DOI: 10.14421/ijid.2021.2287 IJID (International Journal on Informatics for Development), *e-ISSN: 2549-7448*
Vol. 10, No. 1, 2020, Pp. 38-46

The DHCP Snooping and DHCP Alert Method in Securing DHCP Server from DHCP Rogue Attack

Dio Aditya Pradana[1], Ade Surya Budiman[2]
Department of Computer Technology, Faculty of Technic and Informatics, University of Bina Sarana Informatika
Jakarta, Indonesia
[1]dioaditya44@gmail.com, [2]ade.aum@bsi.ac.id

Article History
Received month dd, yyyy
Revised month dd, yyyy
Accepted month dd, yyyy
Published month, yyyy

***Abstract*— Security vulnerabilities in network infrastructure will have an impact on the performance and stability of computer networks. DHCP Server as part of the network infrastructure in charge of distributing host configurations to all devices has the potential to be controlled. If the DHCP Server is successfully controlled, all network devices connected to the server can potentially be controlled. From the observations made at PT. Rekayasa Engineering found a vulnerability in the DHCP Server that has the potential to experience DHCP Rogue or DHCP Spoofing, where the client will fail to communicate with the authorized DHCP Server, as well as open the door for attackers to enter the network. For this reason, DHCP Snooping and DHCP Alert methods are implemented. DHCP Snooping will ensure that every data traffic has been filtered and directed to the registered interface. Meanwhile, the use of DHCP Alert is required in monitoring data traffic during the Discover, Offer, Request, and Acknowledge (DORA) process. In the tests performed, DHCP Snooping and DHCP Alert managed to anticipate attacks that tried to placed DHCP Rogue on the network infrastructure. DHCP Alert, configured on the proxy router, ensures that the DORA process can only occur between an authorized DHCP server and a client. DHCP Snooping test also shows that communication from clients can only be replied to by Trusted DHCP Server. The existence of DHCP Snooping and DHCP Alert makes the host configuration fully controlled by the authorized DHCP Server.**

Keywords—Network Security; Computer Networks; IP Address; Client; Configuration

1 INTRODUCTION

Security threats to data and information are increasing, in line with the increasing amount of data being extracted and processed. For this reason, it is necessary to increase and strengthen the security system in the network so that unwanted things do not occur such as data theft and misuse of access, especially networks in several companies that have confidential data that can only be accessed by certain people, therefore network security needs to be implemented.

Computer networks on an enterprise-scale are designed to be able to distribute services to all devices on the network. This aims to facilitate the management of a large number of devices in terms of their types and numbers. Services with distribution or broadcast model are very vulnerable to attacks, either from inside or from outside the computer network. In the case of a DHCP server, for example, a DHCP Starvation attack can result in the loss of all available IP addresses on the DHCP Server. So, the DHCP server cannot serve IP Address requests from clients, and furthermore, the attacker will continue the series of attacks on the network by creating a fake DHCP Server (DHCP Rogue) that is implanted into the network and directs all communications in the network, fully controlled by the attacker[1][2]. Furthermore, an attacker will be able to sniff all of any information on data traffic running on the network, include breaking security policies in the network regarding confidential data (user privacy)[3].

DHCP is a protocol that is very important in the distribution of IP address in a large networks. DHCP services allow workstations connected to the network and automatically obtaining an IP address[4]. In simple terms, the mechanism involves intense communication between the client and the DHCP server available on the network. The client is the "blind" party in the network, where the client will not be able to distinguish the address of the device on the network. The client does not know which one is the DHCP server on the network. Thus, when the discovery process - the initial process of finding and opening communication with the DHCP server - starts, the client will receive each message in the form of an IP configuration offer (DHCP Offer) from the server in response to the DHCP Discover sent by the client.

Fig. 1 shows an example of the IP address used between a host (A) and a DHCP server on the same LAN[5]. Host A, a client, sends a Discover message, with a source IP address of 0.0.0.0 because host A does not have an IP address to use yet. Host A sends the packet to destination 255.255.255.255, which is sent in a LAN broadcast frame, reaching all hosts in the subnet.

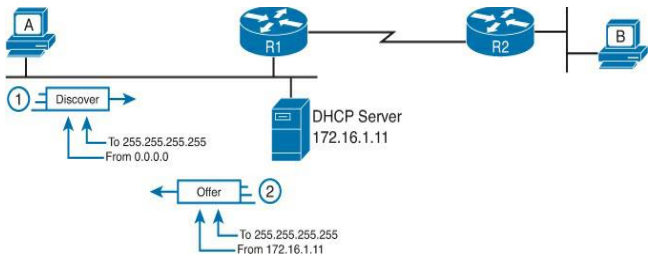

Figure 1. Example of DHCP Client-Server Initial Communication[5]

The DHCP messages work well when the DHCP client and server sit in the same subnet. Once the four messages (Discover, Offer, Request, and Acknowledge) are complete, the DHCP client has an IP address and other IPv4 settings (such as default gateway, subnet mask, etc.), then it can send unicast IP packets as normal. The attacker will exploit this vulnerability, to enter a fake DHCP server into the network, and then send a DHCP Offer to the client. So, once the client is connected to the network, either an authorized DHCP server (on scheme example showed in Fig. 1, it has address 172.16.1.11) or an unauthorized DHCP Server (Rogue DHCP) will send a DHCP Offer to the client.

