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

CHAPTER 1 (Network Foundation)..... 9

Initial idea About Networks 9

Fundamental Overview of Networks 9

Intermediary devices 11

Reliable Network 13

Types of Networks 16

3 Tier Architectural Model Overview 17

2 Tier Architectural Model Overview 18

Spine-Leaf architectural model 18

Types of network topology 18

CHAPTER 2 (TCP/IP Model) 22

Network Architecture 22

TCP/IP Application Layer 24

HTTP Overview 25

Simple HTTP logic 25

Additional Information (HTTP) 25

TCP/IP Transport Layer 26

Transmission Control Protocol 27

TCP Flags 27

Connection-Oriented Communication 27

Three-Way Handshake 28

Flow Control 28

TCP Error Detection/Recovery 30

Same-layer and Adjacent-layer Interactions 31

TCP Header 32

4 Way Handshake 33

User Datagram Protocol 34

TCP/IP Network Layer 35

Characteristics of IP 35
IPv4 Overview 36
Limitations of IPv4 37
IPv6 Overview 37
Routing basic overview 39
Network Layer Summary 41
Data link layer 41
Transmission methods 43
Physical Layer Overview 43
Physical Layer Summary 44
Benefits of a network model 44
Chapter Summary 45
CHAPTER 3 (Ethernet Introduction) 47
Ethernet Introduction 47
Types of Ethernet LANs 47
Network Interface Card 48
Copper Cabling 49
Types of Copper Cables 49
Unshielded Twisted-Pair (UTP) 49
UTP Cabling Standards 50

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.

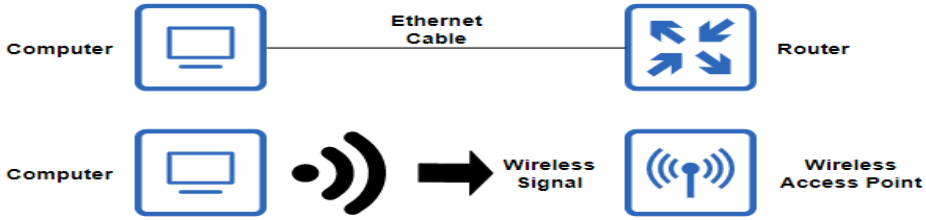


Figure 1 (Basic network diagram)

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 extended ethernet the further inflates LAN access to WAN. Lastly, they also support both DSL and satellite connections, similar to typical networks.

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

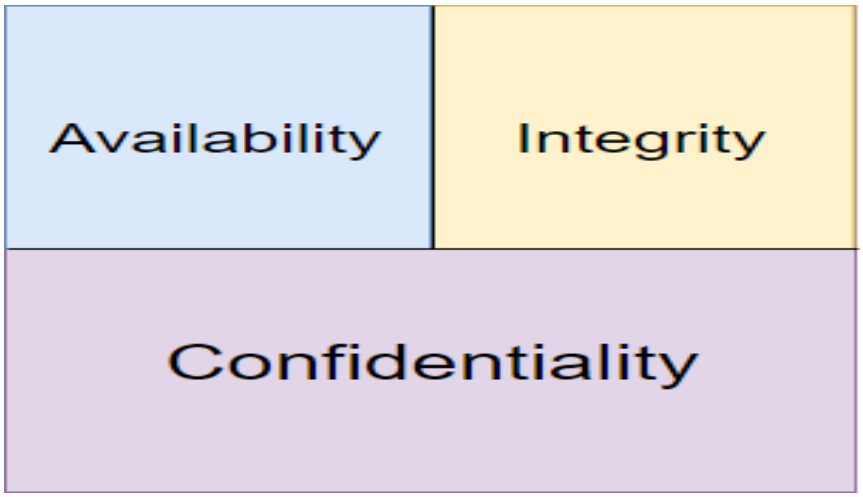


Figure 4 (Security requirements)

Many security threats occur externally and internally. Some common external threats we commonly encounter is 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

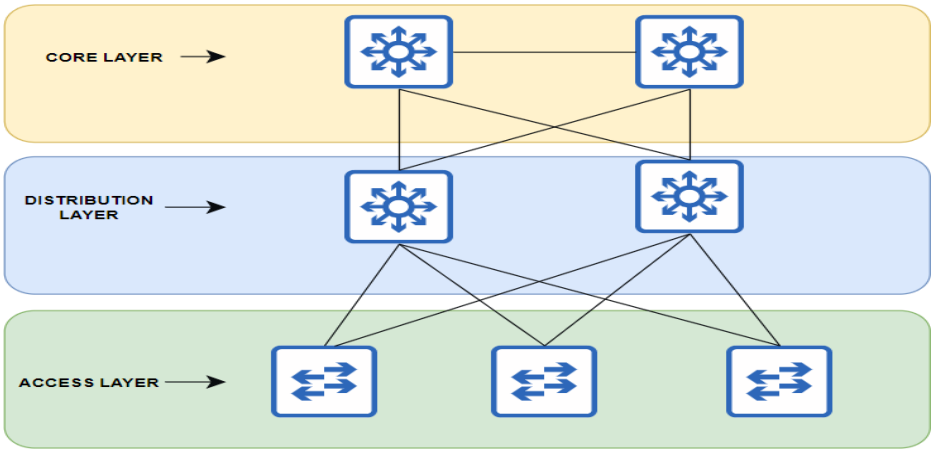


Figure 5 (3 Tier Architectural Model)

