his project involves signal processing, networking, web technologies, and machine learning. This homework focuses on Internet technologies.

Vocab::

* **Router Hop**: The act of a packet moving from one router to another.
* **Discarded**: When a packet is not delivered to it’s destination. \*\*\*What occurs to a packet that is discarded, is it just “deleted” or is it lost in a “limbo”.
* **Physical Network Infrastructure:** The hardware and media that form the foundation for a computer network.
* **Hardware Address:** a 12-digit number, starting with a 0, and consisting of numbers 0-9 and letters A-F. It is unique (like a serial number) to each network interface. Depending on the device or operating system, it can also be referred to as a MAC address, Physical Address or Ethernet ID.

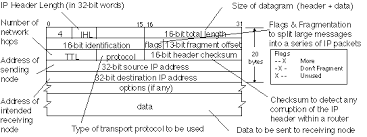
*Dave’s comment: a hardware address does not have to be 12 digits of 0-9 and A-F. The name of the system that uses 0-9 and A-F is hexadecimal. For Ethernet it is 12 hexadecimal digits. EUI-64 is for example 64 bits, which can be represented as 16 hexadecimal digits.*

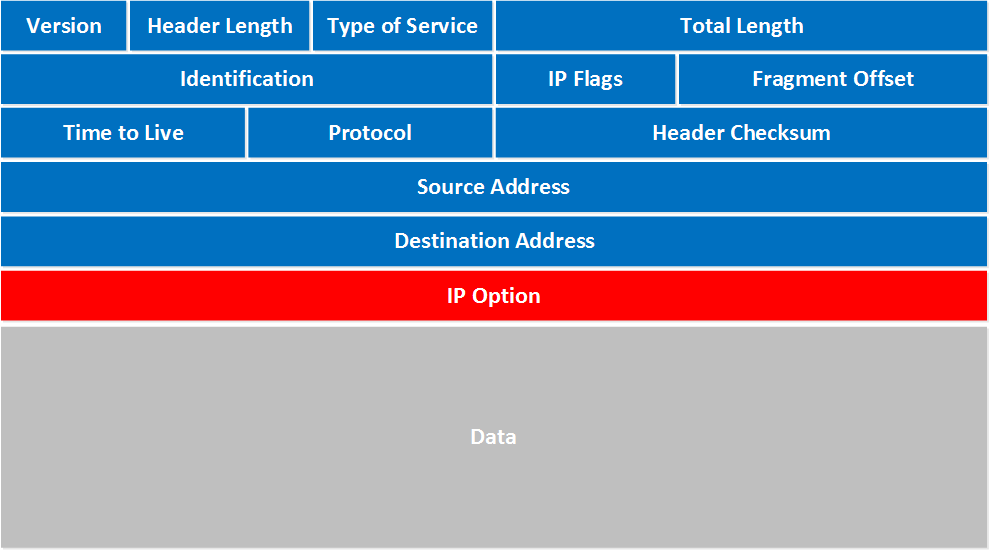
* **Data Framing:** The process of breaking down data streams into “Frames”
* **Data Stream:** The continuous transfer of data at a high rate of speed.
* **Frame:** a digital data transmission unit in computer networking and telecommunication.
* **Physical Transmission Medium:** the transmission path over which a signal propagates such as twisted-pair copper wire, coaxial cable, multimode fiber optic cable, terrestrial radio spectrum and satellite radio spectrum.
* **Data encapsulation:** the process of wrapping data with the necessary protocol information before it is transmitted over a network.
* **DNS:** A system that converts website names (website.com) into an IP address that can be read by machines.

*Dave’s comment: More accurately stated, DNS maps from domain names to IP addresses. The web is just one service that uses domain names. For example:* ssh foo.com *will open an secure shell connection to the computer with domain name foo.com.  
.*

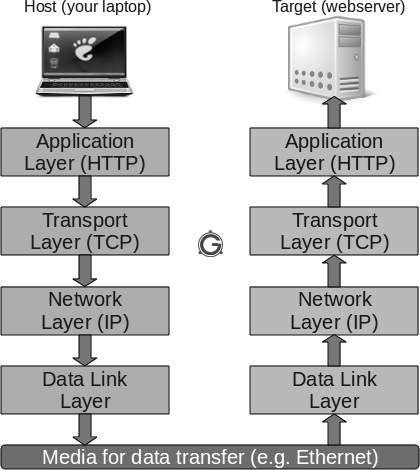
On separate paper or in a file, write the answer to each of these questions.