The status of a computer network that has been attacked on a DHCP server can be marked using the ICMP echo reply message mechanism[6]. If the network client can respond to the ICMP echo reply message, it means that the client gets the IP address configuration from the real DHCP Server. Conversely, if the client does not respond to the message, this indicates that the distribution of addresses on the network has been tampered with or is experiencing an attack.

Several methods have been implemented to deal with attacks against DHCP Server, especially those related to DHCP Rogue attacks. The Secure DHCP (S-DHCP) scheme is used to authenticate the exchange of DHCP messages between the client and the server[7]. Enabling DHCP Snooping on a computer network is done to perform an authentication filter against the DHCP Server on the network[8]. In a broader scale of the attack, the DHCP Snooping method can also be developed using the DHCP Snooping Trusted Port method in the network[9][10].

DHCP Snooping is a layer 2 security feature, with the ability to prevent unauthorized DHCP Server from providing malicious information to clients on the network[11]. The use of DHCP Snooping is very useful for securing confidential information while protecting the network architecture from being attacked, where this mechanism is implemented at every layer on a network[12]. The main purpose of using DHCP Snooping is to regulate the granting of access to IP addresses that have been registered on the router and prevent attackers from accessing or entering into the network[9]. More broadly, DHCP Snooping can be used to prevent various types of attacks on the network, such as Unauthorized DHCP Server Attacks, ARP Man In The Middle Attack, IP/MAC Spoofing Attack and DHCP Packet Flooding Attack[10].

Activating the DHCP Alert feature in Mikrotik and the use of the DHCP Snooping feature on the Switch can be an additional option to patch the security gap. This is by considering that the weakness of this attack lies in the DHCP Discover packet filtering process, when a packet comes from an unregistered client, then with the right configuration, the packet can be blocked [13]. DHCP Alert is a service that uses Authoritative parameters to monitor DHCP Server communications against DHCP requests, while DHCP snooping is a service that prevents or filters out other untrusted servers in providing access to users or client computers.

Based on observations made on computer network security systems at PT. Rekayasa Engineering as the object of this research found vulnerabilities to attacks on the company's

DHCP Server. This attack is in the form of deploying an unauthorized DHCP Server or DHCP Rogue which then establishes communication with network devices that require host configuration to the server. After the communication has been successfully established, the client gets an unauthorized configuration so that it fails to communicate with the network in the process of resource sharing and information transmission. Although the DHCP Snooping feature has been used quite a lot to prevent attacks on the DHCP Server, in this study, the DHCP Alert feature on the Mikrotik Router and DHCP Snooping on the Switch will be combined. Both of these features are expected to strengthen the DHCP Server security system for the research object.

2 METHOD

2.1 Data Collection

Observations and interviews with network administrators and several IT employees on PT. Rekayasa Engineering, as the research object, has been carried out to obtain data and computer network conditions. Furthermore, literature searches and reviews are carried out based on previous research, to obtain a comparison of methods and solutions to problem-solving on the object of research.

2.2 Proposed Problem Solving Method

To solve the problems found in the object of this study, the author uses a general concept of problem-solving on computer networks adopted from J. West, J. Andrews, and T. Dean [14]. The concept is implemented into the steps described in Fig. 2.

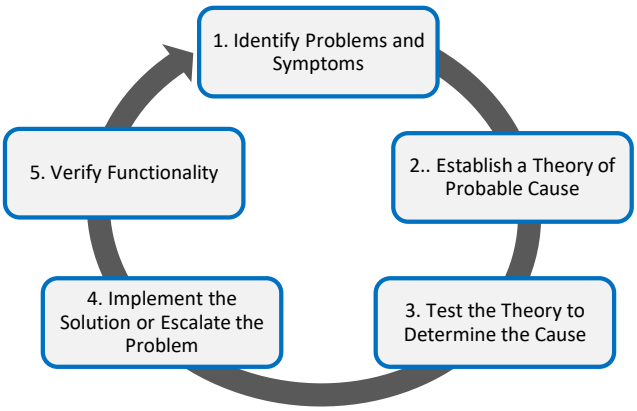

Figure 2. General concept of problem solving

2.2.1 *Identify Problems and Symptoms:* Based on the results of observations and interviews, identification and formulation of problems that occur in the object of research are carried out.

2.2.2 *Establish a Theory of Probable Cause:* From a series of problem occurrences, literature reviews are conducted to compare the problems and solutions that have been given.

