

Networking

UBNetDef, Spring 2024
Week 2

Presenters:
Raymond Harenza

Administrivia

Prerecorded Video Recap

- layers and what they do
- Routing decisions
- LANs and WANs

Learning Goals

- Learn the basics of how network traffic flows
- Interpret a network topology
- Understand OSI network layers 1-3
- Distinguish between network hardware devices
- Configure static networking
- Learn basic network hardening techniques

Agenda

■ What's a network?

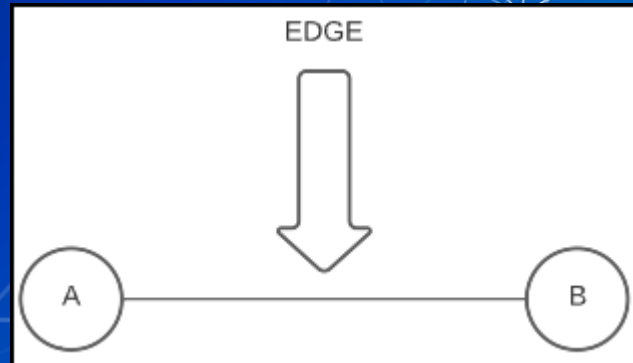
■ OSI Model

- Physical Layer
- Datalink Layer
- Network Layer

■ Topologies and IP assignments

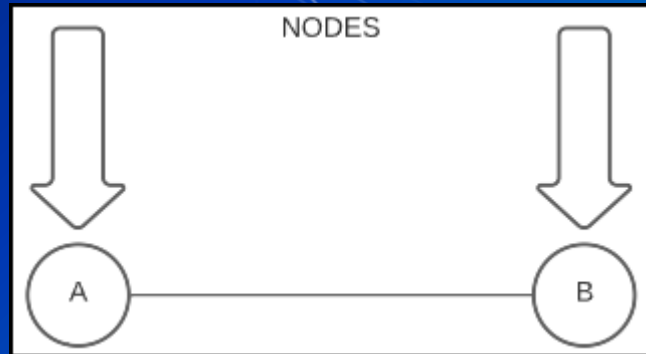
Edges

- The connections
 - Roadways between cities
 - Neural pathways



Nodes

- The connection **points**
 - Cities
 - Neurons



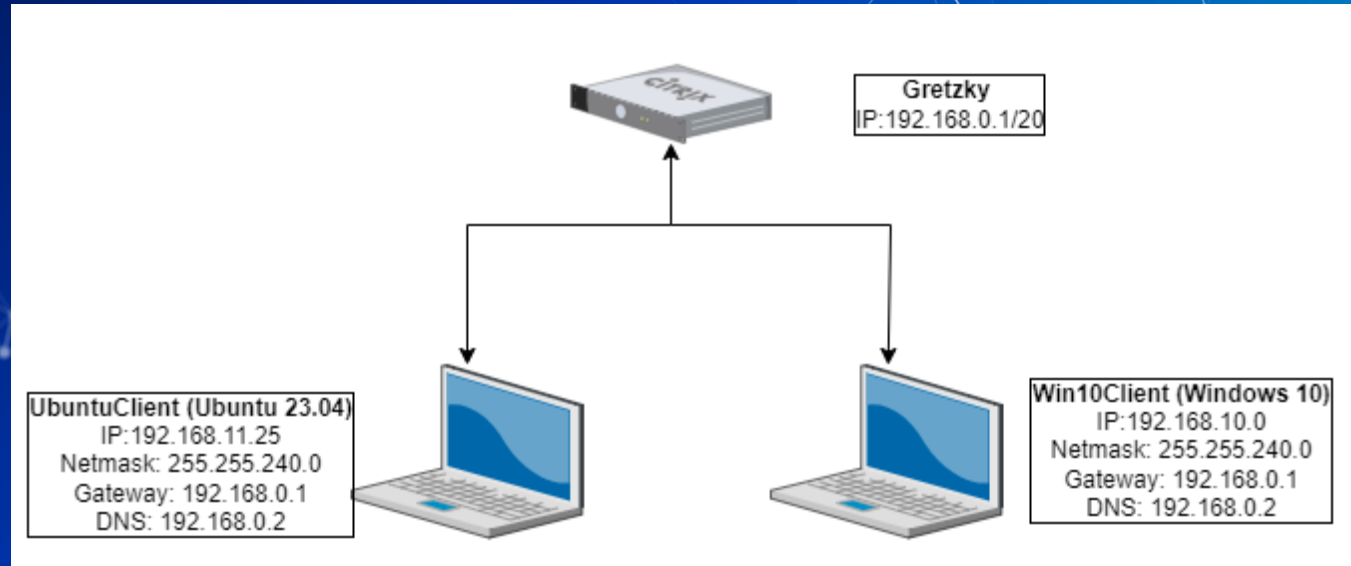
Examples we might see in Class

- Nodes
 - Your physical computer
 - vCenter servers
 - Routers
- Edges
 - Ethernet wires
 - Wireless signals to eduroam

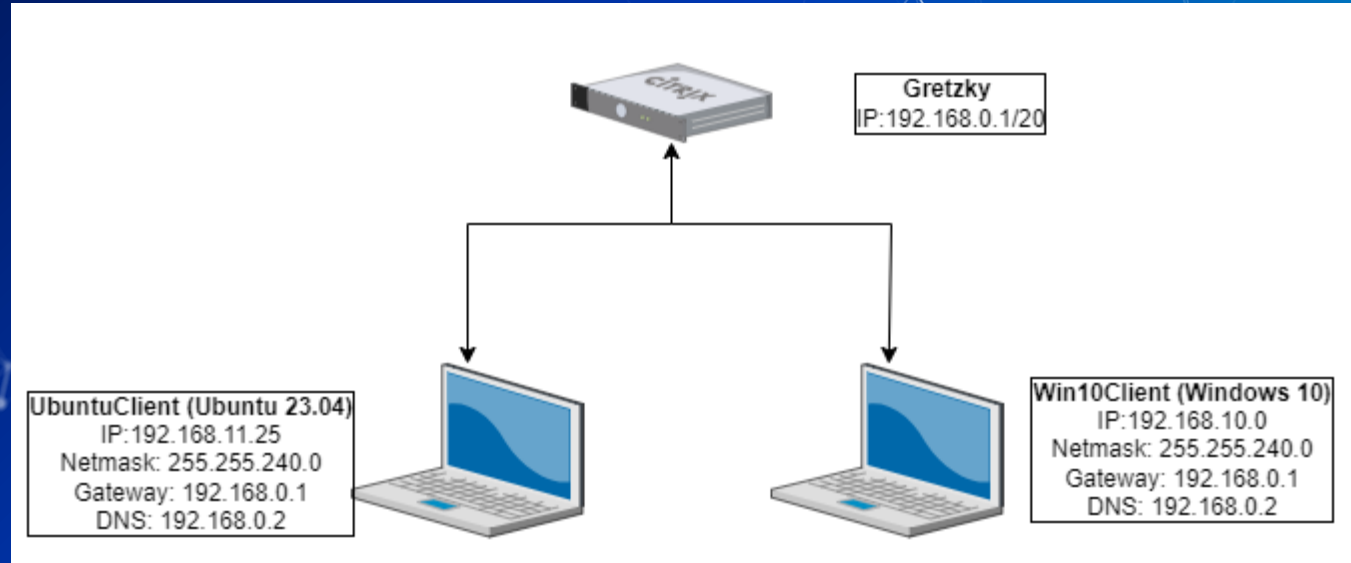
Clients vs. Network Devices

- **Clients:** process and manipulate data
 - Also referred to as "hosts"
 - Examples: computers, servers, gaming consoles, mobile devices, IoT devices
- **Network Devices:** distribute connectivity
 - Examples: routers, modems, switches, other gateways

Which are Clients?



Which are network devices?



Network Devices

- Gateways
 - Receive incoming messages and send outgoing messages
 - Clients only recognize the gateway immediately connected to them
 - Think Doorway
- Routers
 - Pass messages between networks
 - These work with IP addresses

Network Devices

- Switches
 - Distribute messages within an immediate network
 - These work with MAC Addresses
- Gateways, routers, switches can be combined into one piece of hardware

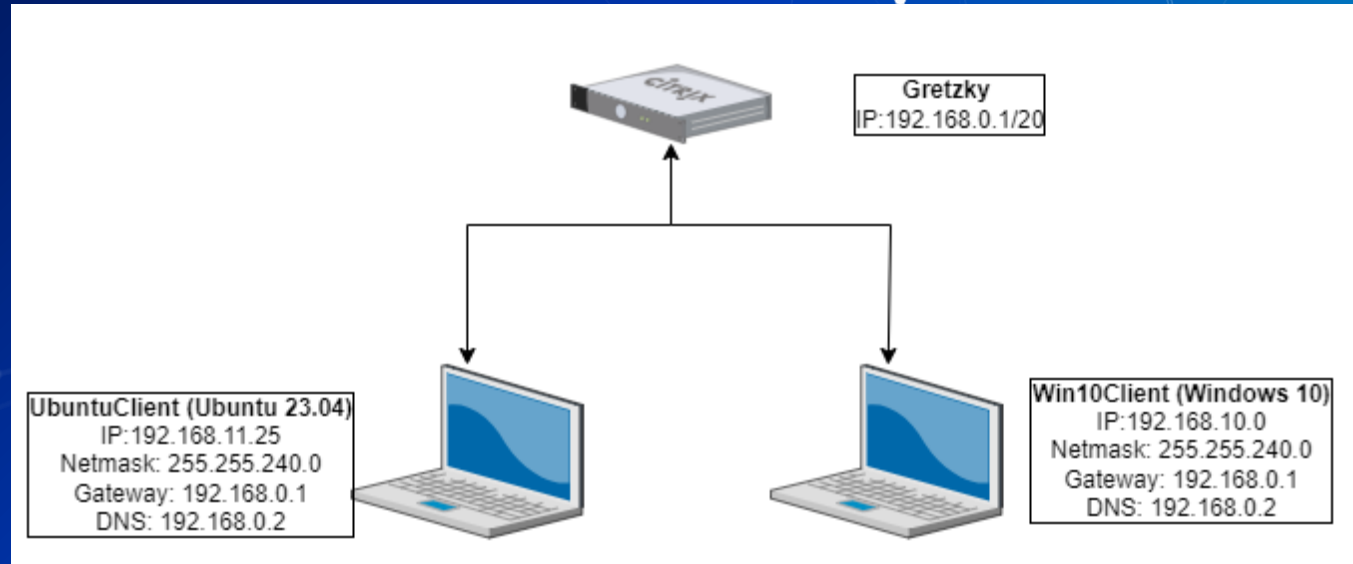
Transmitter vs. Receiver

- **Transmitter (Tx):** Sender of data
- **Receiver (Rx):** Recipient of data

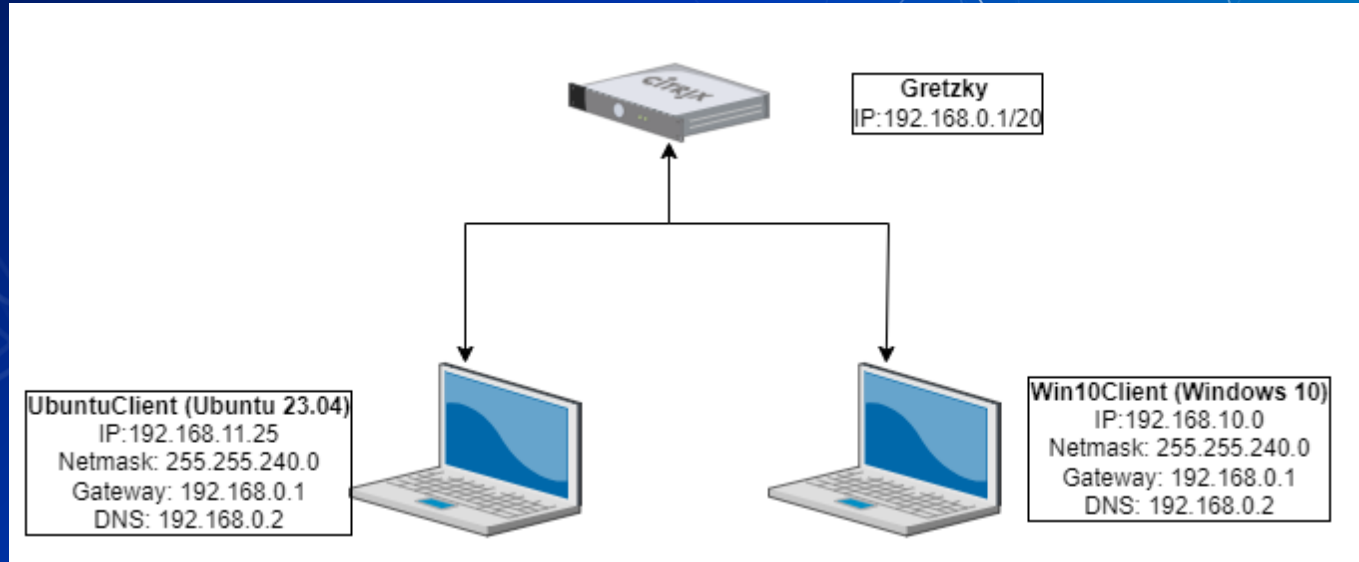
Transmission methods

- **Unicast:** one transmitter, one receiver
- **Multicast:** one transmitter, multiple but not all receivers
- **Broadcast:** one transmitter, all receivers

