**Dynamic Host Configuration Protocol**

**Ruchita Chandramouli Bhonsle**

A20457994

**Network Admin and Operations – ITMO 541**

**Kevin Vaccaro**

Shape

Description automatically generated

Date: April 6, 2021

**Dynamic Host Configuration Protocol**

**Introduction**

The potentiality of devices to connect rapidly and effortlessly is critical in manic-connected world and despite existing for many years, DHCP remains to be important process to ensure to establish connection between the devices and network and thus maintain their configuration accurately.

DHCP diminishes flaws which occurs during manual allocation of the IP addresses and can expand the IP addresses by restricting how long a device can keep the IP address individually.

**DHCP definition**

In order to establish efficient communication between the hosts and other endpoints on the network, a network protocol is utilized on IP network platforms where DHCP server automatically assigns the IP address to hosts. Apart from IP address, DHCP also provides subnet mask, default gateway address, domain name server (DNS) address and other applicable configuration parameters.

**DHCP simplifies IP address management**

DHCP plays a significant role in management of IP on networks. As two hosts cannot have same IP address and its configuration done manually would lead to errors. Automating the process of assigning the IP address to the devices makes life much easier for users and administrators because of even the smallest network need allocation of IPs especially mobile devices which needs IP allocation not on permanent basis so manual allocation becomes more confusing.

**Components of DHCP**

To understand the working of DHCP it is important to know all the components involved in it.

List of components consists of:

DHCP server: A networked device which executes DHCP service responsible of having all the IP addresses and required configuration information. This could be anything that behaves like a host such as router, server or even SD-WAN appliance.

DHCP Client: This can be anything at receiving end which accepts the configuration information from DHCP server such as computer, mobile device, IoT endpoint or any devices whose basically needs to be connected to the network. These connected devices are configured by default to receive the information from DHCP server

IP address pool: This has the collection of addresses made available to DHCP client. Allocation of addresses are done in typically logical order of lowest to highest.

Subnets: When IP networks are divided into segments it is called subnets making the network more manageable.

Lease: The duration of time until which the DHCP client can hold the IP address information. When that duration gets over the client needs to renew it.

DHCP relay: This can router or any hosts that acknowledges the client's message of requesting for IP address that has been broadcasted on the network and takes it forward to configured server. The server then sends the response message to DHCP client via relay agent. This process occurs through centralized DHCP server rather than placing the server on each subnet.

**Advantages of DHCP servers**

Some of the benefits of DHCP servers are

Accuracy of IP configuration: DHCP server minimizes the typographical errors which is otherwise very tedious job to troubleshoot. When dealing with inputs such as 192.162.123.3 it is common to make the mistake therefore IP address configuration parameters needs to be accurately done.

Efficiency of change management: With DHCP it is easier to modify addresses, scopes and endpoints. For example, if IP addressing scheme needs to be changed in the organization from one range to another. The DHCP server is configured with new information and this information is sent across to all new endpoints. Likewise, if there is upgradation or replacement of network device, there wouldn't be any new configuration required.

Automating the IP address administration: In absence of DHCP, the revocation and allocation of IP addresses needs to be done manually by network admins. Tracking what device has which address is ineffective as it is actually impossible to know when device needs to be connected or disconnected from network. DHCP makes this automated and centralized so that all the locations can be managed by single endpoint by network professionals.

**DHCP poses security risks**

There is no process of authentication in DHCP protocol which allows the clients to entire the network quickly. This increases the probability of security risks, which includes unauthorized server providing inaccurate information to clients, unauthorized clients being allocated IP addresses and IP addresses getting deleted from malicious or unauthorized clients

Authenticity of DHCP server cannot be validated from client, the chances of rouge ones to provide incorrect information is high. Consequently, this can lead to denial-of-service attack or man in the middle attack through fake server intercepting the data which could be used for malicious purposes. In support of this type of attack DHCP server allocates the IP address to any type of device as it does not have the process of authentication. Attackers can configure the clients and change its credentials accordingly and use all the available IP address which results in avoiding the endpoints of the organization from accessing the network.

These are the some of the issues which are not focused by DHCP specification. Access to the network can be controlled by relay agent information option which notifies the engineer to tag the DHCP messages as it arrives the network. The authentication of DHCP messages is also possible but the key management becomes complex hence it is held as backup adoption. DHCP can be secured by Network access control (NAC) which is also known as 802.1X authentication. Leading network vendors use NAC as it is easier for implementation.

