

Networking

By Destiney Plaza



Overview

- **What is networking**
- **Architecture**
- **Hardware**
- **Networking Details**
- **Topologies**
- **Build your own network**

Networking

- Connection between two or more devices
- How do humans communicate?
 - Mailing letters
- Devices send letters too!



What devices can connect to a network?

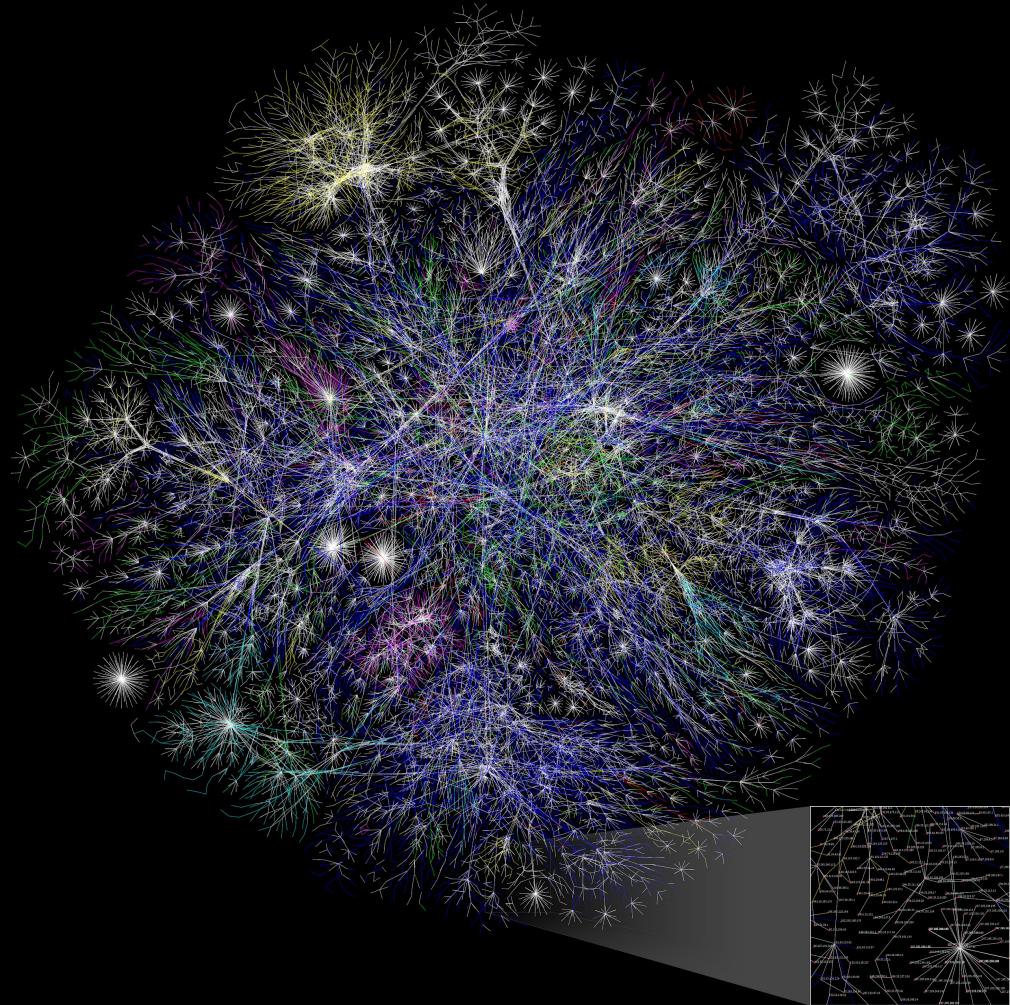
- Computers, mobile phones, peripherals (mouse, webcam, microphone), and IoT devices



Internet

- Large network
 - Network composed of networks
- Governed by protocols
 - Rules for communication
- Information sent is broken down into chunks
 - Packets





Servers

Servers

- What are they?
 - servers store information and contain resources that clients can access
 - provides a service to users or specific programs
 - Can be used to run a variety of applications
- Types of servers:
 - File, SQL, Websites, Active Directory, Virtualization



Clients/End points

Clients/Endpoints

- What do they do?
 - Access servers for information and resources
- Device types:
 - Smartphones, tablets, PCs
- They are connected to a network
 - LAN and WAN
- Programs could be considered to be clients also



Common Network Devices

Common Network Devices

- Switches
- Routers
- Access Points
- Firewall Appliance

Switches

- “A switch acts as a controller, connecting computers, printers, and servers to a network in a building or a campus.(Cisco)”
- Two basic types of switches:
 - Unmanaged
 - “Out of the box” -typically this is your home network (cannot configure it)
 - Managed
 - Can be configured – can manage/adjust locally or remotely



Routers

- Act as a dispatcher
 - Analyze traffic sent across network → chooses best travel route → sends data
- Can come with features such as firewall or Virtual Private Network (VPN)

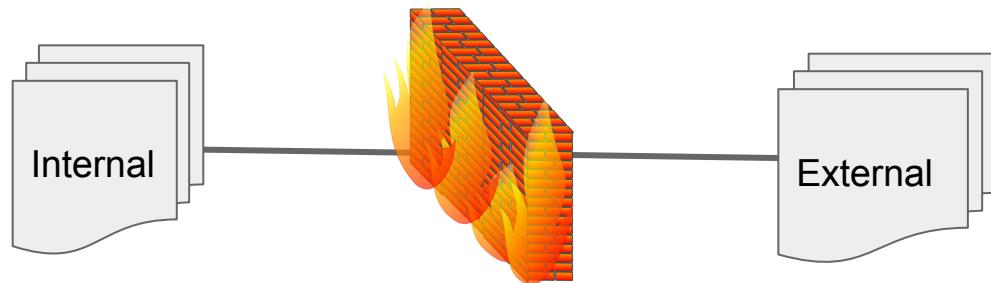


Access Points

- “Allows devices to connect to the wireless network without cables. A wireless network makes it easy to bring new devices online and provides flexible support to mobile workers. (Cisco)”
- Acts as an amplifier
 - Extends the bandwidth that a router provides

