1. The Physical Layer and Data Link

The Physical Layer is concerned with the transferring of raw bits over a channel. This channel can be in the form of a cable or modern wireless communication. Information is carried over these mediums by varying some physical properties. In the case of cable communication the voltage and current values are represented as a function of time. The data is linked in various guided and unguided communication media.

1.1 Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Carrier Sense With Multiple Access or **CSMA** is a computer access method in networking whereby data transmission occurs when the transmission channel is sensed to be *idle* or not currently transmitting data. Devices in the network commonly known as nodes use this technique to avoid collision and transmit their packet data in its entirety. This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the data link layer.

The intent behind CSMA is that the receiving station of any data should be available for the transfer to be completed. In wired networks, if a collision has occurred then the energy of the received signal almost doubles and the station can sense the possibility of collision. In case of wireless networks, most of the energy is used for transmission and the energy of received signal increases by only 5-10% if a collision occurs. CSMA/CA can be summed up with three components.

1. Carrier Sense(CS): Participants may only send data over the network if the transmission medium is free.
2. Multiple Access(MA): Functional communication requires stations that share a transmission medium to follow a binding **protocol**.
3. Collision Avoidance(CA): A complex schedule tries to ensure that two or more participants do not start a transmission at the same time to avoid collisions. If overlapping does occur, this will be detected and the transmission will be tried again.

The Hidden Station problem

Because stations in a wireless network have limited range, it is possible for participants not to recognize each other and unknowingly send packets to a node located between them. Transmissions can overlap at the receiving node, meaning data gets lost. Both transmitters do not

detect the collision and don't start a new delivery attempt. CSMA/CA alone cannot solve this problem, which is why an optional extension was created: "Request To send and Clear To send or RTS and CTS".

Request to send and clear to send (RTS/CTS)

If a participant in a data-transmission determines that the medium is free, the device first sends a "Request to send" or an **RTS** to the participant that is to receive the data. The output computer then makes it clear that it wants to start a transmission and will occupy the transmission medium for a certain time. After the request is received, the receiving node, in turn, sends a "Clear to send" or **CTS** frame to the sender. As with the **RTS** frame, all other participants in the range are informed that the transmission is currently occupied and the transmitter is enabled for transmission. Only then does the original device start transmitting the data. The receiving station also needs to send an **acknowledgement** (ACK) when the data packet has arrived correctly, otherwise the sender of the data assumes that a complication has occurred and resends the data packet.

By extending the CSMA/CA protocol with RTS/CTS, it's possible to reduce collisions on the initial RTS frame. It is still likely that two participants will send a request to send to the same station at the same time. In cases like this, however, the receiver does not send a CTS frame because the RTS frames have not arrived correctly. So, RTS/CTS can solve the hidden station problems: even if the two transmitters don't recognize each other due to the limited range, only the RTS frames are at risk and not the actual data. CSMA/CA then takes effect and the transmission can take place in an orderly fashion. But with this advantage arises the exposed station problem. The situation is initially the same as with the hidden station problem: The middle node is prevented from transmitting, even if a completely different, fourth station would have been the destination of the transmission because it has to wait for the CTS to finish. This transmission would not cause a collision, but it still has to be prevented, which leads to a slow network.

1.2 Address Resolution Protocol

Address Resolution Protocol or ARP is a procedure for mapping a dynamic Internet Protocol address to a permanent physical machine address in a local area network. The physical machine address is also known as a Media Access Control or MAC address. This process of finding an address of a computer in a network is called Address resolution. A computer in an Ethernet LAN is assigned(usually dynamically) a unique IPv4 address which is used for identification and communication. When incoming data destined for a node on a particular LAN arrives at a gateway(Essentially a node that connects two or more networks), it asks the ARP program to find a MAC address that matches the IP address. The address resolution procedure is completed

when the client receives a response from the server containing the required address. The ARP basically stores a cache of physical or MAC addresses but the size is limited and it is periodically cleaned of all entries to free up space. If the address is not “resolved” in the cache or doesn’t exist yet 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.

2. Network Layer

In the OSI model, the network layer is where the inter-network communications occur. The network layer uses the IP protocol for routing(sending packers of data), network testing and data encryption. Anything that has to do with network-to-networking connections is dealt with in this layer(number 3 in the OSI model). This includes setting up the routes for data packets to take, checking to see if a server in another network is up and running, and addressing and receiving IP packets from other networks.

2.1 Internet Control Message Protocol(ICMP)

The Internet Control Message Protocol (ICMP) is a protocol used by network devices to diagnose errors in a computer network. ICMP is mainly used in routers to determine whether or not the data has reached its intended destination. It then uses this information to report errors to the sending node and “informs” it of the irregularities. A simple example can be seen whenever a data packet is too large for the router. In such cases the router will drop the packet and send an ICMP message to the source. A secondary use is network diagnostics using traceroute and ping utility.

