Analysis of Dynamic Host Control Protocol Implementation to Assess DoS Attacks

Shameel Syed
Dept. of Computer Systems, Mehran University of Engineering and Technology
Jamshoro, Pakistan
shameel_uddin@yahoo.com

Faheem Khuhawar
Dept. of Telecommunication, Mehran University of Engineering and Technology
Jamshoro, Country
faheem.khuhawar@faculty.muet.edu.pk

Shahnawaz Talpur
Dept. of Computer Systems, Mehran University of Engineering and Technology
Jamshoro, Pakistan
shahnawaz.talpur@faculty.muet.edu.pk

Aftab Ahmed Memon
Dept. of Telecommunication, Mehran University of Engineering and Technology
Jamshoro, Pakistan
aftab.memon@faculty.muet.edu.pk

Miquel-Angel Luque-Nieto
Institute of Oceanic Engineering Research, University of Malaga
Malaga, Spain
luquen@uma.es

Sanam Narejo
Dept. of Computer Systems, Mehran University of Engineering and Technology
Jamshoro, Pakistan
sanam.narejo@faculty.muet.edu.pk

***Abstract*— Dynamic Host Control Protocol (DHCP) is a protocol which provides IP addresses and network configuration parameters to the hosts present in the network. This protocol is deployed in small, medium, and large size organizations which removes the burden from network administrator to manually assign network parameters to every host in the network for establishing communication. Every vendor who plans to incorporate DHCP service in its device follows the working flow defined in Request for Comments (RFC). DHCP Starvation and DHCP Flooding attack are Denial of Service (DoS) attacks to prevents provision of IP addresses by DHCP. Port Security and DHCP snooping are built-in security features which prevents these DoS attacks. However, novel techniques have been devised to bypass these security features which uses ARP and ICMP protocol to perform the attack. The purpose of this research is to analyze implementation of DHCP in multiple devices to verify the involvement of both ARP and ICMP in the address acquisition process of DHCP as per RFC and to validate the results of prior research which assumes ARP or ICMP are used by default in all of devices.**

Keywords*— *DHCP, DHCP Starvation, DHCP Flooding, DHCP Snooping, Port Security, DHCP Security, Network Security.

I. INTRODUCTION

IP address is a layer-3 address according to Open System Interconnect (OSI) layer architecture which is necessary to establish communication in Internet. It is also essential to establish communication in intranet if VLANs are present and the network is isolated at layer 2. There could be hundreds, if not thousands of hosts available in the network and assigning IP addresses, gateway information, DNS information to all these hosts becomes a hectic and impractical task which would require an extensive amount of human force for completion and could result in a human error. For this purpose, Dynamic Host Control Protocol (DHCP) was introduced [1], which is an application layer protocol and adopts client-server architecture. Purpose of DHCP is to establish automation for the provision of network configuration parameters to hosts. It is considered as a centralized management solution which aims to reduces overall burden on network administrator and remove the human-error factor in provision of IP addresses and related network parameters to the hosts within the network.

DHCP allocates IP addresses to the hosts in three different mechanisms which are as follows:

1. Automatic Allocation: In this mechanism, a permanent IP address is assigned to the host by DHCP server. This prevents the re-usability of IP address in-case the host is down for longer duration of time, or the host has been removed from network infrastructure.
2. Manual Allocation: In this mechanism, network administrator must assign the IP address manually to the host. It is helpful in case where the IP address and unique network parameters needs to be assigned to servers but not helpful in a scenario where the IP addresses needs to be re-used and assigned to multiple hosts for communication purpose.
3. Dynamic Allocation: This is widely used case scenario of DHCP where the IP addresses are dynamically assigned to the hosts which can be re-used if the host is down for a certain duration of time.

Depending upon the policy of network, one of these three mechanisms can be deployed in a network infrastructure where dynamic allocation is the most widely used mechanism out of all three available. It also proves helpful for permanent allocation of IP addresses to the hosts if the hosts are up indefinitely .

Since DHCP is a client-server architecture, certain DHCP messages are exchanged between DHCP server and DHCP client. The format of DHCP message is described in Fig. 1 which has also been taken from RFC 2131 [2].