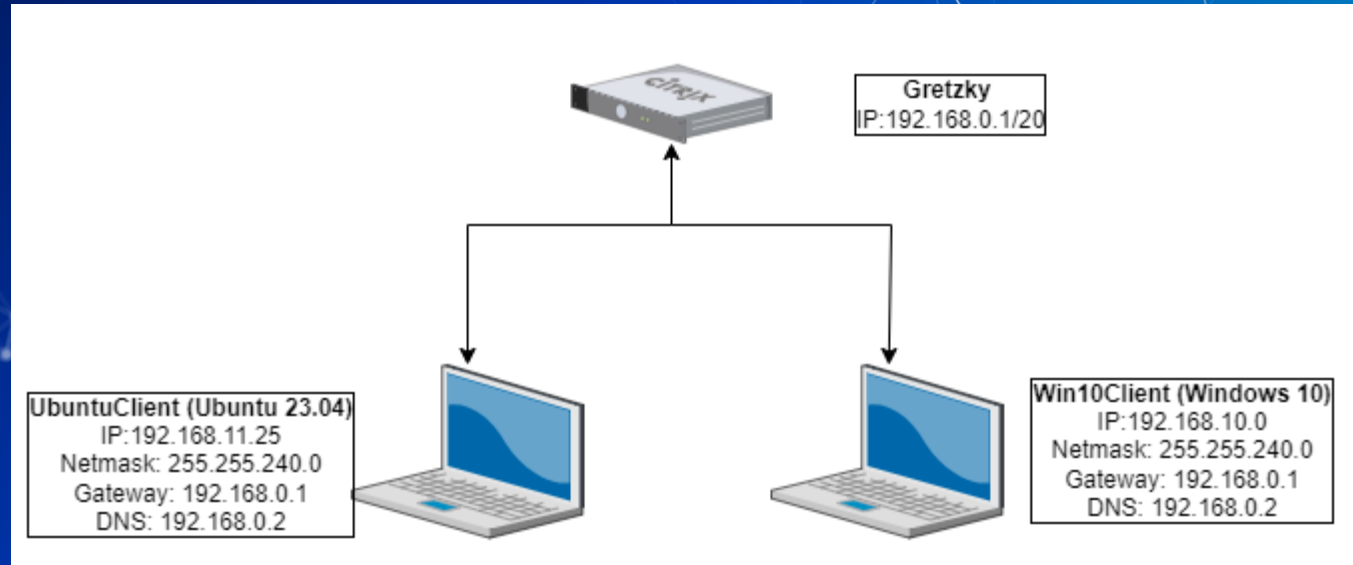
Which broadcast method?



Which broadcast method?



How about a multicast?



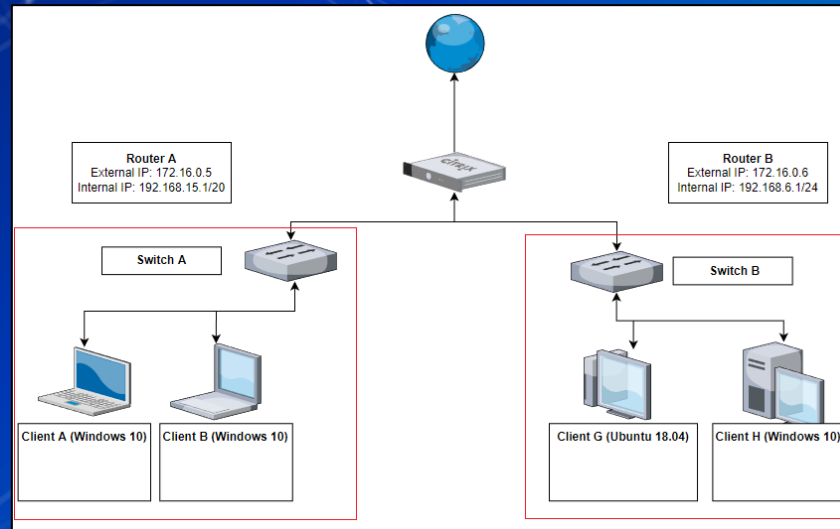
Clients: Clients vs. Servers

- **Clients:** primarily request remote services
 - Examples: mobile device, workstation, laptop, computer
 - Behavior: browse the web, receive updates, provide credentials
- **Servers:** primarily provide remote services
 - Examples: web servers, intrusion detection systems, active directory
 - Behavior: store and provide web pages, distribute updates, verify credentials

LANs

Local Area Network

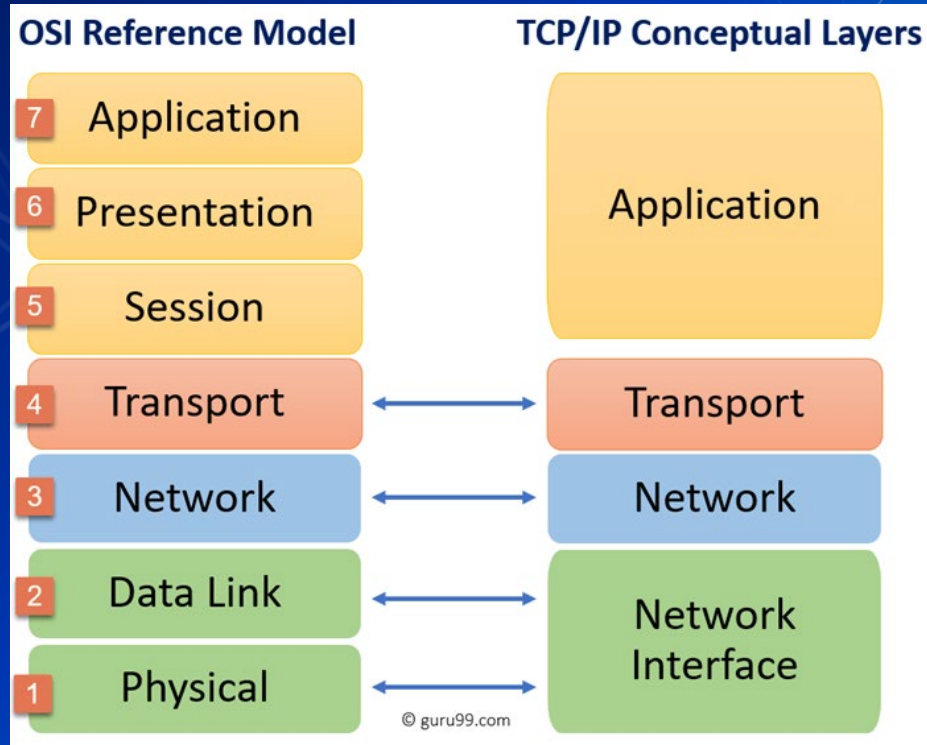
- Devices on the same network share the same communication paths (e.g., cables or wireless links)



Agenda

- What's a network?
- OSI Model
- Topologies and IP assignments

Computer Layering Models

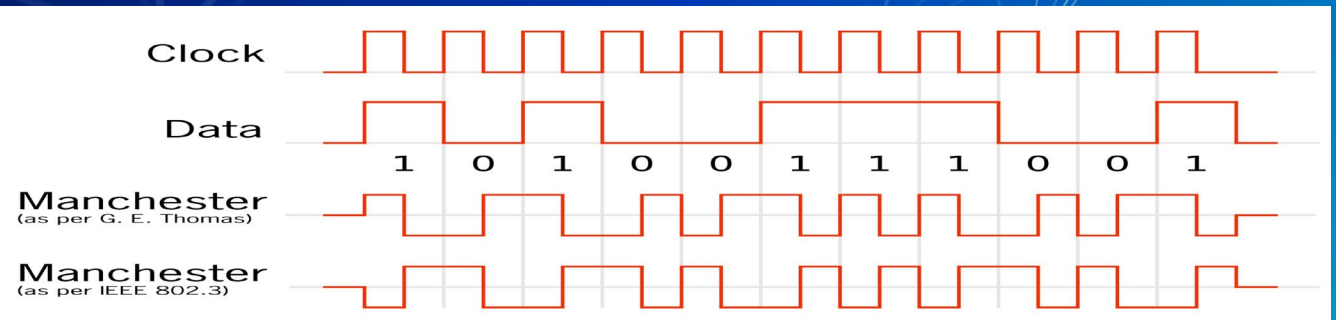


Agenda

- What's a network?
- OSI Model
 - Physical Layer
 - Datalink Layer
 - Network Layer
- Topologies and IP assignments

OSI Layer 1: Physical Layer

- Layer 1: Physical Layer
 - Physical connections
 - Mediums
 - Examples: fiber, radio, ethernet
 - Signals
 - Examples: 1s & 0s
 - Security controls

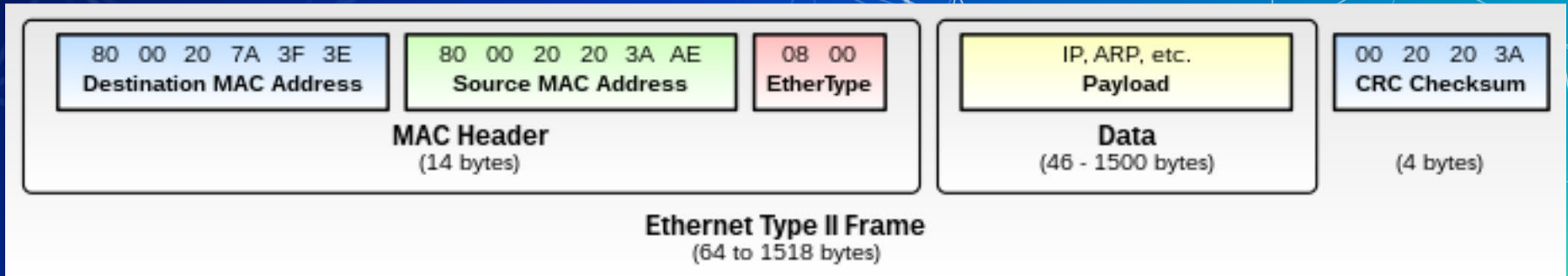


Agenda

- What's a network?
- OSI Model
 - Physical Layer
 - Datalink Layer
 - Network Layer
- Topologies and IP assignments

OSI Layer 2: Datalink Layer

- Layer 2: Datalink Layer
 - Receives bits and delivers them to a processor
 - Unit of data:
 - Frames



Layer 2 Cont.

- Physical receivers are identified by MAC Addresses
 - Example MAC Address: 00-B0-D0-63-C2-26
 - On Your Network Interface Card (NIC)
 - Only seen within the Local Area Network
- Switches usually exist at this layer
 - Switches move data within the network
 - Layer 2 switches use a MAC address table which associates MAC addresses to physical ports
- Vulnerabilities that exist at layer 2



Controls

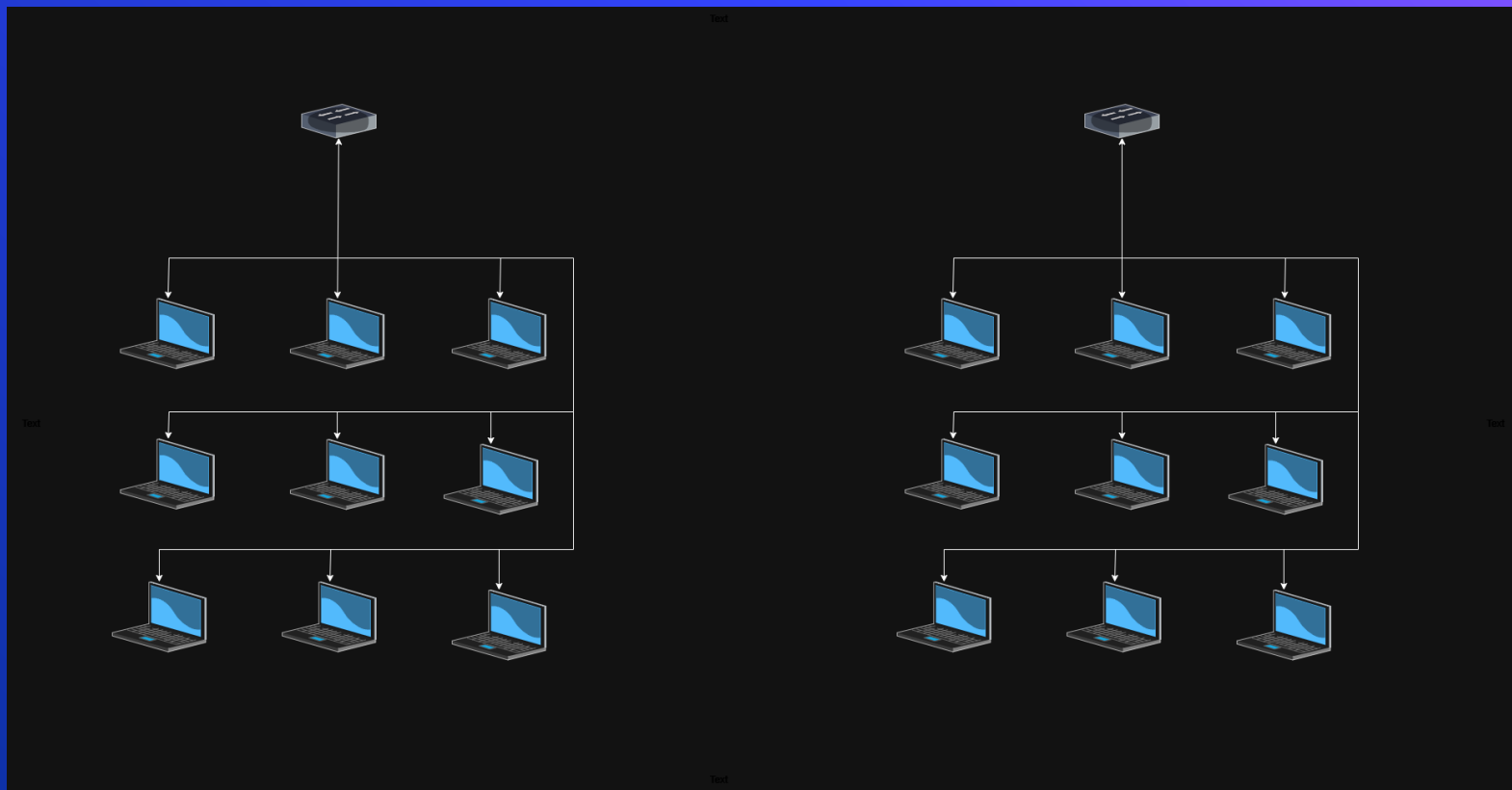
■ Switch layer hardening

- NAC
- Port Level Security
 - Storm control
 - Dynamic ARP Inspection
 - Port activation/deactivation
- Virtual Area Networks (VLANs)