Firewall

- Allows only authorized traffic

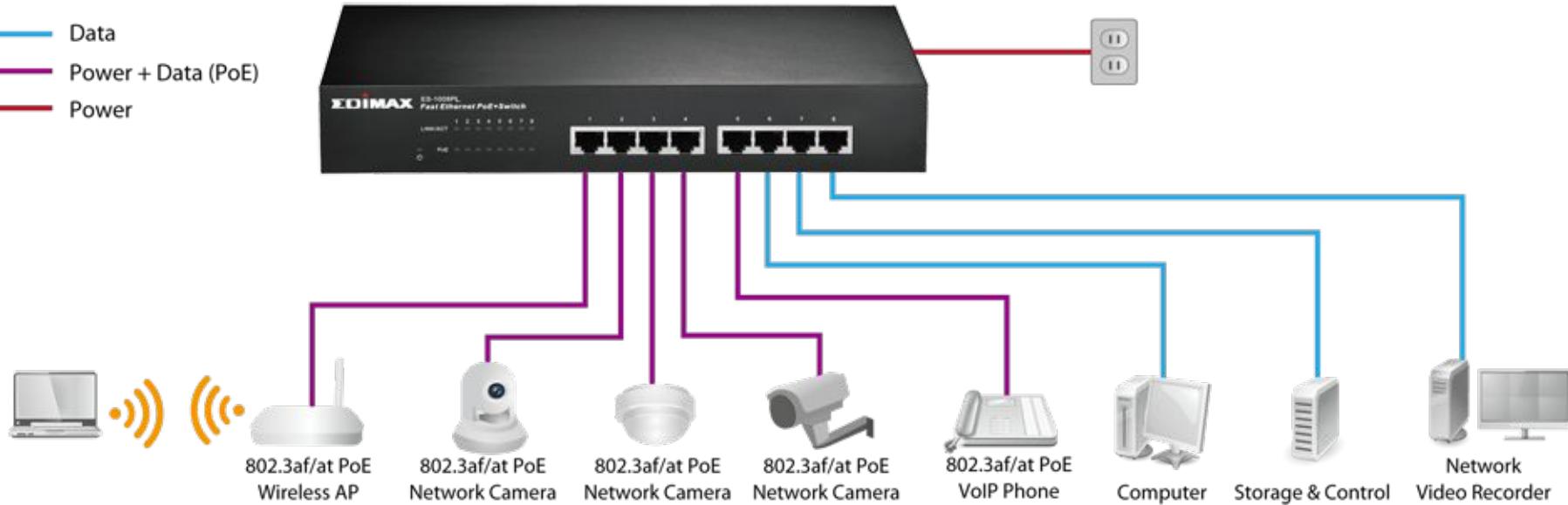


- Can alarm for unusual behavior

Firewalls - What They Cannot Do

- **Cannot** protect against **internal threats**
 - Disgruntled Employees
- **Cannot** protect against threats that are able to **bypass** it
 - Trusted services (SSL/SSH)
 - Malicious software executed within the organization

— Data
— Power + Data (PoE)
— Power



LAN

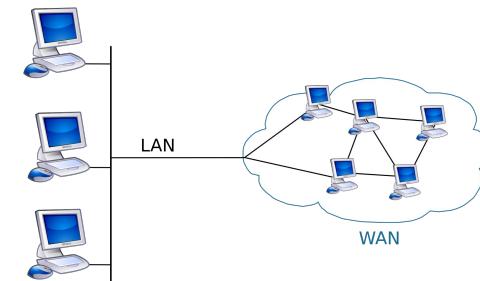
Local Area Network (LAN)

- Simplest type of network
- Viewed as “local neighborhood” of computer devices
- All devices on the same LAN communicate directly with one another across a “switch” (collision domain)
- FUNDAMENTAL SECURITY CONCEPT: network and LAN segmentation
 - Geographical area
 - Device function

WAN

Wide Area Network (WAN)

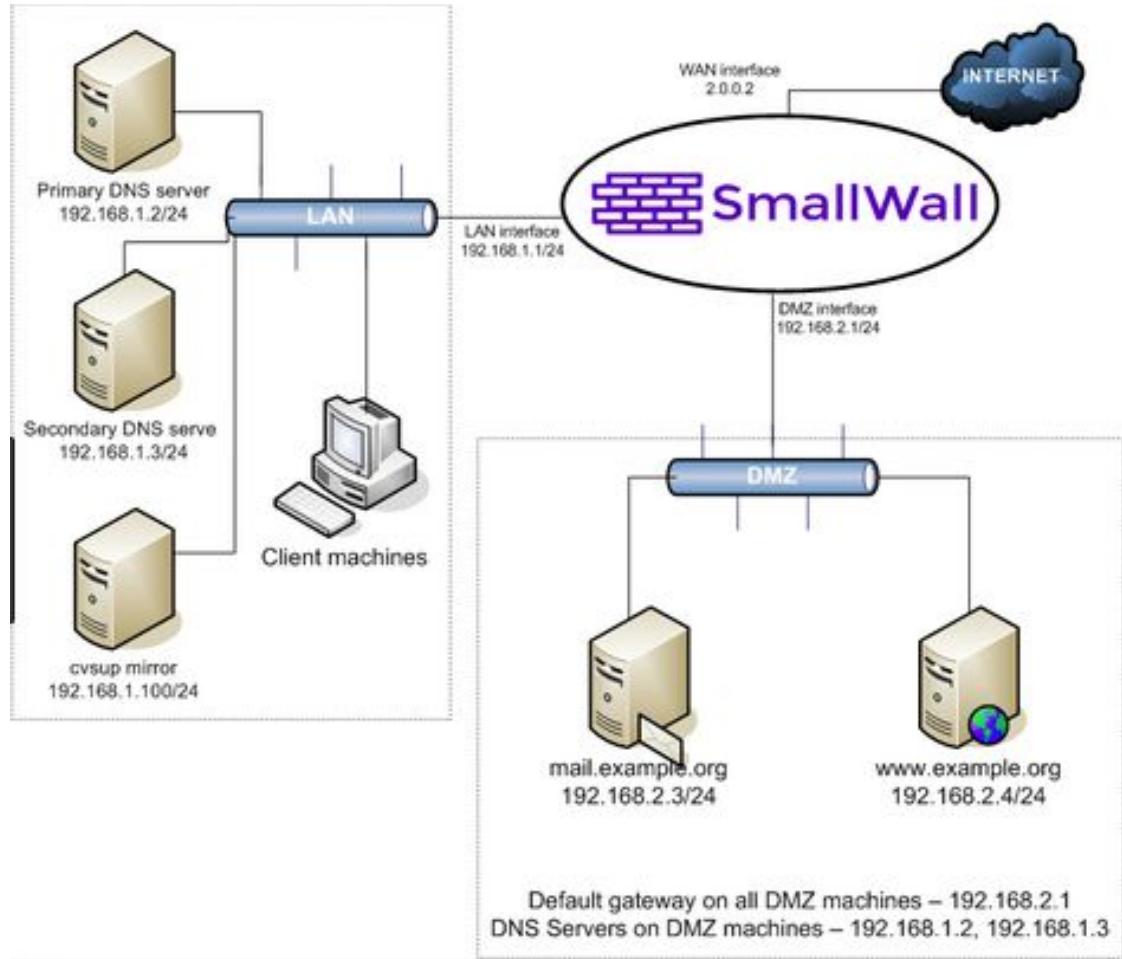
- Composed on LANs connected together
- What is a well known example of a WAN?
 - The internet
- LANs get connected to WANs through routers
 - We can connect LANs to WANs through both wireless and Wired Connections
- WANs can span much larger geographic distances than LANs



DMZ

Demilitarized Zone (DMZ)

- Sub-network
 - Physical or logical
 - Separates an internal local area network (LAN)
- What is in the DMZ?
 - External-facing servers, resources and services
 - they are accessible from the Internet but the rest of the internal LAN remains unreachable
- This provides an additional layer of security to the LAN as it restricts the ability of malicious actors to directly access internal servers and data via the Internet



