Mamun Hossain - 10053073

Part 1: Networking:

Introduction:

To understand networking, we have to know what networking is exactly. We have previously learned that computer networking refers to the interconnection between devices that have the ability to transfer and exchange data and share their resources amongst each other. All devices have the ability to network with each other in some capacity.

You will have devices such as switches and routers that are the skeleton of the computer network. These devices will then connect to a simple device, like your computer or printer, which then will send data to the router so it can choose the best route for the network to pass through.

Switches and routers are very different but they have a distinct way of knowing how they interact with different devices. Some switches have a permanent pre assigned MAC address, whereas some routers will have a network assigned external IP address.

The reason why computer networks prove to be so important is that across organizations, it allows the ease of sharing information, it saves a lot of money, storage, and also adds a high degree of data security, and to this day it is ever evolving, as we have been learning in our distributed course.

Computer Networks Course Summary:

In our previous year, we had begun an introduction to Computer Networks where we had learned and applied our knowledge of C programming and Linux as well as understanding the TCP/IP reference models. We also learned briefly about the OSI network layers and how it interacts with the commands we had instructed in our labs. The goal of the course was to be able to use Cisco hardware and software tools to build small networks, understand the functions, protocols and timing of network devices such as hubs, bridges, switches, routers, and gateways, and to understand ethernet coding and protocol structure. The goal was to increase our understanding of computer networks and being able to even create our own computer network in the future.

7 Layers of the OSI interconnectivity model:

In the OSI interconnectivity model, there are 7 different layers. But it wasn't always the case as several decades ago there were two different models that depicted Computer Networks. That being said, the OSI model goes from layer 7 to layer 1. We will be discussing the following layers: Application (Layer 7); Presentation (Layer 6); Session (Layer 5); Transport (Layer 4); Network (Layer 3); Data Link (Layer 2); Physical (Layer 1). We will begin discussing with layer 7.

Layer 7 - Application:

With the application layer, it will provide a means for the end user to interact with a device that is connected to the specified network. The way the end user interacts can be done in a way such as opening a web browser or network based application (email). To put it simply, the application layer is the data the user can see while the application is running. Some examples of this layer could be, but not limited to: email, instant messaging, browsing the internet, printing documents etc.

Layer 6 - Presentation:

The purpose of the presentation layer is to send the data from an application and convert that in a readable form for the network to access. This basically allows the system to understand and relay the information to the end user. Examples of the session are: Encryption and expansion of a message to allow efficient travel across the network, content translation, graphics formatting, etc.

Layer 5 - Session:

The session layer provides different values to the number of bytes in each session that the end user is using during that period. The main purpose of the session layer is to ensure applications can work on devices, and can manage and terminate bytes and code through a network. Some examples are: Synchronization of data flow, Partitioning of services into functional groups, and creating dialog units.

Layer 4 - Transport:

The transport layer will allow different devices to connect and interact to each other if they are on the same network. Dependant on the network and the application being used, the transport layer can communicate with the devices which is reliable, secure, and offer the best effort communications. Examples of this are: Application identification, Detecting errors in the transmissions, and being able to identify client level entities.

Layer 3 - Network:

The network layer makes sure that the packets of information can be sent through the layer 2 networks and sent to the right locations, also known as logical addresses. With the evolution of modern technology, IP addresses have been made in a way to easily access and connect different networks with each other, as we have seen with different server machines across the world.

Using different things called subnets (separation of the network layer into smaller parts -Figure 1) will help the router use the subnet of the network's IP address to connect to all the devices that are sharing that server information. Now the way the router can accomplish this is by finding the shortest path in the network and calculating the best way to reach each specified network in the organization. An example of this would be from going from one router to another on the network to create the fastest connection. Now a router traveling from one router to another can cause fragmentation, but all the fragmented packets are repaired and put together at the final destination system of the layer network. Some basic security functionality can also be set by the filtering traffic using router addresses or something similar.

