# 1 Requirements

1. You must have a working Ubuntu (or other Linux based) system installed **PRIOR** to this class. Failure to do so will prevent you from doing this assignment.

2. It is recommended, although not required, to work on this assignment in advance and to use the actual assignment day to ask questions and engage in discussion on the topic.

# Contents

**1 Requirements** **1**

**2 Introduction** **2**

**3 Definitions** **2**
3.0.1 OSI Model . . . 2
3.1 Ip Addresses . . . 2
3.2 Link Layer . . . 3
3.3 Packet Routing . . . 3
3.4 Workshop . . . 3
3.4.1 IP Manipulation . . . 3
3.4.2 Layer 4 . . . 3
3.5 VPN and routing . . . 4
3.6 Network Troubleshooting . . . 4

# 2 Introduction

So far all exercices in HP classes have been run only on one computer: your own. Except for the API class you did not have to connect to any other machine. This changes today. The goal of this class is to understand how computers communicate together, exchange information and how information is rooted across the world to form ”The Internet™”

# 3 Definitions

#### 3.0.1 OSI Model

The OSI (Open Systems Interconnection) model is a framework for understanding how communication occurs between devices on a network. It divides the process of communication into seven layers, each of which performs a specific function in the transmission of data. The seven layers of the OSI model are:

1. Physical layer: This layer is concerned with the physical transmission of data, such as electr

   ical signals or light pulses, over a medium, such as a copper wire or fiber optic cable.

2. Data link layer: This layer is responsible for the reliable transmission of data across a link, such as a point-to-point connection or a local area network. It provides error detection and correction, as well as flow control.

3. Network layer: This layer is responsible for routing data packets through a network, such as the internet, based on the destination address of the packet. It also provides logical addressing, such as IP addresses, to identify devices on the network.

4. Transport layer: This layer is responsible for the reliable delivery of data between two devices, including error detection and recovery. It also provides end-to-end flow control and segmentation and reassembly of data.

5. Session layer: This layer is responsible for establishing, maintaining, and terminating communication sessions between devices. It also provides synchronization and flow control for data exchange.

6. Presentation layer: This layer is responsible for the representation and formatting of data, such as encoding and decoding data for transmission. It also provides data translation and conversion between different systems.

7. Application layer: This layer is the highest layer of the OSI model and is responsible for providing services to application programs, such as file transfer or email. It also defines the interface between the application and the network.

In summary, the OSI model provides a standard for understanding the different functions involved in the communication process and how they interact with each other. It allows devices from different vendors to communicate with each other by dividing the communication process into separate layers that can be implemented independently.

## 3.1 Ip Addresses

IP (Internet Protocol) addresses are numerical labels assigned to devices connected to a computer network that uses the Internet Protocol for communication. IP addresses serve as the location address of a device and allow devices to communicate with each other.
There are two main classes of IP addresses: IPv4 and IPv6. IPv4 addresses are 32-bit addresses that are expressed in four octets (eight-bit blocks) and are written in the dot-decimal notation (e.g., 192.168.1.1). IPv4 addresses are divided into five classes: A, B, C, D, and E. Class A addresses are used for large networks, such as those of universities or corporations. Class B addresses are used for medium-sized networks, such as those of hospitals or schools. Class C addresses are used for small networks, such as those of homes or small businesses. Class D addresses are used for multicast applications, while class E addresses are reserved for experimental purposes.
In summary, different classes of IP addresses are used for different sizes of networks and for different types of applications. IPv4 addresses are mainly used for small to medium-sized networks, while IPv6 addresses are used for large networks and for the future expansion of the internet.

1. How are IP addresses used to identify devices on a network?

2. How does a device obtain its IP address?

3. What is the difference between a public and a private IP address?

4. How do network administrators assign IP addresses to devices on a network?

5. How do devices on a network communicate with each other using IP addresses?

6. What is the purpose of a default gateway in a network?

7. What is a subnet mask and how is it used in conjunction with an IP address?

8. How do IP addresses and subnet masks work together to create network segments?

9. What is the difference between IPv4 and IPv6, and how do they differ in terms of address space and addressing schemes?