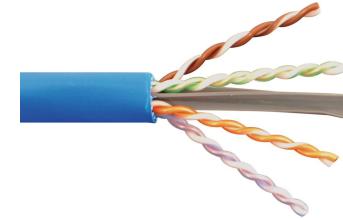
Interfaces and ports



Wireless



Copper



Fiber Optics

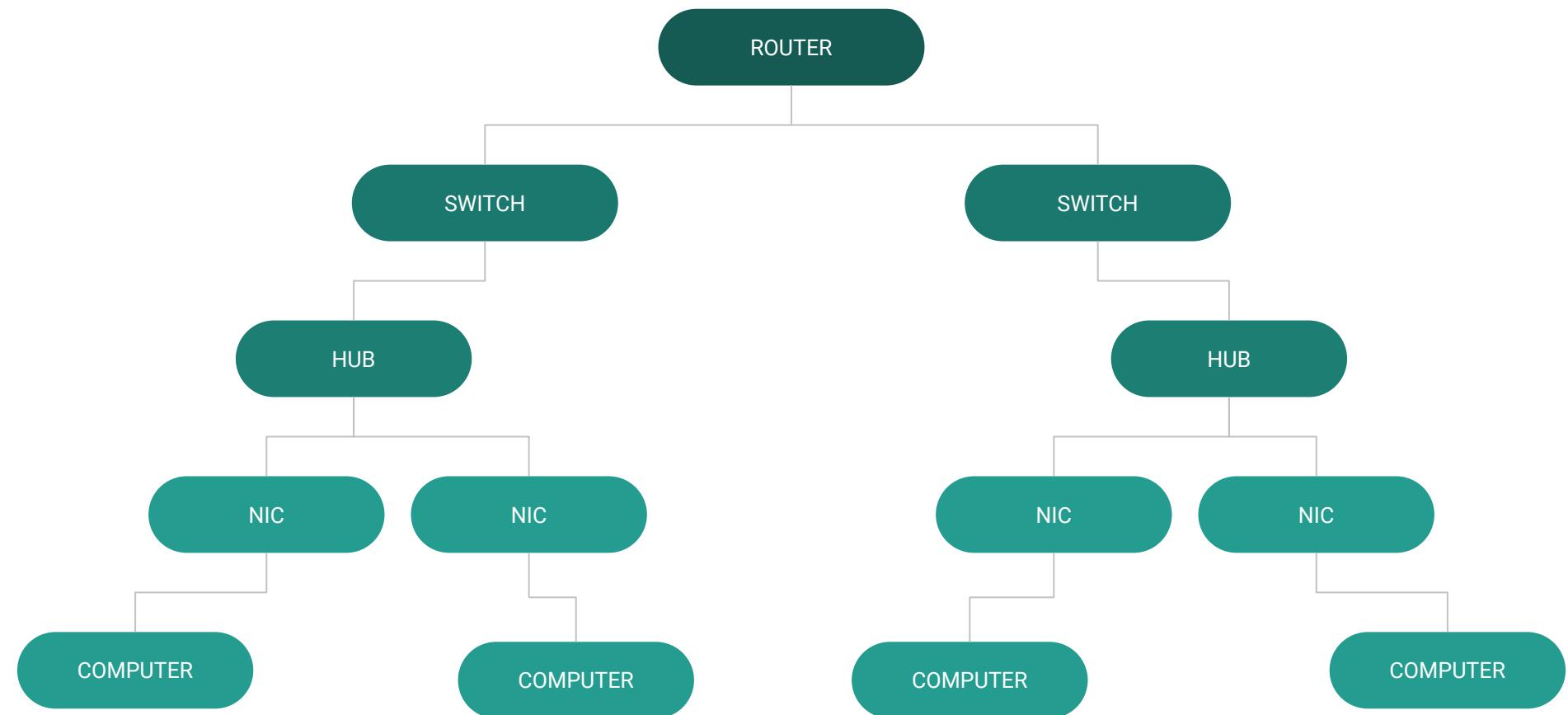


NIC

Network Interface Cards (NIC)

- This is the way computers are able to speak with one another
- Humans use their mouth and ears
- NIC act as “mouth and ear” of the computer
 - Mouth = transmit
 - Ear = receive





MAC

MAC Addresses

- Humans have names and so do computers!
- Hardcoded addresses into a computer's NIC
 - Network Interface Controller/Card
- 48-bit Address
 - made up of a Organizationally Unique Identifier (OUI) and NIC Addresses
 - layer 2 address used by switches

C:\Windows\system32\cmd.exe

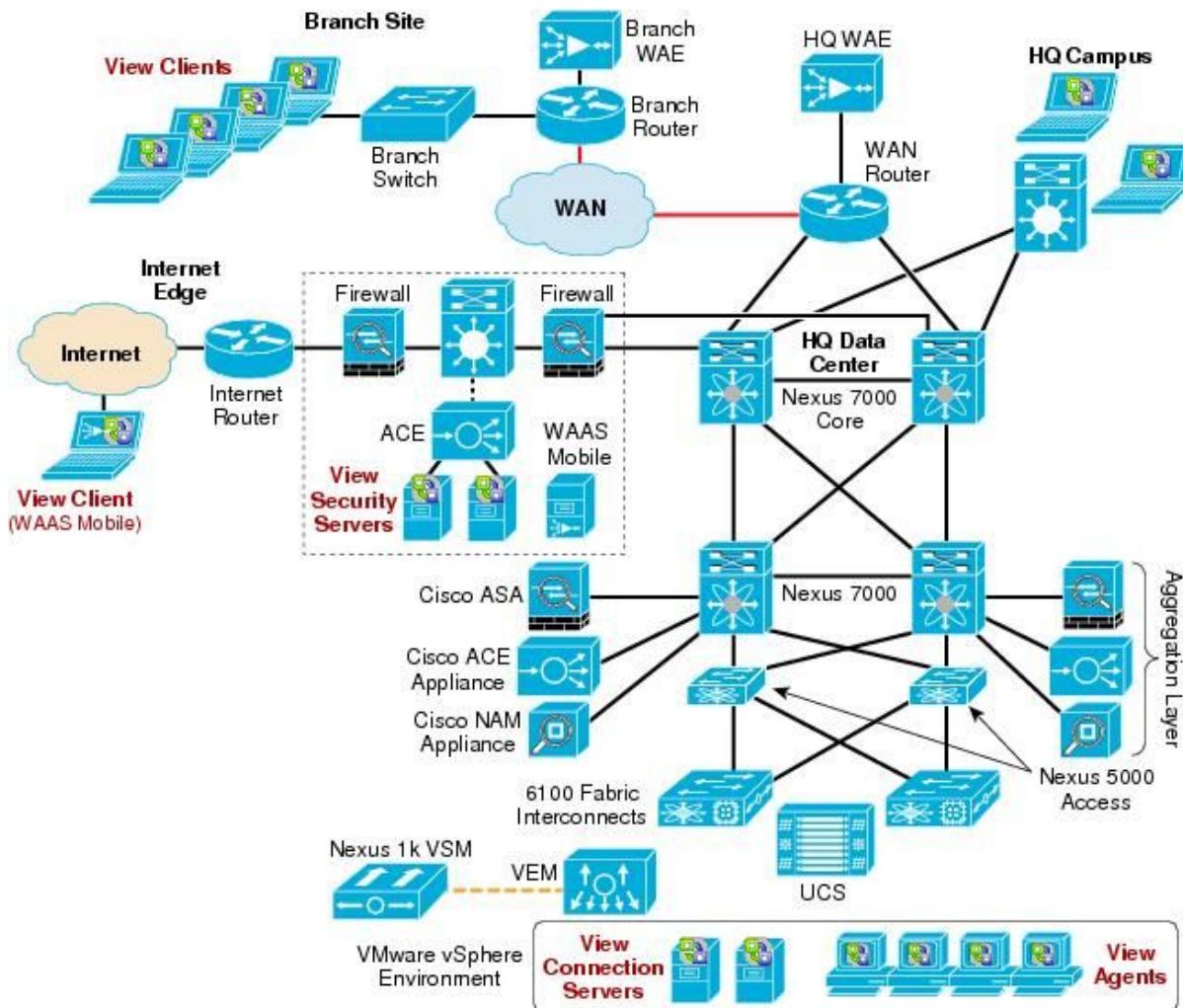
Node Type : Hybrid
IP Routing Enabled. : No
WINS Proxy Enabled. : No

