# Assignment on Internet Technologies, Cloud Computing for CS50L

Total points 10/10

Starting in 2021, all assignments in CS50L are out of 10 points. A score of 7 points or better (70%) is required to be considered to have "passed" an assignment in this course. Please do not resubmit an assignment if you have already obtained a passing score. You don't receive a final grade at the end of the course, so it will have no bearing on your certificate, and it will only slow down our graders!

Unlike CS50x, assignments in this course are graded on a set schedule, and depending on when you submitted, it may take up to three weeks for your work to be graded. Do be patient! Project scores and assignment status on cs50.me/cs50l (e.g. "Your submission has been received...") will likely change over time and are not final until the scores have been released.

Email *

maz786@outlook.com

Name *

Mazafer Ul-Raqib

edX Username

Mazafer

What is your GitHub username?

You only need to tell us if you are concerned about checking your progress in the course and/or you want a free CS50 Certificate after you satisfy all of the requirements of the course. If you do not already have a GitHub account, you can sign up for one at https://github.com/join. You can then use this account to log in to cs50.me/cs50l to track your progress in the course (your progress will only show up after you have received at least one score release email from CS50 Bot, so do be patient!). Don't worry about seeing a 'No Submissions' message on submit.cs50.io, if you find that. The course collects submissions using Google Forms, and only the gradebook on cs50.me/cs50l is important! If you do decide to provide us with a GitHub username, BE CERTAIN IT IS CORRECT. If you provide the wrong username, you will not be able to see your scores.

https://github.com/maz786

This course is graded by human graders, and has a ZERO TOLERANCE plagiarism and collaboration policy. If *any* of your answers are copied and pasted from, or obviously based on (a) an online source or (b) another student's work in the course, in *any* of the course's ten assignments, you will be reported to edX and removed from the course immediately. There is no opportunity for appeal. There are no warnings or second chances. *

It is far better, we assure you, to leave an answer blank rather than risk it. This may be an online course, but it is offered by Harvard, and we're going to hold you to that standard.

◉ I understand this policy and agree to its terms; I hereby affirm that I will not plagiarize any answers or collaborate with any other students in this course .

## ✓ What does a DHCP server do? 1/1

A network server that automatically distributes IP addresses and other network parameters to connected devices is known as a Dynamic Host Configuration Protocol (DHCP) server. In order to obtain an IP address and other configuration data from the DHCP server, a connected device broadcasts a message known as a "DHCP discover." After receiving the request, the DHCP server provides the device with an available IP address, together with information on the subnet mask, default gateway, and DNS server. The device then uses the provided IP address to start communicating on the network and sends a "DHCP request" message to confirm the assignment.

In conclusion, a DHCP server automates the issuance of IP addresses and other configuration data, making it easier to configure IP addresses and other network settings for devices on a network. This helps to prevent conflicts and other problems with IP address assignment and helps to ensure that devices on the network can connect with each other and with other networks.

## ✓ What does it mean if a URL begins with https:// as opposed to http://? 1/1

A URL that starts with "https://" rather than "http://" denotes a secure HTTPS connection for the website. HTTPS, which stands for "Hypertext Transfer Protocol Secure," combines the widely used HTTP protocol for data transmission on the internet with the SSL/TLS security layer to encrypt the data in transit.

Your web browser creates a secure connection with the web server using SSL/TLS when you access a website using an HTTPS connection. As a result, the data being communicated between your web browser and the web server is kept confidential and authentic.

In general, you can detect if a website is using an HTTPS connection by glancing at the URL in the address bar of your web browser. A secure connection is being used by the website if the URL starts with "https://". If the connection is secure, you might also see a lock icon or another indicator in the address bar.

In order to assist safeguard your privacy and security when sending data over the internet, it is generally a good practise to use an HTTPS connection whenever it is feasible. Many websites employ HTTPS connections to assist maintain the security of their users' data, including online banking and retail platforms.

