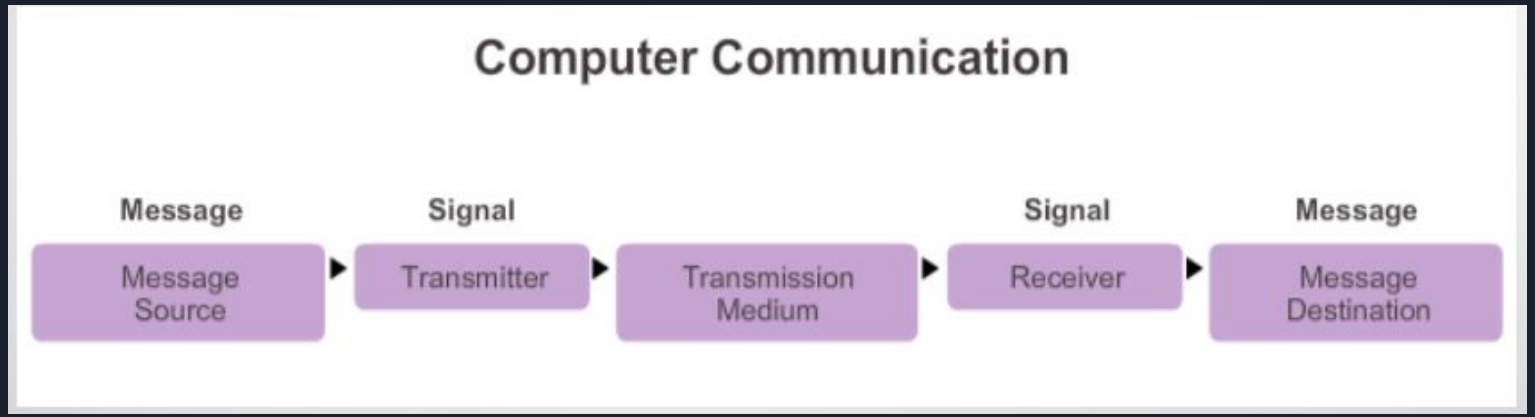
Networking

By: Dewan Islam

What is Networking?

- Networking is the connection between two or more devices
- This connection involves the sending and receiving of data between the two devices which is how they communicate between each other
-



The Internet

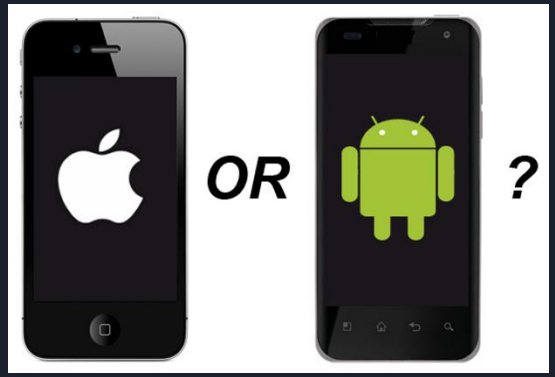
- The Internet is governed by a series of protocols that together form the laws for communication between devices.
- The Internet is essentially a vast network that is made of of billions of other networks
- When devices communicate over the internet the information they are communicating with each other is sent from one section of the internet to another
- The information is broken down into smaller sizes to make for easier transport across the networks, these smaller pieces are known as “packets”

Servers

- A Server is a computer or program that can manage access to a centralized resource or service on a network
- A Servers purpose is to store information and manage network resources
- Provide clients access to resources such as specific programs
- Servers can be used to run many different applications
- Many servers are known as dedicated servers because they are put in place to handle a certain server task
- A server can be setup to control access to a network such as sending and receiving emails, managing printing requests hosting a website
- Theres are several types of servers: File, SQL, Websites, AD, Virtualization

Clients / Endpoints

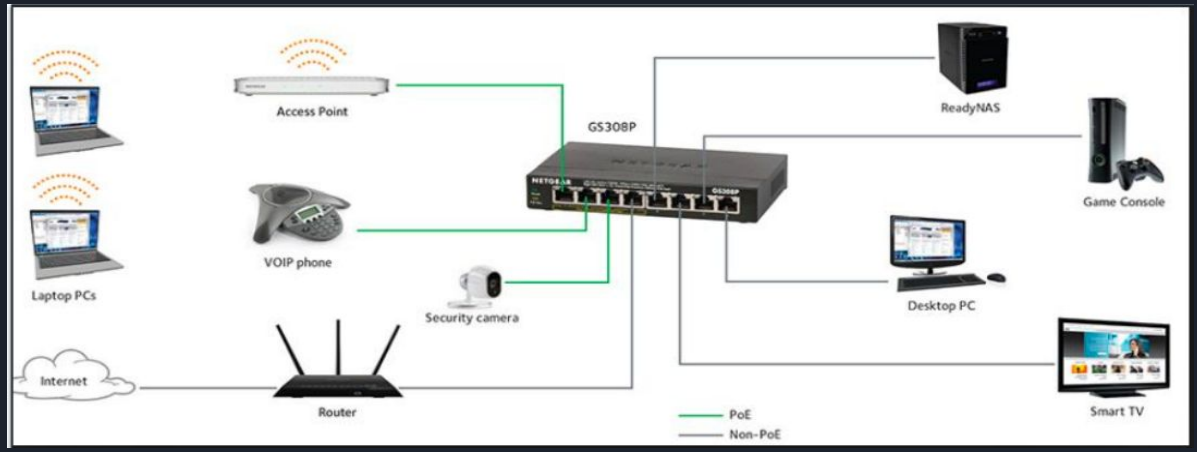
- A client can be a computer or program that sends requests to another program or hardware/software that can access services made available on a server
- Clients access servers for information and resources
- Example of clients can be: Smartphones, Tablets, PCs
- Ex: Web browsers (Chrome/ Firefox) are clients that connect to Web Servers and retrieve Web Pages which are what is displayed back to you
- Ex: Email clients retrieve emails from Mail servers
- These clients are connected to a network (LAN / WAN)



Some Common Network Devices

Network Switches

- A Switch is a networking hardware device that is used to connect devices on a computer network
- There are two basic types of switches (Unmanaged or Managed)
  - Unmanaged: “Out the box, plug and play” Cannot be configured (home networks)
  - Managed: Can be configured and managed locally or remotely
- A switch uses packet switching to receive and forward data to the correct destination device