The Traceroute utility

This ICMP tool does exactly what the name suggests which is to trace the path between two devices in a network. This path is known as the routing path and it is the actual physical path of connected routers that a request must pass through before it reaches its destination. A traceroute reports the time required for each packet switch or hop which can be useful for determining sources of network delay. The ping utility is a simplified version of a traceroute. A ping will test the speed of the connection between two devices and report exactly how long it takes a packet of data to reach its destination and come back to the sender’s device. Although ping does not provide data about routing or hops, it is still a very useful metric for measuring the network latency(time delay) between two devices.

Some Attacks associated with ICMP

1. Flood Attack: This type of attack attempts to overwhelm a targeted device by 'flooding' it with pings. The target has to process and respond to each packet, consuming its computing resources until legitimate users cannot receive service.
2. Ping of Death: Although uncommon these days, A ping of death attack is when the attacker sends a ping larger than the maximum allowable size for a packet to a targeted machine, causing the machine to freeze or crash. The packet gets fragmented on the way to its target, but when the target reassembles the packet into its original maximum-exceeding size, the size of the packet causes a buffer overflow.
3. Smurf Attack: In this instance, the attacker sends an ICMP packet with a spoofed source IP address. Networking equipment replies to the packet, sending the replies to the spoofed IP and flooding the victim with unwanted ICMP packets.

2.2 Open Shortest Path First(OSPF)

The Open Shortest Path First is a routing protocol for IP networks and is an Interior Gateway Protocol (IGP) for the Internet, used to distribute IP routing information throughout a single Autonomous System (AS). The OSPF protocol is a link-state routing protocol, which means that the routers exchange topology information with adjacent nodes. The topology information is found throughout the system, so that every node within the AS has a complete picture of the network topology. This can be used to calculate optimal paths for the transmission of packets. Each OSPF router uses a dijkstra algorithm(algorithm used in graph data structures to find the shortest distance between two nodes) to calculate its own routing table.

The main advantage of OSPF is that the complete knowledge of topology allows routers to calculate routes that satisfy particular criteria. This can be useful for traffic engineering purposes, where routes can be constrained to meet particular quality of service requirements. The main disadvantage of a link state routing protocol is that it does not scale well as more routers are added to the routing domain. Increasing the number of routers increases the size and frequency of the topology updates, and also the length of time it takes to calculate end-to-end routes. This lack of scalability means that this protocol has its optimal usage for a single Automated System.

2.3 Internet Protocol Security(IPSec)

IP security is a protocol that governs data authentication, integrity and confidentiality across two communication points in a computer network. It also defines the encrypted,

decrypted and authenticated packets. The protocols needed for secure key exchange and key management are also defined in it as well. Generally IPSec is used to:

1. Encrypt data
2. Provide security for routers
3. Data authentication (checking the origin or sender of the data)
4. Using tunnelling to protect data transfer between two nodes

Components of IPSec

1. Encapsulating Security Payload (ESP): Provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.
2. Authentication Header (AH): protects against unauthorized transmission of packets.
3. Internet Key Exchange (IKE): Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produce a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets which are not authorized are discarded and not given to the receiver.

Working of IPSec

IPSec has a series of steps that govern secure packet transfer.

1. Host checks whether to use IPSec or not. These packet traffic triggers the security policy for themselves. This is done when the system sending the packet applies an appropriate encryption. The incoming packets are also checked by the host whether they are encrypted properly or not.
2. Internet Key Exchange phase one is started where hosts authenticate themselves over a secure channel
3. The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit
4. IKE phase two begins in which the two hosts exchange the type of cryptographic algorithms to use on the session and agree on secret keying material to be used with those algorithms.
5. The data is exchanged over an encrypted tunnel and finally,
6. The session times out when the communication is complete.

3. Transfer Layer

3.1 Transmission Control Protocol/Internet Protocol (TCP/IP)

The Internet Protocol (IP) is the address system of the Internet and has the core function of delivering packets of information from a source device to a target device. IP is the primary way in which network connections are made, and it establishes the basis of the Internet. All messages that are transferred in this protocol are first broken into dozens of pieces called packets. Packets are the smallest indivisible units of messages in an TCP/IP transfer. Ip is a connectionless protocol meaning that each packet is individually addressed and routed. That's where Transmission Control Protocol (TCP) comes in and it is used in conjunction with IP in order to maintain a connection between the sender and the target and to ensure packet order.

For example, when an email is sent over TCP, a connection is established and a 3-way handshake is made. First, the source sends an SYN "initial request" packet to the target server in order to start the dialogue. Then the target server then sends a SYN-ACK packet to agree to the process. Lastly, the source sends an ACK packet to the target to confirm the process, after which the message contents can be sent. The email message is ultimately broken down into packets before each packet is sent out into the Internet, where it traverses a series of gateways before arriving at the target device where the group of packets are reassembled by TCP into the original contents of the email.