In Class Activity

Packet Polo:

Local Address Resolution Protocol



Break slide

Please return in 15 minutes

Agenda

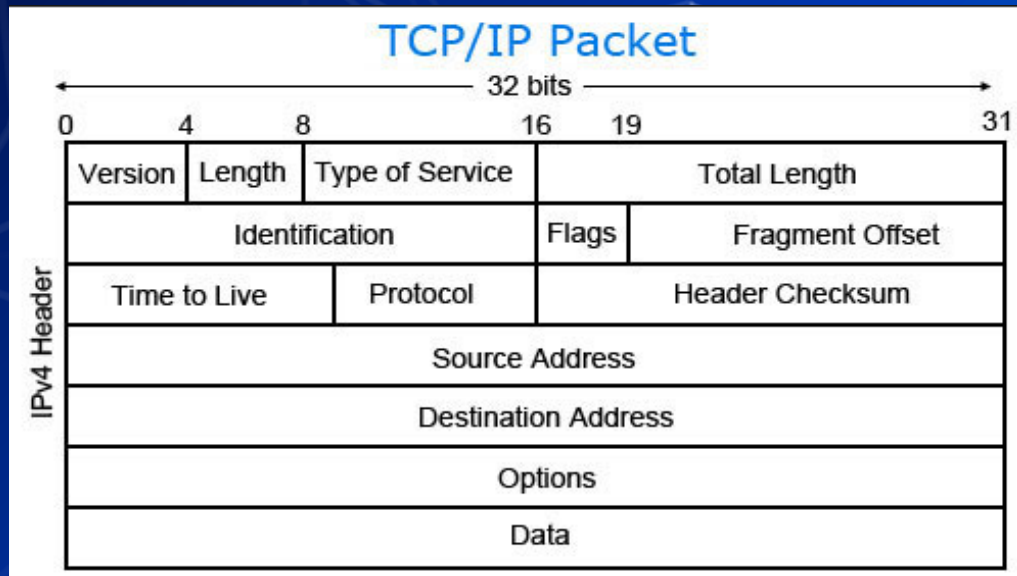
- What's a network?
- OSI Model
 - Physical Layer
 - Datalink Layer
 - Network Layer
- Topologies and IP assignments

OSI Layer 3: Network Layer

- Layer 3: Network Layer
 - Interconnects networks
 - IP Addresses
 - Public and private
 - Requires a network connection to exist
 - 2 different versions of IP addresses
 - IPv4: 10.1.42.15
 - IPv6: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Layer 3 Cont.

- Unit of data:
 - Packets



IPv4 Addresses

- Decimal-octal form (Base 8 bits)
- Separated by octets in range 0-255
 - [octet 1].[octet 2].[octet 3]. [octet 4]
 - Octet 1 - leftmost
 - Octet 4 - rightmost
- For every IP address: **192.168.12.10**
- Some characters represent a network.
 - Some characters represent the **individual device.**

IPv4 Addresses: Designated Private Address Ranges

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

IPv4 Addresses: NAT

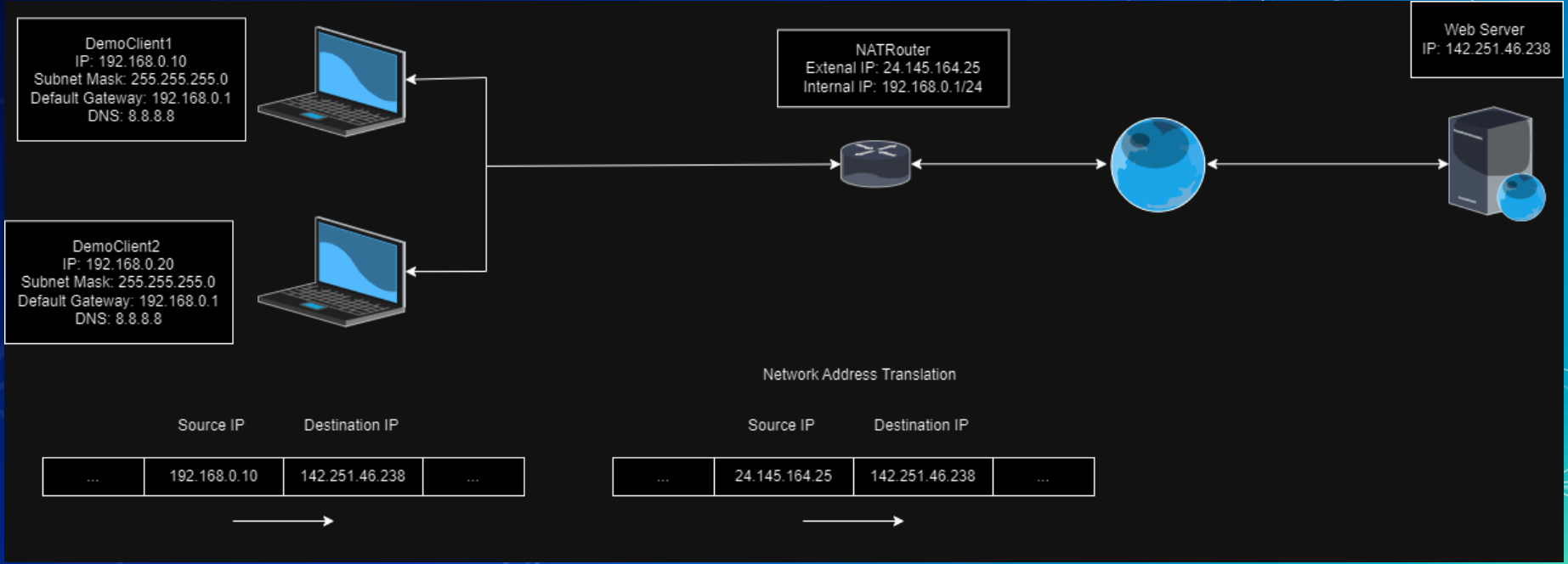
- Network Address Translation (NAT)
 - We would run out of IPv4 address, can only have ~4.3 Billion IPv4 address.
 - Estimated that there was 15.14 Billion IOT devices in 2023
 - How do we save room?

IPv4 Addresses: NAT

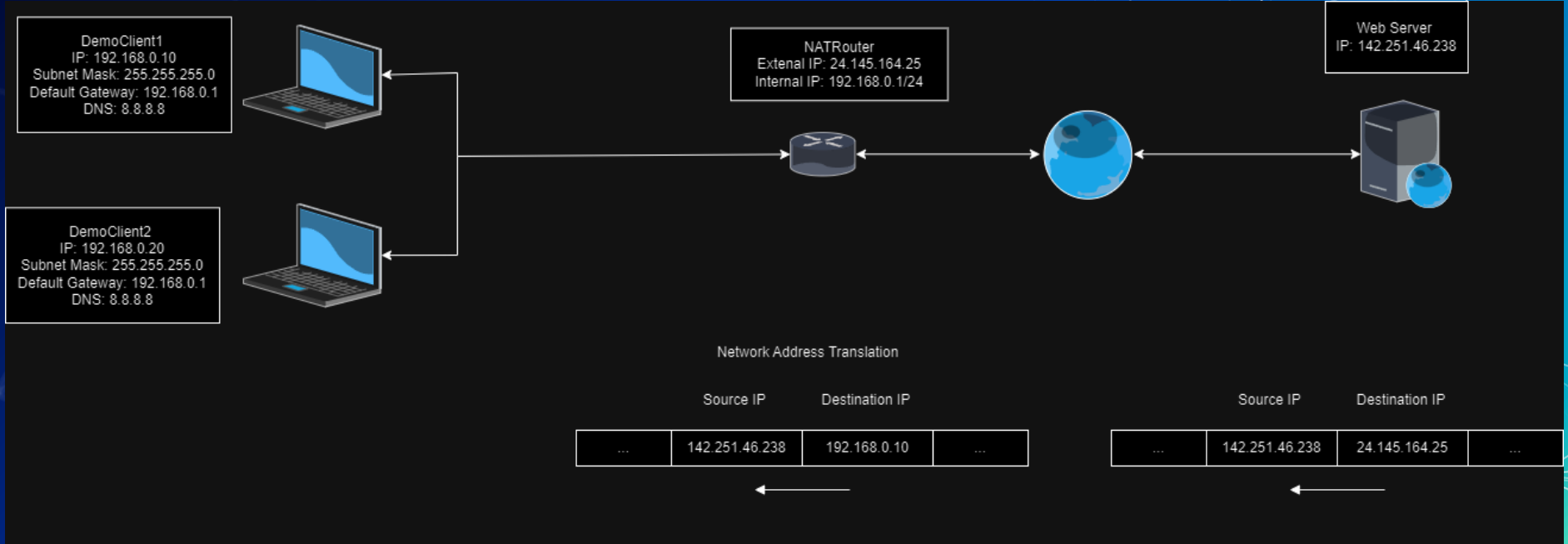
■ Network Address Translation

- We have external and internal IPs
 - External, your Public IP, what the internet sees you as
 - Internal, Private IP, what people on your network see you as
 - Router makes the translation

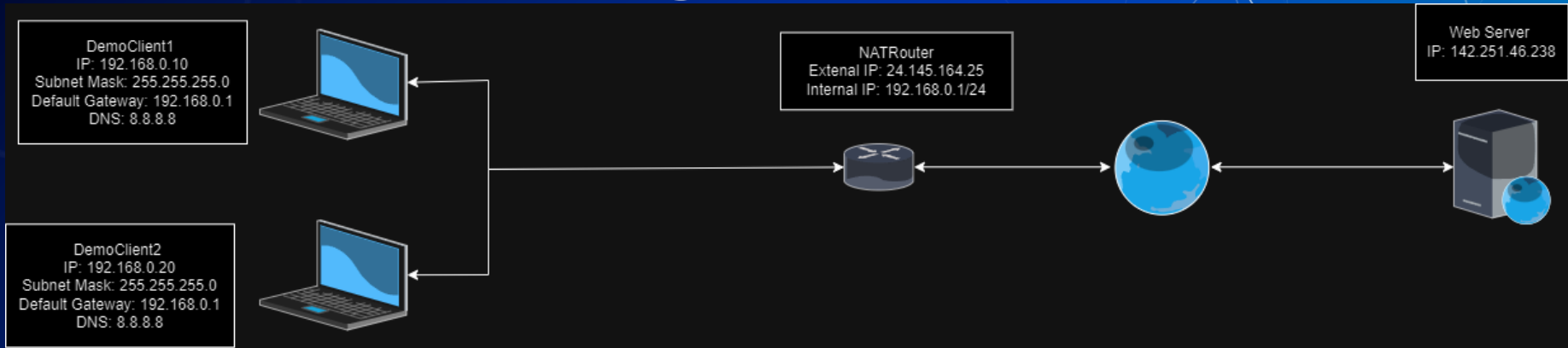
NAT Visualized



The Response

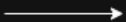


NAT Visualized (again)



Network Address Translation

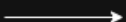
Source IP	Destination IP
...	192.168.0.10
192.168.0.10	142.251.46.238
...	...



Source IP	Destination IP
...	24.145.164.25
24.145.164.25	142.251.46.238
...	...



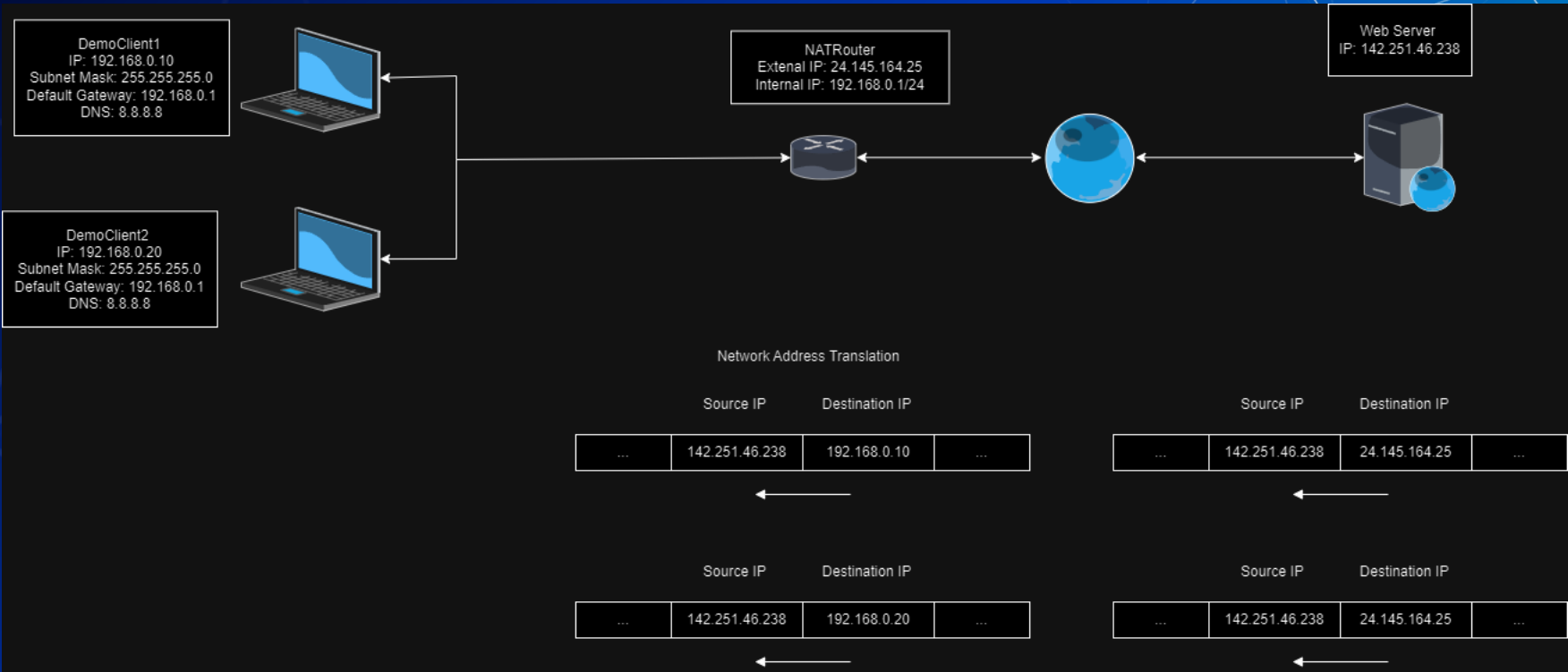
Source IP	Destination IP
...	192.168.0.20
192.168.0.20	142.251.46.238
...	...