Description of each of the fields in DHCP message format as illustrated in Fig. 1 is as follows,

1. OP Code: It is of size 1 octet and contains only BOOTREQUEST and BOOTRESPONSE.

2022 Global Conference on Wireless and Optical Technologies (GCWOT) | 978-1-6654-7105-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/GCWOT53057.2022.9772887

978-1-6654-7105-3/22/$31.00 ©2022 IEEE

2. Hardware Type: It is of size 1 octet which shows the type of hardware.
3. Hardware Length: It is of size 1 octet which denotes the length of hardware.
4. Hops: It is of size 1 octet. It is only set by relay agents, and it denotes number of relays which were used as middle devices.
5. Transaction Identifier: It is of size 4 octets. DHCP client chooses this value randomly to establish association with DHCP server.
6. Seconds: It is of size 2 octets. It denotes number of seconds which have been elapsed for renewal process.
7. Flags: It is of size 2 octets. It is used for broadcast or unicast purpose of sending messages.
8. Client IP Address: It is of size 4 octets. It contains IP address of the client if it is in REBINDING, RENEW or BOUND state.
9. Your IP Address: It is of size 4 octets. It contains IP address of the client.
10. Server IP Address: It is of size 4 octets. It contains IP address of the DHCP Server.
11. Client Hardware Address: It is of size 16 octets. It contains MAC address of the client.

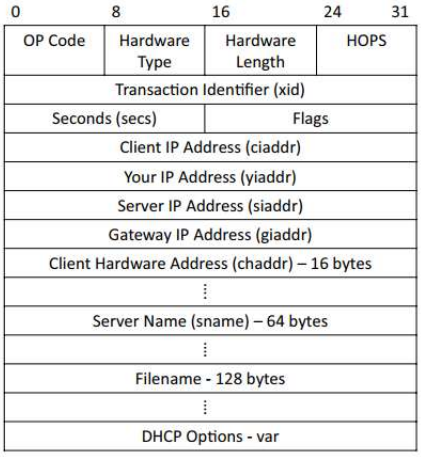

Fig. 1. DHCP Message Format

DHCP messages and their respective usages are described in TABLE I.

TABLE I. DHCP MESSAGE AND ITS DESCRIPTION.

Message	Usage
DHCP DISCOVER	It is a broadcast message which is initiated from DHCP Client.
DHCP OFFER	It is sent as a response from DHCP Server to DHCP request.
DHCP REQUEST	It is sent from DHCP client as a request to assign offered network parameters
DHCP ACK	It is sent as an acknowledgment from DHCP server to DHCP client.
DHCP NAK	It is sent from server to client indicating that client's notion of network is incorrect.
DHCP DECLINE	It is sent from client to server when the requested IP addresses is already in use.
DHCP RELEASE	It is sent from client to server to release the acquired IP address.
DHCP INFORM	It is sent from client to server for acquiring local configuration parameters only.

II. LITERATURE REVIEW

DHCP client needs to complete Discovery, Offer, Request, Acknowledgement (D.O.R.A.) process to successfully acquire an IP address from DHCP server as depicted in Fig. 2.

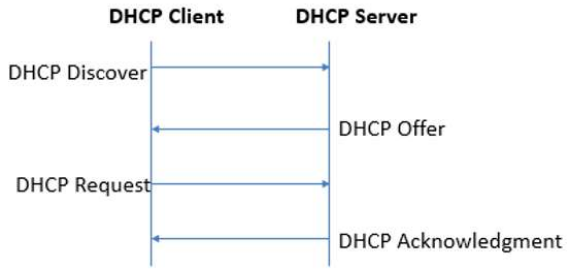

Fig. 2. DHCP IP Address Acquisition

The process for acquiring an IP address assignment is as follows,

1. DHCP client initiates the association by first sending DHCPDISCOVER message as a broadcast message in the network. It is sent as a broadcast message to discover DHCP server within the network.
2. There can be more than one DHCP servers which can receive the message. Upon reception, DHCP server sends DHCPOFFER message to the client as a unicast message.
3. If there are more than one DHCP servers in the network, then DHCP client may receive more than one DHCPOFFER message. DHCPOFFER message which is received firstly by the DHCP client will be chosen then the client sends DHCPREQUEST message as a broadcast message in the network. The purpose of this broadcast is to inform the chosen server that the client wants to accept its parameters and inform the other server that it has not been chosen.
4. When DHCP server receives DHCPREQUEST message, it sends DHCPACK to complete the binding process if there are no problems in DHCPREQUEST message and it has been created as per required standards from the

parameters provided in DHCPOFFER message previously.

