Networking 192.168.1.101

By: Vince

Disclaimer

- I am **NOT** a Networking expert
- you might ask questions that I don’t know the answer to
- Networking is hard to teach
- but I know how to do your homeworks so that counts for something, right?

Goals

- in the past students have struggled with Networking which really hurts their ability to do the assignments
  - this sucks!
- this lecture along with some other techniques were implemented to try and fix this situation
- gain knowledge of the Networking vernacular and basic concepts

Agenda

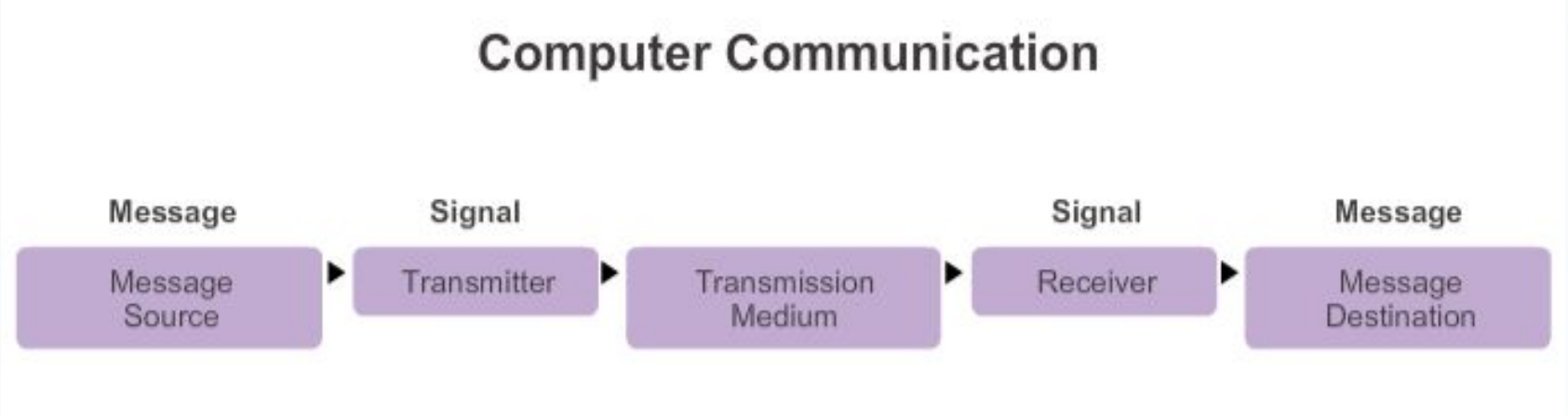
- network infrastructure
- network hardware
- networking details
  - packets, DHCP, IPv4 vs IPv6, routers, clients and much more!
- Topologies
  - used to represent your Network, these are like schematics for Architects
- Build-Your-Own-Network
  - like Build-A-Bear but more fun!

```
Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 3160
Physical Address. . . . . . . . . : F4-06-69-70-74-0C
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . . . . . . . : 2620:cc:8000:484:4d53:2c1f:64e0:c0c6(Preferred)
Temporary IPv6 Address. . . . . . : 2620:cc:8000:484:c00d:530a:1ff1:dd38(Preferred)
Link-local IPv6 Address . . . . . : fe80::4d53:2c1f:64e0:c0c6%17(Preferred)
IPv4 Address. . . . . . . . . . . : 10.84.110.225(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.248.0
Lease Obtained. . . . . . . . . . : Thursday, February 9, 2017 9:38:51 AM
Lease Expires . . . . . . . . . . : Thursday, February 9, 2017 1:30:06 PM
Default Gateway . . . . . . . . . : fe80::208:e3ff:feff:fd94%17
                                    10.84.111.254
DHCP Server . . . . . . . . . . . : 128.205.1.203
DHCPv6 IAID . . . . . . . . . . . : 552863337
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-BE-E5-28-F0-76-1C-A9-BF-59
DNS Servers . . . . . . . . . . . : 128.205.1.200
```

The Interwebs

- the Internet is governed by a series of protocols that form the rules for how communications should happen
- the Internet is a network of networks.
  - there is no centralized point.
  - there are no boundaries.
- information that is sent from one location on the internet to another is broken down into smaller, more manageable pieces called “packets”

So Then What Is Networking?



- Networking is a process of connecting two or more computers for sharing information.
  - way for devices to communicate with one another

So Let’s Start with some Architecture First

- Clients and Servers
- LAN vs. WAN
- DMZ
- Interfaces and Hardware
- Physical Ports
- Devices

Servers

- servers store information and contain resources that clients can access
- provides a service to users or specific programs
- san be used to run a variety of applications
- types of Servers:
  - File, SQL, Websites, Active Directory, Virtualization

- does not necessarily have to look like a server to be a server
- could be compromised through a client