* 1. What is a packet header? Describe each field and its function. A packet header is where information pertaining to a packet can be found. (*Dave’s comment: the packet header contains information necessary to route a packet from a source to a destination or destinations*.) There 13 different fields within a packet header.
* Version field displays the current version IP that is used by the packet.
* The IHL (IP Header Length) is the amount of bytes a IP packet uses ranging from around 20 to 60 bytes.
* The Total Length field details the entire size of the packet including the header and data.
* The Identification field is a unique number that is given to an individual packet but is not always unique if certain conditions are set, such as if the packet were fragmented.
* The flag+fragementation field details whether a packet is fragmented. The first digit of a 3-digit flag must always be 0. The 2nd digit says whether fragmentation is allowed (0 means fragmentation is allowed, and 1 means fragmentation is forbidden. The 3rd digit says whether the packet is the last fragment. (0 means it is the last fragment, 1 means it is not) \*\*\*\*QUESTION\*\*\*\*\* does this mean that there isn’t a way to tell what number packet an IP packet is if it’s not the last?
* (Dave’s comment: every fragment has a fragment offset in units of 8 bytes, e.g., 0 = 0 byte, 1 = 8 bytes, 2 = 16 bytes. One can restore the original packet from the fragments by ordering the fragments in increasing order of the fragment offset and concatenating.
* The Time to Live (TTL) field is a number that represents the maximum amount of router hops an IP packet can do before it is discarded.
* The Protocol field defines what protocol is used by the IP packet (either TCP or UDP).
* The Header Checksum can display whether the packet was corrupted by combining all the 16-bit words in the header.
* The Source Address identifies the origin of the packet.
* The Destination Address identifies the destination of the packet.
* The Options field dictates how the packet.
* The Data field is the code that is sent to the destination.





* 1. What do TCP and IP stand for? (Looking for the words composing the achronym. Subsequent questions will ask for more detail)
* TCP: Transmission Control Protocol
* IP: Internet Protocol
  1. Describe the function of each of the layers in the TCP/IP networking stack: Link Layer, Internet Layer, Transport Layer, Application Layer.
* Link Layer: Physically exchanges the data between the physical network infrastructure and the higher layers of the TCP/IP networking stack. It also dictates the MAC framing, error detection and access to the physical transmission medium.
* Internet Layer: Responsible for routing the packets using IP addresses and is responsible for fragmentation and reassembly.
* Transport Layer: Provides end-to-end communication services for applications. There are 2 types, TCP and UDP.
* Application Layer: This is the top layer and is allows software applications to communicate with each other. Examples of this layer include HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System).



* 1. The OSI model breaks this into 7 layers which are useful conceptually, but they do not directly associate with the design of the Internet. Contrast and compare the TCP/IP model with the OSI 7-layer model.

The OSI model has the following layers:

Physical. This consists of a data connection between a device generating data and the network.

Datalink. The datalink layer is the point-to-point connection that transmits the data to the network layer.

Network. In the network layer, the data gets its address and routing instructions in preparation for its journey across the network.

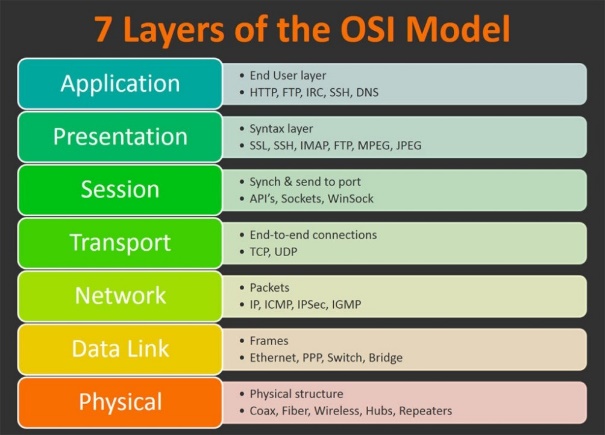
Transport. In the transport layer, the data hops between different points on the network on its way to its destination.

*Dave’s comment: The transport layer provides traffic control, reordering, and reliability. The reordering and reliability. All of these features are optional. For example, UDP does not provide traffic control, reordering, or reliability. If packets arrive out-of-order with UDP, they are received by the application layer in this wrong order. TCP (Transmission Control Protocol) packets are delivered in-order and reliability. Any missing packets are retransmitted. If packets cannot get through, TCP will eventually timeout and eventually drop the connection, but it will try to retransmit multiple times before finally giving up.)*

Session. The session layer has a connection that manages the sessions happening between applications.

Presentation. The presentation layer is where data gets encrypted and decrypted and converted into a form that is accessible by the application layer,

Application. In the application layer, an application, such as an internet browser, gets the data and a user can then interact with it.