✓ During a traceroute, sometimes the entirety of an entry will be an asterisk. Why is that? 1/1

For a hop that does not reply to the traceroute request, the round-trip time (RTT) is often replaced during a traceroute with an asterisk (*). This could occur for a number of reasons.

The router or other network device at that hop might have been set up to ignore traceroute requests, which is one potential explanation. For security or other reasons, certain network administrators might take this action.

Another explanation is that the router or other device at that hop is not receiving the traceroute request due to a network problem. This can be the result of a router issue or a problem with the network connection.

Using a traceroute, you may see the route that network packets follow to get from one place to another. It operates by delivering a sequence of packets to the destination with progressively longer time-to-live (TTL) values while tracking the RTT for each hop. How many hops the packet is permitted to complete before being deleted is determined by the TTL value, a field in the packet header. A router discards a packet and returns an error message to the source when it receives a packet with a TTL value of 1. The traceroute tool may map the path that packets take via the network, pinpointing any instances where packets are dropped or fail to reach their destination by increasing the TTL value for each consecutive packet.

✓ When we try to visit a web page and the server responds to say that page doesn't exist, we ordinarily receive a "404 Not Found" error in the HTTP headers. Provide two examples from lecture of other HTTP "response codes" that David shows, and what they mean. 1/1

200 OK
301 Moved Permanently
302 Found
304 Not Modified
401 Unauthorized
403 Forbidden
404 Not Found
418 I'm a Teapot
500 Internal Server Error

✓ Recall that TCP (tries to) guarantee delivery by ensuring that any lost packets are resent. Provide a *specific* reason why packets might be lost between a sender and receiver. 1/1

When using the Transmission Control Protocol (TCP), packets may be lost between a sender and recipient for a number of specific reasons, including the following:

Packets may be dropped because of insufficient bandwidth or other resources when there is a lot of traffic on the network.

Failure of a router on the path connecting the sender and the recipient could cause packets to be lost.

Packets might be lost as a result of transmission problems brought on by interference or other circumstances.

Failures of the network: Packets may be lost if there is an issue with the network itself, such as a damaged cable or a power outage.

Malware: Malware, such viruses or worms, can obstruct packet transmission and result in packet loss.

Inaccurate routing: Packets may be dropped or forwarded to the wrong location if the routing tables in the routers along the path between the sender and recipient are incorrect.

To ensure dependable delivery, TCP is built to identify missing packets and resend them as necessary. It is still possible for packets to be lost due to the different circumstances stated above, despite the fact that these precautions are in place.

✓ Why might two users appear to some website as having the same IP address, even though they're each actually configured with a different IP address? 1/1

Even though they are individually configured with a different IP address, two users may seem to a website as having the same IP address for a number of different reasons:

Network Address Translation (NAT) is a technology that enables several devices on a private network to share a single public IP address while logging on to the internet. As a result, to external servers and websites, every device connected to the private network will appear to have the same IP address.

Proxy server: A proxy server is a server that stands between a client and a server in communication. The IP address of the proxy is used in place of the client's IP address when a client connects to a server using a proxy. As a result, to external servers and websites, all clients connected to the proxy will appear to have the same IP address.

Virtual Private Network (VPN): A VPN is a private network that links distant people or sites using a public network, typically the internet. The IP address of the VPN server is substituted for the user's IP address when they connect to a VPN. This implies that to external websites and servers, all users connecting to the VPN will appear to have the same IP address.

A load balancer is a tool that splits up incoming traffic among many servers or resources. A load balancer's IP address is used in place of the user's IP address when they connect to a website through it. All users connecting to the load balancer will consequently seem to the website to have the same IP address.

## ✓ How do we distinguish "virtualization" from "containerization"? 1/1

To divide and isolate resources in a computer system, two alternative technologies are used: virtualization and containerization. On a single physical system, both technologies support running numerous programmes or processes, but they do it in distinct ways.