3.2 User Datagram Protocol (UDP)

The User Datagram Protocol is a protocol used in the transfer of time sensitive transmissions like video stream or DNS lookups. It is faster because it doesn't use traditional connection establishment to transfer data but this created exploits like DDoS attacks.

UDP is a standardized method for transferring data between two computers in a network. Compared to other protocols, UDP accomplishes this process in a simple fashion: it sends packets (units of data transmission) directly to a target computer, without establishing a connection first, indicating the order of said packets, or checking whether they arrived as intended. (UDP packets are referred to as 'datagrams'.) UDP is faster but less reliable than TCP. In a TCP communication, the two computers begin by establishing a connection via an automated process called a 'handshake.'(See above for details about three way handshakes). Only once this handshake has been completed will one computer actually transfer data packets to the other. UDP is commonly used in time-sensitive communications where occasionally dropping packets is better than waiting. Voice and video traffic are sent using this protocol because they are both time-sensitive and designed to handle some level of loss. For example VOIP (voice over IP), which is used by many internet-based telephone services, operates over

UDP. This is because a staticy phone conversation is preferable to one that is crystal clear but heavily delayed.

DDos Attacks: UDP can be exploited for malicious purposes. Since UDP does not require a handshake, attackers can 'flood' a targeted server with UDP traffic without first getting that server's permission to begin communication. A typical flood attack sends a large number of UDP datagrams to random ports on its target. This forces the computer to respond with an equally large number of ICMP packets, which indicated those ports were unreachable. The resource required to respond to fraudulent datagrams can exhaust the target which can lead to a denial-or-service to legitimate packets.

4. Session, Presentation and Application Layers

4.1 HyperText Transfer Protocol/Secure(HTTP/HTTPS)

HTTP and its modern Secure counterpart is the primary protocol used to send data between a browser and a website. HTTPS is considered "secure" because it provides encryption when data is transferred. Any website, especially those that require login credentials, should use HTTPS. In modern web browsers such as Chrome, websites that do not use HTTPS are marked differently than those that are. Browsers that take HTTPS seriously have a green padlock in the URL bar to signify the webpage is secure.

HTTPS uses an encryption protocol to encrypt communications. The protocol is called Transport Layer security (TLS), although formerly it was known as Secure Sockets Layer(SSL). This protocol secures communications by using what's known as an asymmetric public key infrastructure. This type of security system uses two different keys to encrypt communications between two parties:

1. The private key: controlled by the owner of a website and it's kept, as the reader may have speculated, private. This key lives on a web server and is used to decrypt information encrypted by the public key.
2. The public key: available to everyone who wants to interact with the server in a way that's secure. Information that's encrypted by the public key can only be decrypted by the private key.

4.2 Domain Name System (DNS)

The domain name system commonly referred to as DNS is basically a phonebook containing all the addresses in a computer. Computers identify themselves with IP addresses which is a 32-bit number but since humans don't communicate with numbers, it might be difficult to understand what 8.8.8.8 (public ip for google servers) mean. Instead the domain name system uses an abstraction that matches the IP addresses with their correct names. This process is called DNS resolution and it involves converting a hostname (such as www.example.com) into a computer-friendly IP address. There are four DNS servers involved in loading a webpage.

1. DNS recursor: The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers. Typically the recursor is then responsible for making additional requests in order to satisfy the client's DNS query. Luckily, recursive DNS resolvers do not always need to make multiple requests because of caching which is a data persistence method that shortens this process.
2. Root name server: The root name server acts as an index that points to specific locations.
3. TLD server: The top level domain server (TLD server) is the next step in the search for a specific IP address, and it hosts the last portion of a hostname (In example.com, the TLD server is "com").
4. Authoritative name server: The authoritative nameserver is the last stop in the nameserver query. If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor that made the initial request. This is the server at the bottom of the DNS lookup chain that will respond with the queried resource record, ultimately allowing the web browser making the request to reach the IP address needed to access a website or other web resources.

4.3 Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of configuring devices on IP networks. A DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.

The IP address information assigned by DHCP is only valid for a limited period of time, and is known as a DHCP lease. The period of validity is called the DHCP lease time. When the lease expires, the client can no longer use the IP address and has to stop all communication with the IP network unless he requests to extend the lease via the DHCP lease renewal cycle. To avoid impacts of the DHCP server not being available at the end of the lease time, clients generally start renewing their lease halfway through the lease period. This renewal process ensures robust IP address allocation to devices. Any device asking for a new IP version 4 address at arrival on

the network and not receiving an answer will use automatic private internet protocol addressing (APIPA) to select an address.

There are four uses of DHCP

- Initial Client Connection: The client requests from the DHCP server an IP address and other parameter values for accessing network services
- IP lease Extension: The client contacts the DHCP server to extend usage of its current IP address
- Client connection after reboot: The client contacts the DHCP server for confirmation that it can use the same IP address being used before reboot
- Client Disconnection: The client requests the DHCP server to release its IP address.

4.4. File Transfer Protocol (FTP)