Source IP	Destination IP
...	24.145.164.25
24.145.164.25	142.251.46.238
...	...



The Response (again)



Subnet Masks

- The smaller the subnet mask, the more possible addresses
- We can use a calculator to help us
<https://www.calculator.net/ip-subnet-calculator.html>

■ What actually is a subnet?

- IP: 192.168.0.1/24
- Binary: 11000000.10101000.00000000.00000001

■ Some characters represent a network ID

- Some characters represent the subnet ID

■ Some characters represent the host ID (individual device)

	Addresses	Hosts	Netmask
/30	4	2	255.255.255.252
/29	8	6	255.255.255.248
/28	16	14	255.255.255.240
/27	32	30	255.255.255.224
/26	64	62	255.255.255.192
/25	128	126	255.255.255.128
/24	256	254	255.255.255.0
/23	512	510	255.255.254.0
/22	1024	1022	255.255.252.0
/21	2048	2046	255.255.248.0
/20	4096	4094	255.255.240.0
/19	8192	8190	255.255.224.0
/18	16384	16382	255.255.192.0
/17	32768	32766	255.255.128.0
/16	65536	65534	255.255.0.0

What happens when change the size of the subnet?

■ IP: 192.168.0.1/22

○ Binary: 11000000.10101000.00000000.00000001

■ IP 192.168.0.1/26

○ Binary: 11000000.10101000.00000000.00000001

■ This is the only time you will ever look at binary in this class

	Addresses	Hosts	Netmask
/30	4	2	255.255.255.252
/29	8	6	255.255.255.248
/28	16	14	255.255.255.240
/27	32	30	255.255.255.224
/26	64	62	255.255.255.192
/25	128	126	255.255.255.128
/24	256	254	255.255.255.0
/23	512	510	255.255.254.0
/22	1024	1022	255.255.252.0
/21	2048	2046	255.255.248.0
/20	4096	4094	255.255.240.0
/19	8192	8190	255.255.224.0
/18	16384	16382	255.255.192.0
/17	32768	32766	255.255.128.0
/16	65536	65534	255.255.0.0

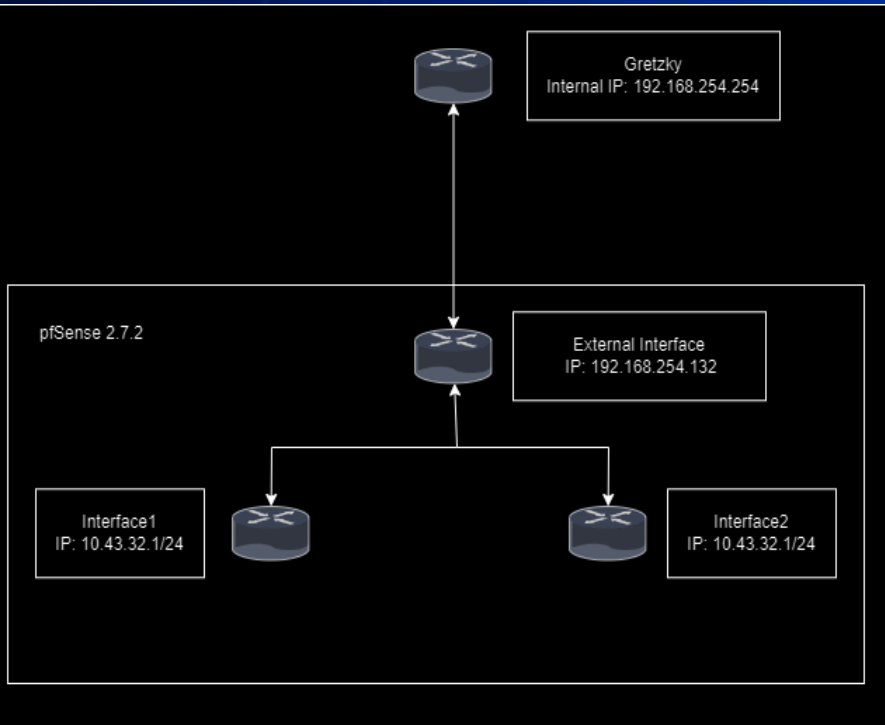
Subnet Masks

- The Subnet indicates how many clients we can have on a network
 - Really neat*
 - Subnets can be written as "255.255.255.0" (decimal-octal) or Classless Inter-Domain Routing (CIDR) notation (e.g., 192.168.12.0/24)
 - /24 gives us 254 different address. No 0 (Network Identifier) or 255 (Broadcast Address)

Static Routes

- A predetermined pathway a packet must travel to reach a specific host or network
 - There is an alternative to static routing e.g., dynamic routing
- When static routes are created they need to specify
 - Destination network or host
 - Subnet of destination
 - Next Hop IP

Static Routes Example

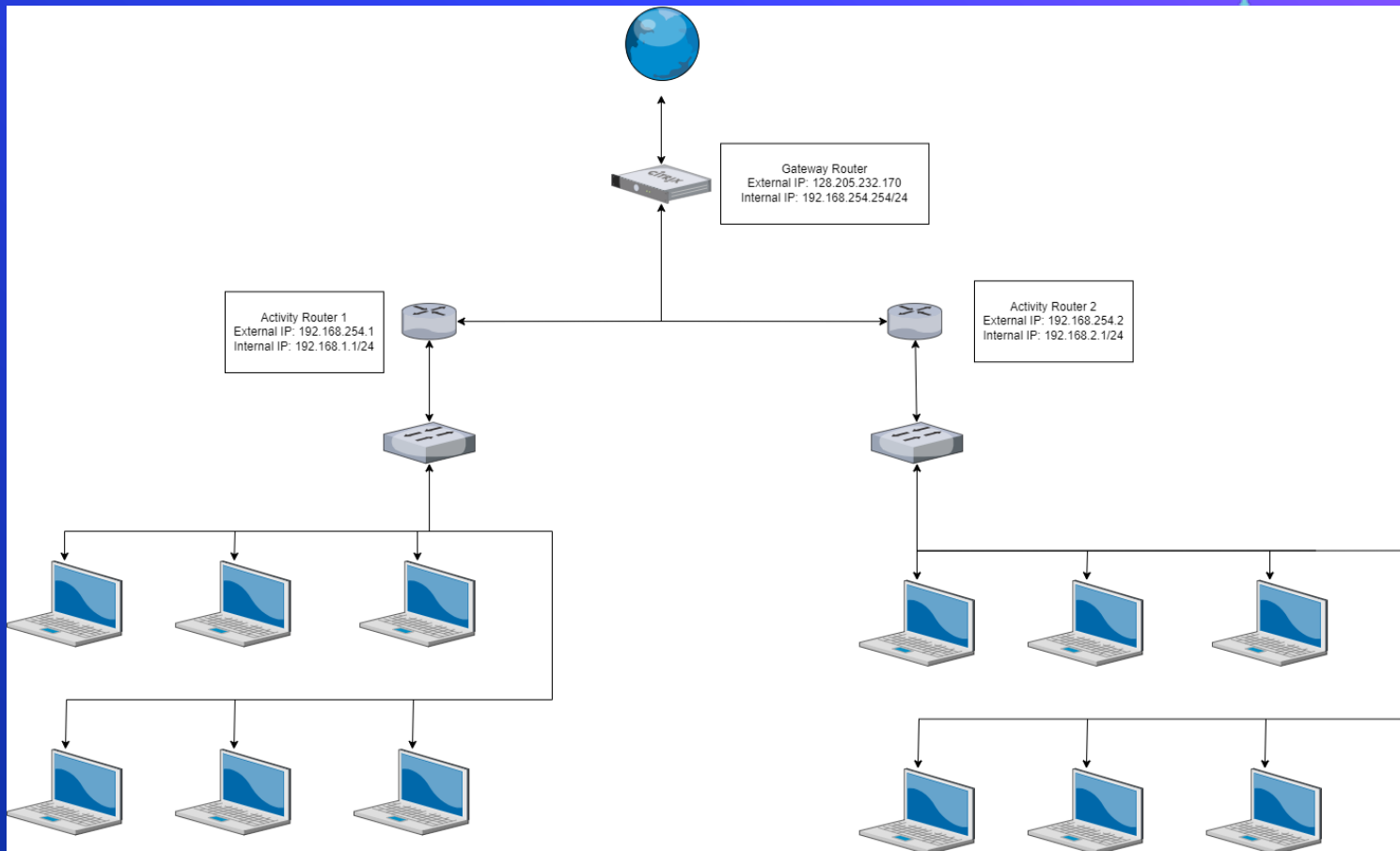


- For Gretchky to be able to communicate with the subnets a static route is necessary, two in this case
- ip route (destination subnet) (subnet mask) (next hop IP)
- ip route 10.42.32.1 255.255.255.0 192.168.254.132
- ip route 10.43.32.1 255.255.255.0 192.168.254.132

In Class Activity

Packet Polo:

Ping



IPv6 Addresses

- Hexadecimal form (Base 16 bits)
- Split into two components; a network and host
- Example: `2001:db8:3333:4444:0000:0000:0007:8888`
 - Shortened: `2001:db8:3333:4444::7:8888`
- Some characters represent a network
 - Some characters represent the **subnet**
- Some characters represent the **individual device**
- Binary if you're interested:
`0010000000000001:0000110110111000:0011001100110011:0100010001000100:0000000000000000:00000000
0000000:000000000000000111:1000100010001000`

Domain Name System or DNS

- A Domain is used to identify a system on the Internet
 - Example@buffalo.edu
 - www.buffalo.edu
 - When we type "dns.google.com", DNS translates to "8.8.8.8"

Dynamic Host Configuration Protocol (DHCP)

- DHCP is a protocol that is used to automatically assign devices IP addresses and network information
- DHCP servers respond to request from devices broadcasting a request for networking information
 - Assigns address based on an assigned pool of IP addresses
 - A DHCP server does not own IP addresses in this pool

Controls Network + Datalink

- Firewalls
- DHCP
- DNS
- NAC (layer 3) port layer security
- Subnetting and network segmentation
- Switch layer controls

Questions?