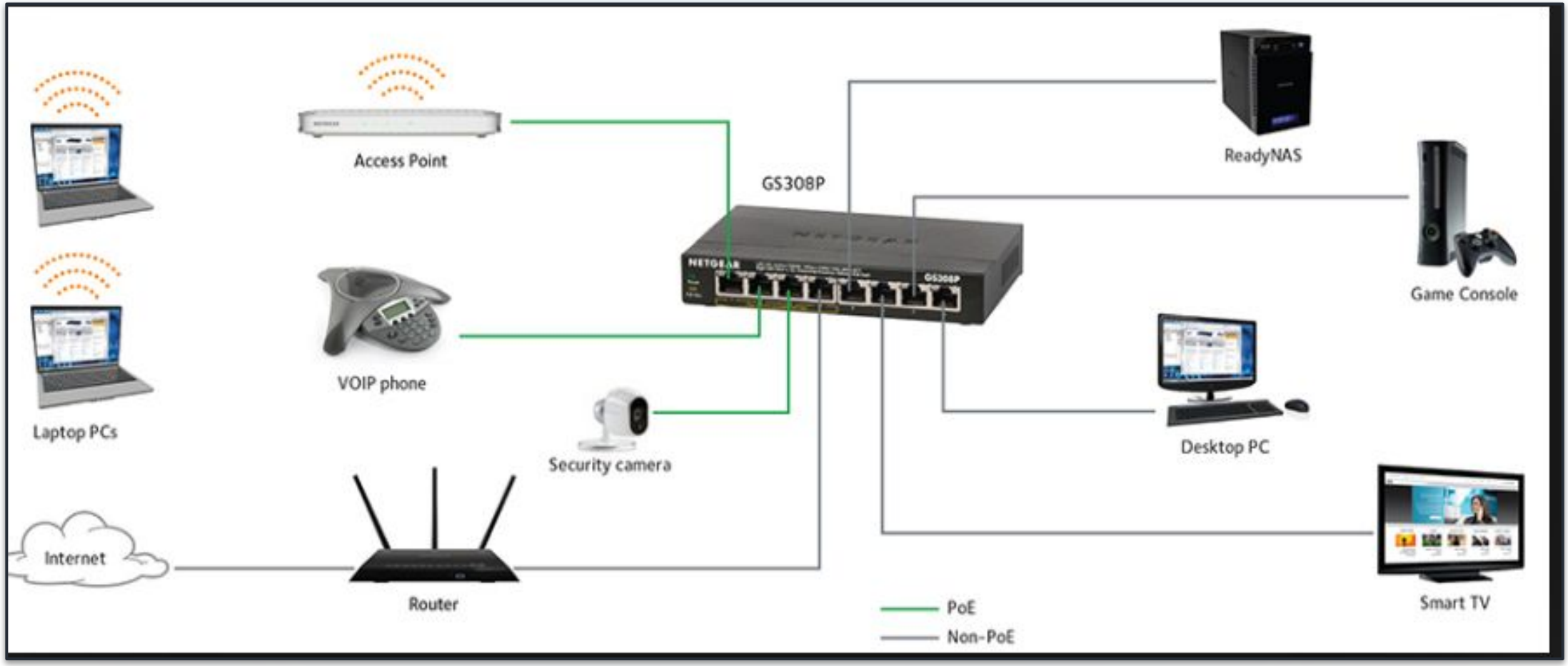
Clients/ Endpoints

- clients access servers for information and resources
- connected to a network (LAN/ WAN.. MAN)
  - Local Area, Wide Are, Metropolitan Area
  - DMZ vs Regular connection
    - DMZ- network is segmented so people on the outside can't get in
  - Most likely segmented on a VLAN(Virtual Local Area Network)
- could be devices such as smartphones, tablets, PCs
- programs could be considered to be clients also

Common Network Devices

- **Router -** forwards data packets to and receives data packets from the Internet
- **Switch -** connects end devices using network cables
- **Wireless Access Point -** consists of a radio transmitter capable of connecting end devices wirelessly
- **Firewall Appliance -** secures outgoing traffic and restricts incoming traffic, Firewall Appliances can be stand alone or running on top of a router

Switch Diagram



Local Area Networks (LAN)

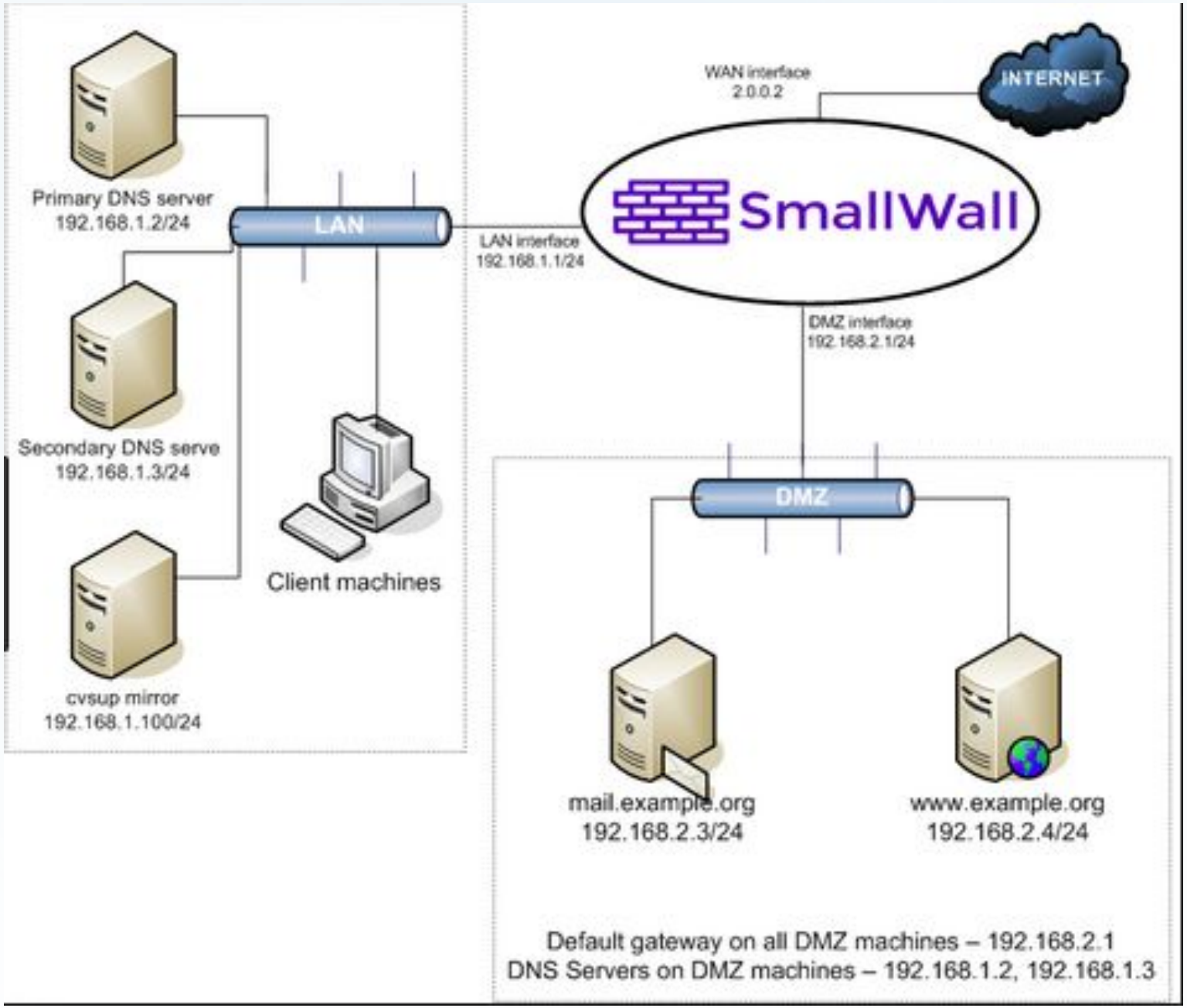
- LANs are the most basic type of network.
- these small networks are the building blocks of the Internet, can be thought of as a “local neighborhood” of computers or devices
- all devices on the same LAN communicate directly with one another across a “switch” (collision domain)
- network and LAN segmentation is a fundamental security concept
- LANs can be organized by:
  - geographic area device type
  - administrative boundary

Wide Area Networks (WAN)

- LANs are connected together to form WANs
  - LANs get connected to WANs through routers
  - the "Internet" is one big WAN
  - we can connect LANs to WANs through both wireless and Wired Connections
  - WANs can span much larger geographic distances than LANs

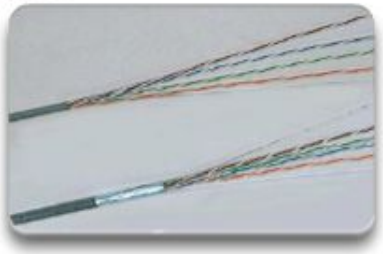
Demilitarized Zone (DMZ)

- a physical or logical sub-network that separates an internal local area network (LAN)
- external-facing servers, resources and services are located in the DMZ so 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


WAN interface
2.0.0.2
INTERNET
SmallWall
LAN interface
192.168.1.1/24
LAN
Primary DNS server
192.168.1.2/24
Secondary DNS serve
192.168.1.3/24
cvsup mirror
192.168.1.100/24
Client machines
DMZ interface
192.168.2.1/24
DMZ
mail.example.org
192.168.2.3/24
www.example.org
192.168.2.4/24
Default gateway on all DMZ machines – 192.168.2.1
DNS Servers on DMZ machines – 192.168.1.2, 192.168.1.3