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

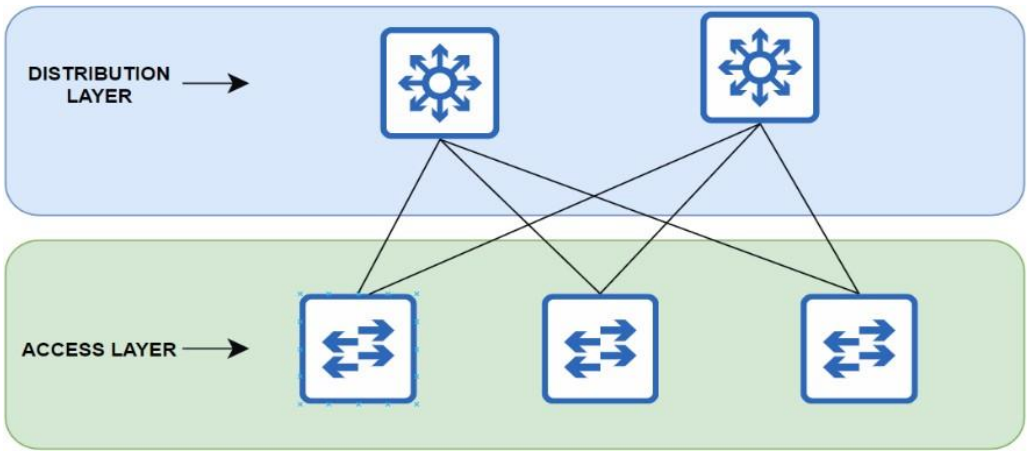


Figure 6 (2 Tier Architectural Model, Spine leaf model)

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 includes 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.)

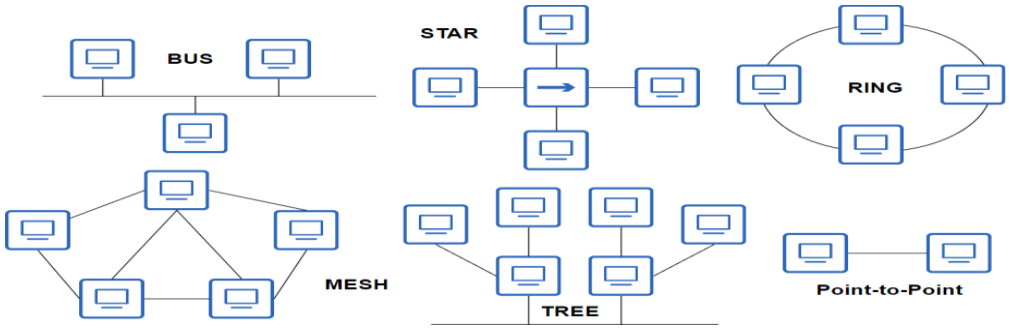


Figure 7 (Network topologies)

Point-to-point topology (p2p) is the most fundamental type of network on the list. As the name describes, it provides a direct connection between both peers, giving one communication path. P2P also has another variant, known as “point-to-multipoint” or P2MP. Similarly, as the name implies, P2MP contains multiple connections between multiple destinations.

Now, let's talk about bus topologies. Bus topologies are a very simple network, but they are no longer common or popular in today's generation. This topology has two distinct and terminated ends, with each device connected to a single cable. As they are only connected to a single cable, it is expected that all computers will see the traffic flowing through the cable; however, the traffic will only be received where it is actually addressed. A bus topology has the advantage of being simple to install and inexpensive. However, it has some drawbacks, such as being difficult to troubleshoot and manage. It's also worth noting that, because we only have one main cable, if that cable breaks, the entire network will fail.

Moving on, a ring topology is a very simple design that consists of a pair of devices linked together via a single main cable, similar to a bus topology. The structure forms a ring, which is why it is known as a ring topology. The data flow is very similar to bus topology in that all traffic is heard by all devices in the network but only received by the destination device. Furthermore, because it only accommodates one main cable, if the main cable fails, the entire network will fail.

Star topologies. This type of topology is very likely to be seen in networks where each and every computer has their own cable connected to one centralized device, usually employed by a hub or a switch. 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. It has many advantages for computing, considering that it can be installed, troubleshooted and managed quite easily too. They are also relatively scalable as you'll only need to bring a cable along with the device you want to add.

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. It also has a single point of failure, if there is a failure on 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.

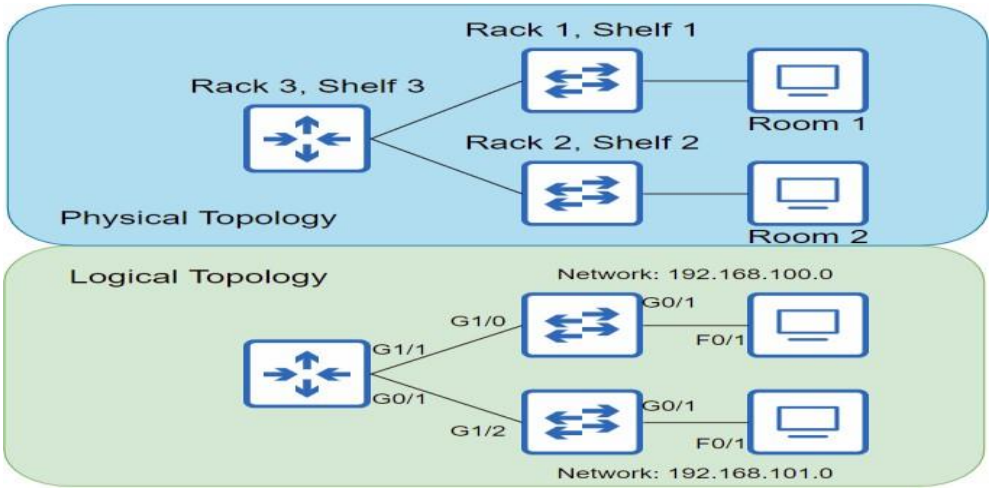
When it comes to fault tolerance, a mesh topology excels because each device provides a communication path to every other device in the network. Mesh networks are well-known for having the most connections per device. It is highly anticipated that it will be fault tolerant due to its large number of cables. To calculate the number of cables within a mesh topology, use the following formula: n(n-1)/2, where n represents the number of hosts in the network. It is worth noting, however, that we have two types of mesh topologies. There are two kinds of meshes: full meshes and partial meshes. A full mesh network has a communication path for every device, whereas a partial mesh network only provides redundant links to some devices within the network. To summarize mesh topologies, they are fairly redundant, but they are unquestionably expensive due to the high demand for cables.