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix
Description : RangeMax Dual Band Wireless-N USB Adapter
Physical Address. : 00-1B-2F-BB-4C-98
DHCP Enabled : Yes
Autoconfiguration Enabled : Yes
Link-local IPv6 Address : fe80::584f:f015:fab:10dc%24(PREFERRED)
IPv4 Address : 10.0.0.4(PREFERRED)
Subnet Mask : 255.255.255.0
Lease Obtained : Miércoles, Febrero 08, 2012 8:53:15 PM
Lease Expires : Jueves, Febrero 09, 2012 8:53:15 PM
Default Gateway : 10.0.0.1
DHCP Server : 10.0.0.1
DNS Servers : 10.0.0.1
NetBIOS over Tcpip. : Enabled

Ethernet adapter Local Area Connection:

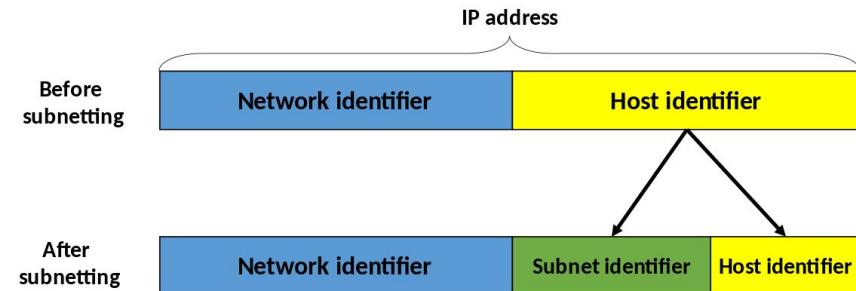
Media State : Media disconnected

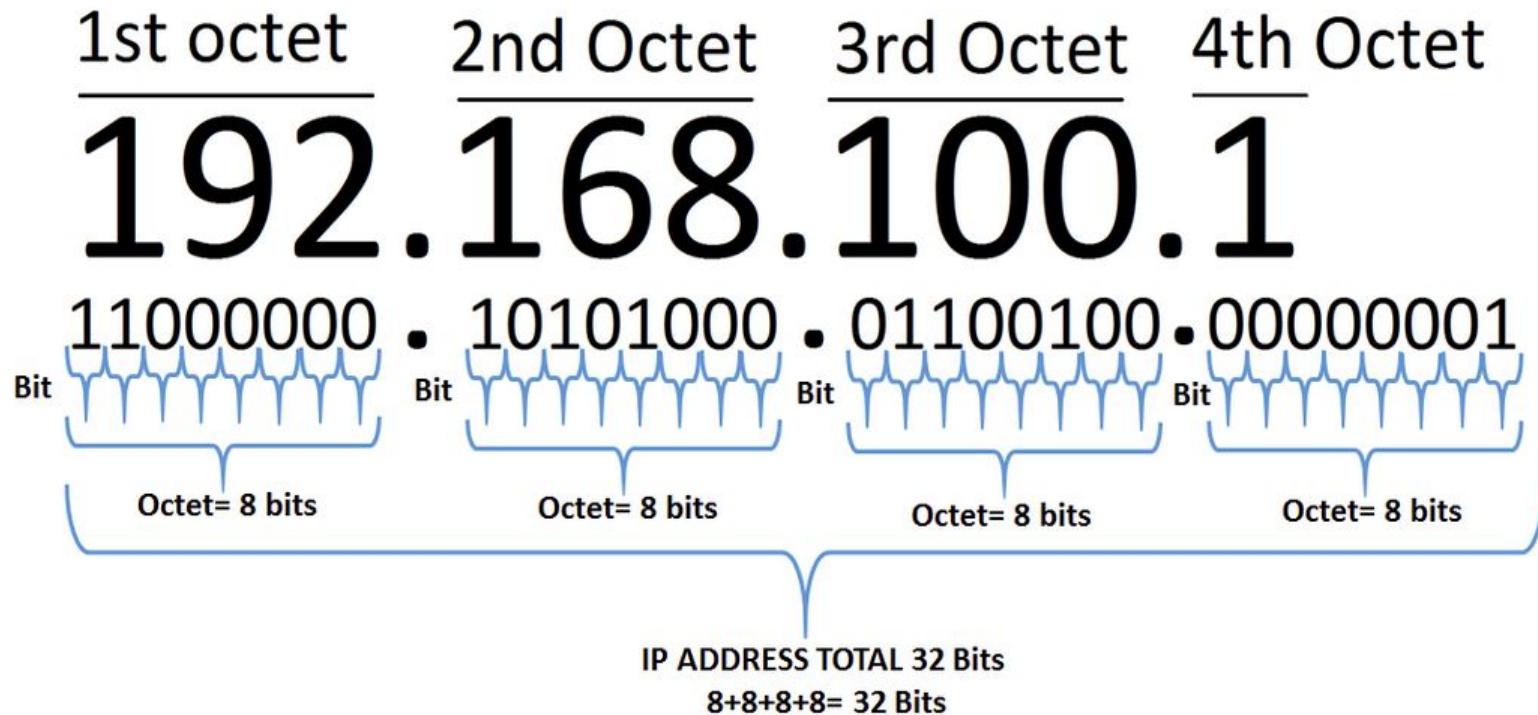


IP

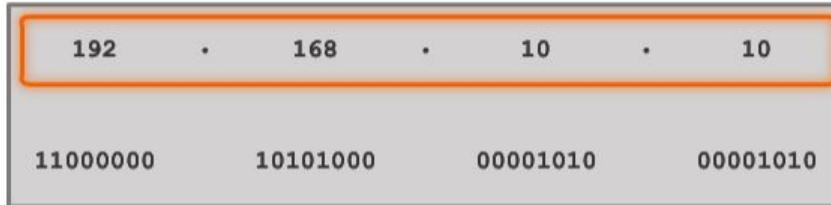
Addresses, IPv4

- What is an IP address?
 - Internet Protocol Address
 - Unique identifier
 - String of numbers separated by periods
 - Uses subnet mask
- Subnet mask - specifies your address vs your neighborhood (Network Identifier)
 - 32 bit number
 - Determines boundaries of a LAN