10. How can network administrators troubleshoot problems related to IP addresses and network connectivity?

## 3.2 Link Layer

A MAC (Media Access Control) address is a unique identifier assigned to network devices, such as computers, routers, and smartphones. It is a 12-digit hexadecimal number that is typically written in the format "XX:XX:XX:XX:XX:XX", where each "X" represents a hexadecimal digit. MAC addresses are used to identify devices on a network and are often used in conjunction with IP addresses to establish communication between devices. MAC addresses are typically stored in the device's hardware and cannot be easily changed. They are used by the network's switches and routers to forward data packets to the correct destination device. MAC addresses are also used in network security protocols to restrict access to certain devices or networks.

1. What is the purpose of a MAC address and how is it used in networking?
2. How does a MAC address differ from an IP address, and how are they used together?
3. Can a MAC address be changed or spoofed, and if so, what are the potential consequences or uses for doing so?
4. How is an IP address assigned to a device on a network, and what are the different types of IP addresses (e.g. private, public, IPv4, IPv6)?
5. How do devices on a network use IP addresses to communicate with each other, and how is the route between devices determined?
6. Can an IP address be shared among multiple devices on a network, and if so, how does this affect communication and network performance?
7. How does network address translation (NAT) work and what is its role in allowing devices on a private network to communicate with the internet?

## 3.3 Packet Routing

Packet routing on the internet is the process of directing data packets from a source device to a destination device through a network of interconnected devices, such as routers and switches. The routing process is based on the destination address of the packet, which is stored in the packet's header. Each device on the internet maintains a routing table, which contains a list of destination addresses and the corresponding next hop, or the device to which the packet should be forwarded. When a device receives a packet, it looks up the destination address in its routing table and forwards the packet to the next hop. The packet continues to be routed through the network until it reaches its destination. Packet routing enables the internet to transmit data from one device to another, regardless of the physical location of the devices.

## 3.4 Workshop

### 3.4.1 IP Manipulation

1. Set your IP address yourself so that the last number is one digit different.
2. Use the traceroute command to discover the path taken by a packet to 1.1.1.1
3. What is ICMP? What is DHCP? What is ARP?
4. Find the RFCs of the protocols above.
5. What is a broadcast address?
6. What is a CIDR representation?
7. Convert the following IP CIDR to IP and Subnet Mask: 192.168.0.3/24, 10.10.0.0/22, 10.0.0.0/8

### 3.4.2 Layer 4

The transport layer is responsible for the reliability of data delivery. The TCP protocol is the most commonly used protocol providing this feature. It is used in conjunction with the Internet Protocol (IP) to form the core of the Internet's communication infrastructure.
TCP is a connection-oriented protocol, which means that it establishes a logical communication channel between two devices before transmitting data. This allows TCP to provide a number of important features, such as error correction, retransmission of lost data, and flow control to ensure that data is transmitted at a rate that the receiving device can handle.
TCP is used by a wide range of applications, including web browsing, email, file transfer, and remote access. To differentiate between all these usages and to enable multiple communication stream at the same time from a machine, TCP uses a port number to identify the connection.

1. Using Wireshark, look at the TCP communication elements going on your machine.
2. List all the active TCP connections on your machine.
3. What other kind of connection does your machine support?
4. What are the different states of a TCP connection.
5. What is Network Address Translation (NAT) and what is it used for?
6. What is ARP spoofing?

## 3.5 VPN and routing

**This part can only be done during the class or if you wish to set up the network backbone yourself.** Is this section of the workshop, you will discover the WireGuard VPN, install it on servers to create a secure connection between them and create routes to direct your traffic securely to a web server. WireGuard is a free and open-source software application and communication protocol that implements virtual private network (VPN) techniques to create secure point-to-point connections in routed or bridged configurations. It was designed as a general-purpose VPN that can be easily implemented in a wide range of software, including Linux, Windows, MacOS, Android, and iOS.