Break slide

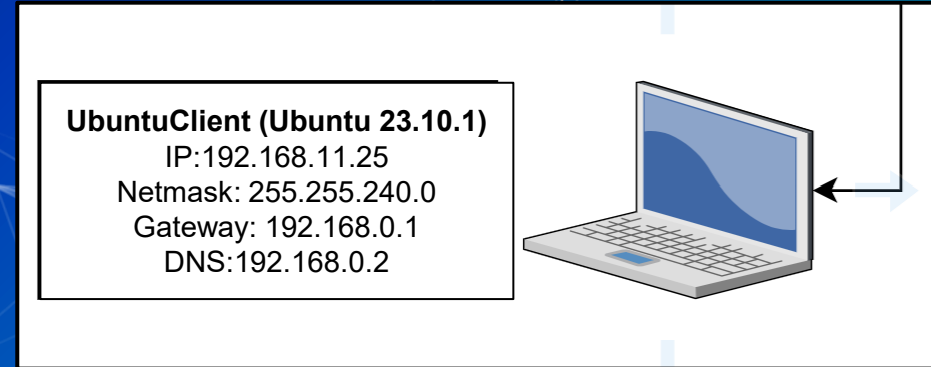
Please return in 10 minutes

Agenda

- What's a network?
- OSI Model
- Topologies and IP assignments

Breakdown of Topology

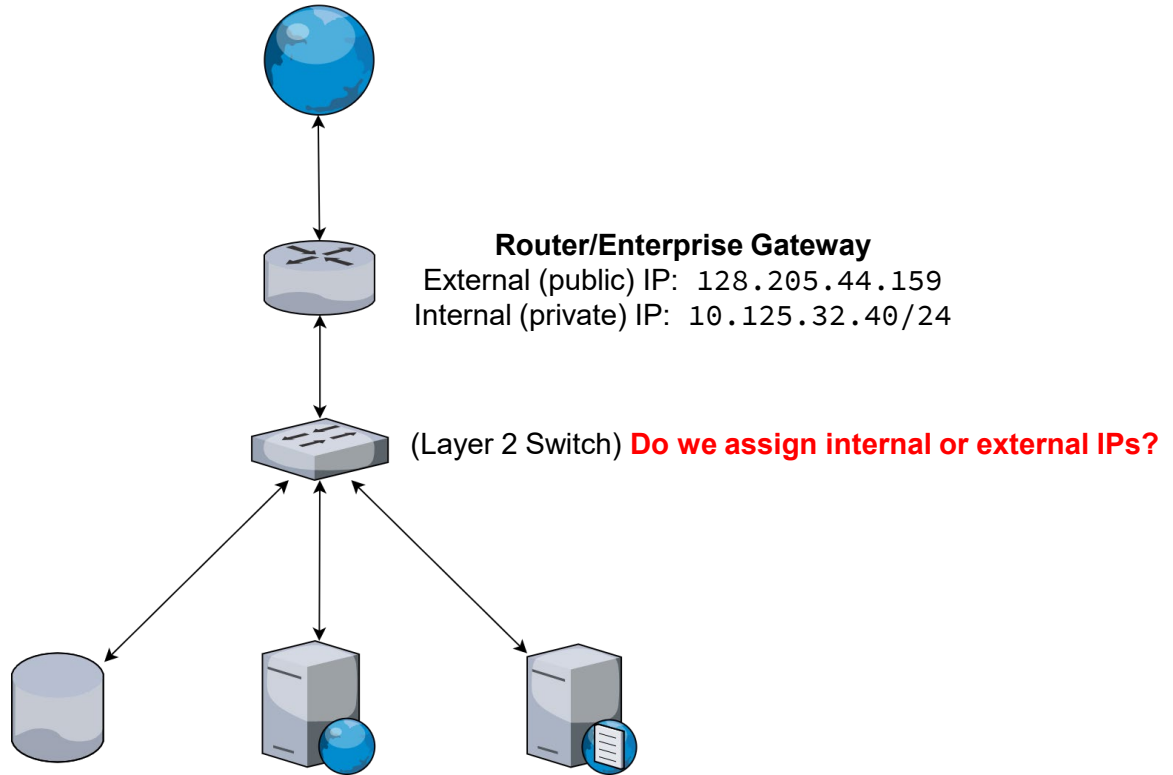
- **IP Address:** Identifies a machine on a network
- **Subnet Mask:** Range of IP addresses allowed on a network
- **Gateway:** A routing device that allows you to connect an external network
- **DNS:** translates domain names (e.g., buffalo.edu) into IP Addresses



In Class Activity

IP Assignment Walkthrough

Example 1



Router/Enterprise Gateway

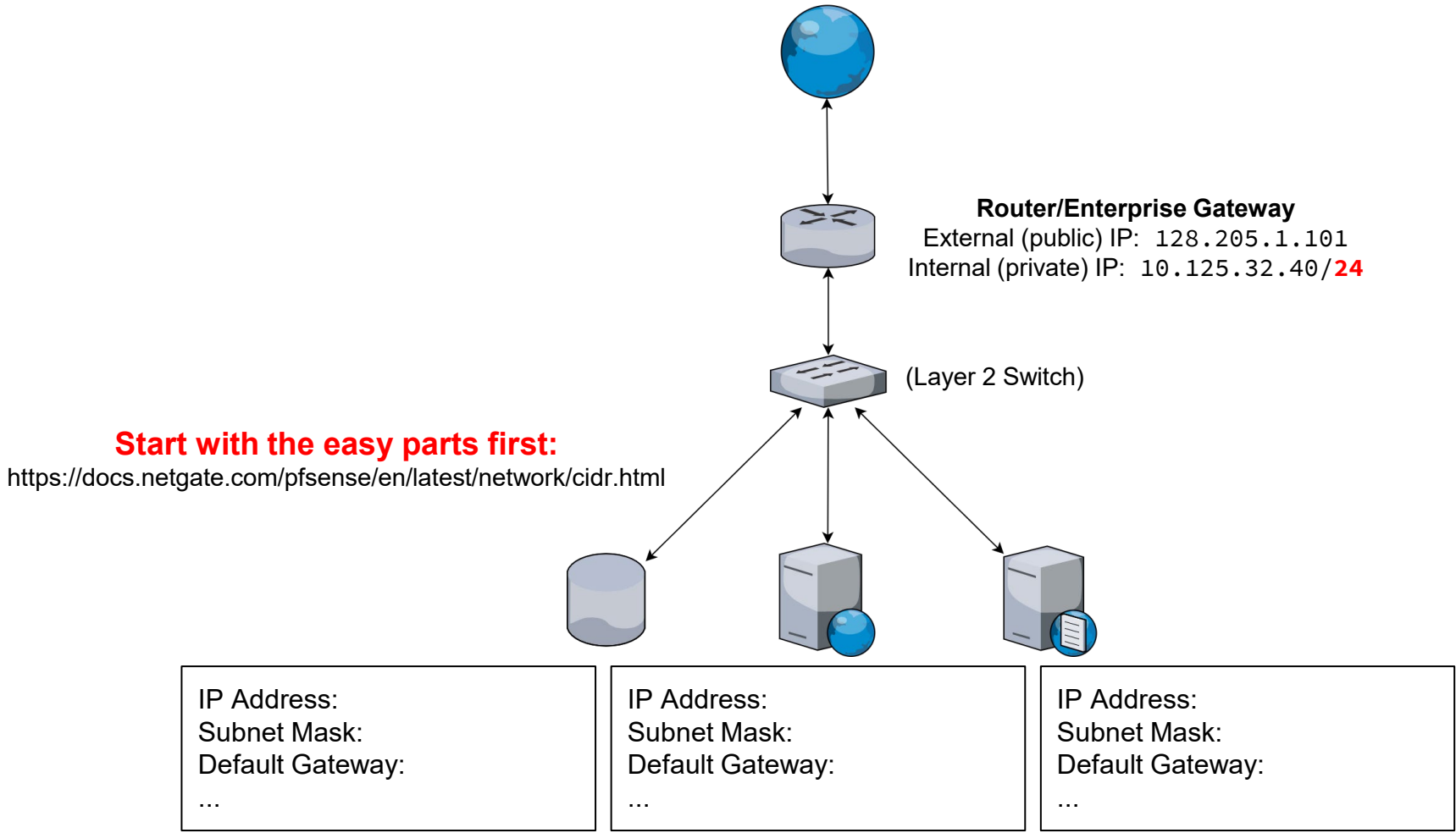
External (public) IP: 128.205.44.159
Internal (private) IP: 10.125.32.40/24

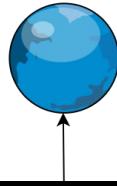
(Layer 2 Switch) **Do we assign internal or external IPs?**

IP Address:
Subnet Mask:
Default Gateway:
...

IP Address:
Subnet Mask:
Default Gateway:
...

IP Address:
Subnet Mask:
Default Gateway:
...





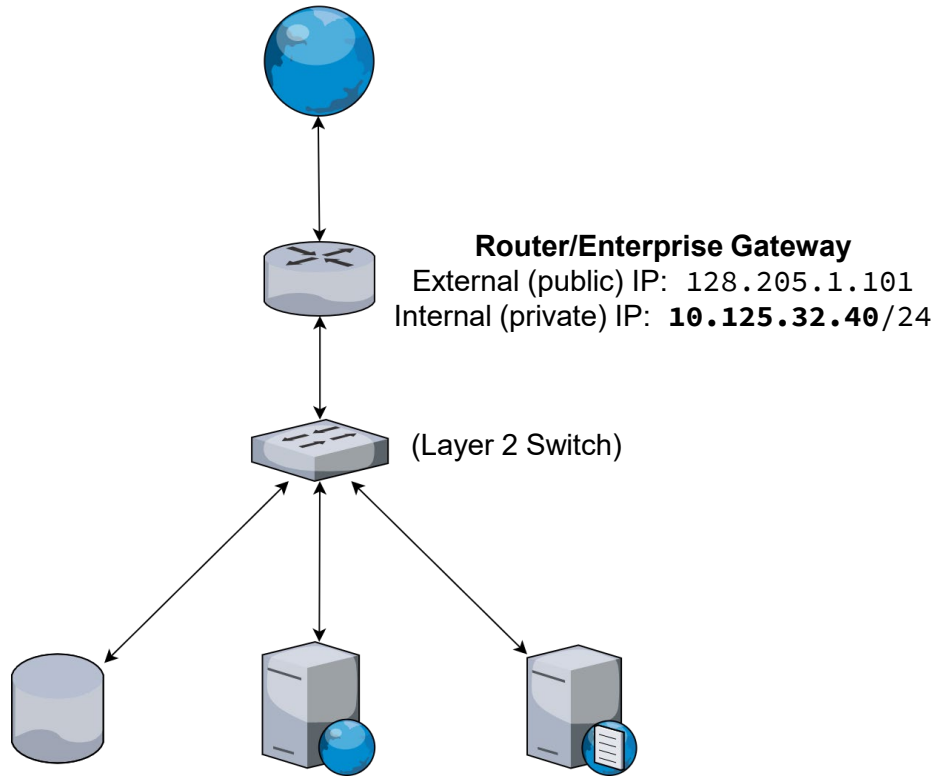
Subnet Mask	CIDR Prefix	Total IP Addresses	Usable IP Addresses	Number of /24 ne
255.255.255.128	/25	128	126	1 half
255.255.255.0	/24	256	254	1
255.255.254.0	/23	512	510	2
255.255.252.0	/22	1024	1022	4
255.255.248.0	/21	2048	2046	8



IP Address:
Subnet Mask: 255.255.255.0
Default Gateway:
...

IP Address:
Subnet Mask: 255.255.255.0
Default Gateway:
...

IP Address:
Subnet Mask: 255.255.255.0
Default Gateway:
...



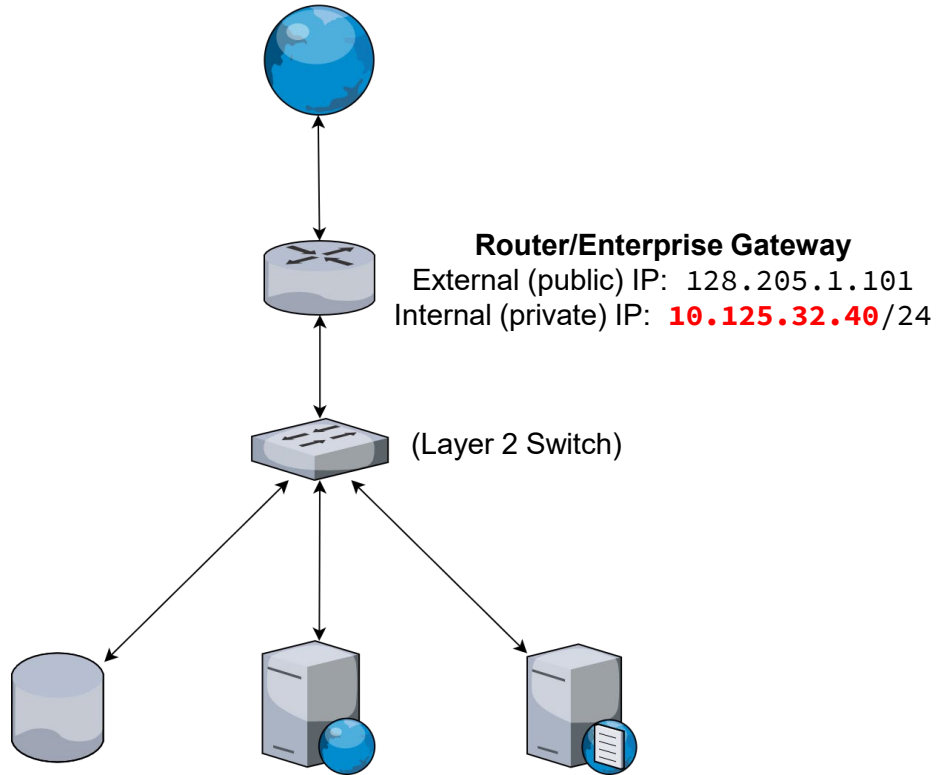
Next easy part:
Default Gateway

IP Address:
Subnet Mask: 255.255.255.0
Default Gateway:
...

IP Address:
Subnet Mask: 255.255.255.0
Default Gateway:
...

IP Address:
Subnet Mask: 255.255.255.0
Default Gateway:
...

Next easy part:
Default Gateway = Internal IP



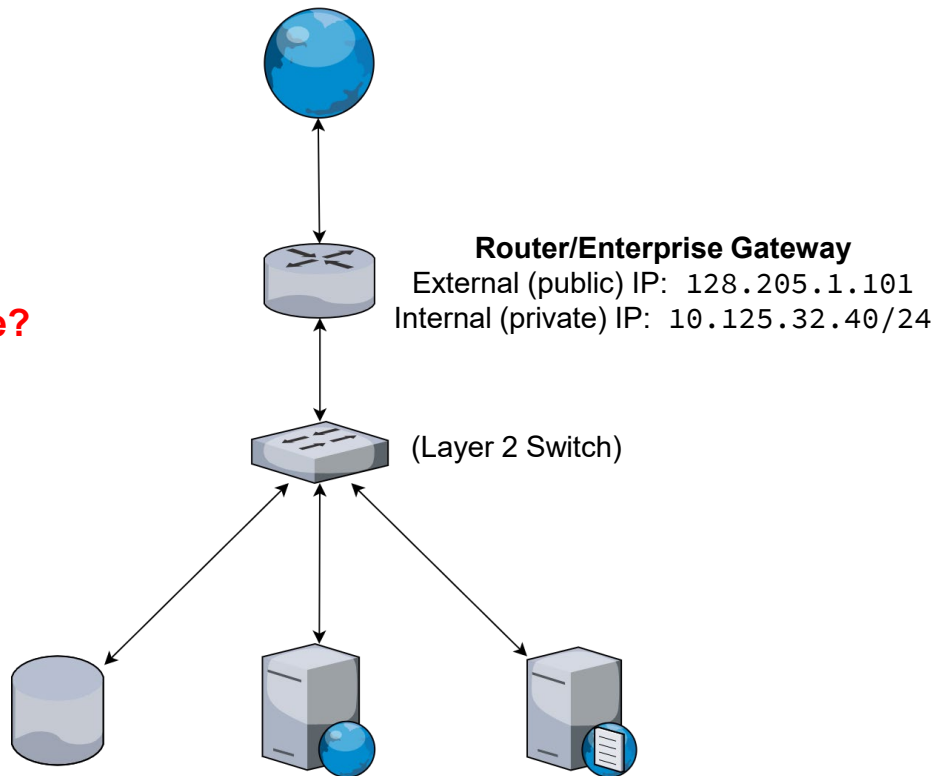
IP Address:
Subnet Mask: 255.255.255.0
Default Gateway: 10.125.32.40
...

