CCNA 201-301 CERT GUIDE

COMPUTER NETWORKING

NETWORKING 101

ROAD TO BEING A CCNA CERTIFIED!

BY FRANCIS G.C.

Computer Networking 101

Introduction

CCNA

201-301

Certification Guide,

Francis G.C.

X.

Copyright Page

Francis

Writer's Signature

Book Introduction

BACKGROUND

This guide offers you multiple strategies you can use to master Computer Networking. Computer networking is a broad topic because it encompasses many areas. This can be overwhelming for new students, and hence to help guide students through their learning journey, this book is designed. Our work will give you a thorough understanding of the latest in network technology and design.

Following the guide will help you understand the basics of computer networks, how local and global networks interact, and how to better the ones we already have. This guide will cover the fundamentals and concepts associated with Networking for your Networking 1-301 certification exam. This book will help you get started with your CCNA and prepare you for the certification exam. I'd like to extend my gratitude to David Martin for inspiring me to write this book.

DISCLAIMER

The information in this book is made available publicly for others to use or adapt. The book is written to help students develop a plan for studying network security. The information provided in this book has been extensively researched and reported citing credible and reliable sources. The paper was written using input from business professionals who have gained experience in this field. Majority of the information were gathered from Cisco.

The document has been prepared to the highest standards possible. I will not be held responsible for any loss or damages someone does to the person or entity due to the information in this book. All images are derived from a website so they do not infringe copyright.

UNDERTAKING

I pledge to provide my readers with authoritative material that they'll find on the exam. Every effort has been made to ensure the accuracy of the content provided. Upon reading this article, you will be equipped to confidently pass your Cisco certification exam. We will provide the necessary information to enhance and develop the reader's knowledge as they proceed through the study.

XII.

Table of Contents

Contents undone…

CHAPTER 1

NETWORK FOUNDATION

CHAPTER 1 (Network Foundation)

Computer Network Perspective

One would likely expect that those with no experience in networking would assume that networks are similar to typical household networks. That's true, but there is still a great deal of variation yet to be discovered in networks. We discuss how people use their wireless connection and how they research things online. This book focuses on your networking knowledge and provides a better framework for basic networking principles.

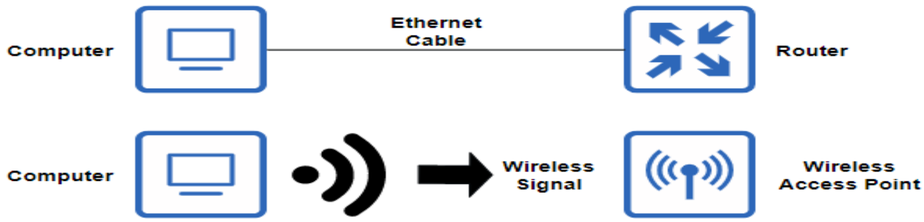


Figure 1 (Basic network diagram)

As illustrated in figure 1, there are two discrete types. A wirelessly connected network, and a wired connected network. The first figure demonstrates a computer connected through Ethernet cables to provide access to the Internet, on the other hand, the second figure demonstrates a tablet using wireless technology to provide internet access among the devices within the network. These wireless technologies make use of digital signals to provide connectivity between various devices, as opposed to the first sample, a wired connection makes use of electrical signals to allow and establish a connection from various destinations. These are the two types of networks that will be most commonly found in today's networks.

Network Overview

A computer network exists that is as simple as thought. A basic description of a computer network is a system of interconnected computers working together to form a network. These computer systems use protocols which are a set of rules on how computers interact which enable communication and connectivity between systems. Networks typically have a minimum size of two. There are numerous types of computer networks defined by their size and function that are discussed in this paper. A computer network consists of 3 Categories, hardware, medias, and services. Devices are usually the physical parts that are typically visible to the human eye. Devices such as routers, switches, hubs, and media such as fiber optic cables, copper cables, and such are discussed later on. And lastly, services are software applications that provide services such as email and web hosting to users across a computer network such as the Internet. A peer-to-peer network usually has clients and servers. A client utilizes services from a server and the server provides the aforementioned services. Networks nowadays such as typical networks and business networks can access the internet through different variations.

For instances, traditional networks may communicate using cable networks: access the internet through cable television service companies, Digital Subscriber lines (DSL): Internet access through mobile networks, Cellular signal: internet connection via cellular signals, Satellite: offers internet access from a far, and dial-up telephones: allows use of phone lines and a modem.

However, for business networks or wide networks rather includes high-speed on connection networks to help the business hence there are specially made connections for it such as, dedicated leased line: reserved circuits that provides WAN connection within a large geographical region, ethernet WAN or also named as Metro Ethernet: An expanded ethernet which further extends the reachability of LAN technology within a large geographical area.

Reliable Network

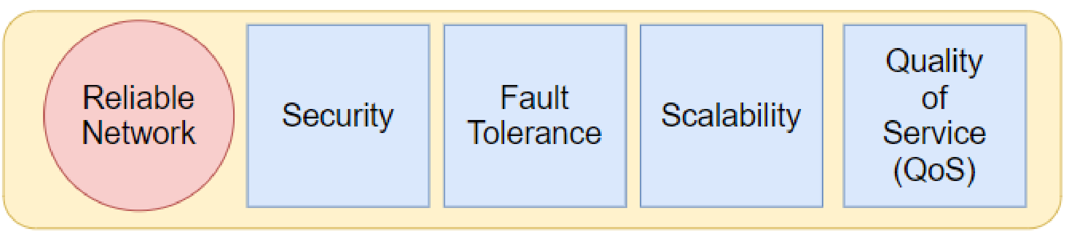


Figure 2 (Features of a Reliable Network)

Data networks need to have these features: fault tolerance, scalability, quality of service, and security. These said features are of great importance because they provide a solid foundation for a high-performing network infrastructure.

Fault tolerance. Network infrastructure must reduce the impact to the network and also respond to network failures. A fault tolerant network provides backup devices or links to help reduce the impact of network performance degradation when a failure occurs. A good example of a fault-tolerant network is a network which provides additional links from the computer systems inside the network. Redundant links allow for multiple paths of data transmission within a network.

Scalability. The network must be able to support the expansion of users while also remaining active. This is critical to the success of networks, because larger networks allow faster expansion of users. A good example of a new access method is to have numerous ports for new user access within a network.

Page 3

The quality of service (QoS). This is a very important requirement inside a network infrastructure because it ensures great quality of data transmission within a network by preventing network congestions and providing priorities base on its importance or sensitivity such as Voice Over IP (VoIP) which are time-sensitive data's and requires fast transmission. The priorities support prioritizing between time-sensitive data transmissions, such as voice and video transmissions, and data transmissions which are not time-sensitive, such as normal data.

Security. This is one of some critical functions of a network infrastructure that support optimal performance. Through this, it protects data from being altered or stolen, and also prevents unauthorized data access or breaches. Security must include data confidentiality: ensures data is in good hands and not to be seen by unwanted viewers, data integrity: ensures data is not altered during transmission, and lastly, availability: having the assurance of timely and reliable access to data services for authorized users.

Types of Networks

As mentioned previously, we will be covering some commonly known network infrastructure including PAN, LAN, MAN, SAN, and WAN, as well as intranets and extranets as part of the topic.

Common Types of Networks:

A Personal Area Network (PAN) is the smallest type of network infrastructure. This type of communication network enables communication between a centralized service and nearby devices. Each connected device within range of each other shares information with a central provider. Focus on a concrete example of a PAN, such as data sharing among others devices.

A local area network (LAN) provides a particular geographical area with access to a number of different devices. The term is used for both wired and wireless communication, and accommodates both wired and wireless local area networks (WLAN). An IP network may be supported by devices that are part of the network. An example of a LAN is a small office network which is a type of designed for homes and small offices.

Metropolitan area network (MAN) is a type of network infrastructure that allows computers to exchange information within a limited geographical area. This device is physically smaller than a LAN, but it's more powerful than a WAN (e.g., a city). This type of infrastructure is typically handled in a corporate setting.

An organization owns a privately-owned network (Intranet). An intranet is an internal network that connects different computers within an organization. It was designed to be only accessed by specific personnel from the organization. An organization may also use an extranet to provide secure access to individuals who work for other organizations. A case study could be a business partner.

Wide area networks (WANs). (WAN). A type of network infrastructure providing access to a large group of people over a large geographical area. Communications are usually overseen by telecommunication. This is one of the most useful aspects of an Ethernet, as it provides connectivity between different networks. The types of the network discussed in the book are often leased communications, and what they cover.

Lastly, Storage Area Networks (SAN). This type of network infrastructure typically utilizes storage devices as its main function. High-speed networks, that provide network access to storage, can be used. These components, such as hosts, switches, storage elements, and such, can be considered.

