REAL-WORLD APPLICATIONS OF DYNAMIC HOST CONTROL PROTOCOL AND SPANNING TREE PROTOCOL

Crystal Li
Team 03, CS330 – Network Communications, School of Technology and Computing, City University of Seattle

Nicole Hessner
Team 03, CS330 – Network Communications, Masters of Science in Computer Science, School of Technology and Computing, City University of Seattle

Tessa Shippley
Team 03, CS330 – Network Communications, Bachelors of Cybersecurity, School of Technology and Computing, City University of Seattle

Gayatri Soni
Team 03, CS330 – Network Communications, Masters of Science in Computer Science, School of Technology and Computing, City University of Seattle

licrystal2@cityuniversity.edu, hessnernicole@cityuniversity.edu, shippleytessa@cityuniversity.edu, sonigayatri@cityuniversity.edu

Abstract

The Open Systems Interconnection (OSI) Model is a near-ubiquitous though-model for network communications. Its seven layers are generally presented in reverse order: (7) application, (6) presentation, (5) session, (4) transport, (3) network, (2) datalink, and (1) physical. In this paper, we explore Dynamic Host Control Protocol and Spanning Tree Protocol, examining how each protocol is used and in what cases each protocol is most useful. We also examine potential cybersecurity attacks that target and exploit Spanning Tree Protocol. Finally, we show examples of where DHCP and STP data are found in real-world packets using Wireshark, a packet analyzer.

Keywords: OSI model, data-link layer, packet analysis, cybersecurity, Spanning Tree Protocol (STP), Dynamic Host Configuration Protocol (DHCP)

1 INTRODUCTION

Dynamic Host Configuration (DHCP) and Spanning Tree Protocols (STP) are key components in efficient network functionality. With DHCP networks are able to dynamically allocate IP addresses to avoid duplicate IP addresses that could cause conflicts. STP is a protocol that is designed to keep packets flowing through a network and minimize the possibility of looping traffic that could cause the network to

become flooded and reduce the available bandwidth. Using Wireshark, it is possible to look at the packets sent by each of these protocols and see what is sent by the source and destination.

2 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to a new device, or node, on a network so they can communicate using IP (Internet Protocol). DHCP automates and centrally manages these configurations. There is no need to manually assign IP addresses to new devices. Therefore, there is no requirement for any user configuration to connect to a DHCP based network.

DHCP can be implemented on local networks as well as large enterprise networks. DHCP is the default protocol used by most routers and networking equipment. DHCP is also called RFC (Request for comments) 2131.

2.1 DHCP Protocol Definitions

- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- DHCP maintains the unique IP address of the host using a DHCP server.
- It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.

DHCP is also used to configure the proper subnet mask, default gateway and DNS server information on the node or device.

There are many versions of DCHP that are available for use in IPV4 (Internet Protocol Version 4) and IPV6 (Internet Protocol Version 6).

2.2 DHCP Functional Description

DHCP runs at the application layer of the TCP/IP protocol stack to dynamically assign IP addresses to DHCP clients/nodes and to allocate TCP/IP configuration information to the DHCP clients. Information includes subnet mask information, default gateway, IP addresses and domain name system addresses.

DHCP is based on client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools.

2.2.1 DHCP Lease Process

- First of all, a client (network device) must be connected to the internet.
- DHCP clients request an IP address. Typically, clients broadcast a query for this information.
- DHCP server responds to the client request by providing IP server address and other configuration information. This configuration information also includes a time period, called a lease, for which the allocation is valid.

When refreshing an assignment, DHCP clients request the same parameters, but the DHCP server may assign a new IP address. This is based on the policies set by the administrator.

2.3 Components of DHCP

When working with DHCP, it is important to understand all the components. Following is the list of components:

- **DHCP Server:** DHCP server is a networked device running the DCHP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.
- **DHCP client:** DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like a computer, laptop, IoT endpoint or anything else that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.
- **IP address pool:** IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.
- **Subnet:** Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.
- **Lease:** Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client has to renew it.
- **DHCP relay:** A host or router that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. DHCP relay can be used to centralize DHCP servers instead of having a server on each subnet.

2.4 Benefits of DHCP

There are the following benefits of DHCP:

Centralized administration of IP configuration:
DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.

Dynamic host configuration:
DHCP automates the host configuration process and eliminates the need to manually configure individual host. When TCP/IP (Transmission control protocol/Internet protocol) is first deployed or when IP infrastructure changes are required.

Seamless IP host configuration:
The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway, IP address of DND server and so on without user intervention.

Flexibility and scalability:
Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily and change IP configuration when the infrastructure changes.