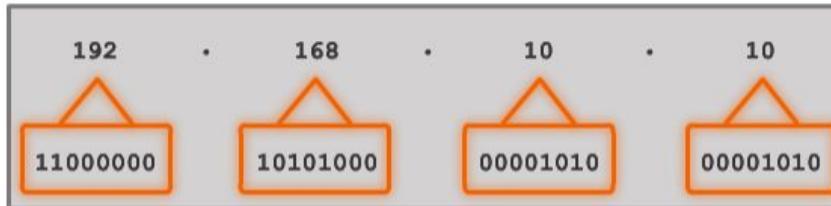




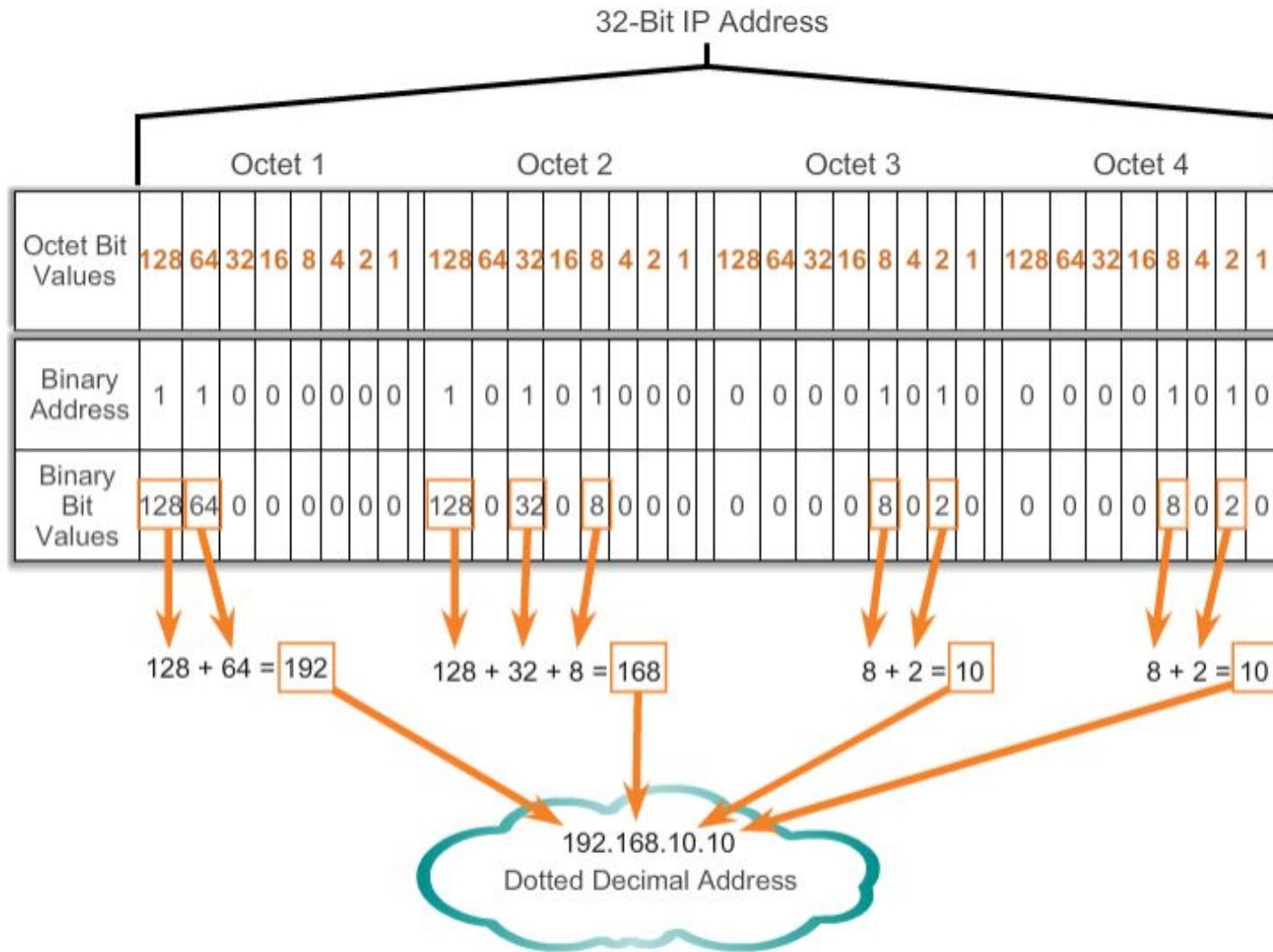
IP Addresses



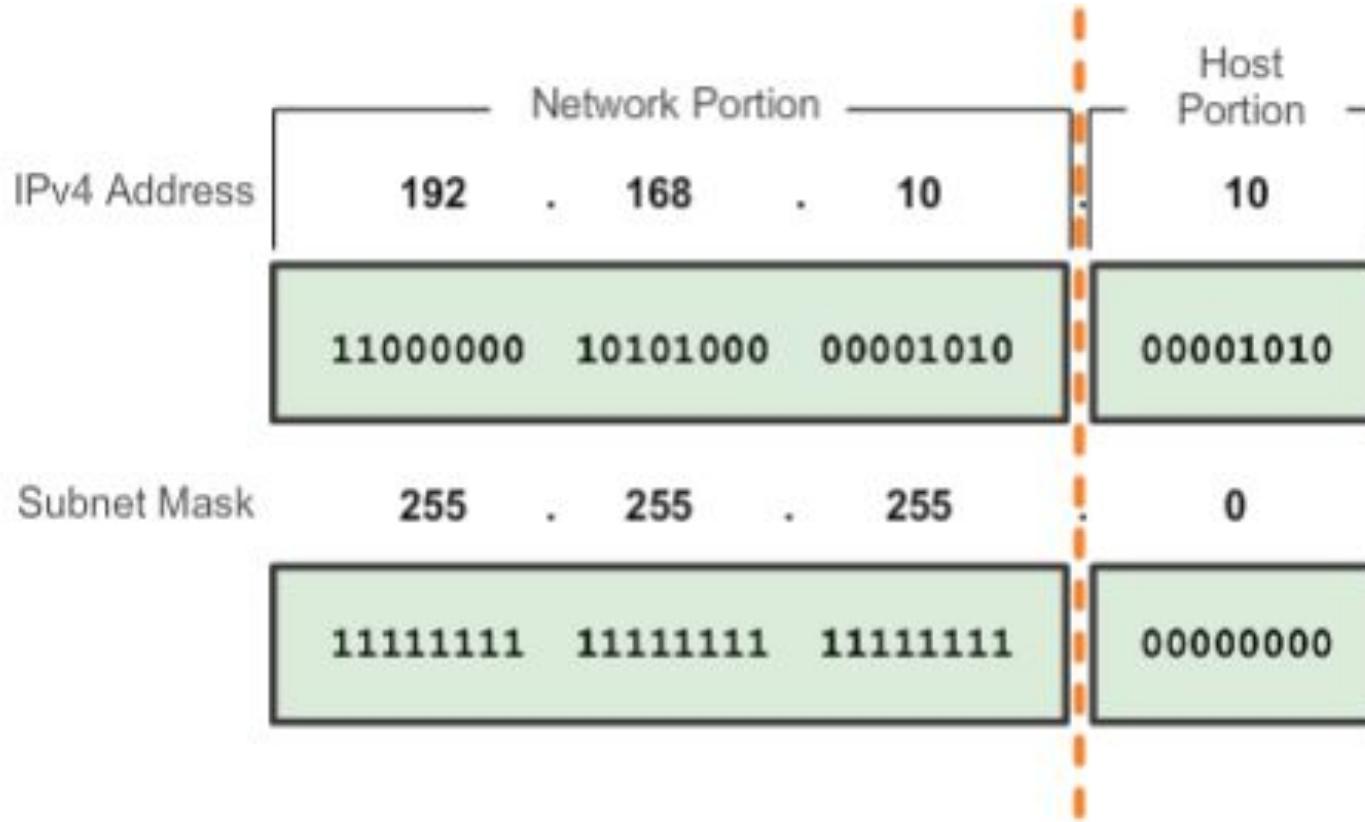
192.168.10.10 is an IP address that is assigned to a computer.



This address is made up of four different octets.