3 Tier Architectural Model Overview

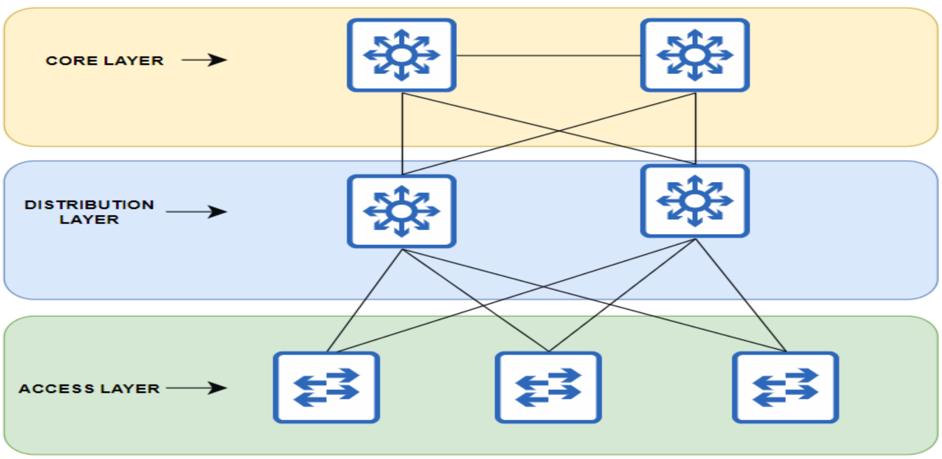


Figure 3 (3 Tier Architectural Model)

The Hierarchical internetworking model is a design model consisting of three layers for network design. It divides an information system into three layers: core, distribution, and access.

The access layer is found at the bottom of the three-layer architectural model. It makes connections to the other layers and provides access to external users. This layer typically includes access switches that enable connectivity between (computers, printers, servers, etc.) The access layer ensures packet delivery between computer systems inside the said network.

The distribution layer is located between the network routing and the data layer. Its main purpose is to provide a set of security policies, including access lists and resource quotas. This section of the network includes switches that ensure distribution and routing of packets between subnets and VLANs.

Finally, the core layer. This is the most important part of the hierarchy. This includes high-end devices such as routers and layer 3 switches which are capable of performing a large amount of data transmission at the same time. The purpose of this layer is to transfer data as quickly as possible from the source to the destination.

The 3-tier architectural model provides the following advantages. This enables a computer network to have better performance, high-speed network devices, better management, and troubleshooting, organized and isolated, better scalability allowing the network to constantly grow without issues or interruptions, and lastly, good redundancy provides multiple paths for data flow inside a network.

2 Tier Architectural Model Overview

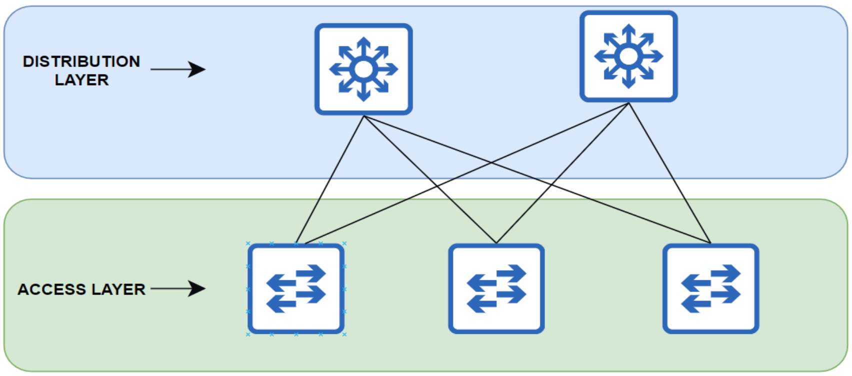


Figure 4 (2 Tier Architectural Model, Spine leaf model)

As opposed to the three-tier architectural model that consists of a base layer, a middle layer, and a top layer, this model consists of a base layer, and a collapse layer. In order to collapse the two layers of the three tier architecture, the distribution and the core layer were merged into a single layer which would go by the name of "Collapse layer". The architecture is a client-server model. An example of a 2-tier architecture in data centers is the spine-leaf architectural model. In figure 3, there are two layers: spine switches and leaf switches. A leaf switch is the primary point of access for network users. The backbone of a communications network, spine switches provide connectivity between all leaf switches inside the network. A 2-tier architecture has its own benefits, such as: latency: allowing for fast transmission, having 2 hops in maximum, performance: having high-speed links, scalability: allowing us to append devices such as spine switches, leaf switches, hosts, etc.

Types of network topology

Network topologies involve wiring the computers together, forming a network. Through these topologies, we can identify the different types of communication networks. As shown in Figure 3, different topologies are illustrated.

Point to point topology is the most fundamental type of network on the list. Communication between two nodes that are directly connected to each other using a wire or a shared medium. For example, Ethernet Computer networks, in which each device is connected within a single cable. All devices are communicating within a single main cable, so there are limited drops and there is no distance between the main cable and the devices. Although the main cable has been severed. There are also notable advantages and disadvantages in different bus topologies. The advantages of a bus topology are that it can be installed very easily and the wiring is more compact.

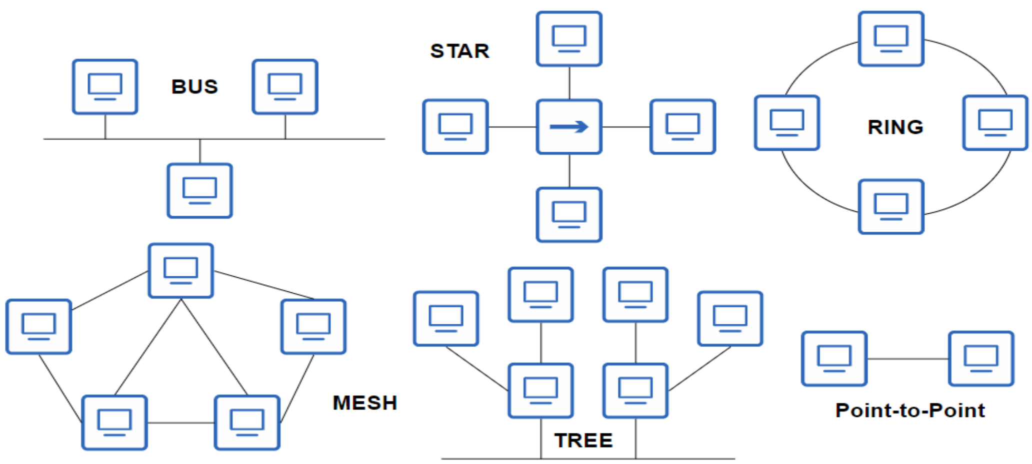


Figure 5 (Network Models)

absolutely necessary, unlike a mesh topology which we will go over next. In a bus topology, faults are difficult to detect, and it's difficult to scale.

A ring topology is a very simple design, consisting of a pair of devices connected on each side. The structure forms a ring and that ring topology makes it count as ring topology. The whole structures act as a repeater because once data is sent, the data is then sent on the other device to be repeated until the original device receives it. The advantages of a ring connected topology are similar to those of a bus connected topology since it is also easy to install. It is simple to modify and update, changing only two links is all that is required. The main disadvantage of a ring topology is the fact that a single link of the network can cause the entire network to be disabled due to the failure of that single link.

Moving on to next item. A star topology is a network in which each device is connected to a central device (or hub). A star topology allows for direct communication between devices but does not require every device to connect to the central device. The way it works is that if one device wants to communicate with another, it sends the data or packet to the central device which then makes the forwarding decisions and then sends it to its designated device destination. Star topology has many advantages for computing, but it can be installed quite easily too. A start topology doesn't require much money to build, only needing a single central device to make decisions. Less wires are required as long as you want fewer end devices. This structure is strong because if one link breaks the whole system won't fall apart. Finally, making things 'faulty' is easier to detect and notice. Even though this is a very popular topology, it also has its limitations. If there is a failure of the central device, then the whole topology would collapse with no way to communicate without a central device. The central device requires greater clarity because it is the central system.

Without a central device, these devices wouldn't be able to communicate without failing. The central device requires greater clarity because it is the central system.

