



## A DENIAL OF SERVICE ATTACK ON DHCP SERVER AND ITS COUNTERMEASURES

Ashutosh Satapathy and Jenila Livingston L. M.

School of Computing Science and Engineering, Vellore Institute of Technology, Chennai, India

E-Mail: [ashutosh.satapathy2013@vit.ac.in](mailto:ashutosh.satapathy2013@vit.ac.in)

### ABSTRACT

Today, Internet is playing a major role for providing education in institutions to increase productivity in industries. To provide flexibilities and reliabilities in internet services, different network components are used. DHCP server is one of the components, used to assign IP addresses to client dynamically. Increasing the number of end machines not only provide benefit to organization, but also make those susceptible to attack. Denial of Service attack is one of the common forms of attacks used to prevent services to end users/ machines. This paper presents a way to perform DHCP Denial of Service attack using VMware Workstation. It also focuses the counter measures to prevent this attack.

**Keywords:** DHCP, DoS attack, network adapters, active directory, switch configuration.

### INTRODUCTION

In this digital world, massive amount of information is generated by end machines (client/ server). So, it requires a unique identification number to take part in network communication. To provide universal transmission between those machines, IP address comes in to the picture which is a 32/ 128 bits number associated with each machine and uniquely identifies it inside a network. As the number of machines increases day to day, manual assignment of IP address to these is really a difficult task. To overcome this situation, Dynamic Host Configuration Protocol (DHCP) plays the major role to provide IP address to end devices dynamically. It is one of the standardized protocol not only provides IP addresses on lease basis but also defeat the problems which is found in former protocols such as Reverse Address Resolution Protocol (RARP), Bootstrap Protocol (BOOTP) used for dynamic IP address allocation[1].

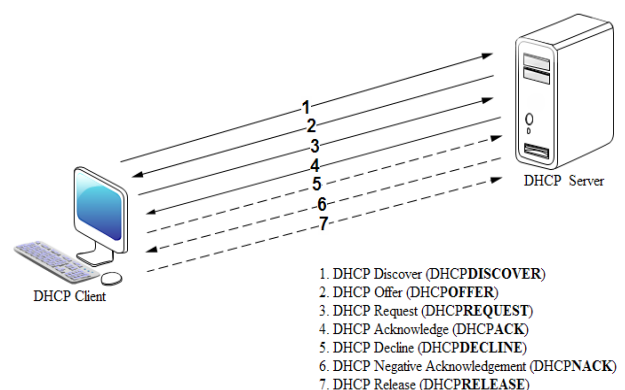
Increase in the number of end devices makes the network susceptible to Denial of Service (DoS) attack. It is one forms of the attacks triggered by attacker to prevent services to legitimate users by bottlenecking or disabling the respective resources and infrastructures[2]. As a precaution, most of the corporates perform Media Access Control (MAC) addresses registration to join new client machines to their network which is not enough to prevent DoS attacks on a DHCP server. The detail operation of DHCP and its DoS attacks are explained below in the upcoming sections.

### DHCP

DHCP is one of the standardized protocols used to provide IP addresses on lease basis as stated earlier. It is quite advanced in term of flexibility and reliability than other protocols such as RARP and BOOTP. When a machine is connected to a network, it requires four pieces of information to transmit data over the network. The four pieces of information are client IP address, its subnet mask, default gateway IP address and DNS server IP address [1]. DHCP server provides the above four information at a single step where BOOTP server takes

two steps to provide these information during machine boot configuration process.

DHCP server can operate in a network or multiple networks. In a network, both server and client carry same network address and server is associated with one scope of IP address pool. In a multiple network, DHCP server and client may or may not be in the same network and DHCP server associated with multiple scopes of IP address pool. If server and client are different network apart, client's first message to server is a broadcast message which is blocked by gateway during IP address negotiation. To prevent such situation, relay agent is configured in the client network which encapsulates client broadcast message in a unicast message and sends to the server. DHCP server uses well known port 67 to listen or reply a client messages. DHCP client uses well known port number 68, socket address (process ID and ephemeral port no) or socket address with transaction ID based on the network configuration. The set of messages exchanged between client and server are explained below and shown in Figure-1.



**Figure-1.** DHCP operation in client-server architecture.

The above figure shows the types of messages flow between a DHCP client and a DHCP server during IP address negotiation. Solid arrow marks indicate flows of the corresponding messages are compulsory in each IP



negotiation whereas dotted arrow marks indicate flow of either one of the corresponding messages or none of these during each IP negotiation.

