The Media Layers of the OSI (Open Systems Interconnection) Reference Model: A Tutorial

Koffka Khan[1]

[1] The University of the West Indies

Received: 11 December 2019 Accepted: 1 January 2020 Published: 15 January 2020

Abstract

The Media Layers of the open systems interconnection (OSI) reference model convert bits to packets. It is a very important aspect of network communication and consists of various networking protocols. At the lowest level the physical layer deals with Media, Signal and Binary Transmission of Bits. Then there is the Data Link layer which deals with media access control (MAC) and logical link control (LLC) Physical Addressing of Frames, for example Ethernet. Finally, there is the Network layer which deals with Path Determination and IP Logical addressing of Packets. This article gives a review of these Media Layers and will contribute to adding knowledge for a networking novice while consolidating concepts for an experienced professional or academic.

Index terms— media, layers, OSI, physical, bits, data link, frames, ethernet, network, packets

1 Introduction

e first talk about being globally connected, then we're going to take a look at the internet, then we're going to look at the network as a platform and then we're going to look at the changing Network environment. So, what does globally connected mean in today's world? We are being increasingly connected more than any time in human history. The globe is getting smaller (not the actual earth!!!) but we as a people are able now to communicate around the globe in real time, whereas we weren't able to do that a hundred years ago. You know if you go back to about 1900 in the United States it would take you about one week to send a letter across the United States. But in today's world we have communication with cell phone technology, or we have chat technology, or we collaborate on videos or we can chat to with each other with text and there are people from the UK from Canada from United States and from New Zealand and Australia and we all communicate together and collaborate. So, the network really has no boundaries! We live and work in a global community, we communicate together through networks and on a global basis and we work, and we play together.

Let's take a look at what allows us to connect together globally. Networks connect us together. Networks come in many different sizes. We can have a small home office network where you might connect two or three different computers to a printer over a Wi-Fi link [58]. You might also have a file server [34]. However, you might not have a web server [24] on a home office or an office network but on a medium to large networks you are going to have those different devices. You're going to have some type of email service for email, a server for web clients etc. All these devices can be connected using a switch. You may have a router then that sends messages out of the network and again you'd have print sharing and file sharing [45], [66].

In this paper you would learn about clients and servers and what are clients and servers [8]. When you're talking about networks and when we hear the term client and server where the client is not necessarily a PC and a file server which is a very powerful computer. The term client and server typically means when you've got a client requesting information and the server provides that information. This model involves tow computers. Therefore, you in that could have two different computers "talking" to each other. One is requesting information from another (e.g. the file server). Note that in some network environments a computer "acts" as a server because it's serving up a file. It doesn't necessarily have to be a physical large server. Hence, in this case the two communicating machines (M2M or machine to machine communication [4], [13]) can be two different devices requesting information from each other.

When we talk about peer-to-peer networks [62] where you have devices that are connected without some type of server in place each computer can be both client and server. There are advantages and disadvantages to either client-server or peer-to-peer communication architectures. One advantage of peerto-peer is that it's easy to set up and is low cost. To set up doesn't take a lot of equipment and it doesn't take a lot of knowledge to be able to set up a peer-to-peer network. However, the security is not as good as you are not able to scale to a larger network easily. You're going to have to then go in and put routers in and create different setup connections.

When we're talking about different network components, you're going to hear the term end devices. End devices are those devices that are requesting information. They can be a computer, a mobile device [60], a tablet [57], or a Smart Watch [36]. An intermediary device are those devices that connect endpoints together or connects an endpoint to another network. They connect the individual end devices to the network and they ensure data flows across the network by providing connectivity. Examples of an intermediary device is a switch. Network media allows us to transmit that data we are transmitting ones and zeros. You'll learn about the OSI model [53] but the OSI model and the TCP/IP model [25] illustrates how the data gets broken down into ones and zeros. Once it gets broken down into ones and zeros it is transported across the network via various types of network media. Your media is going to be anything from the wireless or your wired cable that you have. You might have copper (category 5e or cat6 or coax) [10] or fiber optics [55] or wireless [74] or radio (Bluetooth) [9] to transmit over. You should familiarize yourself with the different networking icons and what they look like [20].

The network represented by physical and logical models. A physical model actually shows how devices are connected together while the logical model shows your IP addresses and information needed for computer to communicate. Thus, you have two different type of topology diagrams. The physical diagram shows the devices and then you have logical shows you the communication information that might be your IP address that might be your IPv4 address [42] and your IPv6 address [33]. There are different types of networks. You have Local area networks (LANs) [61]. A LAN usually span across a small geographical area. If you're in a classroom on a college campus or you're at a small cafe shop or you go to someone's house (they have three or four computers set up at their house) or in a small office are all examples of local area networks (LANs). All the computers can see each other, usually the devices are all interconnected together. At a house you can have a router that comes into your ISP provider [56] or cable provider [2] and then it gets sent to different devices. One can be for video gaming which forms its own local area network and then you can have the rest of the house into an another separate local area network so other family members can all "see" each other and can share files between computers or all persons can print to the same device that's usually going to provide some type of high-speed bandwidth to internal devices.

A wide area network (WAN) [16] connects multiple LANs together. You can kind of think of the Internet as a LAN because it's a lot of local area networks that are connected together. You might think of a college campus. Let's say that a college has three or four different locations and with those locations you're going to connect various LANs or different buildings together and then you're going to have a campus area network (CAN) [43]. There are more network types for example a metropolitan area network (MAN) [16] which might be a city that's connected together. The internet can be considered a large wide area network (WAN) but it's a worldwide collection of interconnected networks. The internet isn't one just one big network it's a bunch of networks connected together-a Network of Networks! and it's not owned by any one individual or group or country. It's really all of them connected together example you might have a government LAN that's connected into intermediary devices, you might have a branch LAN for a company, you know somebody at home is getting connected through their ISP (Internet Service Provider), you might have schools and you might have a large corporation maybe International Business Machines Corporation (IBM) is connecting into the internet or their ISP and so forth. A company's intranet means that communication is going to be only available internally. If you have your security set up properly no one outside the company is supposed to access company information. Extra nets [78] are not open to the public. They are opened up to the internal business then suppliers, collaborators, customers. You might have to have some type of login if you log into a portal into your college that you're attending.

When we're talking about how we connect to the Internet we have different types of connectivity. I've already mentioned the ISP which is an Internet service provider. That's a company that connects into a faster connection they have usually have some kind of fiberoptic system coming in to their local supply so for example where you live in the town then AT&T maybe your service provider and they have run cable from their main headquarters out to all the different homes and they pretty much can have all monopolies in your area. There is a DSL company but they're not very they can't really compete on speeds and there's a there's another company that offers a broadband wireless that you can put an antenna on your home or Digicel providing broadband cable [7]. Note that high-speed is not necessarily broadband and broadband is not necessarily high speed. Broadband just means that it's not the old plain old telephone the telephone system (POTS). It is usually coax or fiber optic cable. Broadband cable means you have broadband digital subscriber line or DSL [79] using the older copper phone lines. You might have Wireless that's connects to some mobile devices. Business DSL [54] is not much different than digital subscriber or broadband customers. It's usually the same lines but it is sometimes put in a different category. You can do leased lines and that's where you may have a company those might run anywhere from you know anywhere from $250 a month maybe up to $1,000 a month depending on where you are (location you live in) and those give you much faster access to the Internet. You can lease multiple lines so that you can have multiple company and then you also have Metro Ethernet [59]. Some towns local power company does provide some fiber optics to particular areas. However, they may not run it all the way to the city. Google is putting Google Fiber [3], [73] in two different cities if you're lucky enough to be in one of those cities you can get fiber optics from there and then the different types of Internet connections e.g. to a home or small office home office or business.

We use the term network as a platform where we talk about the term converged networks. The term converged means that things are being meshed together in traditional separate networks. Each network had its own rules and regulations. In pervious networks you have a network that only did email, you had a network that only did file service or only did the database and that was it. However, the converging network allows us to connect to devices that they have their own technology, that it's capable of delivering data voice, video over the same network infrastructure. Thus, when you hear the term converging network it means everything's being merged into the same network. It's using the same media so you don't put one line in for just doing an email server and interconnect endpoint devices and you're going to have totally different lines for your phones. We just don't do that anymore!!! Where are the converged network? The converged network may have a cat5e or cat6 cable coming in it, goes out to the desktop and it goes into the phone and then the phone connects over to the desktop and then that they all get the same Internet through a router. So the same cable is used. You have some type of medium that goes out and it's the devices and the messages that get sent on the same medium so that's the converged network.

