Networking II

UBNetDef SysSec, Spring 2024
Week 14
Lead Presenter: Ray Harenza

Learning Objectives

- Advanced networking topics configuration
  - VLANs, Static Routes, etc…
- Interacting with router and switch CLIs
- Routing Protocols
- Quality of Service
- High availability technology configuration
- Wireless networking

Agenda - Week 11

1. **Networking**
2. High Availability
3. Network Architecture
4. Wireless Technologies

Networking

Networking point-of-entry

OSI Model

- Language throughout this presentation will be referring to layers of the OSI Model
  - Though almost all of it will be referring to only layers 1-4
- Does anyone remember what device usually exists only at layer 2?
  - What about layer 3?
- What is the data unit at layer 2?
  - What about layer 3?

Subnets

- Logical network divisions
  - Often seen in two notations
    - 192.168.0.1/24
    - 192.168.0.1 255.255.255.0
  - What would the broadcast address be in this subnet?
  - What about the network identifier?

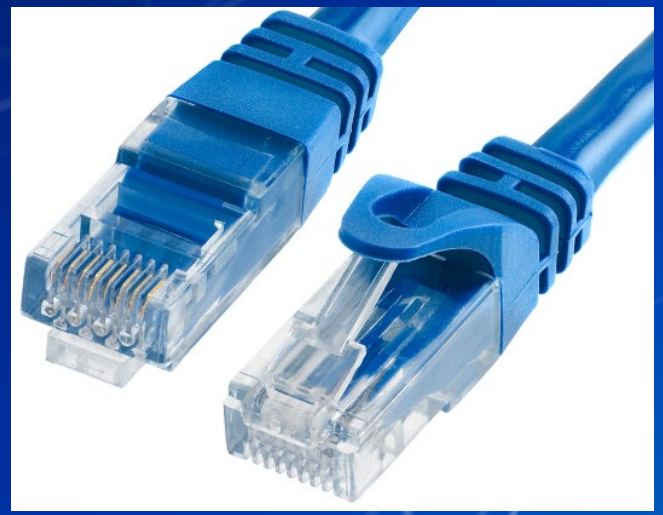
	Addresses	Hosts	Netmask
/30	4	2	255.255.255.252
/29	8	6	255.255.255.248
/28	16	14	255.255.255.240
/27	32	30	255.255.255.224
/26	64	62	255.255.255.192
/25	128	126	255.255.255.128
/24	256	254	255.255.255.0
/23	512	510	255.255.254.0
/22	1024	1022	255.255.252.0
/21	2048	2046	255.255.248.0
/20	4096	4094	255.255.240.0
/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

Networking devices

- Switches
- Routers
- Firewalls
- Endpoints
- Servers
- A lot more

Interfaces

- When referring to interfaces in this lecture it will very often be referring to RJ-45 ports on network devices
  - You are all very likely familiar with what a RJ-45 port is
    - Ethernet ports!



What's unique about networking devices operating systems?

- Almost always propriety operating systems created by the manufacturer
  - Examples include:
    - Cisco IOS
    - FortiOS
    - PAN-OS
  - Not always though!
    - pfSense
    - Most other FreeBSD, OpenBSD, or Linux-Based operating systems
- This means that command syntax, specific steps and capabilities will differ between networking devices between different manufactures
  - Specific protocols may also be propriety
    - Very common with Cisco devices

Network Device CLI

```
Router>
```

- User EXEC mode
  - This is the default when first entering a router
  - It always has the hostname followed by >
  - This permission level cannot make changes to the configuration and has limited read access

```
Router>enable
Router#
```

- Privileged EXEC mode
  - This mode is entered by using the **enable** command
  - This mode allows for changing some configurations of the router and to restart the device

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

- It is further possible to enter configuration mode
  - This can be done with the command **conf terminal**
  - This mode will allow for configuration changes

Startup vs Running Config

- Cisco routers have two separate config files on the device
- Running–config
  - The active configuration file on the device, this is what is edited when you are running commands in the CLI
- Startup-config
  - This is loaded upon restart of the device

Show running-config

- Notice this needs privileged-EXEC mode to run

```
Router#show running-config
Building configuration...

Current configuration : 702 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
```

Show startup-config

- Unless a running configuration is saved a router will load a default configuration, not the startup configuration

```
Router#show startup-config
startup-config is not present
Router#
```

Saving a configuration

- This can be done by using the command:
  - **copy run start**
    - Shortcuts in commands on cisco routers only need to be long enough so that only one command can be finished from the letters typed
  - This is in reality:
    - **copy running-config startup-config**
    - Shortened:
      - **cp run start**

```
Router#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
Router#show startup-con
Router#show startup-config
Using 702 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
```

Network Device Security

- It is possible to use the command **enable password password**
  - This makes it so that it is required to enter a password when going into privileged EXEC mode
- The password is not encrypted in the config files by default
  - It is necessary to run the command **service password-encryption** to encrypt the stored password

```
Current configuration : 746 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
!
!
enable password syssec
!
```

```
Current configuration : 753 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
!
!
enable password 7 0832555D1A1C06
!
```

In Class Activity

Intro to Switch/Router CLI demo

In Class Activity

Packet Tracer

Packet Tracer

- Commands you may find useful:
  - **enable**
  - **config terminal**
  - **interface**
  - **show ip interface brief**
  - **ip address**
  - **no shutdown**
  - **hostname**

Packet Tracer in Class Activity

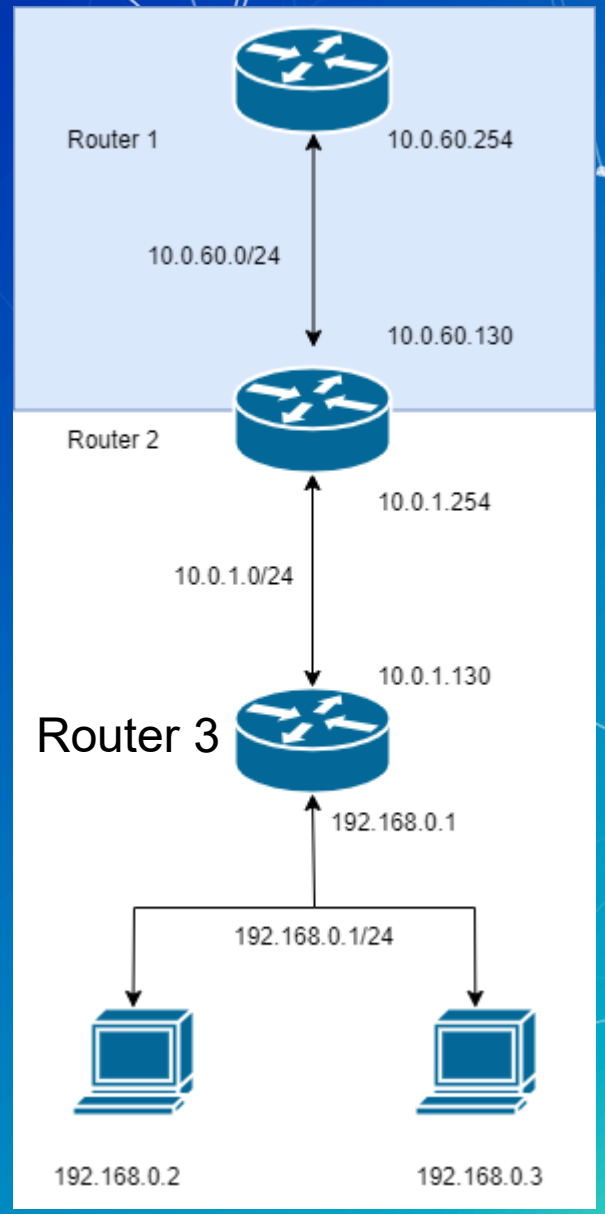
- In your team folder you have a new VM named “PacketTracer”
  - Sign onto this VM with the credentials student:Change.me!
  - On the desktop there is a folder named “Packet Tracer Files”
  - Open the file named cli.pkt
- Connect the devices together using Copper Straight-Through wires
- Configure the IP addresses/subnet mask on each PC
  - Set the gateway to the last useable address
- Configure the interface the switch is connected to on the router
  - Make sure the IP address matches the gateway configured on the PCs
- Open the command prompt on the PCs and test pinging other network devices

Static Routing

- Routers know only how to reach its own IP addresses and destinations in it's directly connected networks
  - This implies that networks more than one jump away need to be specified or discovered in some way
    - Static routing is that process of explicitly specifying networks
    - Dynamic routing allows for discovery with dynamic routing protocols
      - More on this after the in class activity

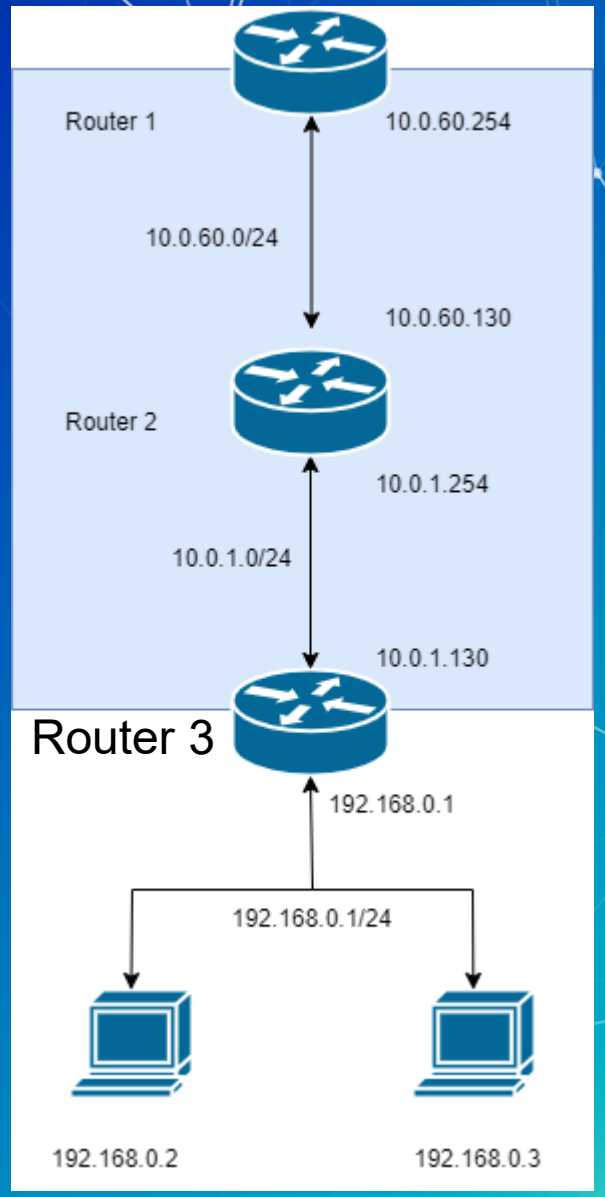
Static Routing Cont.

- Router 1 only knows the network:
  - 10.0.60.0/24
- Router 1 does not know the networks:
  - 10.0.1.0/24
  - 192.168.0.1/24



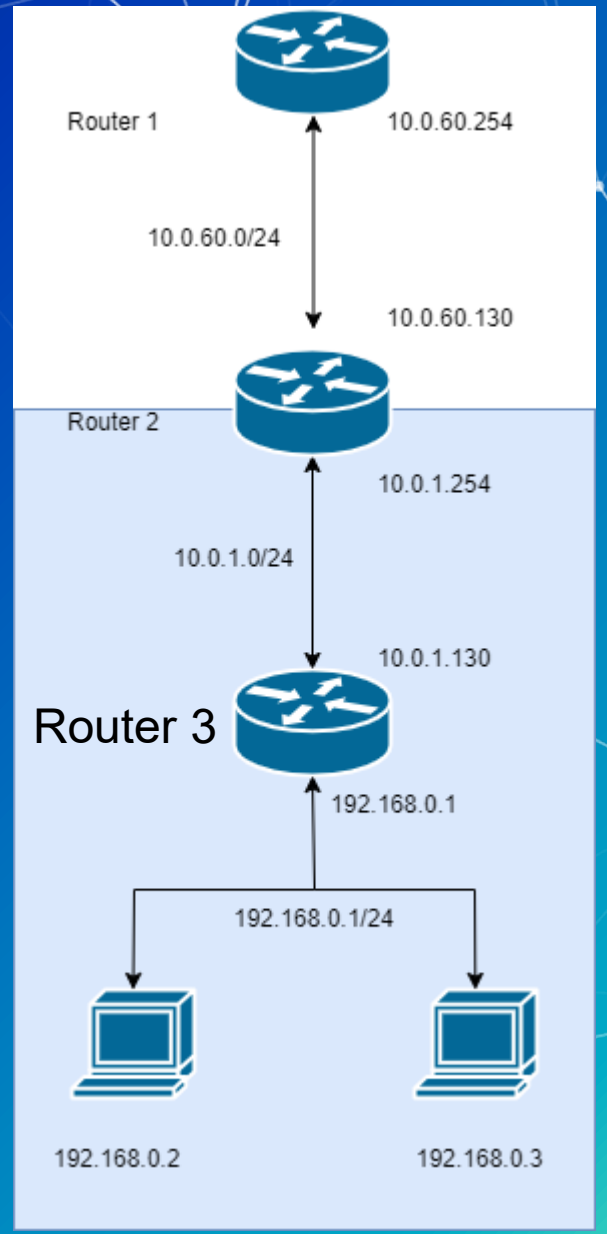
Static Routing Cont.

- Router 2 only knows the networks:
  - 10.0.60.0/24
  - 10.0.1.0/24
- Router 2 does not know the network:
  - 192.168.0.1/24



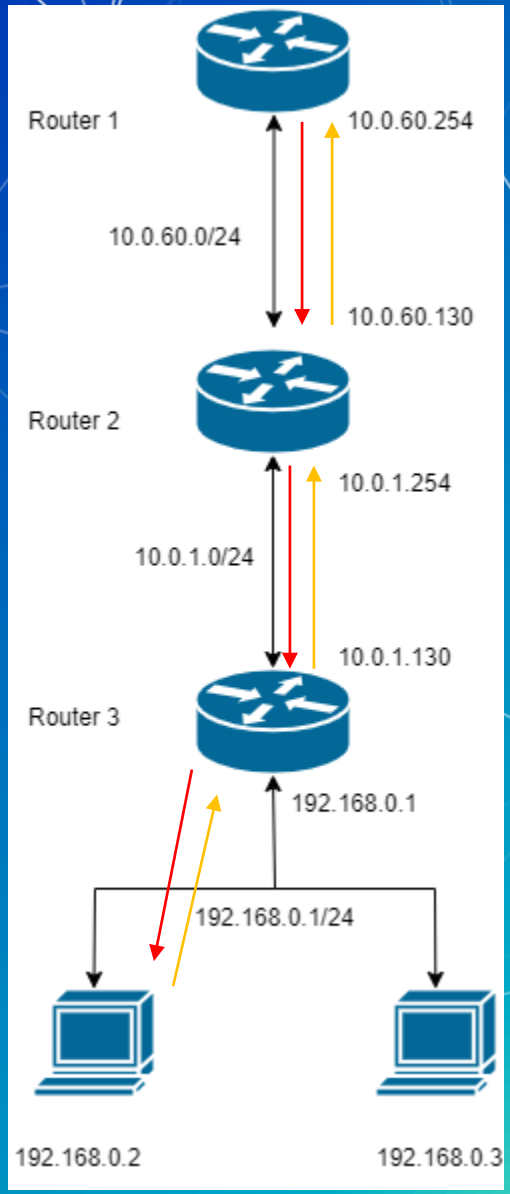
Static Routing Cont.

- Router 3 only knows the networks:
  - 192.168.0.1/24
  - 10.0.1.0/24
- Router 3 does not know the network:
  - 10.0.60.0/24



Static Routing Cont.

- For Router 1 to reach 192.168.0.2 static routes must be configured on Router 1, Router 2 and Router 3



Static Routing Cont.

- 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

In Class Activity

Demo static routing config

In Class Activity

Static Routing

Static Routing

- Additional commands you may find useful:
  - All prior commands from the earlier in class activity
  - ip route
  - do show ip route

Static routing in class activity

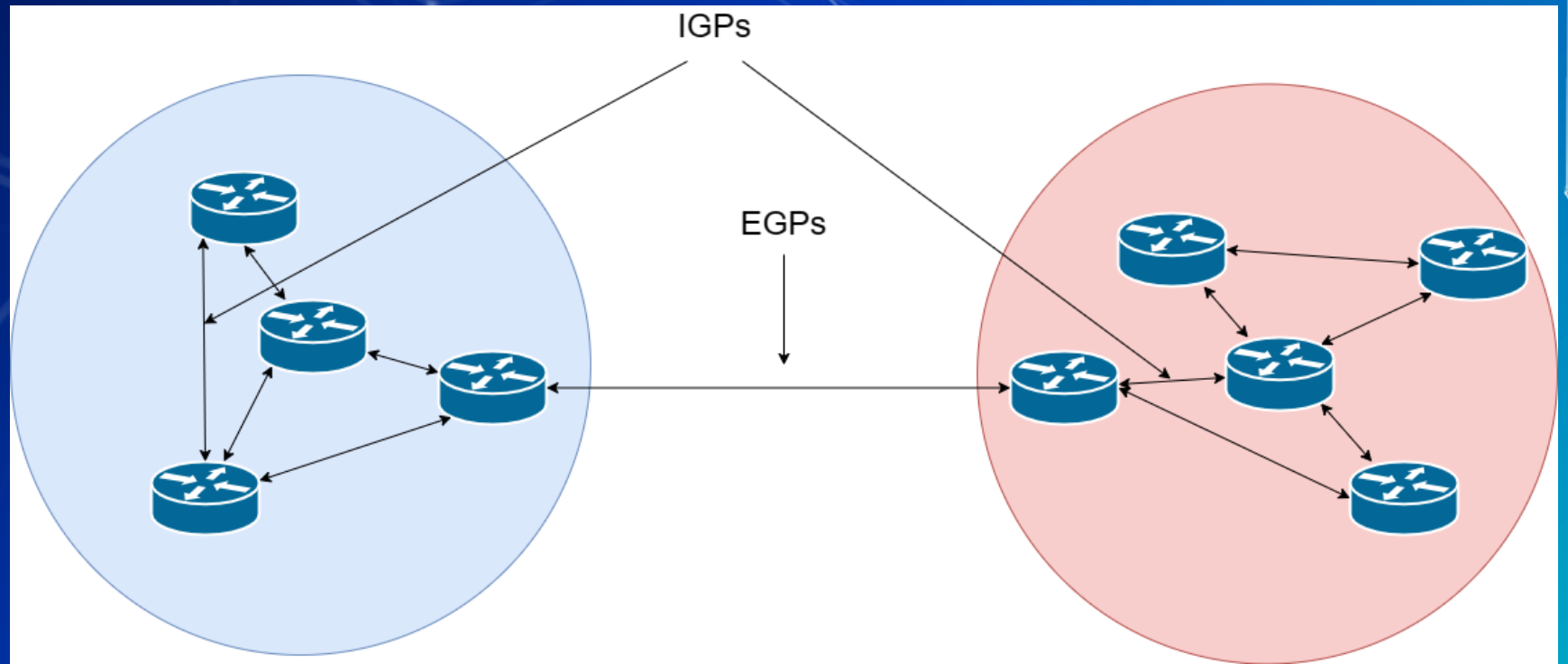
- Open the file staticrouting.pkt
- Configure proper networking to match the information next to the devices
- Configure a static routing to allow for the two clients to ping each other

Routing Protocols

- Interior gateway protocols (IGP)
  - Open Shortest Path First (OSPF)
  - Routing Information Protocol (RIP)
  - Intermediate System to Intermediate System (IS-IS)
  - Enhanced Interior Gateway Protocol (EIGRP)
- Exterior gateway protocols (EGP)
  - Exterior Gateway Protocol (EGP)
  - Border Gateway Protocol (BGP)

IGP vs EGP

- IGPs are used to share routes within an organization's network (WAN)
  - May also be referred to as intradomain
- EGPs are used to share routes between different autonomous systems
  - May also be referred to as interdomain



Routing Protocols Cont.

