ADVANCED NETWORKING HOMEWORK

1. What are packets?

Packets are the small manageable pieces of information that can be transmitted over the internet with ease. In other words, Information is broken down into packets so that it can be transmitted faster and easily.

2. What is the TCP/IP protocol stack?

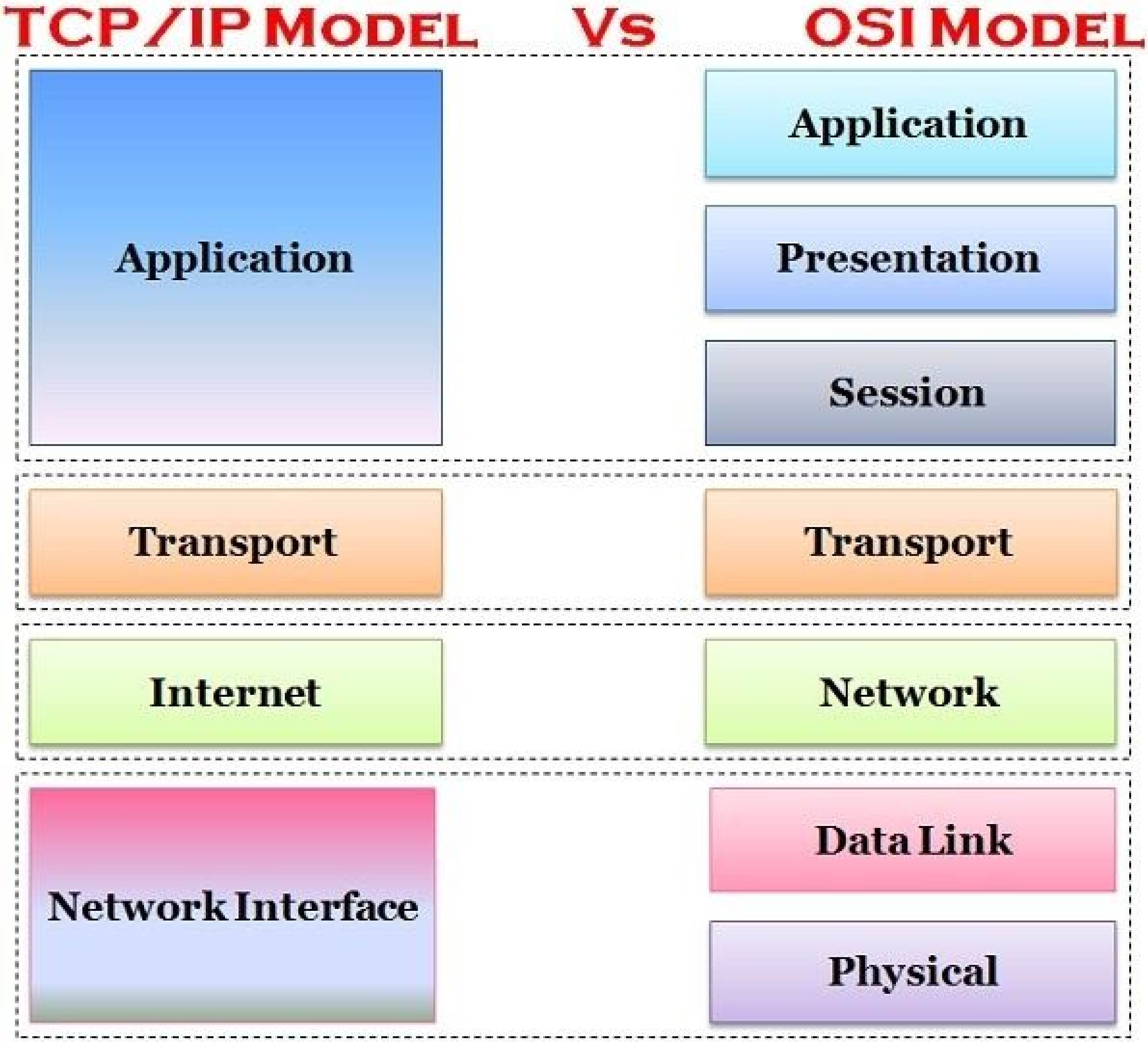
TCP/IP protocol set is a set of rules that divides different functionalities of a system into layers so that they do not interfere with each other and are more manageable. These layers allow us to make the internet more scalable and affordable, since not all layers are needed everywhere in the internet (the network core mostly has lower layers till network layer) . TCP/IP model has following 4 layers -