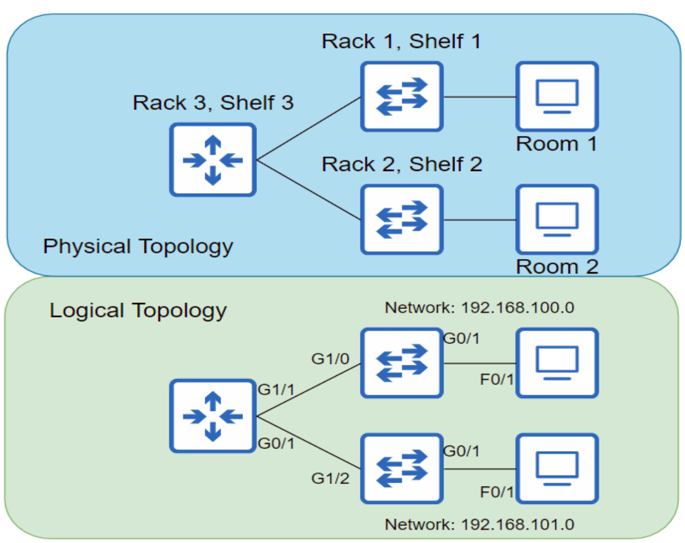
Mesh topologies. Using a mesh topology, every device is connected through a dedicated point to point link. When we say a special emphasis, that means. that the transmission of data between two connected devices is only occurring. The advantages of a mesh topology are that since every device has its own dedicated link, it will eliminate the possibility of congestion and also that it is reliable robust as one link failure won't affect the whole system, and it is easy to detect failures. The best quality of this structure is that it provides the highest security because it has a point to point link. The disadvantages of this product include the number of wires required, and its scalability issues.

a great many individual devices and the number of I/O ports needed due to the number of different devices communicating with each other.

Finally, hybrid topologies A hybrid network design includes two or more ideas. The benefits to our product are that you can choose the topology you need. We can provide a technological platform that can further connect computers and networks. The disadvantages of these are that they are difficult to install, faults are difficult to detect, expensive and overcomplex.

There are two settings of the network topology visualization. One includes physical topology diagrams, while two includes logical topology diagrams. These two diagrams are those used to illustrate how the network is organized and installed. A physical topology map shows where all the devices are physically located, while a logical topology map shows all the devices, ports, and addressing scheme. Figure 5 shows how physical and logical topologies differ.

Figure 6 (Physical and Logical Topologies)



CHAPTER 2

TCP/IP MODEL

CHAPTER 2 (TCP/IP Model)

TCP/IP Networking Model

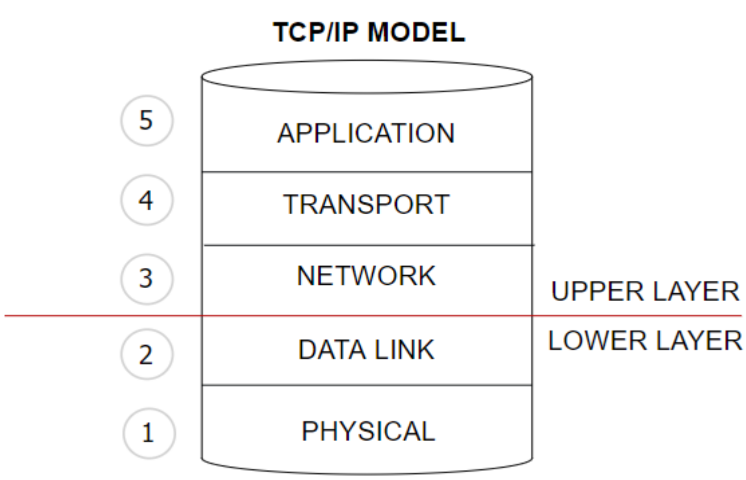
A networking model, referred to as a networking blueprint or network architecture, describes the requirements needed to make a computer network work. Some documents describe the use of a variety of network protocols, which describe a set of rules a computer must follow to communicate with other devices. Specs for cables may also specify the type of cable and cable length needed for a network to function properly.

You can think of networking as a blueprint for how you will build yourself. Just like a blueprint for an architectural project, a blueprint for a computer network is also required to create a computer network that can function. In addition, a network blueprint provides the necessary components for a network to function and to achieve its purpose. In the same way that architects can build a network from scratch, so can you design and build your own personal network from the ground up. It is also easier for you to buy networking products from the same manufacturers.

Overview of the TCP/IP model

Like any other networking model, TCP/IP was developed by a vendor. TCP/IP was created by the United States the Department of Defense during the 1970s. The TCP/IP protocol model describes a huge collection of networking protocols, allowing for multiple communication options. protocols defined in the Request for Comments to define a set of protocols. TCP/IP defines its own proprietary protocols and avoids using works that were already done by other vendors, e.g., Ethernet standards that were developed by the Institute of Electrical and Electronics Engineers (IEEE).

Figure 7 (TCP/IP model, layers)



To help people fully understand TCP/IP, I will divide the TCP/IP protocol into smaller layers. Each category defines its own protocols and standards. Figure 4 illustrates the progression of TCP/IP Version 4.

As shown in Figure 4, the TCP/IP model has all the layers defined. The TCP/IP model has fewer physical layer protocols compared to the OSI model. The focus of this paper is on how data is traveling throughout various networks and devices. In contrast to the higher levels, it focuses on the level of application and how the interface is used.

The TCP/IP model refers to a set of communication protocols that were developed so that devices can communicate with one another. As shown in figure 4, the various protocols of the TCP/IP model are described below.

Figure 8 (Example protocols that are defined on each layer)

TCP/IP Layers	Example Protocols
Application	HTTP, POP3, SMTP
Transport	TCP, UDP
Network	IP, ICMP
Data Link & Physical	Ethernet, 802.11 (Wi-Fi)

TCP/IP Application Layer

The application layer of the TCP/IP model forms the very first layer of the OSI model. The layer of the TCP/IP model that defines our computer system's services and applications, among other things. Even though the application layer defines what an application can do, the application layer is not the defining factor of an application's function and functionality. The application may utilize varied communication systems in the form depicted by Figure 5. As an example, the application layer consists of multiple protocols used on different applications, such as HyperText Transfer Protocol (HTTP), Post Office Protocol version 3 (POP3), and Simple Mail Transfer Protocol. (SMTP).

In the TCP/IP model, the presentation layer is unacknowledged, but acknowledged by the session layer. It is crucial to understand the purpose of these layers to understand the process at hand. The presentation layer is primarily responsible for the translation and presentation of data. It also compresses data and reduces its size so that it can be transmitted faster.

Finally, the tablet helps encrypt data for security purposes. The encryption enhances the security and privacy of the data.
The session layer of the OS is very straightforward. It is an intermediate link involved in handling sessions between source and destination. To start a session, handle the exchange of data, ensure performance by keeping the session active, or reset when disrupted, and to terminate the session when the data exchange is complete. It is accountable for keeping track of its communication modes: plaintext, half-duplex, full-duplex. Modes are further discussed in the following Chapters.

The web browser is the most commonly used application in the TCP/IP model. Web browsers make use of the HTTP/s protocol to pull out contents off from a web server and be able to view the website to our web browsers, such as our favorite social media websites like Instagram, Facebook, Twitter, and such. We will give you a general overview of the Hypertext Transfer Protocol (HTTP), one of our most well-known application protocol on the TCP/IP model (HTTP).

HTTP Overview

To start, it would be beneficial to give a brief introduction of the overall topic. How are we really affected when we attempt to view a website? How does a web browser know what makes up a website?

For example, the user wants to view a webpage from the server of Larry. Bob used a web browser configured to view the home page from the website of a different person. The process will look like Figure 4.

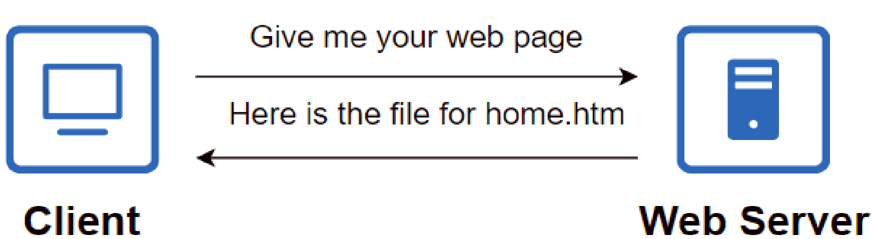


Figure 9 (Basic logic to pull out the contents of a webpage using HTTP)

Simple HTTP logic

In order to simplify, Bob's computer opens the browser for the browser. Bob is then browsing the web on his computer from Larry's computer. Bob's computer first sends an initial request to the website host asking for the homepage of home.htm.

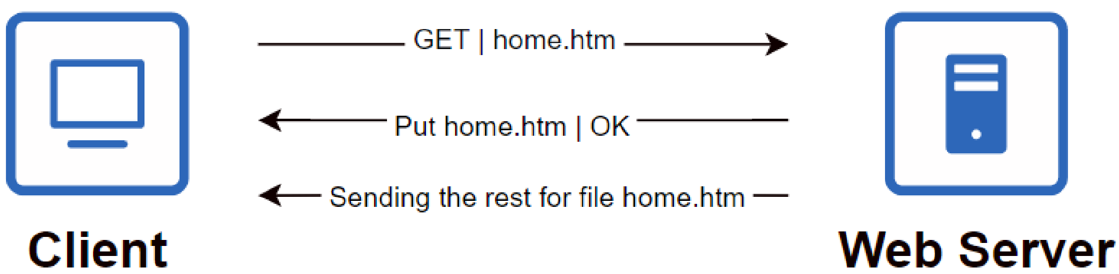
Larry's web server After this, Larry's web server would see the request. After receiving Bob's request, Larry's web server would send the contents of the document to Bob's computer.