Routers

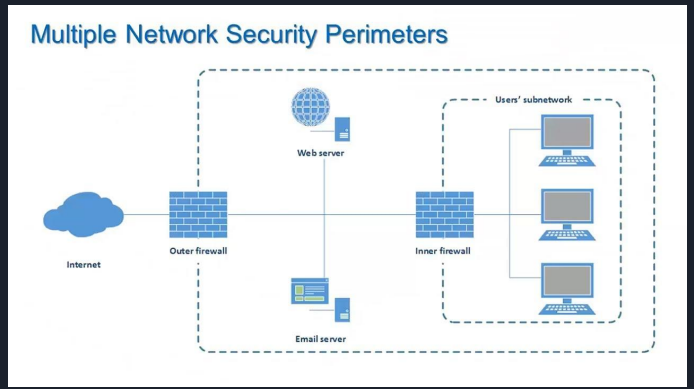
- Routers act as dispacters and are responsible for the sending and receiving of data (packets) to and from the Internet
    - Analyze traffic that needs to be sent across a network
    - Choose the best route for the packets to be sent
    - Sends the data
- Connect multiple networks together as well as connect the computers on the network to the Internet
- Routers allow all networked computers to share a single Internet connection which is great for saving money, especially at large organizations and companies that have hundred of different computers on the network
- Routes can have features such as firewall (a firewall that is on the router and a VPN (Virtual Private Network)

Wireless Access Points

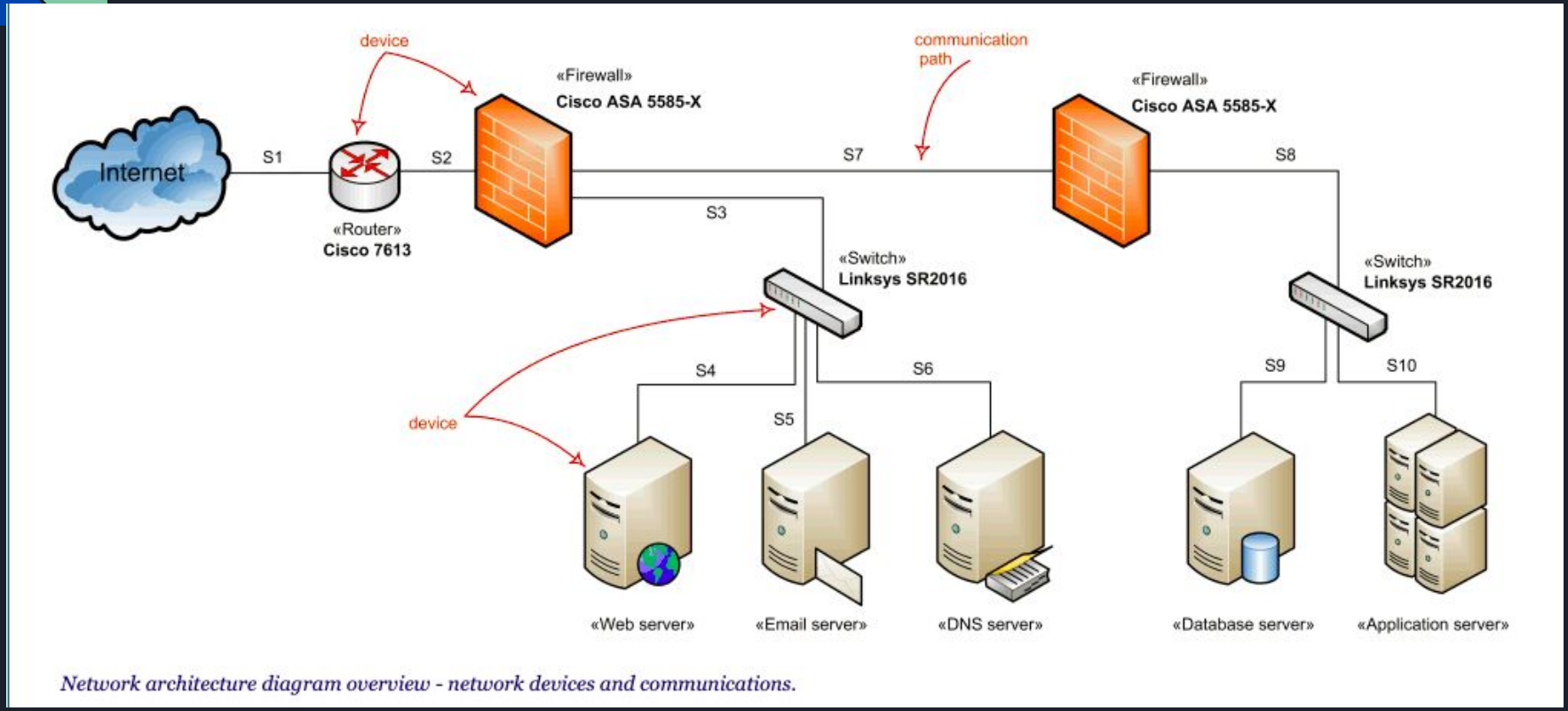
- Wireless Access Points involve Radio transmitter capable of connecting devices wirelessly
- Removes the need for wires
- Expands the bandwidth a router provides
- NOTE: Wireless Access Points are different from a router
    - A router sends data back and forth between two computer networks ex: LAN and the Internet
    - Wireless Access Points connect end user devices to the LAN
        - In a wireless network, routers and wireless access points play distinct but related roles

Firewalls

- Firewalls are used to secure traffic that is being sent out and restricts traffic that's coming into the network
- Only allow authorized traffic to pass through the network
- Can alarm users when there is suspicious or unusual behavior
- Firewalls CANNOT protect against internal threats (Ex: employees)
    - Also cannot protect against threats that are able to bypass firewalls
        - SSL / SSH are truster services that allow traffic to enter and leave without firewall involvement
        - Malicious software that was executed within an organization



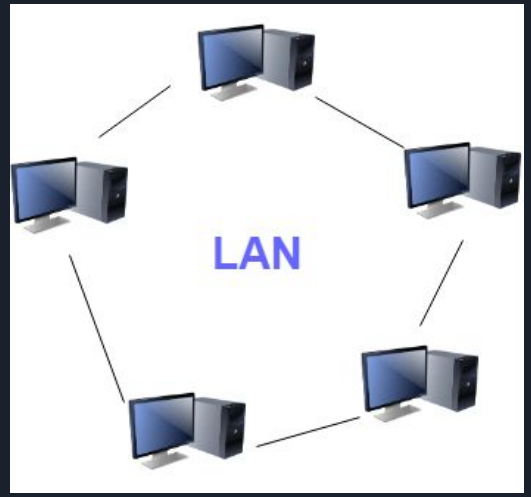
Network Diagram



Network architecture diagram overview - network devices and communications.