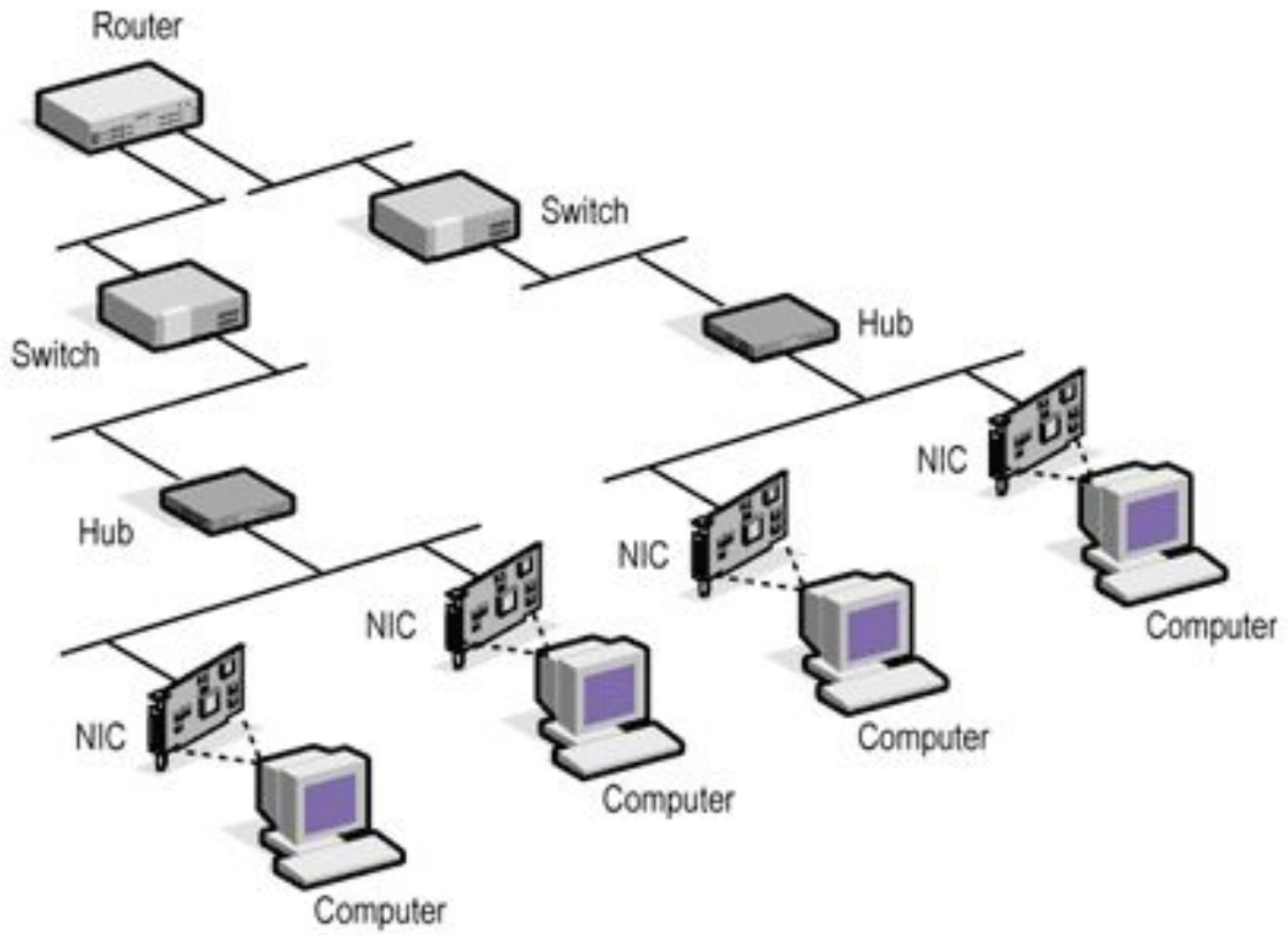
Interfaces and Ports

Copper



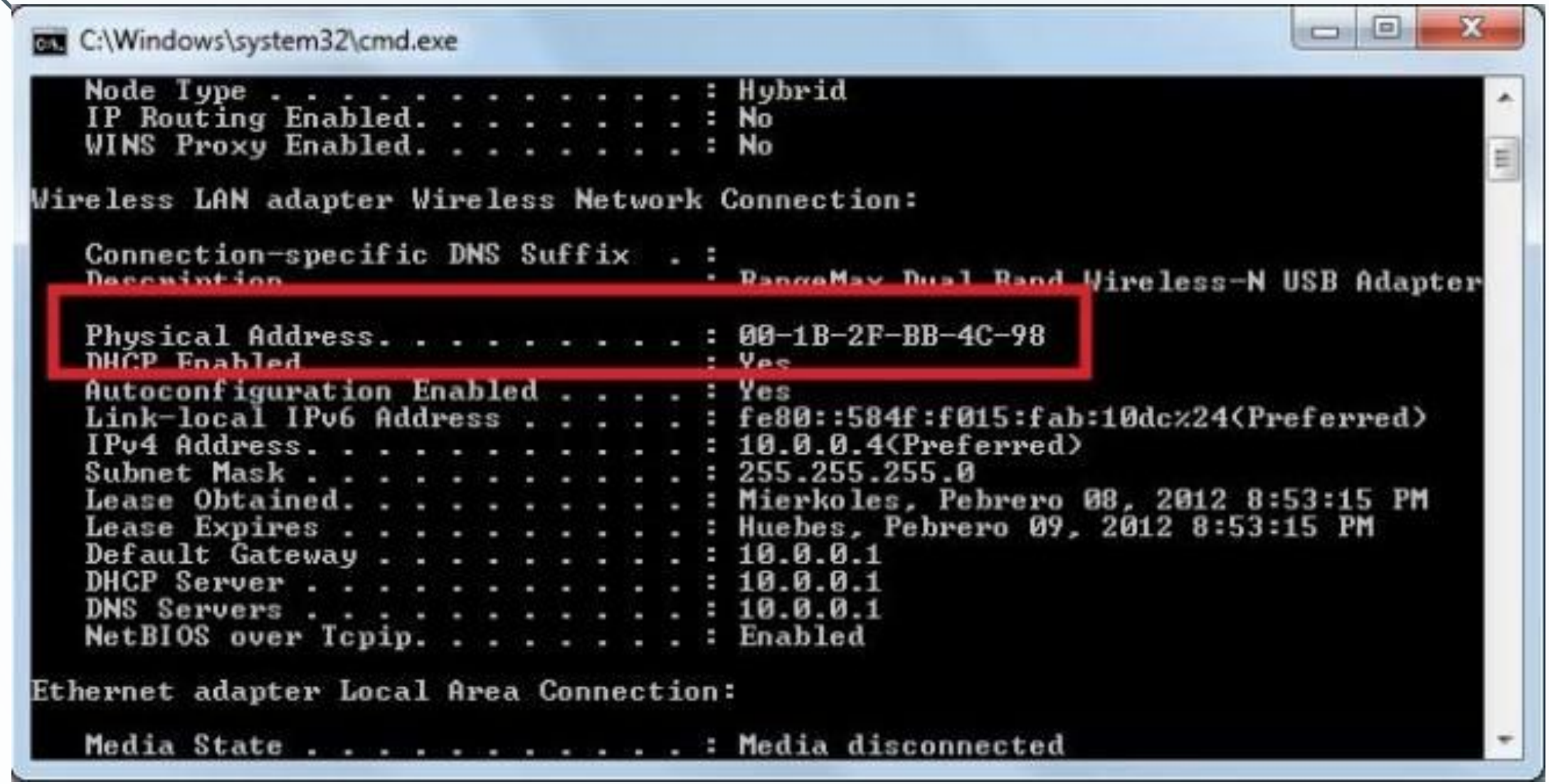
Fiber Optics

Wireless

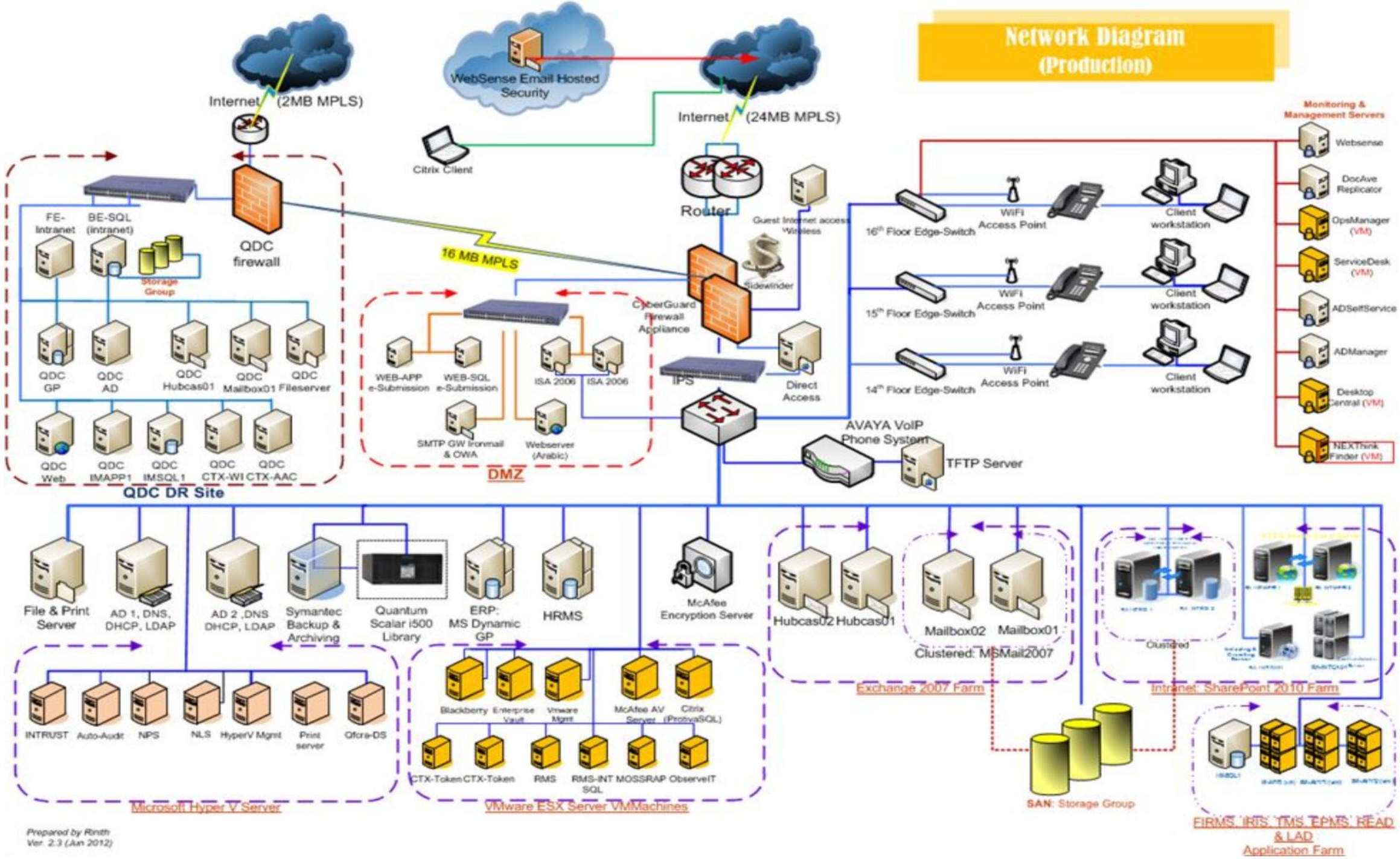

Router
Switch
Switch
Hub
Hub
NIC
NIC
NIC
NIC
Computer
Computer
Computer
Computer

MAC Addresses

- 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. . . . . : Miercoles, Pebrero 08, 2012 8:53:15 PM
Lease Expires . . . . . : Huebes, Pebrero 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

Network Diagram (Production)



