**Final Project: TCP/IP Model within Network Architecture**

Adam Livingston

University of Arizona

CYBV 326: Introductory Methods of Network Analysis

Professor Jonathan Martinez

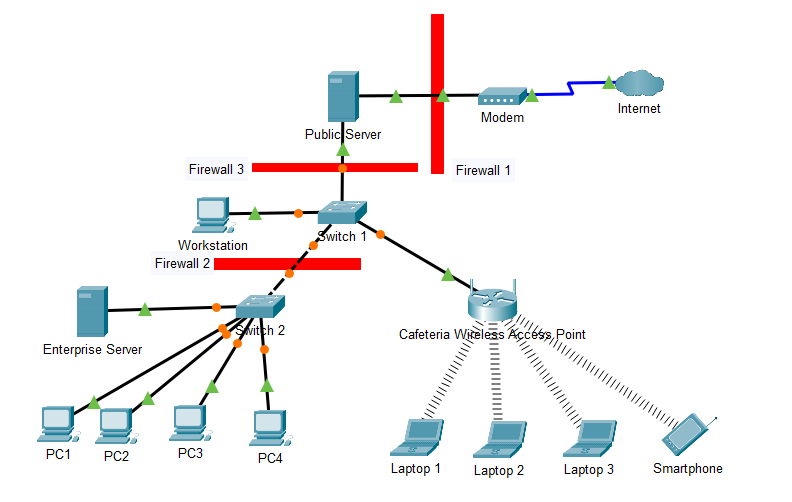
14 December 2021

**Final Project: TCP/IP Model within Network Architecture**

According to Kurose & Ross, “To provide structure to the design of network protocols, network designers organize protocols—and the network hardware and software that implement the protocols—in layers” (p.49). Each layer is home to one or more protocols and provides a service within the network that is embedded in hardware, software, or both. The two predominant models present are the Open Systems Interconnection (OSI) model and the Internet Protocol (IP) Stack (or model). While the OSI model consists of seven layers, the TCP/IP model consists of four layers and “is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.” (Martinez, w1, s48).

This paper will explore an example network architecture consisting of both public and private networks and how information travels in each layer within the framework of the TCP/IP model. Additionally, within the framework of the TCP/IP model will be an examination of attacks at each layer, how the attack is propagated, and mitigation strategies to limit or prevent harm from occurring to an organization victimized by such an attack.

**Network Architecture**



**Architecture Description:**

The above network is divided into three main areas. An organizational network is connected to Switch 2. PCs 1 through 4 are employee workstations that have access to their Enterprise Server to store data, proprietary information, and other important organizational information. A public network is denoted by the Cafeteria Wireless Access Point (WAP). This is designed for people who want access to the internet in the organization’s publicly-available cafeteria. Of course, employees may also use it with wireless devices and access proprietary information unavailable to the public by using a Virtual Private Network (VPN) installed by the IT department on their devices. The third area is designed as a centralized “hub” to connect both public and organizational networks together and to route them towards the internet. This is accomplished via Switch 1. Switch 1 routes traffic from the Cafeteria WAP, the organizational network, and connects them to the public server controlled by “workstation”. Workstation is the administrative control station for the entire network and would run a Linux Command Line Interface (CLI) to make changes, monitor traffic, and maintain the network.

**Resource Requests**

**Layer 4 Application Layer**

Laptop 1 wishes to access a webpage [www.example.com](http://www.example.com). To establish the connection, the device sends an HTTP request message to the host through port 80 using TCP. The data is encapsulated within the HTTP message. When the host accepts the connection, it sends an HTTP response message to the client through port 80 using TCP (Kurose & Ross, p.101-108).

A user on PC1 wishes to send an email to a user on PC2. PC1 composes the email and sends it to their mail host. PC1’s mail server establishes a connection to the mail server host via port 25 using TCP and encapsulating the data in a Secure Message Transfer Protocol (SMTP) handshake to PC2’s mail server. This allows the email data to be transferred securely between two mail hosts. PC2’s mail server places the message in PC2’s inbox where the user can read the message (Kurose & Ross, p.118)

The user on PC2 cannot just simply access the sent email using SMTP, but must use a Mail Access Protocol since SMTP is a push protocol and PC2 needs to pull the data. PC2 will use Post Office Protocol v3 (POP3) via port 110 to pull the POP3-encapsulated message data in a three-phase approach: authorization via login information, transaction to retrieve the message, and update to end the POP3 session. The main drawback of using POP3 is that the emails are downloaded onto the local machine (Kurose & Ross, p.123-125).