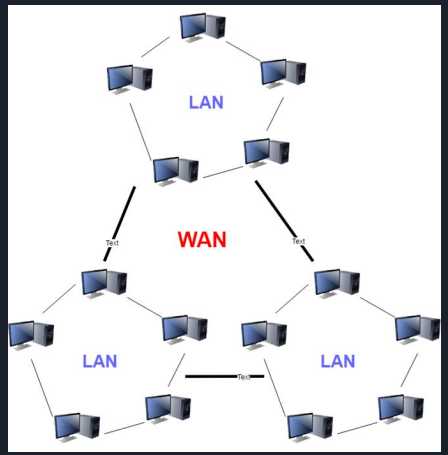
LAN

- Local Area Network
- LANs are the most basic type of network
- All devices on the same LAN communicate directly with one another across a switch
- These small basic networks are the building blocks of the internet
- Network and LAN segmentation is a fundamental security concept
- LANs are organized by
  - geographic area device type
  - administrative boundary



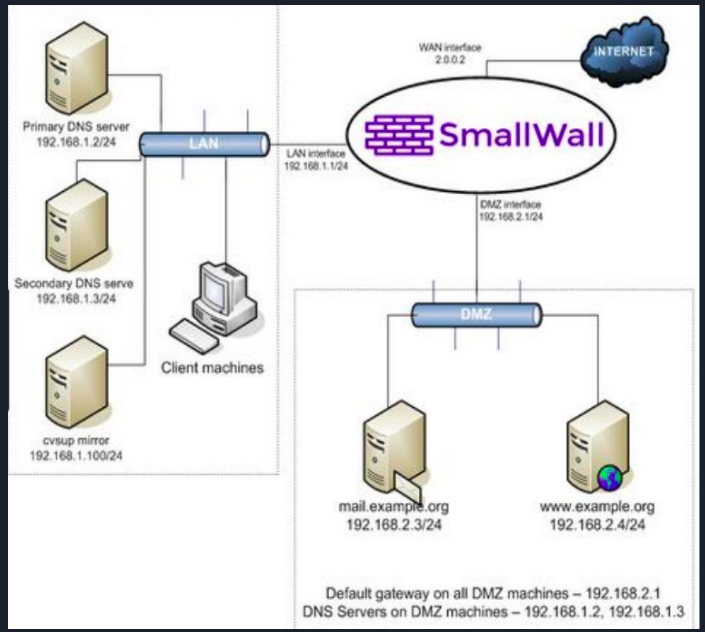
WAN

- Wide Area Network
- WANs consist of LANs that are all connected together
- WANs can span much larger geographic distances than LANs
    - The internet is actually an example of a WAN
- These LANs are connected together through the use of routers
- LANs and WANs can be connected together through wired and wireless connections

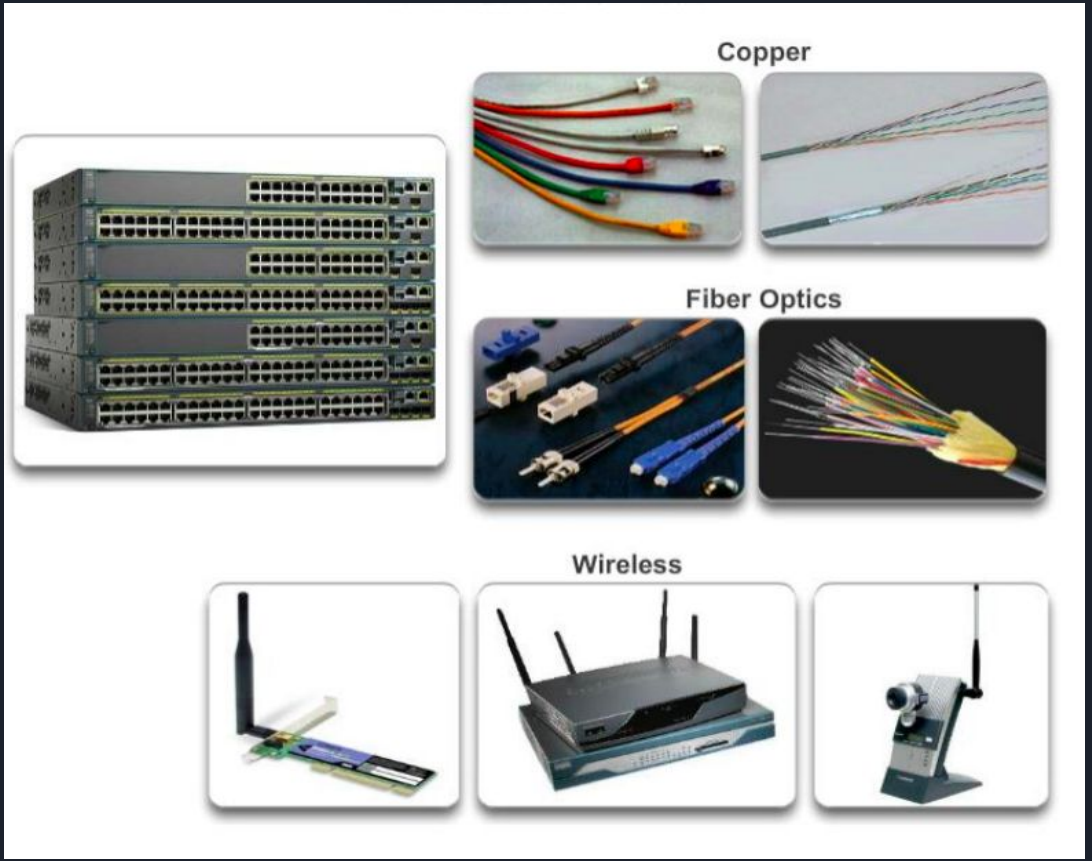


DMZ

- Demilitarized Zone (DMZ)
- Is a physical or logical sub-network that separates an internal LAN (Local Area Network)
- DMZ consists of
  - External facing servers
  - Resources and services can be located in the DMZ (this allows them to be accessible from the internet but the rest of the LAN remains inaccessible)
  - Provides an extra layer of security to the network by restricting the ability of malicious programs to directly access internal servers and data via the internet)