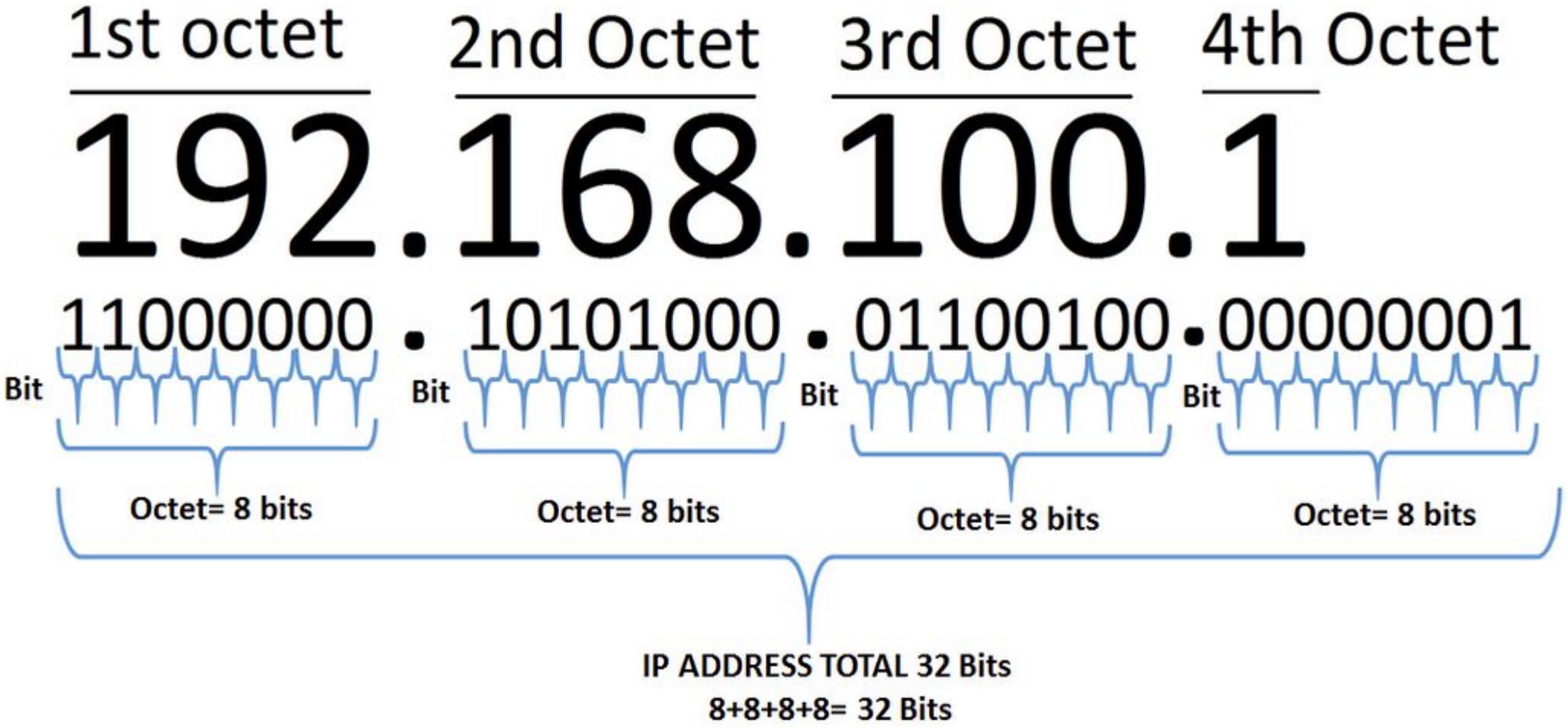

We Will Now Have A
10 MINUTE
INTERMISSION
BEFORE STARTING OUR
NEXT SHOW

Moving Away from Architecture and into Details of Networking

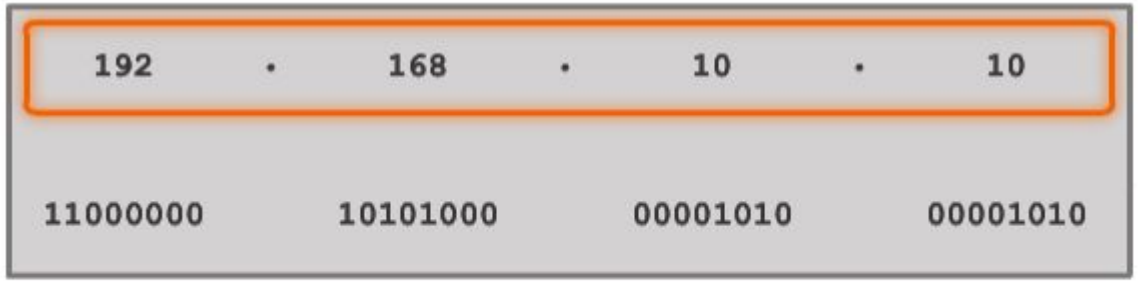
- IP Addresses
- ports
- TCP/IP and OSI
- UDP vs TCP

Addresses, IPv4

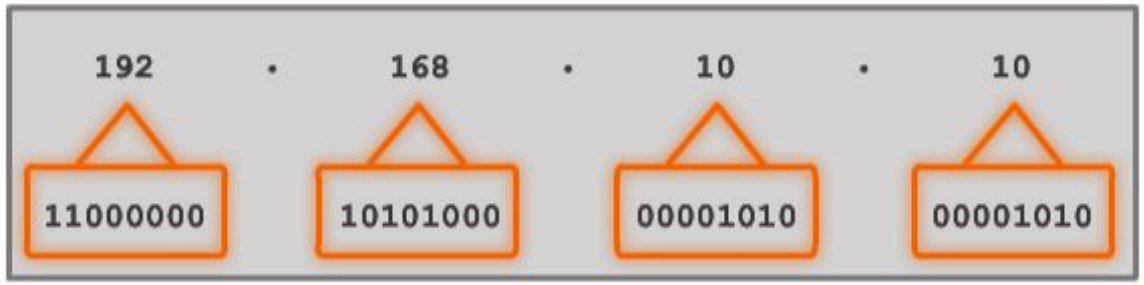
- **IP Address** - together with subnet mask, uniquely identifies end device on the internetwork
- **Subnet Mask** - determines which part of a larger network is used by an IP address


1st octet
2nd Octet
3rd Octet
4th Octet
192.168.100.1
11000000 . 10101000 . 01100100 . 00000001
Bit
Bit
Bit
Bit
Octet= 8 bits
Octet= 8 bits
Octet= 8 bits
Octet= 8 bits
IP ADDRESS TOTAL 32 Bits
8+8+8+8= 32 Bits