For Bob's computer to receive the contents of the webpage, the webpage must first be transferred to Bob's computer.

Additional Information (HTTP)

To better understand how these kinds of restrictions work, let us refer to the image in Figure 7. The following texts discuss the same ideas as the first, but in more depth and detail.

Figure 10 (More detailed explanation of figure 8)



As suggested in Figure 7, we can see that the diagram consists of 3 steps. We will describe additional details as needed on the following text. The steps in the HTTP/s cycle include the GET, POST, and PUT processes.

As in step 1 of Figure 7, the situation is similar. Bob's browser is set to fetch content from Larry's server. In order for Bob's web browser to get the information from that webpage, he has to send an HTTP header containing a "get" with additional information specifying what piece of content is being downloaded. If a request is addressed to an unknown filename, servers generally assume it is for the default page.

In step 2 of figure 7. Once the server received the client's request, the server would acknowledge the request by replying with the code (200) which means that the server received the request successfully. What if the response wasn't acknowledged or found? If the web server failed to find the “Get” request it would respond with an HTTP 404 error code. If ever you receive this, it means that the web page was not found, or that the request was unsuccessful.
Step 2 in Figure 7. When the webserver acknowledges the “get” request. It will, at the user's next request, send the contents of the requested web page. Figure 8 shows the third step of the process which involves sending the contents of the home.htm file to.

It is made available to the client. The contents are also sent through an HTTP header, but of course, all contents can't be fitted in a single HTTP header, so the webserver would send it by

using multiple HTTP headers at the same time, in a certain order, and organizing them sequentially.

TCP/IP Transport Layer

The transport layer provides information about transmission of data over the internet. The transport layer exists only under the application layer and has reduced functionality compared to the higher layers. The transport layer uses two protocols for data transmission. Some protocols include Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) (UDP). This chapter covers two protocols found in this chapter. We will also cover all the features of TCP.

The transport layer speeds up the transmission of data by segmenting and reassembling data. Segmenting and reassembling the data into data streams allows the transport layer to prepare the data before it's sent, and to also verify the entire data stream was sent successfully. It facilitates linkability between applications and acts as a temporary session between applications. The transport layer also contains features that greatly support the data as it transverses from one endpoint to the other. The following section covers the following features.

Transmission Control Protocol

The Transmission Control Protocol (TCP) is an efficient and reliable protocol. TCP provides a variety records services and mechanisms which ensure reliable performance. Numbering and tracking data segments broadcast to a specific host, acknowledging received data, and retransmitting any unacknowledged data after a certain period of time.

TCP Flags

In a reliable connection, TCP uses the acknowledgment concept. Also, there are other flags used during establishing or terminating communication, in addition to the TCP flags. If you have never heard of TCP flags then you should know that they are traits used in a connection that show the status of the connection. These are the available TCP flags that may be used during a TCP session.

SYN flag – under this is the SYN bit. This is typically used as the first step in connecting to a network device on a computer. The SYN flag is used to request a connection from the other side, also known as SYN flooding.

ACK flag – This flag is used to acknowledge successful sent packets. One of the three steps in handshaking is establishing a connection. When a packet is successfully delivered, this flag indicates it was sent properly to its intended destination.

The FIN flag indicates that the transmission is finished, and no more data is being sent. This technology would allow a receiver to know whether a sender is finished sending packets.

URG flag - This flag denotes information that is urgent. This is a rule that prioritizes certain packets and only allows them to transmit if needed.

Push flags and URG flags are similar, but not identical. This directive tells the receiver to immediately process the packets so they can be sent.

RST flag – Lastly, the reset flag. Informing the sender to reset the process is important. When an unexpected packet is received, this is something that happens.

Connection-Oriented Communication

In a TCP connection, both systems have a connection-oriented communication. For this connection to happen, one must establish a connection-oriented communication or a virtual circuit to be able to transmit data from one side to another, this process is called the t*hree-way handshake* or also known as *call setup*. Once the data transfer is done, the sending device would have to terminate the connection to tear down the virtual circuit. This process is called *the* four-way handshake, or a *call termination* process.

Three-Way Handshake

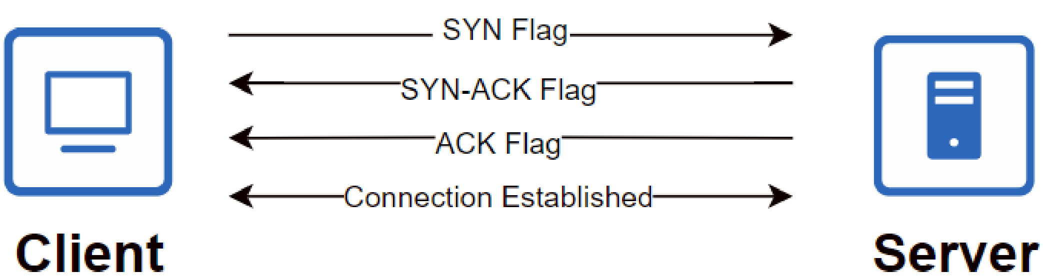


Figure 11 (Connection Establishment)

As illustrated in Figure 8, the 3-way handshake process occurs. Host A is establishing a connection with Server B so that they can transfer data into the other endpoint. In order for the connection to take place, the VC must be established first so it can carry information to the other end.

Step 1: Host A sends a SYN flag to other host (Server). This message is telling the server that the connected device is ready to communicate. If you are to review page 10, SYN is commonly used for establishing a connection with an established host.

Step 3. Once the server received the SYN flag from the sending device, the server then responded by sending an ACK flag to inform Host A that the server finally agreed to establish a connection-oriented connection.

Step 3. Now that the server has agreed to establish a connection, host A then receives the SYN-ACK flag which was sent by the server. This would first inform Host A that the other peer system has agreed with it, and Host A will then send an acknowledgment (ACK) flag which initially informs the other end device that the sender has finally received the acknowledgment (ACK) from the server. At last, after the third step, the connection has been successfully established!

Flow Control

During communication and data transfer, we never expect things to always work smoothly. Congestions occur from time to time during the connection. For example, a high-speed computer system can generate as much data traffic in too short a time to be handled by that system.
but don't worry, TCP has a different feature that can handle these problems. The TCP protocol provides flow control to avoid congestion and manages the amount of data being transferred across the internet between systems.

Flow Control Overview

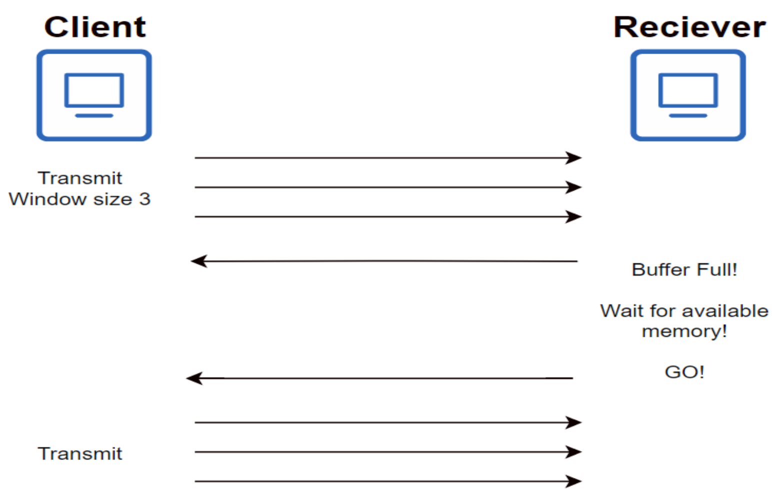


Figure 12 (Transmission with Flow Control)

TCP provides a special network flood control system which forces data to be read at a minimum rate. The concept of TCP flow control helps ensure that the sender does not overwhelm the receiver by sending too many segments into its buffer, and by minimizing the amount of data being sent. More information is available in the following excerpts.

Starting off by sharing flow control's approach to mitigating these kinds of issues. In figure 10, you will see a simple diagram outlining how TCP flow control works. TCP flow control operates more like a traffic light, switch, or stoplight-styled mechanism. When the buffer gets full, the receiving device sends out a “not ready” message which warns the other end that the buffer is full, and that the receiver is not ready to receive packets. If the buffer ever runs out of room, it would send a signal indicating that a message can be sent.

Flow Control Windowing

TCP/IP relies on the concept of windowing. TCP windowing helps to alleviate congestion by increasing the size of packets or adjusting the window size.

Header The windowing option begins by informing the sender how many bytes of data can be transmitted in a certain period of time before waiting for an acknowledgment.

