CCNA 201-301 CERT GUIDE

COMPUTER NETWORKING

NETWORKING 101

ROAD TO BEING A CCNA CERTIFIED!

BY FRANCIS G.C.

Computer Networking Introduction

CCNA 201-301

Certification Guide,
Francis G.C.

Network Certificate

I.

COPYRIGHT PAGE

Computer Networking Introduction.
Networking 101, road to being a CCNA Certified!

Front cover image and Book designer: Francis G.C.
Published as an open-source information in the internet.

Writer: Francis G.C.
Inspiration: David Martin

Writer's Signature

II.

BACKGROUND

This document provides you a variety of techniques that you can use to learn Computer networking. Computer networking is a wide-ranging concern since it covers a broad range of fields. This can be daunting for new students; however, this book is intended to help direct students on their learning journey. This will give you a comprehensive understanding of the latest advances in network technology and design.

This document will aid you to understand the fundamentals of computer networks, how local and global networks connect, and how to enhance those we already have. This will also cover the basics and principles of networking for your CCNA 201-301 certification test. This book will help you get started and prepare for your CCNA. I would like to extend my gratitude to David Martin for encouraging me to write this document.

DISCLAIMER

The materials in this book are made freely available for use or adaptation by others. The book is written to help students build a networking curriculum. The information given in this book has been made base from prior knowledge and from multitude resources; reliable and trustworthy.

The document was written using input from people who have accumulated expertise in this area. The bulk of the information was also obtained from both the internet and books.

This document has been written to the highest possible expectations. I will not be held liable for any loss or harm caused to an individual or organization by the information in this book. All pictures are either self-made or cited if taken from the internet so that they do not infringe copyright. The materials in this book are provided for educational purposes only.

III.

WHAT IS CCNA?

The Cisco Certified Network Associate (CCNA) certification applies to a wide variety of technological specializations that Cisco provides to the IT world. These certifications are highly regarded by employers because they show the applicant's proficiency in the profession.

ABOUT THE WRITER

Hello, my name is Francis, and I am person who has high interest on technologies. I'm a high school student, and as a leisure, I expand my knowledge towards technologies and is motivated to write this document in the hopes of assisting students who are involved in studying networking or who want to pursue a career in it. I hope this document is helpful as a source of information.

You can visit me on GitHub to view my other projects:

 https://github.com/FrancisIGP/FrancisIGP

IV.

Table of Contents

Contents undone…

CHAPTER 1
NETWORK FOUNDATION

CHAPTER 1 (Network Foundation)

Initial idea About Networks

One would likely expect that those with no experience in networking would assume that networks are similar to typical household networks that provides free WiFi access to internet users. That's generally true, but there is still a great deal of variation yet to be discovered about networks. In this book, I will be providing you a solid grasp regarding the fundamentals of computer networking, including how they were built, arranged and function in conjunction.

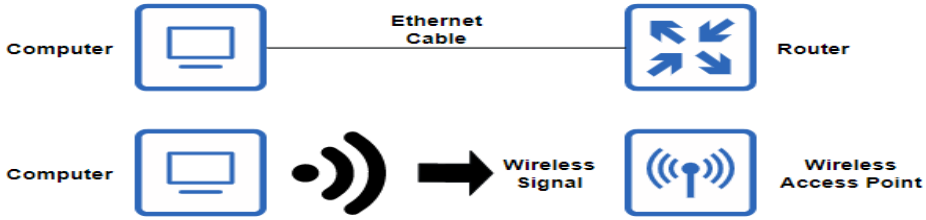


Figure 1 (Basic network diagram)

As illustrated in figure 1, There are two types of discrete networks that we will encounter on today's networks. Wireless and wired. The first figure demonstrates a computer connected through a physical media, known as an ethernet cable. This mainly provides access to the internet with the help of electrical signals. The second figure demonstrates the use of wireless technologies, which utilizes digital signals for communication. Both discrete types have one similarity: to establish a connection from various destinations and allow disparate devices to communicate together.

Fundamental Overview of Networks

A computer network can be depicted in different sizes. It can be as simple as a small home network comprising of few interconnected devices up to a large enterprise network consisting of legions of computers which are administered by organization. An example of network can be two existing computers communicating with each other using a computer language known as binary, which is a set of 1s and 0s arranged in a specific order, identifying what the sender wants to say.

Back in the days, traditional networks used to have separate networks dedicated for each service, each individual network has their own set of rules. This essentially disables them to communicate as a whole. However, in the present, due to network advancement, we were able to converge these networks as a whole and allow them to interconnect with one another without having to worry about building up multiple networks for certain services and data.

According to the dictionary, the definition of a network in general is a set of interconnected people or things. However, in the computer world, it is identified as a collection of interconnected computers that can share resources with one another. These computer systems use protocols which are a set of logical rules that governs on how computers interact which enable effective communication and connectivity between systems. There are numerous types of computer networks defined by their size and function that are discussed later on.

A network infrastructure is built-up of three district categories: hardware, medias, and services. Hardware are usually the physical parts or components that are sensible to the human eye, such as routers, switches, hubs, and medias, medias such as fiber optic cables, copper cables, and such (discussed later on.) And lastly, services which are software applications that provide functionalities to a computer system.

The internet is the world's largest network, also known as the "network of networks", meaning, it's a vast network of interconnected networks. These may come from various sizes and places, such as countries, regions, continents, and so on. The term internet with a capital "I" refers to the World Wide Web (WWW) which you might be familiar of, while the term internet with a lowercase "i" refers to a series of interconnected networks.

Client-Server and Peer-to-Peer

Moving forward to client-server architecture. This is a network where servers and clients exist, as mentioned by its name. This is a much more organized structure compared to peer-to-peer architecture as it's governed by systems known as "servers". Server's, in particular, manages and governing the network. They are extremely powerful, and are, multitasking devices which provides aforementioned services. They are well-known for being superior for having powerful components, such as CPU's, hence it's powerful. They can be a dedicated server that can only perform single task, but they can also be multitasking machines that can perform multiple tasks or services. As for clients, they're the ones who utilizes these aforementioned services. Clients are also known as "end devices".

An end device is a device that obtains an assigned IP address and can be either the source or destination of a network communication. End devices and hosts are usually compared with each other. Well, it's very simple, and end device is any system with an IP address, and a host is any devices that is a part of a network.

Moving on with peer-to-peer (p2p) network. A p2p network is the polar opposite of client-server architecture as everyone inside the network aren't centrally governed. Every device inside a p2p network is all equal when it comes to authority. However, every end device can either be a client which utilizes other's services or a server that provides or shares resources with other systems.

Advantages of peer-to-peer:

- Easy to setup
- Less complexity

Disadvantages of peer-to-peer:

- No centralized administration
- Not as secure
- Not scalable
- Could affect the performance since a device can act as both server and client

Intermediary devices

Within a network, we have special network components known as "intermediary devices" in addition to clients that access networks and servers that deliver these services. Intermediary devices are technologies that link multiple devices within and outside of a network (e.g., Router and Switches.) These technologies use network addresses from end devices to determine the best route for the system to take to reach its intended destination.

Intermediary devices also have the following functionalities:

- ✓ Regenerate and retransmit data if needed (e.g., failed transmission)
- ✓ Store network information and existing pathways in a network. (e.g., routing)
- ✓ Alert's devices when an error occurs.
- ✓ Redirects data to a backup link if a link-failure occurs. (e.g., float routes)
- ✓ Provides priorities to data depending on the configuration. (e.g., prioritizes VoIP)
- ✓ Provides and adds security to the network. (e.g., Access Control Lists [ACL])

NOTE: Don't worry if you can't relate to on some part of this section, because we'll go over it in greater detail later in the book.

Networks nowadays such as traditional networks and business networks can access the internet through different variations. (More context below.)

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

Similarly, as mentioned before, networks use network protocols which are a collection of comprehensive rules that provide means to transmit data. Protocols may include a collection of logical instructions that allow devices to communicate more effectively. Before both devices can communicate and share resources, they must first create and agree on a set of logical rules for successful communication.