In the OSI many of the functions have their own distinct layer while in the TCP/IP model has them in the same layer so it can get confusing if you ask about a layer within the TCP/IP model because those layers aren’t specific enough. You can identify things much easier with the OSI model rather than the TCP/IP model.

1.5. What are some differences between an Ethernet frame header and an IP header?

Ethernet frame headers contain source and MAC addresses while IP headers contain the source and IP address.

1.6. Why do we use both Ethernet addresses and IP addresses?

Because a packet needs to know both the MAC address and IP address in order to get to its destination.

*Dave’s comment: More detail. The IP address is used by IP routers to forward packets toward the right destination. The MAC address only has meaning within the local area networks. Different types of local area networks may have different length addresses, but IP is either 32-bit (IPv4) or 128-bit (IPv6).*

1.7. What is a Internet router? What are some key differences between a router and a switch?

An internet router transfers packets between computer networks. It’s like the highway and the cars are packets. A Network Switch sends packets to more than one device. Sometimes a router will send packets to a switch where its job is to assign it a MAC address or get one for it and set up the ethernet frame. This is done so that all the switch must do is send the packet to the correct port.

*Dave’s Comments: Both switches and routers forward traffic toward the correct destination. Switches operate using MAC addresses. Switches only forward traffic within a Local Area Network (LAN). Routers sit between LANs and forward traffic toward the correct LAN regardless of where that LAN sits in the world.*

1.8. In the TCP/IP model, what layer is TCP?

The Transportation Layer

1.9. In the TCP/IP model, what layer is HTTP?

The Application Layer

1.10. Explain how data encapsulation works in the TCP/IP model.

This is where the header is added so that protocols are applied to the packets as well as other things contained in the header that are crucial to the secure transfer of a packet.

*Dave’s comment: when data is being sent, each layer encapsulates the layers above it. This usually means adding a header (transport, network, and datalink layer headers). When data is received, each layer removes its associated header and passes the data to the layer above.*

1.11. Explain the difference between IPv4 and IPv6. Why was IPv6 introduced?

IPv4 uses 32-bit addresses while IPv4 uses 128-bit addresses and IPv6 has mandatory security and uses a simplified header to allow for faster computing. IPv6 was introduced to fix the limitations of IPv4.

1.12. What is NAT (Network Address Translation) and why is it used?

NATs are devices that connect to a device that applies the same public IP address to a collection of different private networks. This can even be extended to Carrier Grade NATs (CGN) that apply the same IP address to other smaller NATs making an entire neighborhood have the same IP address.

1.13. What is IPv4 address exhaustion?

The deletion of available IPv4 addresses.

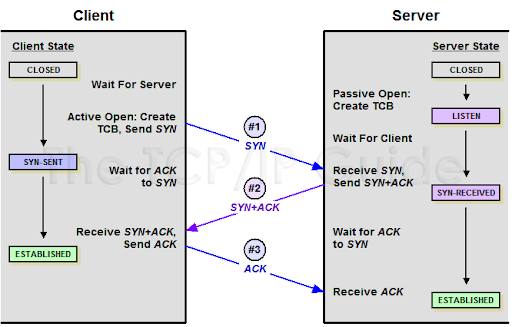
*Dave’s comment: NO!! It is the diminishing supply of unused IPv4 addresses. Competition for IPv4 addresses is using them all up!*

1.14. Describe what happens during the process of a TCP three-way handshake.

SYN: The client sends a segment with a sequence of numbers to the server which is used to keep track of the bytes in the data stream

SYN-ACK: The server then sends back the SYN segment as well as a ACK flag set within a single number segment upon receiving the SYN segment.

ACK: Upon getting the segment the client send a ACK segment containing the ACK flag set and an acknowledgement number.



1.15. What are the differences between TCP and UDP? Give examples of applications that use each protocol.

TCP needs a established connection before it can send data while UDP just sends data before getting an established connection. This makes TCP a much more secure way to send packets as to why it is used in HTTP based applications, like web browsing, but makes it much slower than UDP. Since UDP doesn’t need to established connection it is very efficient making it perfect for gaming or DNS.