There's four characteristics of a network architecture. The first one that you need to have is fault tolerance. Fault tolerance just means that it's not going to go down on you or there's backup to it so if you have multiple lines going to a server for example in a fault tolerant server you might have multiple power supplies so if one power supply goes down it runs on the backup or you may have two network cards into a server so you've got one as a backup. Lack of Scalability means that you can't upgrade that network and put more in devices on it without having to upgrade the major infrastructure. Scalability means that you put things in place so let's say that you put a router and you know a 24 port switch in place. You know Jim only have ten devices on it to begin with, well you know that you can scale all the way up to 24 devices on that switch without having to go and purchase a new switch. That's scalability. Quality of service (QoS) [41], [17]means that you're going to get is consistent bandwidth so for example if you know that you're supposed to be pushing 75 megabits of download speed you're going to consistently get 75 megabits of download speed that's an example of quality of service. Security is the last component and is a very important part of the whole overall network structure.

Bringing your own devices to work or to your workplace or to the college has become very popular in recent years. In the past companies didn't like employees bringing their own devices their own cell phones or iPhones. However, companies have realized that bringing your own device is OK and be able to get on the network because it keeps them from having to purchase it and it keeps them from having to support it other than just the connection to the internet or to the to the network yet allows for online collaboration. Online collaboration is growing e.g. Google Hangouts [15] or YouTube streaming. YouTube stream is essentially an online collaboration because in University students can come into that live stream and they can ask questions and the lecturer can answer those questions in live time on 2-way video communications. You've got Skype and Zoom etc. We have cloud computing where you can put your servers in the cloud. We have Amazon services; you've got Google services and Microsoft services. Cloud services [39] means don't have to store them locally. Cloud computing is putting your information up somewhere other than your local machine where others can access it.

Smart homes and the Internet of Things (IoT) [69] are some trends in technology where household devices communicate to each other and the outside world. You can connect on the Internet then you can put in devices on your refrigerators to monitor and buy your food. Power line networking uses the existing electrical wiring to connect devices together. Whether you realize you could do that or not the existing electrical wiring is copper wiring and you can then send your ones and zeros or you can send your network across the same electrical wiring and then we have wireless broadband. Now that's where you have a wireless internet service provider as you might put an antenna on your house that broadcast that across a wireless broadband service using cellular technology. Cellular technology also allows you to connect to the internet. If you don't have Wi-Fi you can turn your Bluetooth on and then broadcast over to your tablet and or even laptop. If you could get internet on your laptop you could use Bluetooth tethering [29] to get internet on your phone.

2 II.

3 Communication and Network Protocols

We're going to talk about rules of communication, we're going to talk about network protocols and standards and we're going to look at data transfer in the network. Why do we have rules of communication? What do we call rules? What are they? If we're going to communicate between two different languages and I want to speak to someone in English or in French and someone that's French wants to speak to me in English or from French to English. We must establish rules of how we're going to communicate. If I don't speak French and they don't speak English, then we're not going to be able to communicate. We must establish common rules for instance when we speak, we're going to use French or we're going to use Spanish. Let's say that we both speak Spanish, but the French-speaking person does not speak English and I don't speak French but we both speak Spanish so we're going to establish rules that when we communicate with each other we're going to use Spanish. That's an example of establishing rules in the networking world. We established rules and there's a group of people that get together and they establish rules. For example, let's assume there are two different networks and group says that they we're going to put this network together. They are going to set chosen protocols up, rules that are going to happen (so the rules that we establish in networking is that we identify the sender and receiver so we need to know who the sender is and we need to know who the receiver is), we need to have a common language and grammar, we need to have the speed and timing of the delivery established and we need confirmation or acknowledgement of requirements (if that's required then we look at message encoding: how are we going to encode those messages so that they can be sent through the system).

The process of converting information into another acceptable form is the message encoding. When a message goes from your computer to the wire or to a wireless medium, we need to know how that message is going to be encoded or translated, the message formatting and encapsulation, the message size, the message timing, the message delivery options is it going to be uncast multicast or broadcast.

We've established our rules now we're going to look at protocols and standards. We need to have protocols and standards because we need to let things work together. We're going to have a common 'thread' so devices can communicate with each other. The rules that govern communications are called protocols. Let's say that we're going to have an official meeting between two politicians, and we stablished protocols beforehand. We say when those politicians meet, they're going to shake hands then they're going to take pictures then they're going to talk with each other for 15 minutes and then then they're going to do another photo op. That's protocols we're establishing, what's going to happen. In the world of networking the role of protocols [22] we establish is how the message is formatted and structured, it's the process by which networking devices share information about pathways with other network and it's how and when error system messages are passed between devices. The protocol also does the setup and termination of data transfer sessions. The protocol interaction would be for example between a web server and a client. For example, we establish a protocol and I have a computer and I open up a browser and that browser has certain protocols to say okay I'm going to want a web page pull down to my computer. Well there's certain protocols in place to say I need it in a particular format for instance, I need it in HTML [44] format and so it establishes those protocols to do that.

We have a client it goes through the Internet of the cloud and it sends a packet of information and it says I need to get information from this web server, so the protocol stack says we're going to use HTTP (Hypertext Transfer Protocol) [46]. We're going to use Transmission Control Protocol (TCP) [68] and then Internet Protocol (IP) [70] and then we're going to go across the Ethernet so that's our set of protocols or how they are established.

We have protocol Suites and there's been a number of them. The TCP/IP is an open standard [28]. The TCP/IP is the one of the most common that we use today in networking. The TCP/IP models have your application layer, your transport layer, your internet layer and your network access layer. In each layer you have these different protocols that we set up for example you know at the application layer we set up DNS [50]or you set up by FTP [27] or HTTP and then down at the network access layer you set up Ethernet to be able to go across your medium.

Standards organizations like the International Organization for Standardization (ISO) [31] sets up open standards. There are some advantages to open standards are that they can be easily adopted by anybody, they're not controlled by any one person because they're put out on the market. We still have organizations that get together and they regulate open standards. The TCP/IP model benefits by having a reference model (OSI model). The Open Systems Interconnection (OSI) [81] is layered and provides a list of functions. There are seven layers. It describes the interaction between the layers. You do need to memorize the OSI and TCP/IP models if you're going into networking. There are relationships between the two models for example you have the top three (five six and seven) of the OSI model have been collapsed into the application layer on the TCP/IP side and the transport layer is the same, the network layer is called Internet on the TCP/IP and the bottom two (the data link and the physical layers) have been collapsed into the network access layer. Thus, the TCP/IP model is not simpler, it's just collapsed down into four layers instead of seven.

When we transfer data, we have to put it onto the medium and we have to send it along. We can't just send a whole bunch of ones and zeros as the receiving side needs to know when each individual packet is finished. It needs to know what requests came from who or in what order else all those ones and zeros would just get me garbled and the receiver wouldn't be able to make sense of anything. It wouldn't be able to communicate. Thus, based on our protocols we say we're going to have message segmentation (segmentation means that we're going to break that communication into pieces) so we're going to take those ones and zeros and we're going to segment them out into little blocks. Multiplexing [1] is another term (also called interleaving) the pieces which means that they can arrive at different times and then be put back. Encapsulation means that when we are going down the protocol stack and I'm going to move back up to the other end, we encapsulate data. What we're doing is we're taking information at a layer and we're sending it down the OSI model. At the packet is being encapsulated so information is taken, and it's taken to the next layer and it's sent along etc. For example, I'm going to add some information to a layer and then when it gets to the another layer I'm going to add the networking address, you know what where is it coming from where's it going to at the network and then the data link information and when I get down to another layer I'm going to give it what medium it's going to go on so by the time it gets down to this layer we have a full packet. The full packet gets put onto the medium whether it's wireless or wired. It gets sent along and when we get to the other end that full packet information comes. It gets de-encapsulated as it goes back up. It gets up to the application, let's say if it's a web browser or an email client.