Figure 2 (Some network protocols we follow during communication)

As an example, here are some basic rules that a system must obey in order to communicate effectively.

Rule 1, to start a conversation, both endpoints or end devices must agree on which language they will use to communicate with one another. A data must first be encoded into a machine-readable format from the standpoint of a device. Before being transmitted into the media, data will be encoded into bits and translated into the appropriate signal depending on the type of connection.

Rule 2, when a message is sent from source to destination, the data must be formatted in some way. In this situation, data is encapsulated with information (e.g., an IP address) that could potentially support the data as it traverses over the network.

Rule 3, to avoid overflow, missing packets, and other issues, all endpoints would have to have a defined data size. A network normally divides data into smaller chunks to ensure that each packet is received and comprehended.

Rule 4, another point on which both parties must consent is the message timing. Both must understand when to transmit data; if two devices transmit data in the same network at the same time, congestion may occur. Another criterion is flow control, which specifies the speed and volume of data that can be transmitted in a specified amount of time; technical difficulties can occur during transmission if the sender transmits too much data too quickly.

Rule 5, finally, it is worth noting that data can be sent towards a specified number of devices. A data packet, for example, may be transmitted over a single device (unicast), multiple devices (multicast), or an entire network segment (broadcast).

Reliable Network

Figure 3 (Features of a Reliable Network)

In modern networks, a network requires to have these following features to form a good network infrastructure: 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 infrastructures must reduce the impact to the network and also respond to network failures accordingly without interfering its flow. A fault tolerant network provides redundancy to a network 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 backup 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 require fast expansion of users. A good example of a new access method is to have numerous ports for new user access within a network.

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.

Quality of Service (QoS) support prioritizing between time-sensitive data, such as voice and video transmissions, and normal data which aren't time-sensitive.

Lastly, *security*. This is one of the essential functions of a network infrastructure that contributes to peak performance. This prevents data from being corrupted or compromised, as well as unauthorized data access or breaches. Data security ensures that data is in safe hands and is not seen by unauthorized viewers; data integrity ensures that data is not changed during transmission and availability ensures that approved users have timely and secure access to data services.

Network Security Overview

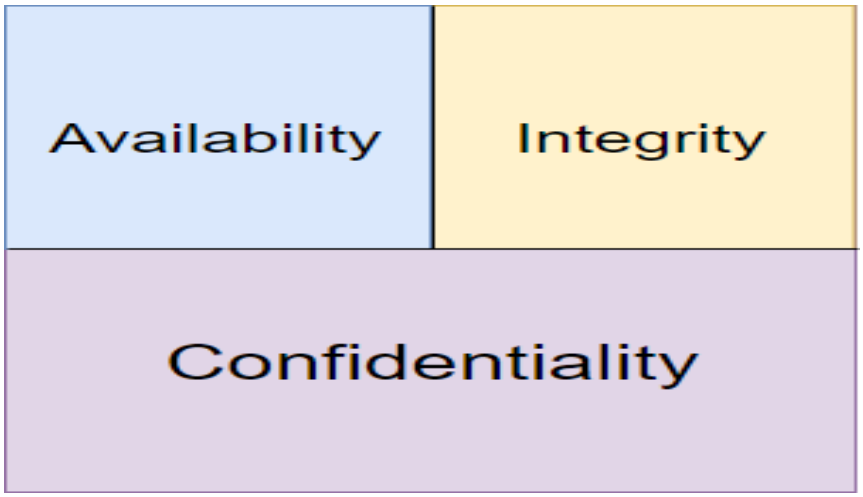


Figure 4 (Security requirements)

Many security threats occur externally and internally. Some common external threats we commonly encounter are the following: Malicious software (malware), Zero-day/hour-attacks, DDoS/DoS, Data theft/interception, identity theft, etc. These are some widely known attacks that occurs frequently. (These attacks are further explained in network security.)

Malware - malicious software and arbitrary code running on a user device as an attempt to collect data, infect, or compromise a system.

Zero-day/hour-attack - an attack that occurs on the first day that a vulnerability becomes known.

Denial of service attacks - attacks designed to slow or crash applications and processes on a network device.

Data interception and theft - an attack to capture private information from an organization's network.

Identity theft - an attack to steal the login credentials of a user in order to access private data.

Security Solutions

Internal protection is critical; safeguarding sensitive assets, such as confidential data and papers, are unquestionably something we should consider. Internal users (e.g., employees) can also be suspects in crimes such as stealing valuable items such as files, computer data, and so on. Essentially,

something that can be done internally that can affect or damage the availability, reputation, and confidentiality of the business.

Furthermore, when it comes to securing networks, whether small or large, there is no single solution. IT Security professionals incorporate various layers of security to provide additional protection. As a result, if a single layer fails, there are still other layers that provide added security.

As we all know, technologies are now advancing, hence internal/external threats also evolve over time, and the same goes for protecting and securing networks. We also look for ways to minimize these vulnerabilities in our systems and manufacture more advanced security solutions in order to improve their overall protection.

For small networks, it is enough to apply rather basic security solutions, as opposed to large networks, it takes multiple security solutions, rather more advanced or powerful ones for better security. (Examples are given below):

Some security solutions for small networks:

- Basic software that provides protection from infected and malicious software by preventing it (e.g., Antivirus)

- Firewall, a simple security feature that blocks unauthorized traffics and filters other network traffics.

Some security solutions for large networks:

- Dedicated Firewall, a more advanced firewall with more features and security.

- Intrusion Detection System (IDS), detect rapidly spreading threats like zero-day or zero-hour attacks.

Network security is something we should consider because it is critical to the safety and privacy of our networks. In large corporations, keeping private data confidential is a major necessity. It is anticipated that all networks will have flaws somewhere, hence, we implement some kind of security in place to prevent unforeseen incidents from occurring (e.g., eavesdropping attacks.) It is also important to remember that the security implementation isn't that simple, as we should consider the network's requirements; it must be adaptable and suitable.

Types of Networks

As previously mentioned, I will cover some well-known network infrastructure, such as PAN, LAN, MAN, SAN, CAN, and WAN, as well as intranets and extranets, as part of the subject.

Common Types of Networks:

The smallest form of network infrastructure is a *personal area network* (PAN). With the help of cellular signals, this form of communication network connects a centralized source to nearby users. Any connected computer within range of one another exchanges data with a central provider. Concentrate on a specific example of a PAN, such as data sharing among devices.

It is also worth noting that this form of network has limited capabilities. Like, when a connected device is too far away from the centralized provider, communication can degrade.

A local area network (LAN) is usually restricted to spanning a particular geographical location; hence, it only provides a limited coverage. The concept is applied to both wired (LAN) and wireless (WLAN) local area network connectivity. A small office/home office (SOHO) network, which is a form of network designed for homes and small offices, is an example of a LAN.

Back in the days, old LAN's can only accommodate at least 30 workstations. However, due to the development of networks throughout the years, the strict limitations for LAN's. For instance, we can now scale a LAN with more than 30 workstations, however large LANs are recommended to consider dividing them into smaller logical zones known as "workgroups".

Workstations, in a low-level perspective, are high-performance computers that are usually manufactured to be employed by a single user. As for workgroups, they are a group or set of computers with no security associations at all.

A *campus area network (CAN)* A campus area network (CAN) is a network that spans multiple buildings. It is the portion of the network that provides data, services, and connectivity to the outside world to those who work in the corporate office or headquarters.

A metropolitan area network (MAN) is a form of network infrastructure that enables computers to share data within a particular geographical area. This network is physically larger than a LAN but is smaller than a WAN (e.g., City, Province). This type of network is usually administered by organizations, corporations, and such.

Private networks known as intranets can also be accommodated by organizations. An intranet is a private network that links computers within a business. It was meant to be accessed only by associated members of the organization. An extranet may also be used by a company to provide safe access to individuals or associates who work for other companies. A business partner is an example.