Reduced IP address conflicts:
Each connected device must have an IP address. However, each address can only be used once, and a duplicate address will result in a conflict where one or both devices cannot be connected. This can happen when addresses are assigned manually, particularly when there are many endpoints that only connect periodically, such as mobile devices. The use of DHCP ensures that each address is only used once.

Efficient change management:
The use of DHCP makes it very simple to change addresses, scopes, or endpoints. For example, an organization may want to change its IP addressing scheme from one range to another. The DHCP server is configured with the new information and the information will be propagated to the new endpoints. Similarly, if a network device is upgraded and replaced, no network configuration is required.

2.5 DHCP Usage Scenarios

There are four key DHCP usage scenarios: 1. Initial Client Connection: the client requests from the DHCP server an IP address and other parameter values for accessing network services 2. IP Usage Extension: the client contacts the DHCP server to extend usage of its current IP address 3. Client Connection After Reboot: the client contacts the DHCP server for confirmation that it can use the same IP address being used before reboot 4. Client Disconnection: the client requests the DHCP server to release its IP address.

We will Consider DHCP if we have:

- Many remote dial-up users
- Users who move from network to network
- A large network where management of addresses at the desktop level is difficult or inconvenient
- More potential users than you have addresses
- Frequent network changes

DHCP is not the best choice for:

- Routers, servers, printers, and other systems that need static addresses
- Sites where there are plenty of available addresses
- Sites where addresses do not change frequently

2.6 Network Criticality of DHCP

DHCP is important to all classes of IPv4 network. Since we have a limited number of addresses per subnet, and not every user requires IP addresses on a non-permanent basis, DHCP allows any given network to support more users than available addresses through IP address leasing. Moreover, DHCP is critical to small networks where mobile devices are used. DHCP lease management stops communication with IP addresses at expiration. Clients connected to the network can renew their lease halfway through the lease period.

DHCP offers many advantages over static IP addresses. Manually assigning IP addresses to every device can be burdensome and it is prone to errors. DHCP assigns IP addresses dynamically eliminates duplicate IP addresses conflict (IBe, 2018). Not only IP addresses, DHCP configures default gateway, subnet mask, Domain Name Server and other relevant networking parameters automatically. DHCP relay agent can forward initial DHCP messages thereby eliminates the need for a DHCP server on every subnet.

3. SPANNING TREE PROTOCOL

Spanning Tree Protocol (STP) is a "loop-free protocol", meaning that its purpose is to prevent data packets from being forwarded in a circle around several interconnected switches of a network indefinitely. Since Ethernet frames do

not have a Time to Live field, this is very important for preventing broadcast packets from taking up unnecessary bandwidth within the network. STP assigns machines in a network one of three port roles: root, non-root, and blocked (Spanning Tree Protocol (STP) Overview, 2021). Each machine encountered during the packet broadcast has a Bridge Protocol Data Unit (BDPU), which is not forwarded in the packet stream, but contains information which is used to determine forwarding priority within the network. Each time a device is added to the network, a Topology Change Notification (TCN) instructs the existing devices that their forwarding tables should be overwritten, as port roles and shortest routing paths may have changed (Techopedia, 2012).

The two pieces of information that determine a machine's forwarding status are its MAC address and its assigned priority. Assuming all machines share the same priority, which has a default value of 32,768, the machine with the lowest MAC address will have the lowest Bridge ID and will be assigned the root role, becoming the Root Bridge. The Root Bridge is always in forwarding mode; any packet received in a broadcast will be forwarded. Non-root ports will forward packets along the lowest cost path, which is determined by properties such as bandwidth and number of hops between switches. Finally, the port with the highest Bridge ID will be a non-designated port and will be in blocking mode. The non-designated ports are the means by which STP establishes a loop-free topology (Networklessons.com, 2017).

I3.2 Vulnerabilities of Spanning Tree Protocol

After gaining access to a network, it could be possible to add a new device that can act as an STP device. If the device is set up with a lower priority number than the other STP devices, it would be able to be elected to be the root. The root device has all the cross-network communications routed through it. With the new device set to the root it can intercept communications and adjust the routing to flood the network. Another possibility would be to get access to the administrator account. It would be possible to edit the STP settings to redirect the flow of communications to flood the network with endless looping data.

Using Bridge Protocol Data Units (BPDUs) created of a non-existent switch with an ID of 1 it is possible to elect the non-existent switch to be the root bridge. Sending more BPDUs outside of the time frame for the max-age of the packets will cause the network to perform another root bridge election. Each time an election is made there is an influx of broadcast or multicast traffic trying to get new routing information. By repeating the process, the network will constantly be in a state of reelection causing a massive flood of packets over the network.