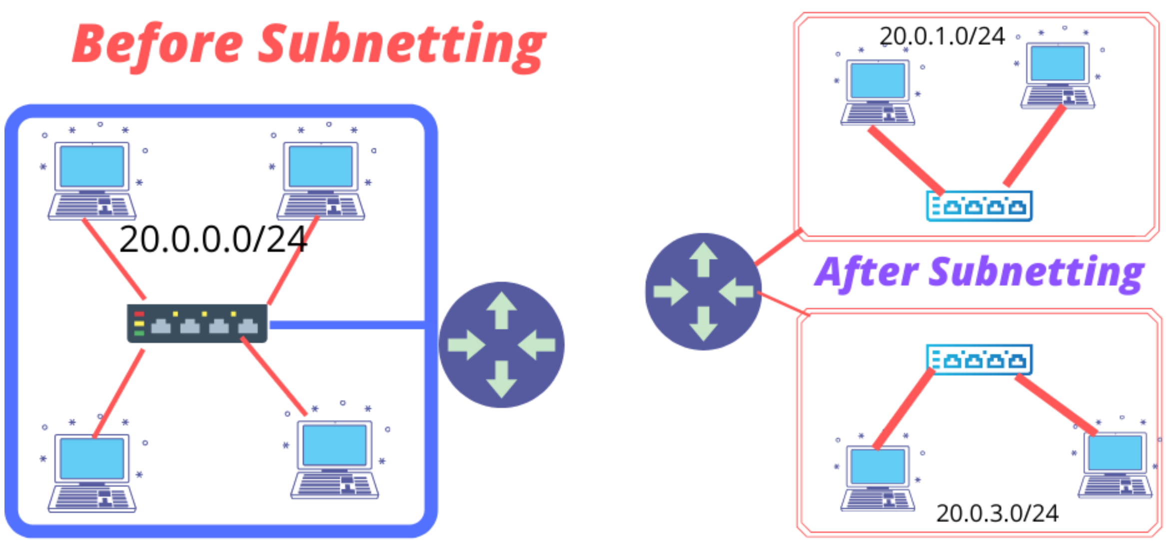

Figure 1: Subnet Example

Layer 2 - Data Link:

For layer 2 of the OSI model, it is only part of a LAN. The way it works is that will allow the network the ability to send and receive messages and packets across a server, while also providing a physical address so the devices can send the information across a network. Some components that are required are Ethernet ports and bridges and network interface cards (NIC). NICs also have assigned MAC addresses that helps with the traffic of information making sure the network doesn't get overloaded with information. Refer to Figure 2 to see how the MAC addresses work in cohesion with the Ethernet switches.