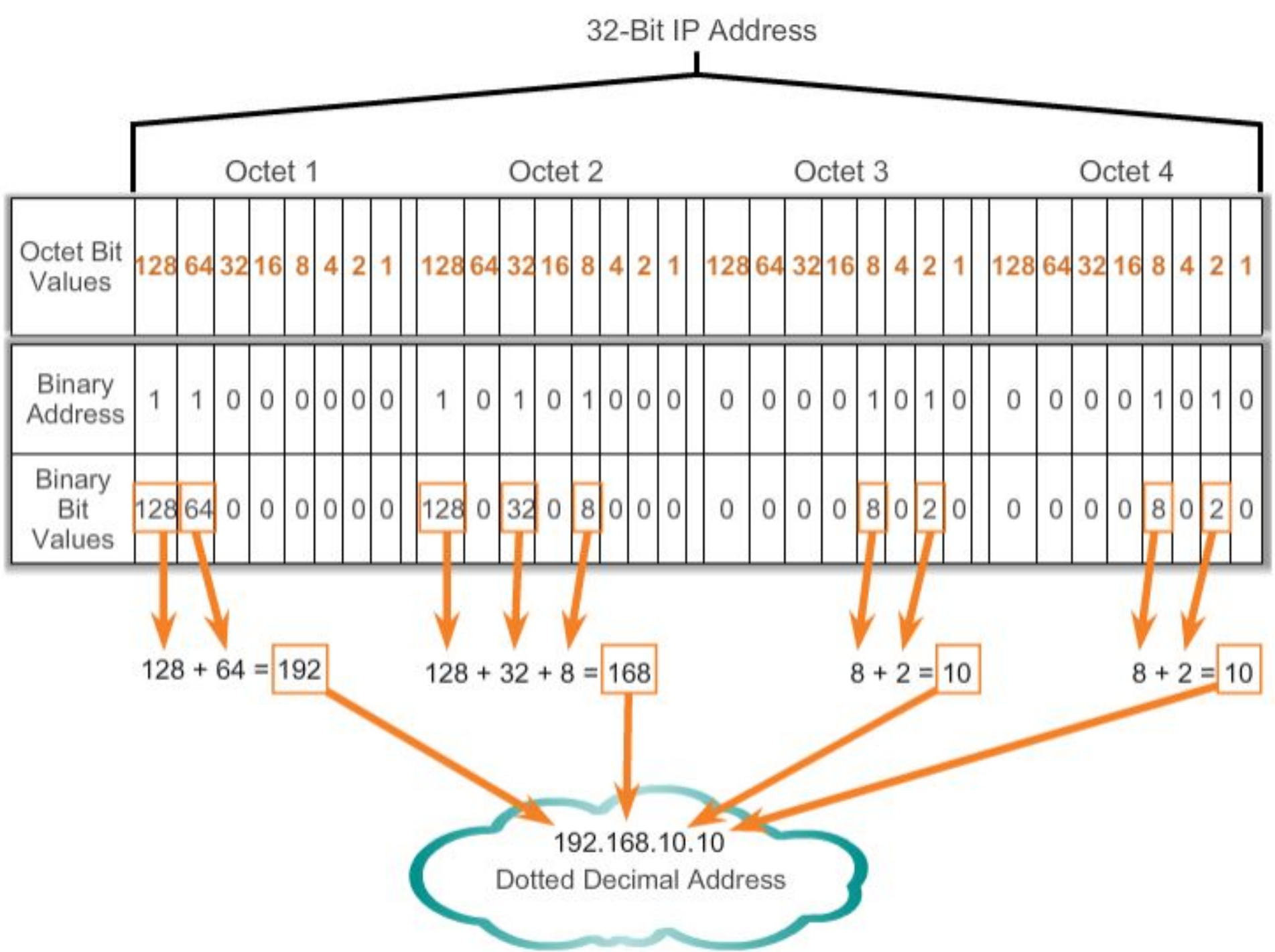
IP Addresses



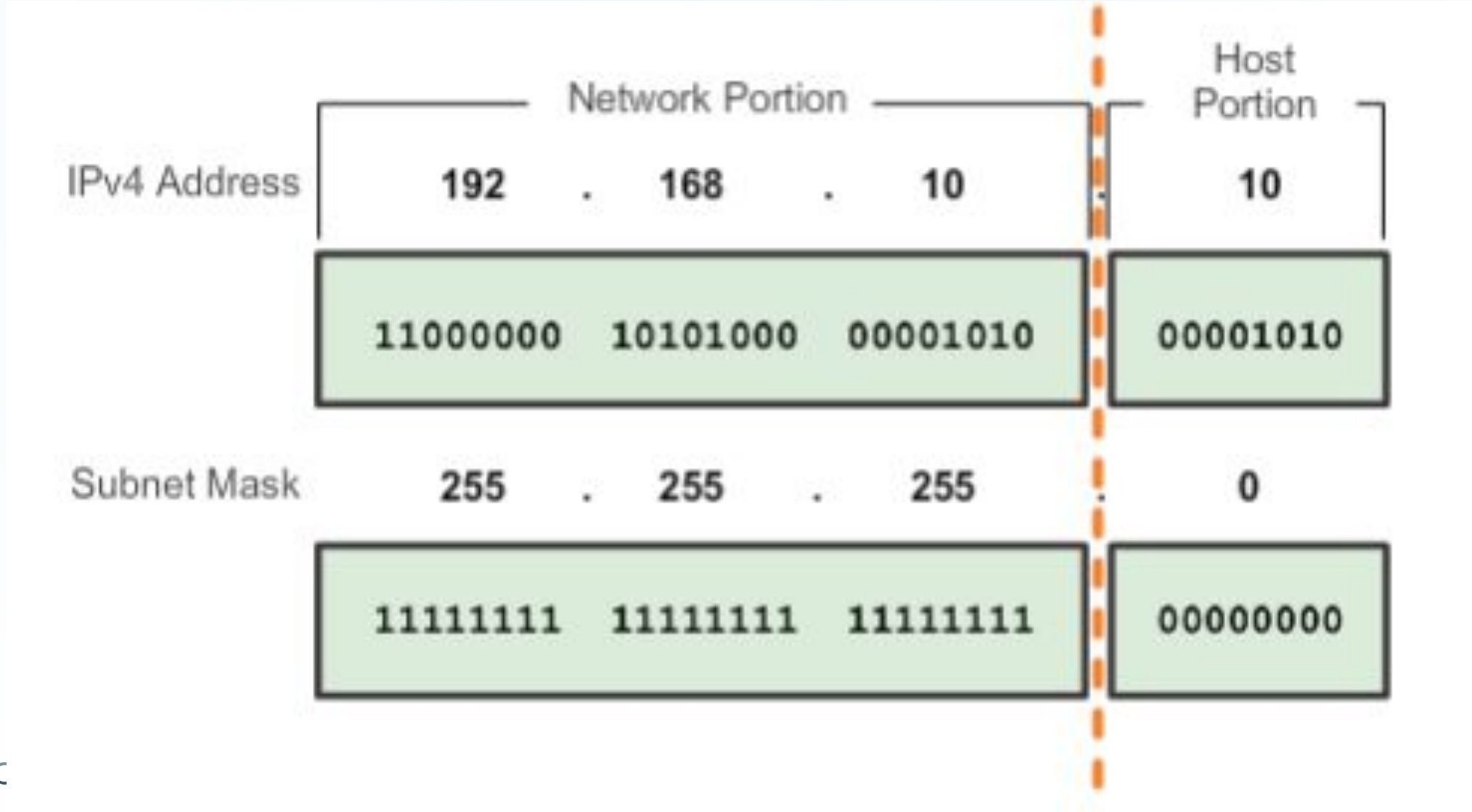
192.168.10.10 is an IP address that is assigned to a computer.



This address is made up of four different octets.


32-Bit IP Address
Octet 1
Octet 2
Octet 3
Octet 4
Octet Bit Values
128 64 32 16 8 4 2 1 128 64 32 16 8 4 2 1 128 64 32 16 8 4 2 1 128 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



Prefix size	Subnet mask	Available subnets	Usable hosts per subnet	Total usable hosts
24	255.255.255.0	1	254	254
25	255.255.255.128	2	126	252
26	255.255.255.192	4	62	248
27	255.255.255.224	8	30	240
28	255.255.255.240	16	14	224
29	255.255.255.248	32	6	192
30	255.255.255.252	64	2	128
31	255.255.255.254	128	2	256

	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 (Logical, not Physical)

- associated with a protocol type, used for connections along with an IP Address
  - HTTPS : 443
  - HTTP: 80, 8080
  - FTP: 21
  - SSH: 22
  - TELNET: 23
  - DNS: 53

More Ports

- can have a total of 65,535 TCP Ports
- well-known ports: 0 to 1023 are the well-known ports or system ports. They are used by system processes that provide widely used types of network services