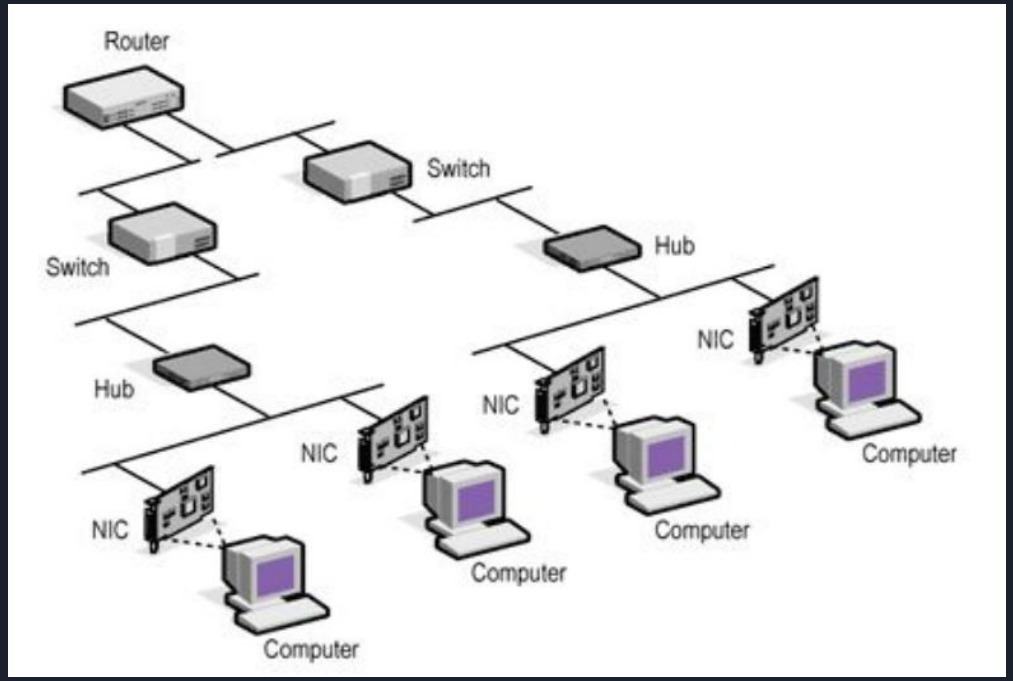


Interfaces and Ports



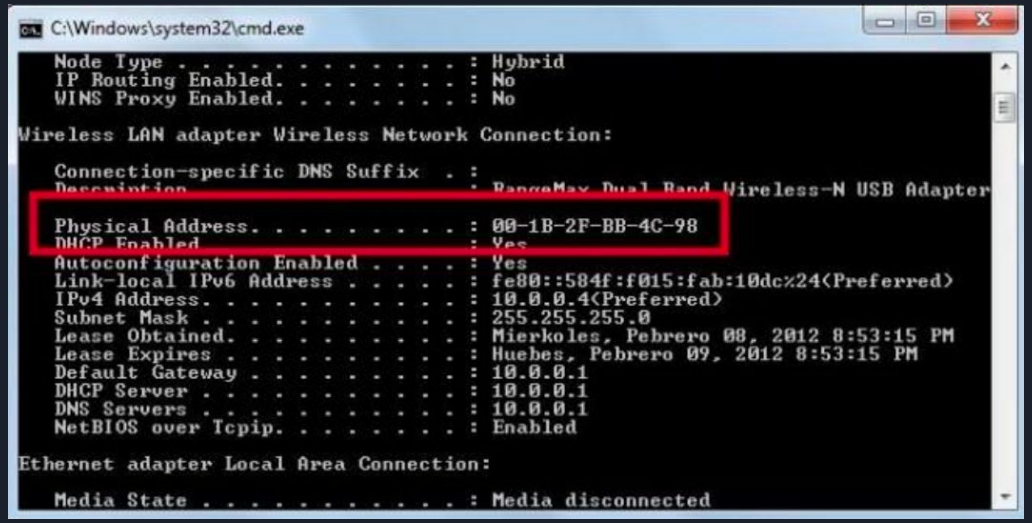
Network Interface Cards (NIC)

- Computers speak with each other through the use of NICs
- Just like how we use our mouth and ears to send and receive information
- The NIC acts as the computers mouth and ears



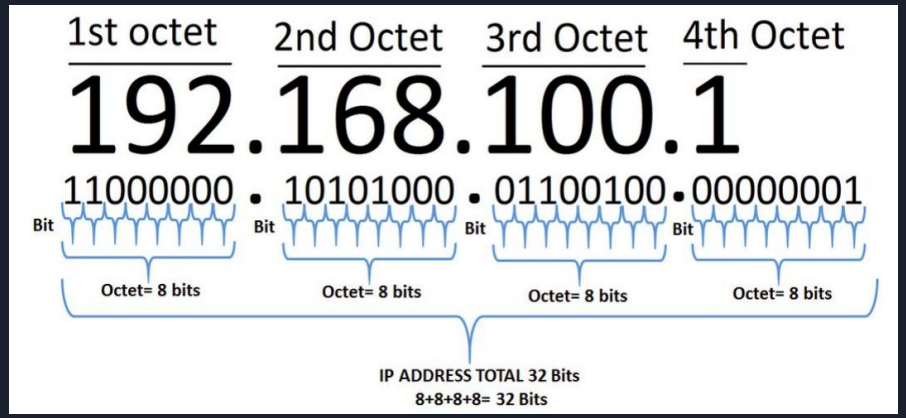
MAC Addresses

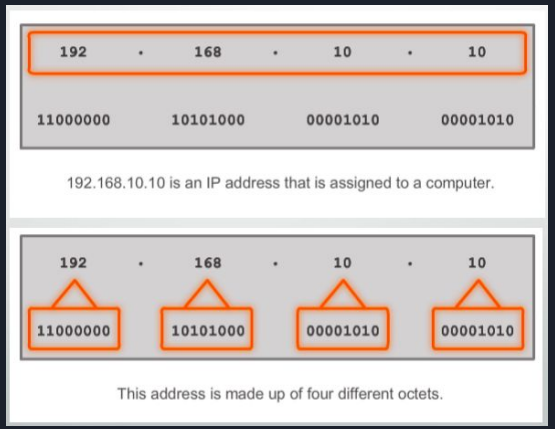
- Think of your computer's MAC Address as its name, just like how you have a unique name your computer does too
- MAC Addresses are hardcoded into a computers Network Interface Card (NIC)
- 48 bit Addresses
  - Made up of OUI (organizationally unique identifier)
  - And NIC Addresses
  - Layer 2 addresses used by switches
  - Insert pic of physical address