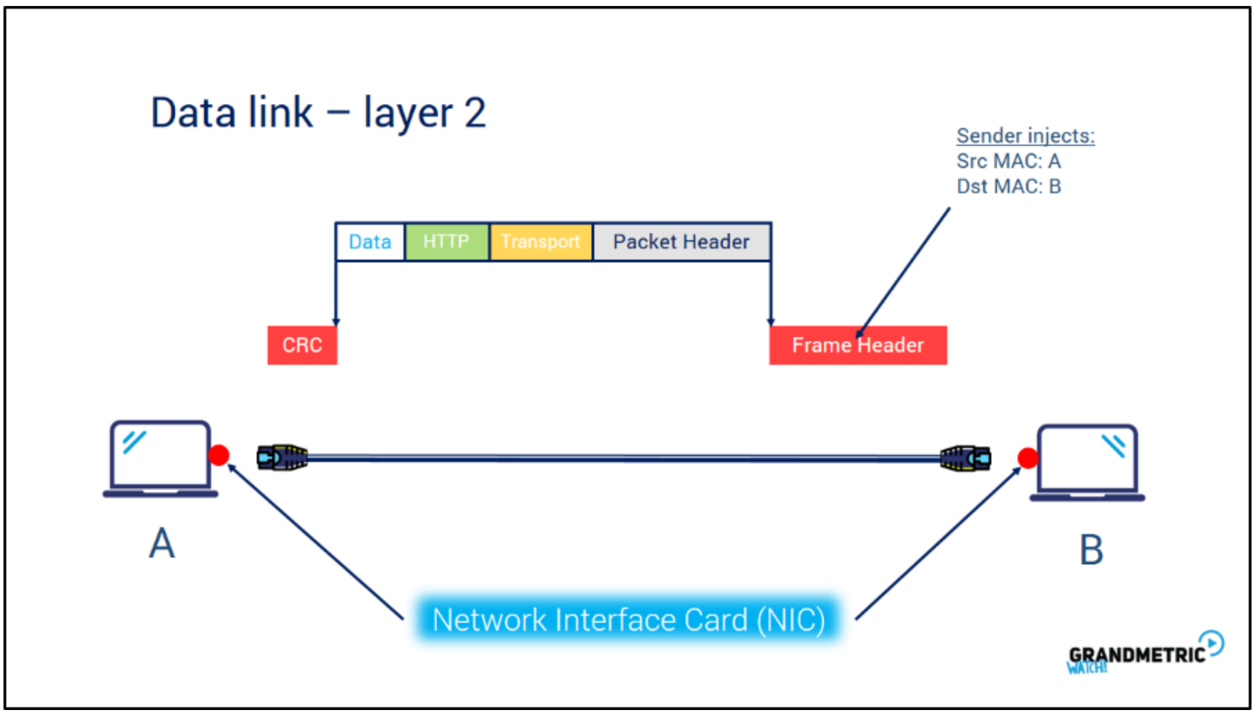

Figure 2: Data link layer working with NIC

Layer 1 - Physical:

The way the physical layer works is taht you have the device send information through the connector which will then go to the patch panel and to the hub and repeater. There are different requirements for the connector, such as the cable that will provide information routing (ex. CAT 6 cable). There are several electrical, mechanical, functional, and procedural requirements before any information can be relayed onto the network. Some examples of the components required are the following: Adapters that can connect the media, Network Interface Cards, Hub, Repeater, Cabling system materials, devices that can connect to the network.

The way this ultimately helps two applications to communicate is because if host connections are not established, if data can't be translated, and if data can't be transferred or received, how will any information across different applications ever be sent? The OSI model solves all these problems and more, making communication between applications seamless.

Part 2: Virtualization

Resource Consolidation:

We have learned that in a distributed system, we partition our resources into computation units. The way this works is that resource utilization can increase and in turn will reduce the cost of the management and associated with the compute processing in different applications, mainly cloud based.

Resource Partitioning:

A lot of large scale solutions can be divided into partitioning to taht way the data can be accessed in separate way. A good example of this is in our systems programming course last year we had to partition our hard drives to allocate our system to be able to use Ubuntu. In doing so, we were able to improve scalability and optimize performance instead of using a Virtual Machine which would have used more computing power.

The reason we partition data is to make sure that we can improve scalability, improve security, improve performance, improve availability, provide flexibility, and match the data to the pattern of use. In doing all these things it would make our usage of the programs and applications much more comfortable.

When we design partitions, there are three strategies: Horizontal partitioning; where we separate the data store but the partitions retain the same schema. Then we have vertical partitioning; where the fields are divided according to the way they are being used. Lastly, we have functional partitioning; where the data is changed in correlation to how the data is being bound in the system itself.

Snow Flocks:

With the issue of needing a cloud server being needed to manage cluster membership and addition of new servers, SnowFlock alleviates these problems with a cloud API call. It uses this API called VM cloning which in turn allows for resource allocation, cluster management, and application logic to apply to these issues immediately.

The way SnowFlock makes its approach is by using the following concepts: Virtualization (which allows for the cloud and machine cloning); Lazy Propagation (VM doesn't clone unless necessary); Multicast (Clones will all have similar attributes); Page Faults (Clone execution with missing memory won't run until page arrives); and Copy on Write (when memory is copied before being overwritten).

With all this, it makes it possible to alleviate stress on the cloud servers and help with ensuring that they do not need to constantly boot new instances from the same template and aids with parallel computing, data mining, and serving web pages.

Generic Homework Questions:

What resources are managed and how?

The resources that are managed are the data that is being partitioned. The way it is being managed is by three different ways, one being the SnowFlock which creates the VM cloning, also with partitioning with consolidation as well as improving the information within resource partitioning.

How does the system described in the article provide the following requirements:

Resiliency in case of failures?

SnowFlock shows resilience in the case of failure by being the counter measure by using VM Cloning when it is necessary.

Scalability in case of expansion in various parameters?

Because of the necessary mutations and the centralization for network traffic, the SnowFlock method causes issues in expansion in various parameters.

Maintainability in response to continuous changes?

On a large scale change, there will be many failures amongst the VM clones. So the reliability on a large scale is very difficult as the server only cares about maintaining its own flow control But because of using the mcdist system, SnowFlock can scale well