Application Layer - This is where the Network Applications work

Transport Layer - This Layer ensures process to process communication between two systems

Network Layer - This is where source and destination IP are set. This Layer handles all the routing and addressing info.

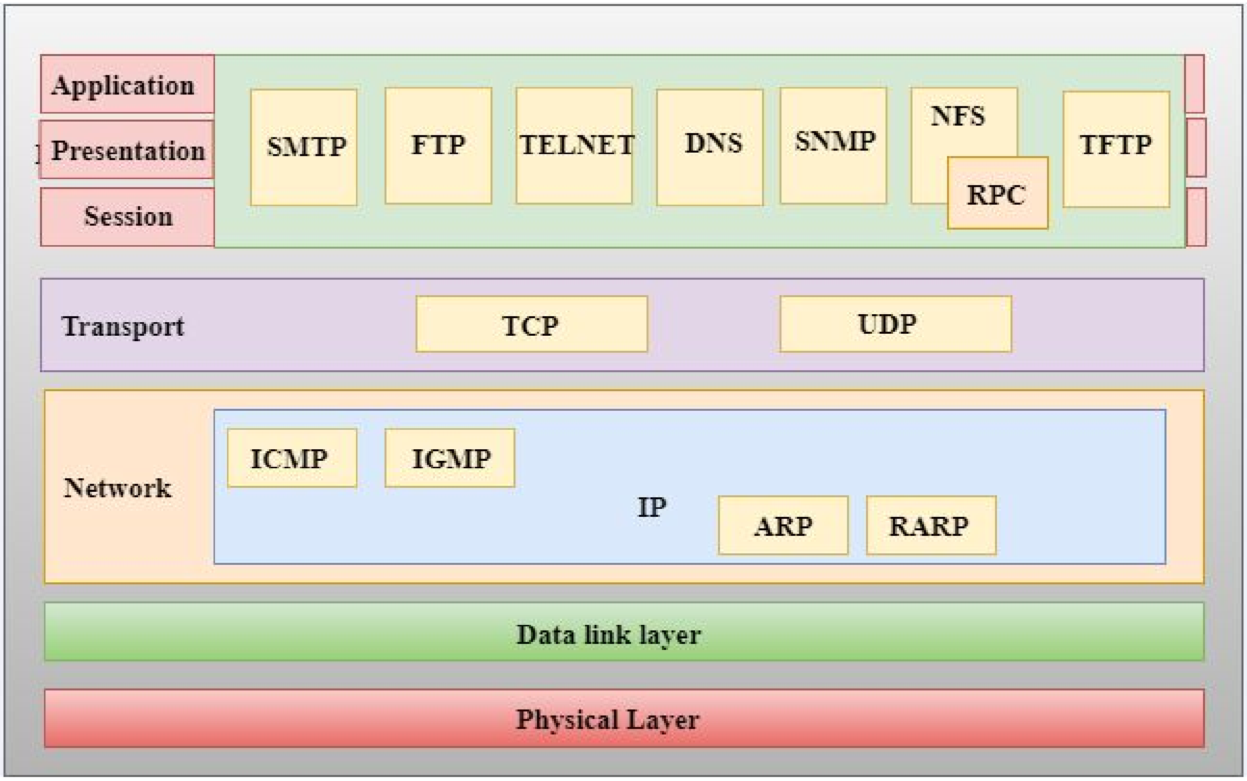
Physical Layer - This Layer is responsible for converting this binary data (frames) into a transmittable signal and vice versa, which is propagated to some remote system through a medium such as Ethernet Cables.