Wide-area networks (WAN). A network infrastructure that provides connectivity to a large number of people across a large geographical area. Telecommunication is generally in charge of these communications. This is one of the most valuable features of a network because it links various networks. WANs are typically slower than LANs and utilizes router ports and private/public data transmission.

We have two common types of WAN: distributed and centralized. A distributed WAN is an internetwork made up of legions of interconnected computers located in disparate locations. As for centralized WANs, it has a centrally located network where remote computers and devices connect to.

Finally, there are *Storage Area Networks (SAN).* This form of network infrastructure involves high-capacity network devices that has the capability to store and dispense network information, (i.e., file servers.)

3 Tier Architectural Model Overview

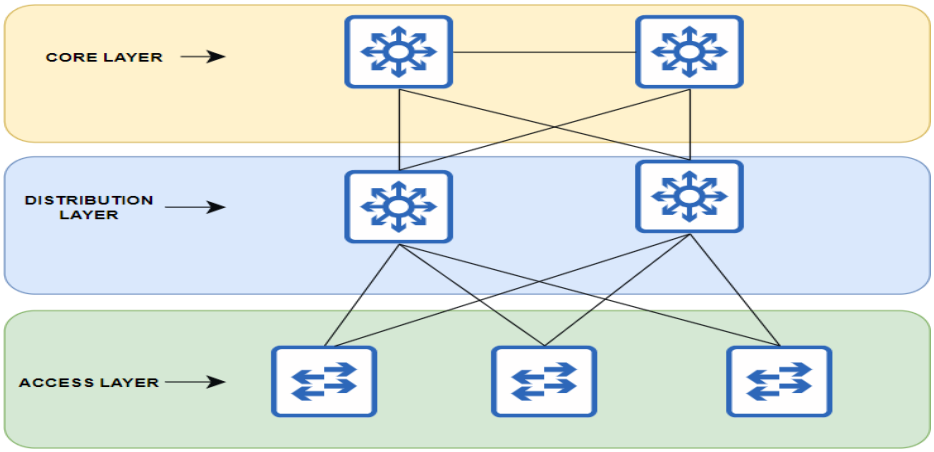


Figure 5 (3 Tier Architectural Model)

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 layer.

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

The distribution layer is located between the access and core 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.

(Subnets and VLANs are discussed later in this book).

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. This is also responsible for routing traffic towards remote networks.

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

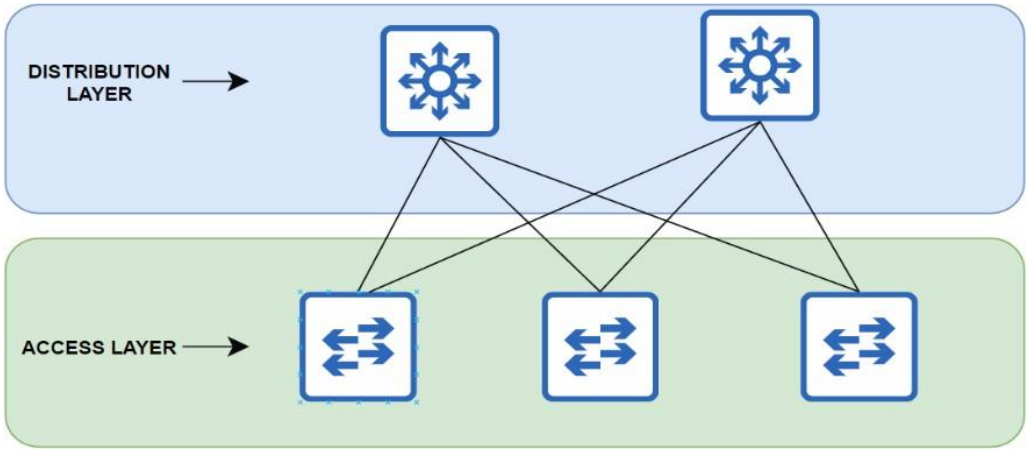


Figure 6 (2 Tier Architectural Model, Spine leaf model)

In contrast to the three-tier architectural model, which includes an access layer, a distribution layer, and a core layer, the two-tier or collapsed core model only includes an access layer and a collapse layer; the core and distribution layers were collapsed into one layer, hence the name "collapsed core." This model is far less expensive than three-tier architecture.

Spine-Leaf architectural model

The spine-leaf architectural model is an example of a 2-tier architecture in data centers. Figure 6 shows two layers of switches: spine switches and leaf switches. The primary point of entry for network users is a leaf switch. Spine switches, the backbone of a communications network, link all leaf switches throughout the network.

A two-tier architecture has its own advantages, such as low latency, which allows for faster transmission... having a maximum of two hops, performance: having high-speed connections, scalability: allowing us to easily append devices such as spine switches, leaf switches, hosts, and so on.

Types of network topology

Network topologies include the wiring, linking, and assembling of computers to form a network. We may classify various types of communication networks using these topologies. Figure 7 depicts various network topologies.

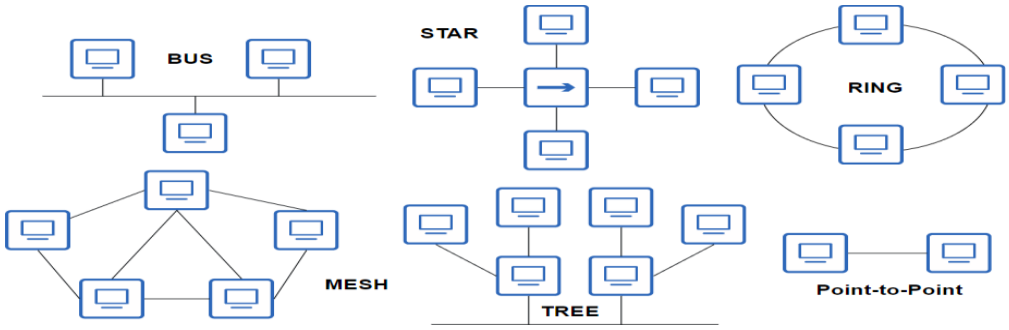


Figure 7 (Network topologies)

Point-to-point topology (p2p) is the most fundamental type of network on the list. As the name describes, it's a connection between two directly connected devices. Either wired or wireless.

P2P also has another variant which is "point-to-multipoint" (P2MP.) P2MP is similar to P2P however instead of having a single peer, it has multiple peer connections.

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. It's also safe to say that the network wouldn't work if the main cable breaks. Same goes as bus topologies. The advantages of both bus and point-to-point topology is that it can be installed very easily and the wiring is more compact, unlike a mesh topology which we will go through later. In a bus topology, faults are difficult to detect, and it's difficult to scale.

Moving on, 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's the reason it's called as a 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 just like the previous topologies discussed.

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.

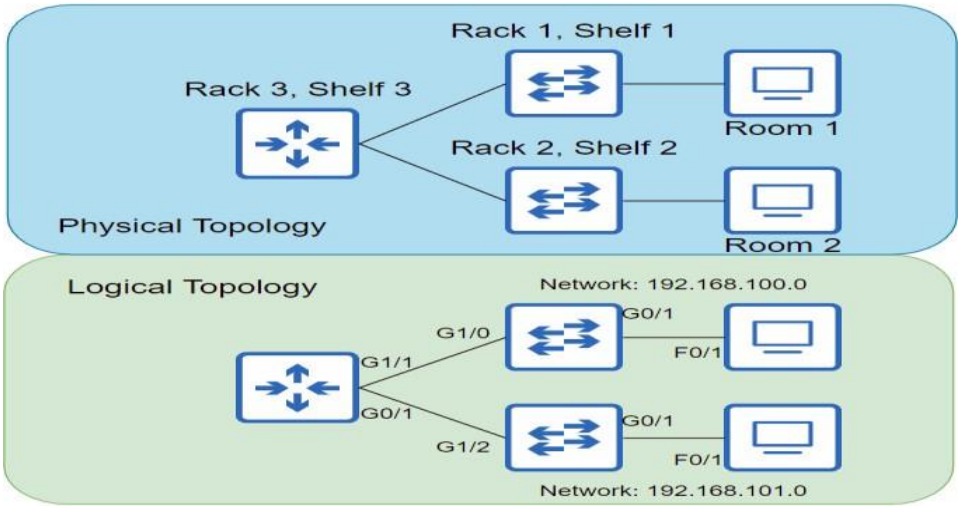
Mesh topologies. Using a mesh topology, every device is connected through a dedicated point to point link. The advantages of a mesh topology are that since every device has its own dedicated link, it will eliminate the possibility of congestion and also that it is reliable robust as one link failure 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 types of topologies. The benefits to this are that you can choose the topology you need. I 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. 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 8 shows how physical and logical topologies differ.