4. DHCP IN PACKET ANALYSIS

Figure 1 shows both the DHCP Release process and the four stages of DHCP Renewal. At 11.789870 seconds, the ipconfig command to release the current IP address is given. Then, the Discover, Offer, Request, Acknowledgement phase begins when the ipconfig command is given to renew the IP. This is shown by packets 47 and 259 having a source IP address of 0.0.0.0, since the IP address of the host has already been released. Then, the IP address 192.168.1.248 is offered again, requested, and then accepted with the ACK message.

Figures 2-6 display examples of packets captured by Wireshark showing examples of the data sent in each type of DHCP message for each step of the IP lease renewal process.

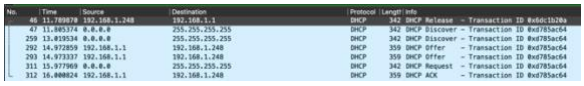

Figure 1. List of DHCP packets captured in Wireshark during DHCP release/renewal process.

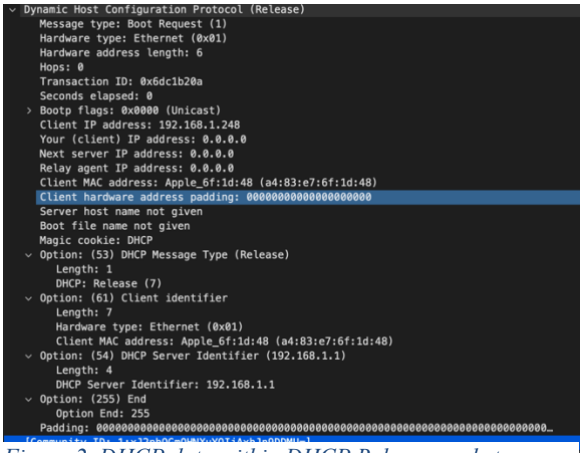

Figure 2. DHCP data within DHCP Release packet, including expanded Options.

As shown in Figure 2, the Release frame contains information such as the current client IP address (which is 0.0.0.0), and other fields that no longer have values, because the client's association with the DNS server has been severed.

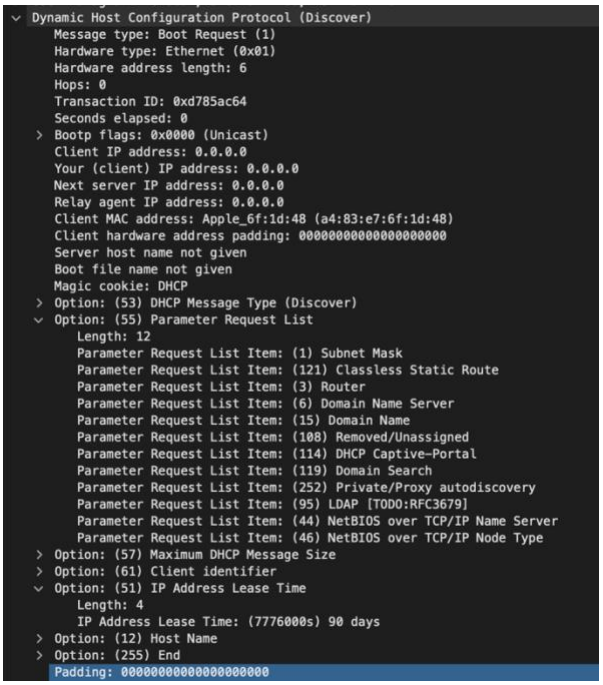

Figure 4. DHCP Discover packet with expanded Parameter Request List and IP Address Lease Time.

Figure 3 shows the DHCP Discover packet, with an expanded parameter request list. The requested parameters include a Subnet Mask, Classless Static Route, Router, Domain Name Server, Domain Name, Recovered/Unassigned, DHCP Captive-Portal, Domain Search, Private/Proxy autodiscovery, LDAP [T0D0:RFC3679], Net BIOS over TCP/IP Name Server, and NetBIOS over TCP/IP Node Type.

The Offer packet, shown in Figure 4, includes options for IP Address lease time. The primary feature of Figure 4, however, is that it indicates that the client has made contact with the DNS server, and the DNS server has an IP address available to offer to the client.