3. What is the OSI model?

The OSI Model is an extended version of TCP/IP model but TCP/IP model is more widely used(due to the Internet). This model has 3 extra layers for modularity, security and segmentation(There were many reasons for creation of the OSI model including communication between networks-primary). These 3 layers are Presentation, Session and DataLink, where the first two lie between Application and Transport Layer, the Data Link layer is present between Network and Physical Layer. It works similar to TCP/IP model with a few differences such as the

MAC and checksums are handled at the Data Link Layer in the OSI model.



4. What is a gateway and what is its role in networking?

Gateways lets us communicate with systems outside of our LAN Network. They are connected to other gateways or routers to send packets to a remote destination(outside LAN). It's one of the most important security checkpoints for a network. It can be used for monitoring traffic and Firewalls can be installed on it.

5. What is an IP address, a subnet mask, and a gateway IP address?

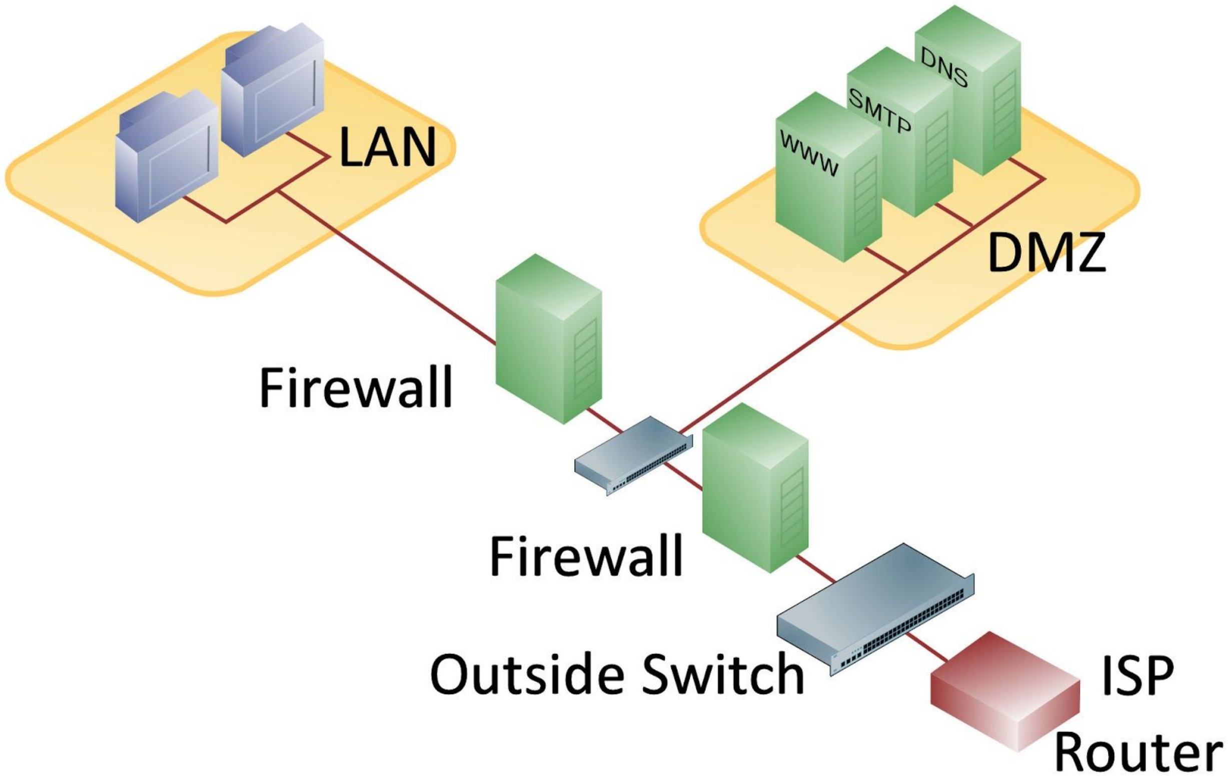
An IP address is just like a home address which is used to uniquely identify each device on the internet.
A Subnet Mask limits the number of systems that can be part of a LAN. It's like a block with several houses with a limit of 10 houses per block, where block signifies LAN, houses signifies IP addresses and 10 signifies the boundary set by the Subnet Mask.
A Gateway IP address is of a device, where packets coming from and going to a destination system outside of the LAN have to pass through. It's like a bottleneck, but it also acts as a checkpoint for all the outside traffic in and out of LAN. There can be multiple gateways for a LAN, connecting to different networks.