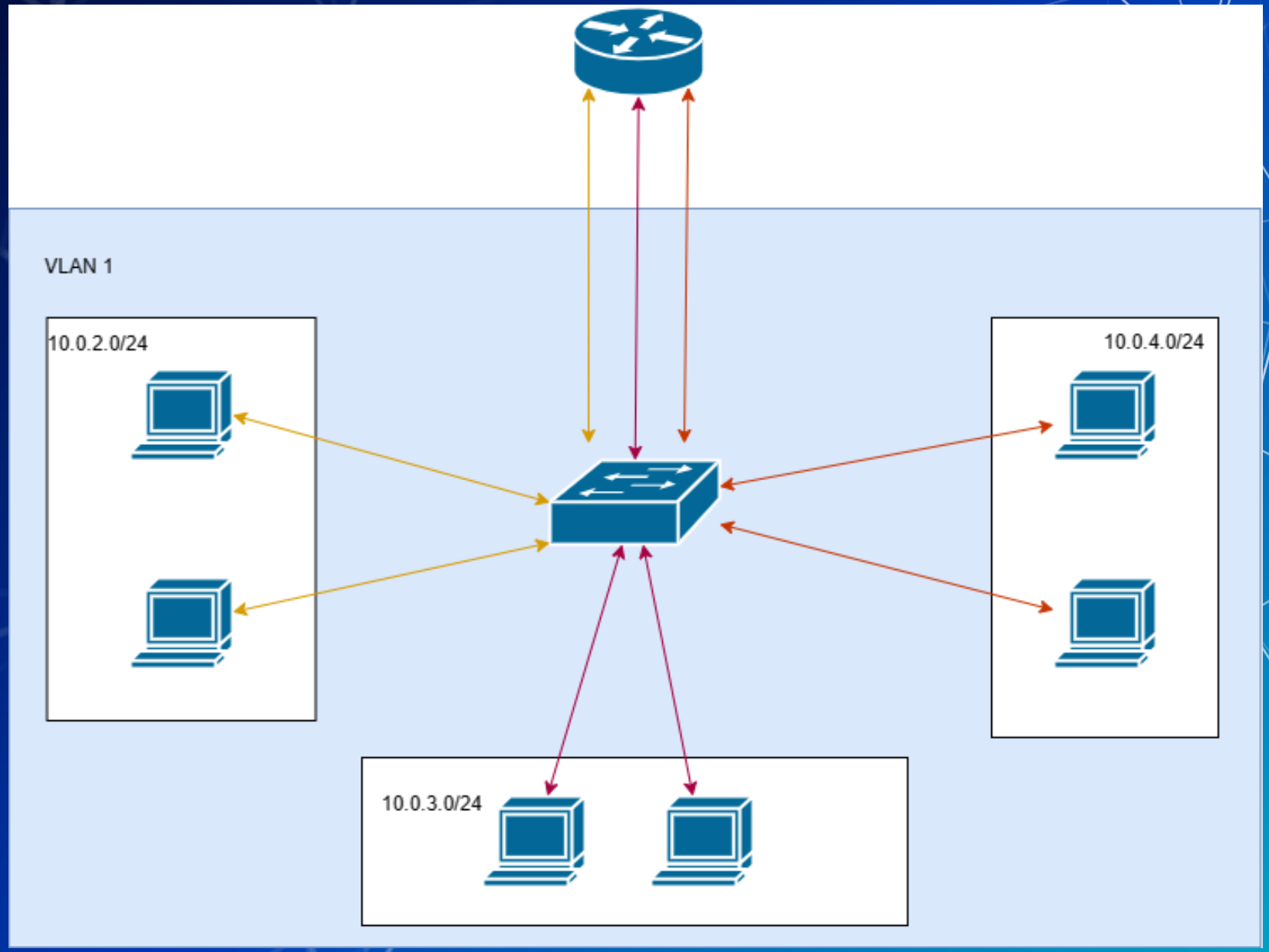
- Usually broken apart into further groups based upon algorithm type:
  - Distance vector
    - Only knows routes its neighbor tells it about and how to reach those destinations, effectively shares route tables
      - Routing protocols: RIP, EIGRP
  - Link state
    - Creates a database of every link each router has on every router
      - Routers share interface information with each other to create this database
    - More intensive resource usage on the router, but often faster to reacting to changes in the network
      - Routing Protocols: OSPF, IS-IS
  - Path Vector
    - Routers share reachable destinations as well as sequences of autonomous systems that must be traversed to reach those destinations
      - Routing Protocols: BGP

Break slide

Please return in 10 minutes

Virtual Local Area Network (VLAN)

- Segments a single LAN into multiple virtual LANS
  - Without configuring a VLAN every host would be in the same broadcast domain
    - This is usually only acceptable in very small networks
- If networks are segmented at layer 3 and VLANs are not used for segmentation at layer 2 broadcast and unicast frames may still be sent to all hosts

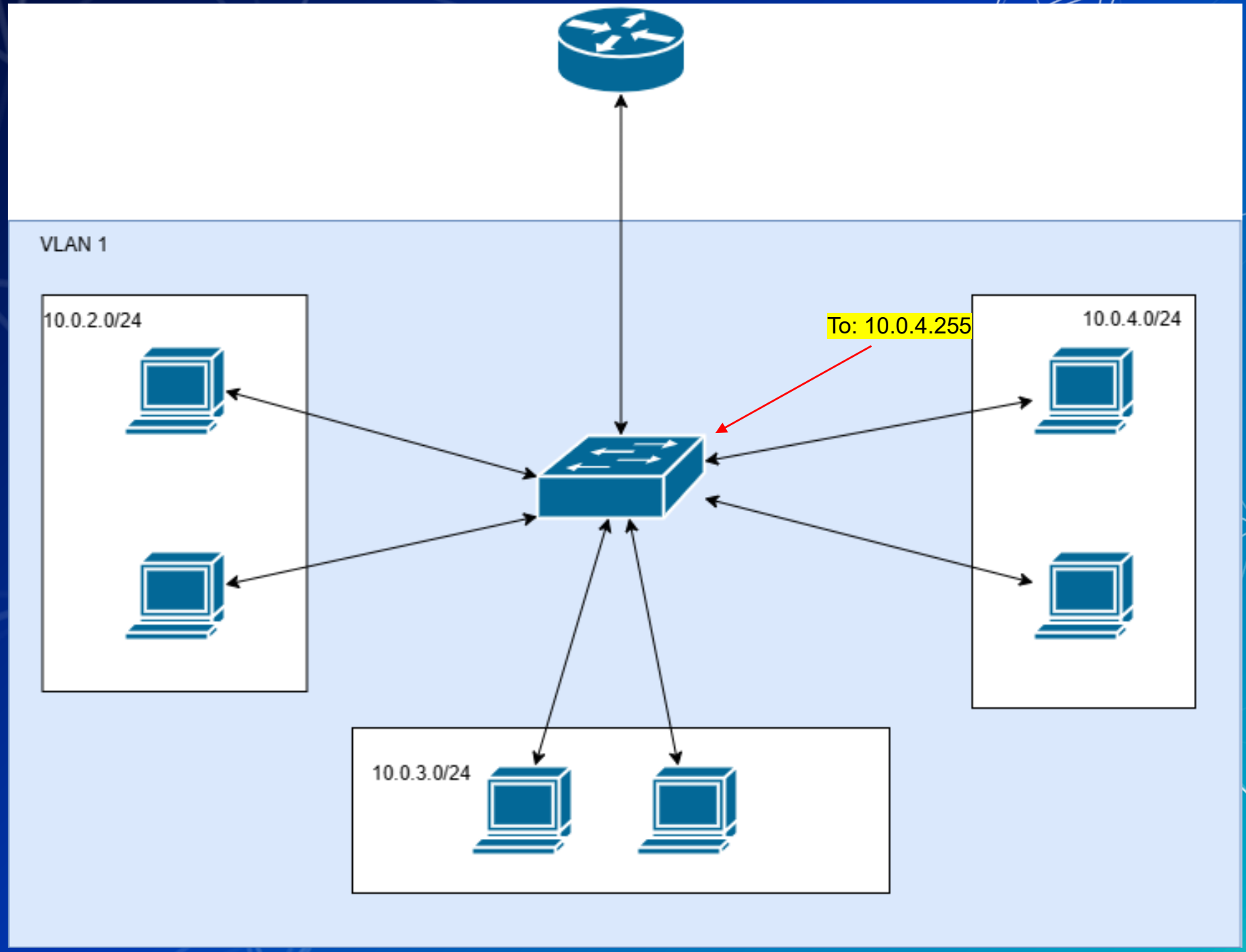

VLAN 1
10.0.2.0/24
10.0.4.0/24
10.0.3.0/24

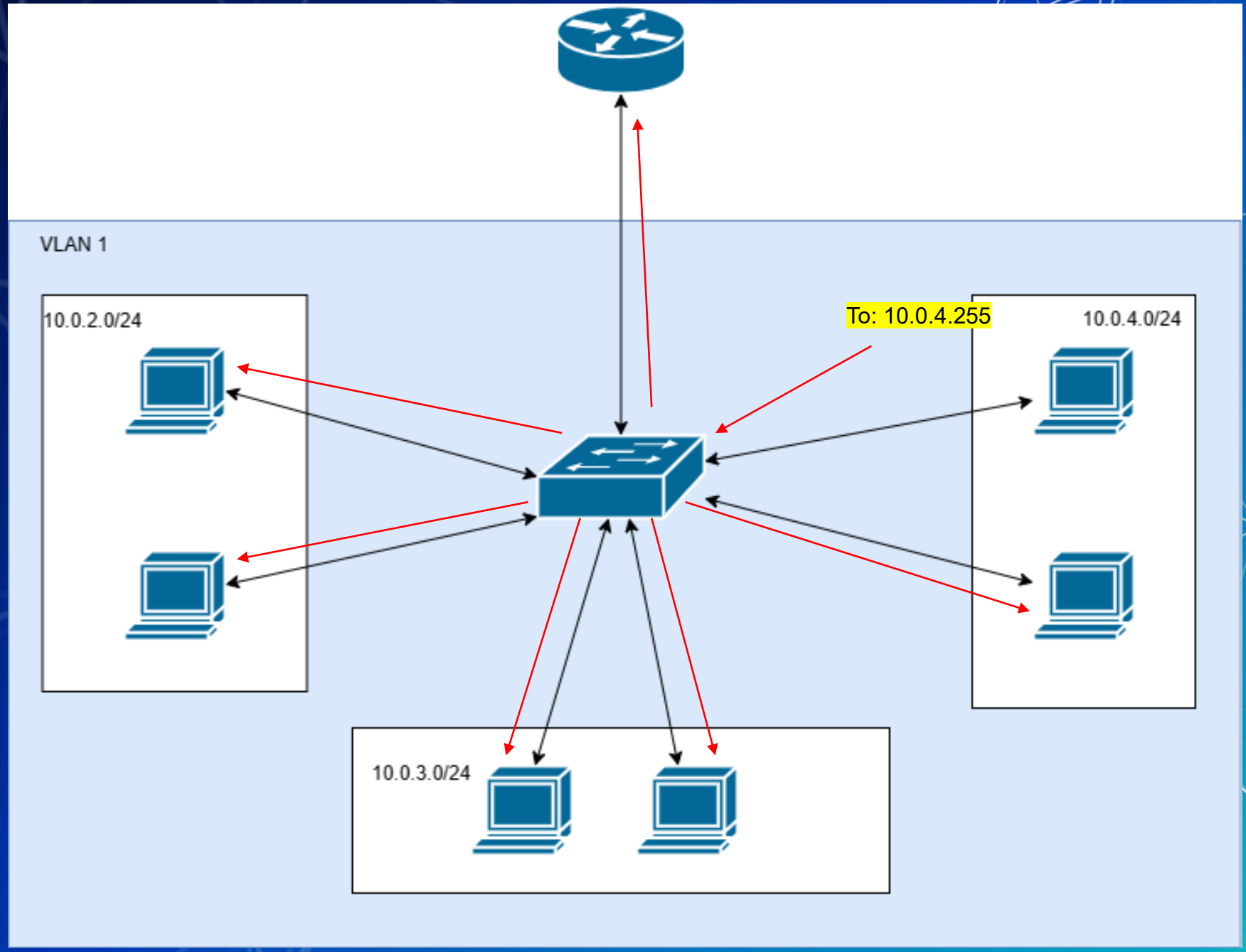
Trunk Ports

- Carry traffic of multiple VLANs
  - Uses VLAN tags to indicate which VLAN the traffic belongs to
    - This information is added to the header of the frame as under the 802.1Q tag

802.3 Ethernet packet and frame structure

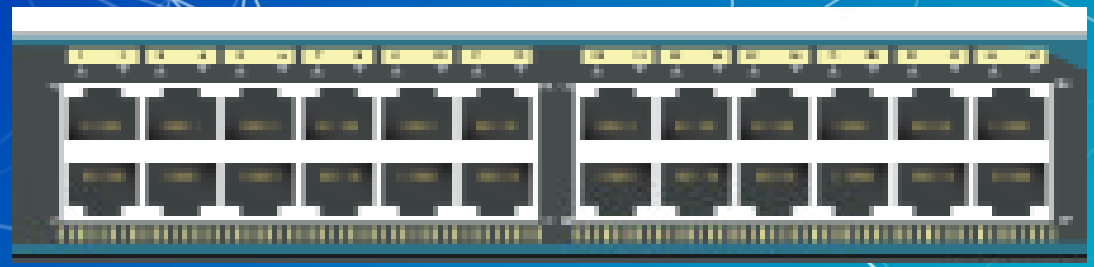
Layer	Preamble	Start frame delimiter (SFD)	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interpacket gap (IPG)
Length (octets)	7	1	6	6	(4)	2	42–1500[c]	4	12
Layer 2 Ethernet frame	(not part of the frame)		← 64–1522 octets →						(not part of the frame)
Layer 1 Ethernet packet & IPG	← 72–1530 octets →								← 12 octets →


VLAN 1
10.0.2.0/24
To: 10.0.4.255
10.0.4.0/24
10.0.3.0/24


VLAN 1
10.0.2.0/24
To: 10.0.4.255
10.0.4.0/24
10.0.3.0/24

Assigning VLANs

- VLANs are configured per-interface
  - Interface is referring to the ports in this case
  - Devices are not necessarily aware that they are connected to a VLAN
- The total possible number of VLANs is 1-4094