For data access we have our network addresses (we have our source IP address, we have our destination IP address) that can either be an IPv4 or IPv6. The addresses ensures the delivery of the IP packet from the original source to the final destination either on the same network or the remote network. The data link addresses (you have the source data link address and you have the destination data link address) ensures the delivery of the data link frame from one network interface card or NIC [11] to another NIC card on the same network. Therefore, the difference between network addresses and data link addresses is that one sends it from one destination to the other on the same network or remote network and the data link addresses are on the same network.

4 III.

5 Network Access

The data link layer protocol is made up of sublayers. You have the logical link control (LLC) [52] which communicates with the network layer and then you have the Mac which defines the media access processes. The term MAC address [40] is "a bit of" the data link layer. Data link layer standards are Institute of Electrical and Electronics Engineers (IEEE), International Telecommunication Union (ITU), ISO and American National Standards Institute (ANSI). We saw some of these previously when discussing the Physical layer. Now media access control is when we control access to the media. But what does this mean? What we're really talking about is the topologies (physical topology and logical topology). Our physical topology is when we're saying what is the actual equipment. So, when you design your physical topology, you're laying your physical topology out. You are going to say I've got a server in a room; I've got a switch at a location and a router located elsewhere. It's going to show where everything is and it's going to label everything so you're going to know where physical equipment it is. Logical topology is the arrangement of devices on a computer network and how they communicate with one another. Logical topologies describe how signals act on the network. For example, you may have switch 1 (S1) but, on the diagram, we're listing out which connection it's tied to. We're giving our IP address [23]; we're saying this is on G0/0 (the link going out to the Internet). We're giving our IP address for that subnet. We're not giving out all the IP addresses we're just saying this is the subnet IP range.

The common physical LAN topologies are point-to-point, hub-and-spoke and mesh [37]. Point to Point topology is the simplest topology that connects two nodes directly together with a common link. A hub and spoke network is a traditional, proven, and widely used topology for all types of networks; it's also called the star topology. Essentially, the access point is physically connected to the Internet with a wire; like spokes on a wheel, all user devices connect to the wireless router in the center. A mesh topology can be a full mesh topology or a partially connected mesh topology. In a full mesh topology, every computer in the network has a connection to each of the other computers in that network. Mesh is more expensive to put into place because you have more wiring in place or you have more media connecting it but it has more redundancy to it. Two star networks connected gives a hybrid. Half duplex [38] of a communications system or computer circuit allows the transmission of signals in both directions but not simultaneously. Full-duplex [38] data transmission means that data can be transmitted in both directions on a signal carrier at the same time.

Carrier Sense Multiple Access or CSMA [71] is a Media Access Control (MAC) protocol that is used to control the flow of data in a transmission media so that packets do not get lost and data integrity is maintained. There are two modifications to CSMA, the CSMA CD (Collision Detection) [64] and CSMA CA (Collision Avoidance) [14], each having its own strengths. CSMA operates by sensing the state of the medium in order to prevent or recover from a collision. A collision happens when two transmitters transmit at the same time. The data gets scrambled, and the receivers would not be able to discern one from the other thereby causing the information to get lost. The lost information needs to be resent so that the receiver will get it. CSMA CD operates by detecting the occurrence of a collision. Once a collision is detected, CSMA CD immediately terminates the transmission so that the transmitter does not have to waste a lot of time in continuing. The last information can be retransmitted. In comparison, CSMA CA does not deal with the recovery after a collision. What it does is to check whether the medium is in use. If it is busy, then the transmitter waits until it is idle before it starts transmitting. This effectively minimizes the possibility of collisions and makes more efficient use of the medium. Another difference between CSMA CD and CSMA CA is where they are typically used. CSMA CD is used mostly in wired installations because it is possible to detect whether a collision has occurred. With wireless installations, it is not possible for the transmitter to detect whether a collision has occurred or not. That is why wireless installations often use CSMA CA instead of CSMA CD. Most people do not really have to deal with access control protocols as they work behind the scenes in order for our devices to work together. CSMA CD has also fallen out of favor with modern wired networks as they were only necessary with hubs and not with modern switches that route the information instead of broadcasting it. Summary:

1. CSMA CD takes effect after a collision while CSMA CA takes effect before a collision. 2. CSMA CA

reduces the possibility of a collision while CSMA CD only minimizes the recovery time. 3. CSMA CD is typically used in wired networks while CSMA CA is used in wireless networks.

A frame is a unit of communication in the data link layer. Data link layer takes the packets from the Network Layer and encapsulates them into frames. If the frame size becomes too large, then the packet may be divided into small sized frames. At receiver' end, data link layer picks up signals from hardware and assembles them into frames. Each frame type has three basic parts: Header, Data and Trailer. The structure of the data link layer frame may be specialized according to the type of protocol used. The frame structure used in two protocols: Point -to -Point Protocol (PPP) [65] and High-level Data Link Control (HDLC) [26] will be different.

We're going to be looking at the physical layer protocols we talked about protocols in previous slides as well as we're going to be talking about the physical layer protocols in these slides. We're going to be looking at Network media, the data link layer protocols and the media access control. Now we are going to identify types of network connections. When we talk about the physical layer connections, we're talking about how we transfer data from one end point to another end point or from an end point to another device. The different types of connections we have maybe a Cisco [77] wireless router or a home router. On the diagram of the router: Your Ethernet switch is where you can plug in your Ethernet cable. Your internet connection is where you put your LAN port. Your embedded wireless antenna doesn't actually pop up but some do. You can use wireless as well broadcast to a wireless card so the network interface card or you'll hear the term NIC. You can connect NICs in a lot of different ways. You can plug in an Ethernet cable to an RJ-45 connection [30] or you can use wireless routers. You can use also put our range extenders. This picks up the signal from the wire or from the router and then passes it on to devices so that if you're not getting a signal far enough you can put those in place.

The purpose of the physical layer is to accept a complete frame from the data link layer and encodes it (remember the encapsulation and de-encapsulation processes [21]. It encodes it as a series of signals that are transmitted onto the local media (it encapsulates the message and it sends it on the media). The digital signal consists of ones and zeroes. You can describe the physical layer media types by either Ethernet which is your copper or you can have fiber optics which is your light-emitting or you can have Bluetooth transmission or you can have wireless transmission through Wi-Fi and there's a few other ones too.

We have standards in place for physical layer. The standards organizations we talked about those in previous slides. Here we're talking about physical layer standards. You have those organizations that say if you're going to do a physical layer or standards in place that says they have to meet these certain specifications. E.g. Ethernet must have X amount of wires and it has to be a certain diameter and it has to be able to carry a certain amount of signal and so forth. These Standards are set forth in that physical layer characteristics. You have the functions of the physical layer, you have the physical components to it, you have encoding and signaling and the functions supporting the data transfer. The data transfer is impacted by the bandwidth. The term bandwidth means the capacity to a medium to carry data e.g. a highway or a road can fit a maximum of 2 or 8 lanes of cars. A small bandwidth might have a two-lane road with traffic going both ways and if you want to increase your bandwidth you add more lanes to that highway so you may have a six-lane highway where you have three lanes on each side or you have three lanes or six lanes of traffic that you can send data. Bandwidth is the "size" of the medium that you can transfer data through. Throughput is a little bit different. It is the measure of the transfer of bits across the media. Thus, bandwidth is how much capacity you have, while your throughput is the actual measure of the transfer of bits. The actual throughput of the data that's actually being sent through occurs over different types of physical media. Copper cabling [47] is one of the most common physical media in networking. The reason it's so common is because it's inexpensive compared to other types of media. Fiber optics is expensive where Ethernet or copper cabling isn't expensive. Ethernet or copper cabling is inexpensive, it's easy to install, it's low resistance to electrical current, the distance and the signal interference is also a good. Characteristics of the copper cabling is that you have pretty good distance with it, and depending upon which category of Ethernet you have or which category of cabling you have it's going to go different differences based on whether it's a coax cable or an Ethernet. Different types of copper cabling are unshielded twisted-pair and shielded twisted-pair. Unshielded twisted-pair is less expensive as shielded twisted-pair uses some extra material (the shielding that goes over the wiring). Let's explore the reason for shielding. Let's say for example you're going to be putting in copper cabling and you've got to put it in next to some high-voltage lines or you're going to be putting it in next to some lights that are causing some interference. You're going to get some kind of electrical interference, so we have to put shielded twisted-pair in so the interference doesn't impact the data being sent to those copper cables. It's shielded so will cost you more. However, the unshielded cheaper but it's more susceptible to interference.