To solve the issue of localized data via POP3, the user in charge of PC2 decides to take a lunch break and takes his smartphone to the cafeteria and accesses his email through an email application. This application uses Internet Mail Access Protocol (IMAP) where the data is encapsulated and is accessed through port 143. IMAP allows the user to access their emails on the mail server without downloading them to a localized device. (Kurose & Ross, p.125-126).

A guest using Laptop 1 visits the home page of the public server and wants to watch a video on the home page. Laptop 1 establishes the connection by sending an HTTP request message to the host through port 80 using TCP. When the host accepts the connection, it sends an HTTP response message which includes the video file to the client through port 80 using TCP (Kurose & Ross, p.148).

**Layer 3 Transport Layer**

Laptop 2 decides to use the Cafeteria WAP to watch Netflix on their lunch break. Once they select a video, UDP is used to stream it. The Netflix server and Laptop 2 will create a socket using a port number within the range of 1024 to 65535 that is available on the server. The Netflix server will stream video back to laptop 2 where the information is encapsulated using UDP segments. UDP is a connectionless protocol that has smaller packet header overhead and is ideal when streaming video due to the amount of continuous data being transferred.

After the user watches their show from Netflix on Laptop 2, they decide they want to play a videogame, specifically Halo: Combat Evolved multiplayer. Laptop 2 and the Halo: CE host create a socket using UDP via port 2302 to continue data transfer when playing online. The information is encapsulated in UDP segments and other players on the server will use port 2302 as well.

A user on PC3 decides to do some web shopping on their break and decides to go to Amazon. To establish the TCP connection through port 80, a three-way handshake must occur in which the information is encapsulated in TCP segment. In the flag field of the segment, PC3 will use a SYN flag to synchronize the connection. Amazon will respond with a SYNACK flag to acknowledge the synchronization request. Finally, PC3 will respond with an ACK flag in the segment to finalize the connection.

Unfortunately, PC3 had some lost packets when trying to establish the TCP connection to Amazon through port 80 during the three-way handshake process. After PC3 sent the TCP SYN segment to Amazon, the TCP ACK segment was lost in transit from Amazon. Since there was a timeout on PC3 waiting to receive the ACK, another SYN segment was sent. Finally, PC3 received the ACK segment from Amazon and the connection is established once the three-way handshake completes.

Now that PC3 is done shopping, they want to terminate the TCP connection with Amazon that has been established on port 80. Using information encapsulated in TCP segments and in the flag portion of the TCP segment, PC3 sends a FIN segment to Amazon. Amazon then sends an ACK segment to PC3 then a FIN segment soon after. PC3 then sends back to Amazon an ACK segment to finalize the connection termination.

**Layer 2 Internet Layer**

Laptop 1 wants to connect to the internet but doesn’t have an IP address, but gains one using a Dynamic Host Configuration Protocol (DHCP) request message using a UDP segment. Laptop 1’s DHCP request has destination port 67 (DHCP server) from port 68 (DHCP client). The UDP segment is then encapsulated in an IP datagram. When DHCP provides the IP address, Laptop 1 will be able to communicate within the network.

The network administrator operating on the workstation wishes to measure the connectivity between devices in the network and measure packet delay or loss, so they use a ping. An Internet Control Message Protocol (ICMP) echo request packet is sent to the devices they wish to test packet delay and loss. Once the device receives the request, they send an ICMP echo reply packet and the data is measured. No port is used and

The network administrator then wants to determine the route that a datagram takes between their workstation and Google, such as any access points or routers that it needs to go through in order to make it to the destination and their associated addresses. The administrator runs a traceroute (*tracert*) which sends a series of IP datagrams carrying a UDP segment to an unlikely port number with sequentially increasing Time to Live (TTL) values for each datagram. When the datagram arrives at the source, the source sends a similar datagram back to the administrator’s workstation which determines round trip time and name/IP address of the router.

Laptop 2 wants to connect to Google as well and sends IPv4 datagrams through port 80 in order to establish the connection via TCP. The IPv4 datagram contains information that identifies both the source and destination address and a myriad of other information that enables it where to go.

Unfortunately, the IPv4 datagram that Laptop 2 sent to Google through port 80 via TCP was too large to be accommodated by the Cafeteria WAP’s capabilities, exceeding its Maximum Transmission Unit (MTU). The IPv4 datagram is then split into fragments in a process called fragmentation. This allows the hardware capabilities to accommodate the datagram payload and are then reassembled at the destination’s transport layer.

