In a simulated computer network environment, to what extent are protocols for computer networks used to transfer packets of data between multiple devices?

An Extended Essay in the Subject of Computer Science.

Presented by

Aman Mohammed Ibrahim

CID# 002294-0019

To

The International Baccalaureate Organization

in partial fulfillment of the requirements

for the International Baccalaureate Diploma

Garner Magnet High School

Garner, North Carolina, USA

May 2016

Project Supervisor: Mr. Ian VanBuskirk

Word Count: 3915

# Abstract

During this growing digital age, computer networks have definitely become the backbone of information transmission. This report investigated the roles of the computer protocols within any computer network, including simulated computer networks.

This report clarifies the definition of a computer network through a prompt description and a concise historical background. Afterwards, it introduces three computer network devices, the router, switch, and hub, and the concept of computer protocols. Once the concepts are introduced, this investigation explores the multiple protocols and their relationships with other protocols and devices. And with the use of a simulation program, the report was able to confirm the purposes and relationships of the protocols and devices.

The methodology of this investigation was simply to collect multiple resources in order to gain an understanding of the intricacy of a computer network.

The conclusion of this report displays that computer networks use protocols constantly, and with the simulation, the complexities can be presented. With the protocols, it allows devices within computer networks to: use an addressing system in order to find the destinations of data packets, automate the assignment of the addresses, and to transfer data packets efficiently. And, without the protocols, the outreach of modern computer networks would not be achievable.

Word Count: 205

Contents

Abstract 1

1. Introduction 3

2. Protocols of a Computer Network 5

3.Simulation 13

4.Conclusion 16

Works Cited 17

1. Introduction

1.1 Explanation of Question

The reason I chose this question is because of the importance of computer networks in today’s society, which depends on the continuous, non-stop flow of information to empower communication, and this importance is only going to grow in the following years. This is true because we live in an age where a computer network is involved in nearly every human activity, whether the involvement is significant or minute. And, I consider that if any existing entity does hold such an importance to humanity, then an individual must take the responsibility of studying and learning about the said entity for the benefit of the individual and humankind. Therefore, I understand that the research of computer networks is my responsibility because of its definite impact to society.

1.2 What is a computer network?

Simply put, a computer network is a collection of computers and other electronic devices communicating to one another. According to Technopedia, a computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. The purpose of communication can range from a cellular device connecting to a local device with Wi-Fi capabilities to sending an email that can go through a countless amount of computer networks before it reaches its destination in milliseconds. With the power of computer communication, computer networks have given us utilities such as international communication, online entertainment, efficient and instant commerce, and so much more. In fact, as I compose this document, I am dependent on computer networks by creating the document on a word processing program that automatically uploads the data on the “deep web” portion of the internet and shares it with only a select few, such as my disciplinarians.

1.2.1 The OSI Model

In the late 1970s, there were two projects that began in order to define a unifying standard for the architecture of computer networks. This resulted in the creation of the Open System Interconnection (OSI) Model in 1983 when the two projects collaborated to publish one standard. This concept was built upon the experiences from earlier computer networking project such as the pioneer known as the ARPANET. The OSI Model is an abstract model of computer networks that is still carried as the standard in today’s technology. The OSI Model is made of seven layers; application, presentation, session, transport, network, data link, and physical. The OSI Model goes into further detail in Appendix 1.

1.2.2 Essential Devices of a Computer Network

The computer network can be made up of countless types of hardware like desktops and peripherals. But, there are three devices that will be covered that were created with the sole purpose of organizing a computer network; the hub, the switch and the router.

Cisco defines the switch and router as the most valuable components in a modern computer network. In fact, their actual interpretation of the terms ‘switch’ and ‘router’ is that switches are used to connect multiple devices on the same network within a building or campus. For example, a switch can connect your computers, printers and servers, creating a network of shared resources. The switch, one aspect of your networking basics, would serve as a controller, allowing the various devices to share information and talk to each other. Through information sharing and resource allocation, switches save you money and increase productivity. And, routers are used to tie multiple networks together. For example, you would use a router to connect your networked computers to the Internet and thereby share an Internet connection among many users. The router will act as a dispatcher, choosing the best route for your information to travel so that you receive it quickly. (Cisco)

Hubs are a common connection point for [devices](http://www.webopedia.com/TERM/D/device.html) in a network. Hubs are commonly used to connect [segments](http://www.webopedia.com/TERM/S/segment.html) of a [LAN](http://www.webopedia.com/TERM/L/local_area_network_LAN.html). A hub contains multiple [ports](http://www.webopedia.com/TERM/P/port.html). When a [packet](http://www.webopedia.com/TERM/P/packet.html) arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets. Hubs serve as a central connection for all of your network equipment and handles a data type known as frames. Frames carry your data. When a frame is received, it is amplified and then transmitted on to the port of the destination PC. In a hub, a frame is passed along or "broadcast" to every one of its ports. It doesn't matter that the frame is only destined for one port. The hub has no way of distinguishing which port a frame should be sent to. Passing it along to every port ensures that it will reach its intended destination. This places a lot of traffic on the network and can lead to poor network response times. As a result, hubs are now considered as counterproductive in the networking world.