Unshielded twisted pair (UTP) cable [67] cancels out Electromagnetic interference (EMI) and Radio Frequency Interference (RFI) signals. You have different types of UTP cable: rollover, crossover and straight through. They are different depending upon how you put the wires through so depending on how the signals get sent through whether it's a rollover or crossover. You can also test you unshielded twisted-pair cable based on the cable pin outs. A device I can plug a point in and then I can use another little small cable that plugs in on the other end or I can plug both ends in and it will send a signal through the wire to tell me is it wired properly. This is the t568a and this is a t568b. The device is going to tell me whether I need a rollover a crossover or straight through. The device is going to tell me if I got that proper wiring done and did those signals get sent through which wires (wire one, two, three, four, five, six, seven, eight) and if is it correct on both ends.

Fiber-optic cabling allows you to transmit data over long distances. I mean much longer distances than regular unshielded twisted-pair Ethernet. It's flexible but the thin strands of glass can be broken so you must be careful when you handle it. It transmits with less attenuation which means it has less signal loss over a greater amount of distance and it's immune to EMI and RFI. It's immune to electromagnetic interference and radio frequency interference. If you do break a bundle of fiber optics cable it takes special tools to reconnect those back up. If you cut an Ethernet cable, it's easy just to take those pairs of wires and connect them back in.

Fiber optics types include media single mode and multimode. You have fiber optic connectors that go on the end. Now we talk about UTP vs Fiber optics. Fiber optics is much more expensive to use so that's why you usually run fiber optics on longer distances or maybe between buildings. Thus, if you're connecting two local area networks together you may see fiber optics go between those buildings. You might see a city having fiber optics being put in and then when you get to the local building or the local area network is where you might use copper for the local area network. Bandwidth support from UTP is up to 10 gigabits, while on fiber optics it is from 10 megabits all the way up to a hundred gigabits. The distance is about 100 to 100,000 meters for fiber optics, while it's one to a hundred meters for UTP. UTP is very susceptible to EMI, RFI and electrical hazards, while fiber-optic side and it come completely immune to EMI, RFI and electrical hazards. However, the high cost, installation skills and safety precautions are impediments for fiber-optic usage.

Data communications over wireless media using radio or microwave frequencies passes distances which are much smaller or much shorter based upon what you're using that is, whether it's Bluetooth or Wi-Fi Bluetooth. Wi-Fi is over a much smaller range. There are different types of Wi-Fi e.g. we have Wi-Fi Bluetooth and WiMAX. There's some other ones out there too e.g. Wi-Fi-802.11a [19], Wi-Fi-802.11b [19], Wi-Fi-802.11g [19] and Wi-Fi-802.11n [6]. The first WLAN standard was created by the Institute of Electrical and Electronics Engineers in 1997. They called it 802.11 [32] after the group's name that was established to monitor its growth. Unfortunately, 802.11 only endorsed a maximum network bandwidth of 2 Mbps which was too slow for most applications. Therefore, 802.11 wireless products are no longer produced. However, from this original standard, a whole family has emerged. At home you may have a Wireless local area network and you might have a router. The router you may have set up and you have your you have your Wi-Fi come in to it. Then you broadcast out and your different devices pick up that signal and they can connect to the internet or your network based upon protocol set up. Thus, if you have Wi-Fi set up let's say on a mobile device and you can connect to the router and get signal and we call the router a wireless access point. A wireless access point allows you to broadcast messages out. There are also wireless NIC cards or Wireless NIC adapters. You can put a wireless NIC adapter on most laptops. However, before 2017 some older ones did not have NICs and you would have to plug those in using a wired connection for them to receive any network signal.

6 IV.

7 Ethernet Protocol

We're going to talk about Ethernet protocol, we're going to look at the sub layers and the Ethernet MAC address, we're going to look at LAN switches and we're going to look at address resolution protocol or ARP [5]. Ethernet encapsulation is when the ethernet operates in the data link layer and the physical layer. Ethernet supports data bandwidth from 10 megabits through 100 gigabits and Ethernet standards defined both the layer 2 protocols and the layer 1 protocols of the OSI model. The MAC sub-layer constitutes the lower sub layer of the data link layer and it's responsible for the data encapsulation and media access control. Ethernet has been evolving since its creation in 1973. Ethernet frame structure adds headers and trailers around the layer three PDU to encapsulate the message being sent. The minimum Ethernet frame size is 64 bytes and the maximum size is 1518 bytes. The frames frame smaller than the minimum or greater than the maximum are dropped. This is because anything smaller or greater could be the result of collisions or unwanted signals. A collision means you get data that hit each other and didn't come all the way through so you have an incomplete frame. If it's lower than 64 you know let's say if it's 61 bytes that's an invalid frame and if it's 1520 that's got extra signal information in there (there's ones and zeros in there that could be corrupt or not wrong information). Thus, the layer just drops those frames as well.

Your Ethernet Frame Fields include your preamble, your destination MAC address, your source MAC address, your Ether Type, your data and then your FCS field. The Ethernet MAC address or MAC addresses or media access control address is written in hexadecimal. It's 48 bits long and expressed as 12 hexadecimal digits. The vendor must use the assigned to the first three bytes so if you look at a machine address code or if you look at a MAC address you can look at the first three bytes and you can research that on the internet and you can find out who the vendor was of that of that that device. All MAC address is with the same OUI (Organizationally Unique Identifier) must be assigned a unique value in the last three bytes. When frames are processed the NIC card compares the destination MAC address in the frame with the device's physical MAC address stored in RAM. If there's a match that frame is passed up the OSI layer. If it doesn't match it passes it on, it discards that frame. It reads all the way up to the destination MAC and it then discards the rest, but it does read it partially. Thus, it does read all frames that come across that local area network. A representation of a MAC address: 00-50-2D-3B-07-BD. It can be represented with colons, dashes or dots and is case insensitive, so it doesn't matter if you capitalize B or C.

Let's talk about unicast broadcast and multicast. A unicast address is used when a frame is sent from a single transmitting device to a single destination device. It is one to one (1-1). A broadcast MAC address is used to address all nodes in a segment. The destination MAC address is the FF FFFFFFFF. It's a 48 1s in binary. It's one too many (1-M) or one too all (1-A). A multicast MAC address used to address groups of nodes in the segment or endpoints. The multicast MAC address is a special value that begins with the first six hex digits and within an IP range. It's one to some (1-S).

Let's switch gears to LAN switches so what are switches. They operate at the layer 2 of the OSI model. An Ethernet switch is a layer 2 device. A switch is a layer 2 device. Sometimes you have hybrids, you have hybrid routers and switches and so those are at layers 2 and 3, but we're just talking about just switches. At this point it uses the MAC address to make forwarding decisions. It does not need IP addressing because IP addressing (IPv4, IPv6) goes to the layer 3 of the OSI model. The MAC address table is sometimes referred to as a content addressable memory or CAM table. The switch will build a table, a MAC address table [48]. Now learning the MAC addresses. Switches dynamically build the CAM by monitoring source MACs. When you plug a device into a switch the switch will start broadcasting and saying who's out there, who is this connected too and the end device if it's set up properly will broadcast back and say hey I'm here, I'm a network interface card and here's my MAC address (and here's a base basic information). Thus, the switch builds a table so every frame that enters a switch is checked for new addresses and the frame is forwarded based on the CAM. The switch does really if you think about what the old-time telephone switch operators do. A person sitting there at a switchboard. They say. "ok who are you calling" and you say "well I'm calling number 0 0 1" and the operator says "ok well let me plug you into that person" and then the next person says "okay I'm calling 0 0 3" and the operator says "well I will plug you into 0 0 3." But you're not actually routing it outside the network because that's a router's job. You are keeping it internally on that local area network (LAN). Since the switch knows where to find specific MAC addresses it can filter frames to that port only. Filtering is not done if the destination MAC is not present in the CAM. Once the tables been built it can dynamically forward those frames, but it needs to build that table first to be able to do that.