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 and how they're wired and connected to one another, while a logical topology map shows all the devices ports, and addressing scheme, and how they communicate virtually.

Figure 8 depicts both logical and physical topologies.

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, on the other hand, are small sections of the network that are linked to the backbone, which serves as the connecting point for all segments.

Topology selection

It is critical that you understand what these topologies offer you, as well as the benefits and drawbacks of implementing them. Choosing a topology isn't as simple as picking one from a menu of available networks. It is critical that you pay attention to what your network requires in order to function properly and as expected. For instance, if you want a network with high fault-tolerance, you'll most likely go with either hybrid or mesh topologies. Here are some guidelines to keep in mind when selecting the best topology for you.

List of standards you should consider:

- ✓ Cost installation
- ✓ Ease of installation
- ✓ Ease of maintenance
- ✓ Fault tolerant
- ✓ Security requirement

To summarize, I've finally provided you with some basic terminology and methodologies for selecting the best network. It is critical that you understand network principles because they will be extremely beneficial to you in the future.

CHAPTER 2
TCP/IP MODEL

s

CHAPTER 2 (TCP/IP Model)

Networking Model

A network model is the design of a computer network which refers to different variety of things. They are blueprints that comprises of protocols, standards and specifications that were made to allow different vendors to manufacture interoperable devices, hence allowing disparate network devices to work in conjunction. On top of that, they define everything that should occur within a network connection. Specifically, things that will help both peers to communicate effectively and efficiently.

Network models like OSI and TCP/IP uses a layered approach, in which, they divide all the procedures that should happen inside a communication in to multiple layers. Each layer inside a network model has their own dedicated tasks, describing its function. They used a layered approach to ease network engineering and comprehension.

You can think of a network model as a blueprint for how you will construct a study house yourself. Just like a blueprint for an architectural project, a blueprint for a computer network is also required to develop a comprehensive network that works effectively, efficiently and accordingly. 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. However, it's is easier for you to purchase networking products from network vendors like Cisco.

For this chapter, we'll be focusing a lot more on TCP/IP model as a way to give you a solid grasp of what these different layers do and how they work accordingly to form a solid network.

Overview of the TCP/IP model

Like any other networking model, TCP/IP was developed by a vendor. TCP/IP was formed by the United States (US) Department of Defense (DoD) during the late 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, published by the Internet Engineering Task Force (IETF), 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).

s

Page 15

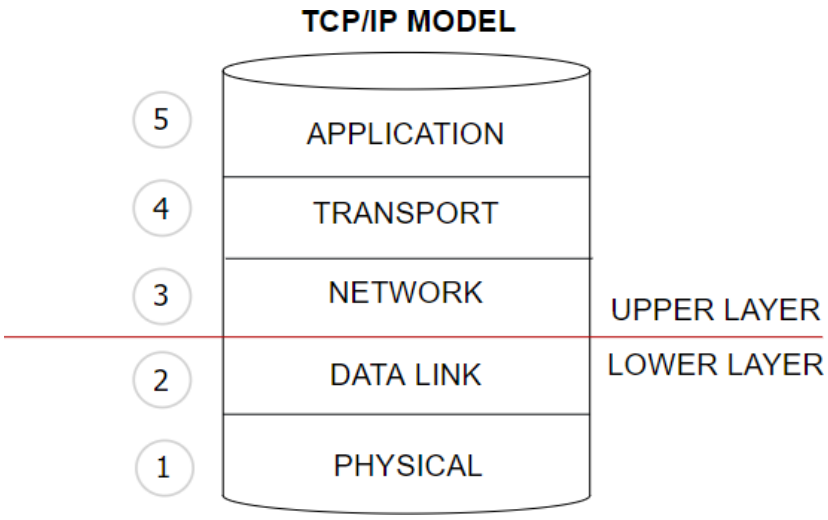


Figure 9 (TCP/IP model, layers)

To help people easily understand the TCP/IP model, it is divided into smaller layers. Each layer defines its own protocols and standards.

The TCP/IP model has all of the layers defined, as shown in Figure 9. When compared to the OSI model, the TCP/IP model has fewer layers. Furthermore, the upper layers define how different applications within a computer interact with one another, whereas the lower layers describe how actual data is transmitted from end-to-end.

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

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 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)

Application Layer

The application layer is the very first layer you'll encounter within the TCP/IP model, residing at the very top of it. 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 layer primarily serves as an interface for software applications, allowing them to send user information down the protocol stack and eventually to its destination. The application layer also determines whether the other peer is available and whether the sufficient resources are available.

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 data translation, presentation and formatting. It provides services like data compression, decompression, encryption, and decryption. It also responsible for translating user data into machine understandable language known as binary.

The session layer of the OSI model is very straightforward. It is an intermediate link involved in handling sessions between source and destination. It is mainly responsible for establishing, managing, and terminating virtual connections from both ends. Additionally, the session layer provides dialog control between both peers. The following are the available modes for dialog control: simplex, half-duplex, and full-duplex. (We'll be covering these modes later in this book.) Finally, the session layer is in charge of isolating disparate data from various applications within a connection.