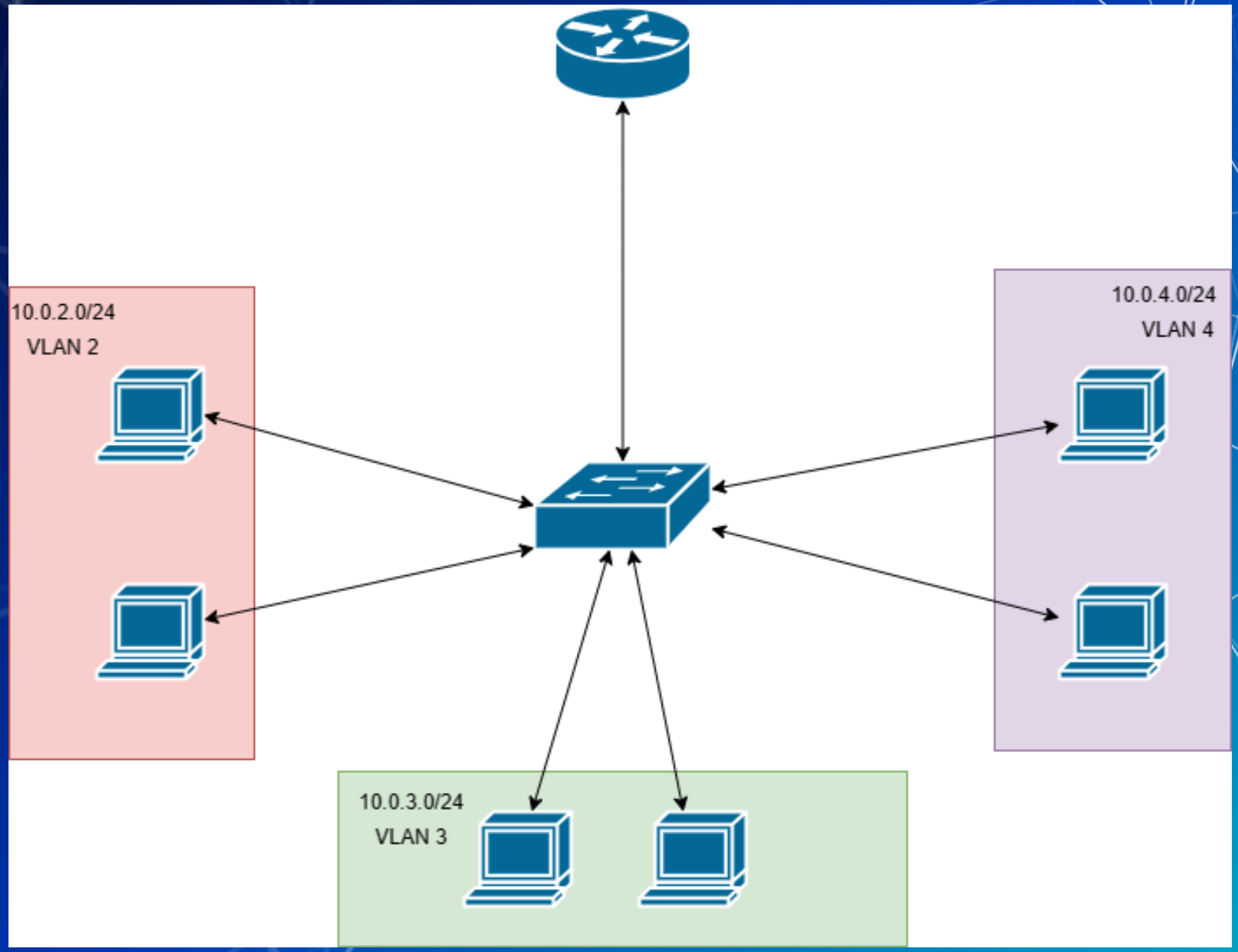


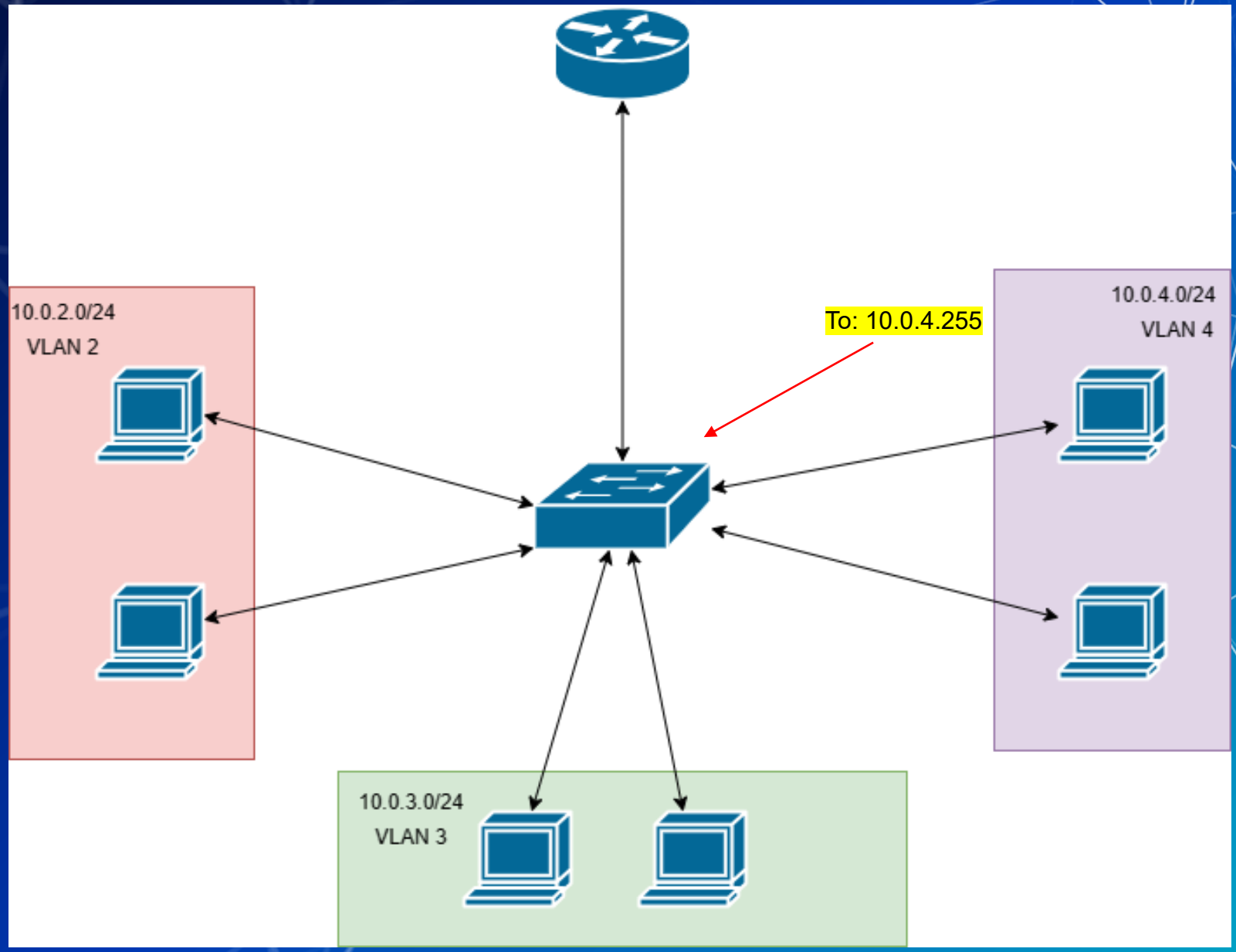
Where does that VLAN range limit come from?

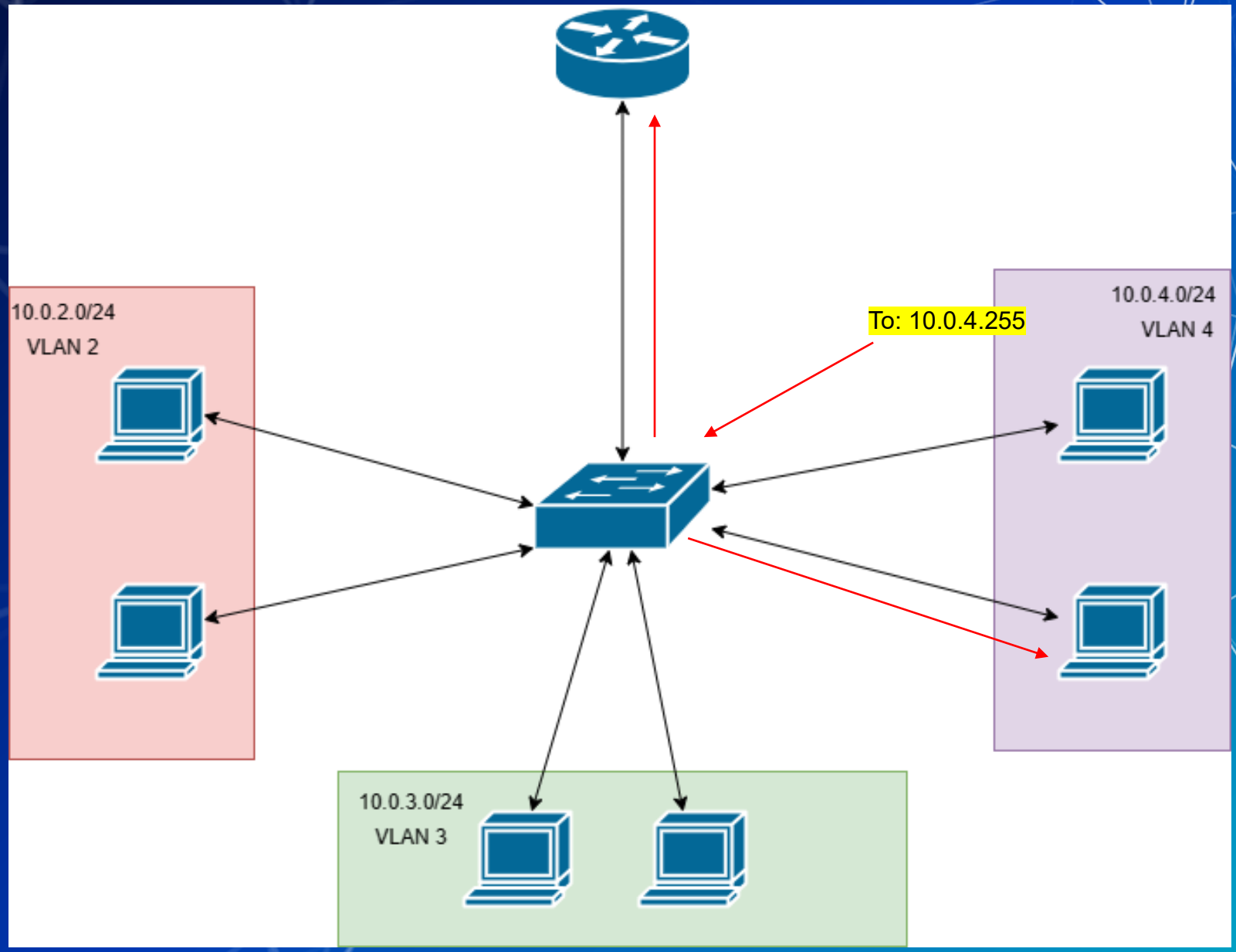
- Looking in depth at the 802.1Q tag will yield that information
- The VLAN ID (VID) is limited to just 12 bites leading that max

802.1Q tag format

16 bits	3 bits	1 bit	12 bits
TPID	TCI		
	PCP	DEI	VID


10.0.2.0/24
VLAN 2
10.0.4.0/24
VLAN 4
10.0.3.0/24
VLAN 3


10.0.2.0/24
VLAN 2
To: 10.0.4.255
10.0.4.0/24
VLAN 4
10.0.3.0/24
VLAN 3


10.0.2.0/24
VLAN 2
To: 10.0.4.255
10.0.4.0/24
VLAN 4
10.0.3.0/24
VLAN 3

In Class Activity

Configuring VLANs using Packet Tracer

Configuring VLANs using Packet Tracer

- Additional commands you may find useful:
  - All prior commands from the earlier in class activity
  - Switchport mode access
  - Switchport access vlan #
  - int range
  - do show vlan brief

VLAN in Class Activity

- Open the file named vlan.pkt using packet tracer
- Make 3 connections between the router and the switch
  - Configure an interface on the router for each VLAN
    - Make sure the IP address matches the gateway configured on the PCs
- Configure the switches interfaces to be in the proper VLAN
- Ping between PCs to check connectivity
  - Send a broadcast ping to see which PCs receive the broadcast
    - This may be easier to see in packet tracer's simulation mode

Quality of Service (QoS)

- Quality of Service is treating packets differently depending on the type of traffic
  - This of often used for prioritization of traffic
- Most commonly seen in IP phones
  - Uses voice over internet protocol (VOIP)
  - Phones are connected to a switch port like other endpoints
  - Phones tend to have an ‘uplink’ port that connects to a switch and a ‘downlink’ port that connects to the PC
    - This saves on switch ports
  - Voice traffic from the phone can be separated from traffic from the PC by placing them in separate VLANs

QoS Continued

- QoS measures and manages traffic based on these characteristics:
  - Bandwidth (maximum rate of transfer)
  - Delay (latency)
  - Jitter (variance in latency)
  - Loss (actual rate of transfer)

How does QoS classify traffic?

- To be able to prioritize traffic it's necessary to classify different types of traffic
  - This can be done using:
    - Priority Code Point (PCP)
      - Within a frame
      - Only works if there is a VLAN tag (802.1Q)
      - 3 bits = 8 possible values

802.1Q tag format

16 bits	3 bits	1 bit	12 bits
TPID	TCI		
	PCP	DEI	VID

PCP value	Priority	Acronym	Traffic types
1	0 (lowest)	BK	Background
0	1 (default)	BE	Best effort
2	2	EE	Excellent effort
3	3	CA	Critical applications
4	4	VI	Video, < 100 ms latency and jitter
5	5	VO	Voice, < 10 ms latency and jitter
6	6	IC	Internetwork control
7	7 (highest)	NC	Network control

Classification Cont.

- Differentiated Services Code Point (DSCP)
  - A field within the IP header of a packet that can be used to identify high/low priority traffic
  - Has 6 bits of length, allowing for 64 different values of classification
    - There's a **very** long list of standardized markings for traffic, two important ones are:
      - Default Forwarding
      - Expedited Forwarding

IPv4 header format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total length															
4	32	Identification																Flags			Fragment offset											
8	64	Time to Live								Protocol								Header checksum															
12	96	Source address																															
16	128	Destination address																															
20	160	Options (if IHL > 5)																															
⋮	⋮																																
56	448																																

QoS Queuing & Scheduling Systems

- The different common queueing systems that exist are:
  - Weighted round robin
  - Class-based weighted fair queuing (CBWFQ)
  - Low Latency Queuing
    - Good for voice traffic
- Shaping
  - Buffers traffic that goes over a configured rate
- Policing
  - Drops traffic if it goes over a specific rate

Access Control List (ACL)

- Allow device access to a network based upon IP and/or MAC address
  - Routers ACLs are stateless firewalls
  - Switches can also not only limit which MAC are allowed on each port, but also the total number of MAC addresses allowed on each port
    - Switches can also use VLANs for this

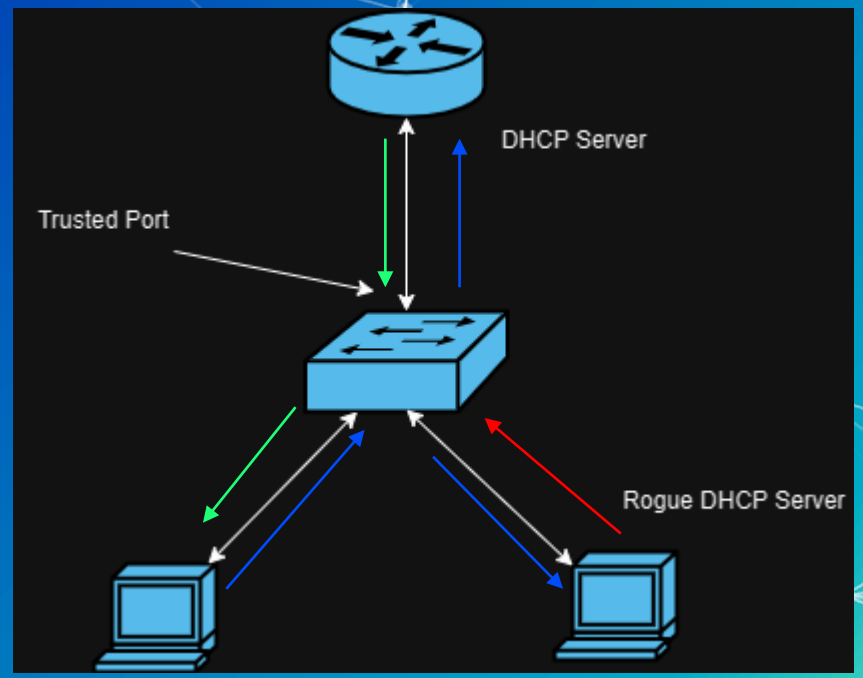
MAC Address	Device Name	Role	vlan	Expiration	Created	Sponsor	Sharing	Domain
78-4F	SON11	UB_Staff	232	2024-10-17 23:10	2022-07-08 12:10	rwharenz	*Disabled*	NURS
E0-D0	SON833	UB_Staff	326	2024-08-15 13:16	2023-08-16 13:16	rwharenz	*Disabled*	NUR
CC-96	SON891	UB_Staff	232	2024-10-21 23:57	2023-02-02 11:03	rwharenz	*Disabled*	NUR
B0-3C	SON830	UB_Staff	999	2024-09-11 21:04	2022-08-03 10:51	rwharenz	*Disabled*	NUR
AC-91	SON815	UB_Staff	232	2024-10-21 15:22	2023-06-23 11:56	rwharenz	*Disabled*	NUR
AC-1A	SON838	UB_Staff	232	2024-08-09 01:36	2023-09-12 13:18	rwharenz	*Disabled*	NUR
AC-1A	SON823	UB_Staff	232	2024-09-17 12:46	2023-09-12 10:23	rwharenz	*Disabled*	NUR

Storm Control

- Monitors traffic over 1 second time intervals
  - Storm control monitors can look at the percentage of traffic that is broadcast, multicast or unicast
  - It can be configured so that is 60% of traffic going through a port is broadcast traffic it will shut down the port
  - This is designed to prevent denial of service attacks and broadcast storms

DHCP Snooping + ARP Inspection

- This is a security feature on switches that filters for DHCP messages received on untrusted ports
  - Routers can block DHCP offers on untrusted ports
  - By default, all ports are untrusted
- Dynamic ARP inspection is nearly identical to this
  - Can be used to block ARP poisoning attacks



Agenda - Week 11

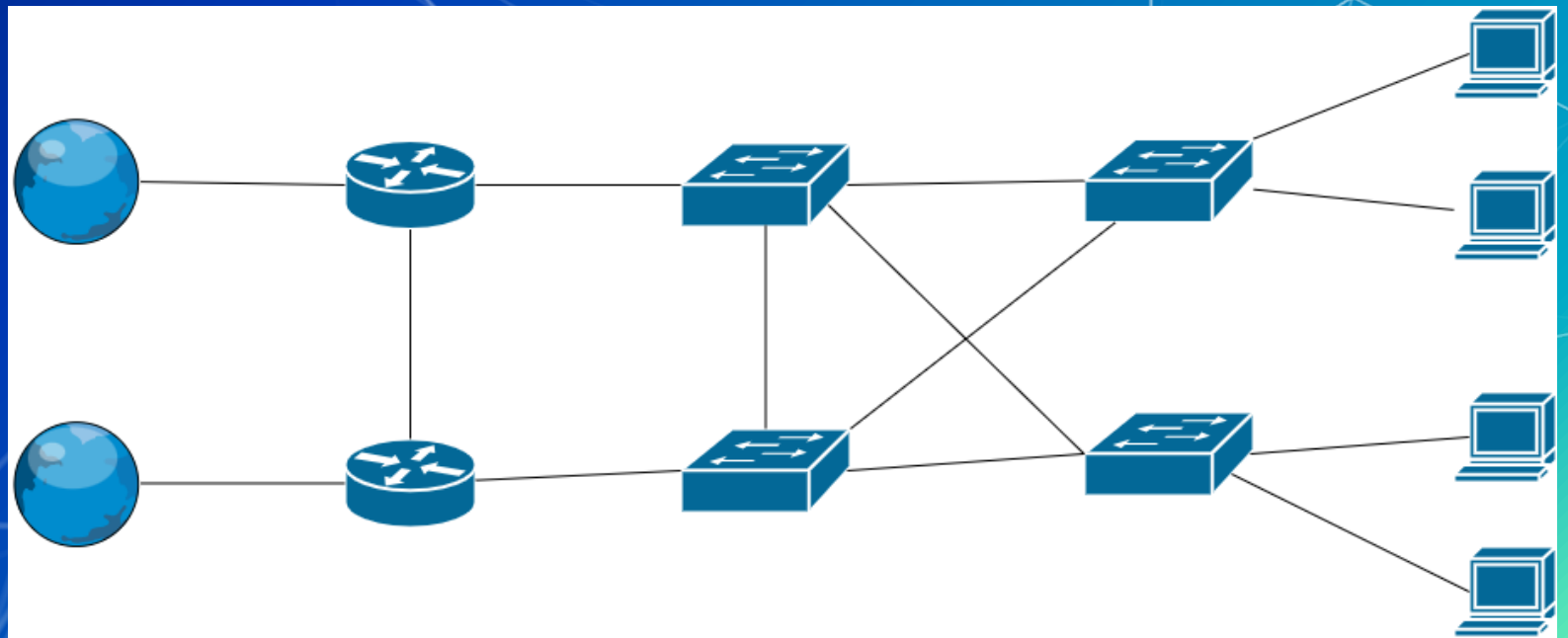
1. Networking
2. **High Availability**
3. Network Architecture
4. Wireless Technologies