*Dave’s comments: There are multiple other differences: reliability and reordering. Reliablity 🡪 retransmitting missing packet. Reordering occurs to ensure packets arrive in order. TCP also provides the illusion of a continuous stream of bytes. The application does not even know where the packet boundaries are.*

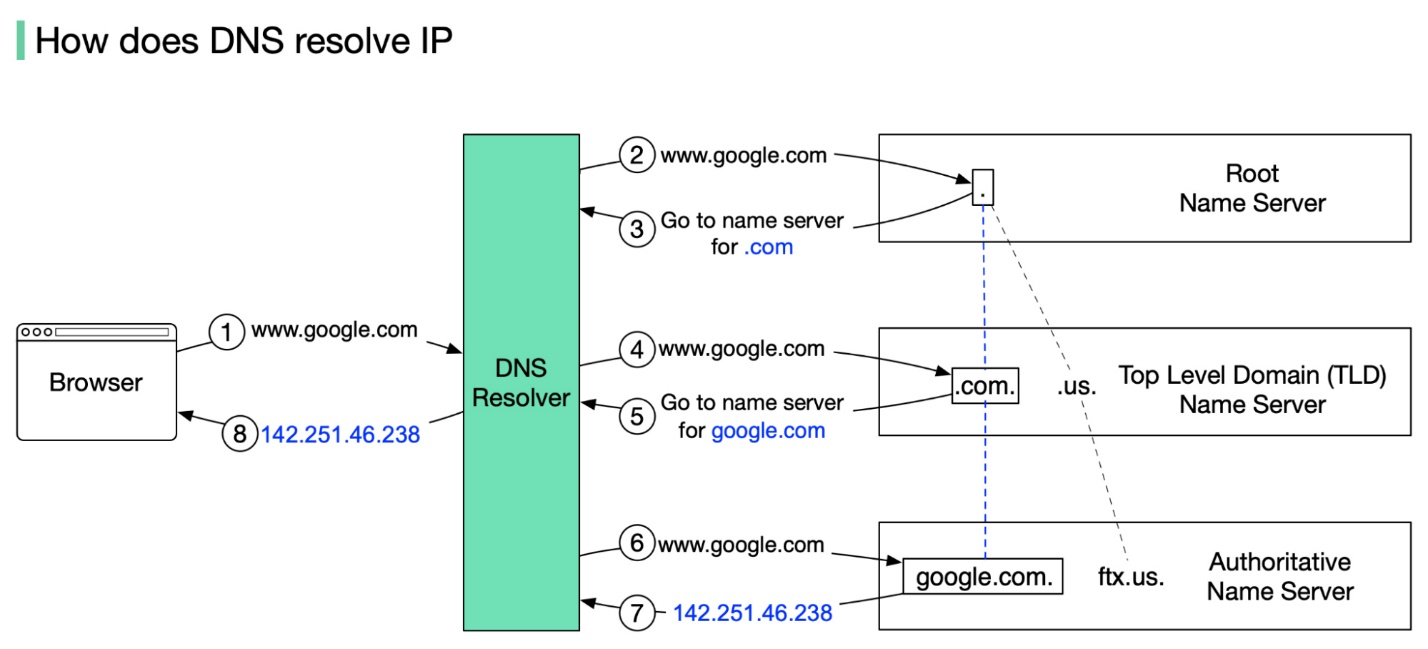
Part 2: Domain Name System

2.1. What is the purpose of DNS (Domain Name System) and how does it work?

DNS is a system that converts website names (website.com) *(Dave’s comment: domain name)* into an IP address that can be read by machines. This allows for a user-friendly interface instead of confusing IP addresses.

1. A user types a website name into the URL.
2. The user’s device queries a DNS Resolver
3. The DNS Resolver sends the requested website name to the Root Name Server if it doesn’t already have the name saved in cache.
4. The Root Name Server then directs it to the TLD which responds with the address of the authoritative name server for the requested domain (e.g., .com, .org, .net). This is the purpose of the .coms and stuff.
5. The DNS Resolver then sends a query to the Authoritative Name Server for that domain.
6. The Authoritative Name Server then responds with the IP address for that requested website name.
7. The DNS Resolver then sends the device the IP address of that website thus sending you to that website

*Dave’s comment: So what happens if you have more than two levels in a domain name, e.g.,* [*www.google.com*](http://www.google.com) *or foo.bar.example.com or alpha.bravo.charley,delta.com?*



2.2. Explain how the DNS resolution process works, starting from when a user types a URL into their browser.

Oh :C

2.3. What are the different types of DNS records, and what does each type do (e.g., A, AAAA, CNAME, MX, TXT)?

* A, gets a domain name for an IPv4 address.
* AAAA, gets a domain name for and IPv6 address.
* CNAME, makes an alias from one domain name to another. (site.com to [www.site.com](http://www.site.com))
* MX, targets the email servers responsible for that specific email domain.
* TX, stores small text information about a domain name.
* NS, targets the authoritative name servers for that domain.
* SOA, contains administrative information about the domain name.
* PTR, makes an IP address to a domain name.
* SRV, targets servers such as SIP, XMPP, LDAP, and more, in a domain.
* SPF, targets which mail servers are authorized to send email on behalf of the domain.