2. Protocols of a Computer Network

2.1 What is a protocol?

When two humans converse, they may have to use the same language but they generally understand each other without having to adhere to rigid rules of grammar or formal language frameworks. Computers, on the other hand, have to have everything explicitly defined and structured. If computers wish to communicate with one another, they have to know in advance exactly how information is to be exchanged and precisely what the format will be. Therefore, standard methods of transmitting and processing various kinds of information are used and these methods are called "protocols". Protocols are established by international agreement and ensure that computers everywhere can talk to one another. There are a variety of protocols for different kinds of information and functions.

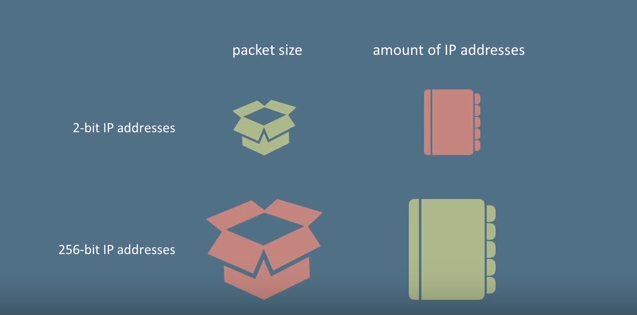
2.1.1 Types of Protocols

2.1.1.1 IP

The Internet Protocol (IP) is the main set of rules that governs the exchange or transmission of data between devices on separate networks. It’s got two main jobs, and for both of them, an easy comparison can be made to the mail system. The two jobs are host addressing and routing. With host addressing, it creates a uniform method in addressing the destination of a data packet in order to send data in the right direction and to avoid having to send the packets to every device. The Internet Protocol dictates the header format of any datagram or data packet, similarly to a label on a package or envelope for a letter, as well as how the data payload is nested within it. With routing, the Internet Protocol predicts and selects the best possible pathway for data transmission across network boundaries. This function is mostly performed by routers, and this function can be compared to sending a parcel internationally. For example, in the mailing system, if someone wants to send a parcel from Raleigh to Manchester, then the package would probably stop by a courier hub in New York then make its way to Manchester, rather than having the parcel make multiple stops in Chicago, Brisbane, Mumbai, Hong Kong, and Paris before reaching Manchester. (Angelescu)

2.1.1.1.1 NAT

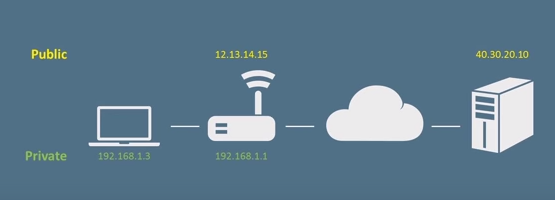
During the early development of the Internet Protocol in the early 1970s, the engineers were concerned with the sizes of the IP addresses. Remember, in every data packet, there is a sender and receiver address, just like the envelope of a letter. The catch-22 was that if they chose to design a small bit-sized IP address model (2 bit), then there would be a low number of possible IP addresses, but the packet sizes would not take up unneeded space or if they chose to design a large bit-sized IP address model (256 bits), then the data packets would take too much space yet there would be a great number of available IP addresses.

  
Figure 2.1: In this illustration, it gives a perception of the protocol’s engineers situation.

The engineers decided to go with a 32-bit sized system that gave them approximately 4.2 billion possible IP addresses, now known as IP version 4 (IPv4). At the time, the computer networks were only used for academic use, therefore, to the engineers, 4.2 billion was more than enough possible addresses. But as of today, 4.2 billion addresses is not nearly enough for the growing number of devices that need to connect to the internet. (Angelescu)

The solution to this problem is Network Address Translation (NAT). The NAT is a method of remapping IP address space by manipulating the relationship between a Local Area Network with the Internet. For example, take a typical Local Area Network that has a home router connected to three devices, a desktop, a laptop, and a smartphone. The Internet Service Provider (ISP) will provide a public IP address for the router in order for it to connect to the internet. In this case, let’s give the router a public IP address of 12.13.14.15. Theoretically, this is a IP address that any other IP addresses can send data packets to. The devices within the Local Area Network also get an IP address, but instead of getting one of the 4.2 billion IP addresses, they receive individual private IP addresses. All private IP address have the same subnet of 192.168.x.x, and this address is assigned by the home router. In this example, the router is given the address 192.168.1.1, the desktop is given the address 192.168.1.2, the laptop is given the address 192.168.1.3, and the smartphone is given the address 192.168.1.4. With Network Address Translation, it allows a network to use both public and private IP addresses to save as many of the 4.2 billion public IP addresses as possible.