High Availability

Redundancy

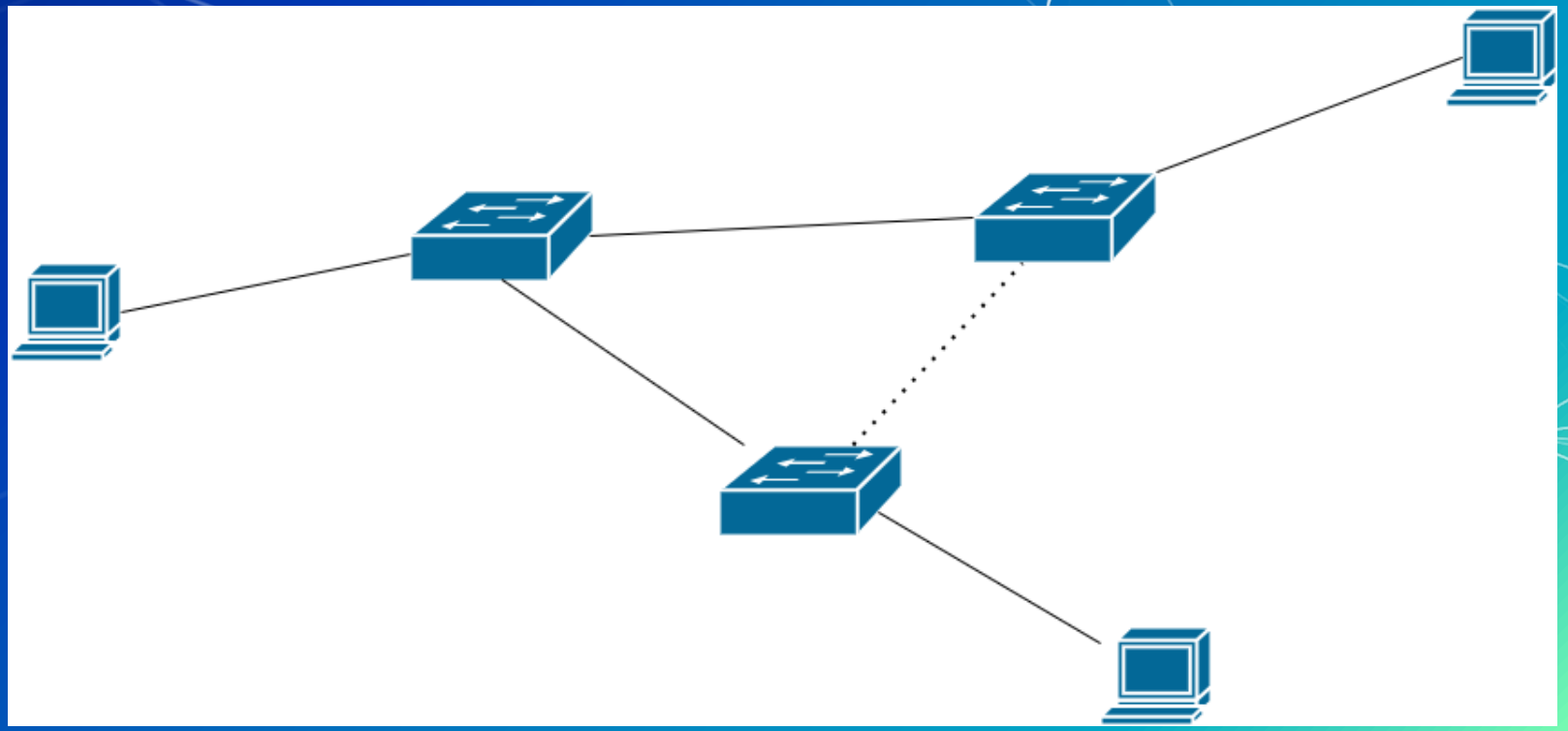
What is high availability?

- High availability is the use of redundancy to minimize downtime
- This means it is necessary to ensure other networking components take over to avoid downtime
- Generally, it is expected that network's function 24/7



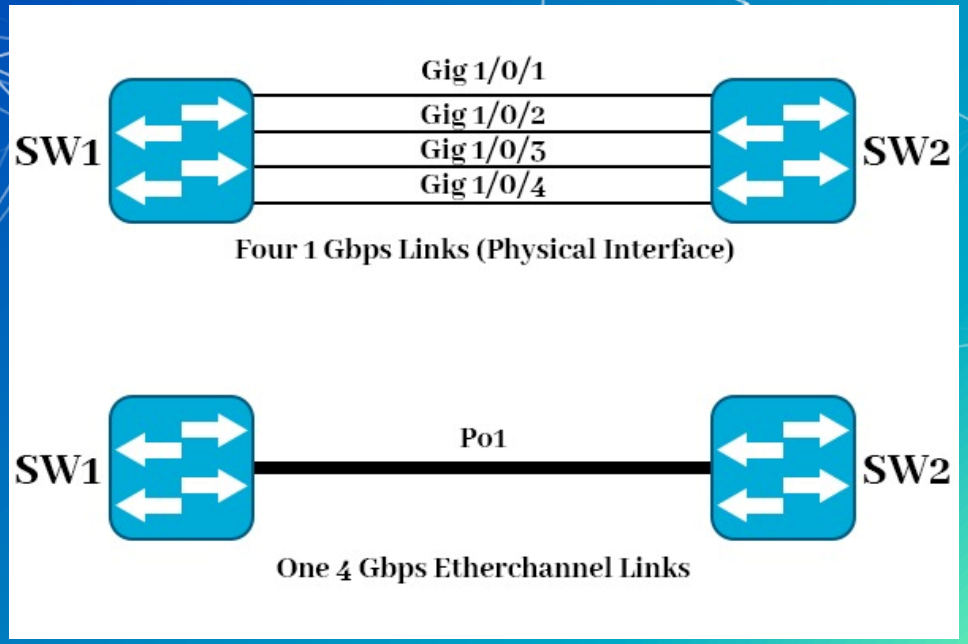
Spanning Tree Protocol (STP)

- STP is used to deactivate certain network ports when there are redundant connections to avoid loops
  - If this did not happen broadcast messages would cripple networks with loops
- Network devices send out a bridge protocol data unit (BPDU) to detect loops in network topologies
- There is an entire calculation process after sending a BPDU message to determine which device is the root bridge and which ports become designated ports
- Non-designated ports are blocking ports



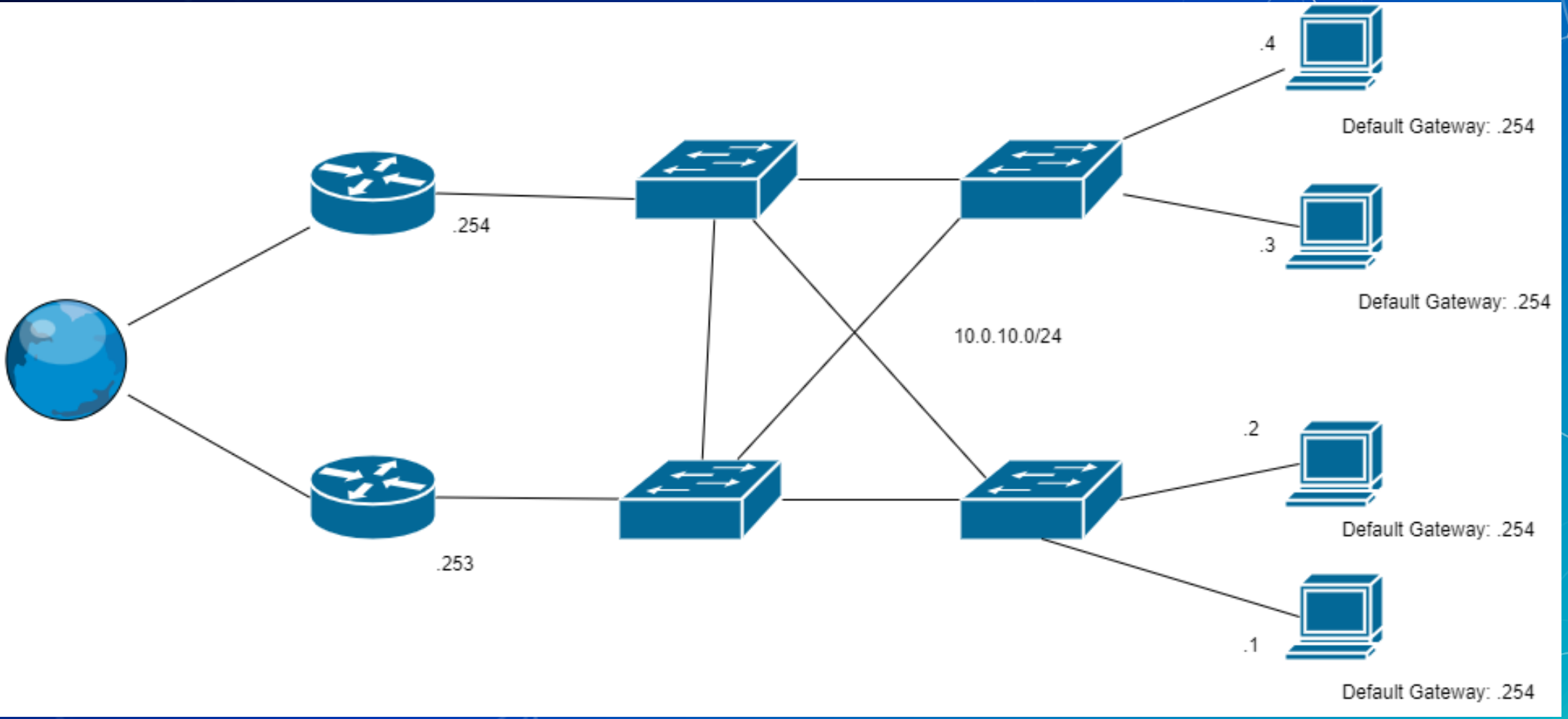
EtherChannel

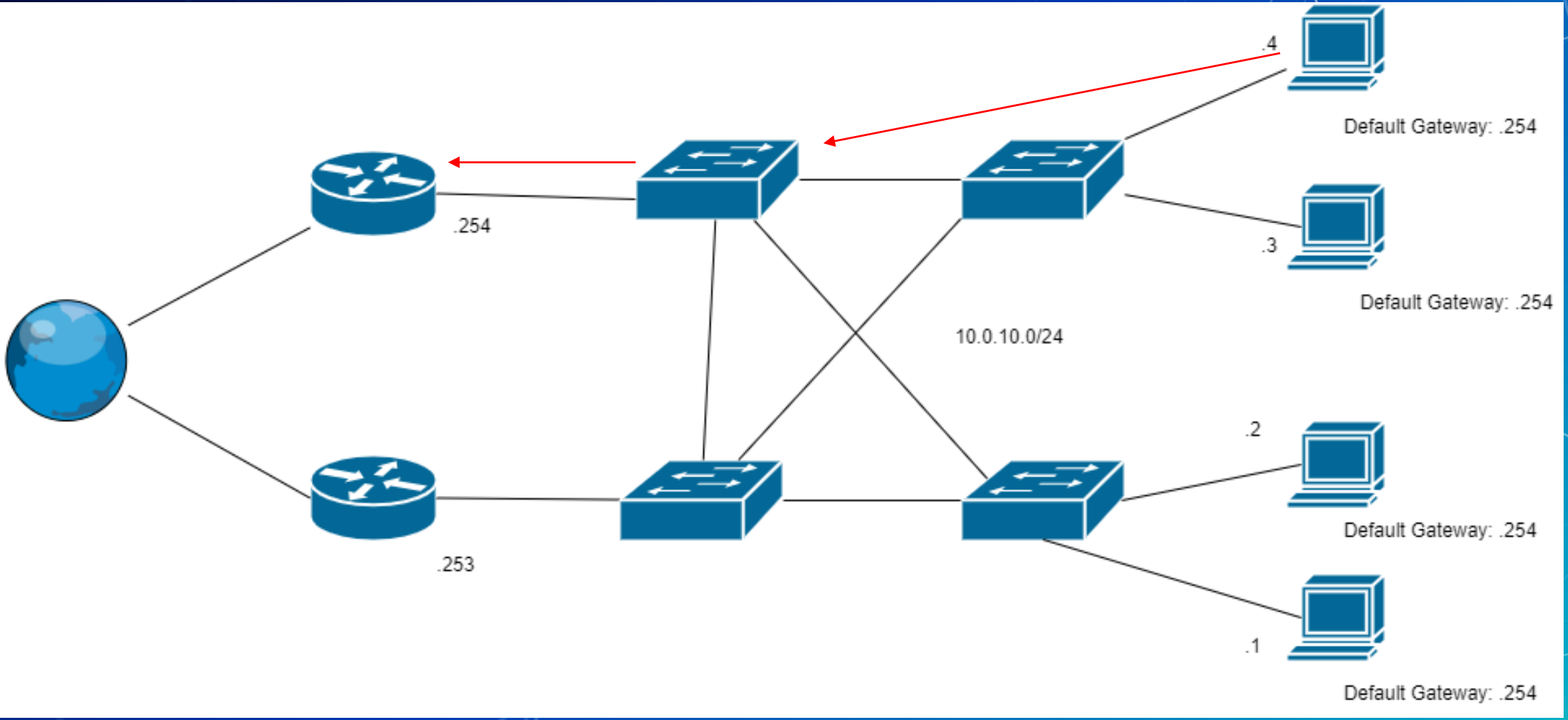
- Sometimes called link aggregation group (LAG) or a port channel
- Groups multiple interfaces together to act as a single interface
  - STP also treats this as a single interface
- Useful for when there are bandwidth limitations

