Course 1: Basic Computer networking

PAN- Perosnal Area Network that is the network your phone works on such as ur bluetooth

LAN is govering by one adminstration for ppeople within the organisation. One adinstration ,confine within an area for a set of people, connection within an internal protocool.

Global network (WAN) the largest lan we have is the internet, it overs larg distances

Internet Networking

The Internet is the physical connection between computers and wires around the world. The Web is the information on the Internet.

The Internet is composed of a massive network of satellites, cellular networks, and physical cables buried beneath the ground. We don’t actually connect to the Internet directly. Instead, computers called servers connect directly to the Internet. Servers store the websites that we use, like Wikipedia, Google, Reddit, and BBC.

Clients don’t connect directly to the Internet. Instead, they connect to a network run by an Internet service provider or ISP, like MTN, Glo and so on. ISPs have already built networks and run all the necessary physical cabling that connects millions of computers together in one network.

An IP address is composed of digits and numbers like 100.1.4.3. When we want to access a website like www.blogspot.com, we’re actually going to their IP address like 172.217.6.46.

Computers have addresses just like houses. Computers on a network have an identifier called an IP address.

Network Protocool

Think of network protocols as a set of rules for how we transfer data in a network.

There are two protocols that you need to know. The Transmission Control Protocol and the Internet Protocol, or TCP/IP for short

The Internet Protocol or IP, is responsible for delivering our packets to the right computers. Remember those addresses that computers use to find something on a network? They’re called IP addresses or Internet protocol addresses. The Internet Protocol helps us route information.\

The Transmission Control Protocol or TCP, is a protocol that handles reliable delivery of information from one network to another. This protocol was an important part of the creation of the internet since it let us share information with other computers. We’ll spend a lot of time diving into these protocols in our upcoming blogs, for now, this is all you need to know.

In summary, L2 switching is used for communication within the same LAN, while L3 routing is used to forward data packets between different networks.

In this scenario, L2 switching would be used within each LAN to allow devices within the same LAN to communicate with each other using their MAC addresses. For example, if an employee in the New York office wants to send a file to another employee in the same office, L2 switching would be used to forward the file directly to the recipient's device.

However, to allow communication between the New York office and the Los Angeles office, L3 routing would be needed to forward data packets between the different networks. The router in the New York office would use the IP address of the destination device in the Los Angeles office to determine the best path to forward the data packet across the internet to reach the Los Angeles office's LAN. Once the data packet arrives at the Los Angeles office, L2 switching would be used within the LAN to forward the packet to the intended recipient's device.

Here are some key differences between IPv4 and IPv6:

Address size: One of the most significant differences between IPv4 and IPv6 is the size of their addresses. IPv4 addresses are 32 bits long, which means that there are a total of about 4 billion possible addresses. In contrast, IPv6 addresses are 128 bits long, which allows for an almost unlimited number of unique addresses. This is important as the number of devices connected to the internet continues to grow.

Address format: The format of IPv4 and IPv6 addresses are different. IPv4 addresses are typically represented in dotted-decimal notation, such as 192.168.0.1. IPv6 addresses are typically represented in hexadecimal notation, such as 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

Security: IPv6 includes built-in support for IPSec, which provides authentication, integrity, and confidentiality for network traffic. While IPSec can be used with IPv4, it is not built-in and requires additional configuration.

Subnetting is the process of dividing a larger network into smaller subnetworks, or subnets, to improve network efficiency and security. It allows an organization to use a single IP address space for multiple smaller networks, rather than having to use separate IP address spaces for each network.

For example, suppose an organization has been assigned the IP address range 192.168.0.0/24. This means that the network has 256 available IP addresses, ranging from 192.168.0.1 to 192.168.0.254, with 192.168.0.0 reserved as the network address and 192.168.0.255 reserved as the broadcast address.

Subnetting requires careful planning and design, as it can affect network performance and security if not implemented correctly. However, when done properly, subnetting can help to optimize network resources and make it easier to manage and secure large networks.

Ping and Traceroute are two common tools used in networking to diagnose network connectivity issues and troubleshoot problems.

Both Ping and Traceroute can be used to diagnose network connectivity issues, troubleshoot network problems, and identify potential bottlenecks or routing issues. They are often used in conjunction with other network tools and techniques to provide a more comprehensive view of network performance and behavior.

Ping is a basic utility used to check if a device or host is reachable on the network. It sends a small packet of data to the destination device and waits for a response. If the destination device responds, it means that it is reachable and there is network connectivity between the two devices. If there is no response, it may indicate a network connectivity issue or that the destination device is offline or configured to not respond to ping requests. (open cmd and put ping web address)

Traceroute is a more advanced tool used to determine the path that network traffic takes to reach a particular destination device or host. It sends a series of packets to the destination device, each with a different time-to-live (TTL) value, which is decremented by each router along the path. When a packet's TTL value reaches zero, the router discards the packet and sends back an error message. Traceroute uses these error messages to determine the path that network traffic takes and displays the path along with the round-trip time (RTT) for each router along the way. (open cmd and put tracert an dIP address)

OSI LAYER

Physical Layer is the wire that are connected together

Application: This is whrer u inout and outout ur data, the software u used is the application layer

Presenationtation LAer: is your computer OSI that makes everything posisble, that is why u use your application

The sesion is reponsisble for reate and mainting sesion on how the application connect to the intert base on the presentanion(OS) connection to the web server

Trasnsport: Transferiing of information from one appliation to another majory betwen the OS and wweb server

Network: this is wherer routers operate. the router is responsible for sending packets of information out into the internet and receiving them. These packets origin and destination is determined by the IP address of your router.

Layer 1 — Physical

The physical layer is literally the physical hardware that makes up the network. This layer has several major functions:

Defining physical specifications

Defining protocols

Defining transmission mode (half duplex & full duplex)

Defining the network’s topology

Purpose of the OSI Model

Even after reading a description of each of the seven layers, you may still be confused as to how the OSI model applies to real life networking. It’s commonly misunderstood how a model can be used to solve real-life problems and in some cases, a model may not be the best approach. However, in many aspects of Information & Communications Technology(ICT), a model can be extremely useful and that is the case for the OSI model.

When first discovering a networking problem, it can be confusing as to where you should start. The OSI model helps you to start figuring out where the problem may reside and therefore, help you to solve the problem. For example, a client’s computer is not able to reach a website. The problem is isolated to one device on the network, so it can be assumed that the problem is likely to be on the application layer. However, after testing you find that the problem still exists when you try a different web browser and so the application layer is ruled out. You then assume that the problem resides on the presentation layer and start looking for faulty settings. After some digging around you find that your client has entered some DNS settings incorrectly and so you then conclude the problem is on the presentation layer.

You may already be using the OSI model for simple problem solving such as the example above without even realizing it. However, when dealing with large, corporate scale networking a purposeful use of the OSI model can make your job much easier and more enjoyable.