**Layer 1 Link Layer (2 remain)**

PC1 wishes to send information to PC2. PC1 knows the IP address of PC2 but they need to establish the connection by using MAC addresses (also known as Link Address). In order to send that information encapsulated in an IP datagram, PC1 will send the information into the network containing PC2’s IP address. The switch will then construct link-layer frame that takes the PC2’s IP address and match it with its MAC address, allowing the information to be sent. This is accomplished through Address Resolution Protocol (ARP) which conducts this translation between the Internet Layer and Link Layer. This can only be accomplished in a LAN.

Laptop 1 wants to connect to the internet but doesn’t have an IP address, but gains one using a DHCP request message encapsulated in an IP datagram. Laptop 1’s DHCP request has destination port 67 (DHCP server) from port 68 (DHCP client). The DHCP request message is then encapsulated/placed within an Ethernet frame with the destination of the DHCP server’s MAC address and also includes Laptop 1’s MAC address. This frame enters the router, is broadcasted to all devices connected, and will hopefully find its intended destination of the DHCP server in the effort to receive an IP address.

Laptop 1 eventually receives an IP address and can now access the internet with the intent to connect to [www.google.com](http://www.google.com). Laptop 1 will send a DNS query message via a UDP segment to port 53, which is then placed in an IP datagram. Once it is in the IP datagram, Laptop 1 will then place the DNS query message into an ethernet frame and send it to the gateway router which will in turn send it to the MAC address of the DNS server. The DNS server will reply with a DNS reply message and send it to Laptop 1 indicating it is ready to connect to Google.

**TCP/IP Stack Attacks**

**Layer 4 Application Layer: SMTP Injection Attack.** A Secure Message Transfer Protocol (SMTP) Injection “injects attacker-controlled SMTP commands into the data transmitted from an application (typically a web application) to an SMTP server for spamming purposes.” (MBSD). SMTP is a protocol used at the application layer to transfer email messages from one mail server to another (Kurose & Ross, p.122) and by being able to manipulate parts of that protocol’s data, such as the email itself, then the attacker can manipulate message body or header information and therefore violate the integrity of the message. SMPT message fields that are subject to such manipulation include To: and From: lines as well as the message body itself. This is able to cause harm to the recipient of the message through the attacker intercepting, modifying, or fabricating a message (Pfleeger, p.8).

This attack exploits a vulnerability in some SMTP applications that do not have input validation (MBSD). The attacker uses the lack of input validation to inject commands into message data and the modified message is processed by the server without validation. The best way to mitigate against an SMPT Injection Attack is to close the exploited vulnerability as described and to validate user input. Not allowing “any newline characters in the input because they let the attacker append email headers” can be achieved in the simplest and most robust way by creating a whitelist of approved characters (Acunetix).

**Layer 3 Transport Layer: UDP Distributive Reflective Denial-of-Service (DRDoS).** A DRDoS “is a form of Distributed Denial of Service (DDoS) attack that relies on publicly accessible UDP servers and bandwidth amplification factors (BAFs) to overwhelm a victim’s system with UDP traffic.” (CISA). A DDoS attack is an umbrella term used to describe attacks that leverage botnets designed to hinder the availability principle of the CIA Triad on the victim (Pfleeger p.423). What the DRDoS Attack does is forge the UDP packet’s source IP address to the victim’s IP address so that the destination server responds to the victim instead of the attacker (CISO). This means that instead of flooding a victim directly with packets, the botnet can disguise themselves as the IP address of the intended victim when connecting to a server using UDP and therefore flooding the victim with the server’s UDP packets.

This attack exploits the large bandwidth and trust of servers utilizing UDP protocols en-masse. To mitigate such an attack, CISO recommends many different steps. To name a couple, one is to utilize stateful UDP inspections (i.e., reflexive access control lists) to reduce the impact of unsolicited UDP packets on firewalls and routers. Using a stateful inspection firewall builds context for each packet by monitoring all open connections through the firewall (Vanhoy, w4, s19) and by building that context the malicious packet requests can be filtered out. Another step is to “use a Border Gateway Protocol (BGP) to create a Remotely Triggered Blackhole” (CISO). Since BGP is used to route all traffic across the internet (Vanhoy, w5, s54) and that attacks against it are sophisticated due to its complicated nature (Pfleeger p.412), the mechanism is inherent in detecting such attacks. The blackhole mentioned by CISO is referenced and cited to packetlife.net, describing an arrangement of routers and packet travel in such a way that malicious packets are dropped after a certain number of hops within said router structure, therefore disappearing into the virtual blackhole.

**Layer 2 Internet Layer: ICMP Smurf Attack.** An ICMP Smurf attack is also a type of DDoS attack that attempts to accomplish compromising the availability principle of the CIA triad by overwhelming: the capacity to meet the service’s needs, timely response to requests, and completion time for services (Pfleeger p.11). As with many DDoS attacks, “the idea of this attack is to overload a server with packets” but is done from a spoofed IP address using a smurf program (IJMER). The attacker sends a large number of ICMP packets from a “broadcast address” that is trusted on the victim’s end, and forces a response to each packet which overwhelms the bandwidth of the victim (IJMER).