Subnet Mask



	Hosts	Netmask	Number of Subnets
/30	4	255.255.255.252	64
/29	8	255.255.255.248	32
/28	16	255.255.255.240	16
/27	32	255.255.255.224	8
/26	64	255.255.255.192	4
/25	128	255.255.255.128	2
/24	256	255.255.255.0	1
/23	512	255.255.254.0	2
/22	1024	255.255.252.0	4
/21	2048	255.255.248.0	8
/20	4096	255.255.240.0	16
/19	8192	255.255.224.0	32
/18	16384	255.255.192.0	64
/17	32768	255.255.128.0	128
/16	65536	255.255.0.0	256

10.42.7.0/24

Ports

Ports (Logical, not Physical)

- Protocol type association
- Used for connections along an IP address

Protocol	Port
HTTP	80, 8080
HTTPS	443
SSH	22
FTP	21
DNS	53
TELNET	23

Ports (continued)

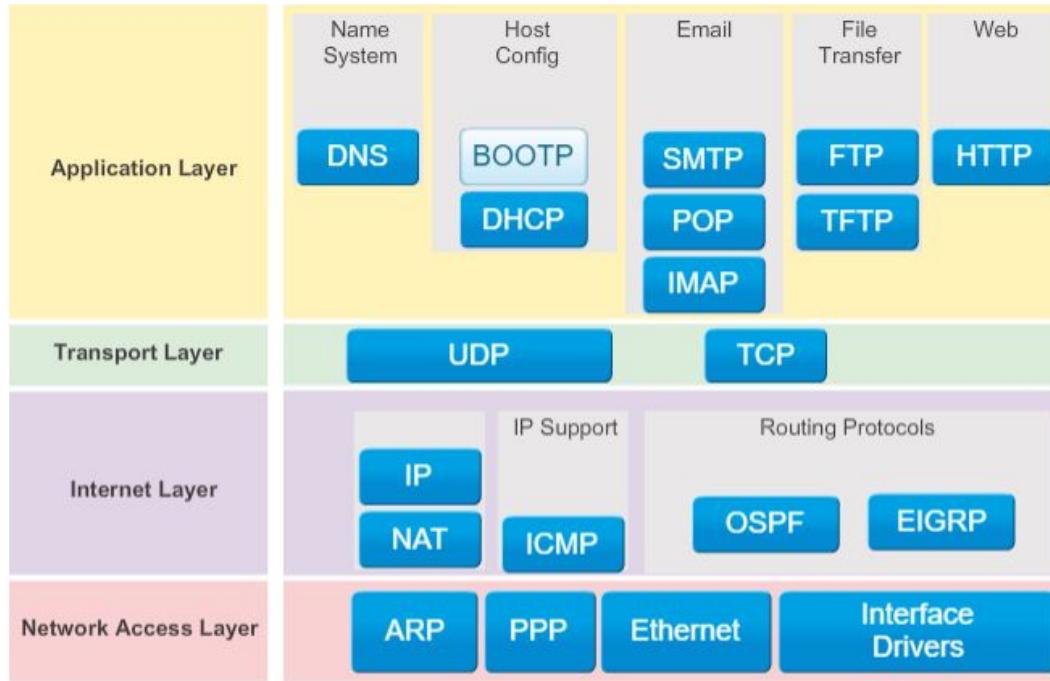
- Well-known: 0 - 1023
 - Used by system process that provide widely used types of network services
- Registered: 1024 - 49151
 - Specific service
 - Assigned by IANA
 - Internet Assigned Numbers Authority (IANA) - global IP address allocation
- Dynamic ports: 49152 - 65535

Domain Name System (DNS)

- Translate an IP address to a name
 - 8.8.8.8 → Google.com
- The users only need to remember a name VS a set of numbers
- Typing www.Google.com will be translated to an IP address

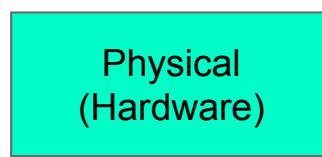
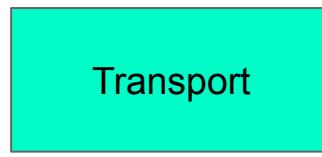
TCP/IP Protocol Stack

TCP/IP Protocol Stack

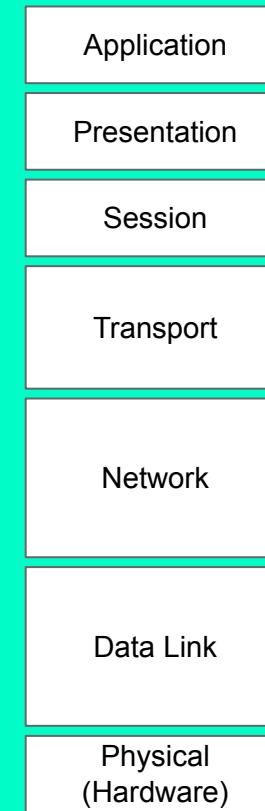


OSI Model

TCP/IP



OSI



TCP/IP

Application

Transport

Network

Physical
(Hardware)

OSI

Application

Presentation

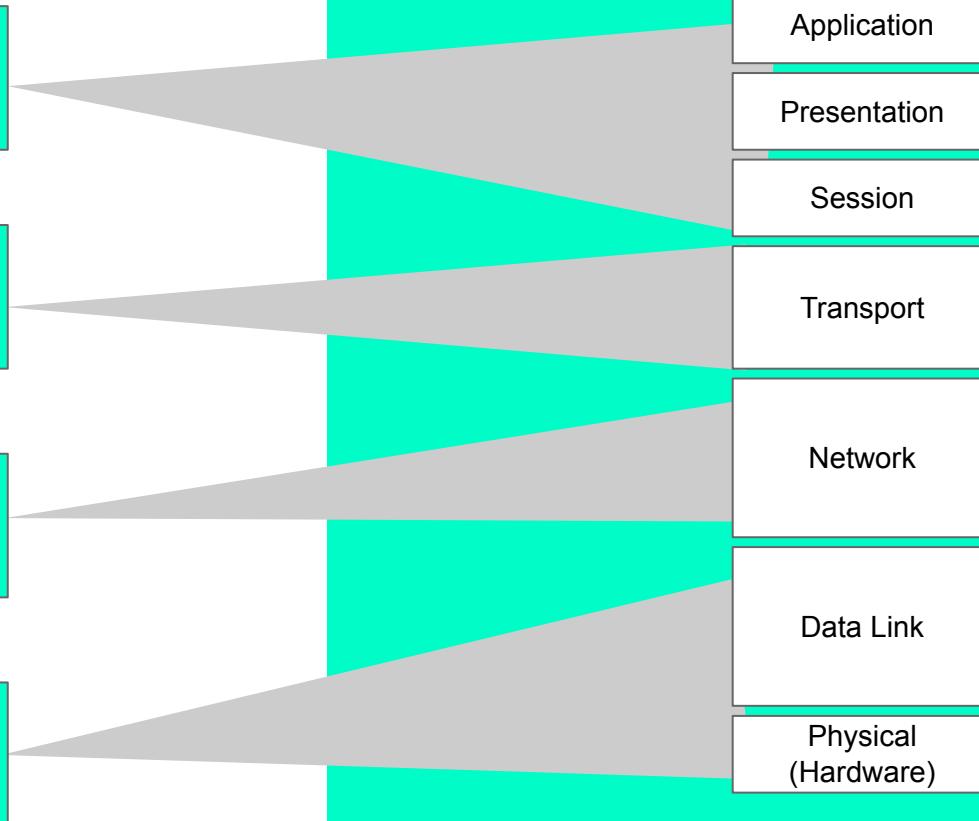
Session

Transport

Network

Data Link

Physical
(Hardware)



OSI Model Explained: Pizza Style

Layer 7: Application



The application layer is the user interface that receives commands from users. Clicking on a link on an internet browser is akin to a customer dialing on their phone to order a pizza.