1. How does Wireguard work? How can you install it?
2. Ask the teacher for the IP addresses and network map of the server you will be using. There are 4 server: 2 are located in london and act as a gateway for our WireGuard server and the other as a gateway to the New York data-center. The other two servers are located in New York and act as a WireGuard client connecting to the London gateway, the last server is hosting our super secret web server. This architecture can be seen in the Figure 1
3. Create a Wireguard VPN between Gateway 1 and Gateway 2.
4. Remove the ability for the web server to be accessed by a public IP.
5. Create a route between the Gateway1 and Gateway2 so that the 2 VPC networks are connected.
6. Change your computer routings to use the Incoming server when you want to reach the Web Server address.
7. Use traceroute to see the different hops to the web server.

## 3.6 Network Troubleshooting

1. What are the different network errors you have seen so far?
2. What is the likely issue for a *Connection Refused* ?
3. What is the likely issue for a *Connection Timed Out* ?
4. What is the likely issue for a *No Route to Host* ?

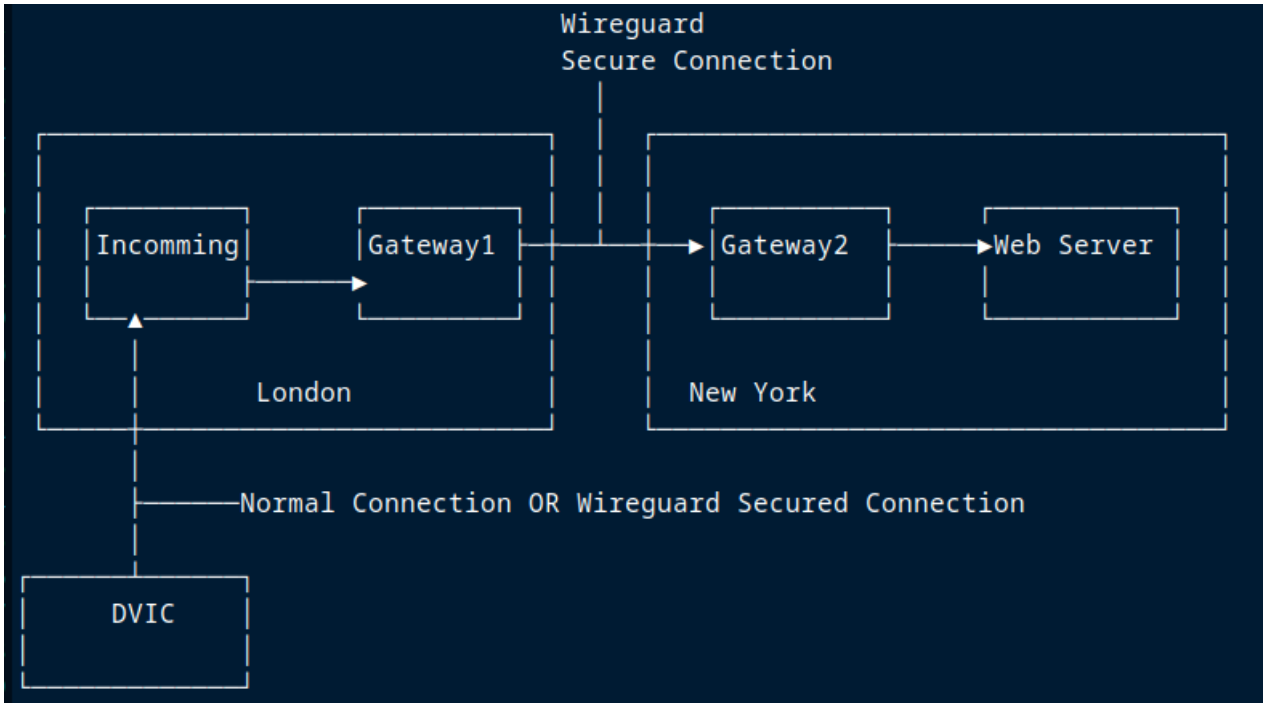


Figure 1: Server Mapping for the exercise in Section 3.5. The 4 servers are in two different datacenters. the goal is to create a routing plan from the incoming server