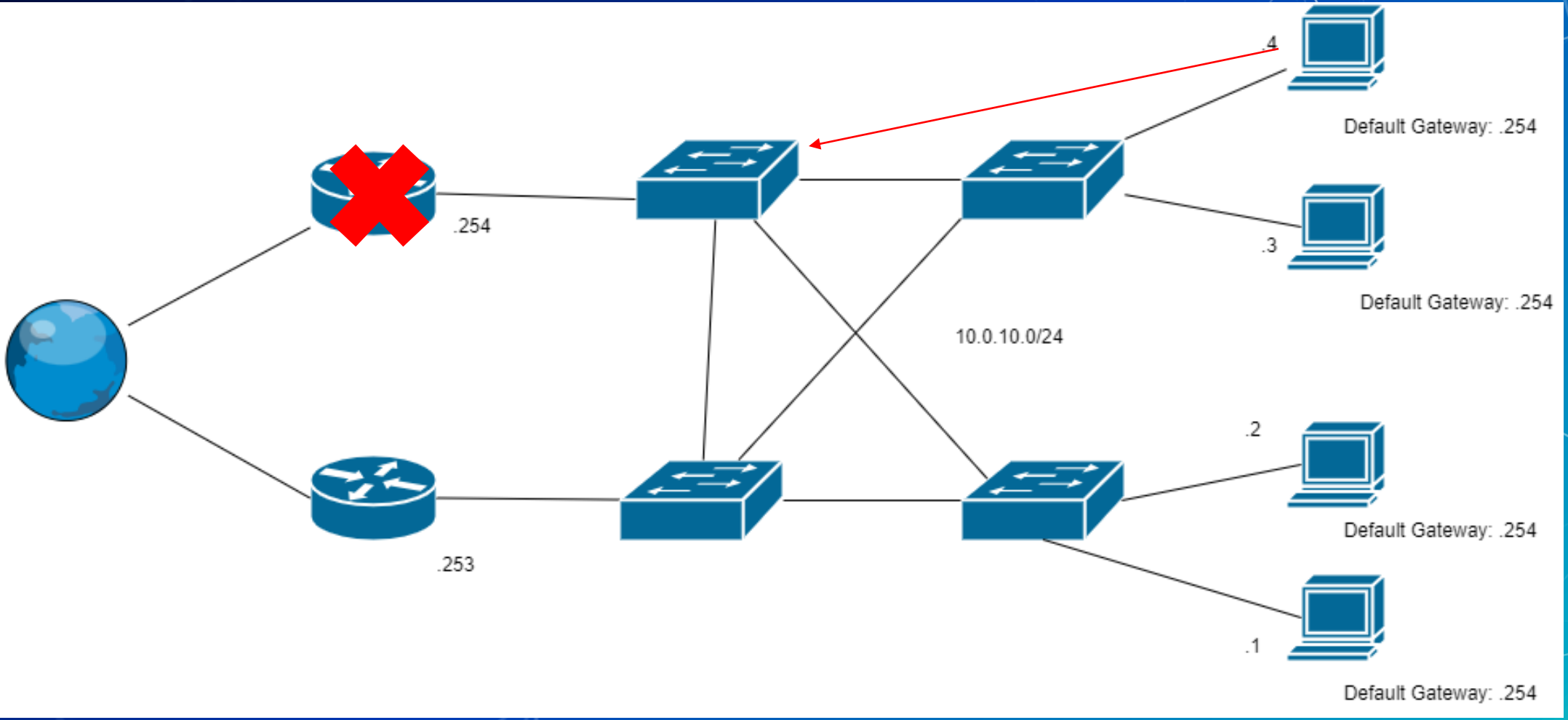


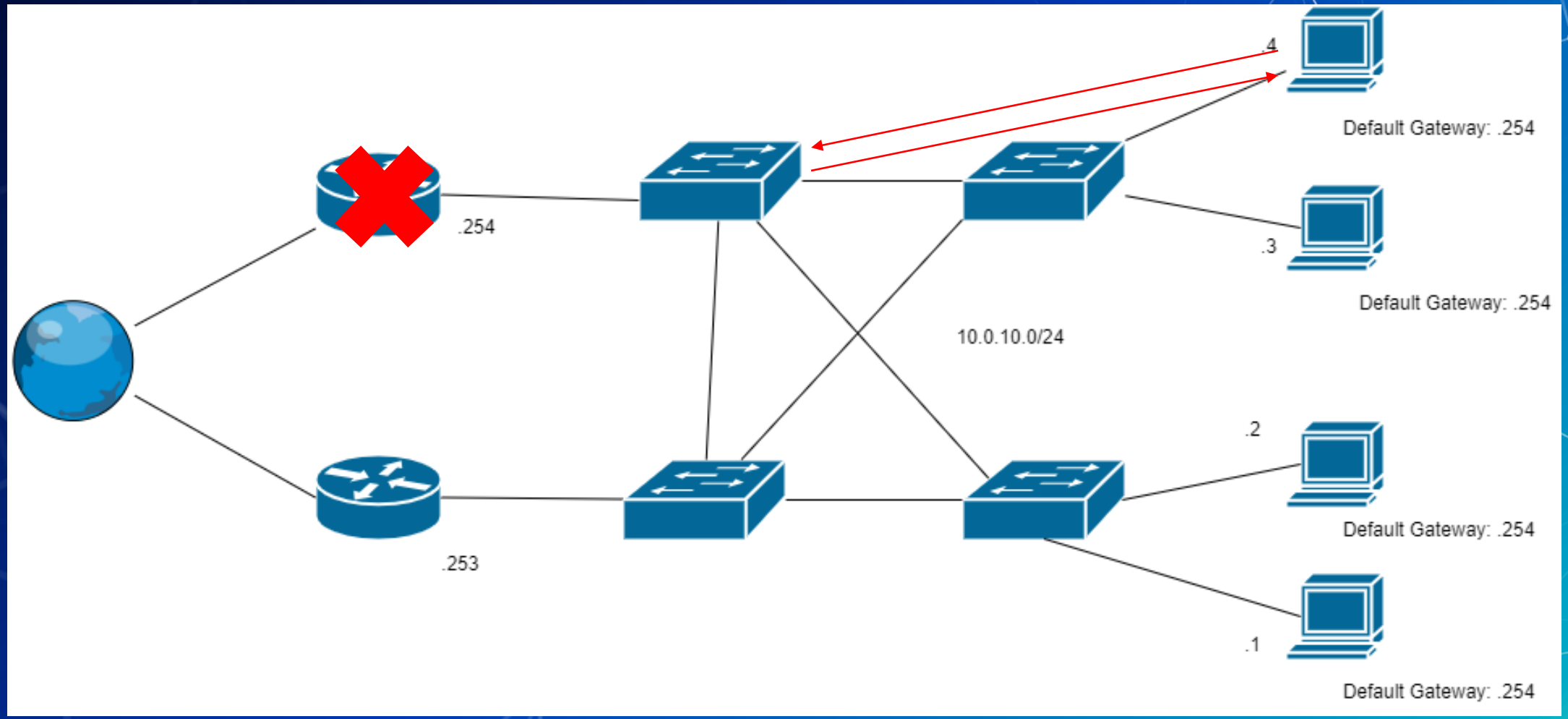
First Hop Redundancy protocols（FHRP)

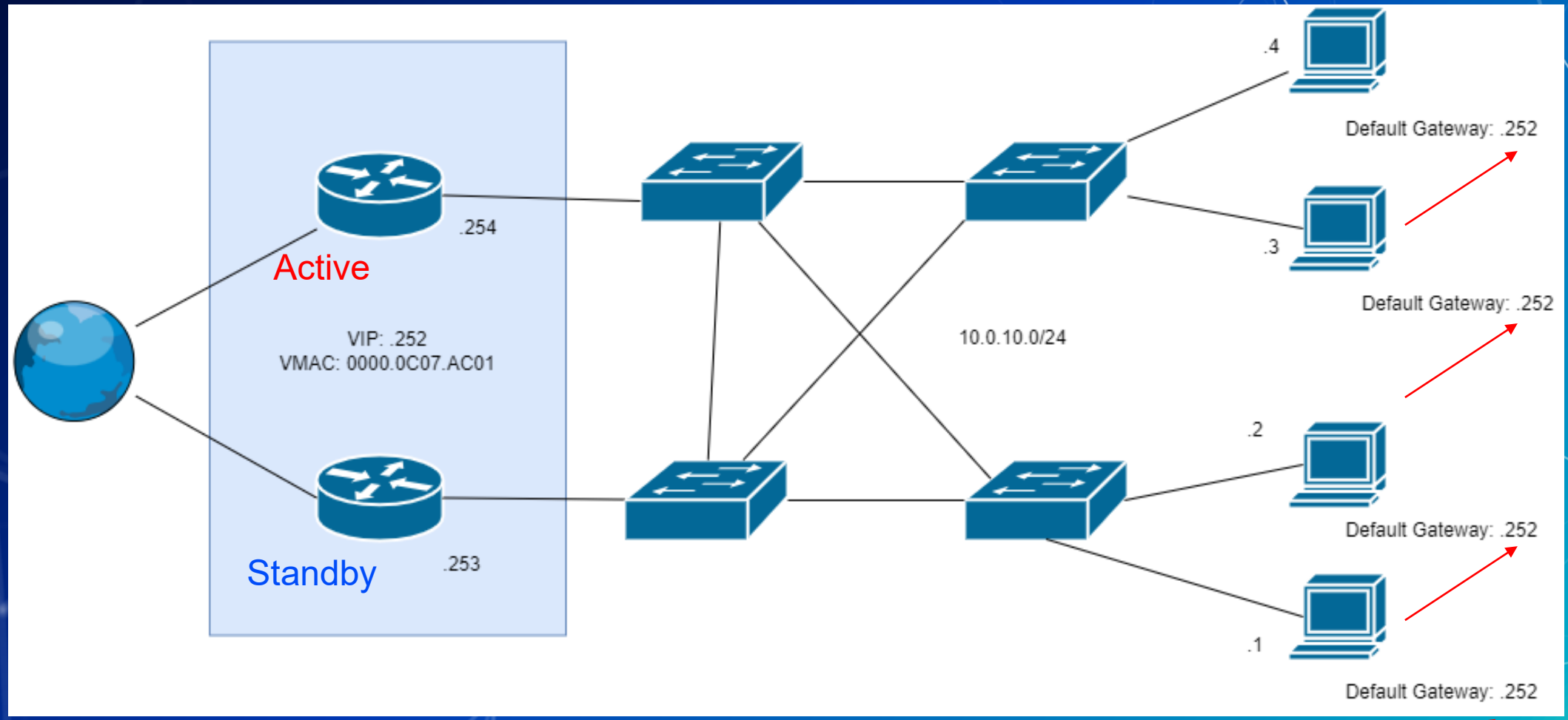
- FHRPs are used to help a device adjust to the failure of a router and protect the default gateway on a network
- This is done using virtual internet protocol addresses (VIP) and virtual mac addresses (VMAC)
- Generally, there is a device on active, and another on standby
  - Every ~1 second the routers check if the other devices are still functioning
- The FHRP protocols help update the switch mac address tables by sending a gratuitous ARP reply
  - A gratuitous ARP reply is an ARP ‘request’ sent without being requested

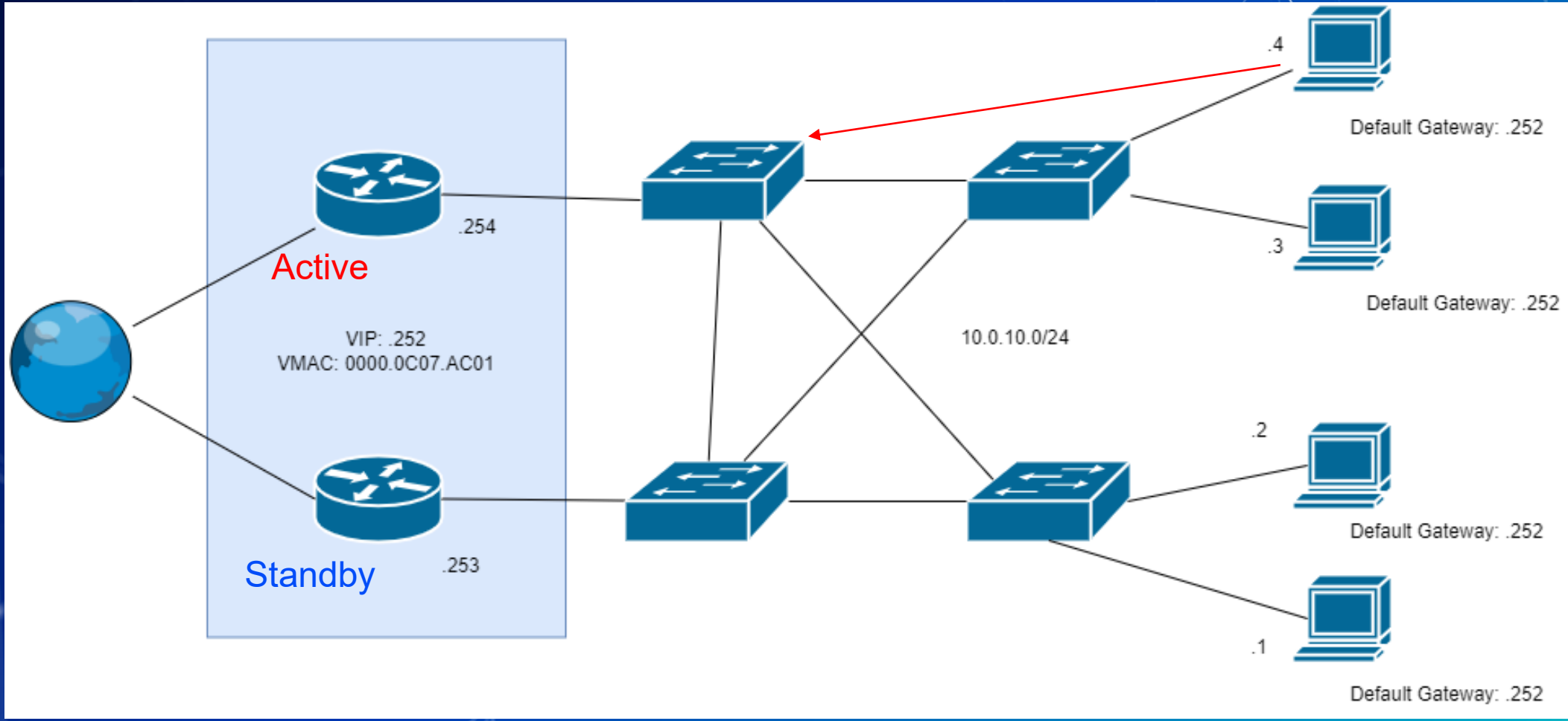

.4
Default Gateway: .254
.254
.3
Default Gateway: .254
10.0.10.0/24
.2
Default Gateway: .254
.253
.1
Default Gateway: .254

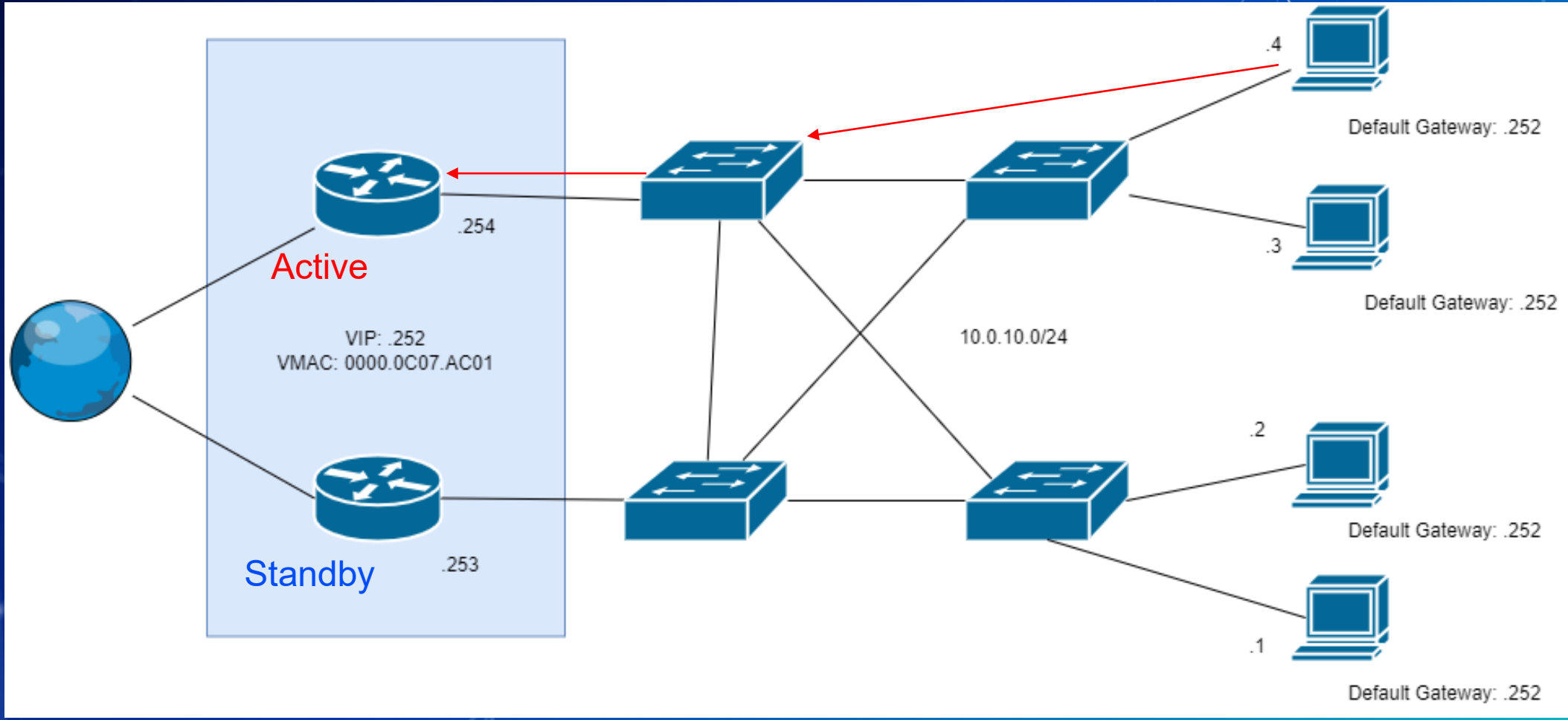

.4
Default Gateway: .254
.254
.3
Default Gateway: .254
10.0.10.0/24
.2
Default Gateway: .254
.253
.1
Default Gateway: .254

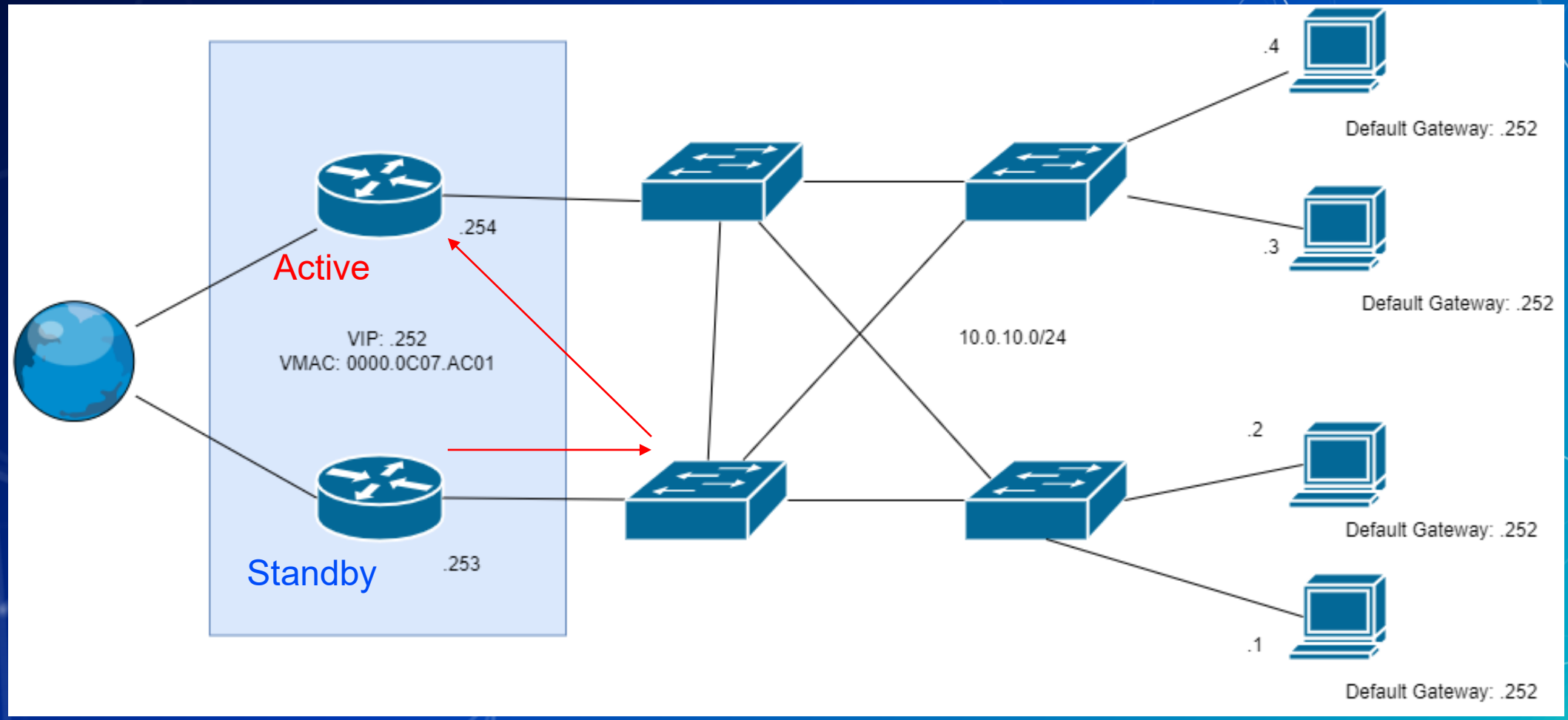

.4
Default Gateway: .254
.254
.3
Default Gateway: .254
10.0.10.0/24
.2
Default Gateway: .254
.253
.1
Default Gateway: .254