On a physical machine, virtualization entails the creation of one or more virtual machines (VMs), each of which runs its own operating system (OS) and applications. A virtual machine (VM) is essentially a software emulator that operates with its own CPU, memory, storage, and network interface just like a real computer would. Because VMs are separate from one another and from the real system that serves as the host, they can run various OSes and programmes without interfering with one another.

On the other side, containerization entails putting apps and their dependencies into small, independent containers that can operate on any platform that has the container runtime. The resource isolation features of the OS are used by containers to allocate resources and isolate processes. Containers share the host OS and kernel. Because of this, containers are lighter and more portable than virtual machines (VMs), but they are also less isolated from one another and from the host system.

In conclusion, while containerization involves putting apps into containers that share the host OS, virtualization is constructing virtual machines that run their own operating systems.

## ✓ In what sense are domain names similar to phone numbers like 1-800-COLLECT? 1/1

In the sense that 1-800 numbers, sometimes referred to as toll-free or freephone numbers, and domain names are both special identifiers that are used to promote communication and make it simpler for individuals to get in touch with one another. A 1-800 number is a special phone number that enables users to make phone calls without paying long-distance fees, whereas a domain name is a distinctive name that is used to identify a website on the internet. To simplify communication and make it simpler for people to find and contact one another, 1-800 numbers and domain names are both employed.

✓ How might a company technologically prevent its employees from spending time on, say, facebook.com? 1/1

Without, say, installing software on each individual computer at the business?

A business could take the following measures to stop staff from using social media sites like Facebook:

Utilize a web filtering tool: To prevent access to particular websites, such as social media platforms like Facebook, many businesses use web filtering software. These tools can be set up to prevent access to particular websites or groups of websites (e.g. social media).

Use a network firewall: A network firewall can be set up to prevent access to particular IP addresses or websites. This would stop workers from using the company's network to visit Facebook or any other restricted websites.

Utilize a content blocking extension: Some online browsers have extensions that let users block particular websites or groups of websites. On corporate computers, these extensions can be installed to prevent access to Facebook and other distracting websites.

Create and uphold internet usage guidelines: Clear criteria for acceptable website usage at work could be established by a firm, along with other internet usage rules. To make sure that staff are adhering to these policies, this might be used in conjunction with monitoring technologies.

Use website filtering software: A variety of software tools are available that allow you to restrict access to certain websites. On corporate computers, these applications can be installed to prevent access to Facebook and other distracting websites.

It's important to note that while some of these choices (like web filtering tools and network firewalls) can be applied at the network level, others (like them) may require software to be installed on specific devices.

✓ How might a user watch Netflix while abroad, even though their account is accessible only to users in, say, the US? 1/1

Even if a user's Netflix account can only be accessed in the US, there are a few choices they may want to take into account:

Make use of a Virtual Private Network (VPN): A VPN is a device that encrypts an internet user's connection and directs it through a server in a location of the user's choosing. The user's location can be "spoof"ed" using this to appear as though they are connecting to the internet from a different nation. While travelling, a user can access their Netflix account by connecting to a US server using a VPN.

Implement a Smart DNS proxy: Similar to a VPN, a Smart DNS proxy only directs traffic required to resolve a website's DNS problems.

Use a Smart DNS proxy: Similar to a VPN, a Smart DNS proxy merely directs traffic required to convert a website's domain name to an IP address (as opposed to routing all internet traffic). This can be used to get around geographical limitations on some websites, like Netflix.

Use a browser extension: You can get around regional limitations on websites like Netflix by using several browser extensions. Similar to a VPN, these extensions operate by routing the user's traffic through a server in the user's preferred location.

It's important to keep in mind that accessing Netflix (or any other website) through a VPN, Smart DNS proxy, or browser extension while the website isn't ordinarily accessible may be against its terms of service. Additionally, these tools may not always be successful in getting around regional restrictions, and they can slow down a user's internet connection.

Debrief

About how many MINUTES would you say you spent on this assignment in total? *

Just to set expectations for future students.

666

Google Forms