Transport Layer

The transport layer provides end-to-end transportation services. It's also responsible for segmenting and reassembling data into data streams which is sequence of digitally encoded signals used to transmit and receive data. The transport layer provides two types of transportation services: reliable and unreliable. Since we're at it, we make use of TCP for reliable transmission and UDP for unreliable transmission. We'll be focusing on reliable transmission regarding what services does it provide to make it reliable.

Transmission Control Protocol

The Transmission Control Protocol (TCP) is a connection-oriented transmission protocol that is efficient and reliable. TCP offers a number of techniques and mechanisms for establishing a reliable connection. Sequencing, acknowledgement, re-transmission, flow control, and many other functions! We'll go over these services in greater detail later.

TCP Flags

In a reliable connection, TCP uses the acknowledgment concept which we'll be explaining in much in-depth soon. If you have never heard of TCP flags then you should know that they are traits used in a connection that show the state of the connection. Also used for handling and troubleshooting a connection. These are the available TCP flags that may be used during a TCP session:

SYN flag – The synchronization flag, or SYN flag for short, is used in the first step of the connection establishment phase to open up a connection for communication.

ACK flag – The acknowledgement flag, or ACK flag for short, is used to acknowledge successfully sent packets during a network communication, as the name implies.

FIN flag – The finish flag, also known as the FIN flag, is used to request that a connection be terminated. This indicates that the sender has no more packets to send, so it releases the reserved resources and gracefully terminates the connection. This is the sender's final packet.

URG flag – The urgent flag, also known as the URG flag, denotes information that is urgent. This is a rule that prioritizes certain packets and notifies the receiver to process the urgent packets before the remaining packets. When all known urgent data has been received, the receiver will be notified.

Push flag – The push flags or PSH flag for short, is somewhat similar with URG flag. This urgently tells the sender to immediately send the segment to network layer as soon as it is received.

RST flag – Finally, there's the reset flag, abbreviated RST. When something unexpected happens during the connection, it is used to terminate or reset the connection.

Connection-Oriented Communication

In a TCP connection, both peers 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 *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

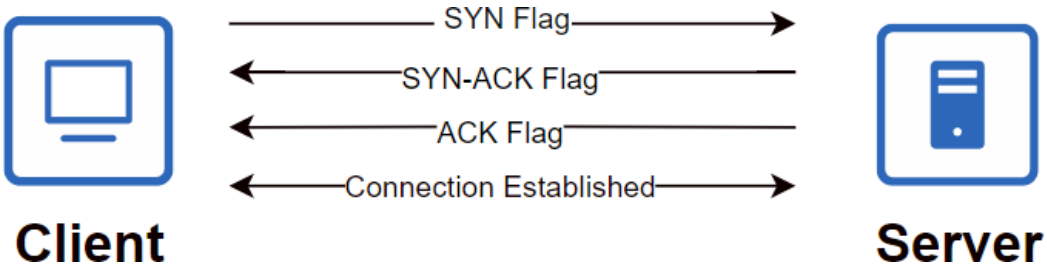


Figure 13 (Connection Establishment)

The three-way handshake process is depicted in Figure 13. The client is connecting to the server so that data can be transferred to the other endpoint. To make the connection, the virtual circuit (VC) must first be established.

Step 1. The client sends a Synchronization (SYN) flag to inform the server that a connection is about to be established. When one device opens a connection, a *virtual circuit* (VC) is formed.

Step 2. The server responds with a Synchronization-Acknowledgement (SYN-ACK) flag. In this stage, both peers are agreeing with certain rules and specifications that both should agree upon, and eventually acknowledging the SYN request from step one.

Step 3. Now that the server has agreed to establish a connection, both peers are now ready to form a bidirectional connection for them to transmit and receive resources. Once the three-way handshake is done, the virtual circuit will now be called an *overhead*.

Acknowledgement

Inside a connection-oriented connection, data integrity is vital. TCP make use of acknowledgements to ensure that a packet is received successfully, if not, TCP retransmits this. This process is known as *positive acknowledgement with retransmission*.

Flow Control

During communication and data transfer, we never expect things to always work smoothly. Congestions could occur from time-to-time during a connection. For instance, a high-speed computer system can generate as much data traffic in a short period of time to be handled by the other system.

To elaborate, in a connection, excess data that isn't ready to be transmitted is stored in a temporary container known as a buffer. We can only store a limited amount of data in a buffer. If a system's buffer is full, it will discard any additional incoming data, causing some of it to be lost during process. This is known as "buffer overflow." We can mitigate these types of events thanks to flow control.

Flow Control Overview

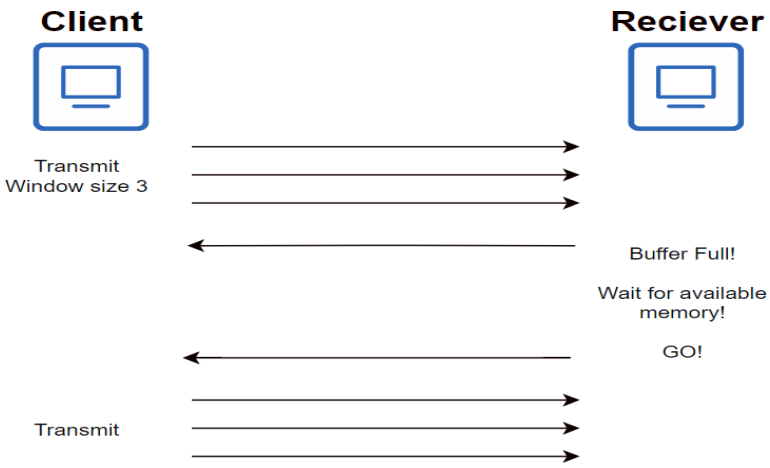


Figure 14 (Transmission with Flow Control)

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 topics.