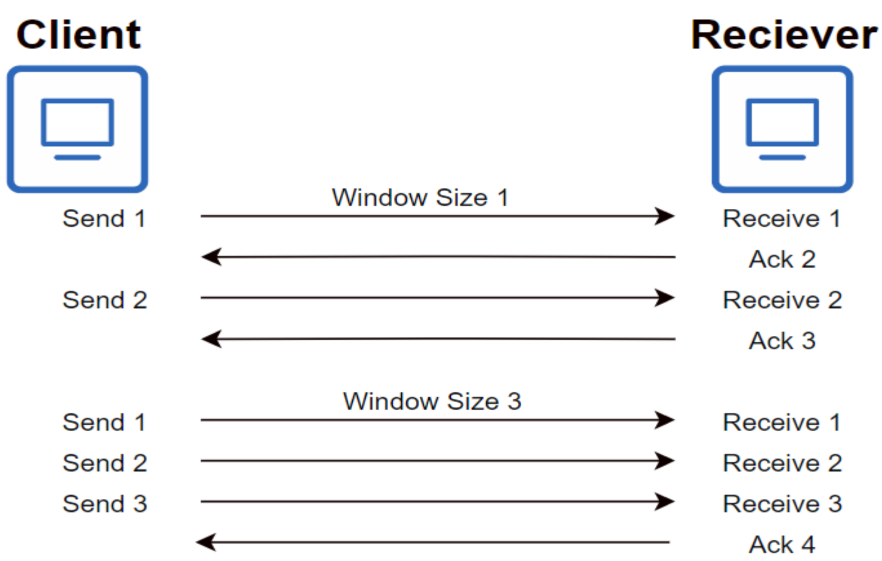


Figure 13 (Windowing Concept)

At the same time, the throughput would be minimal if we have to wait for acknowledgment for each segment of code. With windowing, TCP is able to reduce the number of segments the server sends. Window size defines when to expect an acknowledgment before completing a transfer. The first figure has a window with a size of 1. This means the sender had only 1 item to send.

data segment is sent before the acknowledgment is received after the transmission is completed. The second figure has a window size of 3, which allows the sender to send 3 segments then wait for acknowledgment before sending subsequent segments. This process repeats for many times until it is complete.

To summarize, windowing initially defines how much data a sender can send before the receiver acknowledges, and before sending the next set of segments. This is to limit the number of data transmissions in order to prevent overwhelming the receiver.

TCP Error Detection/Recovery

Since TCP is a reliable transmission protocol, all data must be received and acknowledged by the receiving host as it passes along the internet. In addition, TCP ensured the delivery of data across the network. TCP (Transmission Control Protocol) has a feature that can detect errors and recover lost data segments.

Consider this scenario. Let us go to the topic of the HTTP process. When Bob browses the Internet, his web browser retrieves the contents of the home.htm webpage from the website Larry operates for him. In Figure 12, the Web server has now begun sending the document's contents to Bob's web browser. What if news data is lost by the time it reaches the user? If this did not happen, the website's content would not have been accessible.

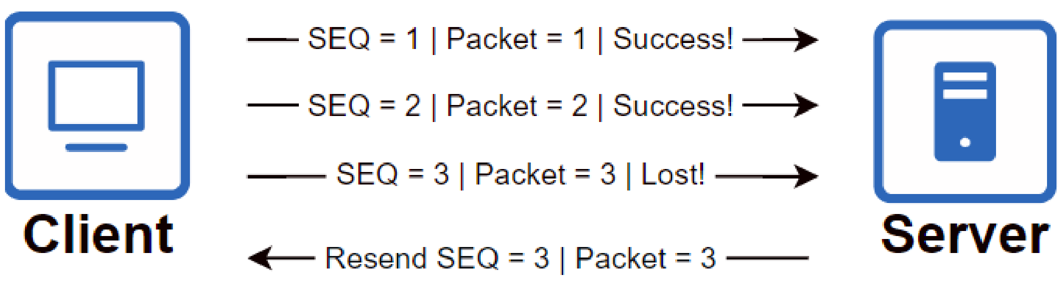


Figure 14 (TCP Recovery Concept)

Here is a diagram illustrating the TCP recovery protocol to achieve this goal. Same scenario. The HTTP request was lost throughout transmission. How can data be recovered? As shown in Figure 11, all of the first three bytes were successfully received. However, the second byte could not be received If the data sent was received, an acknowledgment message would be sent to inform the sender of the receipt. Knowing that one of the data segments was missing, the receiver would have received it. The TCP protocol uses a sequence (SEQ) system. This is implemented

3. The receiver will know that sequence two is missing. That realization led Bob to request that sequence 2 be re-sent.

Same-layer and Adjacent-layer Interactions

Figure 12 shows how adjacent layers interact. Why? Between subsequent layers, the upper layer uses the services provided by the lower layers to commit some prerequisite requirements. Just like in the figure, the HTTP protocol has a recovery services that will attempt to recover lost packets.

On the other hand, the figure demonstrates the role that a particular layer plays. This happens when two computer systems with the same operating system layer want to communicate with each other. Bob's browser sent the data with a TCP header that requested more data from the server.

Figure 15 (Summary: Same-layer and Adjacent-layer Interactions)

Concept	Description
Same-layer Interaction	Each peer systems uses a protocol to communicate with the same layer for both sides. This protocol defines a header that provides instructions.
Adjacent-layer Interaction	On a single computer, lower layers provide services to the layers above it. They are responsible to provide its needed functions/requirements.

TCP Header

Figure 16 (TCP Header)

<table>
<tr><td colspan="2">16-bit source port</td><td colspan="2">16-bit destination port</td></tr>
<tr><td colspan="4">32-bit Sequence number</td></tr>
<tr><td colspan="4">32-bit Acknowledgement number</td></tr>
<tr><td>4-bit header length</td><td>Reserved</td><td>Flags</td><td>16-bit Window size</td></tr>
<tr><td colspan="2">16-bit TCP checksum</td><td colspan="2">16-bit urgent pointer</td></tr>
<tr><td colspan="4">Options</td></tr>
<tr><td colspan="4">Data</td></tr>
</table>

The Transport Layer protocol specifies how data segments are transmitted through the internet. TCP's header size is larger than UDP's, at 20 bytes. This figure shows an example of a packet format. This information is used to support the data in this segment.

Fields:

Source port - Used to identify the application that is sending data from the source host.

Destination port - Used to identify the application that will receive the data at the destination host.

Sequence number - Used to identify the lost segments and maintain the sequencing during transmission.

Acknowledgment Number - Used to send a verification of received segments and to ask for the next segments.

Header Length - A number that indicates where the data begin in the segment.

Reserved - Reserve for future use. Always set to zero.

Code bits - Used to define the control functions such as setting up and terminating the session.

Window size - Used to set the number of segments that can be sent before waiting for a confirmation from the destination.

Checksum - CRC (cyclic redundancy check) of the header and data piece.

Urgent - Used to point any urgent data in the segment.

Options - Used to define any additional options such as maximum segment size

Data - A data piece that is produced from the segmentation

4 Way Handshake

The ultimate discussion regarding TCP concludes with the 4-way handshaking protocol. This is the process of disconnection when both peer systems have finished communicating. See the diagram for an example of the four-way handshake.

Figure 14 shows the 4-way handshake process. That 4-way handshake is the protocol used to end a TCP connection. This describes in detail the process by which a connection between two systems is closed. Here is a detailed step-by-step process of how this process works.

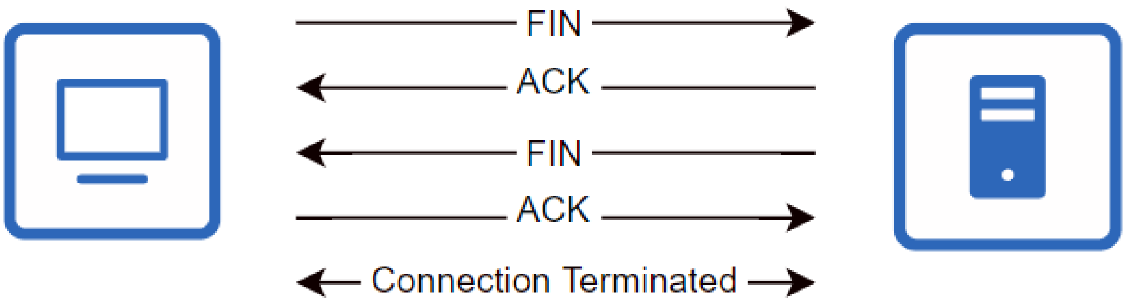


Figure 17 (4-Way Handshake Process)

Step 1. When the sender has nothing more to say, or is about to close, they will indicate this with the FIN (finished) flag. The sender indicates that they are finished with the communication and would like to terminate the relationship.