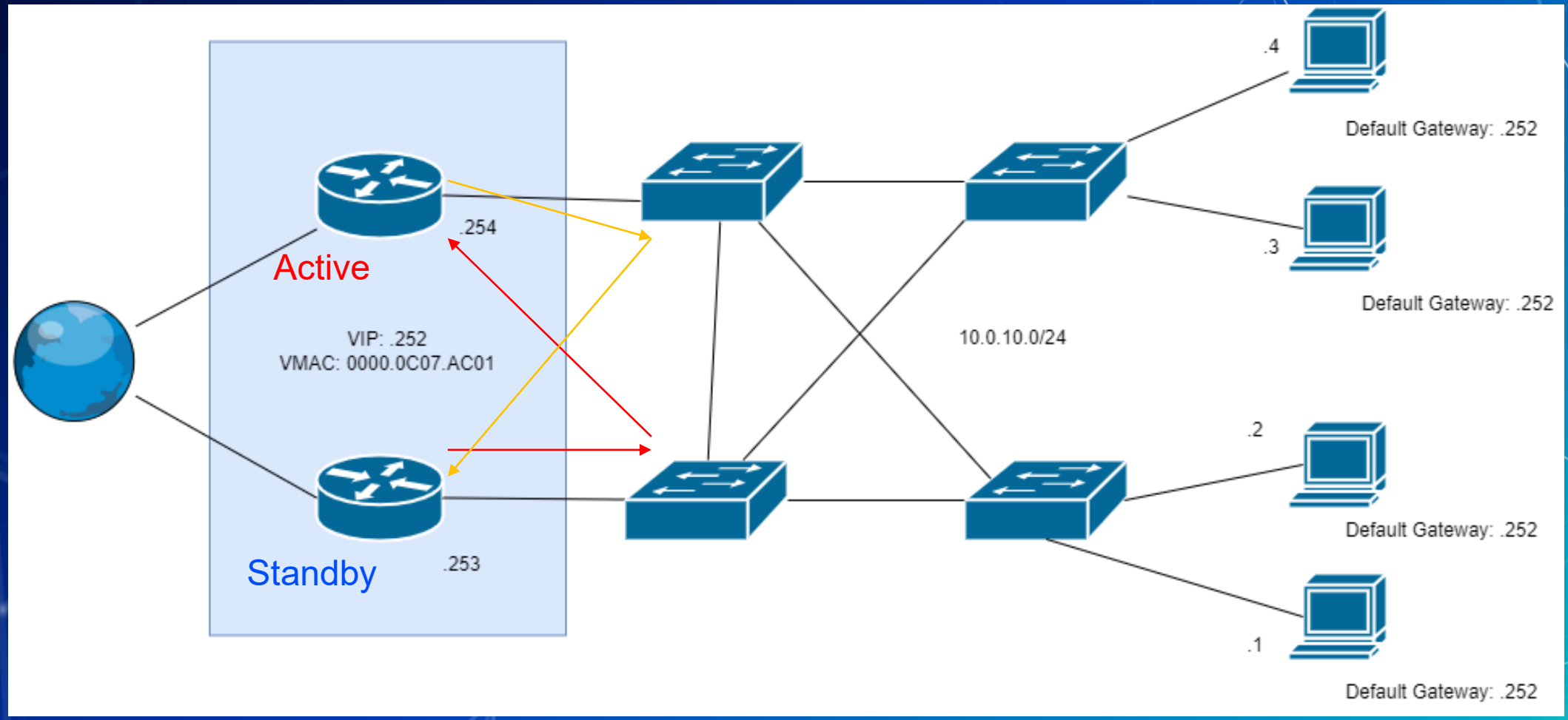

.4
Default Gateway: .254
.254
.3
Default Gateway: .254
10.0.10.0/24
.2
Default Gateway: .254
.253
.1
Default Gateway: .254

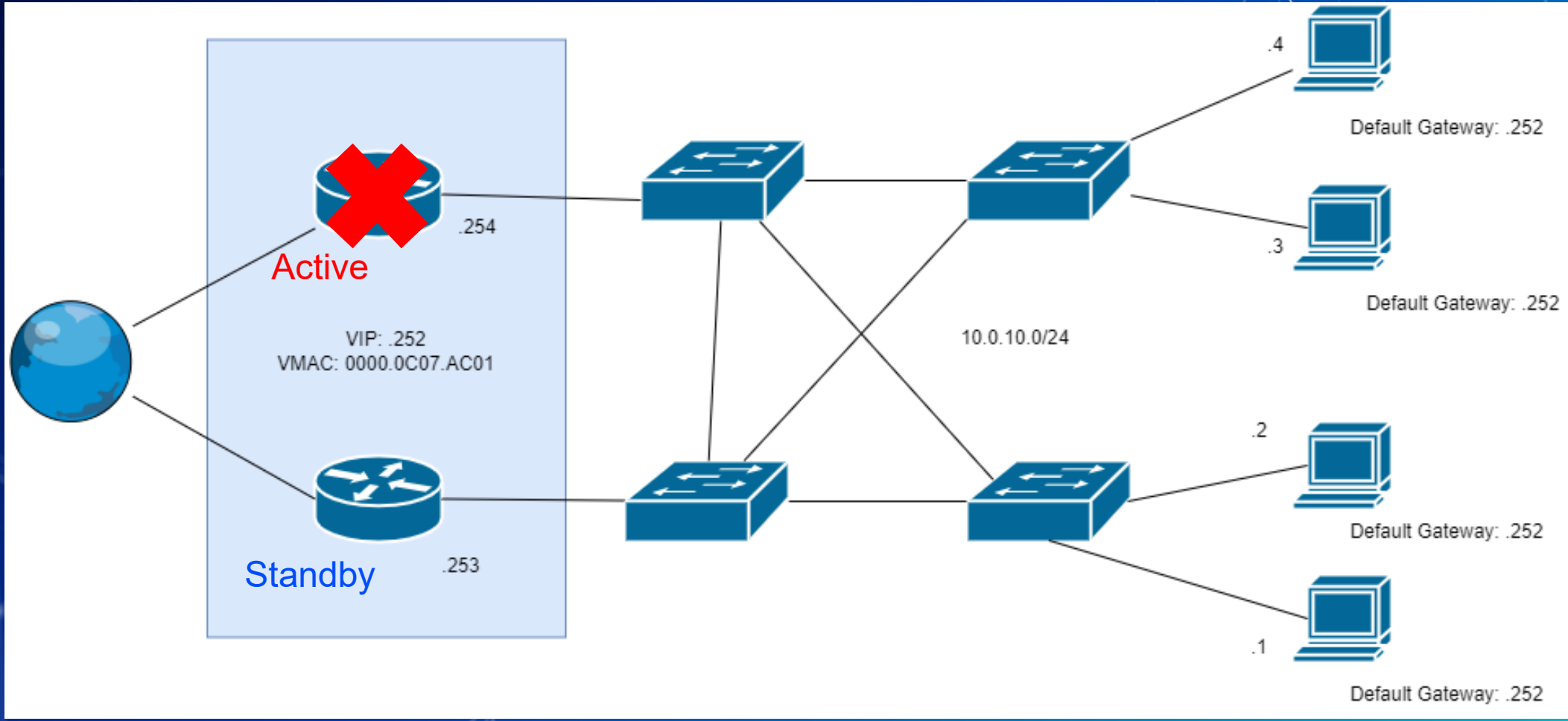

.4
Default Gateway: .252
.254
Active
.3
Default Gateway: .252
VIP: .252
VMAC: 0000.0C07.AC01
10.0.10.0/24
.2
Default Gateway: .252
Standby
.253
.1
Default Gateway: .252

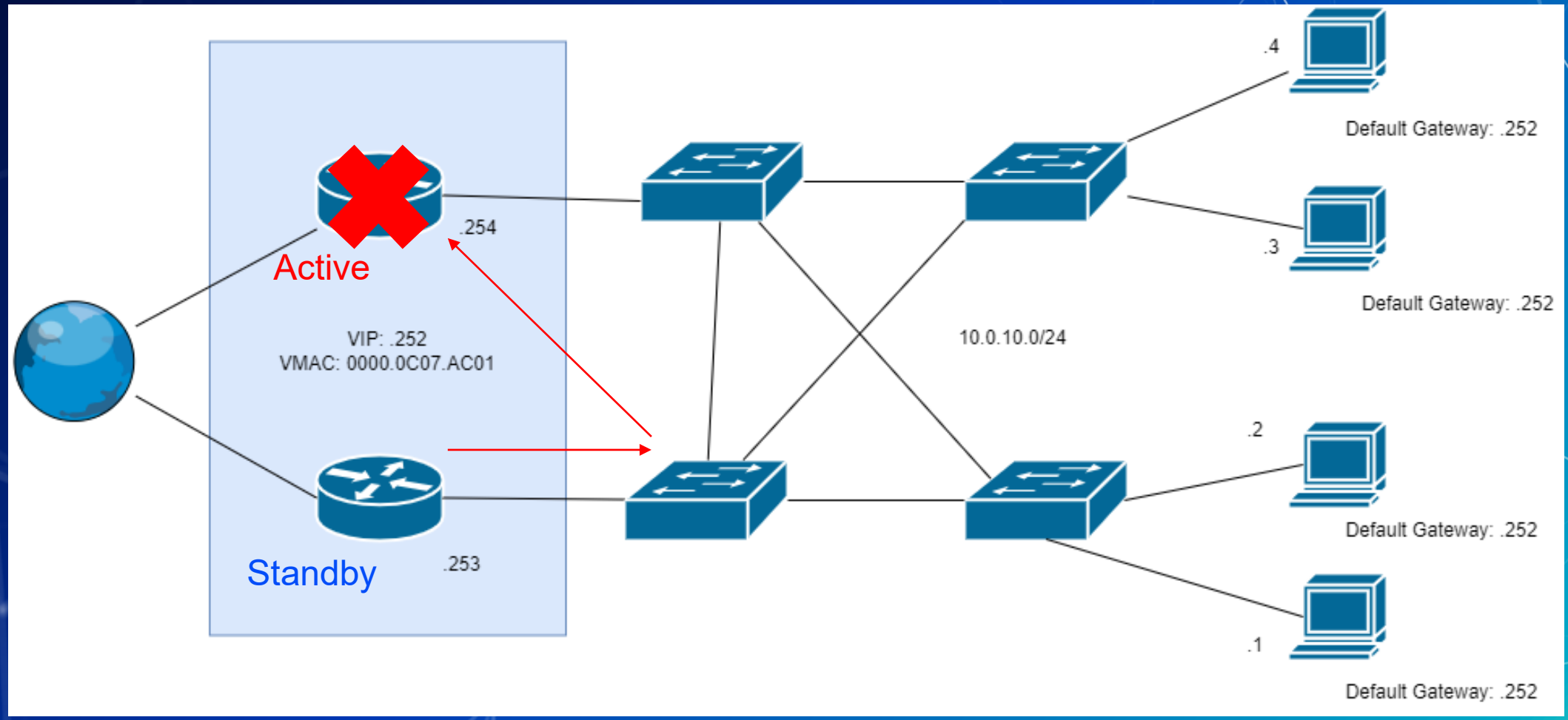

.4
Default Gateway: .252
.254
Active
.3
Default Gateway: .252
VIP: .252
VMAC: 0000.0C07.AC01
10.0.10.0/24
.2
Default Gateway: .252
Standby
.253
.1
Default Gateway: .252

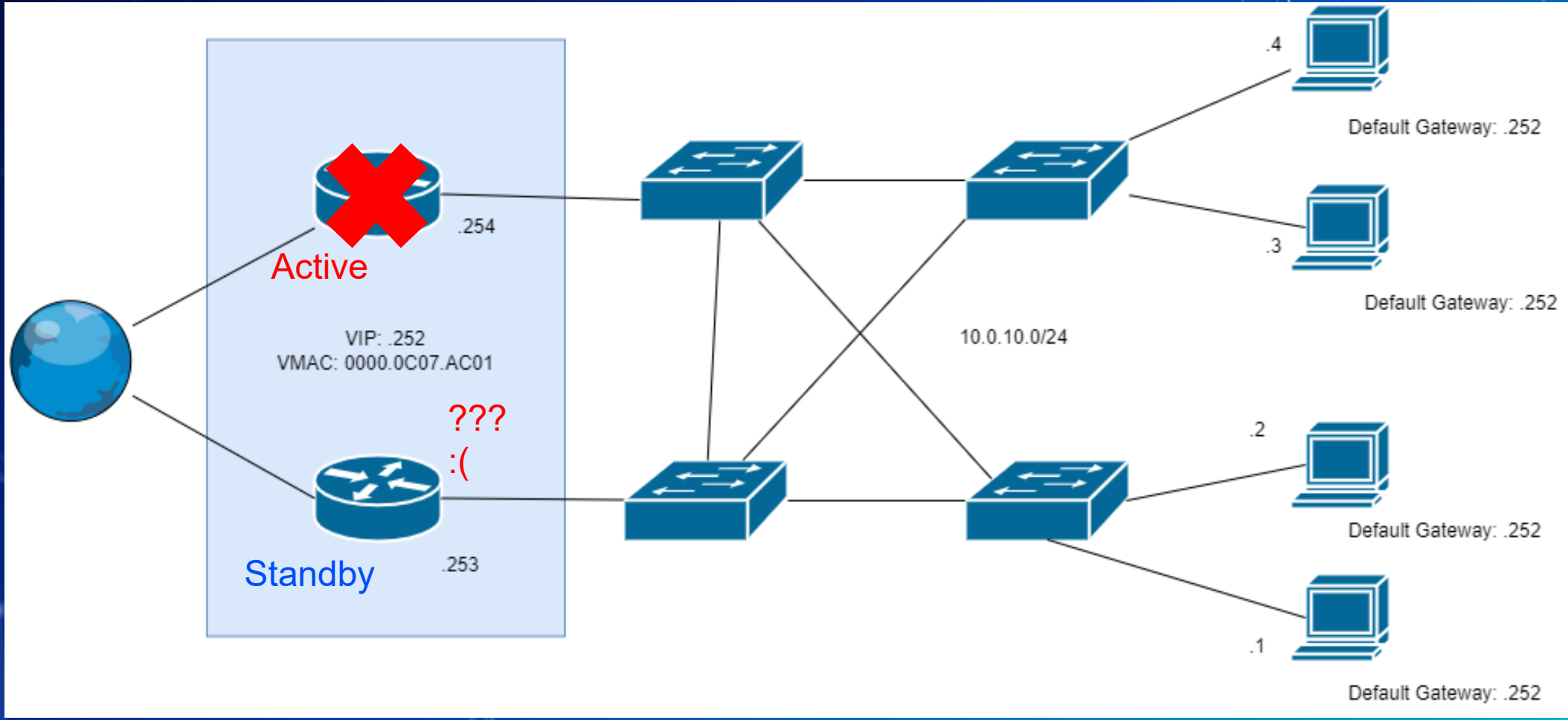

.4
Default Gateway: .252
.254
Active
.3
Default Gateway: .252
VIP: .252
VMAC: 0000.0C07.AC01
10.0.10.0/24
.2
Default Gateway: .252
Standby
.253
.1
Default Gateway: .252

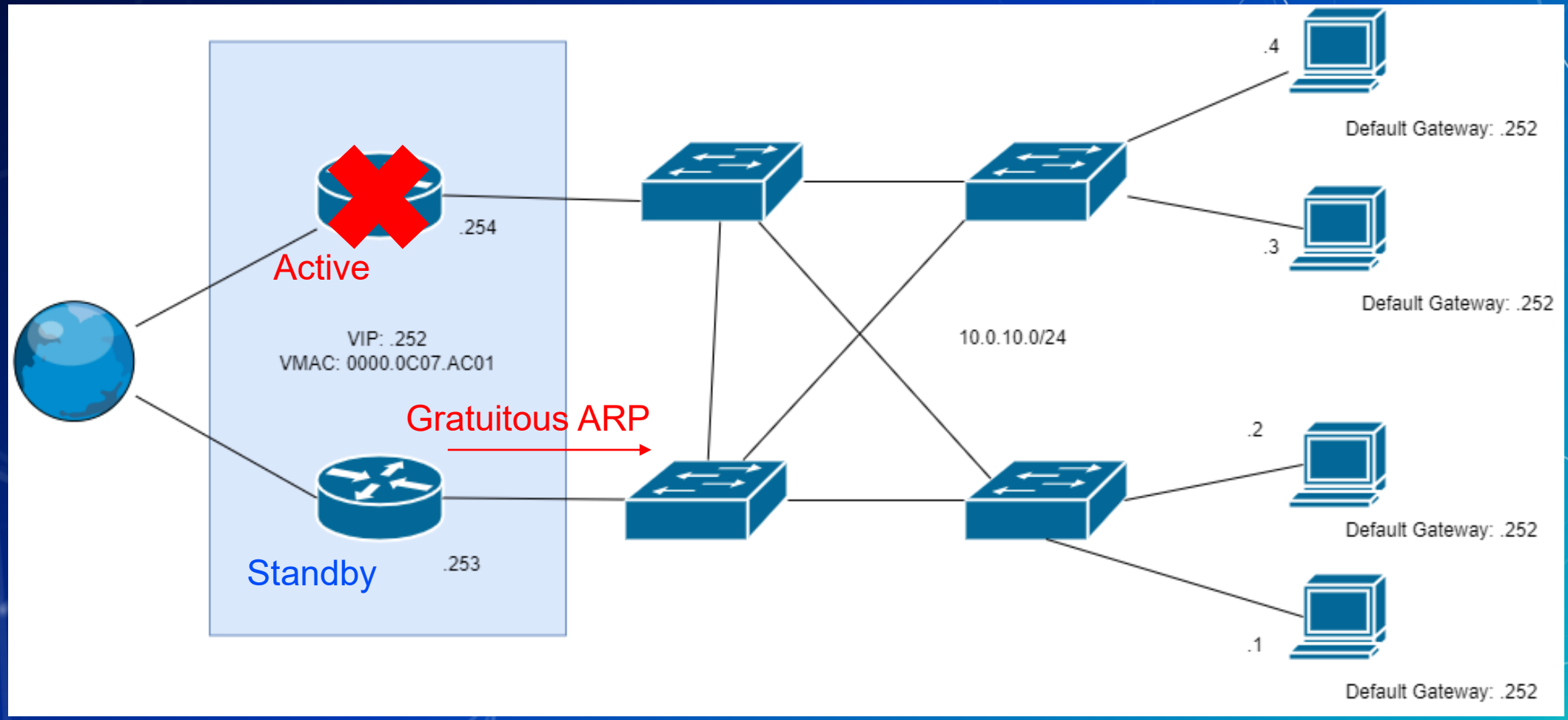

.4
Default Gateway: .252
.254
Active
.3
Default Gateway: .252
VIP: .252
VMAC: 0000.0C07.AC01
10.0.10.0/24
.2
Default Gateway: .252
Standby
.253
.1
Default Gateway: .252