Figure 8 (Physical and Logical Topologies)



Network Backbone and Network Segments

Networks have a backbone to which all network segments and other hosts are connected. It is the network's vital nerve because it serves as a bridge for every segment within a network, allowing them to communicate. Obviously, A backbone should, of course, have robust technology to support all incoming and outgoing network traffic. Network segments are small sections of the network that are linked to the backbone, which serves as the connecting point for all segments.

CHAPTER 2
TCP/IP MODEL

s

CHAPTER 2 (TCP/IP Model)

Network Architecture

A network architecture is the design of a computer network which refers to different variety of things, specifically, the technologies and applications that are necessary on supporting a computer network. A network architecture ensures that a computer network meets its requirements to work efficiently.

It describes the requirements needed to make a computer network function. Some documents describe the use of a variety of network protocols, which describe a set of comprehensive rules a computer must follow to communicate with other devices. Standards may also specify the type of cable and cable length needed for a network to function properly.

You can think of a network architecture as a blueprint for how you will construct a house 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 network vendors.

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 (US) Department of Defense (**DoD**) during the 1970s. The TCP/IP protocol model describes a huge collection of networking protocols, allowing for multiple communication options. Protocols defined are documented in the Request for Comments which defines their functionalities and purposes. 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).

(More context about TCP/IP is given on the following pages).

s

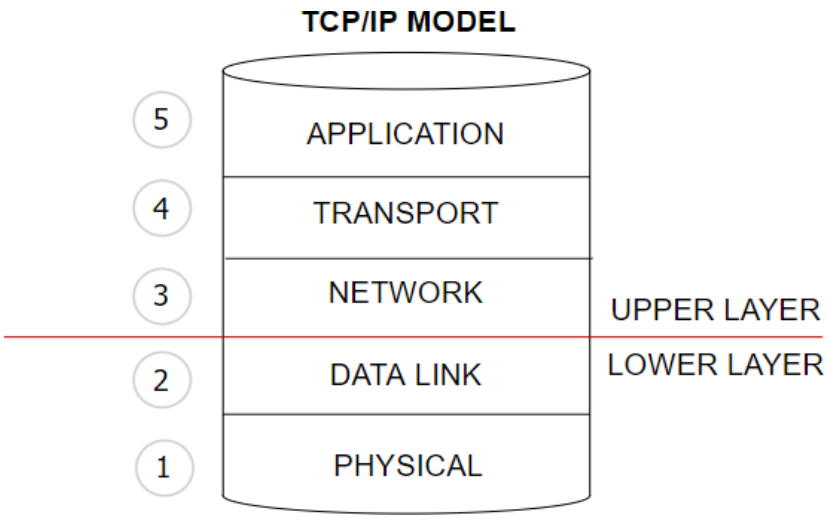


Figure 9 (TCP/IP model, layers)

To help people fully understand TCP/IP, it is divided into smaller layers. Each category defines its own protocols and standards.

As shown in Figure 9, the TCP/IP model has all the layers defined. The TCP/IP model has fewer network layers compared to the OSI model. The lower layers focus 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 by users.

NOTE: OSI model still influences how people think about networks.

The TCP/IP model refers toa set of communication protocols that were developed so that devices can communicate with one another. As shown in figure 10, the various protocols of the TCP/IP model are described below.

Figure 10 (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)

s

Page 16

TCP/IP Application Layer

The application layer forms the very first layer of the TCP/IP 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 does not define the application itself, rather it defines the services or functionalities it needs for it to function.

The application may utilize varied communication systems in the form depicted by Figure 10. 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 and session layer are not presented, but acknowledged by the OSI model. 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 presentation layer helps encrypt data for security purposes. The encryption enhances the security and privacy of the data.

The session layer of the OSI model 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, the session layer must first establish a communication called a virtual circuit (VC). It is accountable for keeping track of its communication modes: simplex, half-duplex, full-duplex. Modes are further discussed in the following Chapters.

The web browser is the most commonly used application in nowadays. 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 protocols on the TCP/IP model.

s

HTTP Overview

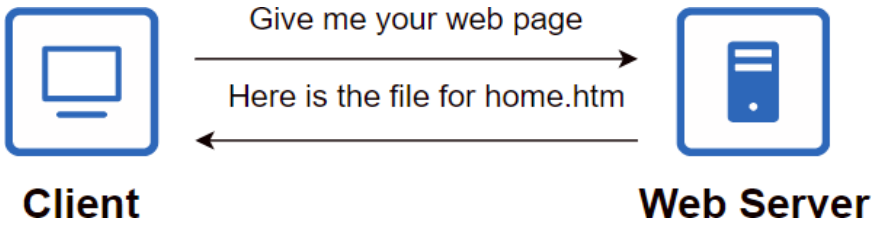


Figure 11 (Basic logic to pull out the contents of a webpage using HTTP)

To start, it would be beneficial to give a brief introduction of the overall topic. What really happens 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 11.

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.

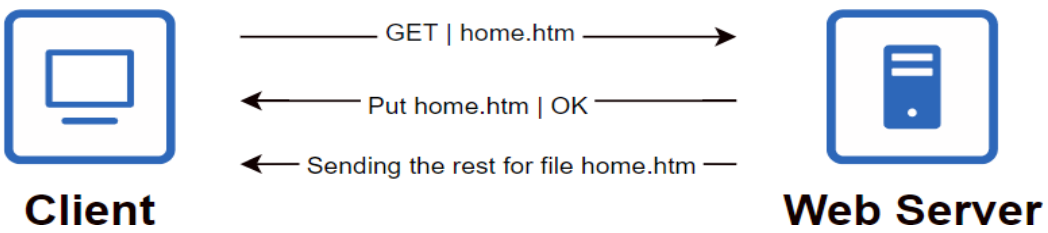
After this, Larry's web server would see the request. After receiving Bob's request, Larry's web server would send the contents of the document to Bob's computer.

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 this work, let us refer to the image in Figure 12. The following texts discuss the same ideas as the first, but in more depth and detail.

Figure 12 (More detailed explanation of figure 11)



As suggested in Figure 12, 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 12, 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 12. 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 12. When the webserver acknowledges the "get" request. It will, at the user's next request, send the contents of the requested web page. Figure 12 shows the third step of the process which involves sending the rest of the contents of the home.htm file.

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). This chapter covers both TCP and UDP functionalities.

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 link ability between applications and acts as a temporary session between applications. The transport layer also contains features that greatly support the data as its 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, 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 tothe 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 – this is the SYN flag. 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 Synchronize.

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.

FIN flag – 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 flag – 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. Forthis 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 *three-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

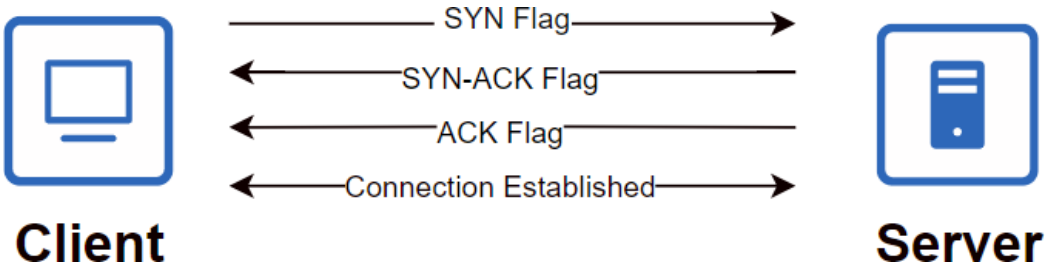


Figure 13 (Connection Establishment)

As illustrated in Figure 13, the 3-way handshake process occurs. The client is establishing a connection with the server so that they can transfer data into the other endpoint. In order for the connection to take place, the virtual circuit (VC) must be established first so it can carry information to the other end.