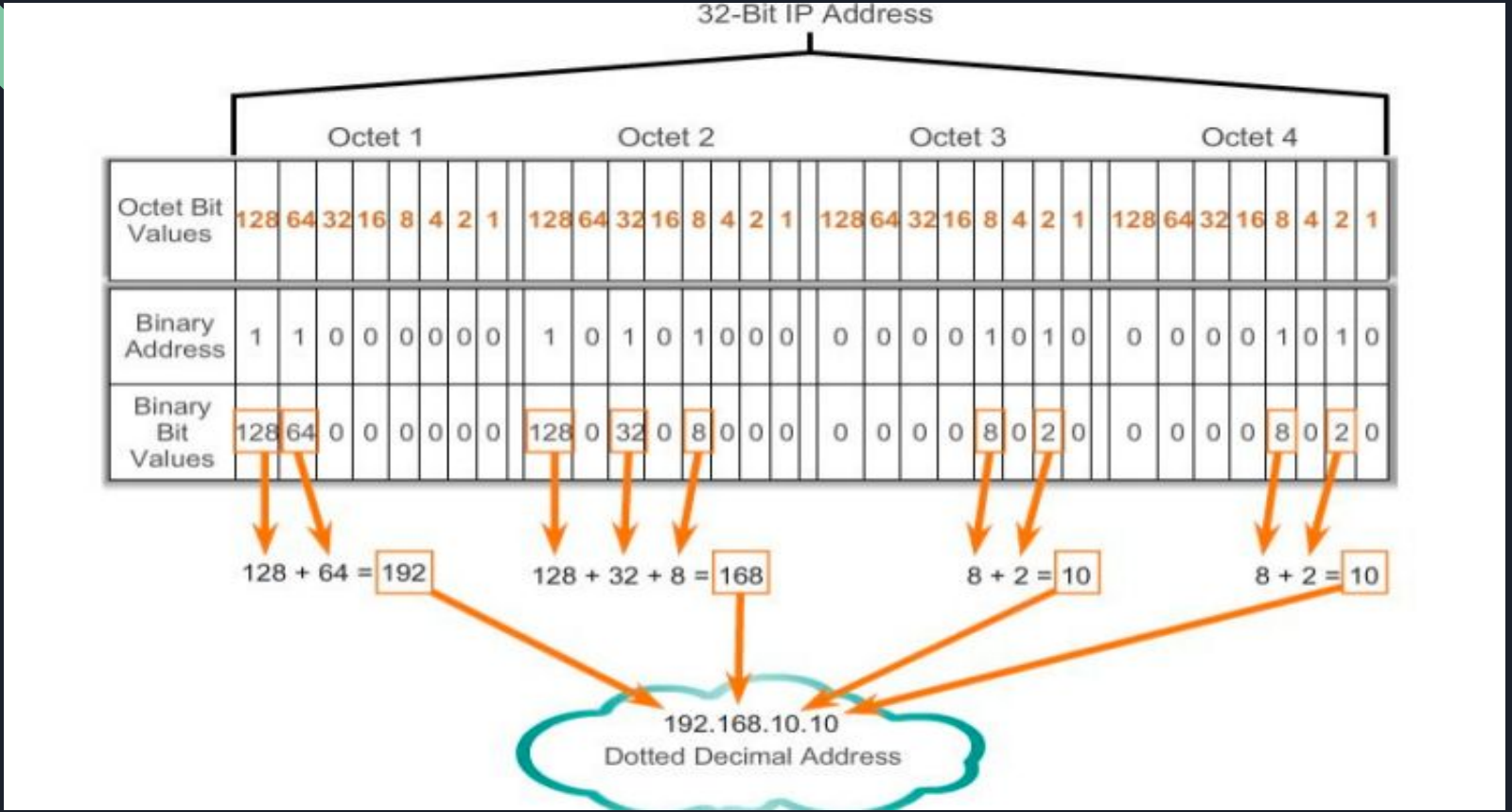
IP Addresses IPv4

- IP Addresses is the Internet Protocol Address
- Unique Identifier
  - String of numbers separated by periods (4 octets)
    - Ex: 192.168.10.10
- Uses Subnet mask which is used to specify your address v your neighborhood (Network Identified
  - 32 bit
  - Determines boundaries of LAN
- Subnet Mask determines which part of a large network is used by the IP address



