refresh client list
1/27/2021 1:26:39 PM : Added 192.168.2.125 @ 90:2B:34:72:28:44 from background scan!
1/27/2021 1:27:30 PM : Added 192.168.2.5 @ 50:8F:4C:5F:5D:C2 from background scan!
1/27/2021 1:27:30 PM : Added 192.168.2.6 @ 20:47:DA:DC:2A:E6 from background scan!
1/27/2021 1:27:30 PM : Added 192.168.2.8 @ DE:27:51:6F:D2:B4 from background scan!
```

35	192.168.2.5	50:8F:4C:5F:5D:C2	On	

Figure 16. Show Log

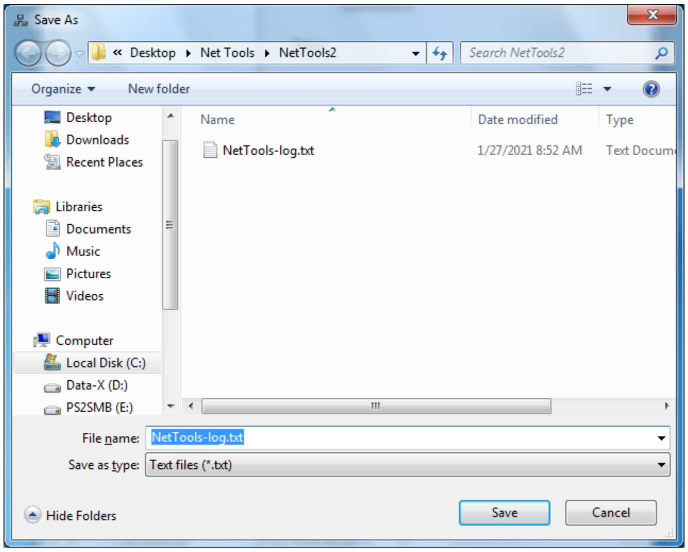
Log What is written is a summary of the processes that occur during the application run, either from the addition of the number of devices or the instructions that have been done by the administrator himself.



SN	IP Address	MAC Address	Status	Client Name
1	192.168.2.101	94:DE:80:46:45:0A	On	EDP-1
2	192.168.2.4	B0:95:75:C8:05:F4	On	
3	192.168.2.88	B4:2E:99:BF:EE:BC	On	
4	192.168.2.100	20:AA:4B:67:14:1A	On	
5	192.168.2.104	94:DE:80:4B:2C:A9	On	Accounting-1
6	192.168.2.105	00:26:18:D4:18:CE	On	Accounting-2
7	192.168.2.107	74:D4:35:25:A7:C6	On	HRD-1
8	192.168.2.109	4C:72:B9:03:8B:6E	On	EQMS
9	192.168.2.111	00:1F:C6:08:84:53	On	
10	192.168.2.112	94:DE:80:4B:D0:F3	On	
11	192.168.2.97	74:EA:3A:85:6C:32	On	

Figure 17. Option

To save the log, click on the lower right corner, then select Save, then a Save dialog box will appear to determine where the log will be saved. This log will store a record of network activity that occurs.



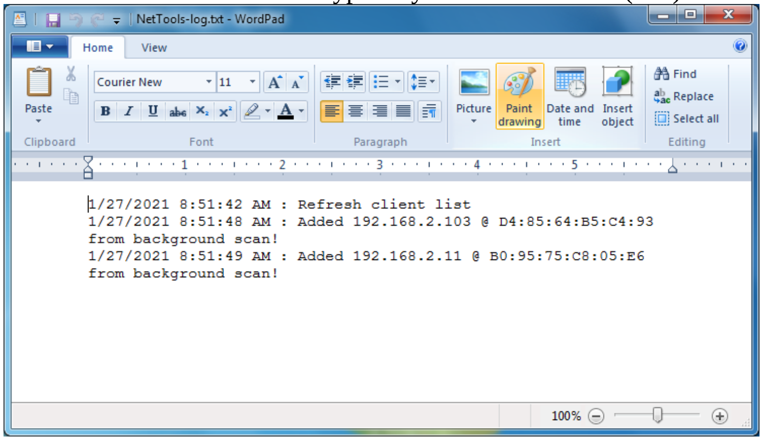
Name	Date modified	Type
NetTools-log.txt	1/27/2021 8:52 AM	Text Docum

File name: NetTools-log.txt

Save as type: Text files (*.txt)

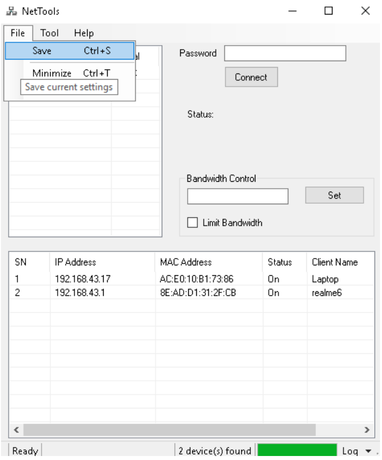
Figure 18. Saving Logs

In this section files can be saved as .txt or other file types if you select All Files (*. *).



```
1/27/2021 8:51:42 AM : Refresh client list
1/27/2021 8:51:48 AM : Added 192.168.2.103 @ D4:85:64:B5:C4:93
from background scan!