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. It serves as an indicator; for example, when the buffer is full, the receiving device sends out a "not ready" indicator, preventing the other end from sending incoming packets. After processing some of its packets within its buffer, it will send a "ready" indicator to the sender, indicating that we are almost ready to send more packets. When everything is ready, a "go" indicator will be sent, resuming packet transmission.

Windowing

Every piece of data is acknowledged within a connection-oriented connection. Consider how slow it would be if each packet required an acknowledgement; however, because there is some time between *sending* the packet and *receiving* an acknowledgement, the TCP windowing mechanism takes advantage of this opportunity to transmit more unacknowledged data within a single acknowledgement.

TCP relies on the concept of windowing to help speed up the transmission process by transmitting multiple data packets that can be affirmed within a single acknowledgement, and to alleviate congestion by increasing packet size or adjusting the window size.

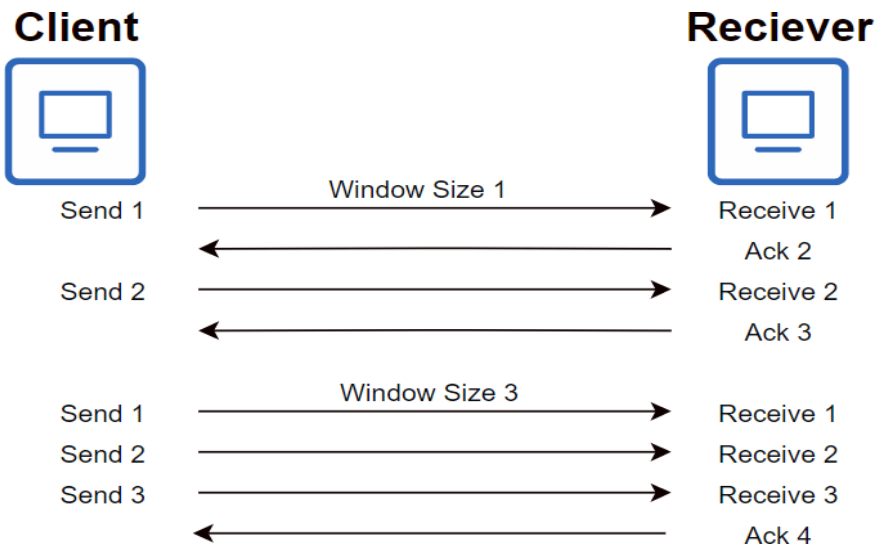


Figure 15 (Windowing Concept)

As shown in Figure 15, in the beginning, the window size is set to 1. This implies that we can only send one packet before receiving an acknowledgement. On the next set, because the window size is set to 3, we can then send three packets before receiving an acknowledgement. If the receiving host does not receive all of the segments, the windowing mechanism can help improve this by adjusting or decreasing the window size.

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 helps us speed up the process of transmission prevent congestion along the process.

TCP Error Detection/Recovery

To accomplish reliability, all data must be received and acknowledged by the receiving host as it passes along the network. TCP provides an error detection and recovery mechanism to ensure that all segments are sent successfully to its destination without any of it getting lost along the process.

I'll be providing you an example of how this mechanism work on the following pages.

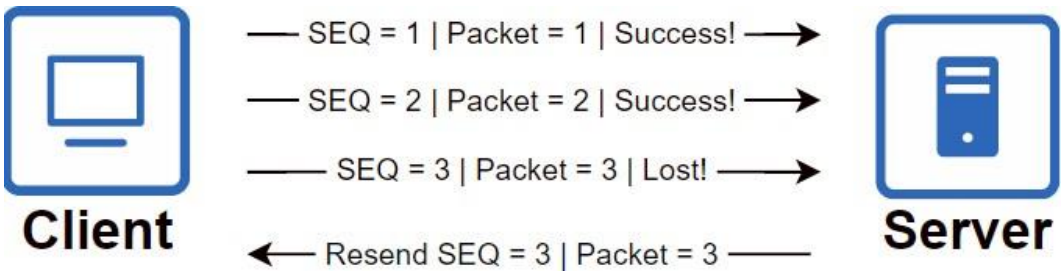


Figure 16 (TCP Recovery Concept)

Here's a diagram of the TCP recovery protocol used to accomplish this goal. Assume we have a client attempting to obtain resources from a web server, and the HTTP request was lost during transmission. How is data recovered? As shown in Figure 16, all packets were successfully received with the exception of packet 2, which was lost along the way.

Here's how it works. The first two packets were successfully sent by the client; however, the third packet was lost. If a packet is lost during transmission, no acknowledgement for that packet is received, informing the sender that a packet was lost along the way. In this diagram, for example, we lost packet three. These lost packets are re-transmitted.

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.