IP Address:
Subnet Mask: 255.255.255.0
Default Gateway: 10.125.32.40
...

IP Address:
Subnet Mask: 255.255.255.0
Default Gateway: 10.125.32.40
...

What address space is available?

Consult: <https://www.subnet-calculator.com/>



IP Address:
Subnet Mask: 255.255.255.0
Default Gateway: 10.125.32.40
...

IP Address:
Subnet Mask: 255.255.255.0
Default Gateway: 10.125.32.40
...

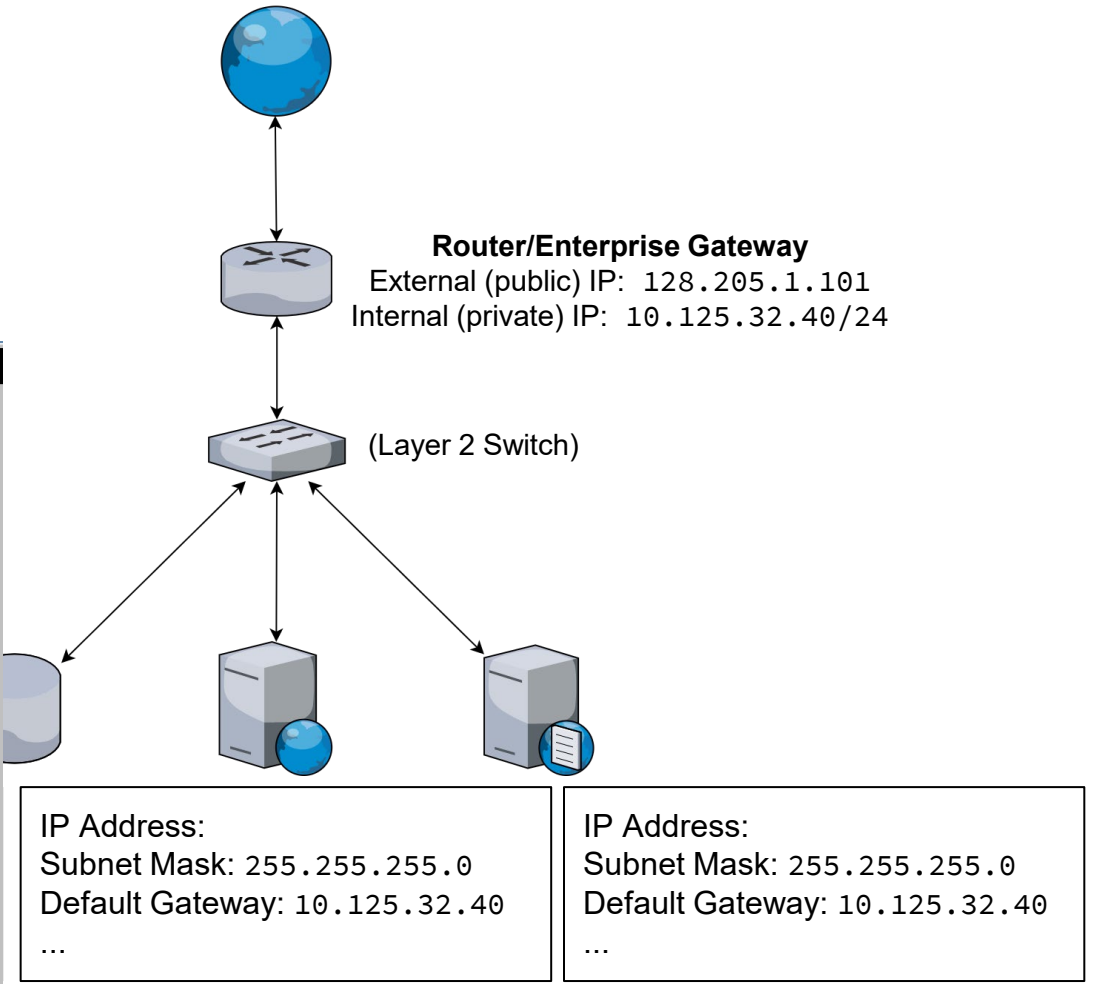
IP Address:
Subnet Mask: 255.255.255.0
Default Gateway: 10.125.32.40
...

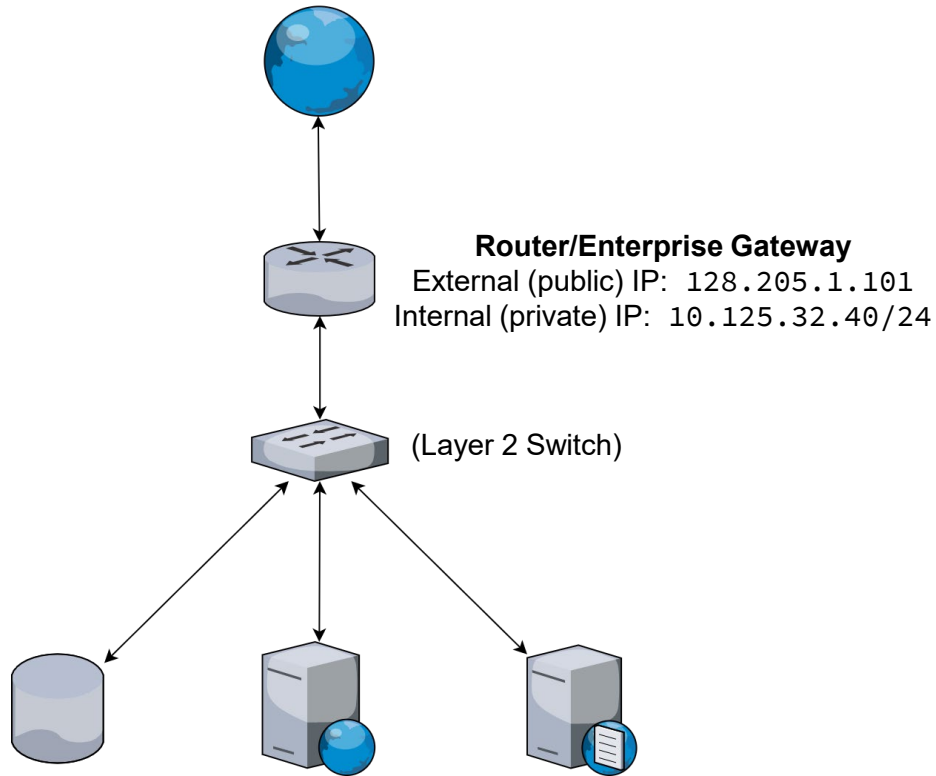
What address space is available?

- Subnet ID and Broadcast Address are unusable

Subnet Calculator

Network Class	First Octet Range
A <input checked="" type="radio"/> B <input type="radio"/> C <input type="radio"/>	1 - 126
IP Address	Hex IP Address
10.125.32.40	0A.7D.20.28
Subnet Mask	Wildcard Mask
255.255.255.0	0.0.0.255
Subnet Bits	Mask Bits
16	24
Maximum Subnets	Hosts per Subnet
65536	254
Host Address Range	
10.125.32.1 - 10.125.32.254	
Subnet ID	Broadcast Address
10.125.32.0	10.125.32.255
Subnet Bitmap	
0nnnnnnn.ssssssss.ssssssss.hhhhhhhh	



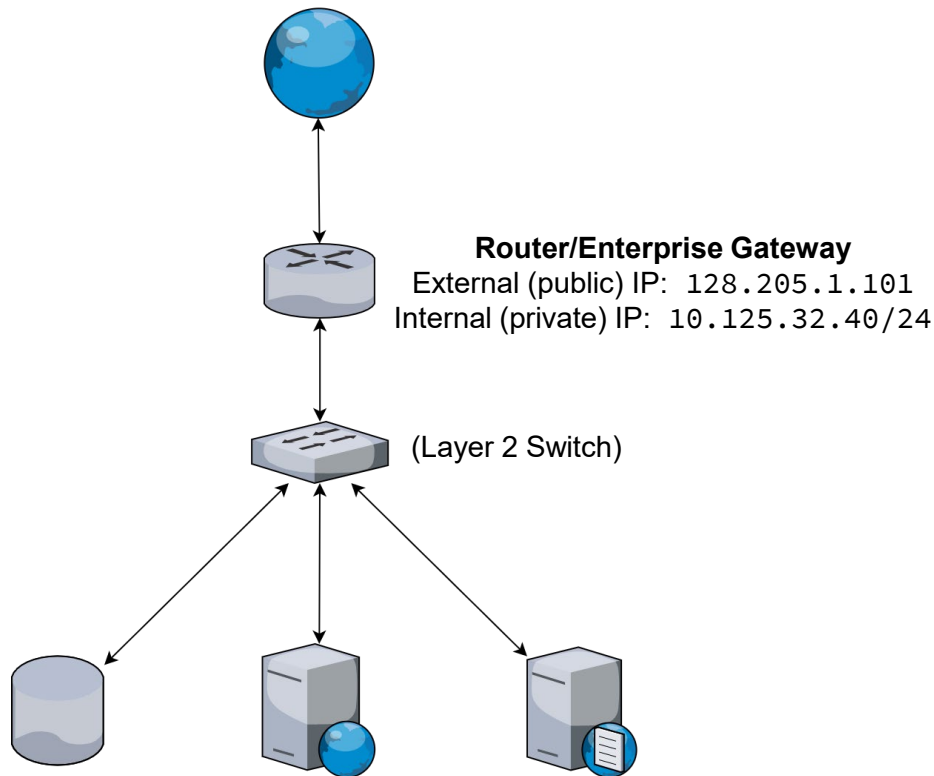


Is this address valid?

IP Address: **10.125.32.0**
Subnet Mask: 255.255.255.0
Default Gateway: 10.125.32.40
...

IP Address: **10.125.32.110**
Subnet Mask: 255.255.255.0
Default Gateway: 10.125.32.40
...

IP Address: **10.125.32.210**
Subnet Mask: 255.255.255.0
Default Gateway: 10.125.32.40
...



IP Address: **10.125.32.14**
Subnet Mask: 255.255.255.0
Default Gateway: 10.125.32.40
...

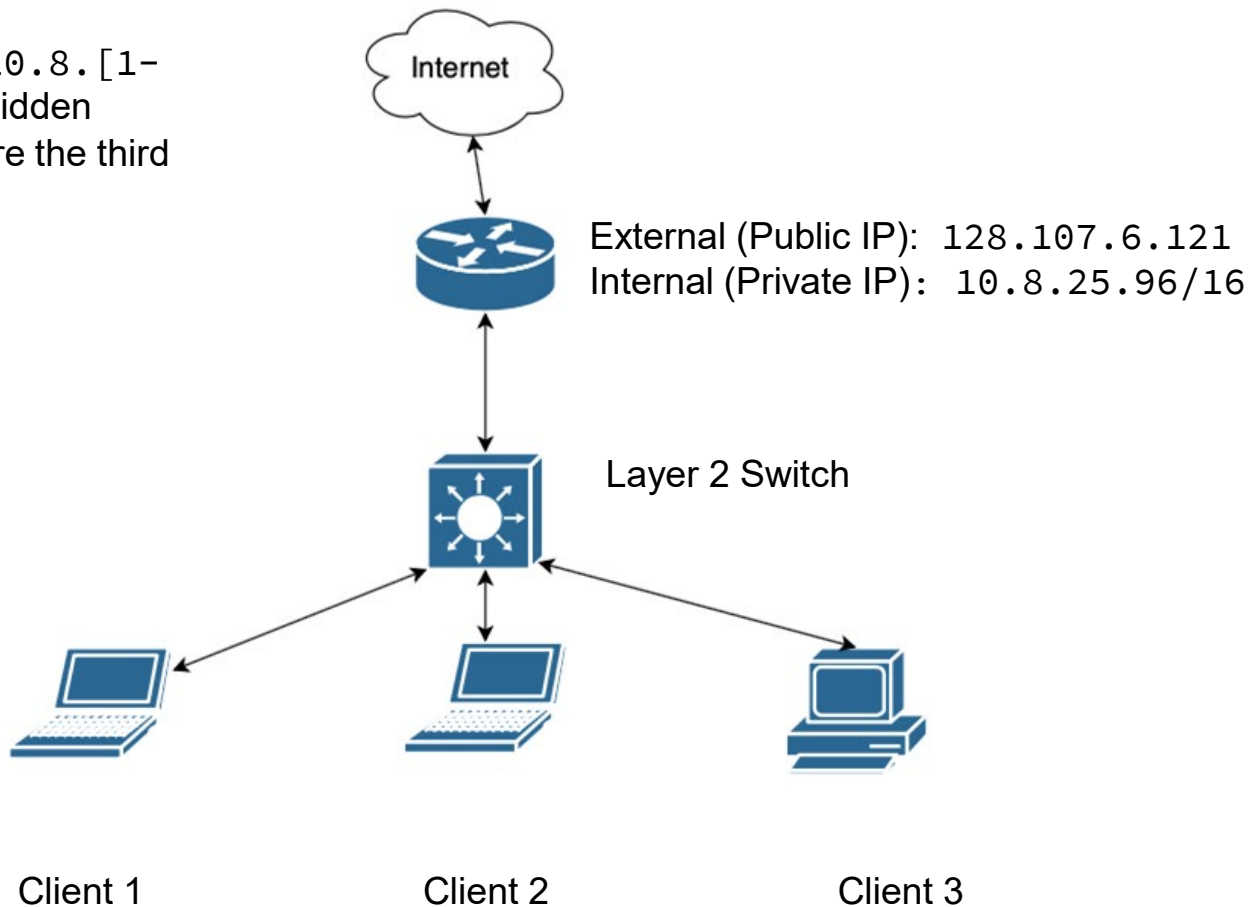
IP Address: **10.125.32.110**
Subnet Mask: 255.255.255.0
Default Gateway: 10.125.32.40
...