Step 1. Host A sends a SYN flag to another host (Server). This message is telling the server that the connected device is ready to communicate. If you are to review the previous pages, 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

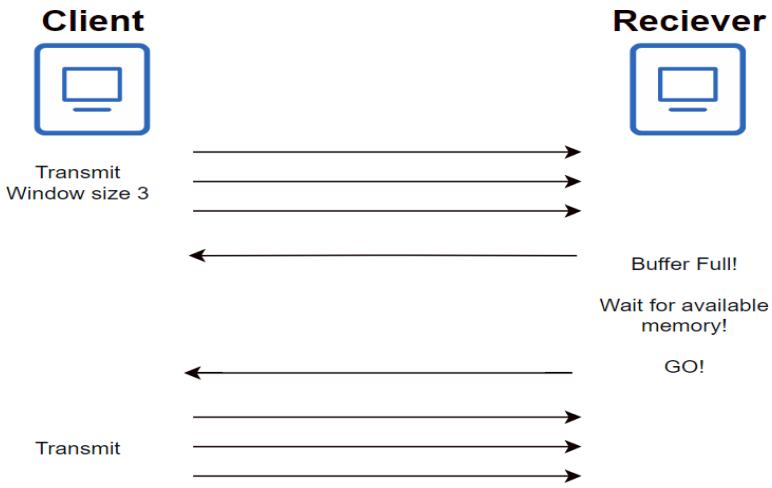


Figure 14 (Transmission with Flow Control)

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 14, 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. 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.

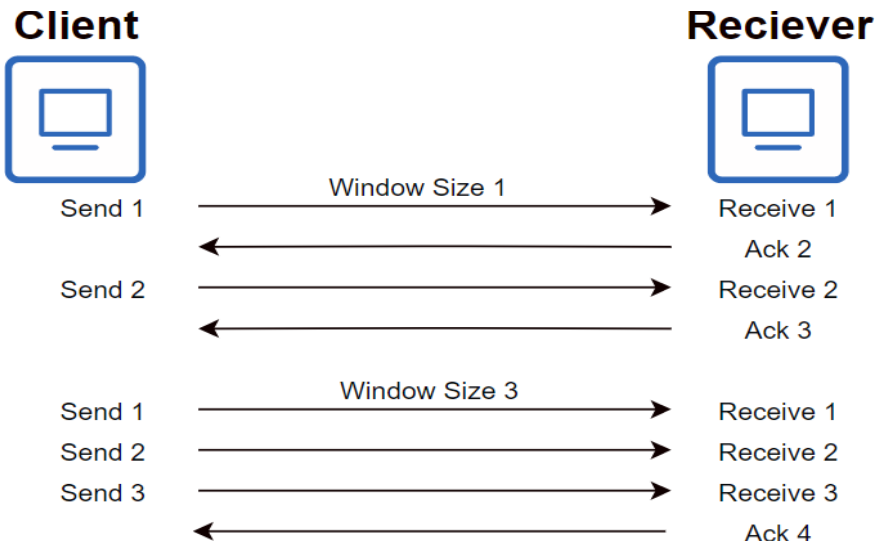


Figure 15 (Windowing Concept)

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 16, 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.

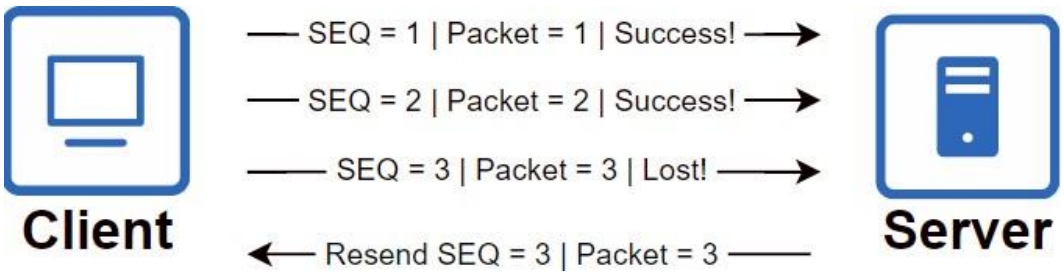


Figure 16 (TCP Recovery Concept)

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 16, 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 17 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.

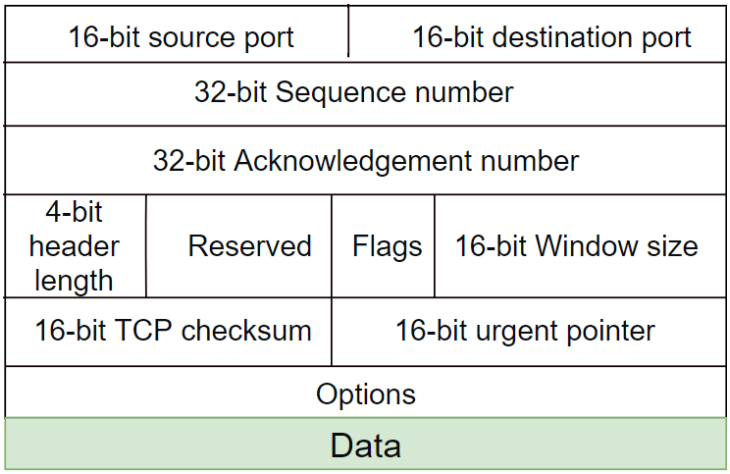
On the other hand, the figure demonstrates the role that a particular layer play. This happens when two computer systems with the same operating system layer want to communicate with each other. Bob's browser sent the data with a TCP header that requested more data from the server.

Figure 17 (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 18 (TCP Header)



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. Figure 18 depicts all the parts inside a TCP header.

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 19 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.

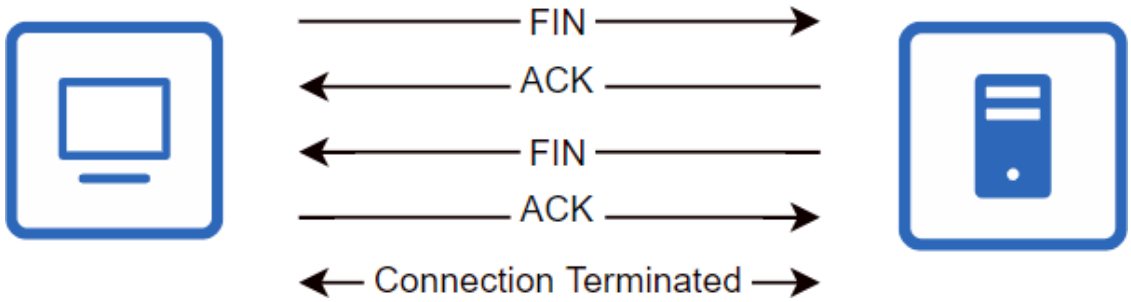


Figure 19 (4-Way Handshake Process)

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. UDP has no way of relaying the datagrams back in the order they were sent.