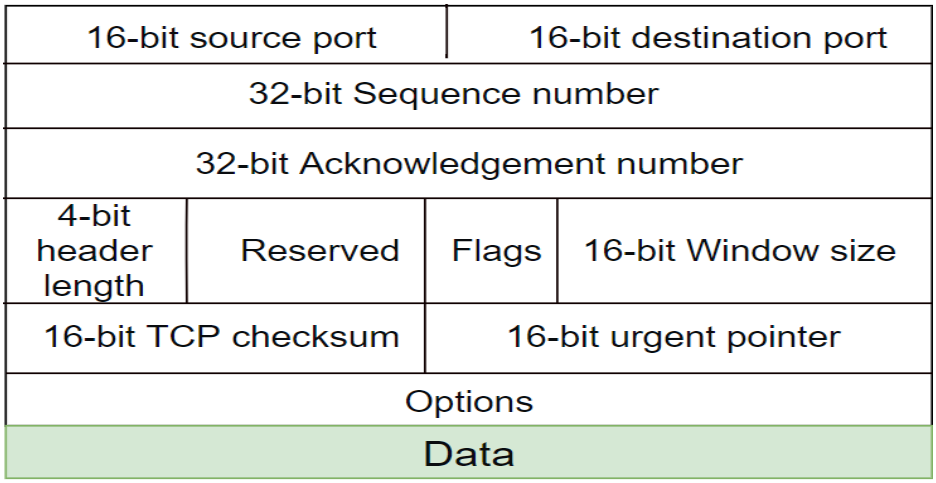
On the other hand, the figure demonstrates the role that a particular layer play. This happens when two computer systems with the same operating system layer want to communicate with each other. The client sent the data with a TCP header that requested more data from the server.

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 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.

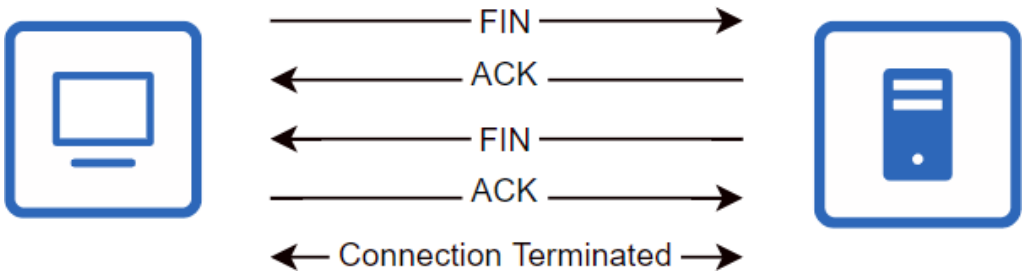


Figure 19 (4-Way Handshake Process)

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

Step 2. The receiver would receive the FIN request once it was completed. The receiver will reply with an acknowledgement to show that the receiver has received the termination request.

Step 3. The receiver will also send a FIN flag to notify the other system that the connection is no longer active and ready for termination.

Step 4. sender will know reply with an ACK flag, indicating that the connection will now be terminated.

After the fourth step, the virtual connection has finally been terminated.

User Datagram Protocol

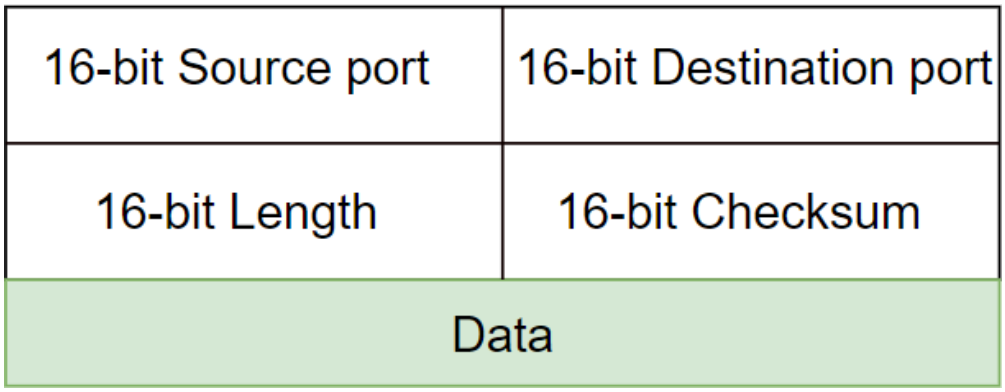


Figure 20 (UDP Header)

UDP, or User Datagram Protocol, is a high-speed but unreliable data transmission protocol. UDP is a protocol that is used to establish low-latency and low-tolerance transfers between applications. It is a best-effort transport protocol that lacks reliability and flow control but has data segmentation and reassembly capabilities similar to TCP. It has a simplified layer, but it does not have the overhead of TCP as a result of the simplification.

UDP doesn't care whether the packet is successfully sent, and does not reassemble data in order. Data may be interpreted as the order it was received and immediately forwarded. UDP does not have any mechanisms unlike TCP.

User Datagram Protocol (UDP) also has a header field, similar to the TCP header. Although it 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 header. Figure 20 illustrates the fields inside a UDPheader.

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 network layer is primarily in charge of allocating logical addresses (IP) that are used for network mapping. It also provides routing services, which is a process in which the network layer maps the network to determine the best path for moving data across the network. It converts data segments into what are known as packets. In this layer, we only use one major protocol: Internet Protocol, or IP for short. Although there are two types of IP based on their versions: Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) (IPv6). We'll go over this in more detail in the following contexts.

In the network layer, there are only two types of packets: data packets and route-update packets. Data packets are used to send user data across the network, whereas route-update packets are used by routers to keep their routing tables up to date. For the time being, it is not necessary for you to understand how route tables work and how these packets differ.

Characteristics of IP

IP is a network layer protocol, acts as a logical address for packets. It is known to have a connectionless nature. It has no connection with the IP address, which means that the IP does not know whether the data has arrived at its destination or whether it has been received by the intended user.

IP is known for its best-effort delivery. (Because best effort delivery implies no guarantee of delivery, IP does not guarantee receipt of all packets.) There is no way to recover corrupted or lost packets as they traverse the network.

Because IP is understood by both wireless and wired mediums, it is media independent. IP transports data across the network in a manner that is independent of other networks. Because the TCP/IP data link layer is in charge of processing and transmitting IP packets across a medium, IP is not limited to a single transmission medium. The network layer, on the other hand, considers the maximum number of frames that a medium can support (MTU). Because of how the Internet works, packets are sometimes split into smaller pieces and reassembled at the destination before being sent. The procedure has been dubbed fragmentation.