### Types of DHCP Messages

- a) **DHCP discover:** It is a broadcast message sent by the client to its network when it starts booting. It indicates the requirement of IP address for active participation in network transmission. DHCP server captures this packet and goes for further processing while other hosts inside the network just discard the message.
- b) **DHCP offer:** Reply to DHCP Discover message, it is the message sent by the server which includes an IP address and its lease duration. Client accepts it by goes on sending DHCP Request message. If DHCP Offer message is not received, it sends DHCP Discover message four times before it will go to sleep and does it again.
- c) **DHCP request:** To confirm the binding between a client MAC address and its offered IP address, DHCP Request message is sent by the client reply to DHCP Offer message. Server will go on binding the client physical address with corresponding requested IP address after receiving this message.
- d) **DHCP decline:** Special case, this is the message sent by a client to DHCP server in response to DHCP Acknowledgement message. If client finds the offered DHCP parameters are invalid or already used by a host inside the network, it sends DHCP Decline to the server. Then both client and server go for IP address negotiation from the beginning with a minimum gap of ten seconds to avoid traffic.
- e) **DHCP acknowledgement:** Successfully binding between a client MAC address and its offered IP address at the server side is notified through DHCP acknowledgement message to client. After receive of this message, client gets the ownership IP address for certain period of time (lease period). Requirement of this IP address for a longer period of time demands exchange of both DHCP Request and DHCP Acknowledgement messages between client and server before expiration of each lease period.
- f) **DHCP negative acknowledgement:** Lease expiration before generation of DHCP Acknowledgement messages is informed through DHCP Negative Acknowledgement packet. If a client receives this message, it will go for a new IP address negotiation by sending DHCP Discover message again.

- g) **DHCP release:** No more requirement of IP address is intimated to DHCP server by DHCP Release message. When a client machine is shutdown or disconnected from a network, this message is sent by the client to server. So that IP address depletion is avoided by utilization of IP address pool by the server efficiently.

### DHCP DoS attack

In network, numerous types of attacks launched by attackers to exploit vulnerabilities of victims are called network threats. These are mainly classified into six types such as social, service abuse, eavesdropping, interception and modification, DoS and physical access threats[3]. DoS attack is one of the biggest network threats used by the attacker to block the information exchange between victim and legitimate users by overwhelming the network resources or by disabling those. DDoS attack is same as DoS attack but a large number of systems are involved to perform this operation. Some of the DoS attacks are SYN flood, ICMP flood, ping of death, Smurf, Teardrop, Fraggle, Land and service request flood etc. [2]. These attacks can be mitigated by applying private security policies or data mining based techniques [4], [5].

DHCP DoS attack is one of the service request attack is used to target DHCP server. It is launched either by flooding DHCP server with massive amount of DHCP message or by planting a rogue DHCP server inside the network. In the first case, a number of legitimate IP addresses are used by attacker to bottleneck DHCP server IP pool. When a client sends a DHCP discover message to server, server sends a DHCP offer message and lock down the corresponding IP address in response as discussed in section 2.1. A certain number of DHCP discover and offer messages at a particular time interval makes all the IP address locked down. As a result, server drops the DHCP discover messages from legitimate clients, causes DHCP flood attack [6]. It is prevented by authentication of a machine MAC address to join it in a network.

Registration of a machine MAC address is not enough to prevent DHCP DoS attack. In the second case, a registered MAC address is used to plant rogue DHCP server to execute this offence which is discussed in the next section.

### ATTACK MODEL

To perform this DHCP DoS attack, a registered client machine is used to plant DHCP server by installing it on a Virtual Machine (VM). Virtual machine is an instance or emulation of physical system which is running an OS on the top of physical system [7]. The virtual machine running a server OS is treated as guest server. Host uses OS to carry and run virtual machines on the top of it is known as host OS. Hypervisor is a piece of software is used to isolate host OS from the virtual machine OS which makes multiple OS(s) are running in a single system. Hypervisors are mainly of two types (Type-1 and Type-2). Type-1 hypervisor is also called bare metal or native hypervisor. It runs directly on the top of machine



hardware whereas the Type-2 hypervisor requires an OS, on the top of which it will run [8].