Once this process is completed, an IP address is acquired by the host, and it can now establish communication on Internet. If the client requires more information from the server, it sends DHCPINFORM message and if it no longer requires the received IP address and network configuration parameters, it sends DHCPRELEASE message to the DHCP server. If there is some problem with received parameters i.e., in case of IP address duplication, it sends DHCPDECLINE message to the server. Similarly, if there is some problem with DHCPREQUEST message from the client, DHCP server sends DHCPNAK message to the client.

There is an involvement from two other protocols which are Address Resolution Protocol (ARP) and Internet Control Message Protocol (ICMP) during D.O.R.A. process. The purpose of ARP is to discover and identify hardware address (MAC address) of a device from its provided IP address whereas, ICMP is used for diagnostic purpose to ensure that the host is up and running. These protocols are used in conjunction with D.O.R.A. process for IP address acquisition to ensure that IP conflict does not occur within the network during or after the provision of the IP address from DHCP server.

A. DHCP Attacks

Purpose of DHCP is to serve IP addresses and network configuration to the hosts, however, DHCP flooding and DHCP starvation attacks prevents DHCP server from serving IP addresses and network related configuration to the clients, thus achieving DoS in DHCP services.

1) DHCP Flooding:

It is achieved when DHCP client continuously sends DHCPDISCOVER, DHCPINFORM or any other DHCP related message which is not immediately dropped by DHCP server but processed by it, thus resources of DHCP server will be consumed which will further prevent DHCP server to serve legitimate hosts present in the network in timely manner. If the attack is severe, it may leave DHCP server unable to serve legitimate clients at all.

2) DHCP Starvation:

The purpose of this attack is to starve DHCP server from its IP addresses. Since there is a pool of IP addresses which is configured in DHCP server and when it offers and acknowledges an IP address to a certain host, it marks it as 'unavailable'. In this attack, threat actor completes D.O.R.A. process continuously to make sure that the DHCP server runs out of all the IP addresses, making it unable to serve legitimate hosts afterwards.

B. Prevention Mechanism for DHCP Attacks

Multiple approaches are available to detect and mitigate attacks related to DHCP. Port security and DHCP snooping are one of those approaches which are available by default in most of networking switches.

1) Port Security:

Port security is a layer-2 feature which is not designed as a security feature specifically for DHCP but for overall security of the port, however, it provides protection from DHCP flooding attacks. One of its features is to limit total number of MAC addresses per frames such that if total number of frames with variable MAC addresses arrives at the port, the port either goes into a shutdown mode or it starts dropping further traffic. This proves to be an effective measure against DHCP flooding attack to prevent flooding after a certain configured threshold. An extension of port security mechanism for wireless networks has been proposed in [3].

Port security will fail to protect DHCP flooding and DHCP starvation attack if the MAC address in the header arriving in every frame is same and MAC address in 'chaddr' field of DHCP message is different.

Port Security can prevent attack launched from Yersinia or Hyenae attacking tools [4], however, it will fail to prevent an attack launched from DHCPStarv, DHCPig, DHCPwn and DStar because these tools use static MAC address in Ethernet field but variable hardware address in 'chaddr' field within DHCP message.

2) DHCP Snooping:

It is one of the security prevention mechanisms for DHCP attacks where the ports are either configured as 'trusted' or 'untrusted'. Port which is connected to DHCP server must be configured as trusted and the port which is connected towards DHCP client must be configured as untrusted. If a message which is supposed to be sent from DHCP server like DHCPOFFER or DHCPACK arrives at untrusted port, it is immediately dropped. Thus, the ports which are not connected to DHCP server must always be configured as untrusted. Furthermore, DHCP snooping can also limit rate of DHCP traffic at port level. It also drops the traffic if there is a mismatch between MAC addresses present in Ethernet header and 'chaddr' field of DHCP message.