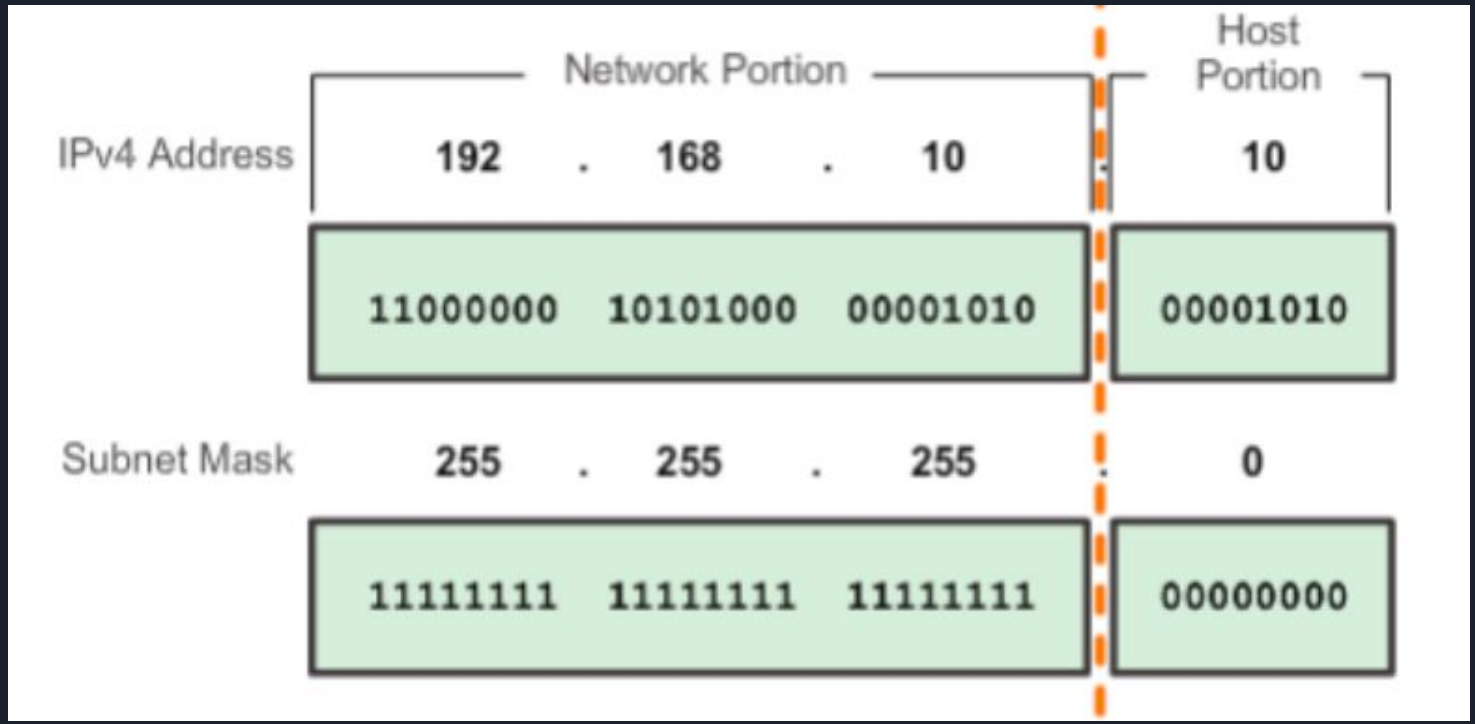


IP Address


32-Bit IP Address
Octet 1
Octet 2
Octet 3
Octet 4
Octet Bit Values
128 64 32 16 8 4 2 1
Binary Address
1 1 0 0 0 0 0 0
1 0 1 0 1 0 0 0
0 0 0 0 1 0 1 0
0 0 0 0 1 0 1 0
Binary Bit Values
128 64 0 0 0 0 0 0
128 0 32 0 8 0 0 0
0 0 0 0 8 0 2 0
0 0 0 0 8 0 2 0
128 + 64 = 192
128 + 32 + 8 = 168
8 + 2 = 10
8 + 2 = 10
192.168.10.10
Dotted Decimal Address

Subnet Masks

- Subnet Mask determines which part of a large network is used by the IP address



Ports (Logical, not Physical)

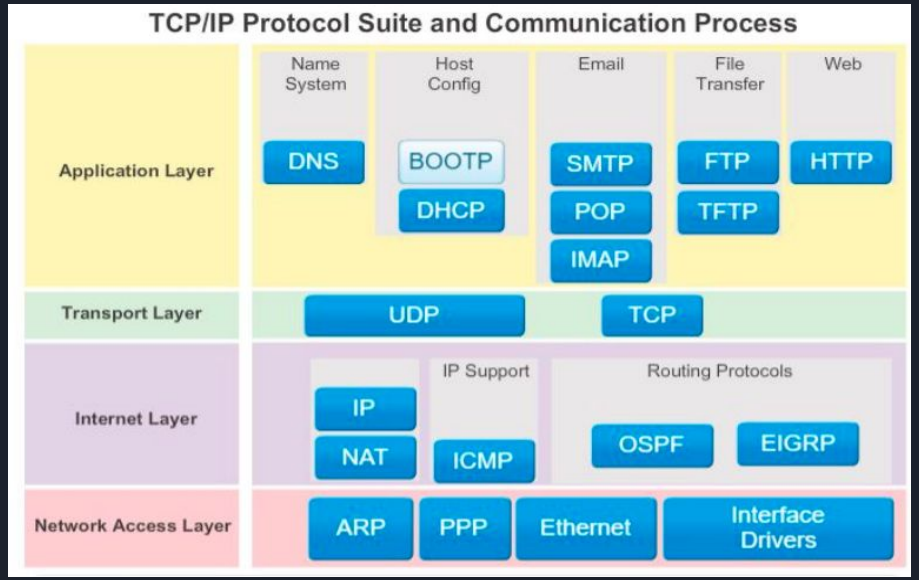
- Ports are associated with a protocol type, used fo connections along with IP addresses
- Common ports
    - HTTPS: 443
    - HTTP: 80, 8080
    - FTP: 21
    - SSH: 22
    - DNS: 53
- The well-known ports: 0 - 1023
- Registered ports: 1024 - 49151
    - Assigned by IANA Internet Assigned Numbers Authority, American non profit responsible for global IP address allocation
- Dynamic ports: 49152 - 65535
    - Contain either dynamic or private ports that cannot be registered with IANA

Domain Name Systems (DNS)

- The DNS translates an IP Address to a name
  - Ex: 8.8.8.8 translates to google.com
  - 128.205.201.57 to buffalo.edu
- DNS was created to help us from having to remember numbers
- Things are easy for us because we just need to remember the name of the website as opposed to the string of numbers associated with the IP address