2.2.3 *Test the Theory to Determine the Cause:* Based on theories or cases that have been found, testing is carried out on the computer network that is currently running (existing network), to ensure the similarity of the problems and possible causes.

2.2.4 *Implement the Solution or Escalate the Problem:* the next step is to apply a theoretical solution, in the form of the required configuration settings, on network devices related to the problem at hand.

2.2.5 *Verify Functionality:* Ensure that the solution given can function properly to solve the problem, by conducting a series of tests on the network that has been reconfigured according to the solution offered in the previous stage.

3 RESULT AND DISCUSSION

3.1 Existing Network

The computer network blocks contained in the research object can be seen in Fig. 3. In general, the research object uses a client-server network model with wired-transmission media, there is one server that is managed using VMware which is then divided into several servers such as a Proxy server, Mail Server, Web Server, SAN (Storage Area Network), License Server (Application) and Database Server. Also, there are several rooms designated for switches to distribute data to clients, namely the Core Room, Distribution Switch Room 1, and Distribution Switch Room 2. Inside the Core room, along with the server, there is also a Core Router that connects switch areas 1, 2, and 3 and a switch as a core server switch. Meanwhile, the Distribution Switch room functions to receive data from the core room and distribute it to each client.

Based on a written agreement, with consideration of the privacy of the research object, in this study, the authors did not publish the detail of the network schematic on the object of research. However, in general, the physical network topology of the research object is as depicted in Fig. 3, where the concepts of problems and solutions in this study are more related to logical topology, rather than to physical topology.

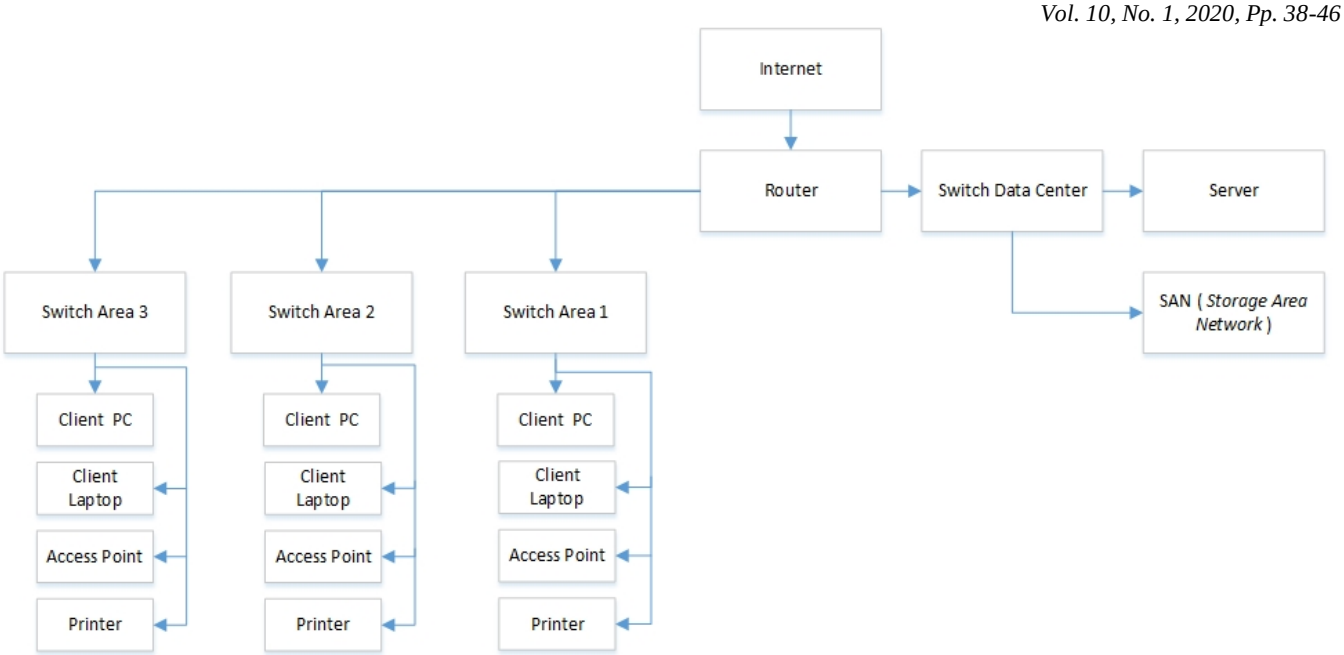

Figure 3. Network block diagram at PT. Rekayasa Engineering

3.2 Existing Network Testing

The security system on existing network is without DHCP Alert or DHCP Snooping configuration.

3.2.1 *Testing Existing Network Without DHCP Alert:* On Fig. 4, shown a test scheme against network security. It is simulated that there is a DHCP Rogue, in the schematic in Fig. 4.