Step 2. The receiver would receive the FIN request once it was completed. I will send a confirmation (ACK) back to show that I have received your request. Notice the two flags received from the receiver.

Step 3. The receiver is required to send a FIN flag to notify the other system that the connection is no longer active.

Step 4. The last step in the termination process is adjudication. If both the sender and receiver each receive a flag indicating a termination of the session, the sender knows that both are ready to terminate the session. The sender would send an ACK flag in response to the NTP's NTP request to close the session.

Once the four steps are completed, a virtual circuit is terminated which prevents it from occurring again. The four steps of how two computer networks are connected together.

User Datagram Protocol

User Datagram Protocol, or UDP, is a high-speed data transmission protocol. UDP is used to establish low-latency and loss tolerant transfers between applications on the web. UDP provides a best-effort transport protocol that has no reliability and flow control, but has a similar data segmentation and reassembly as TCP. UDP has a simplified layer, but without the overhead of TCP due to the simpler transmission method.

Once all data segments have been received, UDP does not reassemble data in order. Data may be interpreted as the order it was received and immediately forwarded. UDP does not use sequence numbers like TCP, only the RDNN. UDP has no way of relaying the datagrams back in the order they were sent.

16-bit Source port	16-bit Destination port
16-bit Length	16-bit Checksum
Data	

Figure 18 (UDP Header)

User Datagram Protocol (UDP) also has a header field, similar to the TCP header. Although UDP has less bytes than TCP, it carries a smaller data payload than TCP. The plot in the figure above depicts the UDP header. Due to the removal of some headers, the UDP header contains fewer bytes than the TCP/IP header.

Fields:

Source port - Port number of the application that is transmitting data from the source computer.

Destination port - Port number of the application that will receive the data at the destination.

Length - Denotes the length of the UDP header and the UDP data.

Checksum - CRC of the complete segment.

Data - Data which it received from the application.

TCP/IP Network Layer

The highest level of the TCP/IP networking model is the TCP/IP network layer. This layer provides many features so that end devices can exchange data throughout the network. This service includes addressing: allocation of unique IP addresses, data encapsulation: the process in which we add IP header information which supports the data as it is transmitted across the network, de-encapsulation: the removal of IP header inside the data for examination after arrival to the destination, and lastly, routing: the selection of best path to route the packet across the network. These services are mentioned later in the paper. The TCP/IP model also consists of multiple network layers with other protocols similar to the others, such as the Internet Protocol that exists in the Internet layer (IP). We have two.

Though there are several types of IP according to their versions, IPv4 and IPv6 are discussed later on. Internet Protocol, a network layer protocol mainly designed with low overhead, is used to provide needed information to support data as it is being delivered from source to destination over an interconnected system of networks, although, IP is not designed to track or manage the flow of packets. IP is also known as the Connectionless mode, Best effort, and media-independent. The following characteristics are mentioned as follows.

Characteristics of IP

IP is known to have a connectionless nature. It doesn't have any connection with the I.P address which means that IP doesn't know whether the data has reached the destination, and doesn't know whether it has been received by the intended user or not.

IP also has its reputation for its best effort delivery. Best effort delivery means no guarantee of delivery, which means IP doesn't guarantee receipt of all packets. There is no method for recovering corrupted or lost packets as they pass through the network. Ip provides location information about the destination without revealing the identity of the packet sender.

IP is understood both in wireless and wired mediums, so it is media independent. IP carries data across the network independent from other networks. The TCP/IP data link layer is responsible for processing and transmitting IP packets across a medium, therefore, IP is not limited to a specific transmission medium. However, the networking layer takes into consideration of the maximum number of frames that a medium can support (MTU). Due to the way the Internet works, packets are sometimes split up into smaller pieces and reassembled on the destination before being sent. The process has been known as fragmentation.

IPv4 Overview

Just like TCP and UDP, and IP packet in several important fields pertaining to the packet the packet holds. An IPv4 packet header consists of 32 bits and contains many fields including the version, destination-specific, time-to-live (TTL), protocol, source, and destination IP addresses. The following information is discussed further in the following section. The diagram below shows the different sections of an IPv4 packet.

NOTE: More information about IPv4 and IPv6 given in the following pages.

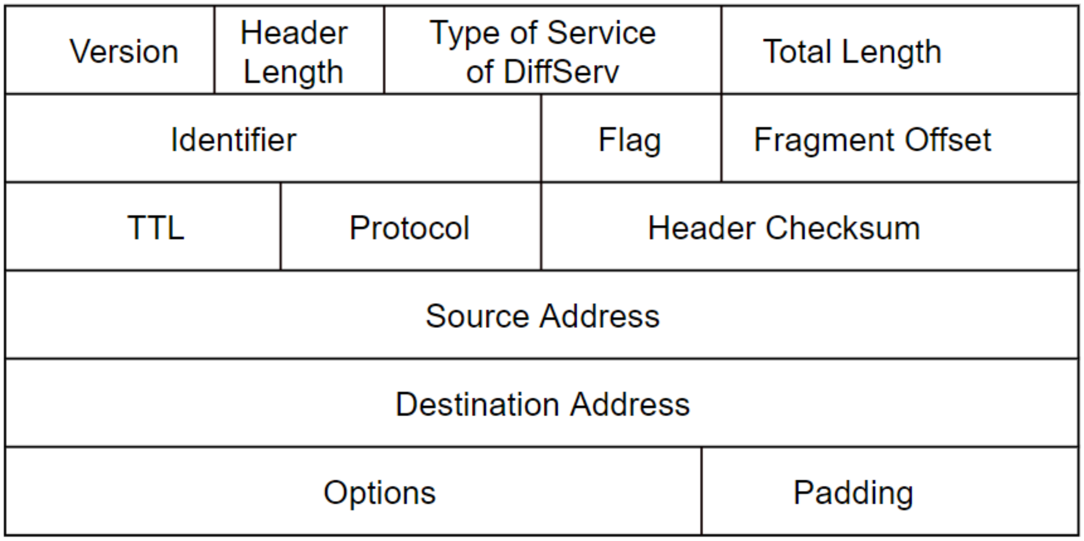


Figure 19 (IPv4 Packet Header, Fields)

Version - Contains a 4-bit binary value set to 0100 that identifies this as an IP version 4 packet.

Differentiated Services or DiffServ (DS) - Formerly called the Type of Service (ToS) field, the DS field is an 8-bit field used to determine the priority of each packet. It is used to carry information to provide quality of service features. New technologies are emerging that require real-time data streaming and therefore make use of the DSCP field. An example is Voice over IP (VoIP) that is used for interactive data voice exchange.

Time-to-Live (TTL) - Contains an 8-bit binary value that is used to limit the lifetime of a packet. The packet sender sets the initial TTL value, and it is decreased by one each time the packet is processed by a router. If the TTL field decrements to zero, the router discards the packet and sends an Internet Control Message Protocol (ICMP) Time Exceeded message to the source IP address.

Protocol - Field is used to identify the next level protocol. This 8-bit binary value indicates the data payload type that the packet is carrying, which enables the network layer to pass the data to the appropriate upper-layer protocol. Common values include ICMP (1), TCP (6), and UDP (17).

Source IP - Contains a 32-bit binary value that represents the source IPv4 address of the packet. The source IPv4 address is always a unicast address.

Destination IP - Contains a 32-bit binary value that represents the destination IPv4 address of the packet. The destination IPv4 address is a unicast, multicast, or broadcast address.

The Internet Header Length (IHL), Total Length, and Header Checksum fields are used to identify and validate the packet. Other fields are used to reorder a fragmented packet. Specifically, the IPv4 packet uses Identification, Flags, and Fragment Offset fields to keep track of the fragments. A

The router must fragment a packet to another medium which has a smaller maximum transmission unit.

Limitations of IPv4

As we are all aware, IPv4 has its own limitations, given that IP addresses are set to exhaust. The expansion of the Internet routing table which stores information used by routers to determine the best routes. As more routes are being stored, the intermediary device's memory and resources are gradually being consumed as tons of routes are being stored. Lastly, without complete end-to-end connectivity: this is due to the use of Network Address Translation (NAT), which enables multiple devices sharing a single public IP address, but these addresses are shared, therefore, the IPv4 address of an internal network host are hidden. This is an issue with technologies that require full connectivity over the Internet.

IPv6 Overview

The Internet Protocol version 6 addresses many disadvantages of IPv4. This is because IPv6 is a new protocol that has more advanced features that make it better than IPv4. IPv6 was manufactured with further enhancements having more address space: IPv6 addresses are based on 128-bit hierarchical addressing as opposed to IPv4 with 32 bits, improved packet handling: The IPv6 header has been simplified with fewer fields, and lastly, it eliminates the use of NAT: IPv6 has a much larger quantity of public IPv6 addresses, eliminating the use of NAT, therefore, avoiding and minimizing issues experienced by applications requiring end-to-end connectivity.

