Project 1 – DNS and Basic Tools

CIIC 4070 – Computer Networks

Alberto I. Cruz Salamán

802-18-0591

Prof. Kejie Lu

Computer Science and Engineering

Table of Contents:

I. Introduction

This paper is a project for the CIIC 4070 course at UPRM. It will expand upon the research of the student surrounding the topics and questions prompted by the professor in regards of the DNS protocol and some application exercises using the Wireshark package tool. It will explain some fundamental details of DNS, followed by a comprehensive analysis and comparison of its layered structure with the theoretical design that is currently being discussed in class and it will finalize this report with some real-life examples of the usage of this protocol in some common web URLs. A video will be made while exploring the links with Wireshark due to it being a requirement and for being a tool to measure the level of understandment acquired from the investigative process.

II. Basics of DNS

The DNS (*Domain Name System*) is a protocol that works in the application layer of a computer network, establishing how the interaction between a device and a service provider connected through the internet will occur. It is managed by ICANN [2] (Internet Corporation for Assigned Names and Numbers) who confirms and maintains the several domains that utilize the protocol [5] and the IETF (*Internet Engineering Task Force*) who oversee and update the several specifications of DNS structure in a technical level in the form of RFC standards (Request for Comment). Some of these main RFC standards include:

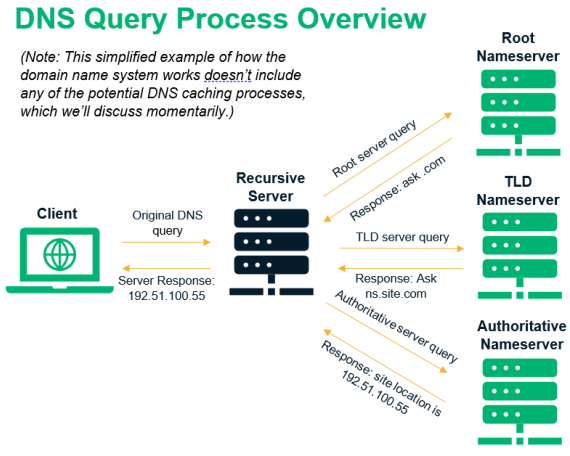
- RFC_1034 - *DOMAIN NAMES - CONCEPTS AND FACILITIES* [7]
    - Introduces the concept of DNS and the domain style names, their use for Internet mail and host address support, and the protocols and servers used to implement domain name facilities. In short, the conventions and terminology to follow in the development and expansion of the protocol.
- RFC_1035- *DOMAIN NAMES- IMPLEMENTATION AND SPECIFICATION* [8]
    - Clearly defines the data types, functions, structure, and format to be built for any device that wishes to utilize de DNS protocol.
- RFC_1122 - *Requirements for Internet Hosts - - Communication Layers* [9]
    - This RFC describes the link layer, IP layer, and transport layer of the RFC protocol and several ways to go about implementing it into a working model for a host device. It is paired up with RFC_1123.
- RFC_1123 - *Requirements for Internet Hosts - - Application and Support* [10]
    - Names the standard protocols to enable internet access to a host device and how it will

operate with the several requests he will receive. It is paired up with RFC_1122.

- RFC_7766 - *DNS Transport over TCP - Implementation Requirements* [3]
    - It indicates all the prerequisites to include TCP as transport protocol and includes an overall guide on how to proceed with transactions between the two.

There are many more, but these are important because they establish and define the protocol, the way to instantiate a host machine and begin transactions of information utilizing a very common transport protocol.

All these details come together to formulate the essential function of the DNS: to sync up names that are composed of commonly recognizable sequences of characters, transform them into domain numbers and match them with computer IP addresses. All of that to ease the requests a standard user wishes to make with a service provider that resides on a remote server.[11]

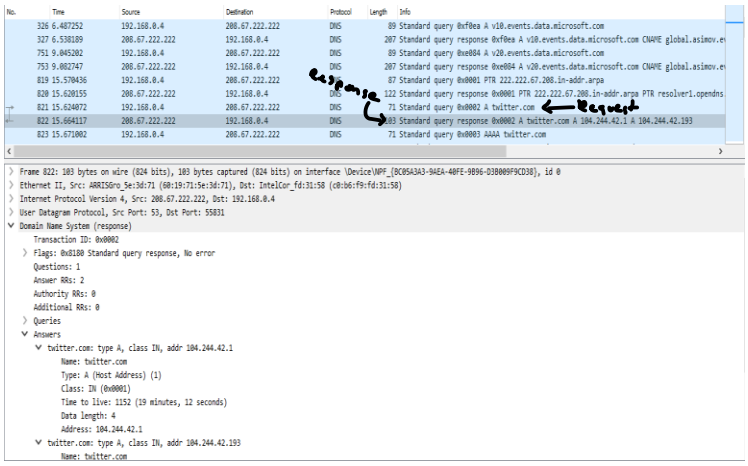


[1]