**Securing DHCP servers**

There are several measures in order to secure DHCP servers and clients. These measures can vary from surveilling the membership into DHCP administration group to performing specific DHCP service configuration. Specifying some of the measures:

Keeping default name registration behavior

When DHCP server provides the IP configuration information to DHCP client by default DHCP server registers the PTR resource record for the client simultaneously client registers its own A resource record. It is recommended to maintain this default behavior so that DHCP server can sustain the ownership of PTR resource record. Modification of this default behavior can lead to inaccurate DNS information if client changes the subnet and TCP/IP configuration information is provided by different DHCP servers which cannot change the DNS resource records.

Evaluating DHCP database for BAD\_ADDRESS entries

In DHCP database when IP address is registered as BAD\_ADDRESS, there could be strife with an already existing address on the network. This takes places when DHCP server assigns the IP address to DHCP client that is in use. After getting the IP address configuration information from DHCP server, DHCP client sends the address resolution protocol packet to confirm that IP address is not in use. If the client gets to know that IP address is in use, it informs the DHCP server which in return marks the reservation as BAD\_ADDRESS.

The leasing of BAD\_ADDRESS can take place under different scenarios. If the overlapping of DHCP scopes DHCP servers where two DHCP servers assigns the same IP address and when DHCP client claims the IP address to be in use, the second DHCP server marks that IP address as BAD\_ADDRESS. Another scenario to consider when threat vectors can allocate multiple static address to one computer. If those address are allocated by DHCP server and when DHCP client sends ARP and gets to know that IP is in use then DHCP client refuses the offered-IP address from DHCP server.

DHCP auditing should be enabled

For keeping the track of which DHCP server assigns the IP address to which DHCP client and from where BAD\_ADDRESS entries are emerged, this can be achieved through enabling the DHCP auditing. By enabling the enable DHCP auditing logging option in the properties of DHCP server in DHCP console. Daily log files of DHCP service are provided through this option which can be found in folder: %windir%\system32\dhcp. Apart from enabling DHCP auditing in DHCP console, we can define the maximum size of DHCP log file by adjusting the HKLM\SYSTEM\CurrentControlSet\Services\DhcpServer\Parameters\DhcpLogFilesMaxSize registry entry

Membership of DHCP Administrators group needs to be monitored

DHCP administrators group members are given the permission to configure DHCP servers. These administrators are responsible for generating DHCP scopes and DHCP reservation and determining the DHCP configuration options.

Closely keeping the track of membership in the DHCP Administrators group, membership in the local Administrators group, the Domain Admins group, and the Enterprise Admins group to find out who has the required permissions to manage DHCP services. Membership in these groups allows management of all DHCP servers in the domain.

A member of the DHCP Administrators group cannot authorize a DHCP server in Active Directory. Only members of the Enterprise Admins group can perform this task. You can delegate the right to authorize DHCP servers by following the solution proposed in Knowledge Base article 239004, How to Allow Non-Root or Enterprise Administrators to Authorize RIS Servers in Active Directory.

Listing out some of basic security measures DHCP servers are

* Protecting DHCP servers physically
* To secure the data of system volume utilization of NTFS file system should be done.
* Implementation and maintenance of strong anti-virus solution
* Ensuring that DHCP servers are located behind firewall
* All open unused ports need to enclosed
* Updating the software patches
* DHCP traffic can be further secured by utilizing VPN tunnel
* Least number of privileges needs to be granted for performing administrative tasks on DHCP servers
* Programs and software should be installed or implemented from trusted sources only
* All applications and programs need to be terminated or uninstalled when it is not used on DHCP servers
* Filtering of MAC address can be done
* DHCP activity needs to be regularly monitored by reviewing DHCP logs and keeping the track of statistical information on DHCP servers

To Enhance to security of DHCP servers on Window 2003, following measures can be implemented:

Computer is forced by secure updates to be authenticated in Active Directory before it reaches DHCP server for obtaining IP addresses.

In windows2000 DHCP server or windows 2003 DHCP server DHCP authorization makes sure to these servers are authorized in Active Directory before it starts functioning in the network platform.

**Backing up and restoring DHCP database**

To recover the lost and corrupted DHCP database it is important to back the DHCP database on DHCP server. The entire content of DHCP database on DHCP server is backed up if backing up database has been done.

The process of manually backing up DHCP database is as follows

After clicking start button, there would be administrative tool options where DHCP and DHCP console would appear. Right clicking the DHCP server where DHCP database would appear which needs to be backed up. Then selecting backup option from shortcut menu.