Layer 6: Presentation



The presentation layer translates requests received from the application layer into a common networking language. In order for our pizza customer to place an order, she needs to speak a common language with the person taking her order.

Layer 5: Session



This layer can be compared to making a phone call and having the other person pick up the phone. Without another party on the line, no location- or network-related conversation would occur.

Layer 4: Transport



You can think of the transport layer as quality control. Suspicious packets will not make it past a firewall. Similarly, low-quality pizzas will not go out for delivery.

Layer 3: Network



The network layer determines the best way to route information. Similarly, our pizza delivery person will rely on a GPS to map out a customer's location.

Layer 2: Data



One of the major functions of the data link layer is to provide a physical MAC address so that requested information can find its destination. Without a physical address, our pizza delivery man would not be able to complete his delivery.

Layer 1: Physical



The physical layer comprises of the physical hardware components in a network. In this final stop, our now starving customer will receive her delivery.

OSI Model Explained: Pizza Style

Layer 7: Application



The application layer is the user interface that receives commands from users. Clicking on a link on an internet browser is akin to a customer dialing on their phone to order a pizza.

Layer 6: Presentation



The presentation layer translates requests received from the application layer into a common networking language. In order for our pizza customer to place an order, she needs to speak a common language with the person taking her order.

Layer 5: Session



Okay that was a large sausage pizza with veggies. That will be \$12.75.



This layer can be compared to making a phone call and having the other person pick up the phone. Without another party on the line, no food-related or network-related conversation would occur.

Layer 4: Transport



You can think of the transport layer as quality control. Suspicious packets will not make it past a firewall. Similarly, low-quality pizzas will not go out for delivery.

Layer 3: Network



The network layer determines the best way to route information. Similarly, our pizza delivery person will rely on a GPS to map out a customer's location.

Layer 2: Data



One of the major functions of the data link layer is to provide a physical MAC address so that requested information can find its destination. Without a physical address, our pizza delivery man would not be able to complete his delivery.

Layer 1: Physical



The physical layer comprises of the physical hardware components in a network. In this final step, our now starving customer will receive her delivery.

OSI Model	TCP/IP Protocol Suite	TCP/IP Model
Application		
Presentation	HTTP, DNS, DHCP, FTP	Application
Session		
Transport	TCP, UDP	Transport
Network	IPv4, IPv6, ICMPv4, ICMPv6	Internet
Data Link	PPP, Frame Relay, Ethernet	Network Access
Physical		

Transport Layer

- TCP
 - Reliable
 - Connection oriented
 - Three way handshake
 - SYN, SYN-ACK, ACK
- UDP
 - Not reliable
 - Faster transmission
 - Streaming

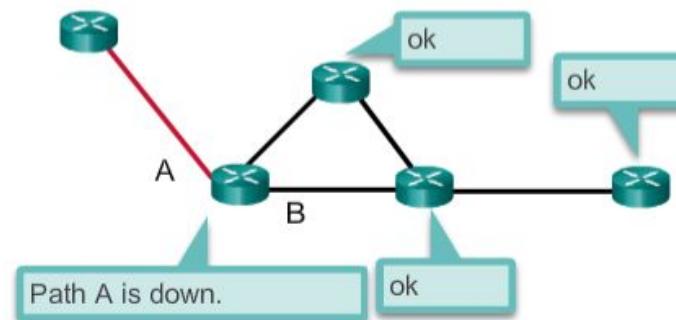
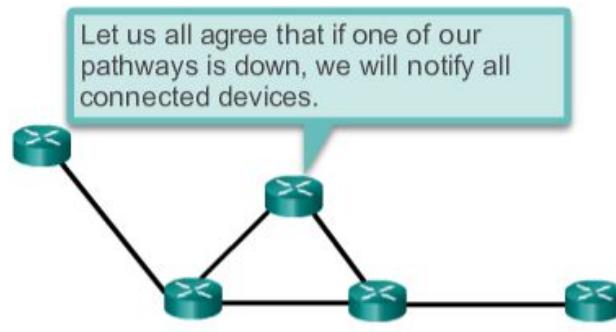
Protocols

Router Protocols

- **Routers:**
 - Rend messages to one another
 - Establish communication
 - Establish routing tables
- **Examples:**
 - BGP- Border Gateway Protocol
 - RIP- Routing Information Protocol
 - EIGRP- Enhanced Interior Gateway Routing Protocol
 - OSPF- Open Shortest Path First

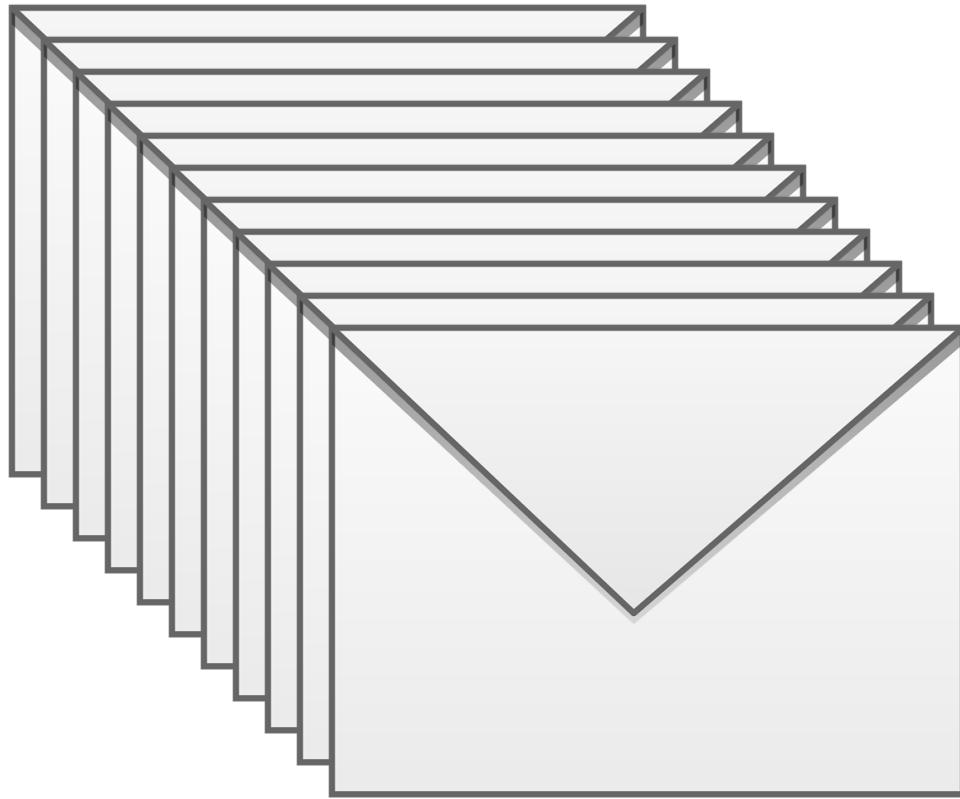
Network Protocol example

Who is notifying that Path A is down?