The scale in which the DNS operates usually is WAN connections. This protocol is widely used in intercontinental transactions and sometimes in smaller scales. The structure of this protocol is a hierarchical, decentralized one (this is because it manages a database system that surge from an origin to point but diversifies into many more).[6]

The DNS protocol can receive multiple responses at the same time. This is an optimization made by the IETF to send additional data/addresses to the cache memory of the host devices and reduce the memory latency in subsequent queries made after the first call. Cache memory, being the fastest, allow for quick referrals to already established data points in less volatile memory storage containers. [4]

III. Layered Model Analysis for DNS



Website: twitter.com

Thanks to the Wireshark package tool it is possible to discern the different protocols in each layer. In the last level (Application) the Domain Name

System is the active protocol identified with the Transaction ID. It's followed by the UTP in the Transport layer identified with the Port. Next, the Network layer is present with the IPv4 protocol using the IP address of the server as the identifier. Finally, the Data Link and Physical layers use the ETHERNET II protocol (or WI-FI protocol), identified with an EtherType octa-hexadecimal key.

Layer	Protocol	Id
Application	DNS	Transaction Id
Transport	UTP	Port
Network	IPv4	IP address
Data Link	WI-FI	EtherType
Physical	WI-FI	EtherType

IV. More exercises about DNS and Wireshark

Website	IP address	Location	Owner
www.uprm.edu	136.145.30.109	Mayaguez, PR	UPR system
www.upr.edu	136.145.11.14	Cayey, PR	UPR system
www.google.com	142.250.64.174	USA	Google
www.amazon.com	54.239.28.85	Virginia, USA	Amazon
www.facebook.com	157.240.14.35	California, USA	Facebook
www.netflix.com	54.165.153.56	Virginia, USA	Amazon
www.etsi.org	195.238.226.27	Alpes-Maritimes, FR	Orange

V. Conclusions

Throughout this investigative process the overall concept and purpose of the DNS protocol became clearer. The student learned to identify DNS packages in Wireshark and to identify the sources exchanging information and queries in the computer.

VI. References

[1] C. Crane, "What Is a DNS Server and Why the Internet Wouldn't Work Without the DNS System," *Experfy Insights*, 08-Jun-2020. [Online]. Available: https://www.experfy.com/blog/software/what-is-a-dns-server-and-why-the-internet-wouldnt-work-without-the-dns-system/. [Accessed: 06-Feb-2021].

[2] ICANN, *ICANN*, 2002. [Online]. Available: https://www.icann.org/groups/ssac/dns-security-update-1. [Accessed: 05-Feb-2021].

[3] J. Dickinson, S. Dickinson, Sinodun, R. Bellis, A. Mankin, D. Wessels, and ISC, "DNS Transport over TCP - Implementation Requirements," *IETF Tools*, Mar-2016. [Online]. Available: https://tools.ietf.org/html/rfc7766. [Accessed: 06-Feb-2021].

[4] K. Fujiwara, "Abstract," *Returning additional answers in DNS responses*, 29-Oct-2017. [Online]. Available: https://tools.ietf.org/id/draft-fujiwara-dnsop-additional-answers-00.html#:~:text=By%20providing%20multiple%20answers%20in,ask%20for%20the%20subsequent%20queries.&text=Developers%20of%20DNS%20servers%20know,service%20resolvers'%20query%20patterns%20well. [Accessed: 06-Feb-2021].

[5] M. Muller, *Who manages, runs and maintains DNS servers?*, 30-Mar-2013. [Online]. Available: https://www.quora.com/Who-manages-runs-and-maintains-DNS-servers. [Accessed: 05-Feb-2021].

[6] Novell Inc, *Novell Documentation*, 2003. [Online]. Available: https://www.novell.com/documentation/dns_dhcp/?page=%2Fdocumentation%2Fdns_dhcp%2Fdhcp_enu%2Fdata%2Fbehdbhhj.html. [Accessed: 06-Feb-2021].

[7] P. Mockapetris, “Domain names - implementation and specification,” *IETF Tools*, Nov-1987. [Online]. Available: https://tools.ietf.org/html/rfc1035. [Accessed: 06-Feb-2021].

[8] P. Mockapetris, “Domain names - concepts and facilities,” *IETF Tools*, Nov-1987. [Online]. Available: https://tools.ietf.org/html/rfc1034. [Accessed: 06-Feb-2021].

[9] R. Braden, Ed., “Requirements for Internet Hosts - Communication Layers,” *IETF Tools*, Oct-1989. [Online]. Available: https://tools.ietf.org/html/rfc1122. [Accessed: 06-Feb-2021].

[10] R. Braden, Ed., “Requirements for Internet Hosts - Application and Support,” *IETF Tools*, Oct-1989. [Online]. Available: https://tools.ietf.org/html/rfc1123. [Accessed: 06-Feb-2021].

[11] VeriSign, “How DNS Works In Six Steps,” *Verisign*, 01-Jan-2014. [Online]. Available: https://www.verisign.com/en_US/website-presence/online/how-dns-works/index.xhtml. [Accessed: 06-Feb-2021].