Local Area Network (LAN) Switches [63] support different Switching Methods. Important Switching Methods are store and forward, cut-through and fragment-free. Switching Methods determine how a switch receives, processes, and forwards a Layer 2 Ethernet frame. Frame forwarding methods has storeand-forward and cut through switching. Cut through switching is a method for packet switching systems, wherein the switch starts forwarding a frame (or packet) before the whole frame has been received, normally as soon as the destination address is processed. It is fast forward switching, it's the lower lowest level of latency. Low latency and speed is obtained as it immediately

The Media Layers of the OSI (Open Systems Interconnection) Reference Model: A Tutorial

8 Global Journal of Computer Science and Technology

Volume XX Issue I Version I 36 Year 2020 ( ) forwards a packet after reading the destination address. In cut-through switching, the switch copies into its memory only the destination MAC address (first 6 bytes of the frame) of the frame before making a switching decision. A switch operating in cut-through switching mode reduces delay because the switch starts to forward the Ethernet frame as soon as it reads the destination MAC address and determines the outgoing switch port. Problem related with cut-through switching is that the switch may forward bad frames. Fragmentfree (runtless switching) switching is an advanced form of cut-through switching. Fragment free switching switch stores the first 64 bytes of the frame before forwarding. The switches operating in cut-through switching read only up to the destination MAC address field in the Ethernet frame before making a switching decision. The switches operating in fragment-free switching read at least 64 bytes of the Ethernet frame before switching it to avoid forwarding Ethernet runt frames (Ethernet frames smaller than 64 bytes). In Store and Forward switching, Switch copies each complete Ethernet frame into the switch memory and computes a Cyclic Redundancy Check (CRC) [12]for errors. If a Cyclic Redundancy Check (CRC) error is found, the Ethernet frame is dropped and if there is no Cyclic Redundancy Check (CRC) error, the switch forwards the Ethernet frame to the destination device. Store and Forward switching can cause delay in switching since Cyclic Redundancy Check (CRC) is calculated for each Ethernet frame.

An Ethernet switch [35] may use a buffering technique to store and forward frames. Buffering may also be used when the destination port is busy. The area of memory where the switch stores the data is called the memory buffer. This memory buffer can use two methods for forwarding frames, port-based memory buffering and shared memory buffering. In port-based memory buffering frames are stored in queues that are linked to specific incoming ports. A frame is transmitted to the outgoing port only when all the frames ahead of it in the queue have been successfully transmitted. It is possible for a single frame to delay the transmission of all the frames in memory because of a busy destination port. This delay occurs even if the other frames could be transmitted to open destination ports. Shared memory buffering deposits all frames into a common memory buffer which all the ports on the switch share. The amount of buffer memory required by a port is dynamically allocated. The frames in the buffer are linked dynamically to the destination port. This allows the packet to be received on one port and then transmitted on another port, without moving it to a different queue. The switch keeps a map of frame to port links showing where a packet needs to be transmitted. The map link is cleared after the frame has been successfully transmitted. The memory buffer is shared. The number of frames stored in the buffer is restricted by the size of the entire memory buffer, and not limited to a single port buffer. This permits larger frames to be transmitted with fewer dropped frames. This is important to asymmetric switching, where frames are being exchanged between different rate ports.

Full duplex means that both ends of the connection can send and receive simultaneously. Half duplex means that only one into the connection can send at a time. Automatic medium-dependent interface crossover (Auto-MDIX) [80] is a feature that allows the switch interface to detect the required cable connection type (straight-through or crossover) and automatically configure the connection appropriately. Auto MDX detects the type of connection required and configures the interface accordingly. It helps reduce configuration errors. What happens is that the newer devices have Auto MDX on them will automatically detect and set its connection to full duplex if the other person is using this. Layer 2 addresses are used to move the frame within the local network. That's key to remember when we're at the layer 2, we're staying with inside the local area network. Layer 3 addresses are used to move the packets through remote networks which are outside your LAN. That's when it goes to the routing portion and gets routed somewhere else. A destination on the same network: physical addresses or MAC addresses are used for Ethernet NICs to Ethernet NIC communications on the same network. They communicate on the LAN without being routed and use layer 2 only. If you need to route outside of your LAN, you will go to your layer 3 and start to use IP addressing. ARP is address resolution protocol that is the combination of MAC and IP to facilitate to end-to-end communication. Address Resolution Protocol (ARP) is a procedure for mapping a dynamic Internet Protocol address (IP address) to a permanent physical machine address in a local area network (LAN). The physical machine address is also known as a Media Access Control or MAC address. The job of the ARP is essentially to translate 32-bit addresses to 48-bit addresses and vice-versa. This is necessary because in IP Version 4 (IPv4), the most common level of Internet Protocol (IP) in use today, an IP address is 32-bits long, but MAC addresses are 48bits long. ARP works between network layers 2 and 3 of the Open Systems Interconnection model (OSI model). The MAC address exists on layer 2 of the OSI model, the data link layer, while the IP address exists on layer 3, the network layer. In IPv6, which uses 128-bit addresses, ARP has been replaced by the Neighbor Discovery protocol [51]. When a new computer joins a LAN, it is assigned a unique IP address to use for identification and communication. When an incoming packet destined for a host machine on a particular LAN arrives at a gateway, the gateway asks the ARP program to find a MAC address that matches the IP address. A table called the ARP cache maintains a record of each IP address and its corresponding MAC address. All operating systems in an IPv4 Ethernet network keep an ARP cache. Every time a host requests a MAC address in order to send a packet to another host in the LAN, it checks its ARP cache to see if the IP to MAC address translation already exists. If it does, then a new ARP request is unnecessary. If the translation does not already exist, then the request for network addresses is sent and ARP is performed. ARP broadcasts a request packet to all the machines on the LAN and asks if any of the machines know they are using that particular IP address. When a machine recognizes the IP address as its own, it sends a reply so ARP can update the cache for future reference and proceed with the communication.

V.

9 Network Layer

We discuss the network layer protocols so we're doing the layer 3, we describe the purpose of the network IPv4 vs. IPv6 and we're going to take a look at routers. What is the network layer? The network layer is the layer 3 of the OSI model. In the previous sessions we looked at the physical and the data link layer. We looked at switches in previous session and how those worked. Well in this session we're going to look at the networking layer. The networking layer provides end-toend transport processes. It addresses devices, it encapsulates, it routes and it de-encapsulates. The layer of protocols that we're going to talk about and use is the IPv4 and IPv6. In the case of the sender the layer 3 is going to encapsulate data, it's going to take the data and encapsulate it and send it down to the network stack. The network layer is going to encapsulate the information and say okay here's my IP address and so forth and then the layer 2 is going to put the MAC addressing information and it's going to send it down to the physical medium. Let's talk about the characteristics of the IP protocol. When we encapsulate the IP segments into IP packets for transmission the network layer adds a header so packets can be routed to the destination. If you have IP connectionless it means the sender doesn't know if the receiver is listening or whether the message arrived on time. The receiver doesn't know anything that is coming so when you hear IP connectionless you just mean that the sender is trying to send the information but with no guarantees. In some countries when you send a piece of mail to the Postal Service you just put a piece of mail in your mailbox. A postal worker picks it up that morning. The person receiving the mail may or may not know that they're getting a piece of mail. On the other end that mail just shows up so that's connectionless. But if you go to the post office and you say I want to send this piece of mail but I want a return receipt. This means when the main gets to the receiver the person that receives the piece of mail signs a piece of paper and says "yes" I've received this message/mail and then you get the message/mail back. This would be connection oriented. IP best effort delivery means there's no guarantees that a delivery is going to be made. The IPv4 packet has been around a long time but it's being phased out. IPv6 is coming in because we ran out of IPv4 addresses. But IPv4 is going to be around for a long time. It is still very important. We now look at the IPv4 packet header and packet information. We have version, Internet header length, differentiated services, total length, identification, flag, fragment offset, time-to-live, header checksum, source IP address and destination IP address. The time-to-live means the packet will not hang out on the network forever. It's just going to say it's got so this got so long to live and if it doesn't get to its destination in an amount of time it just going to be destroyed. You don't want packets just floating around forever and gumming up everything. The IPv6 address space has improved packet handling and it eliminates the need for network address translation (NAT) [75]. You don't have to do NAT tables anymore which is nice because every device has an IPv6 address. Thus, encapsulating the IPv6 you have a simplified header format. There's no checksum process so it's more efficient. We have version, traffic class, flow label, payload length, next header, hop limit, source IP address and destination IP address. The 20-bit flow label field in the IPv6 header can be used by a source to label a set of packets belonging to the same flow. A flow is uniquely identified by the combination of the source address and of a non-zero Flow label. The purpose of flow label is to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. The flow label field makes routing more efficient. A Next Header field in the IPv6 header indicates the next extension header. Within each extension header is a Next Header field that indicates the next extension header. The last extension header indicates the upper layer protocol (such as TCP, UDP [76] (User Datagram Protocol), or ICMPv6 [18] (Internet Control Message Protocol, version 6)) contained within the upper layer protocol data unit. The 8-bit field also puts an upper limit on the maximum number of links between two IPv6 nodes. In this way, an IPv6 data packet is allowed a maximum of 255 hops before it is eventually discarded. An IPv6 data packet can pass through a maximum of 254 routers before being discarded. The 16-bit payload length field contains the length of the data field in octets/bits following the IPv6 packet header. The 16-bit Payload length field puts an upper limit on the maximum packet payload to 64 kilobytes. You have your source IP address and your destination IP address. We've looked at IPv4 and we've looked at IPv6 so now let's take a look at routing.