In one scenario, the laptop from the Local Area Network may want to know the latest weather information in the local area from a web server with the IP address of 40.30.20.10. Therefore, the laptop will need to send the request through the home router, then through the internet, and finally reach the web server.

  
Figure 2.2: Illustration of example scenario

First, the laptop will need to send out a data packet requesting the information, “What is the current temperature in Raleigh, NC?”. This same packet will also contain the addresses of the source and destination devices. The source address would show up as “192.168.1.3:4231”, and the information after the colon is the port number of the source. Before sending the data packet right through the internet, this is where NAT begins doing its job. The data packet will reach the router and the router will create a public side for the private side of the laptop’s IP address. As a result, the data packet will change its source address from “192.168.1.3:4231” to “12.13.14.15:24604”. Therefore, when the web server replies to the request that comes from the router, the address the web server is sending to is compatible because it is a public address from the router rather than a private one from the laptop. Once the home router receives the response from the web server, it will change the packet’s destination address from “12.13.14.15:24604” to “92.168.1.3:4231” in order for the laptop to interpret the data packet from the web server.

Once again, a comparison to the mailing system is possible. In a single street, there can be multiple apartments with different street addresses, and two separate apartment buildings can both have a room number 100, but they are still considered as completely different rooms. Just like the room numbers in an apartment building, a computer network can contain devices with private IP addresses that are similar to other private addresses in different networks, like 192.168.x.x, but the public address of the router is what differentiates the multiple computer networks. (Beal)

2.1.1.2 DHCP

The Dynamic Host Configuration Protocol (DHCP) is basically a protocol that creates IP addresses for clients, or computers. Before the creation of the Dynamic Host Configuration Protocol, IP addresses were allocated manually. Therefore, during the assignment of IP addresses, errors were common, including putting the same IP address on separate devices which causes conflict between the devices. And, the assignment can become more difficult when the network contains a large number of devices. As a result, the algorithm known as the Dynamic Host Configuration Protocol was created. With the protocol, whenever a device connects to a network, the device will send a message to the router requesting an IP address because it does not have one, then, the router will respond with an offer and the new host will accept that offer, thus, the router will confirm the device's IP address. (Angelescu)

The Dynamic Host Configuration Protocol has two requirements: a DHCP server installed in a router, and a DHCP client installed in every host. The protocol also has four major steps. The first step is called “DHCP discover”, and in this step a new host needs to discover the location of the DHCP server. The host will then send a DHCP discover request to every device on the computer network, this is called “broadcasting”. Basically, when a new host sends out this request, it is asking if any devices could assign it an IP address. Once the DHCP server receives and interprets the DHCP discover, then it will move to the next step, “DHCP offer”. During the second step, the server will offer an IP address with the DHCP offer, and just like in the last step, the server will broadcast its offer to every device in the network because it is unsure of the origin of the new host. Next step, the new host will broadcast a DHCP request to accept the message from the previous step, DHCP offer. Finally, the final step is DHCP acknowledgement, and in this step, once again the server will broadcast a message that confirms that the DHCP request is official and the new host will have an IP address to identify itself within the network. All in all, the four steps are called: discover, offer, request, and acknowledge. (“Automatic IP Address Assignment: How DHCP Works”)

2.1.1.3 Transport Protocols

The two transport protocols that will be covered will include: the User Datagram Protocol (UDP), and the Transmission Control Protocol (TCP). These protocols are prominent in the Transport Layer of the OSI Model. The main purpose of this layer and the protocols is to allow multiple applications to have the ability to use one network connection simultaneously. (Angelescu)

2.1.1.3.1 UDP

The User Datagram Protocol is usually considered as the lightweight, connectionless choice between the two protocols. This is because the UDP header is made up of only eight bytes compared to the twenty bytes of the TCP header. Also, unlike TCP, UDP is connectionless and it does not need a connection to maintain the protocol. (Angelescu)

Because data corruption can be common within a computer network, UDP has a primitive form of error detection. The UDP’s packets only carry a sixteen byte checksum, but they are not very reliable. This is because whenever UDP does detect any error or corruption, the corrupted segment will be discarded instead of recovering it, in some cases, UDP will keep the corrupted segment and it will only leave a warning flag on the application. Therefore, UDP does not attempt to compensate for lost packets. Every packet gets sent out only once; if a packet is lost during the transport process, then it is unrecoverable. Also, UDP does not guarantee packets will arrive in order. This is why text messages on cell phones may not be received by the recipient or may be received in the incorrect order. Moreover, UDP does not have any congestion control even if the network is already busy, thus, this can lead to more packets being dropped. Consequently, UDP may be lightweight, but it may not be as reliable. ("UDP and TCP: Comparison of Transport Protocols.")