6. What is the difference between a local area network and a wide area network? What is a DMZ?

A Local Area Network or LAN is a small network of devices that are connected to each other either directly or through a switch like device. Basically it’s a network independent of other networks which can be without a gateway and can exist in isolation from the outside networks(internet).

WAN or Wide Area Network is a network or LANs connected through routers and gateways.

A DMZ or Demilitarized Zone is a perimeter or screen subnet which means that it exposes the services requiring more exposure to external resources to the outside network(internet) , adding additional security to LAN by restricting traffic in and out of LAN through Firewalls(assuming you are using firewalls otherwise no use of it) and only exposing the services in DMZ to be accessed through the web(internet).



7. What is least privilege in network security?

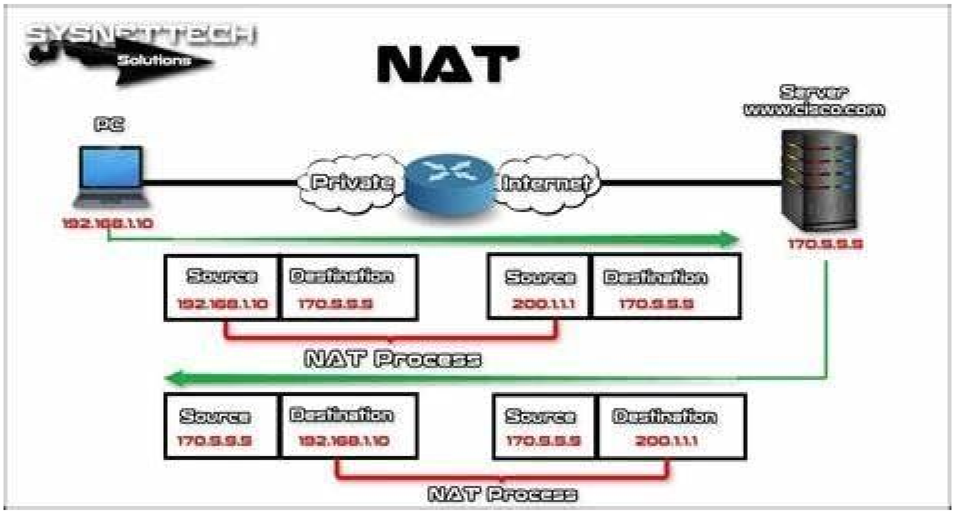
Least Privilege in Network Security means that firewall rules should allow only minimum access required for a service. In other words, only the permission that is required must be granted.

8. What is segmentation in networking/network security?

Segmentation is the most important concept in Network Security. The main idea is to divide a network based on different criterias such as type of service, functionality, area, etc , so that only a limited number of devices on a network (within a segment) can broadcast and connect to each other. This allows to add additional layers of indirection and firewalls which will help improve security of the network.