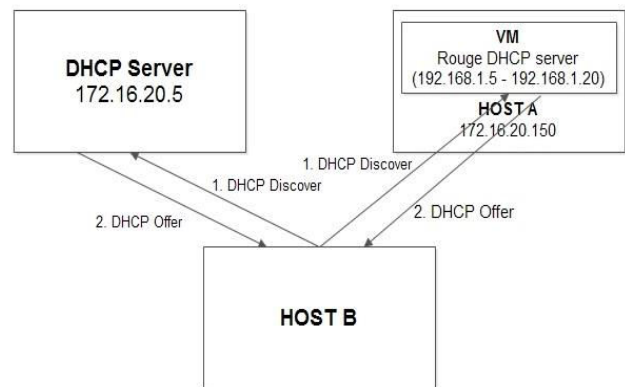
Virtual machine's network adapter inside host will be configured to make it accessible to different networks such as virtual machines' network in a single system, virtual machines-host network in a single system or host network (public network). Different types of network connections used by VM network adapter to customize its network are external/ bridged, internal, NAT and private/ host-only[9]. Virtual machine configured with external network adapter makes it getting an IP address from the host network which is treated as a system inside the public network virtually.

A Type-2 hypervisor with any number of guest server operating systems are configured with external network adapter to access internet services. By connecting a VM to internet, it not only gets a host network IP address but also goes on undetected due to its unique identification (dynamic MAC address). Virtual machine configured with server OS and bridged/external networking is used to launch the DHCP DoS attack as discussed below.

#### Steps

- First, Type-2 hypervisor is installed on a MAC address registered client machine having active internet connection.
- A VM is created on top of the hypervisor which will run any server OS.
- DHCP server is installed and configured on a server operating system VM.
- VM network adapter will be set to bridged type network connection.
- At last, internet connection to the host machine is checked because that client machine is one of the victims to be affected by the DHCP DoS attack.

As explained in the section DHCP, machines send DHCP Discover message during its boot up or after expiration of its lease timer. DHCP Discover message is a broadcast message. In response to this message, DHCP server sends an Offer message. Suppose the rogue DHCP server planted by an attacker receives the Discover message before the authorized DHCP server, it replies with a DHCP Offer message which causes acquisition of an IP address different from actual IP address later. This is possible due to existence of random delay in network. Machines near to the rogue DHCP server are mostly affected by this DoS attack.



**Figure-2.** DHCP messages flow from and to newly joined client.

As shown above, when a new client (HOST B) joins to network, it broadcast DHCP Discover packets to its network. Presence of the DHCP server and the rogue DHCP server inside network capture DHCP Discover message and send DHCP Offer messages in response. HOST B closeness to the rogue DHCP server or network delay between HOST B and the real DHCP server makes it accept the rogue DHCP Offer message. Acquiring a bad IP address puts HOST B in DoS zone.

#### RESULTS

In this experiment setup, VMWare Workstation 12 and Windows server 2012 R2 are used as Type-2 hypervisor and VM operating system respectively. Both are running on top of the host operating system Windows server 2012 R2. After installation of DHCP server on the VM, virtual network adapter is set to bridged networking. It can be performed in Linux environment by using any Linux server OS and VMWare Workstation.

```

Connection-specific DNS Suffix . : XXXXXXXXXXXXX
Link-local IPv6 Address . . . . . : fe80::b813:8746:83c0:6ccf%12
IPv4 Address. . . . . : 172.16.20.111
Subnet Mask . . . . . : 255.255.252.0
Default Gateway . . . . . : 172.16.20.1
  
```

**Figure-3.** IP Configuration in a client machine.

IP configuration of one of the client machines having active internet connection and 172.16.20.111/22 is the system IP address before DoS attack as shown in Figure-3.

DHCP	Start IP Address	End IP Address
WIN-OAPIUB66B58.vspeaker.com	192.168.1.5	192.168.1.20
IPV4	192.168.1.15	192.168.1.20
Scope [192.168.1.0] vspeaker.com		

**Figure-4.** IP address pool of rogue DHCP server.

IP address pool of a rogue DHCP server running in a virtual machine is shown in Figure-4. Scope [192.168.1.0] vspeaker.com indicates IP address pool belongs to 192.168.1.0/24 network address.



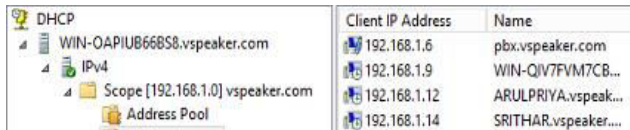
```

Connection-specific DNS Suffix . : vspeaker.com
Link-local IPv6 Address . . . . . : fe80::b813:8746:83c0:6ccf%12
IPv4 Address. . . . . : 192.168.1.9
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

```

Figure-5. DHCP DoS attack.