When we are leaving the local area network there needs to be a decision about the next hop. There's three types of destination. You can send it to yourself, the local host or remote host. The router reads the routing information it gets and says ”I'm not going to do anything with this packet again” or ”I will send it to a computer within my LAN” or ”do I need to send it out to my remote host.” (via my remote connections). You can set up a default gateway. It's typically a router that goes outside the local area network. It routes traffic to other networks. It has a local IP address in the same address range as other hosts on the network. It's a gateway, it's a gatekeeper, it tells what goes in and out of the LAN. The host will use the default gateway when sending packets to remote host. You can use the netstat command netstat dash R to display the hosts routing table on a Windows machine and you would get the same thing on Linux. A router routing tables have a forwarding decision to make. Routers and host forward packets in a similar fashion. However, the main difference is that routers have more interfaces, while hosts have only one. Devices on a remote network are reached through a gateway. In the IPv4 routing table the router routing table stores information that the router knows about. You can use ”show ip route” to display the routing table. The table also has information on how the route was learned, its trustworthiness and a rating on it. It also contains which interface to use to reach that specific destination. Directly connected routing table entries can be either C or an L. C identifies a directly connected network. It's automatically created when the interface is connected with an IP address and activated. L identifies if this is a local interface. This is the IPv4 address of the interface on the router.

We now look at remote network routing table entries. A remote destination can't be reached directly so packets have to be routed. Remote routes contain the addresses of the intermediate devices to be used to reach the destination. A router in a LAN knows nothing about the devices in another LAN. Thus for the two to communicate, the router in one LAN says ”hey I've got a packet but I've got an ID” (let's just say that two end device are trying to communicate), the router says ”ok well that's not on the local network so let me forward this onto my known destinations, and I'm going to forward it to this next router.” An intermediate router picks up the message and says ”hey wait a minute I know that IP address, it's on my routing table and I'm going to forward it on internally.” (The IP is on the intermediate router's LAN). Then the switch on the same LAN forwards it on through based on MAC addressing (that ARP table that we talked about in the previous sessions, where you have an ARP table and an IP address that are that are known). The next hop is among the series of routers that are connected together in a network and is the next possible destination for a data packet. More specifically, next hop is an IP address entry in a router's routing table, which specifies the next closest/most optimal router in its routing path.

The physical anatomy of a router. They have a CPU, they have memory, they have input/output devices, they use an operating system, they have power supplies, they have RAM built (your main RAM is built into the board), they have ROM and flash memory. They have lots of ports that support different types of connections. You have LAN and WAN interfaces. routers have LAN and WAN ports with LAN being local and WAN being white area. Different models ship with different ports depending upon the age. Ethernet it's a very common on different router models. When you're talking about the software the iOS image file is stored in the flash. Flash stores other system files and NVRAM [49] (Non-volatile random-access memory) stores configuration parameters. Your ”startup-config” is in NVRAM. Random access memory is your running memory that gets that gets reset every time the device reboots. When you boot up the router says ”ok I'm going to go to my flash, what image do I have? let me load that, do I need to load any other system files? then I'm going to go to NVRAM to pick up my configuration file and start running. In RAM I will now have my iOS [72] running, my running config and any changes I make. Remember you need to save those changes to your startup-config or the next time you reboot those changes won't work. You can also do a show version output to get the amounts of memory installed.

10 VI.

11 Conclusion

The Media Layers of the open systems interconnection (OSI) reference model convert bits to packets. It is a very important aspect of network communication and consists of various networking protocols. At the lowest level the physical layer deals with Media, Signal and Binary Transmission of Bits. Then there is the Data Link layer which deals with media access control (MAC) and logical link control (LLC) Physical Addressing of Frames, for example Ethernet. Finally, there is the Network layer which deals with Path Determination and IP Logical addressing of Packets. This article gives a review of these Media Layers and will contribute to adding knowledge for a networking novice while consolidating concepts for an experienced professional or academic. [1]

Volume XX Issue I Version I 32 Year 2020) Multiplexing is a method by which multiple analog or digital signals are combined into one signal over a shared medium. A protocol data unit (PDU) is a single unit of information transmitted among peer entities of a computer network. A PDU is composed of protocol specific control information and user data. Encapsulation is a method of designing modular communication protocols in which logically separate functions in the network are abstracted from their underlying structures by inclusion or information hiding within higher level objects.
(
Global Journal of Computer Science and Technology

Figure 1:

Figure 2:

[Mangold et al.] , Stefan Mangold , Sunghyun Choi , Peter May , Ole Klein , Guido Hiertz , Lothar Stibor . IEEE 802.11.

[Liu et al. ()] 'A cooperative MAC protocol for wireless local area networks'. Pei Liu , Zhifeng Tao , Shivendra Panwar . *IEEE International Conference on Communications*, 2005. ICC 2005. 2005. 2005. IEEE. 5 p. .

[Schollmeier ()] 'A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications'. Rüdiger Schollmeier . *Proceedings First International Conference on Peer-to-Peer Computing*, (First International Conference on Peer-to-Peer Computing) 2001. IEEE. p. .

[Popovic et al. ()] 'A DSL for modeling application-specific functionalities of business applications'. Aleksandar Popovic , Ivan Lukovic , Vladimir Dimitrieski , Verislavdjukic . *Computer Languages, Systems & Structures* 2015. 43 p. .

[Gien ()] 'A file transfer protocol (FTP)'. Michel Gien . *Computer Networks* 1976. 1978. 2 (4-5) p. .

[Sunny et al. ()] 'A generic controller for managing TCP transfers in IEEE 802.11 infrastructure WLANs'. Albert Sunny , Sumankumar Panchal , Nikhil Vidhani , Subhashini Krishnasamy , S V R Anand , Malati Hegde , Joy Kuri , Anurag Kumar . *Journal of Network and Computer Applications* 2017. 93 p. .

[Pei et al. ()] 'A neighbor discovery protocol for directional antenna networks'. Guangyu Pei , M A Albuquerque , Jae H Kim , Douglas P Nast , Paul R Norris . *MILCOM 2005-2005 IEEE Military Communications Conference*, 2005. IEEE. p. .

[Atkinson and Bhatti ()] 'Address resolution protocol (ARP) for the identifier-locator network protocol for IPv4 (ILNPv4)'. R Atkinson , S N Bhatti . *IRTF* 2012. 6747. (RFC)

[Kim et al. ()] 'An acceptance model for smart watches'. Ki Kim , Dong-Hee Joon , Shin . *Internet Research* 2015.