2.4. What is the difference between a recursive DNS resolver and an authoritative DNS server?

Recursive DNS resolvers recursively resolve DNS queries for clients by querying multiple DNS servers until the requested information is found. Authoritative DNS servers host DNS information for specific domain names and provide answers to queries regarding them.

2.5. Describe what happens during a DNS query and response process.

A DNS query is sent through the DNS Rersolver and is checked through it’s cache’s and if not found then it is sent through a sequence of servers until the device is given the equivalent IP address.

2.6 What is a DNS zone, and how does it relate to DNS records?

A portion within the DNS namespace that has specific DNS records and mappings between domain names.

2.7. What is DNS caching, and how does it improve performance?

Before a query is sent through it is checked through a cache system. It checks to see if the query has been sent before and if so it will just use the save IP address instead of finding it again.

2.8. What is TTL in the context of DNS responses?

It allows for a more efficient query by not allowing for server hopping to be continuous.

2.9. Use dig or nslookup to find the A record for olemiss.edu. What is/are the IP address(es)?

130.74.120.3

2.10. Use dig or `nslookup' to find the NS record for the root name servers.

ns1.olemiss.edu.

ns2.olemiss.edu.

dns0.ncl.ac.uk.

2.11 Use 'dig' or 'nslookup' to find the NS records for the cs.olemiss.edu name servers?

tim.cs.olemiss.edu.

Dave’s answer: % dig NS cs.olemiss.edu

; <<>> DiG 9.10.6 <<>> NS cs.olemiss.edu

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63938

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 4000

;; QUESTION SECTION:

;cs.olemiss.edu. IN NS

;; ANSWER SECTION:

cs.olemiss.edu. 3600 IN NS dc01.cs.olemiss.edu.

cs.olemiss.edu. 3600 IN NS dc02.cs.olemiss.edu.

;; ADDITIONAL SECTION:

dc01.cs.olemiss.edu. 3600 IN A 130.74.96.4

dc02.cs.olemiss.edu. 3600 IN A 130.74.96.5

2.12. Explain the role of the root DNS servers in the DNS hierarchy.

They can directly answer queries within the root zone.

2.13. What is a reverse DNS lookup and how is it different from a forward DNS lookup?

A reverse DNS lookup takes an IP address and finds its domain name. It is the reverse of a forward DNS lookup.

Part 3: Security

3.1. What is HTTPS and how is it different from HTTP?

Hypertext Transfer Protocol Secure uses encryption to provide a secure connection over the internet.

3.2. Explain the role of SSL/TLS in HTTPS.

It provides a secure connection via encryption.

3.3. What are digital certificates, and how do they contribute to secure communications?

They are electronic documents that verify a user's identity. This makes it to where if you don’t have a digital certificate, then you aren’t allowed to connect.

3.4. Describe the concept of public-key cryptography and how it is used in secure communications.

There are 2 keys a private and a public key that are mathematically related. When user A wants to send a secure message to user B, user A encrypts the message using user B's public key. Since only Party B possesses the corresponding private key, only they can decrypt and read the message.

*Public-key cryptography is also good for authentication. User A encrypts the message using A’s private key. Anyone with A’s public key can decrypt the message, but only someone with A’s private key could have encrypted the message. Since it is a private key, it is assumed that only A has the private key and as such only A could have encrypted the message. This therefore authenticates A as the source.*

3.5. What is a Certificate Authority (CA) and what role does it play in web security?

The CA is a 3rd party that confirms the legitimacy of a digital certificate.

3.6. Explain the difference between symmetric and asymmetric encryption.

Symmetric encryption uses the same key for en- and decryption while Asymmetric encryption uses a public key for encryption and saves a private key for decryption.

3.7. What is a VPN (Virtual Private Network) and how does it enhance security?

A VPN routes the user's internet traffic through a remote server. This allows a user to browse the internet without worrying about attacks from hackers because their connection is encrypted.

*Dave’s comment: A VPN does provide an additional layer of encryption between VPN endpoints, and it can be used to encrypt all communications between two networks that are connected to the endpoints of the VPN. It is also often used as a relay that is in a different country or different jurisdiction thereby providing the appearance of the user being in that different country or jurisdiction. This can get around region restrictions. It can also be used to redirect traffic through a relay to hide the destination of the traffic. This last use case is often used within China to get around the Great Firewall of China.*

3.8. What is a firewall, and how does it protect a network?

A firewall is a network security device that monitors and controls inward and outward network traffic. It bars malicious attacks from getting into a network.