IP Address: **10.125.32.210**
Subnet Mask: 255.255.255.0
Default Gateway: 10.125.32.40
...

Example 2

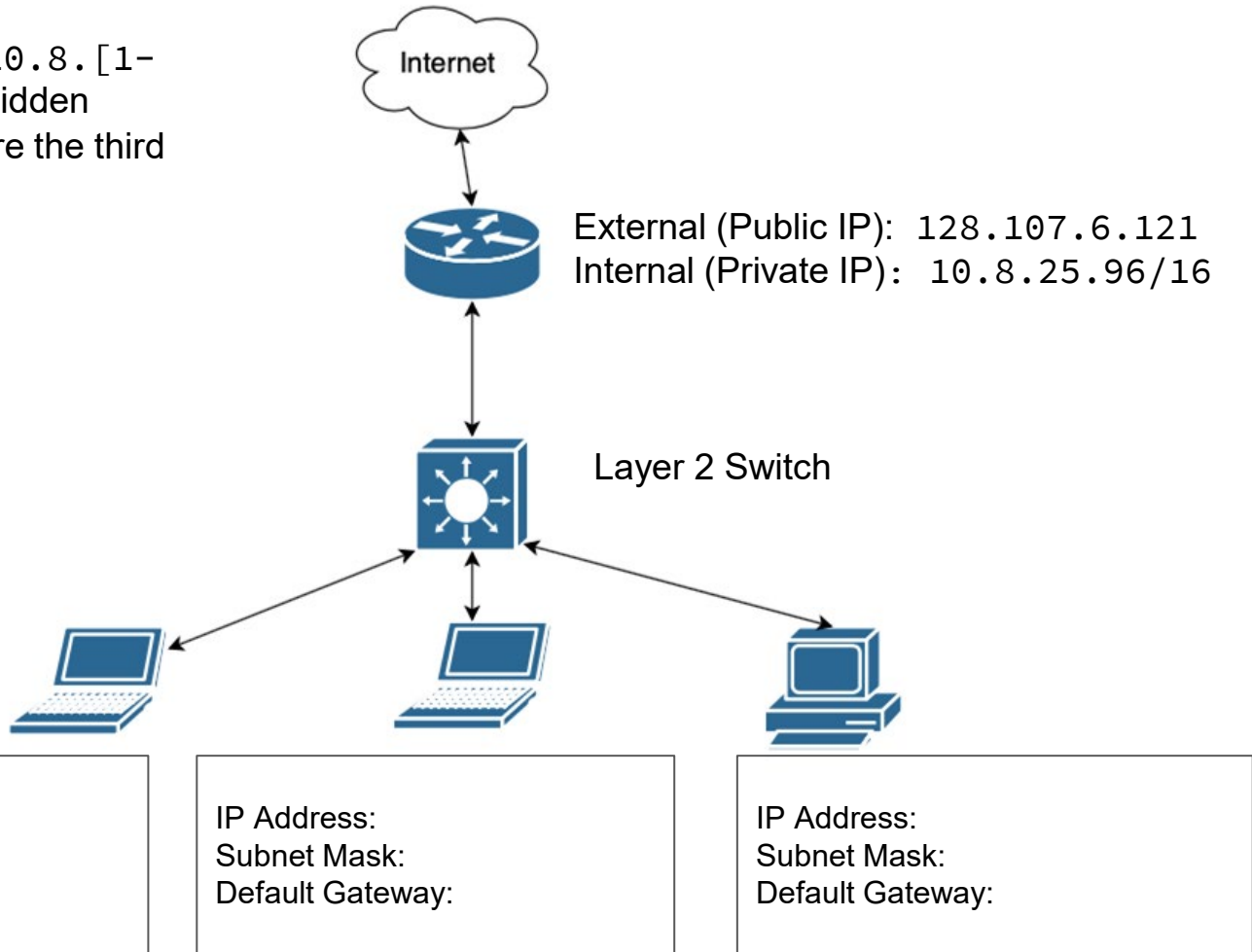
Rules:

- IP address range 10.8.[1-24].[any] is forbidden
- No clients can share the third octet



Rules:

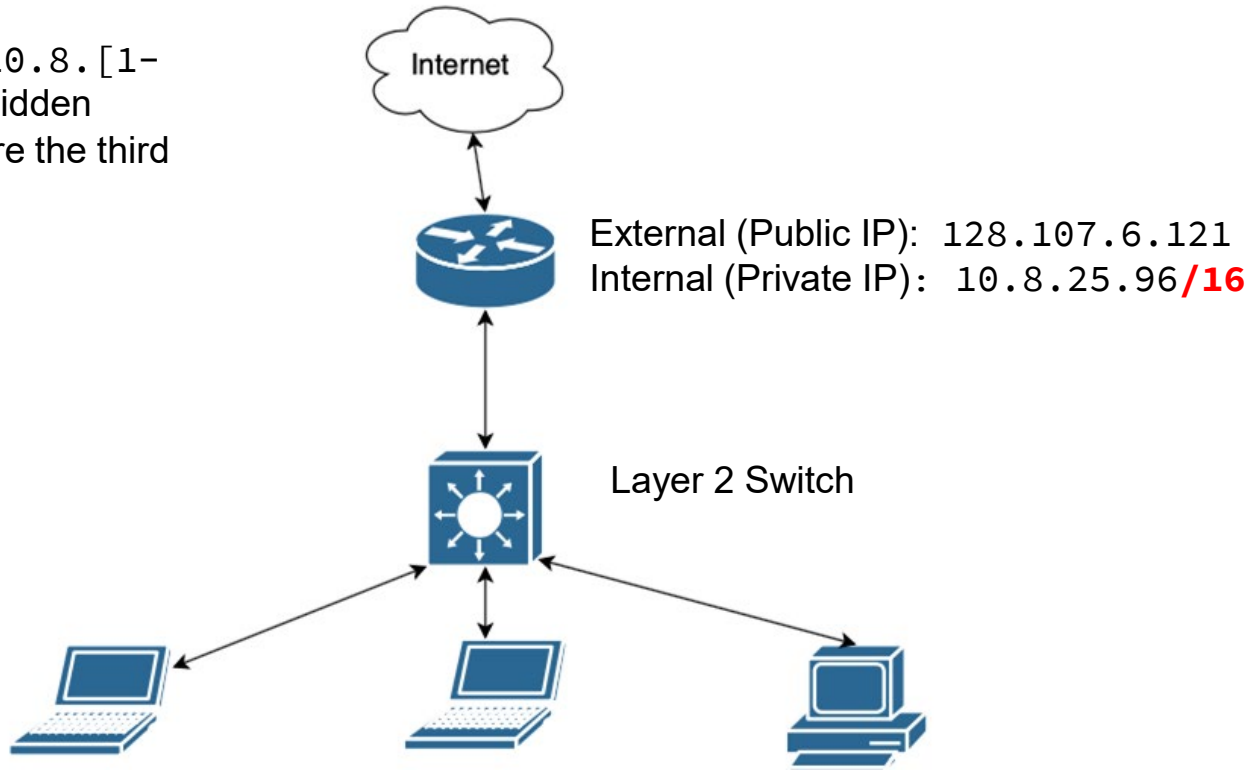
- IP address range 10.8.[1-24].[any] is forbidden
- No clients can share the third octet



Once again, let's start easy. What are the subnet masks for our 3 clients?

Rules:

- IP address range 10.8.[1-24].[any] is forbidden
- No clients can share the third octet

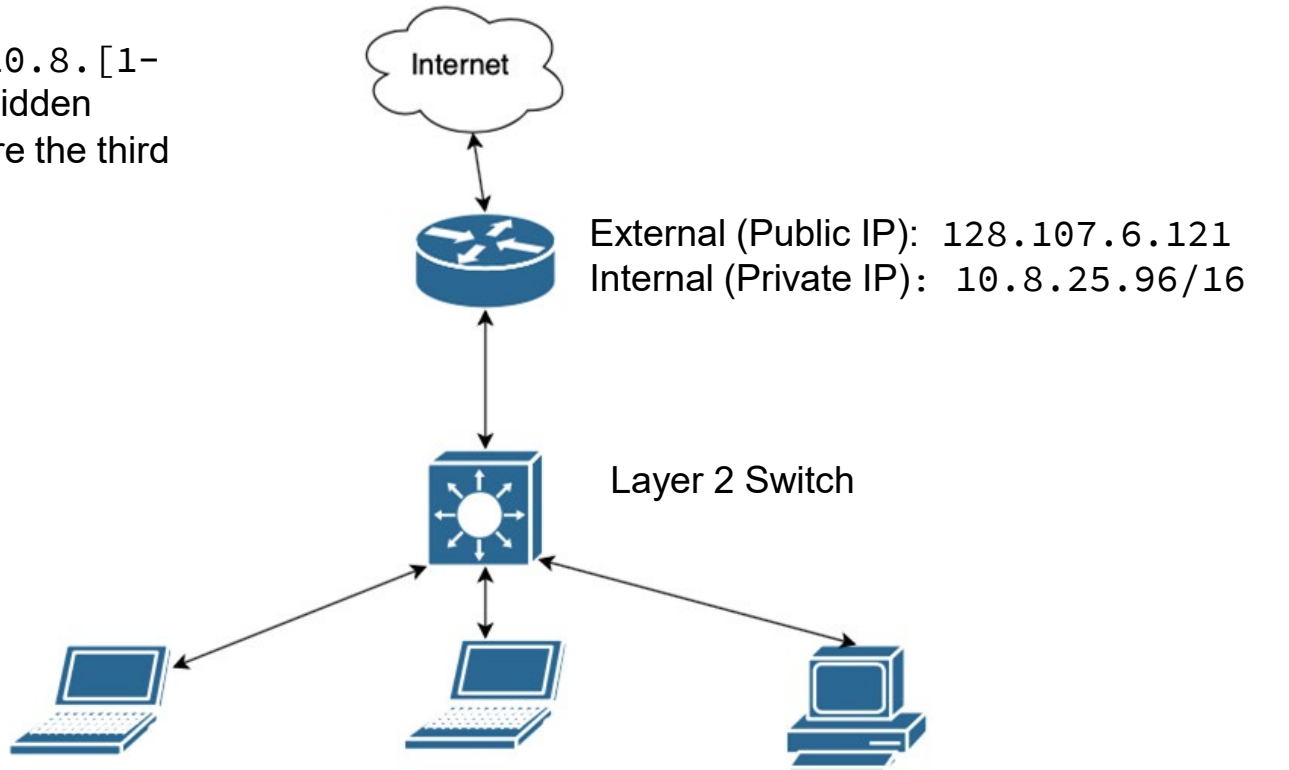


Once again, let's start easy. What are the subnet masks for our 3 clients?

Subnet Mask	CIDR Prefix	Total IP Addresses	Usable IP Addresses	Number of /24 netw
255.255.0.0	/16	65,536	65,534	256

Rules:

- IP address range 10.8.[1-24].[any] is forbidden
- No clients can share the third octet



Once again, let's start easy. What are the subnet masks for our 3 clients?

IP Address:
Subnet Mask: 255.255.0.0
Default Gateway:

IP Address:
Subnet Mask: 255.255.0.0
Default Gateway:

IP Address:
Subnet Mask: 255.255.0.0
Default Gateway:

Rules:

- IP address range 10.8.[1-24].[any] is forbidden
- No clients can share the third octet

What is our default gateway?