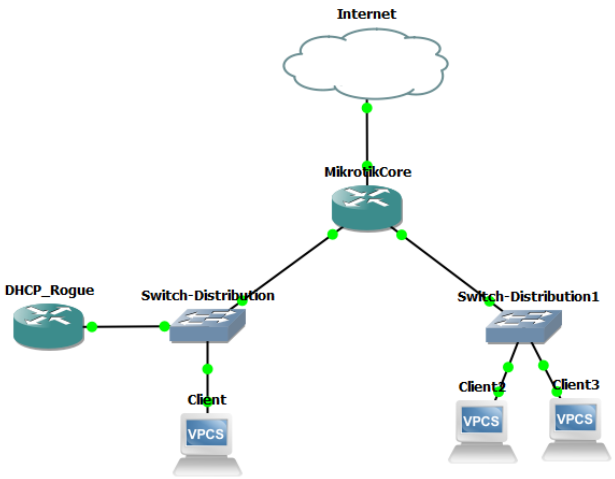

Figure 4. Testing scheme of existing network (without DHCP Alert)

From the scheme, client 2 (which is on Switch Distribution 1) is then tested to communicate with the DHCP Server available on the network, to obtain an IP address.

```
Client2> dhcp
DORA IP 192.168.88.253/24 GW 192.168.88.1

Client2> ping 8.8.8.8
*192.168.88.1 icmp_seq=1 ttl=64 time=9.189 ms (ICMP type:3, code:0, Destination network unre
*192.168.88.1 icmp_seq=2 ttl=64 time=8.036 ms (ICMP type:3, code:0, Destination network unre
*192.168.88.1 icmp_seq=3 ttl=64 time=8.379 ms (ICMP type:3, code:0, Destination network unre
*192.168.88.1 icmp_seq=4 ttl=64 time=7.263 ms (ICMP type:3, code:0, Destination network unre
*192.168.88.1 icmp_seq=5 ttl=64 time=9.087 ms (ICMP type:3, code:0, Destination network unre
```

Figure 5. Existing network test results (without DHCP Alert)

In Fig. 5, the results showed that client 2, gets the IP address from DHCP Rogue and cannot access the internet network with the IP Address and Gateway obtained. DORA stands for Discover, Offer, Request and Acknowledge, which is a series of processes used in DHCP to provide an IP address for a client or host device.

In the test results in Fig. 5, client 2 get IP Address 192.168.88.253/24 and Gateway 192.168.88.1. When a client with that address tries to test connectivity to address 8.8.8.8 (which is the Google DNS Server), connectivity cannot be established (destination network unreachable).

Based on the test, besides client2, other devices, i.e. client and client 3, also perform the DORA process, and get their respective configurations. Received configurations are IP Address, Subnet Mask, Gateway and DNS. The address configuration obtained from the test results is shown in detail in Table 1.

Table 1. Address Obtained from Testing Without DHCP Alert

Device	Interface	IP Address	Subnet mask	Gateway	DNS
Mikrotik Core	Ether 2 - 3	192.168.2.1	255.255.255.0	-	8.8.8.8
DHCP Rogue	Ether 1	192.168.88.1	255.255.255.0	192.168.88.1	1.1.1.1
Client	Switch – Eth 2	192.168.2.254	255.255.255.0	192.168.2.1	8.8.8.8
Client 2	Switch 1 – Eth 2	192.168.88.253	255.255.255.0	192.168.88.1	1.1.1.1
Client 3	Switch 1 – Eth 1	192.168.1.14	255.255.255.0	192.168.1.1	8.8.8.8

As seen in Table 1, several clients get IP addresses, subnet masks, and gateways from Mikrotik Core while other clients get IP addresses, subnet masks, and gateways from DHCP Rogue. Identified from the IP Address and Gateway obtained, client 2 is a device that gets configuration from DHCP Rogue.

3.2.2 *Testing Network Running Without DHCP Snooping:* For testing running networks without DHCP Snooping, the simulation is performed using DHCP Rogue added to a running network that already has an authorized DHCP Server. The running network schematic for this test is shown in Fig. 6.