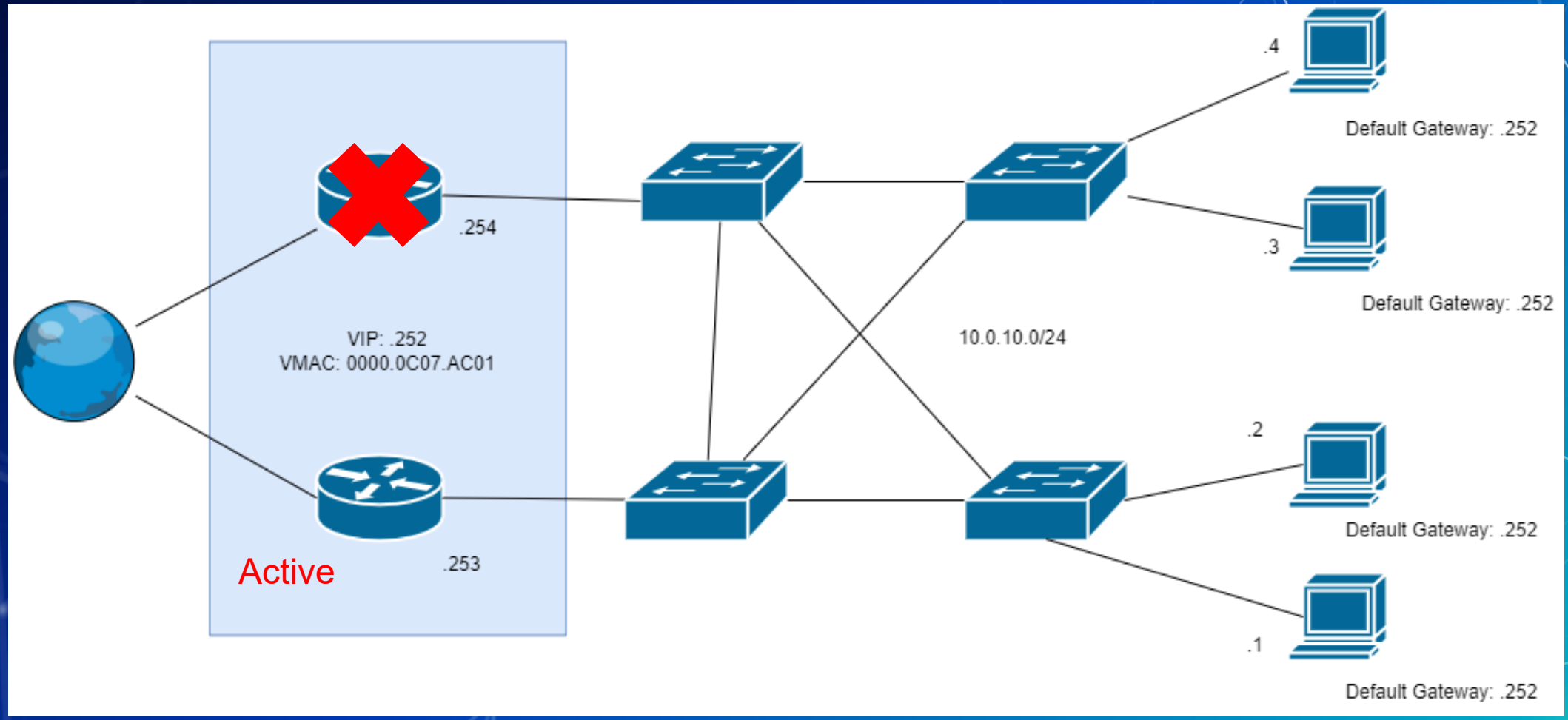

.4
Default Gateway: .252
.254
Active
.3
Default Gateway: .252
VIP: .252
VMAC: 0000.0C07.AC01
10.0.10.0/24
.2
Default Gateway: .252
Standby
.253
.1
Default Gateway: .252

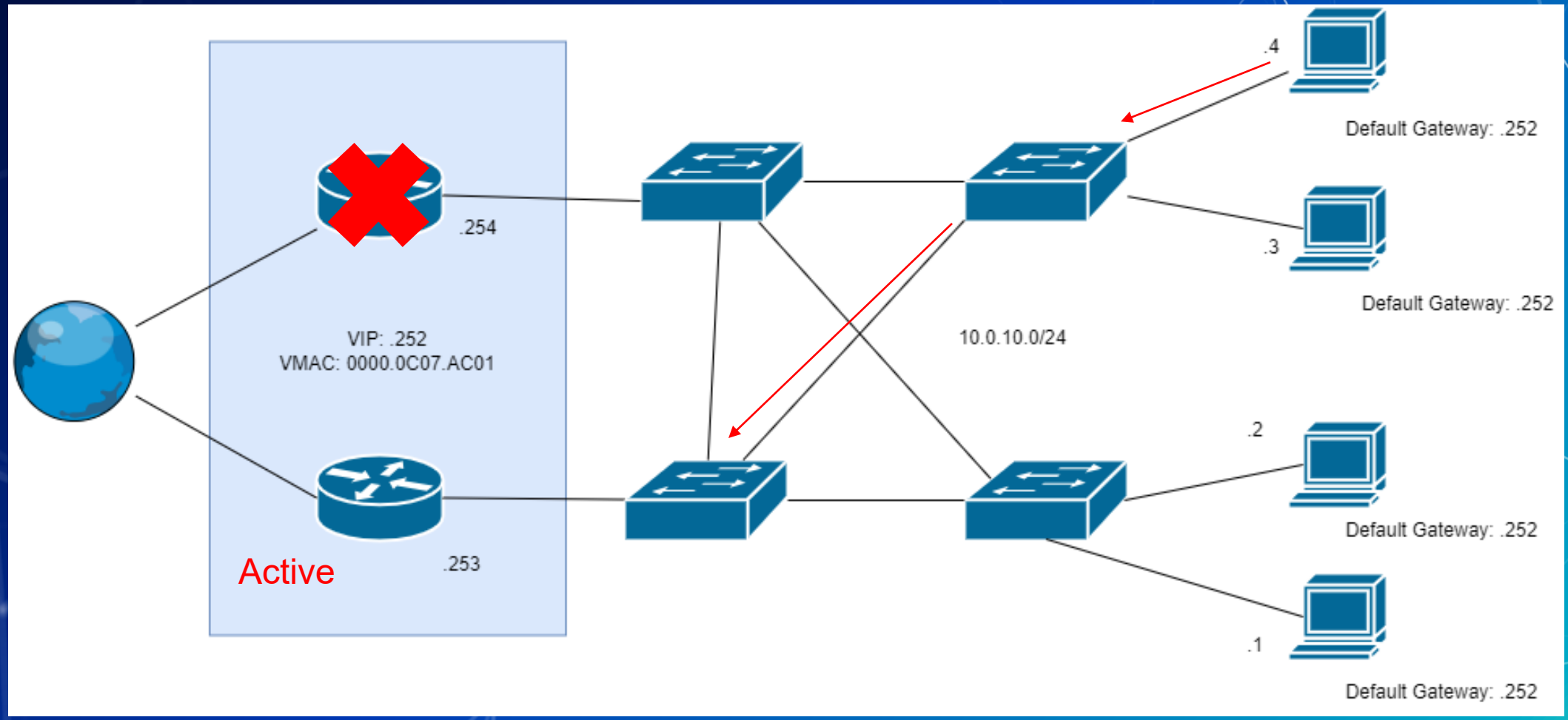

.4
Default Gateway: .252
.3
Default Gateway: .252
.254
Active
VIP: .252
VMAC: 0000.0C07.AC01
10.0.10.0/24
.2
Default Gateway: .252
Standby
.253
.1
Default Gateway: .252

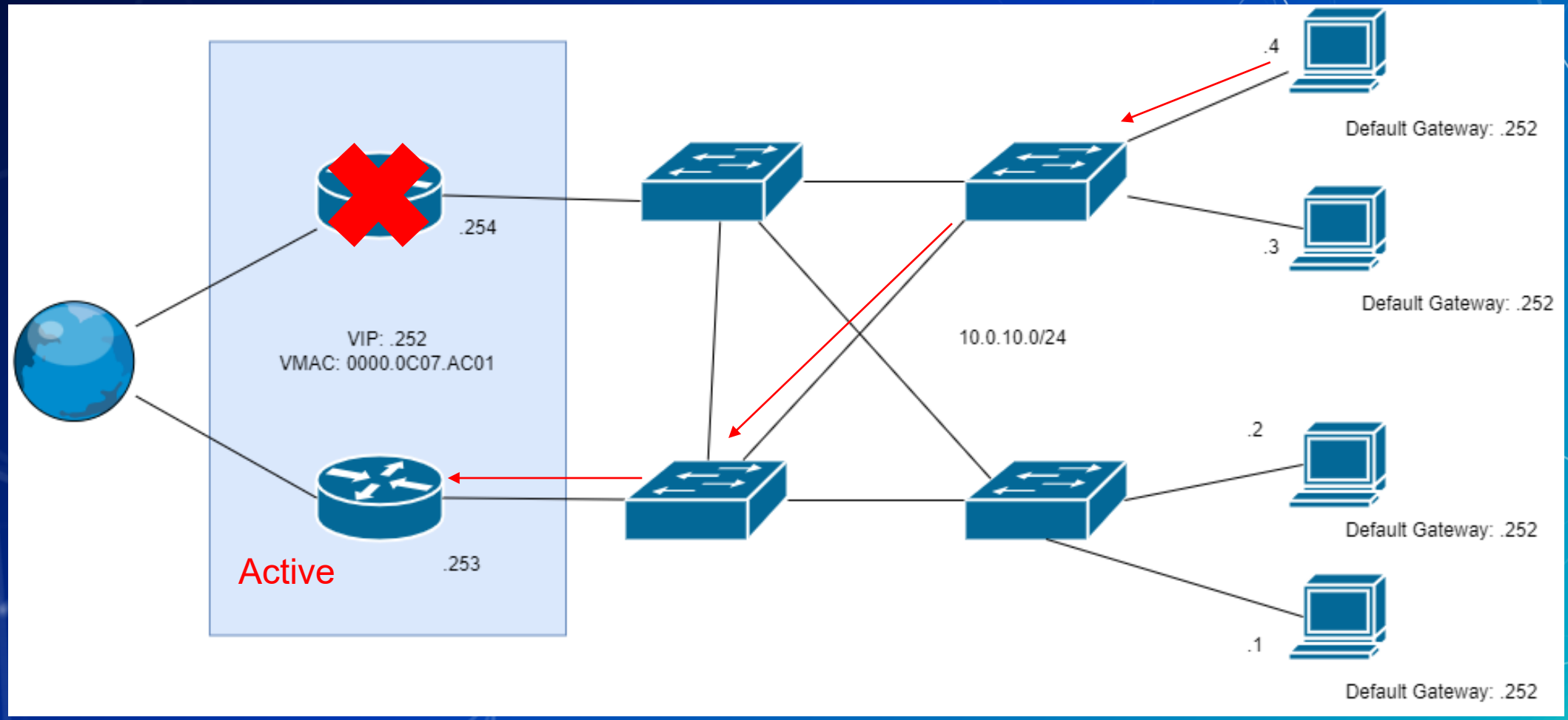

.4
Default Gateway: .252
.3
Default Gateway: .252
.254
Active
VIP: .252
VMAC: 0000.0C07.AC01
10.0.10.0/24
.2
Default Gateway: .252
Standby
.253
.1
Default Gateway: .252


.4
Default Gateway: .252
.3
Default Gateway: .252
.254
Active
VIP: .252
VMAC: 0000.0C07.AC01
10.0.10.0/24
???
:(
.2
Default Gateway: .252
Standby
.253
.1
Default Gateway: .252


.4
Default Gateway: .252
.254
Active
.3
Default Gateway: .252
VIP: .252
VMAC: 0000.0C07.AC01
10.0.10.0/24
Gratuitous ARP
.2
Default Gateway: .252
Standby
.253
.1
Default Gateway: .252


.4
Default Gateway: .252
.254
.3
Default Gateway: .252
VIP: .252
VMAC: 0000.0C07.AC01
10.0.10.0/24
.2
Default Gateway: .252
Active
.253
.1
Default Gateway: .252


.4
Default Gateway: .252
.254
.3
Default Gateway: .252
VIP: .252
VMAC: 0000.0C07.AC01
10.0.10.0/24
.2
Default Gateway: .252
Active
.253
.1
Default Gateway: .252


.4
Default Gateway: .252
.254
.3
Default Gateway: .252
VIP: .252
VMAC: 0000.0C07.AC01
10.0.10.0/24
.2
Default Gateway: .252
Active
.253
.1
Default Gateway: .252

FHRPs

- The different protocols tend to have slightly different capabilities, naming and syntax
  - Host Standby Router Protocol (HSRP)
    - Cisco proprietary
    - MAC Format: 0000:0C07:ACXX
  - Virtual router redundancy protocol (VRRP)
    - Open standard
    - Calls routers master and backup instead
    - VMAC format: 0000.5e00.01XX
  - Gateway Load Balancing Protocol (GLBP)
    - Cisco proprietary
    - VMAC format: 0007.b400.XXYY
- Load balancing also relies on a similar function to FHRPs

Break slide

Please return in 10 minutes

Agenda - Week 11

1. Networking
2. High Availability
3. **Network Architecture**
4. Wireless Technologies

Networking Architecture

Design

Small home and office (SOHO)

- Refers to a small office of a small company or small home office with few devices
- Typically consist of a home router acting as a:
  - Switch
  - Router
  - Firewall
  - Wireless access point
  - Modem

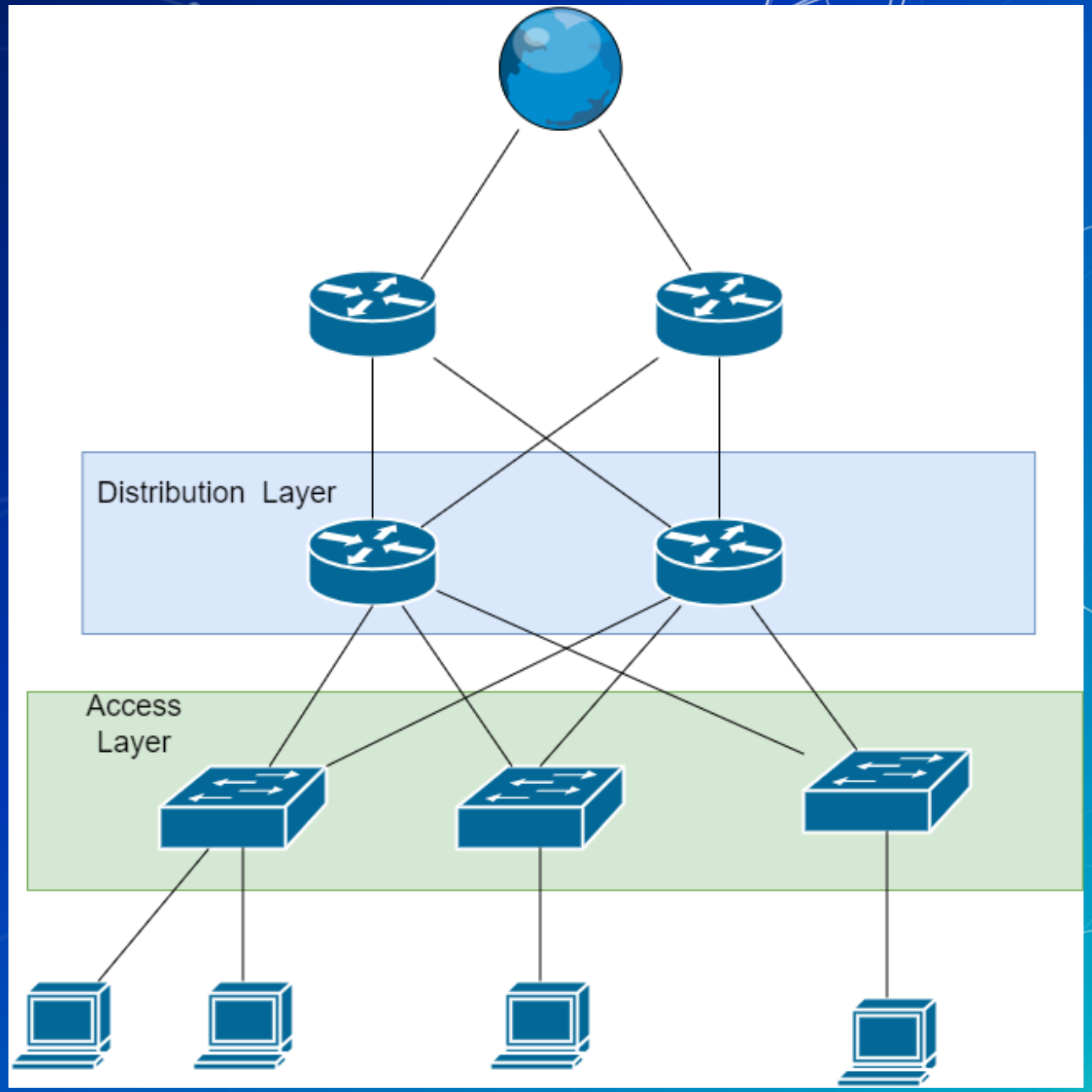
How does network architecture mature?