IPv4 Overview

An IP packet, like TCP and UDP, contains several important fields. The version, destination-specific, time-to-live (TTL), protocol, source, and destination IP addresses are all included in the 32-bit IPv4 packet header. The diagram below depicts the various sections of an IPv4 packet.

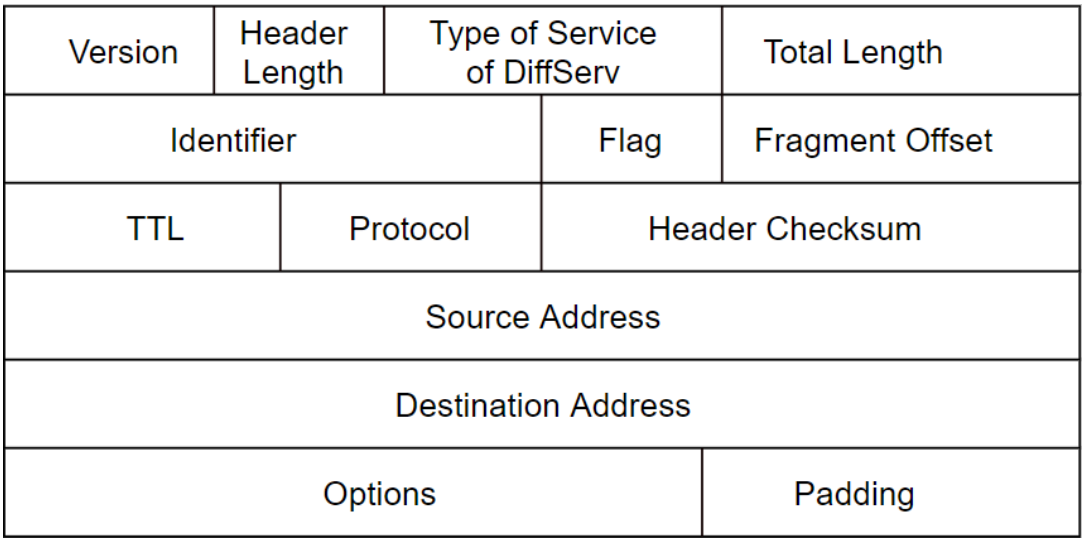


Figure 21 (IPv4 Packet Header, Fields)

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

Differentiated Services or DiffServ (DS) - The DS field, formerly known as the Type of Service (ToS) field, is an 8-bit field used to determine the priority of each packet. It is used to transport data in order to provide quality of service features. New technologies that require real-time data streaming and thus make use of the DSCP field are emerging. Voice over IP (VoIP), which is used for interactive data voice exchange, is one example.

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.

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.

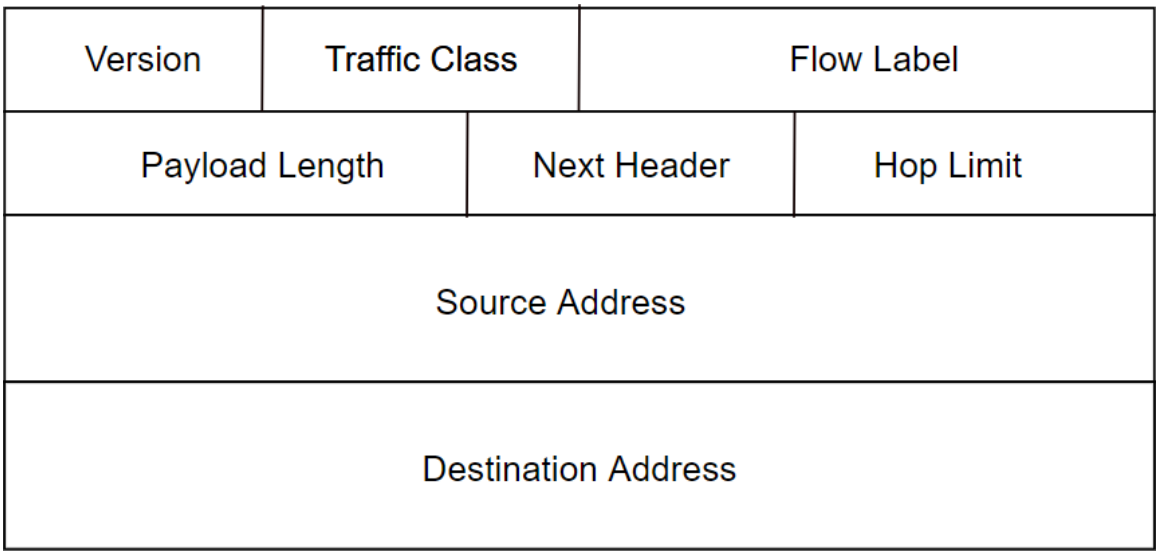


Figure 22 (IPv6 Packet Header, Fields)

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.

Data-link layer

The data-link layer is closely related to the physical layer it provides physical transmission and error notification and flow control. The data-link layer ensures that data's being sent locally reaches to its proper destination using hardware (MAC) addresses. The data link layer consists of two sublayers: The Logical Link Control (LLC) and the Media Access Control (MAC).

LLC is responsible for interacting with the upper and lower layers, preparing network packets to be sent through the physical media. As opposed to, MAC, it is mainly responsible for assigning unique hardware addresses, or what we call MAC address.

Encapsulation and De-encapsulation process

Before or during the transmission of a packet outside of a network, information must be held to guide it as it travels over the internet. A single data packet within a network is made up of multiple pieces of information. Each layer provides a header containing control information as the data passes through it. *Encapsulation* refers to the process of adding headers from each layer to a data set. While, *de-encapsulation* is the process of tearing down the headers so that the receiver can view them.