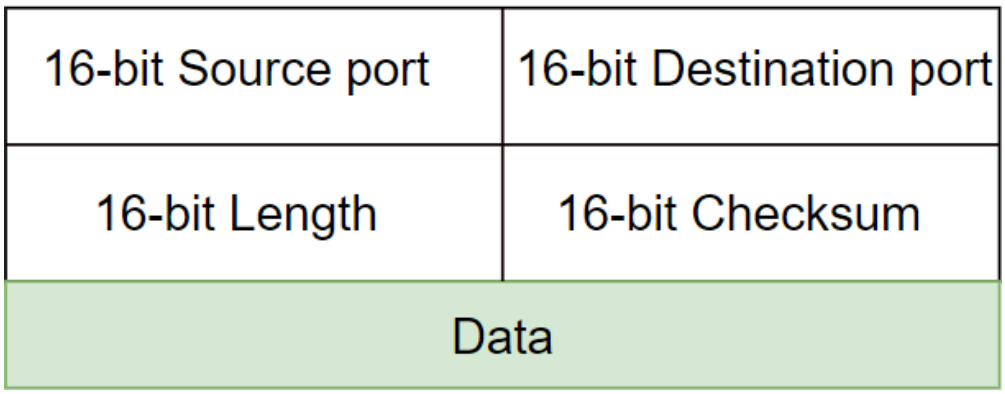


Figure 20 (UDP Header)

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. Figure 20 illustrates the fields inside a UDP 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 document.

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 IPv6are 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 IP 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.

Page 28

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.

Page 25

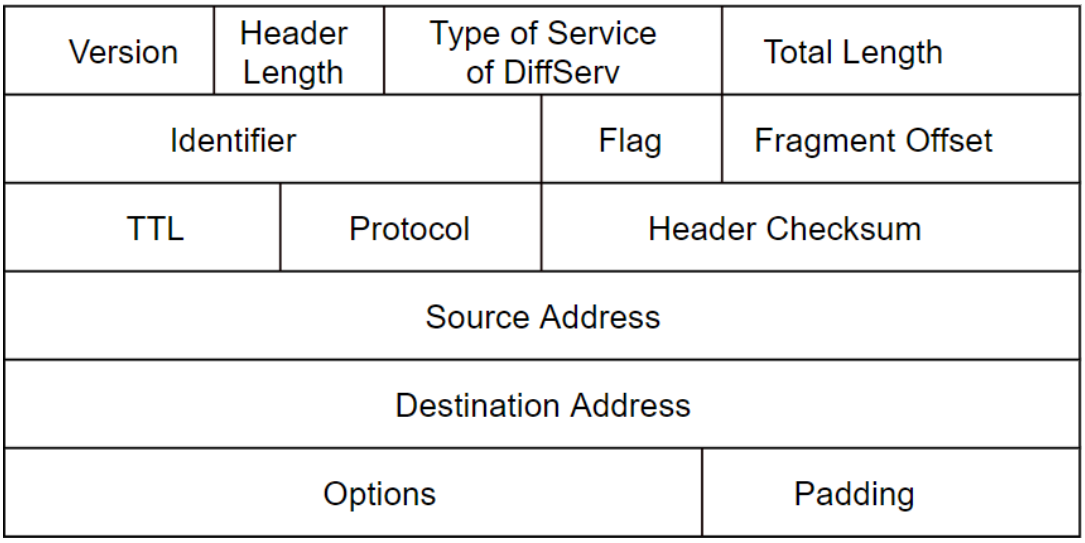


Figure 21 (IPv4 Packet Header, Fields)

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.

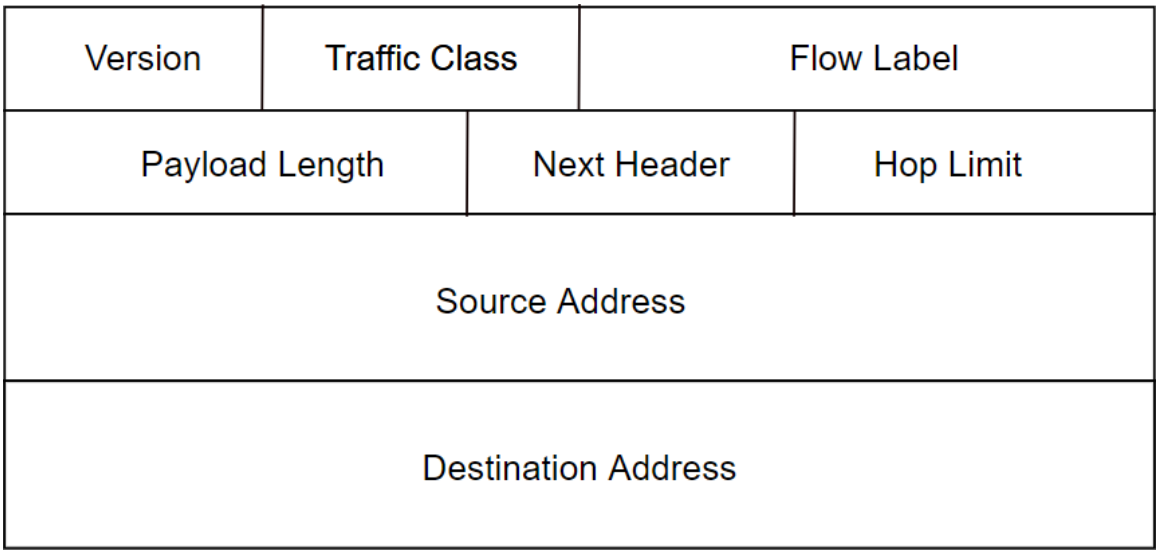


Figure 22 (IPv6 Packet Header, Fields)

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 22 demonstrates the areas 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 also acquire IP addresses from devices through protocols, dynamically. The most widely used method of dynamic address assignment is Dynamic Host Configuration Protocol (DHCP).

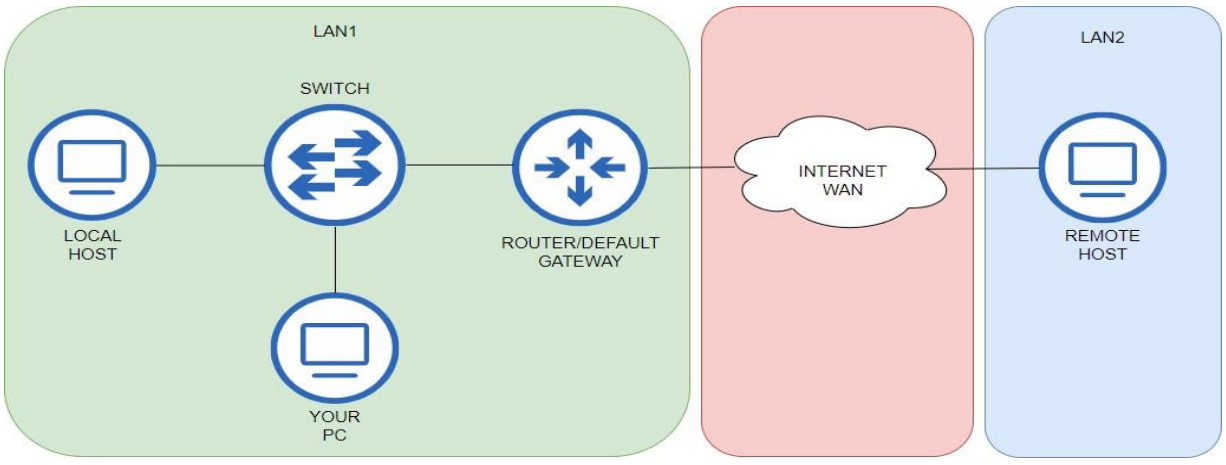
(DHCP is soon covered in this book).

Routing basic overview

The TCP/IP layer is also well known for handling packet routing and forwarding messages from specified sources. (The routing is discussed below). When sending packets, the host can send packets from any location.

A machine could send a packet to itself using a specialized IP known as the loopback interface (127.0.0.1), which is mainly used to evaluate the TCP/IP protocol stack of a computer. A host could send a data packet locally, which could be shared with other hosts on the same network (local). Finally, packets may also be sent remotely to a host on the same network and/or across different networks.

Figure 23 (Sample illustration)



Page 32

A packet, whether to be sent locally, remotely, or on its own, the TCP/IP network layer uses IP addresses and subnet masks, primarily acting as a packet identifier during packet routing and forwarding.