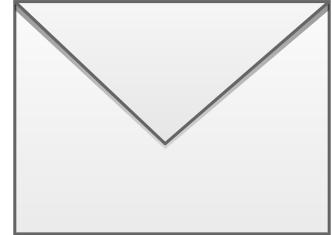
Packets

Packets



MAILING LETTER STEPS

- Sealing message into envelope
- Looking up address to write on envelope
- Determine if you can either hand deliver or give it to the mailman instead
 - If mailman then give message
 - Then mailman passes letter to other mailman
 - Else, hand deliver
- Wait for response



IP Packets

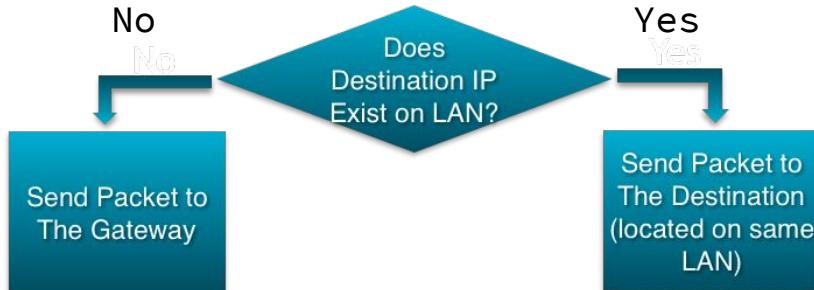
- What do they contain?
 - Source IP Address
 - Sending device
 - Destination Ip Address
 - Receiving device (used by routers to forward a packet to its destination)
 - Source MAC Address
 - Destination MAC address (used by switches to forward packets)
- Frame Check Sequence(FCS)
 - Checks for errors and if it is found then the packet are dropped

Flow of Data and Packets

- IP Layer determines if the client you are sending your packet to resides on your LAN
 - By looking at your:
 - Client's IP address
 - Client's subnet mask
 - Destination IP address

What handles LAN traffic?

- Switches handle the LAN traffic (layer 2 devices)
- LAN traffic is handled through MAC Addresses
- Address Resolution Protocol (ARP) request
 - What IP goes to what MAC address?
 - Is it in the ARP table? If not, forward to router or default gateway



DHCP VS Static

DHCP VS Static Addressing

- Static
 - Assign each address manually
 - IP address will not change
 - Printers, IP phones
- DHCP
 - Preferred method for IPv4 assignments to host on large networks
 - Reduces burden of network staff and virtually eliminates entry errors
 - Dynamically assigns address throughout the network
 - Usually needs a DHCP server and DHCP Client

IPv6

IPV6

- Created to replace IPv4
 - No more IPv4 addresses to give out
- 8 x 16 bit (128 bit) alphanumeric addresses in decimal notation separated by ‘.’s. For example
2001:0000:3238:DFE1:63:0000:0000:FEFB – IPV6

Public VS Private Addresses

Public Addresses VS Private Addresses

- Public
 - Intranet communication
- Private
 - Mainly home networks or companies
- NOTE: UB is Public Addressed
- Scenario:
 - If you go to anyone's house and run a **ipconfig**, you'll get an IP of 192.168.1.x or something similar, this is private address

Commands

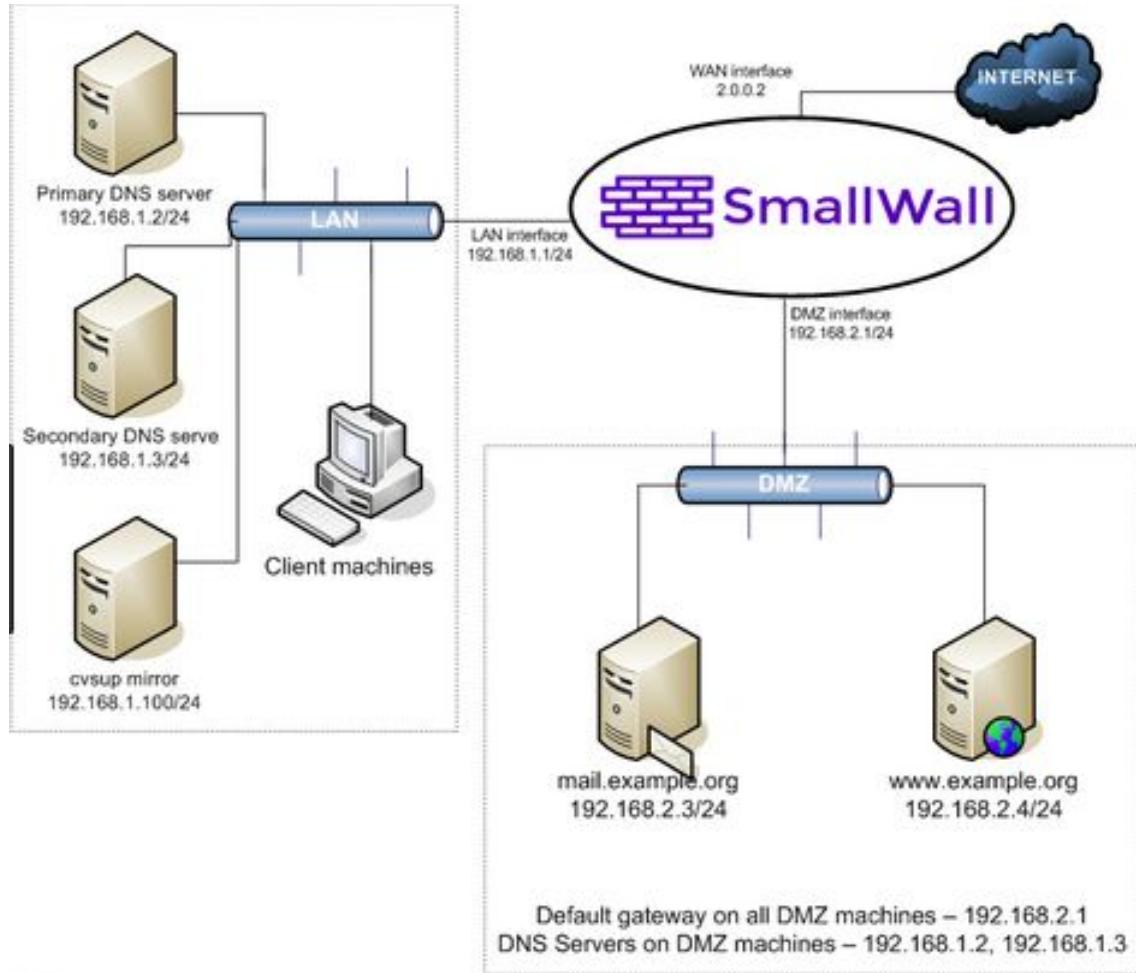
Testing Connections

- **ping** – checks for network connection
 - this one is tricky, many things block ping
- **tracert** – shows hops to a destination
- **nslookup** (Windows) – shows the dns server information
- **ipconfig** (Windows) – displays generic IP addressing info
- **ipconfig /all** (Windows) – shows detailed information for all network adapters
- **ifconfig (Linux)** – displays generic IP addressing info
- **netstat** – Shows active connections
- **nmap** – port scanner, widely used

Topologies

Topologies

- Topologies are diagrams of your network
 - Most places you work will have many, always make one
 - They can be very high level or detailed
- You will create yours on LucidChart (Part B of HW)
<https://www.lucidchart.com/blog/make-network-diagram-free>



Let's Draw Our Own, using pfSense

- Understanding this is very important to understand your homework and the next three of them!