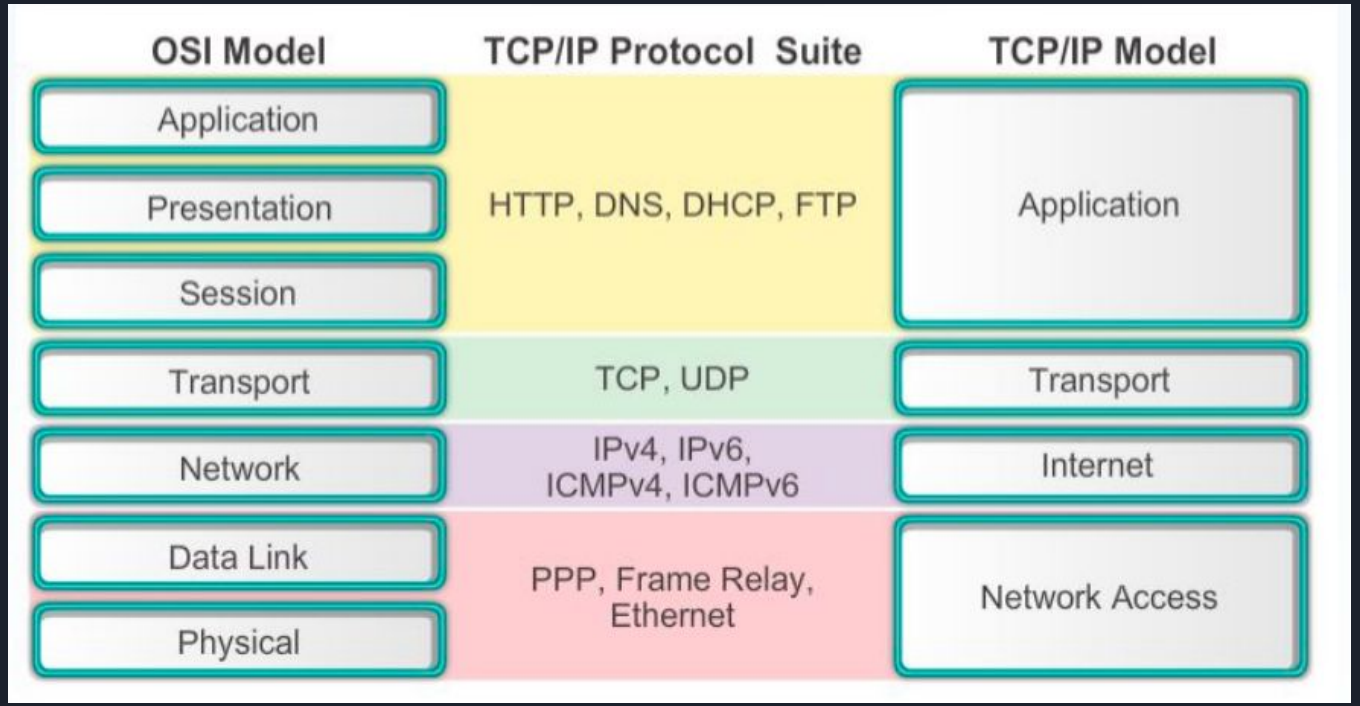
TCP/IP

- Transmission Control Protocol / Internet Protocol
- Is a suite of protocols that are used to interconnect network devices on the internet
  - Specifies how data is transferred over the internet
    - How its is broken into packets
    - How it is addressed
    - How it's going to be transmitted
    - How it will be routed
    - How it will be received



OSI Model

- Open Systems Interconnection Model
- Used for data network design, operation specifications and troubleshooting
- More advanced than the TCP/IP Model
- 7 layers as opposed to 4 on TCP/IP

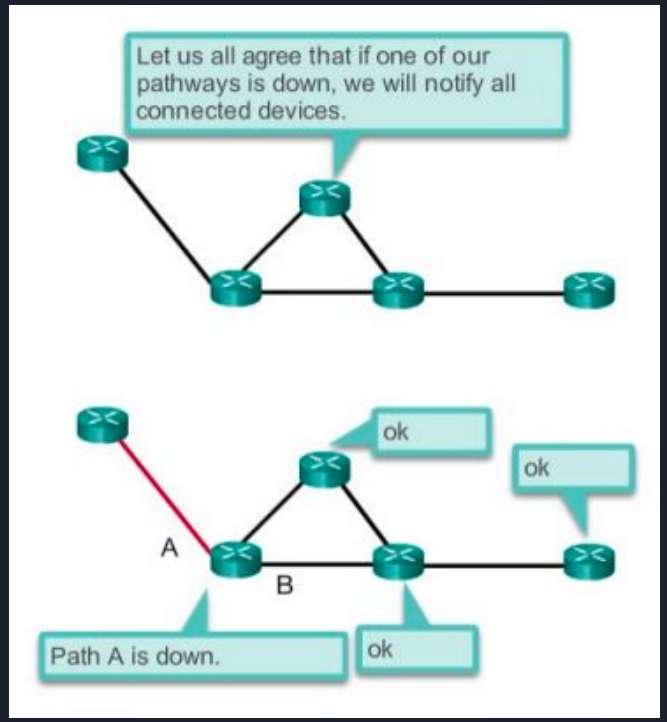


Transport Layer

- TCP v.s UDP
- TCP (Transmission Control Protocol)
  - Reliable
  - Connection oriented
  - 3 way handshake (SYS, SYN-ACK, ACK)
  - Best for applications that require high reliability but not time sensitive
  - Packets get organized in order specified, guaranteed data transfer in correct order
- UDP (User Datagram Protocol)
  - Not reliable
  - Connectionless, relationship between programs ends after packets are sent
  - Best for applications that require fast, efficient transmission
    - Ex: streaming, gaming
  - Packets are all independent of each other so there is no order, ordering can be managed by the application layer if needed
    - No guarantee that packets sent will be received

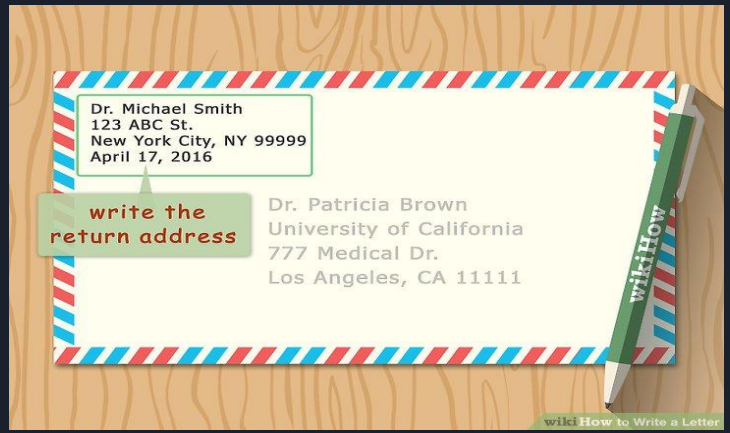
Network Protocols

- Routers use these protocols to communicate with each other
  - Rend messages to each other
  - Establish communication
  - Establish routing tables
- Examples:
  - BGP: Border Gateway Protocol
  - RIP (Kobe): Routing Information Protocol
  - EIGRP: Enhanced Interior Gateway Routing Protocol
  - OSPF: Open Shortness Path First
  -



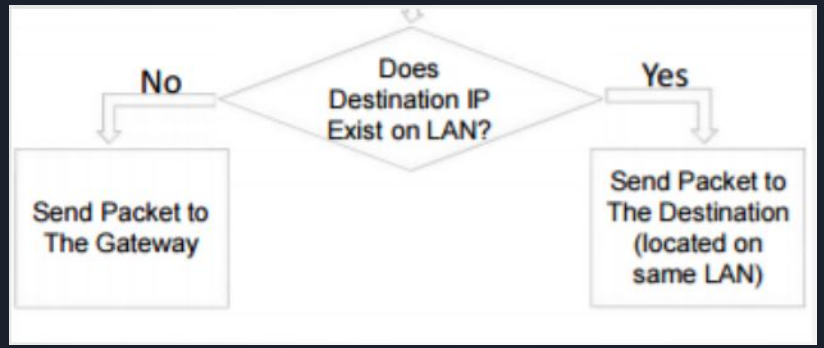
Packets

- IP Packets
  - Contain two IP addresses
    - Source IP Address: IP of the sending device
    - Destination IP Address: IP address of the receiving device
      - Used by routers to forward packets to correct destination
- IP Packets also contain
  - Source MAC Address: your MAC address
  - Destination MAC Address
- Frame Check Sequence (FCS)
  - Checks for errors to make sure ones with errors are dropped before reaching destination IP