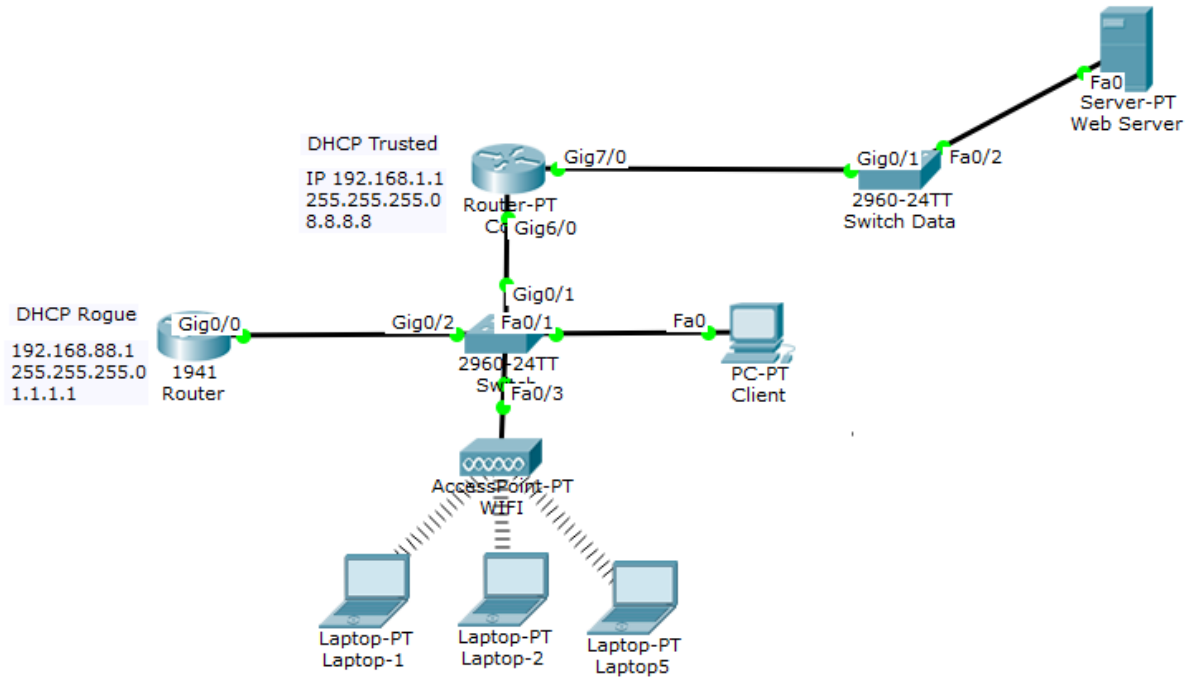

Figure 6. Testing scheme of existing network (without DHCP Snooping)

To test the impact of a network without DHCP Snooping also the addition of a DHCP Rogue, an IP address configuration is performed on one of the connected devices, as shown in Fig. 7.

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig

Wireless0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::20B:BEFF:FE9B:6342
   IP Address.....: 192.168.88.5
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.88.1
```

Figure 7. Running network test results (without DHCP Alert)

From Fig. 7, can be seen that one of the clients gets the configuration that comes from DHCP Rogue. The client gets IP Address 192.168.88.5 with Gateway 192.168.88.1. The configuration results in the device not being able to connect to the network (the Trusted DHCP server has an address of 192.168.1.1), as well as the confusion in the distribution of IP addresses on the network.

Detailed of network test results without DHCP Snooping can be seen in Table 2.

Table 2. Address Obtained from Testing Without DHCP Snooping

Device	Interface	IP Address	Subnet mask	Gateway	DNS
DHCP Trusted	Core Gig6/0	192.168.1.1	255.255.255.0	192.168.1.1	8.8.8.8
Server DNS	Fa0/0	8.8.8.1	255.255.255.0	8.8.8.1	
DHCP Rogue	Router Gig0/0	192.168.88.1	255.255.255.0	192.168.88.1	1.1.1.1
Client	Switch Fa0/1	192.168.1.11	255.255.255.0	192.168.1.1	8.8.8.8
Laptop 1	WIFI	192.168.88.5	255.255.255.0	192.168.88.1	1.1.1.1
Laptop 2	WIFI	192.168.1.14	255.255.255.0	192.168.1.1	8.8.8.8
Laptop 5	WIFI	192.168.88.4	255.255.255.0	192.168.88.1	1.1.1.1

From Table 2, it can be identified on Table 2 that Laptop 1 and Laptop 5 get a configuration that comes from DHCP Rogue.

3.3 *Proposed Configuration*

Physically, there are no changes or adjustments needed to overcome problems related to thickening the security system on the object of research. The suggestions given relate to logical adjustments to the configuration of network devices. Logically, the desired concept is that when a client requests an IP address from DHCP, the client will exchange messages with the DHCP Server. A message in the form of a data packet containing a request for this IP address will be broadcast throughout the network. Furthermore, the switch will be filtered first so that the packet is not sent to DHCP Rogue and the packet will only be forwarded to a trusted port, or to a server that has been configured DHCP Alert first.

Thus, only authorized DHCP Server can assign IP addresses. If there is an unknown DHCP Server, it will be ignored, because DHCP traffic has been filtered both on the Switch and on the Router so that unknown DHCP cannot reply to message exchanges with clients, which means that the message can only be replied to by authorized or trusted DHCP.

3.3.1 *Configuration of DHCP Alert on Winbox:* After entering the login menu on Winbox, a connection is made to the address 192.168.1.9, then enter the IP menu and the DHCP Server sub-menu, to setup DHCP Alert.

On the DHCP Alert tab, create the desired DHCP Alert rules, as illustrated in Fig. 8.

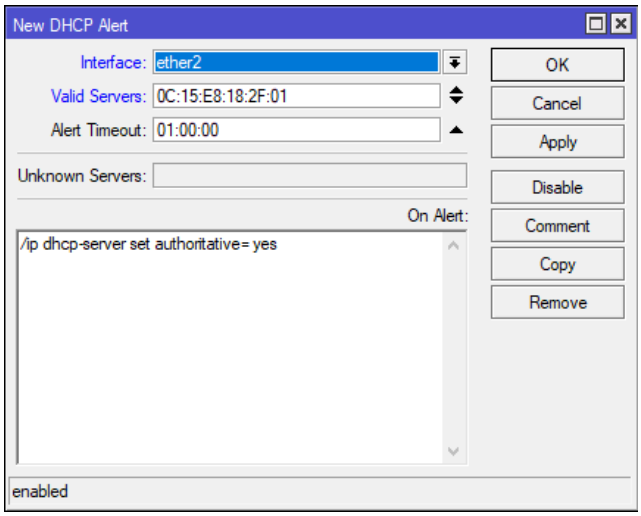

Figure 8. Rule of DHCP Alert

The details of the desired parameters are as follows:

1. *Interface*. This parameter relates to the port that DHCP Alert will configure. Ether2 is used.
2. *Valid Server*. This parameter contains the physical address or MAC Address port where the DHCP Alert is configured. In this case filled with 0C:15:E8:18:2F:01
3. *Alert Timeout*. Shows the number of time intervals before the DHCP Alert detects fake or unauthorized DHCP. Configured 1:00:00.
4. *Unknown Server*. This parameter will be filled if DHCP Alert finds unauthorized DHCP on the network. This column will show the MAC Address of the unauthorized DHCP.
5. *On Alert*. It is a parameter to determine the reaction of DHCP Alert if it finds unauthorized DHCP on the network, in this case, uses the command `/ip dhcp-server set authoritative=yes`, which will make only the authorized DHCP that can assign IP addresses to clients.

3.3.2 *Configuration of DHCP Snooping on Cisco Switch:* Next is the configuration that will be given to the Cisco Switch to implement the DHCP Snooping feature. From the Command Line Interface on the switch, enter the following configuration:

```
Switch>en

Switch#conf t
```

The next command is to activate the DHCP Snooping service

```
Switch(config)# ip dhcp snooping
```

Then the selection of the interface to be opened, namely Gigabit Ethernet port 0/1 or gig0/1

```
Switch(config)#int gig0/1
```

Followed by the command to ensure that the interface that was opened earlier is a trusted interface and can be passed by data traffic in the form of the desired DHCP packet.

```
Switch(config-if)#ip dhcp snooping
    trust

Switch(config-if)#ex
```

After completing a series for the selected interface, the same steps are continued on the next interface, namely Fast Ethernet 0/1 (fa0/1) and Fast Ethernet port 0/3 (fa0/3)

```
Switch(config)#int fa0/1

Switch(config-if)#ip dhcp snooping
    trust

Switch(config-if)#ex

Switch(config)#int fa0/3

Switch(config-if)#ip dhcp snooping
    trust

Switch(config-if)#ex

Switch#
```

After the configuration is given, check the status of the IP DHCP Snooping that has been given, by entering the command

```
Switch#show ip dhcp snooping
```

The results of the command given above, will show the detailed status of each interface on the switch, as shown in Fig. 9

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
none
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/3            yes        unlimited
FastEthernet0/1            yes        unlimited
GigabitEthernet0/2         no         unlimited
GigabitEthernet0/1         yes        unlimited
Switch#
```

Figure 9. Interface status on configured switch

From Fig. 9, it shown that there are 3 interfaces that were given the configuration command for DHCP Snooping, namely Fast Ethernet 0/3, Fast Ethernet 0/1 and Gigabit Ethernet 0/1, given the status of "Trusted". Meanwhile, Gigabit Ethernet 0/2 is listed as "Untrusted".

Option 82 contained in the detailed status in Fig. 9, is called the relay agent information option and is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers recognizing the relay agent information option may use the information to implement IP address or other parameter assignment policies. The DHCP server echoes the option back verbatim to the relay agent in server-to-client replies, and the relay agent strips the option before forwarding the reply to the client[15]. Option 82 can also be referred to as the DHCP Information Option, which contains additional information from a client. This information includes the MAC address of the switch, or remote ID Sub option, and a port identifier or port identifier. Option 82 is used in network environments using a distributed DHCP server / DHCP Relay.

The benefit of using Option 82 is, DHCP Server can use the identity of the relay agent and source port information from the client. Furthermore, activating option 82 will improve the protection of access to the network by blocking any attempts that try to imitate an authorized client. In addition, all attempt possibilities will be prevented from imitating response packets that originate from authorized DHCP Server.