External (Public IP): 128.107.6.121
Internal (Private IP): 10.8.25.96/16



Layer 2 Switch



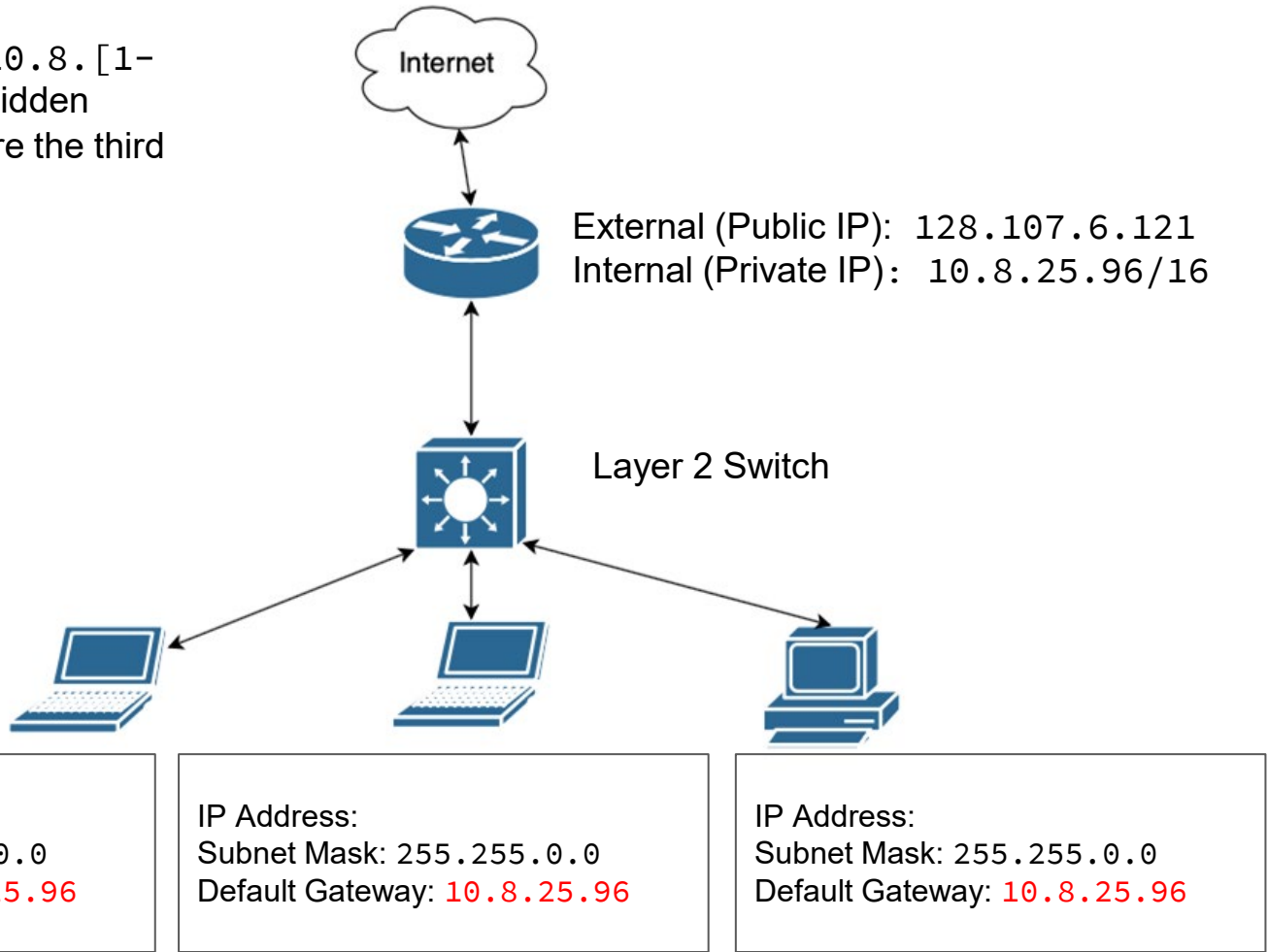
IP Address:
Subnet Mask: 255.255.0.0
Default Gateway:

IP Address:
Subnet Mask: 255.255.0.0
Default Gateway:

IP Address:
Subnet Mask: 255.255.0.0
Default Gateway:

Rules:

- IP address range 10.8.[1-24].[any] is forbidden
- No clients can share the third octet



Rules:

- IP address range 10.8.[1-24].[any] is forbidden
- No clients can share the third octet

What is our IP Address?



External (Public IP): 128.107.6.121
Internal (Private IP): 10.8.25.96/16



Layer 2 Switch



IP Address:
Subnet Mask: 255.255.0.0
Default Gateway: 10.8.25.96

IP Address:
Subnet Mask: 255.255.0.0
Default Gateway: 10.8.25.96

Subnet Calculator	
Network Class A <input checked="" type="radio"/> B <input type="radio"/> C <input type="radio"/>	First Octet Range 1 - 126
IP Address 10.8.25.96	Hex IP Address 0A.08.19.60
Subnet Mask 255.255.0.0	Wildcard Mask 0.0.255.255
Subnet Bits 8	Mask Bits 16
Maximum Subnets 256	Hosts per Subnet 65534
Host Address Range 10.8.0.1 - 10.8.255.254	
Subnet ID 10.8.0.0	Broadcast Address 10.8.255.255
Subnet Bitmap 0nnnnnnn.ssssssss.hhhhhhhh.hhhhhhhh	

Rules:

- IP address range 10.8.[1-24].[any] is forbidden
- No clients can share the third octet



External (Public IP): 128.107.6.121
Internal (Private IP): 10.8.25.96/16



Layer 2 Switch



Is this a valid IP address?

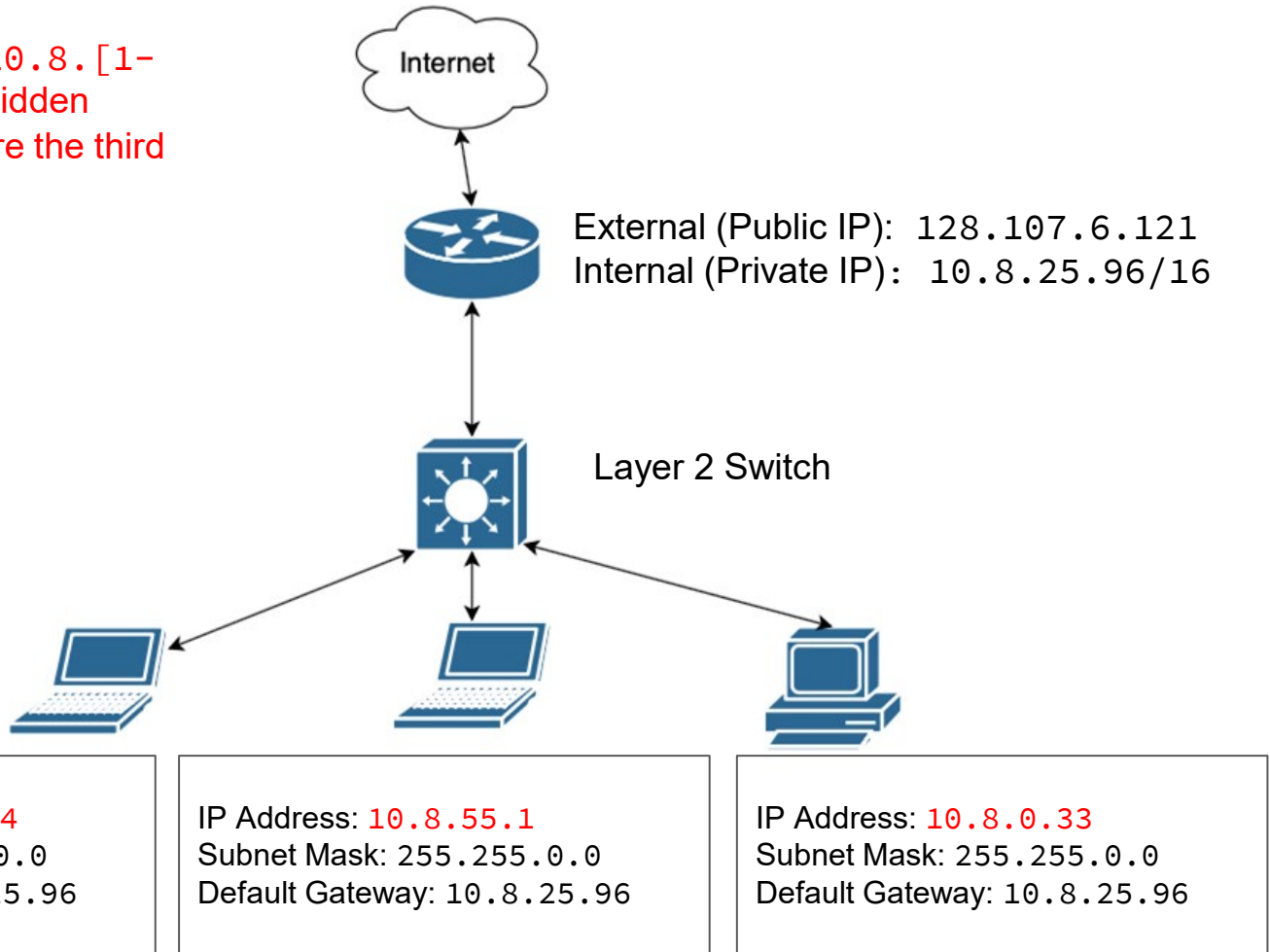
IP Address: 10.8.0.254
Subnet Mask: 255.255.0.0
Default Gateway: 10.8.25.96

IP Address: 10.8.55.1
Subnet Mask: 255.255.0.0
Default Gateway: 10.8.25.96

IP Address: 10.8.0.33
Subnet Mask: 255.255.0.0
Default Gateway: 10.8.25.96

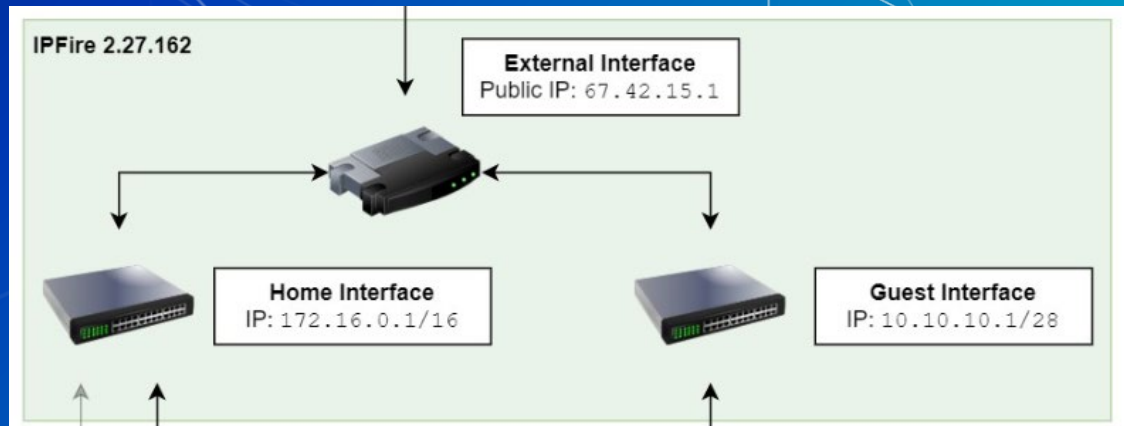
Rules:

- IP address range 10.8.[1-24].[any] is forbidden
- No clients can share the third octet



Composite Network Device

- When one hardware device manages more than one network interface
- Style guide has a great explanation and example



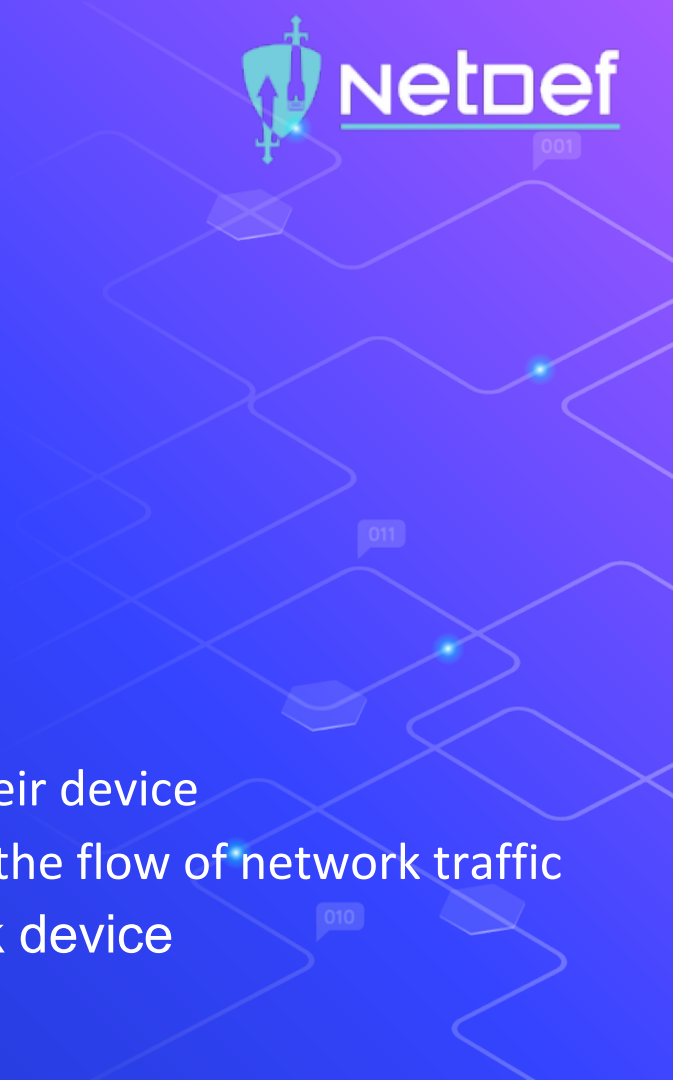
In Class Activity

Network Topology Walkthrough

Creating a Network Topology

⬡ In draw.io:

- ⬡ Open a new diagram
- ⬡ Click on + More Shapes
- ⬡ Select one of the following
 - ⬡ Clipart, Cisco19, Citrix
- ⬡ Click on Apply
- ⬡ Expand your selection from the dropdown list
- ⬡ Drag and drop the figures corresponding to their device
- ⬡ Connect each device with an arrow indicating the flow of network traffic
- ⬡ Select a Rectangle to label each network device
- ⬡ See the Topology Style Guide for more details



List of devices to be included on the topology:

Name (network devices)	Operating System	IP
Demorouter	pfSense 2.7.2	74.110.50.221
demointerface1		10.50.40.1/20
demointerface2		10.60.40.1/20

Name (endpoints)	Operating System	IP	Subnet Mask	DNS	Default Gateway
Demo1	Ubuntu 23.10	?	?	8.8.8.8	10.50.40.1
Demo2	Windows 10	?	?	8.8.8.8	10.60.40.1

Summary and Wrap-up

Today's achievements:

- We learned how **network devices** work with network traffic.
- We reviewed the components of a network **topology**.
- We examined the OSI networking **layers** 1-3.
- We explored why **layering** matters.

Homework 02

Parting questions

Now is the time!

Class dismissed

See you next week!