These are effective measures against DHCP flooding, DHCP starvation and DHCP spoofing attacks where the limiting factor and mismatch factor prevents DHCP flooding and DHCP starvation attack and configuration of trusted and untrusted ports prevents DHCP spoofing attack.

DHCP snooping prevention mechanism fails to work against DHCP spoofing attack if the attacker is outside the broadcast domain [5].

3) DHCP Authentication:

Multiple authors have used DHCP authentication mechanism as a preventive mechanism. [6] used digital certificates for authentication. [7] introduces a complete DHCP authentication module. [8] also provides certificate-based access control along with authentication. [9] uses Kerberos for authentication purpose. [10] uses symmetric key for authentication to propose P-DHCP. [11] uses PKI and PGP for authentication of DHCP.

C. Novel Attacks Bypassing Prevention Mechanisms

Classic DHCP attacks do not work in wireless network as well as in those wired network in which port security and DHCP snooping is enabled, however authors have devised different techniques to make these attacks a success from different approaches [12].

1) DHCP Starvation using Server-Side Conflict:

DHCP starvation attack by creating a conflict at DHCP server is proposed by [13], which works as follows,

1. For a wireless network, DHCP client first associates itself with Access Point (AP) and then attempts to send DHCPDISCOVER message, whereas, in wired network,

as soon as host boots up and connects to the network, it sends DHCPDISCOVER message directly without any association step.

2. Once DHCP server receives DHCPDISCOVER message from DHCP client, it selects one of the available IP addresses from its pool, which will be offered to the client. However, before sending DHCPOFFER message, DHCP server attempts to probe the network to verify that this IP address is not in use by some other host.
3. Implementation of DHCP service may vary from vendor to vendor and device to device. For example, DHCP server may either use ICMP or ARP to perform this operation. If DHCP server uses ARP for probing purpose, then it creates an ARP request and broadcast it into the network. If DHCP server uses ICMP for probing purpose, then it creates an ICMP request and broadcast it into the network.
4. Threat actor present in the network receives this request. If it is an ARP request, the threat actor forges a fake ARP response which indicates that the IP address is in use by the threat actor. If it is an ICMP request, the threat actor forges a fake ICMP response which indicates that the IP address is in use by the threat actor.
5. Upon reception of the fake response forged by threat actor, DHCP server marks the IP address as 'unavailable' in its database and sends another ARP or ICMP request with a different available IP address in its pool. Threat actor again forges the fake response. This process repeats until the DHCP server runs out of available IP addresses in its pool.

The proposed attack bypasses both port security and DHCP snooping as it does not use any DHCP related messages to perform the attack. It simply responds to ARP request and ICMP request messages to perform the attack.

2) DHCP Starvation using Client-Side Conflict:

Another conflict can be caused but from client side to perform a successful starvation attack in DHCP service within the network infrastructure which is proposed in [14]. Following are the steps of this attack:

1. Malicious client first configures itself with an IP address right after joining the network without making any noise and forwarding any traffic to avoid its MAC address being stored in DHCP snooping's database.
2. Victim client completes D.O.R.A. process to acquire an IP address from DHCP server.
3. Depending upon the configuration of DHCP service in client, it may produce ARP or ICMP request message and broadcast it into the network.
4. Upon reception of ARP or ICMP request, malicious client forges a fake ARP or IMCP response and sends it to the client.
5. When victim DHCP client receives this response, it assumes that the acquired IP address is in use by some other host and it sends DHCPDECLINE message to the DHCP server, upon which DHCP server offers another IP address.
6. The process repeats until DHCP server runs out of IP addresses from its pool.

This technique also bypasses Port Security and DHCP snooping for the same reason as described in previous section as the malicious client does not send DHCP specific messages in the network. Furthermore, when the malicious client configures itself with an IP address and prevents any interaction in the network, so it also bypasses Dynamic ARP Inspection (DAI) security feature available in the network.

D. Shortcomings in Related Studies

Studies has been done over the years for the detection or mitigation of DHCP attacks. Authors in [14] and [15] made use of training and testing of models using probability and Machine Learning (ML) approach for DHCP. Upon different implementations by different vendors for different devices, the inclusion of these devices may vary.