The Figure 5 Request frame shows that the client still does not have an association with the DNS server. The main feature of the Request frame is that it contains an Option field for a Parameter

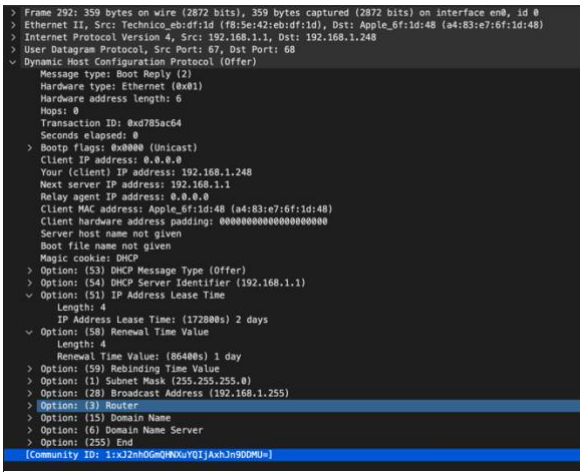

Figure 3. DHCP Offer packet.

Request List. Our DHCP frame from the live packet capture shows that the options requested included common configuration features such as a Subnet Mask, Router, Domain Name Server, and Domain Name. There are also replies to all of the requested parameters from the DHCP Discover packet in figure 3.

Finally, the ACK packet in Figure 6 acknowledges that the IP address that was offered by the DNS server was accepted and will be used from this point forward.

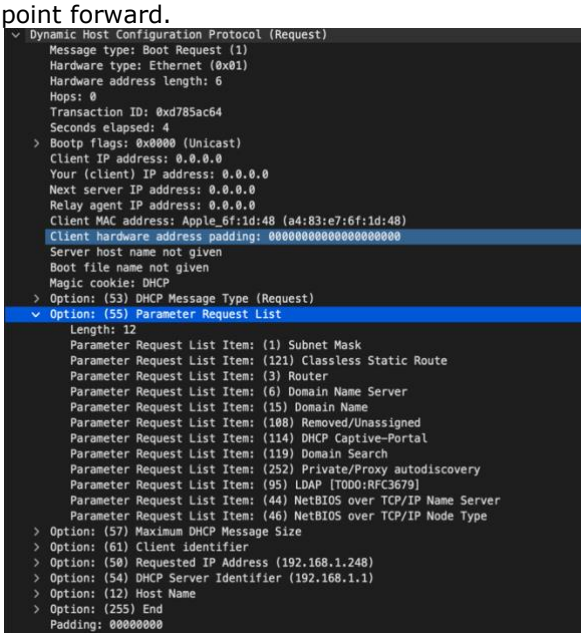

Figure 5 DHCP Request packet.

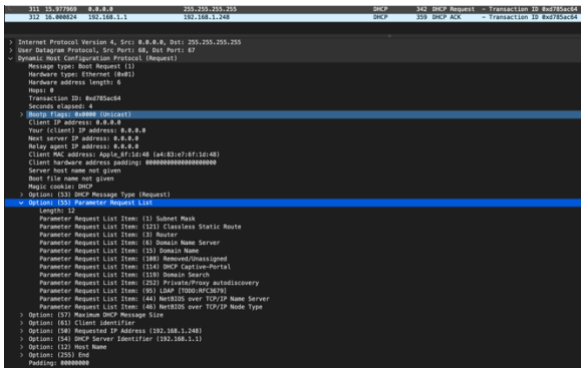

Figure 6. DHCP ACK packet.

5. CONCLUSION

DHCP is easily scalable and when configured properly can make the addition of new devices to a network very simple to do. STP can prevent endless looping data streams that could clog the network leading to longer transmission times and possible network failures. Each of these protocols are very useful for keeping networks running smoothly as new devices are added and old ones are removed.

6. REFERENCES

Cisco Systems. (2017, December 5). STP Problems and Related Design Considerations. https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10556-16.html

DHCP defined and how it works. (March 14, 2022). Networkworld.com. https://www.networkworld.com/article/3299438/dhcp-defined-and-how-it-works.html

Ibe, Oliver C. (2018). Fundamentals of Telecommunication Networks. Wiley.

Microsoft Doc, Dynamic Host Configuration Protocol (DHCP), July 29, 2021 retrieved on February 24, 2022 from https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top

Networklessons.com. (2017, November 1). Introduction to Spanning-Tree [Video]. YouTube. https://www.youtube.com/watch?v=wOsbtA4Hx04

Spanning Tree Protocol (STP) Overview. (2021, October 22). Cisco Meraki. https://documentation.meraki.com/MS/Port_and_VLAN_Configuration/Spanning_Tree_Protocol_(STP)_Overview

Techopedia. (2012, June 7). Bridge Protocol Data Unit (BPDU). Techopedia.Com. Retrieved March 20, 2022, from https://www.techopedia.com/definition/793/bridge-protocol-data-unit-bps and a

Tomicki, Lukasz. (2020, September 9). *Attacking the Spanning-Tree Protocol.* https://www.tomicki.net/attacking.stp.php