If the packet was sent locally, it would be sent to the intermediary system through the network to be routed to its proper destination. Whereas, if a packet is to be transmitted from one network address to another network address, it must be redirected. We will route data outside of a network through a layer 3 intermediary system called a router (routers are responsible for accepting packets inside the network, and routing packets outside the network).

This method is referred to as routing. The path is the method of finding the routes to our destination. Usually, a router at the local level is referred to as the default gateway.

The router is a network unit that can redirect traffic on the basis of a network to which it is connected. In order to think things through, our network is a door that enables external packets to enter and also sends internal packets to other networks.

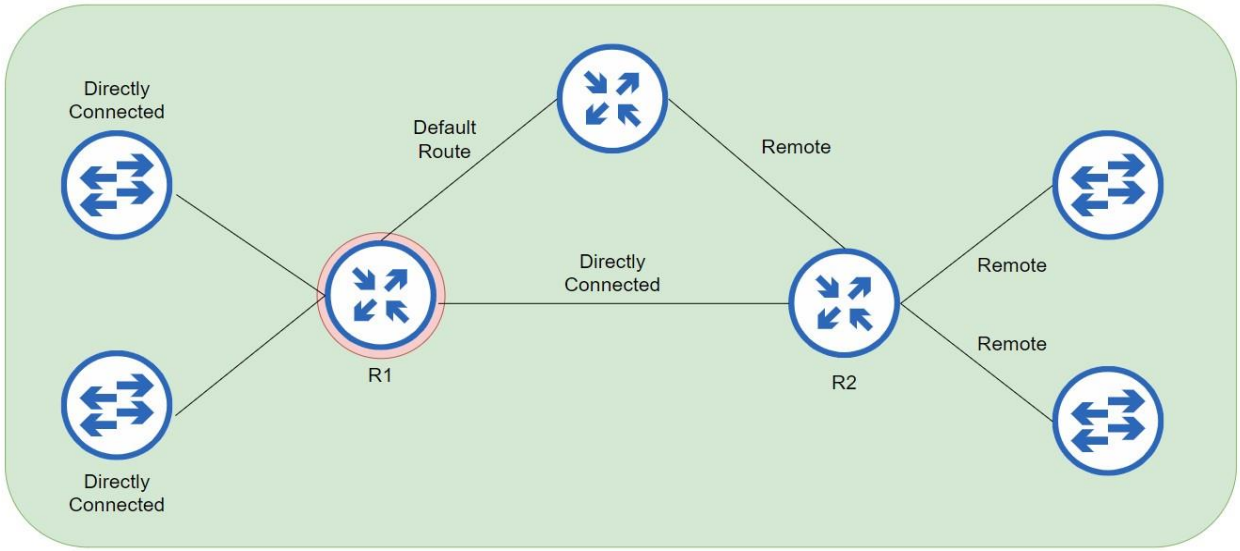
An IP address can be identified as an individual on the network. If the default gateway to the network is not known, it is not possible to go beyond the local network, and vice versa. The default gateway is a key component used for remote host access.

After being able to take a simple overview of how host forwarding decisions operate, let us understand how these packets are sent from host to host within and outside the network. Clearly, when a host sends a packet from one device to another, it has to go through different procedures. The IP address assignment table of the router is a form of table called the routing table. This routing table consists of the routing information that is widely used to decide the best route a packet takes to reach its location.

There are three key types of routes that you need to be familiar with when it comes to creating route tables. These paths are either direct, remote, or default. Directly connected routes are directly connected router interfaces that include inbound and outbound transit. Remote routes are routes which are independent of dedicated facilities. In the end, default routes Default routes are only used when the last resort is needed. This is useful in cases where there are no other ways to access the destination network.

Figure 24 indicates the various types of routes. Network 1 consists of the main routers. All links which are directly linked, and any links which are connected only by means of other links, shall be regarded as part of a single path. The second link, R2, is configured as the default route, meaning that all packets that is found in the routing table will be sent via the default route.

Figure 24 (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 3 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 under the network layer. It is responsible for providing access to the upper layers, preparing frames on or before media transmission, and much more. It is mainly responsible for exchanging ethernet frames between source and destination through physical media. The following details will provide you with a brief introduction to the data link layer.

The data link layer consists of two sublayers: The Logical Link Control (LLC) and the Media Access Control (MAC). The LLC helps the upper layers to communicate with the lower layers. It

offers detailed information that defines the protocol to be used for the frame as before it is transmitted over the medium.

In comparison to the MAC, it is responsible for managing or taking care of the frame as well as during transmission. It also provides details, specifically a hardware address, or what we call the MAC address that was created by your Network Interface Card (NIC) as an address identifier and accesses various network technologies. In addition, the MAC also has the capability to communicate with wireless technology 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 destination. 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.

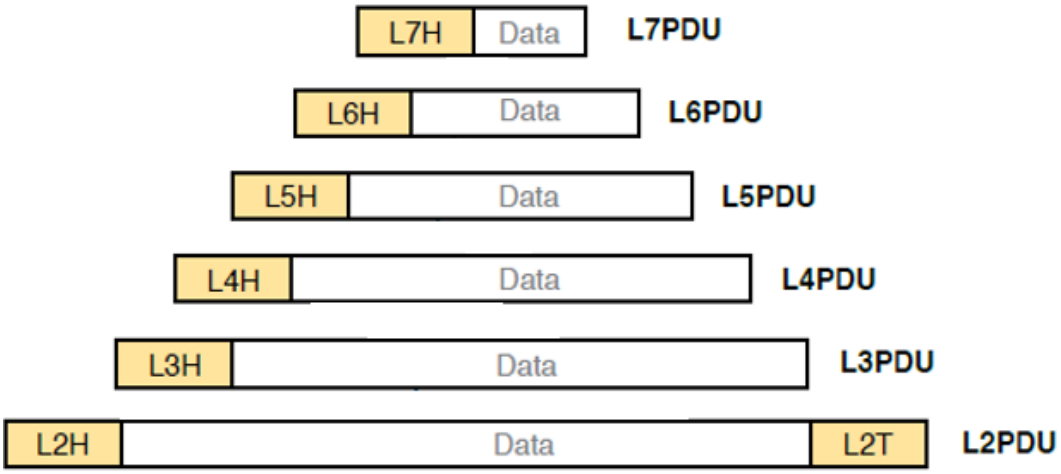
Step 4 Encapsulate the data supplied by the network layer inside a data-link layer header and trailer.

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 25 (Protocol Data Units)



Transmission methods

The data-link layer and the transport layer also have several methods for efficiently transmitting data through the medium: segmentation, multiplexing.

Multiplexing would allow other users within the network to share a single data transmission connection across the network. In comparison to segmentation, a single data splits into several segments that initially boost the efficiency of data transmission networks. For example, if any or more messages are missing, only certain parts or parts that are missing need to be retransmitted again.

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.

NOTE: These physical mediums and other components are further discussed in Chapter 3, Ethernet Introduction.

Extra Terminology

Bandwidth – Bandwidth is the amount of data a medium could carry and transmit.

Throughput – Throughput is the measurement of data transferred across the media over a given period of time.

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.

Benefits of a network model

The benefits of using a layered model to define network protocols and operations including: assistance in designof protocols as protocols that operate at one particular layer must have precise information which it acts upon and precise instructions to its linking layers.

Competition is expected to help both vendors make more offers. Holding from technology causing upheaval or displacement in other layers. Providing a standard vocabulary and usages for explaining networks and services.

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
ETHERNET INTRODUCTION
(W.I.P.)

CHAPTER 3 (Ethernet Introduction)

Ethernet Introduction

As you might know, Ethernet is a huge deal in the field of networking; addressed why later. When we refer to the word "Ethernet," we can think of a wide variety of meanings as Ethernet is a family of LAN standards that defines both the data link and the physical layer that were both described in the previous chapter (Chapter 2, TCP/IP Networking Model).