Shortcomings in these studies are the usage of ICMP protocol [16] or ARP protocol [14], where, the authors assumed that these protocols behave in exact same fashion in all the devices of all the vendors.

DHCP does not have any authentication feature authentication feature by default which was later proposed in RFC 3118 [17]. Two different techniques have been proposed, namely delayed authentication and configuration token [18], which uses 'option' field in DHCP messages. However, it is 255 bytes which poses a problem for large size of data. To encode a larger data, technique was introduced in [19]. Delayed authentication uses Hash-based Message Authentication Code (HMAC) and involves MD5 message-digest algorithm along with a pre-shared secret key to generate Message Authentication Code (MAC) for DHCP messages. This technique solves the problem of message authentication and DHCP entity authentication with the help of shared secret-key, but it fails to demonstrate the management of shared secret key in the presence of large number of DHCP clients. Furthermore, the weakness in MD5 hash function has already been demonstrated in [20], showing how collisions can be found almost instantly.

Configuration token is also based on shared secret token between DHCP client and DHCP server, however, this scheme only protects DHCP server, and it fails to support authentication in DHCP messages.

Other shortcomings involve complex involvement of protocols which cannot be integrated with built-in DHCP which may overwhelm the networking device. Some authors trained ML model, however the dataset used in those models is outdated and does not contain novel attack scenarios discussed in the literature.

III. Experimental Work (Server-Side)

In this research, experiments have been performed on DHCP services present in products of Microsoft, Cisco, and Huawei. Results are captured using Wireshark packet capturing tool. The function of Wireshark is like other packet capturing tool which captures traffic in PCAP format and stores the traffic in storage device.

A. Router

An experiment has been conducted twice in two different models of Huawei, and once in a Cisco device. DHCP server is configured in routers and then the behavior is analyzed.

Topology for the experiment of cisco is emulated using GNS3 which is shown in Fig. 3.

Fig. 3. Analysis of DHCP in Cisco Router C3600

Scope of DHCP pool is configured with 192.168.0.0/24 where DHCP server is configured with 192.168.0.1 which assigns IP addresses from 192.168.0.2 to 192.168.0.253. The traffic has been captured from Wireshark from server side which is shown in Fig. 4.

No.	Time	Info
5	25.328382	DHCP Discover - Transaction ID 0xabc09225
6	25.383704	DHCP Offer - Transaction ID 0xabc09225
7	26.328529	DHCP Request - Transaction ID 0xabc09225
8	26.338710	DHCP ACK - Transaction ID 0xabc09225

Fig. 4. Wireshark Result of Cisco Router C3600

Second experiment for router is performed on Huawei AR1220 which is presented in Fig. 5. 10.1.1.0/24 is configured as a scope for DHCP pool where 10.1.1.254 serves as a DHCP server.

Fig. 5. Analysis of DHCP in Huawei Router AR1220

During the D.O.R.A. process, it does not send ICMP echo request message to detect IP conflict problem in the network as illustrated in the Wireshark result demonstrated in Fig. 6.

No.	Time	Info
1	0.000000	DHCP Discover - Transaction ID 0x6cc3
2	0.015000	DHCP Offer - Transaction ID 0x6cc3
3	2.000000	DHCP Request - Transaction ID 0x6cc3
4	2.015000	DHCP ACK - Transaction ID 0x6cc3

Fig. 6. Wireshark Results of Huawei Router AR1220

Another experiment on Huawei AR2220 router is performed having same configuration as previous experiment. The result of which are mentioned in Fig. 7.

No.	Time	Info
1	0.000000	DHCP Discover - Transaction ID 0x73b6
2	0.031000	DHCP Offer - Transaction ID 0x73b6
3	2.000000	DHCP Request - Transaction ID 0x73b6
4	2.015000	DHCP ACK - Transaction ID 0x73b6

Fig. 7. Wireshark Results of Huawei Router AR2220

In these experiments, DHCP server present in the routers neither broadcasts ARP, nor broadcasts ICMP request message to detect duplicate IP address in the network.

B. *Experiments on Switches*

Two experiments have been performed on Huawei's switch used in eNSP Simulator. One of the experiments involve S3700 with the same topology and configuration discussed earlier. The results of which are shown in Fig. 8.