2.1.1.3.2 TCP

On the other side, the Transmission Control Protocol is considered as the reliable, connection-based choice. As a connection is being set up, the connection must be negotiated before the protocol can do anything. The procedure of the negotiation is known as the “three-way handshake”. This is because it works in these three steps:

1. The initiator will ask the receiver if they would like to connect.
2. The receiver will retrieve the message, and it will then reply to the message.
3. The initiator will retrieve the reply, and if the message was a positive to the initiator's request, then the initiator will send the data packet.

With TCP, it uses this procedure in various of other situations such as delivery acknowledgments of data. With the use of delivery acknowledgment, TCP is capable of recovering files in a method known as retransmission. Whenever the initiator does not get a delivery acknowledgement from the receiver after a certain amount of time, then the initiator will assume that the data packet was lost and it will resend the data packet until there is delivery acknowledgement. TCP also has congestion control by delaying transmission when the current network is busy or congested.

Just like UDP, there are disadvantages to this protocol. As mentioned before, TCP header size is large compared to the alternative, which affects the efficiency of the protocol. Also, as a result of congestion control, data may not be sent out immediately, and it may not be received in the preferred time. For example, when using an online video call service like Skype, the intention is to make the call seem like a real-time conversation. With TCP’s congestion control, the protocol will deliberately introduce latency, thus, the video call will not fit the experience of a real-time conversation. Also, because TCP is always retransmitting packets and acknowledging packets, it causes TCP to have a bigger overhead. With a bigger overhead, an application using TCP can need a larger bandwidth than an application with UDP, and in most cases, this is an undesirable situation, especially when receiving every single data packet is not necessary. (Cisco) For example, when streaming video, there is not enough time for every single packet to be acknowledged or retransmitted if it goes missing. This is because video streaming does not need to recover every single packet loss, it has its own ways to compensate for the losses. Consequently, TCP is considered as the reliable yet connection-based protocol.

3. Simulation

3.1 What is the Cisco Packet Tracer?

Cisco Packet Tracer is a network simulation program that allows students to experiment with network behavior. As an integral part of the Cisco Networking Academy comprehensive learning experience, the Packet Tracer provides simulation, visualization, authoring, assessment, and collaboration capabilities and facilitates the teaching and learning of complex technology concepts. (Pablo Esquivel)

3.2 Packet Tracer - Hub Network

When using the Packet Tracer for a hub network, I used hub type 1841, since it is usually the basic standard for training or testing on the Cisco Packet Tracer. Then, I added, six end devices, five desktops and one server. The server was added because a hub is primitive when it come to the executing basic networking protocols. In this case, the server was most definitely needed in order for the hub to use the Dynamic Host Configuration Protocol, which automatically assigned I.P. addresses to every end device, including the server, and the hub. In this simulation, although the simulated devices cannot access areal inter-network, or internet, the simulation still uses concepts within NAT, like the use of preset private subnets or private IP addresses like 192.168.x.x. With the IP addresses, the simulation was able to send messages and simulated data packets through this network. Because it is a hub, every message was broadcasted, thus, showing another reason why hubs are considered as primitive and inefficient because hubs disregard IP addresses as tools to finding a data packet's destination as result of the limited technology on hubs. The major purpose for the IP addresses in this network is to let a device know whether it is meant to be destined “receivee” of the message because every single device will be broadcasted the message from the hub. If the message or data packet has a device's IP address as the destination, it will interpret the data and it may choose to respond depending on the conditions, otherwise, the device will just disregard the data packet. Also, in the hub network, transport protocols are not executed, especially since every data packet is treated the same by a hub no matter the header of the datagram or data packet.

3.3 Packet Tracer - Routing and Switching

In this simulated computer network, it will contain multiple routers, switches and end devices. Every router will be model 1841, as this is also the standard for the Cisco Networking Academy, and there are three routers each connected to their own switch. The three switches are Cisco models known as 2960-24TT, and every switch is connected to an end device, a desktop.