IP configuration of a client machine during DHCP DoS attack is shown in Figure-5. Its DNS suffix and IP address are changed to *vspeaker.com* and *192.168.1.9/24* respectively.



Client IP Address	Name
192.168.1.6	pbx.vspeaker.com
192.168.1.9	WIN-QIV7FVM7CB...
192.168.1.12	ARULPRIYA.vspeak...
192.168.1.14	SRITHAR.vspeaker....

Figure-6. IP addresses of some of the victims of DHCP DoS attack.

Figure-6 shows IP addresses of some of the victims is depicted by the DHCP DoS attack and their network address is changed from *172.16.20.0/22* to *192.168.1.0/24* network.

## COUNTER MEASURE

DHCP DoS attack can be prevented by proper authorization and configuration of client machines and network components inside a network. One possible solution is to perform MAC address authentication before IP address negotiation. It is not enough to prevent the attack as discussed in a previous section. This DHCP DoS attack can be checked by client's Active Directory service authentication and advanced switch configuration.

### Active directory

It is the directory database developed by Microsoft for centralized authentication and management of computer and user accounts in a particular domain. Computer and user accounts are the records in Active directory database which carries information about each computer and user in a domain. Each client with a user account is not only monitored but also it is prevented installation of softwares (DHCP) by Active directory's group policies [10].

### Switch configuration

In organizations, L2 and L3 switches are used to connect multiple machines in a single network or multiple sub networks (subnet). DHCP server uses port no 67 to send and receive DHCP messages to and from its clients. So, access control list must be configured at each interface to block port no 67 except the interfaces connected to DHCP server. In advance, specific ports are opened at switches which allow clients have access to certain services [11]. Sample codes to block port no 67 in port no 0-23 of a switch are given below:

```

Switch(config)#ip access-list extended BLOCK_DHCP
Switch(config-ext-nacl)#deny udp any any eq 67
Switch(config-ext-nacl)#allow any any

```

```

Switch(config-ext-nacl)#end
Switch(config)#interface gigabitEthernet 0/23
Switch(config-if)#ip access-group BLOCK_DHCP in
Switch(Config-if)#end

```

## CONCLUSIONS

DHCP is used for dynamic allotment of IP addresses to client machines on lease basis. Dynamic distribution of IP address does not only prevent address depletion issue but also offers its proper management using DHCP server. Poor and inadequate network configurations open path for attackers to initiate attacks. This paper presents a way to execute a DHCP DoS attack and the counter measures to prevent it. Finally, in future more research has to be done to raise the level of security by reducing the vulnerabilities exist inside a network.

## REFERENCES

- [1] Forouzan B., A. 2010. Host Configuration: DHCP. TCP/IP Protocol Suite, 4th ed., New York: McGraw-Hill, 2010, pp. 568-581.
- [2] Graves K. 2010. Denial of Service and Session Hijacking. Certified Ethical Hacker Study Guide, 4th ed., Danvers, MA: Wiley. pp. 173-193.
- [3] Butcher, D., Li, X., and Guo, J. (2007). Security challenge and defense in VoIP infrastructures. IEEE Transactions on Systems, Man, and Cybernetics-Part C: Application and Reviews. 37(6): 1152-1162.
- [4] Le, D. (2014). D-DoS attack defense in next generation networks using private security policy. IAES International Journal of Information and Network Security, 3(3).
- [5] Waguih H. 2013. A data mining approach for the detection of denial of service attack. IAES International Journal of Artificial Intelligence. 2(12): 99-106.
- [6] Morgan D. Using the DHCP protocol for a denial-of-service attack.
- [7] Ruest D. and Ruset N. 2009. Begin the Five-Step Process. Virtualization: A Beginner's Guide, McGraw-Hill. pp. 13-43.
- [8] Obasuyi. G. and Sari A. 2015. Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment. IJCNS. 08(07): 260-273.
- [9] Davis D. 2013. Understanding Virtual Networking in VMware Workstation 9. VirtualizationAdmin.com, [Online]. Available: <http://www.virtualizationadmin.com>.



com/articles-tutorials/vmware-server-worksation-play-erarticles/understanding-virtual-networking-vmware-worksation-9.html. [Accessed: 18-Jun-2016].

- [10] M. Tulloch M. 2013. Active Directory. Introducing Windows Server 2012 R2 Technical Overview, 1<sup>st</sup> ed., WA: Microsoft. pp. 123-136.
- [11] Cisco. 2015. Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S, 1<sup>st</sup> ed. San Jose, CA: CISCO. pp. 1-218.