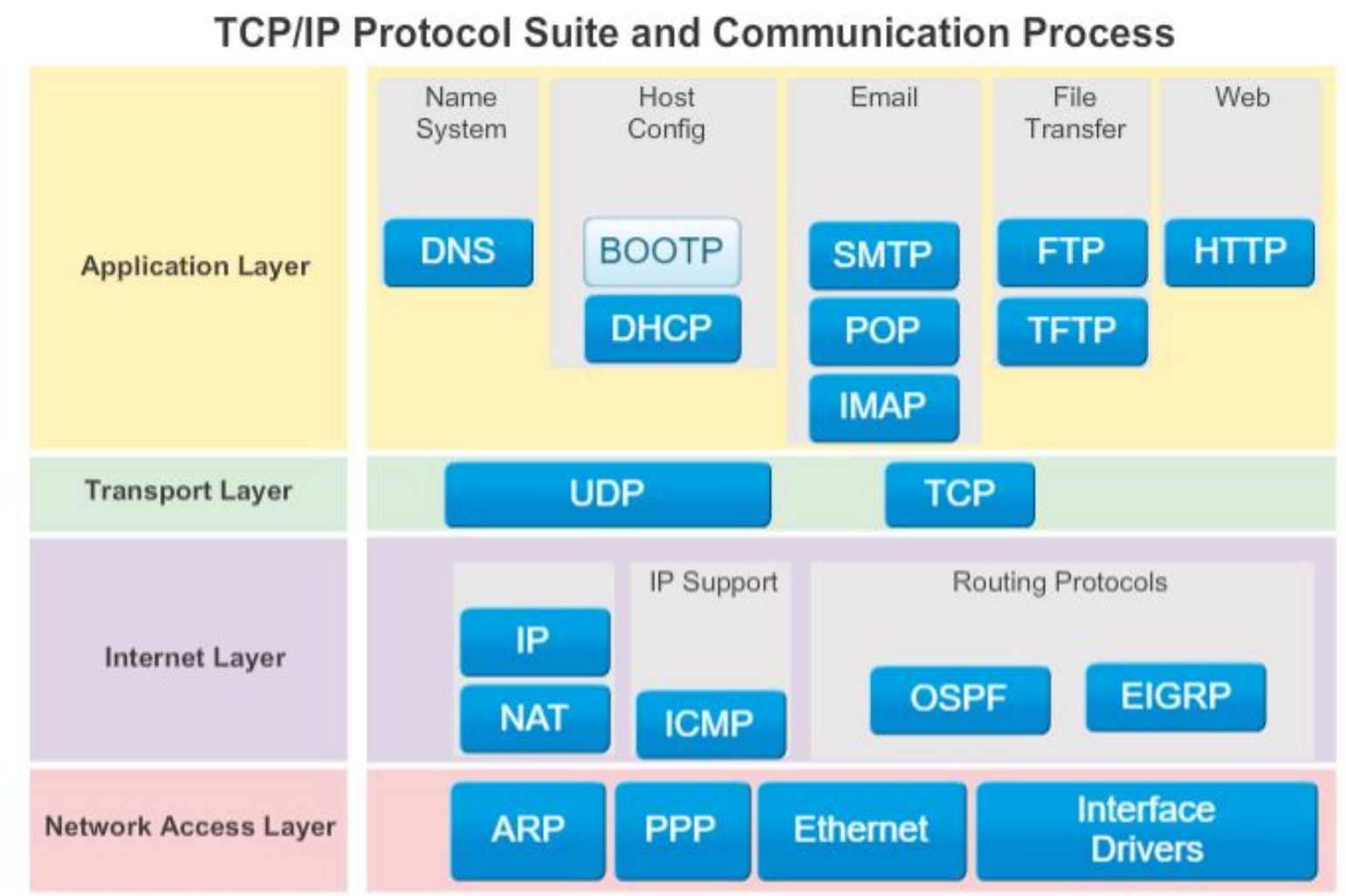
MORE Ports

- registered ports: the range of port numbers from 1024 to 49151 are the registered ports, they are assigned by IANA for specific service upon application by a requesting entity.
- dynamic ports: the range 49152–65535 contains dynamic or private ports that cannot be registered with IANA.
- IANA: The Internet Assigned Numbers Authority (**IANA**) is a function of , a nonprofit private American corporation that oversees global IP address allocation,

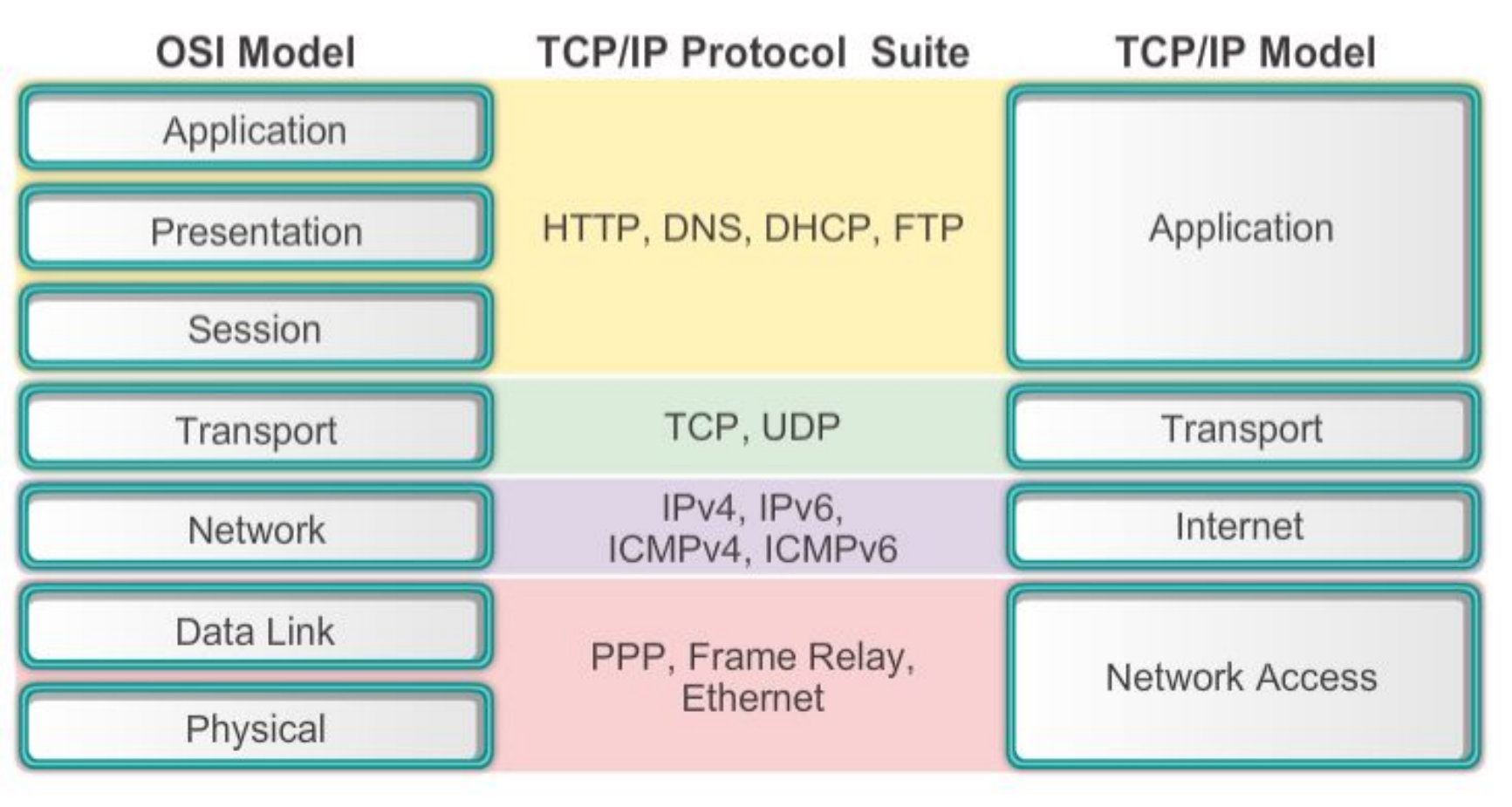
Domain Name System (DNS)

- translates an IP address to a name
- humans are bad at remember numbers that's why DNS was created
- example 128.205.201.57 is mapped to www.buffalo.edu
- so when you type www.buffalo.edu in the web browser
  - DNS translates that domain name to an IP address to connect to the website

TCP/IP


TCP/IP Protocol Suite and Communication Process
Application Layer
Name System
Host Config
Email
File Transfer
Web
DNS
BOOTP
DHCP
SMTP
POP
IMAP
FTP
TFTP
HTTP
Transport Layer
UDP
TCP
Internet Layer
IP Support
Routing Protocols
IP
NAT
ICMP
OSPF
EIGRP
Network Access Layer
ARP
PPP
Ethernet
Interface Drivers

TCP/IP vs. OSI Model



Transport Layer

- TCP
  - connection oriented
  - three way handshake (SYN, SYN-ACK, ACK)
  - reliable
- UDP
  - not reliable
  - used for faster transmission, such as streaming