The components that make up the Ethernet network are cables, protocols, specifications, and other elements that make up the Ethernet LAN. Please notice that the Ethernet specifications are established by the Institution of Electrical and Electronics Engineers (IEEE).

Ethernet is a very broad topic, so I've written a dedicated chapter to give you a simple overview of Ethernet LANs.

Types of Ethernet LANs

Likewise, ethernet can be many things. First, let's start by giving you a brief overview of how typical SOHO LANs are structured and constructed. The SOHO network can consist of a variety of devices, including Ethernet and Wireless connections.

In order to further illustrate this, ethernet will provide a physical link for data access between different devices within the network. There are various elements that we can recognize as part of an Ethernet LAN, such as an intermediary system called an Ethernet switch, which provides ports for Ethernet cables to link to. It also has improved features, which are further discussed in the incoming bits. We also have another type of unit, called a router, which includes routing features that allow local networks to connect with external networks.

Network vendors are now producing multi-functional modules that we can use on our networks. When I say package, a solitary system can be made up of multiple features that other devices have. For example, a single device, let's say a router, may contain the functionality of other devices; a bundle router consists of a switch, a firewall, and an IDP/IPS kit (functionalities). Normally, the average SOHO router has four or eight ports.

Common SOHO networks will also allow wireless networking. Inside the wireless LAN, we use radio waves to relay bits from source to destination; they are also specified by the Electrical and Electronics Engineer Institution (IEEE). As standard 802.11. Wireless LANs often use another type of system, named "Wireless Access Point (AP), which has a similar purpose as a network hub; broadcasting wireless devices to access network resources.

A traditional router that can often handle both wireless and wired communications and is often commonly referred to as a "wireless router."

Large businesses (enterprises that are usually managed by large organizations) are similar to small enterprises, but they have a much wider reach. The enterprise network may be made up of multiple network devices specifically designed to meet the needs of the enterprise network to run and may also be made up of multiple intermediary devices that help to sustain the network.

An ethernet switch, for example. A network needs multiple network switches to service a much wider network, but there are switches that can accommodate a lot of devices, but we usually use multiple devices. For example, several switches within the corporate network use a centralized switch, known as the "SWD" switch. It's primarily to improve the efficiency of the network.

NOTE: If you don't know any of the intermediary devices listed, don't worry as I'm going to cover this while explaining the Ethernet in-order to give these devices more sense.

Network Interface Card

You may have already heard the word "*Network Interface Card*" from the previous chapter. It is essentially a piece of hardware component installed inside a device. This is commonly used for wired networks, but also used for wireless networks which is referred as a "*Wireless Network Interface Card (WNIC)*".

Figure 26 (Network Interface Card)
Image taken from: www.shutterstock.com

This piece of component that enables end devices to be able connect to the network. A NIC card is manufactured alongwith a hardware address called "Media Access Control (MAC) address" which I've given a brief overview from the previous chapter (Chapter 2, TCP/IP Model)

Copper Cabling

With copper cables, electrical signals are used to relay bits across the network. These types of cables are commonly used due totheir low cost and ease of installation, but because copper cables use electrical signals, there is a high risk of signal interference during transmission. Copper cables usually have the following issues:

Electromagnetic Interference (EMI) – This is when signals are interrupted during transmission by other signals carried by other mediums (copper) that may corrupt the data signals being transmitted.

Crosstalk – This is a kind of noise created by electromagnetic fields. This is when the active communication is interrupted by the signals from the adjacent wire, resulting in the other medium overhearing some portion of the conversation from the other wire.

To counteract this, manufacturers wrap copper mediums with metallic layers, thereby securing copper cables to avoid EMI interruptions, as opposed to crosstalk, they twist the cables together to cancel crosstalks.

In addition, copper wires are limited in terms of distance. The longer the signal travels, the higher the chance it will fail, so manufacturers follow a distance limitation specified for the creation of copper cables.

Types of Copper Cables

- *Unshielded Twisted-Pair Cables (UTP)*
- *Shileded Twisted-Pair Cables (STP)*
- *Coaxial Cables*

Unshielded Twisted-Pair (UTP)

Unshielded Twisted-Pair cables are one of the most common networking media in today's world. UTP is much more inexpensive compare to Shielded Twisted-Pair (STP) cables and is terminated by an RJ45 connector that is usually used to link hosts to intermediate devices such as an Ethernet switch or a router. Though, UTP does not have the best protection for noise prevention compared to STP (following information will provide more information why).

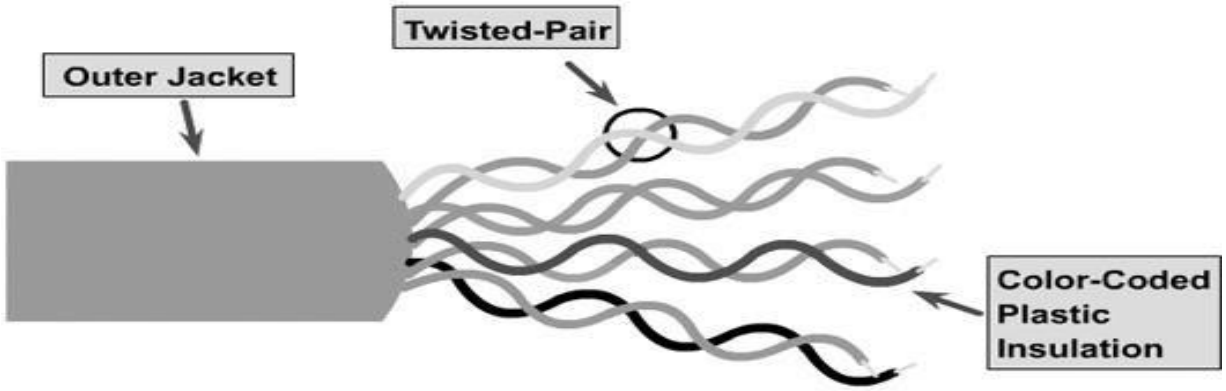


Figure 27 (Unshielded-Twisted Pair)
Image taken from: www.ciscopress.com

The UTP cable has three layers (showed in Figure 27): the outer jacket, the twisted pair and the color-coded plastic insulation. In the same way, the outer jacket is used to shield the cables from any physical harm, the twisted pairs are used to avoid signal interference and, finally, the color-code plastic insulation is used to separate the cables from each other and often serves as an identifier.

As previously mentioned, UTP is much more vulnerable to signal interference such as EMI or RFI than STP because it lacks any defense against these effects. However, it is worth noting, that even if UTP does not have the ability to counteract signal interference, it is capable of limiting the negative effects of crosstalk.

These days, UTP manufacturers pair wires in a circuit by twisting them together (shown in Figure 27) to avoid crosstalk and restrict signals from deteriorating for improved efficiency. However, when manufacturers conform to such standards, it further regulates how many twists or braids are permissible for a given wire length.

UTP Cabling Standards

We should also keep in mind that the manufacturers of UTP cables not only adhere to certain restrictions, but also to certain standards developed by the *Institute of Electrical and Electronics Engineers (IEEE).* When selecting a UTP cable, you can use these criteria to determine which type of cabling standard better fits your budget and network. Some of the most widely used specifications in cabling environments are described in the following lists (page 37):

Page 42

- Cable types
- Cable lengths
- Connectors
- Cable termination
- Methods of testing cable

UTP cables, as you may be aware, are rated based on their capabilities and efficiency. They are categorized into categories depending on how fast their bandwidth is (for example, Category 3 [Cat3], Category 5 [Cat5], and Category 6 [Cat6]); the higher the category, the more bandwidth it can hold. These UTP cable types are gradually evolving over time.

Furthermore, *Category 5 Enhanced (Cat5e)* UTP cable is now the least suitable type of UTP cable, with *Category 6 (Cat6)* being the preferred type for cable installations. Fiber Optic Cables, on the other hand, are a newer form of cable that we will discuss later in this chapter (Chapter 3, Ethernet Introduction).

TO BE CONTINUED…