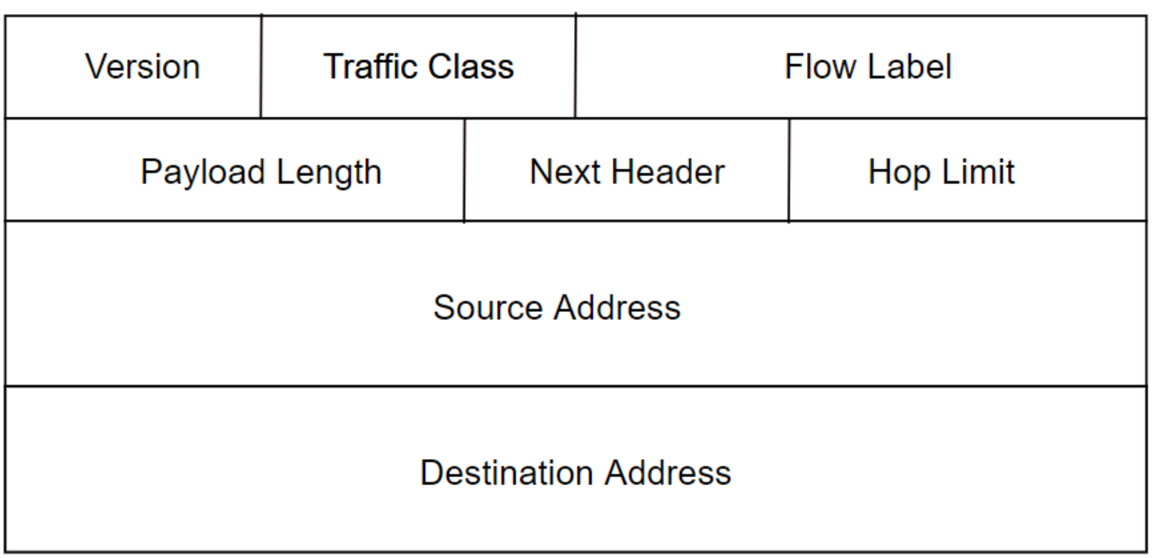


Figure 20 (IPv6 Packet Header, Fields)

One of the most significant aspects of IPv6 is how its structure is more simplified and efficient. The simplified IPv6 packet header offers many advantages over IPv4 including better routing efficiency, efficient packet handling, and scalability in performance and forwarding rate. No need to process checksums.

With respect to IPv6, the structure is much simpler and more efficient. The figure presented in figure 17 demonstrates the area within the IPv6 packet header. In the IPv6 header, this field includes:

Version - This field contains a 4-bit binary value set to 0110 that identifies this as an IP version 6 packet.

Traffic Class - This 8-bit field is equivalent to the IPv4 Differentiated Services (DS) field.

Flow Label - This 20-bit field suggests that all packets with the same flow label receive the same type of handling by routers.

Payload Length - This 16-bit field indicates the length of the data portion or payload of the IPv6 packet.

Next Header - This 8-bit field is equivalent to the IPv4 Protocol field. It indicates the data payload type that the packet is carrying, enabling the network layer to pass the data to the appropriate upper-layer protocol.

Hop Limit - This 8-bit field replaces the IPv4 TTL field. This value is decremented by a value of one by each router that forwards the packet. When the counter reaches 0, the packet is discarded, and an ICMPv6 Time Exceeded message is forwarded to the sending host, indicating that the packet did not reach its destination because the hop limit was exceeded.

Source IPv6 Address - This 128-bit field identifies the IPv6 address of the sending host.

Destination IPv6 Address - This 128-bit field identifies the IPv6 address of the receiving host.

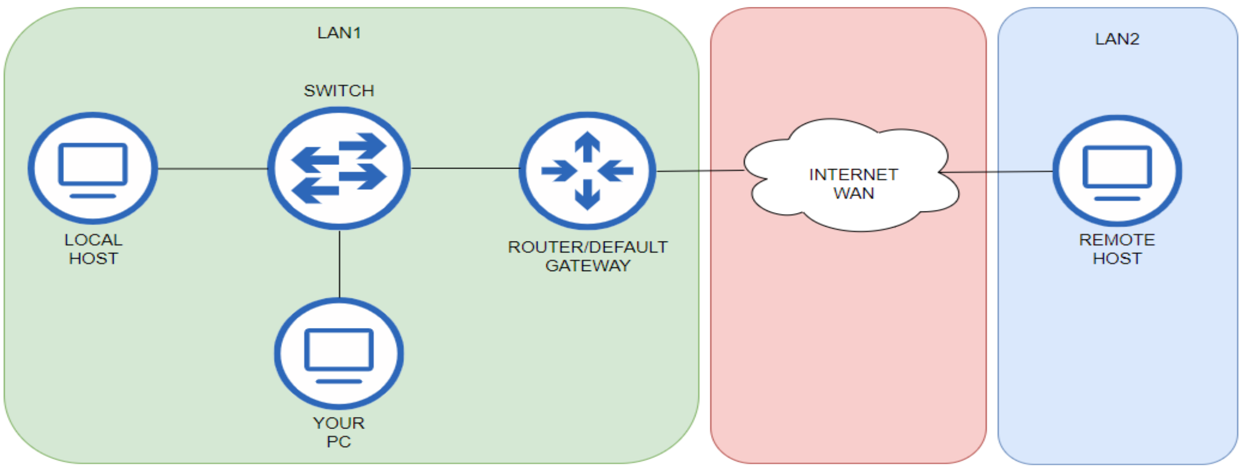
An extension header may be included in an IPv6 packet (EH). This provides network information that can be used for Internet fragmentation, security and mobility, and more. Unlike previous IPv4 protocols, IPv6 routers do not fragment routed packets.

IP address can thus be acquired through multiple means. IP addresses can be gathered statically or obtained dynamically. You can manually configure an IP address on a device, but you can acquire IP addresses from devices through protocols. The most widely used method of dynamic address assignment is DHCP (DHCP). More is said on static and dynamic addressing in the book.

Routing basic overview

The TCP/IP layer is also well known for handling packet routing and directing messages from specified sources. (Routing is discussed further below). When forwarding packets, a host can send packets from any location. A computer could send a packet to itself by using a specialized IP known as the loopback interface. (127.0.0.1), primarily being used to test a computer's TCP/IP protocol stack. A host could locally send a data packet which can be shared with other hosts in the same network (local). Lastly, it can also send out packets remotely to a host across the same network and/or across different networks.

Figure 21 (Sample illustration)



A packet, whether it is to be sent locally, remotely, or to itself, the TCP/IP network layer use IP addresses and subnet masks, mainly functioning as an identifier for the packet during packet routing and forwarding.

If the packet were sent locally, it would be sent through the network to an intermediary device to be routed to its proper destination. Whereas, if a packet is to be sent from one network address to another network address, routing must be performed. We would route data outside a network through a layer 3 intermediary device called a router (routers are responsible for accepting packets inside the network, and routing packets outside the network). This process is known as routing. Routing is the process of identifying routes to our destination. Usually, a router at the local level is referred as the default gateway.

A router is a network device that can route traffic based on the network it's connected to. In order to think things through, our network is a door that allows external packets to enter and also sends out internal packets to other networks. One IP.

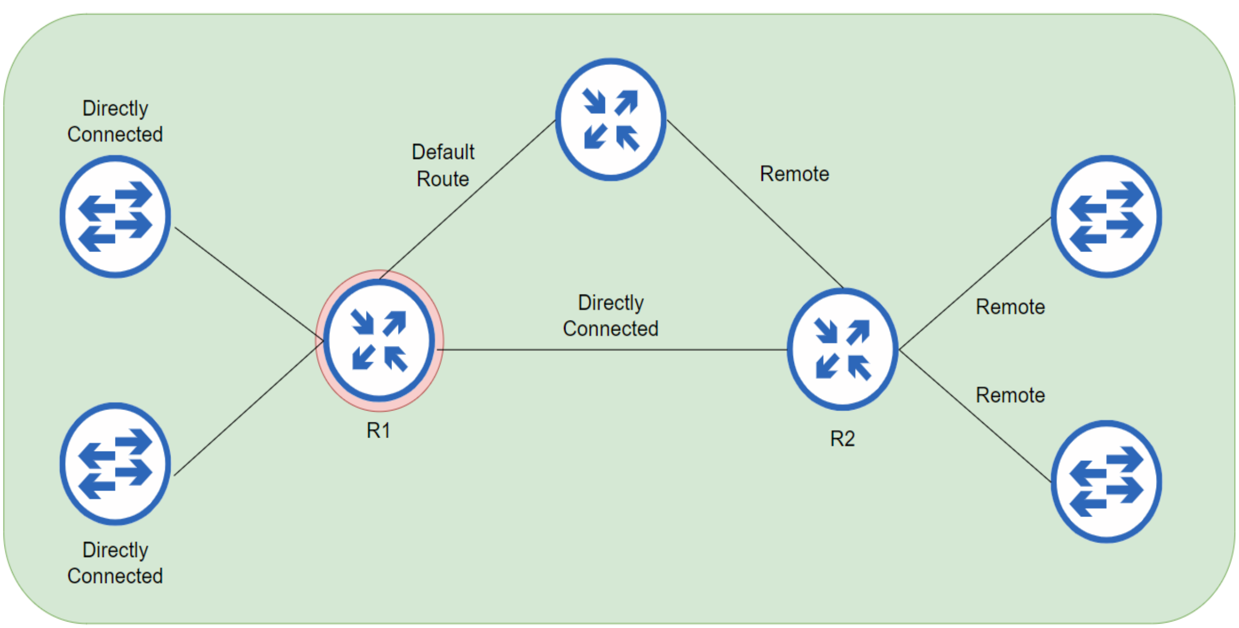
an address can be noted as a person who is in a room. If the network's default gateway is not known, it is not possible to go outside the local network, and vice versa. The default gateway is an essential component utilized for remote access to hosts.