19	31.796000	DHCP Discover - Transaction ID 0x5cba
20	32.312000	Who has 10.1.1.126? Tell 10.1.1.1
21	33.328000	DHCP Offer - Transaction ID 0x5cba
23	33.812000	DHCP Request - Transaction ID 0x5cba
24	33.828000	DHCP ACK - Transaction ID 0x5cba

Fig. 8. Wireshark Results of Huawei Switch S3700

Second experiment involves S5700 with same configuration of 10.1.0.0/24 having DHCP server at 10.1.1.1 and assigning IP addresses from (10.1.1.2 to 10.1.1.253) through D.O.R.A. process is demonstrated in Fig. 9.

4	5.609000	DHCP Discover - Transaction ID 0x62cc
5	6.109000	Who has 10.1.1.126? Tell 10.1.1.1
7	7.109000	DHCP Offer - Transaction ID 0x62cc
8	7.609000	DHCP Request - Transaction ID 0x62cc
9	7.609000	DHCP ACK - Transaction ID 0x62cc

Fig. 9. Wireshark Result of Huawei Switch S5700

In these two experiments, the DHCP server present in the switches broadcast ARP request in the network to detect if the same IP address is in use by some other host.

C. *Experiments on Firewall*

An experiment has been performed on Huawei's USG6000V firewall having same topology with similar configuration as discussed earlier. Additionally, policies were defined to allow traffic to flow from server to client and vice-versa. Results of experiments on firewall are shown in Fig. 10.

2	42.579000	DHCP Discover - Transaction ID 0x509
3	42.657000	Who has 10.1.1.212? Tell 10.1.1.1
4	43.500000	DHCP Offer - Transaction ID 0x509
5	44.594000	DHCP Request - Transaction ID 0x509
6	44.594000	DHCP ACK - Transaction ID 0x509

Fig. 10. Wireshark Results of Firewall USG6000

D. *Experiments on Virtualization Platform*

Experiments have been performed on VirtualBox and VMware for type-2 hypervisor where operating system in install inside and the built-in DHCP is tested and analyzed. Result for VirtualBox is demonstrated in Fig. 11.

8	55.503011481	DHCP Discover - Transaction ID 0xe1474378
9	55.503554694	DHCP Offer - Transaction ID 0xe1474378
10	55.504186615	DHCP Request - Transaction ID 0xe1474378
11	55.508970016	DHCP ACK - Transaction ID 0xe1474378

Fig. 11. Wireshark Results of VirtualBox

Similarly, the results of experiments on VMware with similar configuration topology are shown in Fig. 12.

3	0.004597754	DHCP Discover - Transaction ID 0x864f4c13
4	0.005236874	Echo (ping) request id=0xd470, seq=0/0, ttl=16 (no response found!)
5	0.005237104	Who has 192.168.174.129? Tell 192.168.174.2
9	1.007576506	Who has 192.168.174.129? Tell 192.168.174.2
10	1.010640364	DHCP Offer - Transaction ID 0x864f4c13
11	1.011140052	DHCP Request - Transaction ID 0x864f4c13
12	1.012215930	DHCP ACK - Transaction ID 0x864f4c13

Fig. 12. Wireshark Results of VMware

The DHCP server present in VirtualBox neither uses ARP nor ICMP to detect duplicate IP addresses, whereas VMWare uses both ARP and ICMP protocols for detection purpose.

E. *Experiments on Wireless Router*

Using same topology and configuration, experiments have been performed on two real wireless routers of TP-Link company with model WR940N and WR840N.

The results suggest that WR940N neither used ARP nor ICMP, however, the results were different in WR840N model as seen in Fig. 13.

528	27.691217	DHCP Discover	- Transaction ID 0x4c6b4baf
541	27.773555	DHCP Offer	- Transaction ID 0x4c6b4baf
542	27.775854	DHCP Request	- Transaction ID 0x4c6b4baf
548	28.160590	Who has 192.168.2.112? Tell 192.168.2.1	
551	28.294060	DHCP ACK	- Transaction ID 0x4c6b4baf

Fig. 13. Wireshark Results of TP-Link Wireless Router

The result shown in Fig. 13 are completely different than any of the previous results since the ARP request is generated after DHCP-REQUEST message instead of DHCP-DISCOVER message.