[Han et al. ()] 'An integrated home server for communication, broadcast reception, and home automation'. Intark Han , Hong-Shik Park , Kwang-Roh Youn-Kwaejeong , Park . *IEEE Transactions on Consumer Electronics* 2006. 52 (1) p. .

[Acampora and Karol ()] 'An overview of lightwave packet networks'. Anthony S Acampora , Mark J Karol . *IEEE Network* 1989. 3 (1) p. .

[Bektas et al. ()] 'Bluetooth communication employing antenna diversity'. Filiz Bektas , Bojan Vondra , Peter E Veith , Leopold Faltin , Alfred Pohl , A L Scholtz . *Proceedings of the Eighth IEEE Symposium on Computers and Communications. ISCC*, (the Eighth IEEE Symposium on Computers and Communications. ISCC) 2003. 2003. IEEE. p. .

[Oliviero and Woodward ()] *Cabling: the complete guide to copper and fiber-optic networking*, Andrew Oliviero , Bill Woodward . 2014. John Wiley & Sons.

[Velte and Velte ()] *Cisco A Beginner's Guide. McGraw-Hill Education Group*, Toby Velte , Anthony Velte . 2013.

[Pagiamtzis and Sheikholeslami ()] 'Content-addressable memory (CAM) circuits and architectures: A tutorial and survey'. Kostas Pagiamtzis , Ali Sheikholeslami . *IEEE journal of solid-state circuits* 2006. 41 (3) p. .

[Sagari et al. ()] 'Coordinated dynamic spectrum management of LTE-U and Wi-Fi networks'. Shweta Sagari , Samuel Baysting , Ivan Dolasaha , Wade Seskar , Dipankar Trappe , Raychaudhuri . *2015 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2015. IEEE. p. .

[Sen et al. ()] 'CSMA/CN: Carrier sense multiple access with collision notification'. Souvik Sen , Romit Roy Choudhury , Srihari Nelakuditi . *IEEE/ACM Transactions on Networking* 2011. 20 (2) p. .

[Tian et al. ()] 'Detecting bitrate modulation-based covert voice-over-IP communication'. Hui Tian , Jun Sun , Chin-Chen Chang , Yongfeng Huang , Yonghong Chen . *IEEE Communications Letters* 2018. 22 (6) p. .

[Bell] *Different types of transmission lines used in communications: applications and uses. 1. Coaxial cable*, Graham Bell .

[Avila-Navarro et al. ()] 'Dualband printed dipole antenna for Wi-Fi 802.11 n applications'. E Avila-Navarro , C Cayuelas , C Reig . *Electronics letters* 2010. 46 (21) p. .

[e Wireless LAN for Quality of Service Proc. European Wireless ()] 'e Wireless LAN for Quality of Service'. *Proc. European Wireless*, (European Wireless) 2002. 2 p. .

[Filibeli et al. ()] 'Embedded web server-based home appliance networks'. M Filibeli , Can , M Oznurozkasap , Rehacivanlar . *Journal of Network and Computer Applications* 2007. 30 (2) p. .

[Groba and Springer ()] 'Exploring data forwarding with Bluetooth for participatory crowd monitoring'. Christin Groba , Thomas Springer . *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2019. IEEE. p. .

[Carvalho et al. ()] 'Extended performance research on Wi-Fi IEEE 802.11 a, b, g laboratory open point-to-multipoint and point-to-point links'. De Carvalho , H Pacheco , Veiga , Cf Ribeiro , A D Pacheco , Reis . *Transactions on Engineering Technologies*, (Singapore) 2016. Springer. p. .

[Vlosky et al. ()] ‘Extranets: impacts on business practices and relationships’. Richard P Vlosky , Renée Fontenot , Lydia Blalock . *Journal of business & Industrial marketing* 2000.

[Hitz et al. ()] ‘File System Design for an NFS File Server Appliance’. Dave Hitz , James Lau , Michael A Malcolm . *USENIX winter*, 1994. 94.

[Tse and Viswanath ()] *Fundamentals of wireless communication*, David Tse , Pramod Viswanath . 2005. Cambridge university press.

[Difrancisco et al. ()] ‘Global Broadcast Service (GBS) end-to-end services: protocols and encapsulation’. Michael Difrancisco , J Stephenson , C Ellis . *MILCOM 2000 Proceedings. 21st Century Military Communications. Architectures and Technologies for Information Superiority (Cat. No. 00CH37155)*, 2000. IEEE. 2 p. .

[Pearce et al. ()] ‘Global Measurement of {DNS} Manipulation’. Paul Pearce , Ben Jones , Frank Li , Roya Ensafi , Nick Feamster , Nick Weaver , Vern Paxson . *26th {USENIX} Security Symposium ({USENIX} Security 17)*, 2017. p. .

[Azzam ()] *High-speed cable modems: including IEEE 802.14 standards. McGraw-Hill Professional*, Albert A Azzam . 1997.

[Oda and Yamaguchi ()] ‘HTTP/2 performance evaluation with latency and packet losses’. Naoki Oda , Saneyasu Yamaguchi . *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2018. IEEE. p. .

[Liu et al. ()] ‘Hybrid half-duplex/full-duplex cooperative non-orthogonal multiple access with transmit power adaptation’. Gang Liu , Xianhao Chen , Zhiguo Ding , Zheng Ma , F. Richard Yu . *IEEE Transactions on Wireless Communications* 2017. 17 (1) p. .

[Alfonsi ()] ‘I want my IPTV: Internet Protocol television predicted a winner’. Benjamin Alfonsi . *IEEE Distributed Systems Online* 2005. 6 (2) .

[Prasad ()] ‘IEEE 802.11 system design’. Neeli R Prasad . *2000 IEEE International Conference on Personal Wireless Communications. Conference Proceedings (Cat. No. 00TH8488)*, 2000. IEEE. p. .

[Borrelli ()] ‘IEEE 802.3 cyclic redundancy check’. Chris Borrelli . *Virtex Series and Virtex-II Family, XAPP209 (v1. 0)*, 2001.

[Popescu-Zeletin ()] ‘Implementing the ISO-OSI reference model’. Radu Popescu-Zeletin . *ACM SIGCOMM Computer Communication Review* 1983. 13 (4) p. .

[Bruns et al. ()] ‘Intelligent M2M: Complex event processing for machine-to-machine communication’. Ralf Bruns , Jürgen Dunkel , Henrik Masbruch , Sebastian Stipkovic . *Expert Systems with Applications* 2015. 42 (3) p. .

[Conta et al. (1998)] *Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification. RFC 2463*, Alex Conta , Stephen Deering , Mukesh Gupta . december. 1998.

[Thapliyal ()] ‘Internet of Things-based consumer electronics: reviewing existing consumer electronic devices, systems, and platforms and exploring new research paradigms’. Himanshu Thapliyal . *IEEE Consumer Electronics Magazine* 2017. 7 (1) p. .

[Powers ()] *Introduction to fiber optic systems*, John P Powers . 1993. McGraw-Hill Professional.

[Meng et al. ()] ‘IPv4 address allocation and the BGP routing table evolution’. Xiaoqiao Meng , Zhiguo Xu , Beichuan Zhang , Geoff Huston , Songwu Lu , Lixia Zhang . *ACM SIGCOMM Computer Communication Review* 2005. 35 (1) p. .

[Hinden et al. ()] ‘IPv6 global unicast address format’. Robert Hinden , Stephen Deering , Erik Nordmark . *Network Working Group Request for Comments* 2003. 3587.

[Knight and Lewis ()] ‘Layer 2 and 3 virtual private networks: taxonomy, technology, and standardization efforts’. Paul Knight , Chris Lewis . *IEEE Communications Magazine* 2004. 42 (6) p. .

[Yang et al. ()] ‘Lesson Learnt from Smart Home Automation Systems’. Yang , Theresa Kuo-Pao , M Beaubouef , Chiu . *Journal of Emerging Trends in Computing and Information Sciences* 2015. 6 (3) .

[Trogdon ()] ‘Lessons from google fiber: Why coordinated cost reductions to infrastructure access are necessary to achieve universal broadband deployment’. Holly Trogdon . *Fed. Comm. LJ* 2013. 66 p. 103.

[Carles Dohler (ed.)] Anton-Haro . *Machine-to-machine (M2M) communications: architecture, performance and applications*, Mischa Carles, Dohler (ed.)