1/27/2021 8:51:49 AM : Added 192.168.2.11 @ B0:95:75:C8:05:E6
from background scan!
```

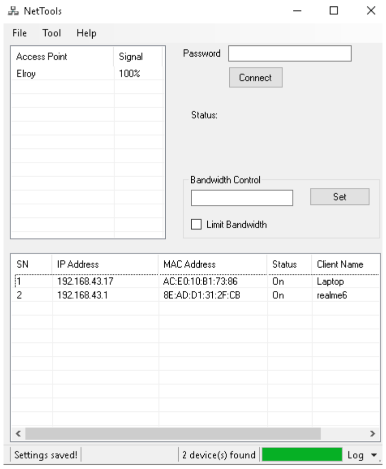
Figure 19. Saved Logs



SN	IP Address	MAC Address	Status	Client Name
1	192.168.43.17	AC:E0:10:B1:73:86	On	Laptop
2	192.168.43.1	8E:AD:D1:31:2F:CB	On	realme6

Figure 20. Saving Configurations

This section is used to store settings such as client names and commands that have been registered in it. And when data such as client name and status have been stored, the connection in the process is stopped or turned off when closing the application when it is opened again and will continue from the previous setting storage point.



Access Point	Signal
Elroy	100%

SN	IP Address	MAC Address	Status	Client Name
1	192.168.43.17	AC:E0:10:B1:73:86	On	Laptop
2	192.168.43.1	8E:AD:D1:31:2F:CB	On	realme6

Settings saved!

Figure 21 Saved configuration

The settings that have been made are saved, and when the program is opened again will continue from the save point that was done. At this stage the administrator has named the client based on the incoming IP address

V. CONCLUSIONS

Based on the analysis that has been carried out, and designing and testing the application, it can be concluded that:

a. This application can be used for network administration or network to obtain information and control the network that is connected.
b. This application has various data calling times based on the large number of devices on the network, ranging from 5 seconds - 10 minutes.
c. This application can be used as a network administration tool because it has the Open Close IP Access feature and by using the Simple Network Management Protocol it makes it easier for network administrators to control their network.

REFERENCES

[1] R. Pradikta, A. Affandi, and E. Setijadi, "Rancang Bangun Aplikasi Monitoring Jaringan dengan Menggunakan Simple Network Management Protocol," *J. Tek. Pomits*, vol. 2, no. 1, pp. 154–159, 2013.

[2] A. Kusaeri, *Monitor Jaringan*. Yogyakarta: Penerbit Andi, 2010.

[3] M. Muhajidin and N. D. P. Putra, "Rancang Bangun Sistem Informasi Monitoring Perkembangan Proyek Berbasis Web," *J. Tek. Ind.*, vol. 11, no. 1, pp. 75–83, 2010.

[4] F. Fachruddin, "Implementasi Sistem Monitoring SLA Bandwidth dalam Aplikasi CACTI," 2009.

[5] www.ipswitch.com, "Secure and Managed File Transfer Software - Ipswitch," 2021. https://www.ipswitch.com/ (accessed Jun. 22, 2021).

[6] N. Agrawal, B. Pradeepkumar, and S. Tapaswi, "Preventing ARP spoofing in WLAN using SHA-512," in *2013 IEEE International Conference on Computational Intelligence and Computing Research*, 2013, pp. 1–5.

[7] S. Shukla and I. Yadav, "An innovative method for detection and prevention against ARP spoofing in MANET," *Int. J. Comput. Sci. Inf. Technol. \& Secur.*, vol. 5, no. 1, pp. 207–214, 2015.

[8] B. Nenovski and P. Mitrevski, "Real-world ARP attacks and packet sniffing, detection and prevention on windows and android devices," 2015.

[9] M. F. A. Rahman and P. Kamal, "Holistic Approach to ARP Poisoning and Countermeasures by Using Practical Examples and Paradigm," *Int. J. Adv. Technol.*, vol. 5, no. 2, pp. 82–95, 2014.

[10] G. Jinhua and X. Kejian, "ARP spoofing detection algorithm using ICMP protocol," in *2013 International Conference on Computer Communication and Informatics*, 2013, pp. 1–6.

[11] J. S. Meghana, T. Subashri, and K. R. Vimal, "A survey on ARP cache poisoning and techniques for detection and mitigation," in *2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN)*, 2017, pp. 1–6.

[12] D. Srinath, S. Panimalar, A. J. Simla, and J. Deepa, "Detection and Prevention of ARP spoofing using Centralized Server," *Int. J. Comput. Appl.*, vol. 113, no. 19, 2015.

[13] R. Towidjojo, "Mikrotik Kungfu Kitab 2," *Jakarta: Jasakom*, pp. 76–78, 2013.

[14] M. Syaifuddin, B. Andika, and R. Imanta Ginting, "Analisis Celah Keamanan Protocol TCP/IP," *J. Ilm. Saintikom*, vol. 16, no. 2, 2017.

[15] D. Wijonarko, "Zabbix Network Monitoring Sebagai Perangkat Monitoring Jaringan Di SKPD Kota Malang," *J. ELTEK*, vol. 12, no. 1, pp. 27–38, 2017.

[16] H. Wardhani, "Intrusion Detection System," 2011. https://helenamayawardhani.wordpress.com.