Similarly, experiments were performed on D-Link's wireless router, which produced different results as shown in

1	0.000000	DHCP Discover	- Transaction ID 0xfe089c15
2	0.000384	Echo (ping) request	id=0x40d2, seq=0/0, ttl=64 (no response found!)
7	0.902558	DHCP Offer	- Transaction ID 0xfe089c15
8	0.903891	DHCP Request	- Transaction ID 0xfe089c15
13	1.147302	DHCP ACK	- Transaction ID 0xfe089c15

Fig. 14. Wireshark Results of D-Link Wireless Router

These are also different results since none of the experiments discussed so far produced ICMP echo message to detect IP address duplication.

F. Experiments on Windows Server

Similarly, experiments have been performed on Windows Server 2008, 2012, 2016, 2019, in which it has been observed that ICMP echo message is used to validate IP address duplication. However, it can be manually turned OFF and turned ON by system administrator. Results for different traffic flow of DHCP server analysis are summarized in TABLE II.

TABLE II. DHCP SERVER ANALYSIS

Device	ICMP	ARP
Cisco Router C3600	No	No
Huawei Router AR1220	No	No
Huawei Router AR2220	No	No
Huawei Switch S3700	No	After DHCP Discover
Huawei Switch S5700	No	After DHCP Discover
Huawei Firewall USG6000	No	After DHCP Discover
VirtualBox 6.1.8	No	No
VMWare Workstation 15.1.0	After DHCP Discover	After DHCP Discover

Topology with DHCP server and relay configuration has been demonstrated in Figure 15, for which, the Wireshark result for DHCP server is demonstrated in Figure 16 and for DHCP relay is demonstrated in Figure 17.

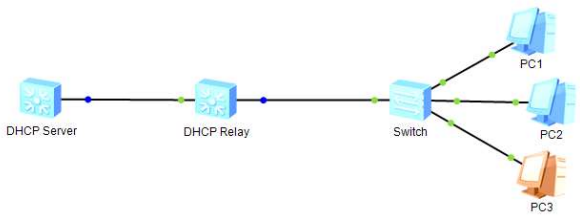

Fig. 15. Multi-Switch DHCP Topology

No.	Time	Info	Protocol
34	54.734000	DHCP Discover - Transaction ID 0x4e5f	DHCP
35	55.234000	Echo (ping) request id=0x0000, seq=655…	ICMP
36	55.766000	Echo (ping) request id=0x0000, seq=655…	ICMP
38	56.234000	DHCP Offer - Transaction ID 0x4e5f	DHCP
40	58.703000	DHCP Request - Transaction ID 0x4e5f	DHCP
41	58.719000	DHCP ACK - Transaction ID 0x4e5f	DHCP
42	60.141000	DHCP Discover - Transaction ID 0x4e79	DHCP

Fig. 16. Wireshark Results of Multi-Switch DHCP Server

No.	Time	Info	Protocol
13	20.797000	DHCP Discover - Transaction ID 0x4…	DHCP
14	21.344000	Who has 10.20.20.254? Tell 10.20.2…	ARP
15	22.344000	DHCP Offer - Transaction ID 0x4…	DHCP
17	24.797000	DHCP Request - Transaction ID 0x4…	DHCP
19	24.844000	DHCP ACK - Transaction ID 0x4…	DHCP

Fig. 17. Wireshark Results of Multi-Switch DHCP Relay

IV. EXPERIMENTAL WORK (CLIENT-SIDE)

Experiments have been performed on Windows 7, Windows 8, Windows 10, Ubuntu 16.04, Kali Linux 2020.3. All of these produce similar result in which ARP request is sent as a broadcast message in the network for the verification of IP address duplication as shown in Fig. 18. In the scenario where the duplicate IP address is present in the network, it sends DHCPDECLINE message to the server.