Flow of Data and Packets

- IP Layer determines the location of the client you are sending packets to
  - Determines the location through the use of the
    - Clients IP address
    - Clients subnet mask
    - Destination IP address
- LAN traffic is handled through the use of switches (layer 2 devices)
  - Handled through MAC Addresses
- Address Resolution Protocol (ARP) request
  - What IP does to what MAC address
    - Is it in the ARP table?
      - No? Ok, forward to router or default gateway



DHCP v Static Addressing

- Static
  - Assign each address manually
  - IP Address will not change
    - Great for printers, IP phones
- DHCP
  - Prefered method for IPv4 assignments to host on large networks
    - Reduces burden of network staff and basically eliminates entry errors
  - Dynamically assigned address throughout the network
    - Usually requires a DHCP server and client

IPv6

- 6 > 4 right?
- IPv6 was created to replace IPv4 as the name hints
- This was due to no more IPv4 address left to give out
- 8 * 16 bit (128 bit) alphanumeric address in decimal notation separated by .
    - Ex: 2001:0000:3238:DEF1:63:0000:0000:FEFB - IPv6

Public Addresses v. Private Addresses

- Public Address
  - Used for intranet communication
- Private Address
  - Mainly home networks or company networks
- UB is actually Public Addressed
- Ex:
  - Visiting a friend and you connect to their wifi network
    - If you run ‘ipconfig’ in command line you will get the IP similar to
      - 192.168.1.x
    - This is a private address

Commands

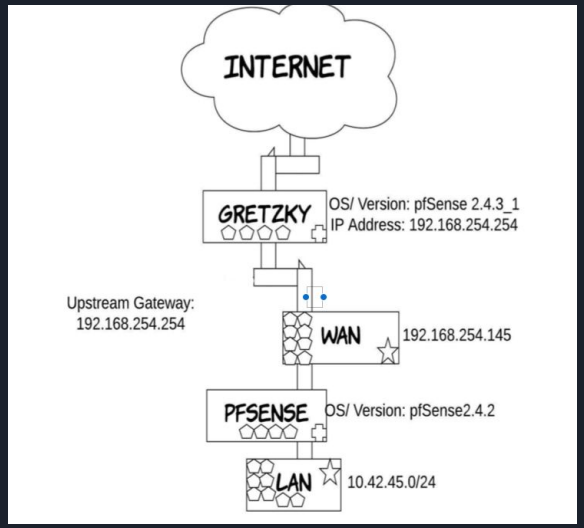
Some common commands you will be needing for homework(s) to test connections

- ping : check your network connection
  - NOTE: Many things can block your ping
- ipconfig : shows generic IP addressing information on Windows machines
- ipconfig /all : shows in depth information for all network adapters on Windows
- tracert : shows hops to a destination
- nslookup : displays DNS server information
- ifconfig : shows generic IP addressing information on Linux machines
- netstat : displays active connections
- nmap : port scanner
-
  - Some helpful linux commands: https://maker.pro/linux/tutorial/basic-linux-commands-for-beginners
  - Some helpful Windows commands: https://www.digitalcitizen.life/command-prompt-how-use-basic-commands

Topologies

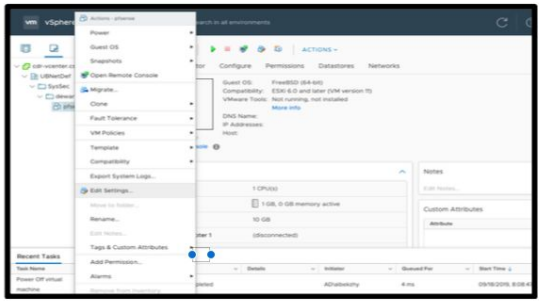
- IMPORTANT FOR ALL HOMEWORKS GOING FORWARD

- Topologies are diagrams of your network that contain information specific to each device and connection on a network
- Most places you may end up working have many Topologies
- We will be using LucidChart for your homeworks this semester
  - www.lucidchart.com



Runbooks

- Step by step instructions on how to install and configure
- As if you are teaching someone with little to no experience in the topic
- Required for your first homework, due NEXT FRIDAY



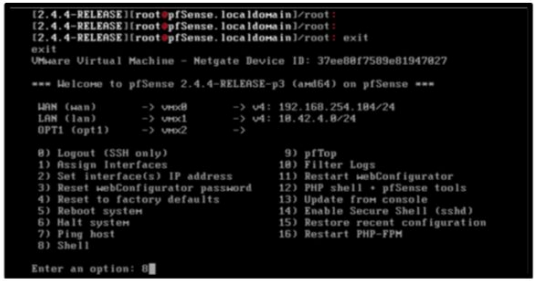
- Click on CD/DVD drive 1 and click on ‘Datastore ISO file’
- Click on cdr-iscsi1
- Choose ISOs
- Select pfSense
- Choose latest avaliable file
- Select the box for ‘client’
- Hit OK
- This will setup pfSense for you

STEP2: Install pfSense.

- Launch web console in Vsphere for pfsense
- Select ‘Install pfSense’

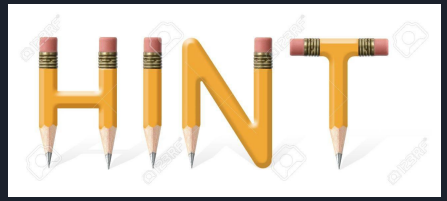
STEP6: Test Functionality.

- You can test the functionality of the IP addresses you configured by pinging Google
- Choose option 8 in the pfSense Home Page menu for Shell



- Should bring you to the command prompt
- Type ‘ping 8.8.8.8’ that will call out to Google, this tests the connection to the Internet through the IPs that you setup.

Homework



- This weeks hw is on pfSense
  - pfSense is an open source firewall and router
  - For this hw you will install and configure the router with the pfSense operating system
  - You will also install and configure the client machine with a Linux operating system
- Steps that should be outlined in your first homework
  - Log into vSphere with your assigned account
  - Load ISO image to the VM
  - Install pfSense
  - Assign interfaces in pfSense (LAN, WAN, DMZ)
  - Configure LAN
  - Configure WAN
  - Configure DMZ
  - Test functionality (Refer back to Commands slide for help)
  - REMEMBER TO INCLUDE SCREENSHOT FOR ALL STEPS
  - Map out the Networks Topology as it sits after completing pfsense installation and configuration

Mattermost