[Mbit/sec) SONET/ATM signals over unshielded and shielded twisted pair copper wire [Conference Record] LOBECOM’ 92-Communications for Global Users: IEEE ()]b68 ‘Mbit/sec) SONET/ATM signals over unshielded and shielded twisted pair copper wire’. *[Conference Record] GLOBECOM’ 92-Communications for Global Users: IEEE*, 1992. IEEE. p. .

[Santitoro ()] ‘Metro Ethernet Services-A Technical Overview’. Ralph Santitoro . *Metro Ethernet Forum*, 2006. 2003.

[Tracy ()] 'Mobile Application Development Experiences on Apple¿ s iOS and Android OS'. Kim W Tracy . *Ieee Potentials* 2012. 31 (4) p. .

[Na and Rajaravivarma ()] 'Multimedia file sharing in multimedia home or office business networks'. Jun Na , V Rajaravivarma . *Proceedings of the 35th Southeastern Symposium on System Theory*, (the 35th Southeastern Symposium on System Theory) 2003. 2003. IEEE. p. .

[Dev et al. ()] 'Network management system using multifunction icons for information display'. Roger H Dev , Eric W Gray , Eric S Rustici , Walter P Scott . *U.S. Patent* 261,044, issued November 9. 1993. 5.

[Chae et al. ()] 'Optical CSMA/CD media access scheme for Ethernet over passive optical network'. Chang-Joon Chae , Elaine Wong , Rodney S Tucker . *IEEE Photonics Technology Letters* 2002. 14 (5) p. .

[Zimmermann ()] 'OSI reference model-the ISO model of architecture for open systems interconnection'. Hubert Zimmermann . *IEEE Transactions on communications* 1980. 28 (4) p. .

[Tobagi and Hunt ()] 'Performance analysis of carrier sense multiple access with collision detection'. Fouad A Tobagi , V Bruce Hunt . *Computer Networks* 1976. 1980. 4 (5) p. .

[Cho et al. ()] 'Performance analysis of the IEEE 802.16 wireless metropolitan area network'. Dong-Hoon Cho , Jung-Hoon Song , Min-Su Kim , Ki-Jun Han . *First International Conference on Distributed Frameworks for Multimedia Applications*, 2005. IEEE. p. .

[Petras and Hettich ()] 'Performance Evaluation of a Logical Link Control Protocol for an ATM air interface'. Dietmar Petras , Andreas Hettich . *International Journal of Wireless Information Networks* 1997. 4 (4) p. .

[Gelenbe et al. ()] 'Performance evaluation of the HDLC protocol'. Erol Gelenbe , Jacques Labetoulle , Guy Pujolle . *Computer Networks* 1976. 1978. 2 (4-5) p. .

[Messier et al. ()] 'Performance monitoring of a wireless campus area network'. Andrew Messier , Jared Robinson , Kaveh Pahlavan . *Proceedings of 22nd Annual Conference on Local Computer Networks*, (22nd Annual Conference on Local Computer Networks) 1997. IEEE. p. .

[Bertozzi et al. ()] 'Power aware network interface management for streaming multimedia'. Davide Bertozzi , Luca Benini , Bruno Ricco . *2002 IEEE Wireless Communications and Networking Conference Record. WCNC 2002 (Cat. No. 02TH8609)*, 2002. IEEE. 2 p. .

[Pan et al. ()] 'Pure logic CMOS based embedded non-volatile random access memory for low power RFID application'. Liyang Pan , Xian Luo , Yaru Yan , Jirong Ma , Dong Wu , Jun Xu . *2008 IEEE Custom Integrated Circuits Conference*, 2008. IEEE. p. .

[Bar-Noy et al. ()] 'Pushing dependent data in clientsproviders-servers systems'. Amotz Bar-Noy , Joseph Seffinaor , Baruch Schieber . *Wireless Networks* 2003. 9 (5) p. .

[Cicconetti et al. ()] 'Quality of service support in IEEE 802.16 networks'. Claudio Cicconetti , Luciano Lenzini , Enzo Mingozzi , Carl Eklund . *IEEE network* 2006. 20 (2) p. .

[Simpson ()] *RFC1661: the point-to-point protocol (PPP). RFC Editor*, William Simpson . 1994.

[Tsirtsis ()] *RFC2766: Network Address Translation-Protocol Translation (NAT-PT)*, George Tsirtsis , Pydas-risuresh . 2000.

[Liu ()] 'Services computing: from cloud services, mobile services to internet of services'. Ling Liu . *IEEE Transactions on Services Computing* 2016. 5 p. .

[Duchene et al. ()] 'State of the art of network protocol reverse engineering tools'. Julien Duchene , Colas Le Guernic , Eric Alata , Vincent Nicomette , Mohamed Kaâniche . *Journal of Computer Virology and Hacking Techniques* 2018. 14 (1) p. .

[Stephens et al.] W E Stephens , T C Banwell , G R Lalk , T J Robe , K C Young . *Transmission of STS-3c*,

[Hoang et al. ()] 'Switched real-time ethernet with earliest deadline first scheduling protocols and traffic handling'. Hoai Hoang , Magnus Jonsson , Ulrikhagstrom , Anders Kallerdahl . *Proceedings 16th International Parallel and Distributed Processing Symposium*, (16th International Parallel and Distributed Processing Symposium) 2001. IEEE. p. 6.

[Forouzan and Behrouz ()] *TCP/IP protocol suite*, Forouzan , A Behrouz . 2002. McGraw-Hill, Inc.

[Werner ()] 'The HDSL environment (high bit rate digital subscriber line)'. J-J Werner . *IEEE Journal on selected areas in communications* 1991. 9 (6) p. .

[Hiertz et al. ()] 'The IEEE 802.11 universe'. Guido R Hiertz , Dee Denteneer , Lothar Stibor , Yunpeng Zang , Xavier Pérez Costa , Bernhard Walke . *IEEE Communications Magazine* 2010. 48 (1) p. .

[Goralski ()] *The illustrated network: how TCP/IP works in a modern network*, Walter Goralski . 2017. Morgan Kaufmann.

[Heires ()] 'The international organization for standardization (ISO)'. Marcel Heires . *New Political Economy* 2008. 13 (3) p. .

[Egevang and Francis ()] *The IP network address translator (NAT). RFC 1631, may*, Kjeld Egevang , Paul Francis . 1994.

[Seifert ()] *The switch book: the complete guide to LAN switching technology*, Rich Seifert . 2000. John Wiley & Sons, Inc.

[Mirri et al. ()] 'Towards accessible graphs in HTML-based scientific articles'. Silvia Mirri , Silvio Peroni , Paola Salomoni , Fabio Vitali , Vincenzorubano . *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2017. IEEE. p. .

[Schatt and Schatt ()] *Understanding local area networks*, Stanley Schatt , Stanley Schatt . 1992. Sams.

[Sarker and Wells ()] 'Understanding mobile handheld device use and adoption'. Suprateek Sarker , John D Wells . *Communications of the ACM* 2003. 46 (12) p. .

[Pruet and Siang Ang ()] 'Understanding tablet computer usage among primary school students in underdeveloped areas: Students' technology experience, learning styles and attitudes'. Putjorn Pruet , Chee Siang Ang , Deravifarzin . *Computers in Human Behavior* 2016. 55 p. .

[Alizadeh et al. ()] 'Urban governance and big corporations in the digital economy: An investigation of sociospatial implications of Google Fiber in Kansas City'. Alizadeh , Tony H Tooran , Edward Grubesic , Helderop . *Telematics and informatics* 2017. 34 (7) p. .

[User Datagram Protocol, and Datagram Sockets UDP ()] 'User Datagram Protocol, and Datagram Sockets'. *UDP* 1980. (User Datagram Protocol)

[Chan et al. ()] 'Using Google Hangouts on Air for medical education: a disruptive way to leverage and facilitate remote communication and collaboration'. Teresa Chan , Nikita Joshi , Michelle Lin , Neil Mehta . *Journal of graduate medical education* 2015. 7 (2) p. .

[Smith and Eaton ()] *Wi-Fi Home Networking*, Raymond Smith , Dennis Eaton . 2003. McGraw-Hill, Inc.