3.4 Proposed Configuration Testing

3.4.1 *Test for DHCP Alert Implementation:* After configuring DHCP Alert, the test is carried out on client 2, which previously tested before implementing DHCP Alert (see section 3.2.1), obtained the IP Address from DHCP Rogue so that it failed to communicate with the internet network. In Fig. 10, the results of network testing that have implemented DHCP Alert are shown.

```
Client2> clear ip
IPv4 address/mask, gateway, DNS, and DHCP cleared

Client2> clear arp

Client2> clear hist

Client2> dhcp
DORA IP 192.168.88.253/24 GW 192.168.88.1

Client2> dhcp
DORA IP 192.168.2.253/24 GW 192.168.2.1

Client2> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=114 time=27.344 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=114 time=27.288 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=114 time=26.524 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=114 time=33.777 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=114 time=26.022 ms
```

Figure 10. Proposed configuration test results (with DHCP Alert)

As seen in Fig. 10, the IP Address that the client gets after implementing DHCP Alert, where this condition can occur because the request packet that the client sends to the DHCP Server contains an IP address that is not recognized by the authentic DHCP Server, namely `DORA IP 192.168.88.253/24 GW 192.168.88.1`. So then the original DHCP will send a NACK (Negative Acknowledgment) so that the client-server repeats the DORA process. After the `dhcp` command is sent once again, the results are read `DORA IP 192.168.2.253/24 GW 192.168.2.1`. Then tested connectivity to the Google DNS Server address, connectivity was successfully established.

Table 3 shows the complete address data that was successfully given to all clients after DHCP Alert was applied to the simulated network.

Table 3 Address Obtained from Testing With DHCP Alert

Device	Interface	IP Address	Subnet mask	Gateway	DNS
Mikrotik Core	Ether 2 – 3 (Bridge)	192.168.2.1	255.255.255.0	192.168.1.1	8.8.8.8
DHCP Rogue	Ether 1	192.168.88.1	255.255.255.0	192.168.88.1	1.1.1.1
Client	Switch – Eth 2	192.168.2.254	255.255.255.0	192.168.2.1	8.8.8.8
Client 2	Switch 1 – Eth 2	192.168.2.253	255.255.255.0	192.168.2.1	8.8.8.8
Client 3	Switch 1 – Eth 1	192.168.1.14	255.255.255.0	192.168.1.1	8.8.8.8

From Table 3, it can be seen that each client can get an address from an authorized DHCP Server. This is based on the DHCP data traffic that has been directed to the trusted DHCP Server only, while communications with the DHCP server that result in an unknown address will be ignored.

3.4.2 *Test for DHCP Snooping Implementation:* After the DHCP Snooping configuration is carried out, the test is carried out with the same scheme as the scheme used on a running network without DHCP Snooping (see section 3.2.2). The results of the tests carried out after the application of DHCP Snooping are shown in Fig. 11.

From the configuration shown in Fig. 11, the client gets the IP address 192.168.1.19 with the gateway 192.168.1.1.

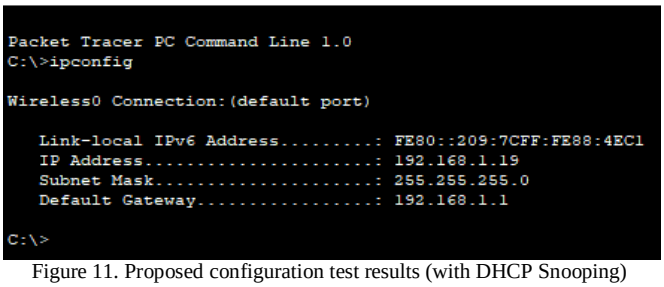

Figure 11. Proposed configuration test results (with DHCP Snooping)

With DHCP Snooping, DHCP data packet traffic has been filtered and directed to the registered interface (trusted interface), so that communication from clients can only be replied to by Trusted DHCP Server, according to the settings in DHCP Alert.

Complete details of the address obtained after implementing DHCP Snooping can be seen in Table 4. The results of network testing with DHCP Snooping show clearly that all IP addresses on the client have received a distribution from the Trusted DHCP Server.

Table 4. Address Obtained from Testing With DHCP Snooping

Device	Interface	IP Address	Subnet mask	Gateway	DNS
DHCP Trusted	Core Gig6/0	192.168.1.1	255.255.255.0	192.168.1.1	8.8.8.8
Server DNS	Fa0/0	8.8.8.8	255.255.255.0	8.8.8.1	
DHCP Rogue	Router Gig0/0	192.168.88.1	255.255.255.0	192.168.88.1	1.1.1.1
Client	Switch Fa0/1	192.168.1.11	255.255.255.0	192.168.1.1	8.8.8.8
Laptop 1	WIFI	192.168.1.19	255.255.255.0	192.168.1.1	8.8.8.8
Laptop 2	WIFI	192.168.1.14	255.255.255.0	192.168.1.1	8.8.8.8
Laptop 5	WIFI	192.168.1.25	255.255.255.0	192.168.1.1	8.8.8.8