Then browser for folder dialog box opens, selecting particular folder for DHCP database should be backed up. Confirming this with OK.

Restoring DHCP database

After clicking start, administrative tool appears where DHCP tab has option of DHCP management console. Then right click on DHCP server for which DHCP database needs to be restored and selecting restore option from shortcut menu. Then browser for folder dialog box opens, selecting particular folder for DHCP database should be restored.

**DHCP Starvation Attack**

This malicious digital attack targets DHCP servers. Through this attack combative actors sends bogus DISCOVER packets to DHCP servers until it drains out all available IP addresses. Once that takes place attackers can reject the authorized device’s IP address request or even direct them to fake DHCP connection which can lead to Man-in the middle Attack

**DHCP spoofing attack**

Once a DHCP starvation attack and a malicious DHCP server are set up, attackers can begin distributing IP addresses and other TCP / IP configuration settings to DHCP clients on the network. TCP / IP configuration settings including the default gateway IP address and DNS servers. Network attackers can now replace the legitimate real IP addresses of the standard gateways and the IP addresses of DNS servers with their own IP addresses.

After the IP address of the network device default gateway is changed, the network client sends external network traffic to the attacking computer. Attackers can now capture sensitive user data and launch "middleman" attacks. This is known as a DHCP spoofing attack. Attackers can also set up malicious DNS servers and redirect end-user traffic to spoof websites and launch phishing attacks.

**How does a DHCP starvation attack work?**

In a DHCP starvation attack, the hostile actor sends many fake DISCOVER packets until the DHCP server is sure it has used the available pool. Customers looking for an IP address find they do not have an IP address and service is denied. In addition, they may be looking for other DHCP servers that the enemy actor can provide. And using a hostile or fictitious IP address, that hostile actor can now read all traffic a subscriber sends and receives.

In a hostile environment where a malicious computer is running a tool like Yersinia, there may be a computer sending a DHCP DISCOVER packet. This malicious client doesn't send a handful - it sends hundreds and hundreds of malicious DISCOVER packets, using a fake and fictitious MAC address as the source MAC address for each request.

If the DHCP server replies to each of these fake DHCP DISCOVER packets, the entire pool of IP addresses may be exhausted and this DHCP server may think that there are no more IP addresses left to offer valid DHCP requests.

Since DHCP servers no longer have IP addresses to offer, attackers will usually have to enter their next DHCP server. This rogue DHCP server then distributes the IP addresses.

For attackers, it has the advantage that clients using this IP address and using this default gateway can now be routed through the attacker's computer if the fake DHCP server distributes the IP address including DNS information. That was all it took for an enemy actor to carry out a "Middle Man" (MITM) attack.

**Protection against DHCP starvation attack**

Configure the following interface to reduce DHCP starvation attacks that use DHCP packets packaged with a different source MAC address:

Run the mac-address max-mac-count command to set the MAC training limit. For more information on these commands, disable unknown frame forwarding when the MAC training limit is reached.

To prevent DHCP starvation attacks that use DHCP requests packaged with the same source MAC address, you can enable MAC address verification on the DHCP server. The DHCP server compares the chaddr field of received DHCP requests with the source MAC address in the frame header. If they are the same, the DHCP server will verify that the request is valid and process it. If they are not the same, the server rejects the DHCP request.

**Some of the best DHCP practices are**:

**Running DHCP best practice analyzer**

Best practice analyzer is tool found in windows server and it is found in server management tool which is capable of verifying DHCP configuration against Microsoft guidelines.

**Documentation of IP addresses or using IP addresses management tool (IPAM)**

For small scale organization’s network excel sheet should be sufficient for tracking IP scheme’s VLANs and static IP assignments. For larger network IP address management tool is recommended which can automate IP address tracking, alert and report the scope usage and can quickly search for IP addresses, comments and hostnames.

**Utilizing DHCP failover**

To have greater availability of the DHCP server DHCP failover feature can be used. Where two DHCP servers share DHCP information so that if one DHCP server goes down other one can provide the client with required information so that service is not compromised. DHCP failover is built in option available in Windows server operating systems. There are two types of failover design one is hot standby design and other is load balance design.