- The network has more redundancy built in and allows for higher bandwidth
- This is generally done through a separation of tasks based on groups of networking device
- May focus on north-south traffic or east-west traffic

2 Tier Design

- Access Layer
  - The layer that end hosts connect to
  - QoS marking is usually done here
  - Security services such as port security (ACL) is typically done here
- Distribution Layer (sometimes called collapsed core layer)
  - Usually the border between layer 2 and layer 3
  - Aggregated connections between access layer switches
  - Connects to services such as the internet

2 Tier Design

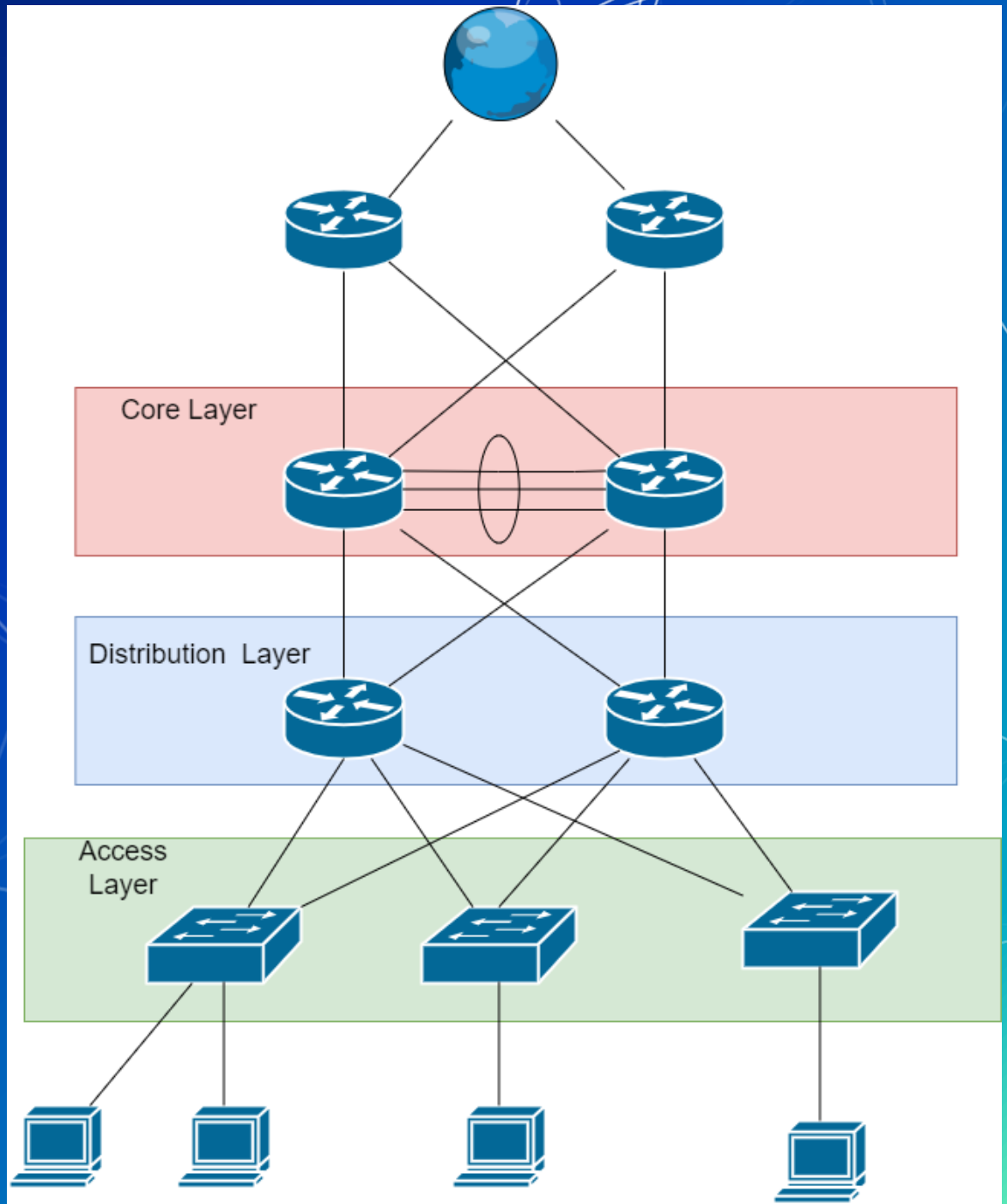


3 Tier Design

- Access layer
  - Same as prior
- Distribution layer
  - Same as prior
- Core layer
  - Connects distribution layers together
  - Often has a focus on speed
  - Connections are all layer 3

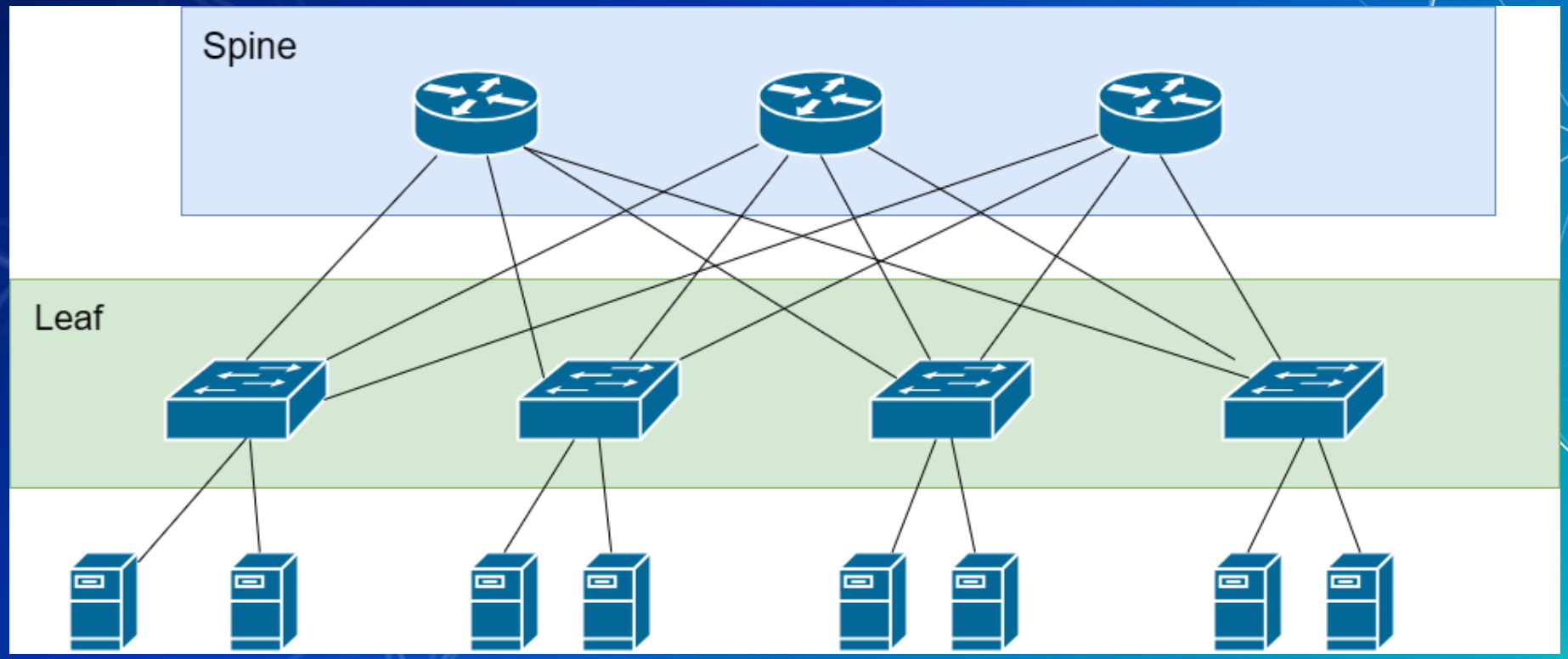
3 Tier Design

- Can anyone name a technology mentioned earlier in this lecture that is potentially being utilized in this topology?



Spine-Leaf architecture

- High redundancy topology often used in data centers
- Much more efficient for east-west traffic (between servers)



Software Defined Network (SDN)

- Uses software to define networking instead of hardware
  - vSphere

Software Defined Network

vSphere Demo

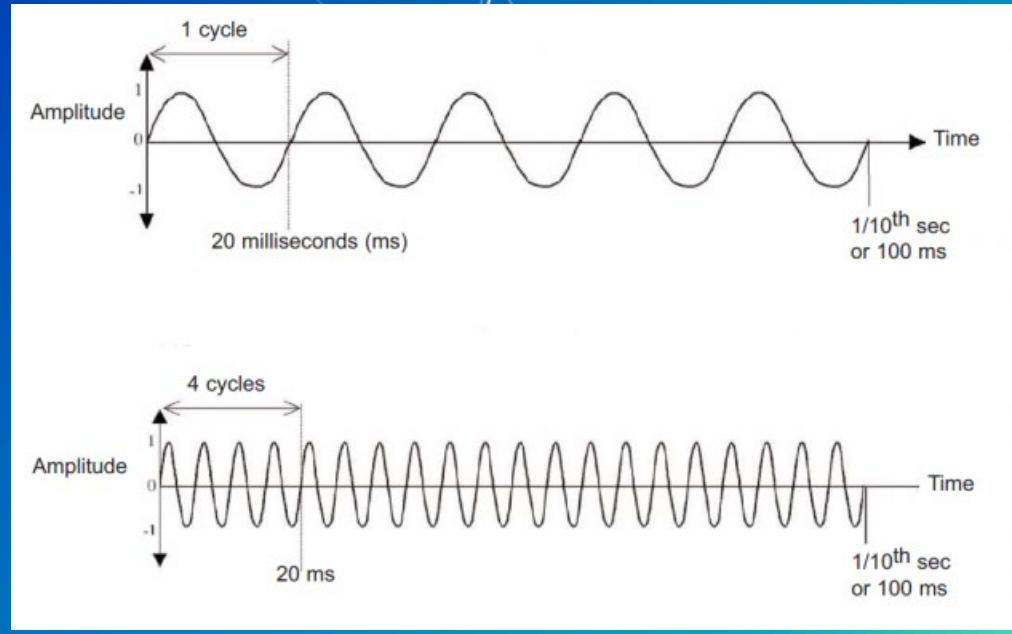
Wireless Technologies

Agenda - Week 11

1. Networking
2. High Availability
3. Network Architecture
4. **Wireless Technologies**

What are wireless technologies?

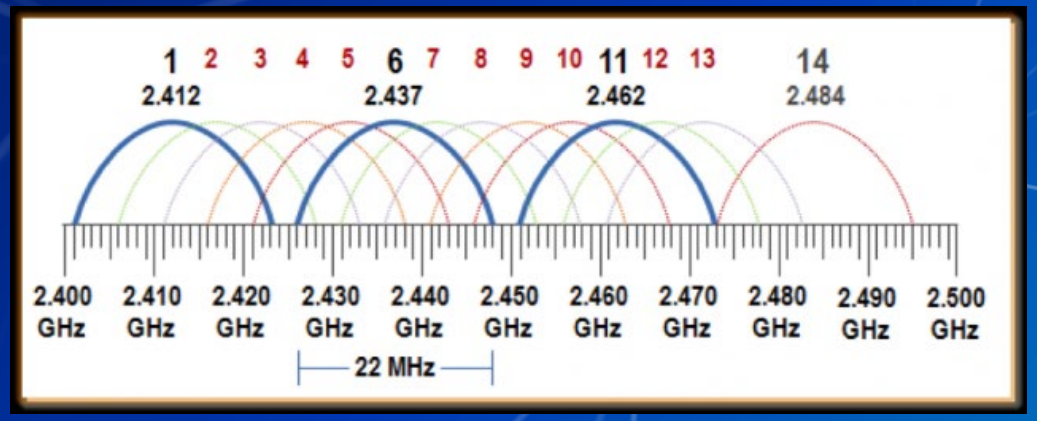
- Wi-Fi
  - This is what this portion of the lecture will focus on
- Bluetooth
- Cellular
- …Many different types of radio

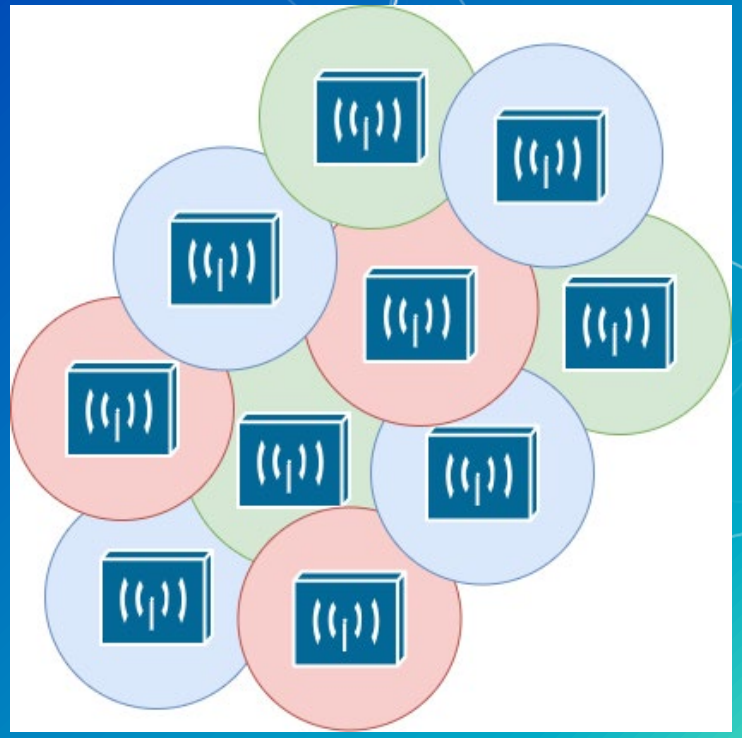


- What connects all of these?
  - They all use waveforms to transmit information
  - How this works will not be the focus

Wi-Fi

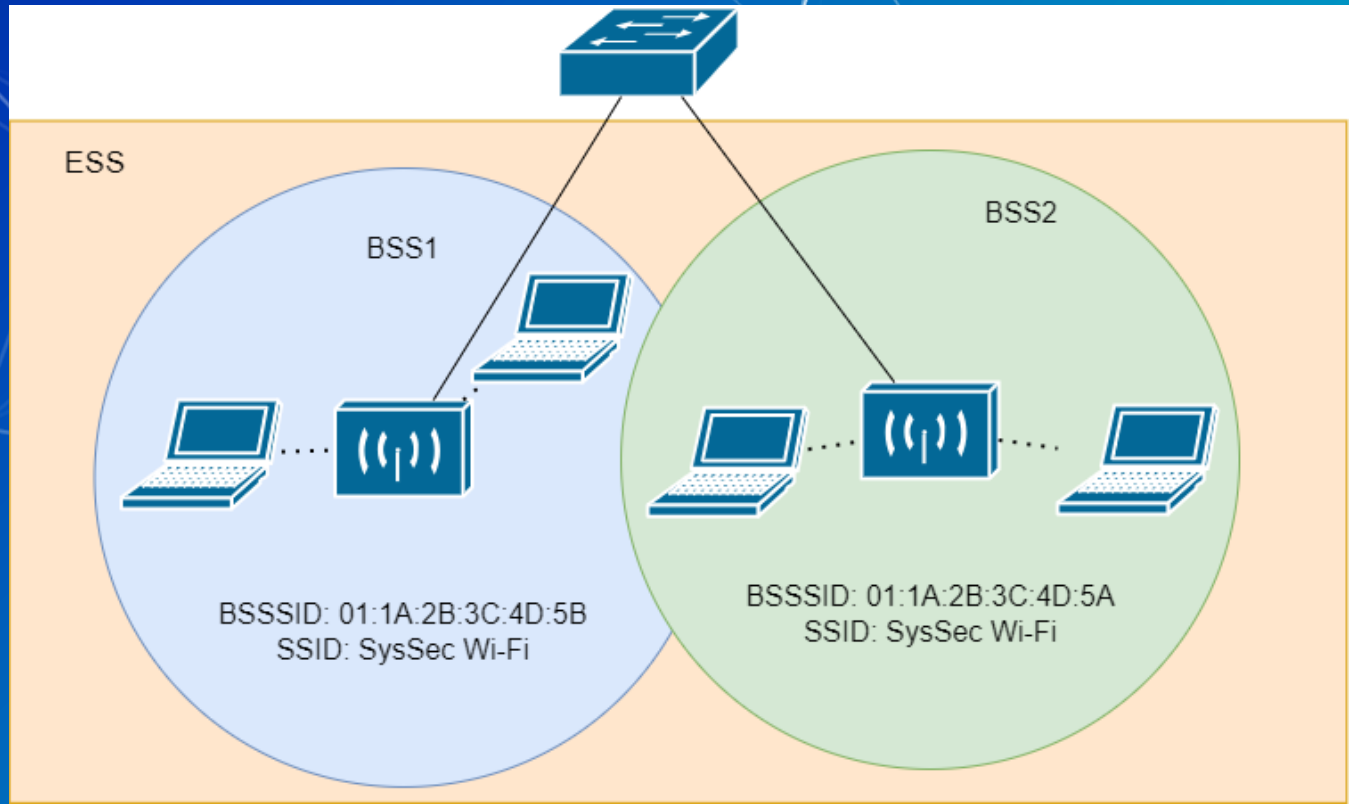
- Primary purpose is for wireless internet connectivity
- Based on the IEEE 802.11 standard
- Operates at a few different ranges (sometimes called channels)
  - 2.4 GHz
  - 5 GHz
  - 6 GHz





Wi-Fi architecture

- A basic service set (BSS) is a single area where clients connect to each other using 1 access point
  - Each have a unique set identifier (BSSSID)
    - This is pretty much a MAC address
  - They can have a shared Service Set Identifier (SSID)
    - This is the network name
- Combine BSS's to create a larger Extended Service Set (ESS)



Generations of Wi-Fi

- Wikipedia has a good table showing this
- Over time speeds have become significantly faster

Generation	IEEE standard	Adopted	Maximum link rate (Mbit/s)	Radio frequency (GHz)
Wi-Fi 8	802.11bn	2028	100,000[44]	2.4, 5, 6, 7, 42.5, 71[45]
Wi-Fi 7	802.11be	2024	1376–46,120	2.4, 5, 6[46]
Wi-Fi 6E	802.11ax	2020	574–9608[47]	6[b]
Wi-Fi 6		2019		2.4, 5
Wi-Fi 5	802.11ac	2014	433–6933	5[c]
Wi-Fi 4	802.11n	2008	72–600	2.4, 5
*(Wi-Fi 3)**	802.11g	2003	6–54	2.4
*(Wi-Fi 2)**	802.11a	1999		5
*(Wi-Fi 1)**	802.11b	1999	1–11	2.4
*(Wi-Fi 0)**	802.11	1997	1–2	2.4

Wi-Fi Security

- Wi-Fi has also become more secure over time with improved authentication and encryption mechanisms
- WEP (Wired Equivalent Privacy)
  - Very flawed and has many, many vulnerabilities
    - Ratified in 1999
- WPA (Wi-Fi Protected Access)
  - Ratified in 2003 as a replacement to known vulnerable WEP
  - WPA2
    - Ratified in 2004
    - Two authentication modes
      - Personal mode: Uses a pre shared key (home wifi)
        - Uses a four way handshake
      - Enterprise mode: Uses an authentication server and a form of EAP
  - WPA3
    - Ratified in 2018
    - New security features
      - Simultaneous authentication of equals
      - Forward Secrecy
      - Better protected management frames

Authentication Mechanisms

- Extensible Authentication Protocol (EAP)
  - EAP-FAST
  - PEEP
  - EAP-TLS
  - EAP-TTLS
- Authentication Server
  - Radius/Diameter
  - LDAP
  - TACACS+

Parting Questions?

Now is the time!

Class Dismissed

See you next week!