4 CONCLUSION

DHCP Server security vulnerability at PT. Rekayasa engineering has the potential to lead to the installation of a Rogue DHCP by attackers. The existence of the unauthorized DHCP Server causes the client device to communicate with the DHCP Server to get an unauthenticated host configuration and makes the client fail to connect to the corporate network and is further under the control of the attacker who has provided a fake gateway to the client. From the tests carried out through network scheme simulations on the research object, DHCP Snooping configuration strengthened by DHCP Alert has succeeded in preventing DHCP Rogue from providing unauthenticated host configurations to clients by directing client and server communications to only interfaces that have been registered (registered interface)), while preventing the unauthorized DHCP Server from replying to the DHCP Message from the client at the beginning of the DORA process between the client and server. Thus, DHCP Message traffic can only occur between an authorized DHCP Server and a client.

REFERENCES

[1] M. Yaibuates and R. Chaisricharoen, "Starvation Delayed DHCP Service for Enabling Pool Recovery," *Malaysian J. Comput. Sci. Inf. Technol. Electr. Eng.*, no. Special Issue 2019, pp. 15–34, 2019, doi: 10.22452/mjcs.sp2019no2.2.

[2] N. Abdulhafiz, E. Faith, and O. Oyenike, "Mitigating DHCP Starvation Attack Using Snooping Technique," *FUDMA J. Sci.*, vol. 4, no. 1, pp. 560–566, 2020.

[3] S. Naaz and F. A. Badroo, "Investigasi Protokol DHCP dan DNS Menggunakan Wireshark," *IOSR J. Comput. Eng.*, vol. 18, no. May-June 2016, 2016, doi: 10.9790/0661-1803020108.

[4] A. Yan, S. Jing, Q. Qi, and B. Xiao, "A Study on Campus Network Access and Export Management," in *2nd Workshop on Advanced Research and Technology in Industry Application (WARTIA 2016)*, 2016, no. WARTIA 2016, pp. 1814–1818, doi: 10.2991/wartia-16.2016.359.

[5] W. Odom, *Cisco CCNA: Routing and Switching 200-120 Official Cert Guide Library*, April 2013. Indianapolis, USA: Cisco Press, 2013.

[6] M. Yaibuates and R. Chaisricharoen, "Implementing of IP address Recovery for DHCP Service," *Int. J. Appl. Eng. Res.*, vol. 13, no. 5, pp. 2659–2662, 2018, [Online]. Available: http://www.ripublication.com.

[7] O. S. Younes, "A Secure DHCP Protocol to Mitigate LAN Attacks," *J. Comput. Commun.*, vol. 04, no. 01, pp. 39–50, 2016, doi: 10.4236/jcc.2016.41005.

[8] Z. Miftah, "Simulasi Keamanan Jaringan Dengan Metode Dhcp Snooping Dan Vlan," *Fakt. Exacta*, vol. 11, no. 2, p. 167, 2018, doi: 10.30998/faktorexacta.v11i2.2456.

[9] T. Ariyadi, "Mitigasi Keamanan Dynamic Host Control Protocl (DHCP) Untuk Mengurangi Serangan Pada Local Area Network (LAN)," *Inovtek Polbeng - Seri Inform.*, vol. 3, no. 2, pp. 147–154, 2018, doi: 10.35314/isi.v3i2.455.

[10] R. Natarajan, "Different Possibilities of DHCP Attacks and Their Security Features," *Glob. Res. Dev. J. Eng.*, vol. 1, no. 1, pp. 20–23, 2015.

[11] MikroTik, "DHCP Snooping and DHCP Option 82," *Manual:Interface/Bridge*. https://wiki.mikrotik.com/wiki/Manual:Interface/Bridge#DHCP_Snooping_and_DHCP_Option_82 (accessed Jan. 19, 2021).

[12] D. Diwan, V. K. Narang, and A. K. Singh, "Security Mechanism in RIPv2 , EIGRP and OSPF for Campus Network - A Review," *Int. J. Comput. Sci. Trends Technol.*, vol. 5, no. 2, pp. 399–404, 2017.

[13] D. Kurnia, "Analisis Serangan DHCP Starvation Attack Pada Router OS Mikrotik," *J. Ilm. Core IT*, vol. 8, no. 5, pp. 12–17, 2020.

[14] J. West, J. Andrews, and T. Dean, *Network+ Guide to Networks*, 8th Ed. Boston, USA: Cengage Learning, 2019.

[15] D. C. Hewlett-Packard, "HP Switch Software Multicast and Routing Guide for K/KA/KB.15.18," *August, 3rd*, 2015. https://techhub.hpe.com/eginfolib/networking/docs/switches/K-KA-KB/15-18/5998-8164_mrg/content/ch12s11.html (accessed Jan. 01, 2021).