**DHCP lease duration tips**

Tip 1- To increase the lease time for fixed devices: In smaller network lease time could be set for 8 hours by default whereas in larger networks workstations do not move that often so their time period could be set for 16 days of DHCP scopes so that they don’t go through entire DHCP process just to obtain the IP address eventually helps in decrease of network traffic associated with DHCP

Tip 2- decrease the lease time for guest/ wireless devices: For these devices lease time should be provided for 1 hour as they would need temporary access for just few hours because if we provide guest Wi-Fi with DHCP scopes it will get exhausted of all available IPs quickly.

**DHCP MAC address filtering**

This is one of the features which assists in either blocking or allowing IP address allocation based on MAC address. This is advantageous if DHCP scopes needs to assign IP addresses to explicit group of devices. Simultaneously becomes useful to know unwanted devices on VLAN accessing the IP address.

**Setting DHCP server options**

DHCP options can be configured at two different levels one at server or per each DHCP scope. And it additionally helps in auto configuring TCP/IP setting on client devices.

The most common options used are:

003 router

006 DNS server

015 DNS domain name

**Subnetting and network segmentation**

Advantages of network segmentation

From security point of view by keeping the devices in different network helps in having better control over the network. Limitation of later movement in the network helps in preventing attackers and viruses.

Helps in improving the network performance: Deploying all the devices in the one big network will increase the size of broadcast domain which can lead to issues like spanning tree loops, broadcast and multicast storms. Dividing the network will help in separating the broadcast domains.

Control visitor/guest access: Separating guest network traffic from accessing private network traffic which can be filtered and block the access to internal network.

**Learn PowerShell DHCP commands**

PowerShell makes the tasks easier to perform in larger network which has thousands of DHCP scopes, and it is time saving as well.

Some of the PowerShell commands are

Installing DHCP role: Install-WindowsFeature -IncludeManagementTools DHCP

Monitor DHCP lease: Get-DhcpServerv4Scope | Get-DhcpServerv4Lease

Backing up DHCP server: Backup-DhcpServer -ComputerName "dhcp1.ad.activedirectorypro.com" -Path "C:\Windows\system32\dhcp\backup"

DHCP lease from MAC address: Get-DhcpServerv4Scope |Get-DhcpServerv4Lease |where {$\_.ClientId -like “b4-b6-86-b4-\*\*-\*\*” }

Addition of DHCP scope: Add-DHCPServerv4Scope -EndRange 10.2.1.254 -Name Vlan110 -StartRange 10.2.1.1 -SubnetMask 255.255.255.0 -State Active

Getting all DHCP reservations for a scope: Get-DHCPServerv4Lease -ScopeId 10.2.1.0

Getting all IPv4 scopes: Get-DHCPServerv4Scope

Creating DHCP reservation: Get-DhcpServerv4Lease -ComputerName dhcpserver1 -IPAddress 10.2.1.8 | Add-DhcpServerv4Reservation -ComputerName server1

**Conclusion**

It is known fact that through DHCP network managers have saved time, money and made their network environment more powerful and flexible. DHCP has ranged from being simple tool for allocation of IP addresses to link-local interfaces to different aspects or phases of networking tool thus helping in maintaining irreplaceable large-scale networks. Allocation and de-allocation of IP addresses is possible due to relay agents and DHCP servers across the world. As changes in network architecture along with their possible capabilities, DHCP has also evolved significantly alongside them by providing more automation in assigning the IP address and enhancing the speed of renewing lease to nodes. Along with IPv6 capabilities DHCP abilities also plays an important role in increasing the access to multiple nodes at single time. We can wind up from this by considering that even though DHCP is integral part of internet, it still needs to evolve and become more advanced for maintaining its coexistence along with constantly changing networking world.

**Bibliography**

Kerravala, Z. (2018, August 21). *Dynamic host configuration protocol simplifies and improves the accuracy of IP addressing but can raise security concerns*. NETWORKWORLD. <https://www.networkworld.com/article/3299438/dhcp-defined-and-how-it-works.html>

Allen, R. (2020). *Top 16 DHCP Best Practices: The Ultimate Guide*. Active Directory Pro. <https://activedirectorypro.com/dhcp-best-practices/#powershell-dhcp>

Heintzkill, R. (2020). *What is a DHCP Starvation Attack?* CBTNuggets. <https://www.cbtnuggets.com/blog/technology/networking/what-is-a-dhcp-starvation-attack>

*DHCP Security*. (2019). Softpanorama. <http://www.softpanorama.org/Net/Application_layer/DHCP/dhcp_security.shtml>

*Securing DHCP Servers*. (2012). Securing DHCP Servers. <https://www.tech-faq.com/securing-dhcp-servers.html>