After being able to take in the basic overview of how host forwarding decisions work, let us further understand how these packets are sent from host to host inside and outside network. Clearly, when a host sends a packet from one system to another, this must go through various procedures. A router's IP addressing assignment table is a type of table called a routing table. This routing table consists of the routing information commonly used to determine the best path a packet takes to reach its location.

There are three major types of routes that you must become familiar with when it comes to generating route tables. These paths are direct, remote, or default. Directly-connected routes are directly-connected router interfaces that require inbound and outbound transit. Remote routes are routes that are independent of dedicated facilities. Finally, default routes Default routes are used only when last resort are required. This is useful in situations when no other options exist to reach the destination network.

Figure 21 shows the different roadway types. Network 1 comprises of the main routers. All links that are directly connected, and any links that are connected only by means of other links, are considered as part of a single route. The second link, R2, is configured as a default route, meaning, all packets that don't match a route will be sent through the default route.

Figure 22 (Sample illustration)



Network Layer Summary

The network layer supplies the IP packet header with the source address and destination address, together with an associated port number, to make the data as the packet is being routed across the network. For layer 2 routing, the receiving node's decision to choose the path of the packet depends on the packet header's destination IP address. Similarly, the packet header's source IP address is also being used to determine the best path for delivery where the network is using layered switching approach.

The router should be trusted to retrieve information from the network, and based on that information, should make a decision about what action to take. We need to know that IP addresses are used to make sure that the packets are heading to the correct place in the network. For more information, as you advance through this guide, you will find how the payment information is routed.

Data link layer

The data link layer of the TCP/IP model is located beneath the network layer. It's responsible of providing access to the upper layers, preparing frames on or before transmission through the media, and lot's more. It is mainly responsible for exchanging ethernet frames between source to destination over physical medias. The following information will provide you a brief introduction regarding the data link layer.

The data link layer composes of two sublayers: Logical Link Control (LLC) and Media Access Control (MAC). The LLC enables the upper layers to be able to interact with the lower layers. It provides specific information which identify what protocol to utilized for the frame as before it is transmitted over the medium. As opposed to the MAC, it is responsible of handling or taking care of frame as during transmission. It also provides an information, specifical a hardware address or what we call the MAC address which was manufactured by your Network Interface Card (NIC) as an address identifier and access various network technologies. In addition, the MAC also has capabilities to interact with wireless technologies such as Wi-Fi and Bluetooth for transmission.

Encapsulation and De-encapsulation process

On or before a packet is sent outside a network, one must hold information to initially guide it as it being transmitted over the internet. Inside a network, a single data composes of multiple information. As the data goes through each layer, each layer provides a header containing supporting information. The process of adding headers of each layer to a data is what we call the “encapsulation” process. As opposed to “de-encapsulation”, it’s the way around. It is responsible to tear down the headers to be viewed by the receiver. Encapsulation occurs on the sender’s side, while de-encapsulation occurs on the receiver’s side. Process is discussed furthermore in the following block of texts.

The method used to submit data using TCP/IP can be separated into five stages. The first four stages of the encapsulation performed by the four TCP/IP layers are delineated and evaluated. The phase is the actual data transfer from the host to the target. In reality, over 50% of people use the five-layer. The TCP/IP model illustrates one tier in the sequence of layers. The steps are defined below:

Step 1 Create and encapsulate the application data with any required application layer headers.

Step 2 Encapsulate the data supplied by the application layer inside a transport layer header.

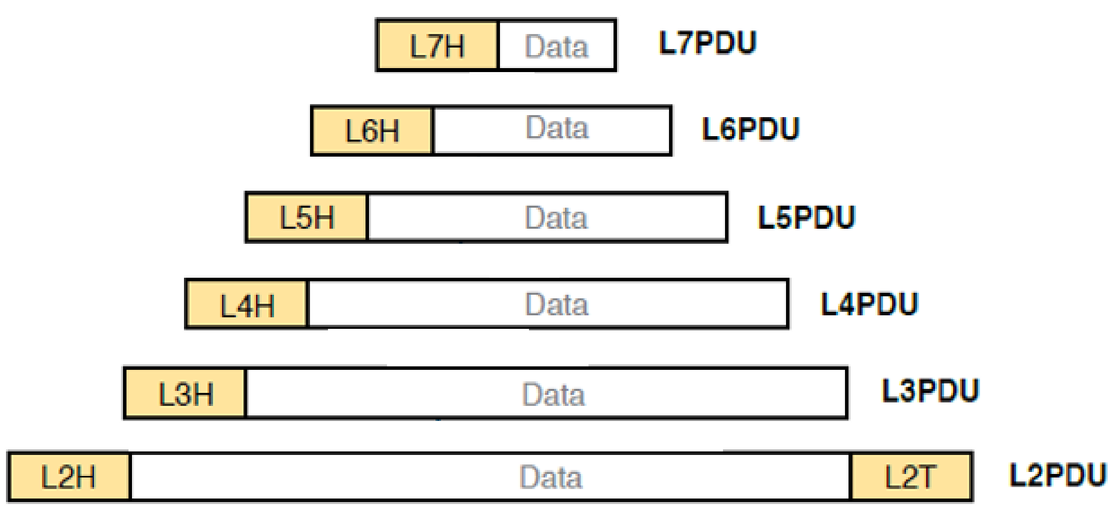
Step 3 Encapsulate the data supplied by the transport layer inside a network layer (IP) header.

Step 4 Encapsulate the data supplied by the network layer inside a data-link layer header and trailer.

Step 5 Transmit the bits. The physical layer is used to encode a signal into the medium. Convey the definitions.

One explanation this chapter spends considerable time demonstrating the steps involved in encapsulation because of the terminology. When explaining the mechanism of networking, people refer to segments as packets, and frames as notifications. These are called Protocol Data Units (PDU) that encapsulate different data and correspond to the headers and/or trailers specified by a specific layer, and the data following the header. The words, though, vary a great deal. For instance, section for the actual layer, packet for the data link layer, and frame for the network layer.

Figure 23 (PDU’s)



Physical Layer Overview

The TCP/IP data link layer offers the means to route the bits in a frame from one network medium to another. The Physical layer embraces a full frame from the application layer and encodes it as a set of signals that are broadcast into the local network medium. The parts that make up a picture are obtained by the matching units.

There are three simple means of grouping various media styles. The physical layer creates the data representation and compression/expansion of bits for various forms of transmitting medium such as:

Copper cable - The signals are patterns of electrical pulses.

Fiber-optic cable - The signals are patterns of light.

Wireless - The signals are patterns of microwave transmissions.

Physical Layer Summary

The Physical layer offers the means for transporting the bits of a data link frame in a network, albeit from the viewpoint of the network. The physical elements involve the electronic hardware equipment, media, and other connectors that send and receive the data that reflect bits. Various hardware elements such as network interfaces, wires, and cable layouts are defined in specifications relevant to the physical layer. The specifications include three distinct types, namely the physical substrate, frame encoding process, and signaling system.

Chapter Summary

In this segment, a simple overview was provided regarding the layers of a networking model. The chapter is composed of five distinct sections, with special facets of them. The Application layer offers the basis for user interaction to the network. The Presentation layer is responsible for displaying the details in its correct format. The Session layer creates, maintains, and terminates sessions between data sources and record storage. The transport layer supports the transport of data from source to destination, with the aid of its various features. The network layer provides network details which provides means to routing data and the internet alongside all of its functions which helps this layer meet its requirements. The data link layer is responsible for the preparation of data before it is transmitted across the transmitting medium. And eventually, the Physical layer encodes data into their correct formats (signal) chiefly appropriate by the medium.

CHAPTER 3
WORK IN PROGRESS
(W.I.P.)

TO BO CONTINUED…