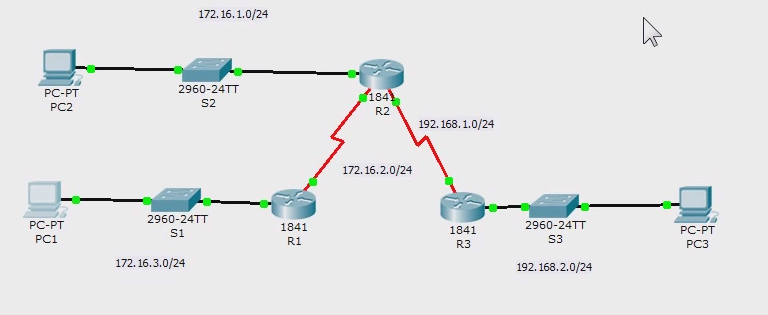


Figure 3.1: After configuration, this is the end result of the computer network. The elliptical-shaped disques are routers, the boxed device is the switch, and the others are desktops.

In figure 3.1, this artificial computer network is also known as a static routed network. Static routing is used for networks that are not anticipated to grow very much. Thus, the IP addresses for this network must be manually assigned to only the routers. Before simulating a data packet transferring through this network, the devices must be assigned addresses through a Command Line Interface (CLI) on the Packet Tracer.

Once the routers are configured, the router's DHCP server will begin to assign addresses to other devices throughout the network by broadcasting the assignments. And, when transferring packets with a UDP header, on occasion, some of the data packets may go missing, and if multiple packets are sent at once, they usually do not arrive in the same order. With TCP, in the simulation, packets show latency and take longer times to arrive than UDP packets because of concepts like the three way handshake. In fact, the simulation will show the three way handshake occur by showing visuals of the packet being sent back and forth.

4. Conclusion

In conclusion, protocols are essential to any computer network, especially to a computer network’s major purpose of data transfer. With this research, it is possible to understand the behind-the-scenes details of a tool, whose purpose is commonly undervalued by the general public. Therefore, in this report, after introducing computer networks, it introduces two major components of computer networks, devices and protocols. After introducing the two, the deep details of the two components were uncovered. For devices, the router, switch, and hub were defined, described and presented. Afterwards, the report explains four basic protocols that are present in nearly every modern computer network, Internet Protocol, Dynamic Host Configuration, and Transfer Protocols. For every protocol, its purpose was defined, its methods were described, and it was presented with simulations. The definitions originated from multiple sources such as Cisco, the purpose was defined through multiple analogies to compare its digital procedure with real life procedure, and the simulations certified and confirmed the definitions and descriptions. Consequently, the report substantiates the methodologies of the network protocols.

# Works Cited

Angelescu, S. (n.d.). Routing and Switching. In *CCNA Certification All-In-One For*

*Dummies* (Second ed.). John Wiley & Sons.

"ARPANET -- The First Internet." Http://www.livinginternet.com/. Livinginternet.com,

7 Feb. 2000. Web. 3 Aug. 2015.

"Automatic IP Address Assignment: How DHCP Works." *YouTube*. PieterExplainsTech,

23 Oct. 2013. Web. 9 Aug. 2015.

Beal, Vangie. "What Is The Difference Between IPv6 and IPv4?" *Webopedia*.

ITBussinessEdge, 27 Jan. 2010. Web. 11 Aug. 2015.

"Computer Protocols- TCP/IP, POP, SMTP, HTTP, FTP and More." Computer Protocols-

TCP,IP, UDP, POP, SMTP, HTTP, FTP, and More. The Windows Learning

Center. Web. 7 Sept. 2015.

"Computer History Museum | Timeline of Computer History : Networking Entries."

Http://www.computerhistory.org/. Computer History Museum. Web.

2 Aug. 2015.

"Internet Protocol - IPv4 vs IPv6 as Fast As Possible." *YouTube*. Techquickie,

24 July 2014. Web. 9 Aug. 2015.

"Networking Basics: What You Need To Know." Cisco. Web. 8 Aug. 2015.

Pablo Esquivel, J. (n.d.). *Cisco Packet Tracer 5.3*. Cisco.

Pacchiano, Ron. "The Difference Between Hubs, Switches and Routers."

*Webopedia*. ITBussinessEdge, 17 Nov. 2006. Web. 11 Aug. 2015.

"The OSI Model's Seven Layers Defined and Functions Explained." Microsoft

Support. Microsoft. Web. 8 Aug. 2015.

"UDP and TCP: Comparison of Transport Protocols." *YouTube*. PieterExplainsTech,

23 July 2013. Web. 12 Aug. 2015.

Appendix 1

The OSI Model