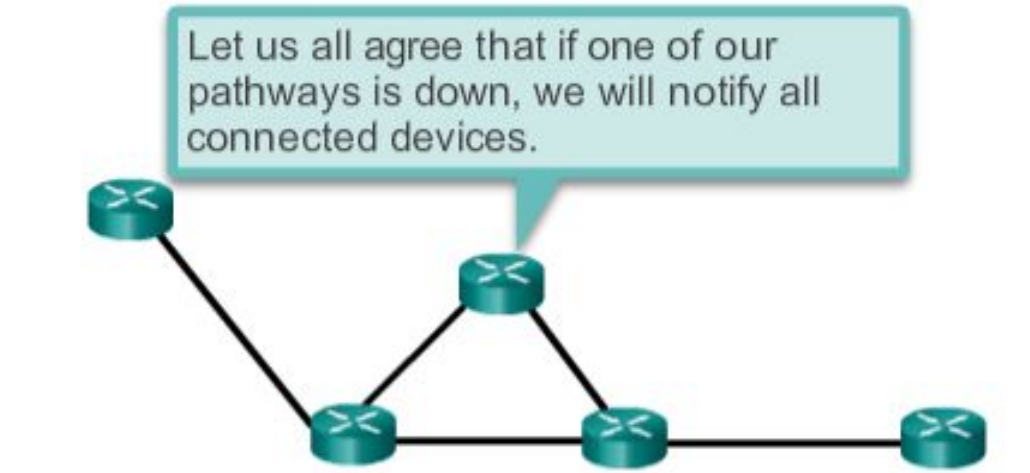
OSI vs TCP/IP Cont

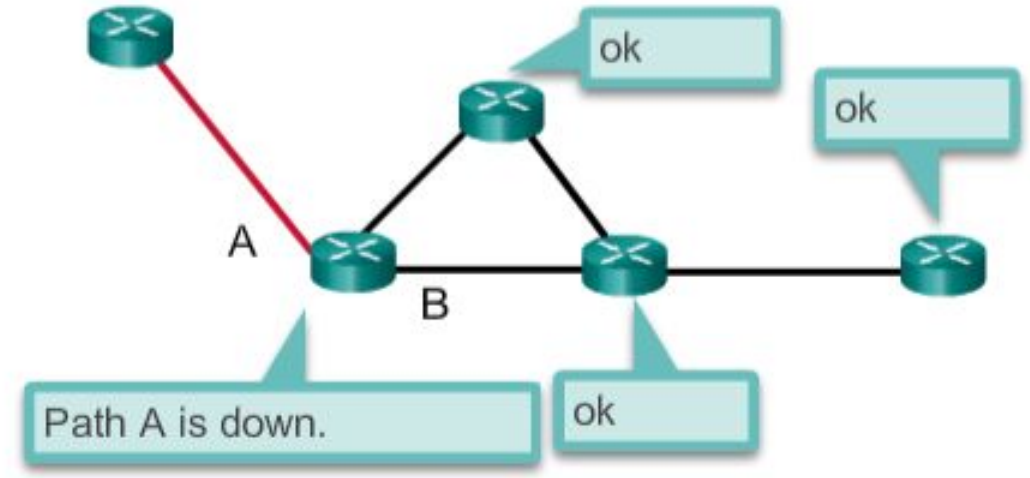
- OSI Model
  - it is used for data network design, operation specifications, and troubleshooting.
- TCP/IP
  - less detailed model than OSI
  - internet model
  - both models are the primary models used when discussing network functionality.

Network Protocols

- routers use these to communicate with one another
  - 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



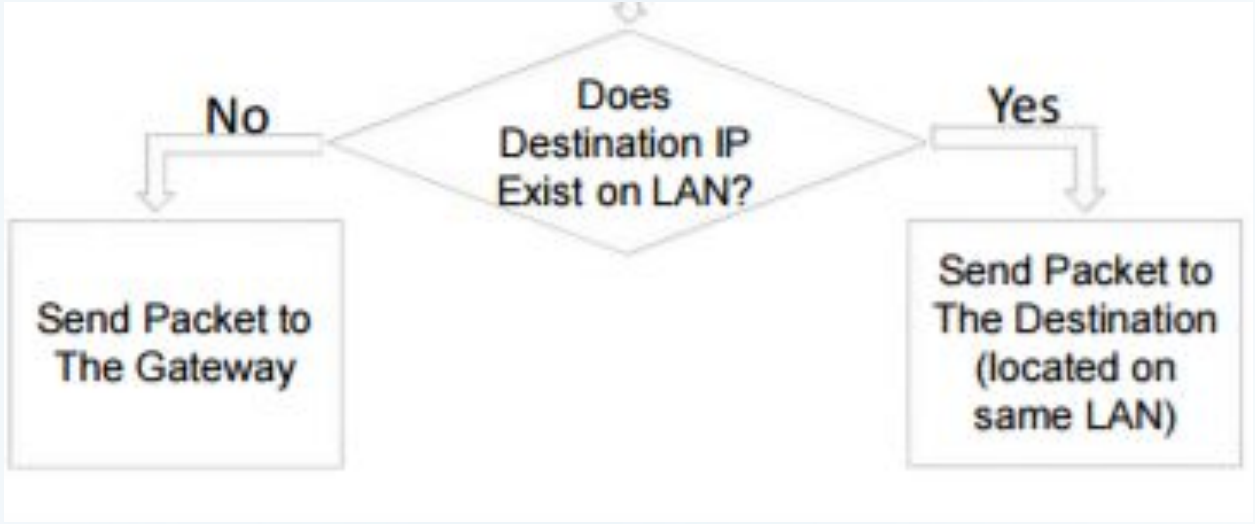


IP Packets

- an IP packet contains two IP addresses:
  - **Source IP address** - the IP address of the sending device
  - **Destination IP address** - the IP address of the receiving device. The destination IP address is used by routers to forward a packet to its destination
  - **Source MAC Address -** your MAC address
  - **Destination MAC Addresses**- used by switches to forward packets
- Frame Check Sequence (FCS)
  - checks to see if there are errors in packets, if there is, It's dropped for a new one

Flow of Data and Packets

- the IP layer determines if the client your sending a packet to resided on your LAN by looking at:
  - your client's IP address
  - your client's subnet mask
  - your destination IP address



- switches handle 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 Addressing

- static addressing means manually assigning each address manually,
  - IP Addresses won't change
  - good for devices like printers and IP phones
- DHCP is generally the preferred method of assigning IPv4 addresses to hosts on large networks because it reduces the burden on network support staff and virtually eliminates entry errors.
  - dynamically assigns addresses throughout the network
  - usually needs a DHCP server and DHCP Client

IP Classes

- Class A – 16,777,216 hosts
- Class B – 1,048,576 hosts
- Class C- 65,536 hosts

Class	Private Networks	Subnet Mask	Address Range
A	10.0.0.0	255.0.0.0	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.0.0	255.240.0.0	172.16.0.0 - 172.31.255.255
C	192.168.0.0	255.255.0.0	192.168.0.0 - 192.168.255.255

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
- tends to be ignored
- stephenorjames favorite

Public Addresses Vs. Private addresses

- public is used for intranet communication
- private is used mainly in home networks or companies
- UB is Public Addressed
- think, 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

Testing Connection

- 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


We Will Now Have A
10 MINUTE
INTERMISSION
BEFORE STARTING OUR
NEXT SHOW

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!