9. What is a home router and what does it do?

Most home Routers work as a NAT (Network Address Translation) Firewall. NAT allows a router to act as a single point of contact between the internet and a private network. Home routers usually provide a combination of services such as Gateway, NAT, DHCP, DNS, Firewall, WAP, etc. Home Routers are connected to ISPs (Internet Service Provider) WAN which are further connected to provide interconnectivity between different regions.
Home Routers using NAT provide a layer of security by hiding the local IP addresses from the outside networks and handling each request individually, so that it's hard to identify a separate entity within a home network from outside networks(internet).



References

Main Source - Lecture Slides
Some googling for understanding (for example DMZ)
My ideas may be influenced by the book ***Computer Networking - A Top Down Approach***, but I didn't use it for the assignment.

Lecture Summary- What I learned

We learned about how the internet works, and how it's governed by protocols to send information across the internet in the form of small manageable pieces called packets.

We got to know about the history of the internet and how it has evolved from a small institutional network into a large network of networks which from a bird eye's view may look like a neuron map(which is amazing if you let it sync in for a second.

We learned about different layering models (TCP/IP and OSI) used to manage functionality, access, security, costs, robustness and reliability of networks and end points on the networks. We learned that the TCP version is sort of a more generalized version of the OSI model.

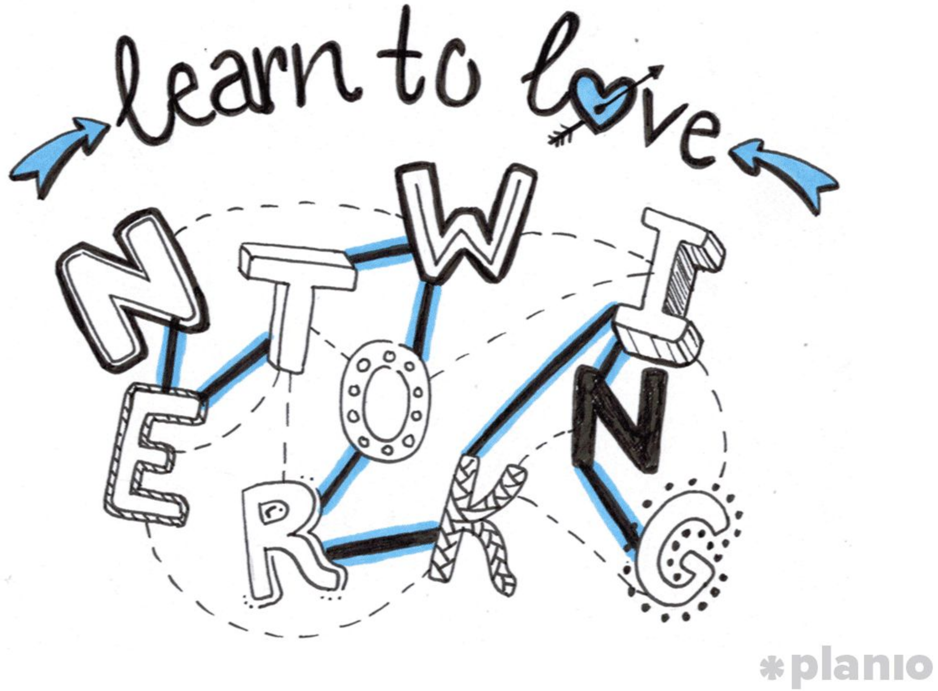
We learned the operation and working of different protocols in different layers and the data flow and encapsulation they perform.

We learned about the importance of port numbers and IP addresses in packet routing similar to postal service.

We learned about concepts like network segmentation and least privilege and how network layers work without interfering with each other.
We learned about different types of networks and different technologies used for them with many variations.

We learned about home routers and how they protect our security as well as provide us services we need.

To conclude, there was a lot covered in this lecture like how gateways work, how local machines are identified, how DHCP works, and how protocols like ARP, TCP, UDP, IP, etc work with practical examples and demonstrations. It left us with a lot of topics we can explore and work upon.


learn to love
NETWORKING
planio