On page 139 of Kurose & Ross, an example ICMP attack is given in which attackers tried to DDoS Domain Name Service (DNS) servers. The attack was largely unsuccessful as many of the servers that were targeted were equipped with packet filters that blocked ICMP ping messages. It can therefore be deduced that to protect against such an attack an organization should block or filter large volumes of ICMP ping messages from any and all IP addresses. Additionally, these filters should have parameters of trusted IP address ranges in the Local Area Network (LAN) that drops network traffic outside of the determined range (Infosec).

**Layer 1 Link Layer: Jamming Attack.** According to IJCA, a subset of DoS attack “at the first layer known as the Physical layer, [a] jamming attack may be launched which reduces the throughput of the network to unacceptable levels.” Since the physical layer and data-link layer in the OSI model overlap with the Link layer of the TCP/IP model which encapsulates information in bits or data-streams, this type of attack fits directly in with layer 1 of the TCP/IP model. There are many different types and subtypes of hardware (known as jammers) designed to accomplish this attack, but in essence they accomplish the same thing: A jamming attack exploits the radio frequencies used in wireless networks by using said jammer designed to intentionally cause interference (IJAHUC).

To mitigate such an attack, an organization must employ a two-pronged approach of detection of such devices and countermeasures. Detection of jammers must take into consideration “working form (individual, distributed, or centralized) [of the jammer], detection metric, overhead, cost, and implementation difficulty” and countermeasures must “consider the type of jammer [the organization is] against, whether reactive or proactive, working form (individual, distributed, or centralized), overhead, cost, [and] implementation difficulty.” To summarize the recommendations of the IJAHUC for detection and countermeasures, an organization must locate the jammer based off of its area of effect and frequencies affected. To counteract the effect of the jammer, the device can either be physically removed once located or to map network traffic around the affected frequencies or network hardware.

**Conclusion**

Throughout the TCP/IP stack, resource requests travel in a logical fashion throughout every layer in order to provide and obtain information from client and host. This dance occurs not only in close proximity to the user, but across the globe in nigh-incalculable volume at extraordinarily high speeds. From visiting web pages, reading email, to playing video games online, massive amounts of data are transferred, processed, encapsulated, and translated in order to view it on a computer screen. Within these complicated and intertwined networks that provide people with their livelihoods and entertainment are vulnerabilities that can be exploited by malicious persons. It is up to everyone, from the cybersecurity professional to the layman user of their home PC, to protect their information and to take simple yet comprehensive steps to ensure that their assets are protected.

**References**

Kurose, J. F., & Ross, K. W. (2022). *Computer networking: A top-down approach*. Pearson.

Pfleeger, C. P. (2015). *Security in computing*.

Alani, M. M. (2014). Guide to OSI and TCP/IP models. Springer.

Terada, T. (2015). SMTP Injection via recipient email addresses. MBSD Technical Whitepaper.

Martinez, J. (2021). Lectures 1-13 [PowerPoint Slides]. University of Arizona CYBV 326 Introductory Methods of Network Analysis.

Vanhoy, J. (2021). Lectures 1-7 [PowerPoint Slides]. University of Arizona CYBV 301 Fundamentals of Cybersecurity.

Muscat, I. (2020, July 15). What Are Email Injection Attacks. Acunetix. Retrieved December 10, 2021, from <https://www.acunetix.com/blog/articles/email-header-injection/>

UDP-Based Amplification Attacks | CISA. (2017, January 17). Cybersecurity & Infrastructure Security Agency (CISA). Retrieved December 10, 2021, from <https://www.cisa.gov/uscert/ncas/alerts/TA14-017A>

A Review of Network Layer and Transport Layer Attacks on Wireless Networks. (2019, January 29). IJMER. International Journal of Modern Engineering Research, 8(12).

ICMP attacks. (2021, August 9). Infosec Resources. Retrieved December 11, 2021, from https://resources.infosecinstitute.com/topic/icmp-attacks/

Cheema, R., Bansal, D., & Sofat, S. (2011). Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks. IJCA. International Journal of Computer Applications, 23(7), 7–15. https://doi.org/10.5120/2901-3801

Grover, K., Lim, A., & Yang, Q. (2014). Jamming and anti-jamming techniques in wireless networks: a survey. IJAHUC. International Journal of Ad Hoc and Ubiquitous Computing, 17(4), 197. https://doi.org/10.1504/ijahuc.2014.066419