4	2.015000	DHCP ACK	- Transaction ID 0x6cc3
5	3.015000	Gratuitous ARP for 10.1.1.254 (Request)	
6	4.000000	Gratuitous ARP for 10.1.1.254 (Request)	
7	5.000000	Gratuitous ARP for 10.1.1.254 (Request)	

Fig. 18. Wireshark Results of Client-Side behavior

V. CONCLUSION AND FUTURE WORK

The paper presents comprehensive study on DHCP services present in different devices of multiple vendors. Research experiments performed on DHCP service present in Cisco, Huawei, Microsoft, D-Link, TP-Link, VirtualBox and VMWare demonstrate that ICMP and ARP are not integrated with DHCP D.O.R.A process in identical manner as per the requirement of RFC, which suggests that ICMP should be used for detection of IP address duplication.

These findings can be used to improve the novel attacks provided by previous studies to keep this variable factor of ARP and ICMP in check along with provided prevention mechanisms. For future work, we will perform analysis on other widely used layer protocols.

REFERENCES

[1] S. Steinke, "Dynamic Host Configuration Protocol," in *Network Tutorial*, CRC Press, 2003, p. 184–187.

[2] R. Droms, "RFC2131: Dynamic Host Configuration Protocol," RFC Editor, 1997.

[3] H. Mukhtar, K. Salah and Y. Iraqi, "Mitigation of DHCP starvation attack," *Computers & Electrical Engineering,* vol. 38, p. 1115–1128, September 2012.

[4] M. Aldaoud, D. Al-Abri, A. A. Maashri and F. Kausar, "DHCP attacking tools: an analysis," *Journal of Computer Virology and Hacking Techniques,* vol. 17, p. 119–129, January 2021.

[5] S. Akashi and Y. Tong, "Classification of DHCP Spoofing and Effectiveness of DHCP Snooping," in *Proceedings of the International Conference on*

Advances in Computer Technology, Information Science and Communications, 2019.

[6] D. D. Dinu and M. Togan, "DHCP server authentication using digital certificates," in *2014 10th International Conference on Communications (COMM)*, 2014.

[7] D. D. Dinu and M. Togan, "DHCPAuth - A DHCP message authentication module," in *2015 IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics*, 2015.

[8] J. Demerjian., A. Serhrouchni. and M. Achemlal., "Certificate-Based Access Control and Authentication for DHCP," in *Proceedings of the First International Conference on E-Business and Telecommunication Networks*, 2004.

[9] K. Hornstein, T. Lemon, D. B. D. Aboba and D. J. Trostle, "DHCP Authentication Via Kerberos V," Internet Engineering Task Force, 2001.

[10] O. S. Younes, "Securing ARP and DHCP for mitigating link layer attacks," *Sādhanā,* vol. 42, p. 2041–2053, November 2017.

[11] D. I. N. U. Dumitru Daniel, M. TOGAN and B. I. C. A. Ion, "ON DHCP SECURITY," *PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A,* vol. 18, pp. 403-412, 2017.

[12] N. Hubballi and N. Tripathi, "A closer look into DHCP starvation attack in wireless networks," *Computers & Security,* vol. 65, p. 387–404, March 2017.

[13] N. Tripathi and N. Hubballi, "Exploiting DHCP server-side IP address conflict detection: A DHCP starvation attack," in *2015 IEEE International Conference on Advanced Networks and Telecommuncations Systems (ANTS)*, 2015.

[14] N. Tripathi and N. Hubballi, "Detecting stealth DHCP starvation attack using machine learning approach," *Journal of Computer Virology and Hacking Techniques,* vol. 14, p. 233–244, November 2017.

[15] N. Tripathi and N. Hubballi, "A probabilistic anomaly detection scheme to detect DHCP starvation attacks," in *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2016.

[16] M. Yaibuates and R. Chaisricharoen, "ICMP based Malicious Attack Identification Method for DHCP," in *The 4th Joint International Conference on Information and Communication Technology, Electronic and Electrical Engineering (JICTEE)*, 2014.

[17] R. Droms, "RFC3118: Authentication for DHCP Messages," RFC Editor, 2001.

[18] O. S. Younes, "A Secure DHCP Protocol to Mitigate LAN Attacks," *Journal of Computer and Communications,* vol. 4, no. 0, pp. 39-50, 2016.

[19] T. Lemon and S. Cheshire, "RFC3396: Encoding Long Options in the Dynamic Host Configuration Protocol ({DHCPv}4)," RFC Editor, 2002.

[20] M. M. J. Stevens, "On Collisions for MD5," 2007.