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 User information is converted in to data to best sent through the network.

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.

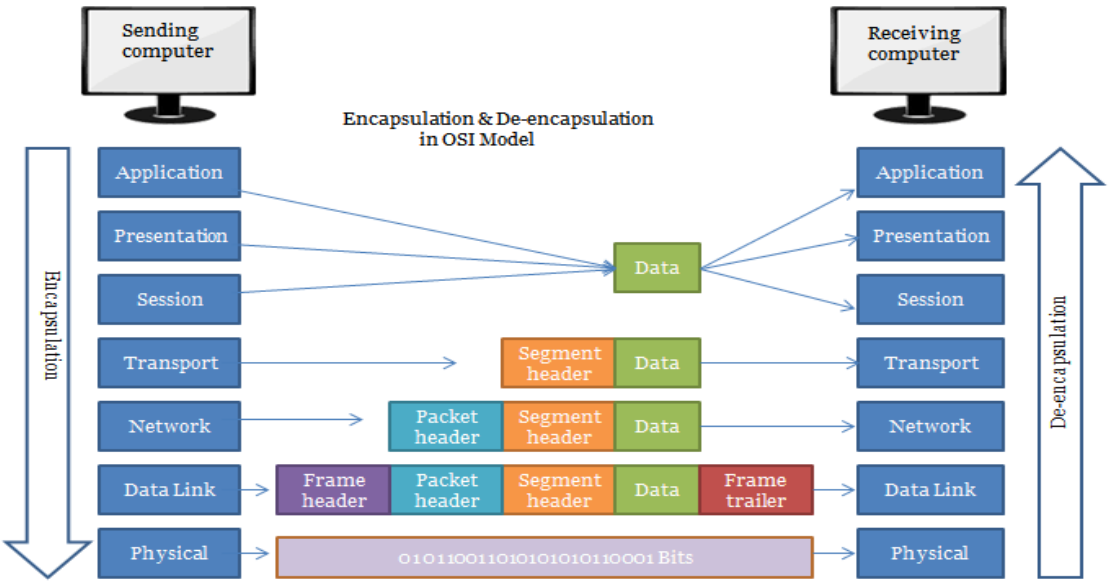
Step 4 Encapsulate the data supplied by the network layer inside a data-link layer header and trailer.

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

One explanation in this chapter spends considerable time demonstrating the steps involved in encapsulation because of the terminology. Inside a network stack, each layer communicates with each other. In order for them to communicate and exchange information, each layer uses Protocol Data Units (PDU) to encapsulate a data in a form of headers or trailers which contains control information.

Figure 3 depicts the process of encapsulation and de-encapsulation, along with the different protocol data units we use inside a protocol stack.

Figure 23 (Encapsulation, de-encapsulation process, and PDU)



Transmission methods

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

Multiplexing allows other network users to share a single data transmission connection across the network. When compared to segmentation, a single data set is divided into several segments, which initially improves the efficiency of data transmission networks. For example, if one or more messages are missing, only the missing parts or parts must be retransmitted.

Physical Layer Overview

The Physical layer offers the means for transporting the bits through the media in a form of signals. It converts bits to signals (i.e., electrical or digital signals) before transmitting across the medium. The physical layer 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.

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.

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.

Chapter Summary

This segment provided an in-depth overview of the layers of a networking model. The chapter is divided into five sections, each with a unique focus. The Application layer serves as the foundation for user interaction with the network. The Presentation layer is in charge of displaying the details in the proper format. The Session layer creates, manages, and ends sessions between data sources and record storage. The transport layer facilitates data transport from source to destination. The network layer provides network details, as well as a means of routing data and the internet, in addition to all of the functions that help this layer meet its requirements. The data link layer is in charge of preparing data for transmission across the transmitting medium. Finally, the Physical layer encodes data into the appropriate formats (signals) for 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 24 (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 to their 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).

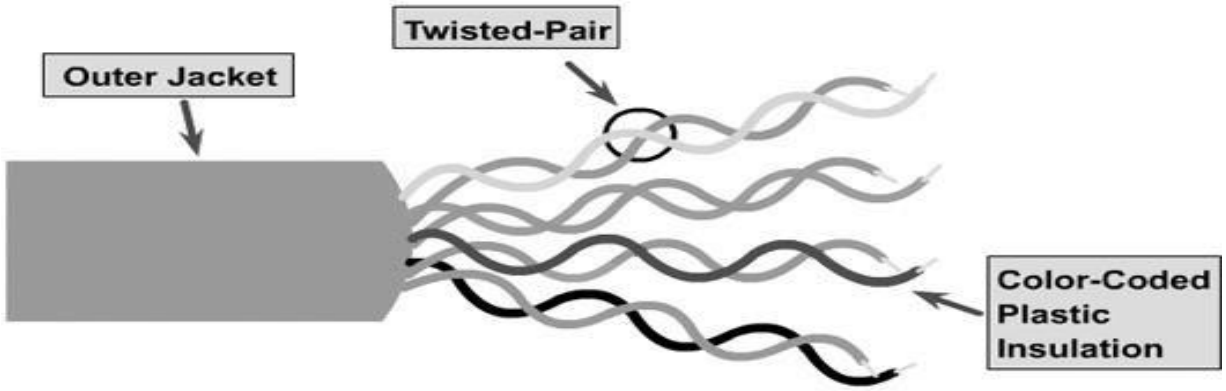


Figure 25 (Unshielded-Twisted Pair)
Image taken from: www.ciscopress.com

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 38

- 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…