Ethernet Fundamentals

CompTIA Network+ (N10-007)

Ethernet Fundamentals

- In early computer networks, there were many different network technologies competing for a portion of the market share
- Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), and others fought for dominance
- Currently, Ethernet is dominant for Layer 1
- Due to Ethernet's popularity, it is important to understand the fundamentals of Ethernet

Origins of Ethernet

- Was first run over coax cables (10Base5, 10Base2)

- Ethernet has changed to using twisted pair cables

- 10BASE-T is Unshielded Twisted Pair
  - Maximum speed: 10 Mbps
  - Maximum distance: 100 meters

How should devices access the network?

- Deterministic
  - Very organized and orderly
  - Need an electronic token to transmit
  - For example, Token Ring networks

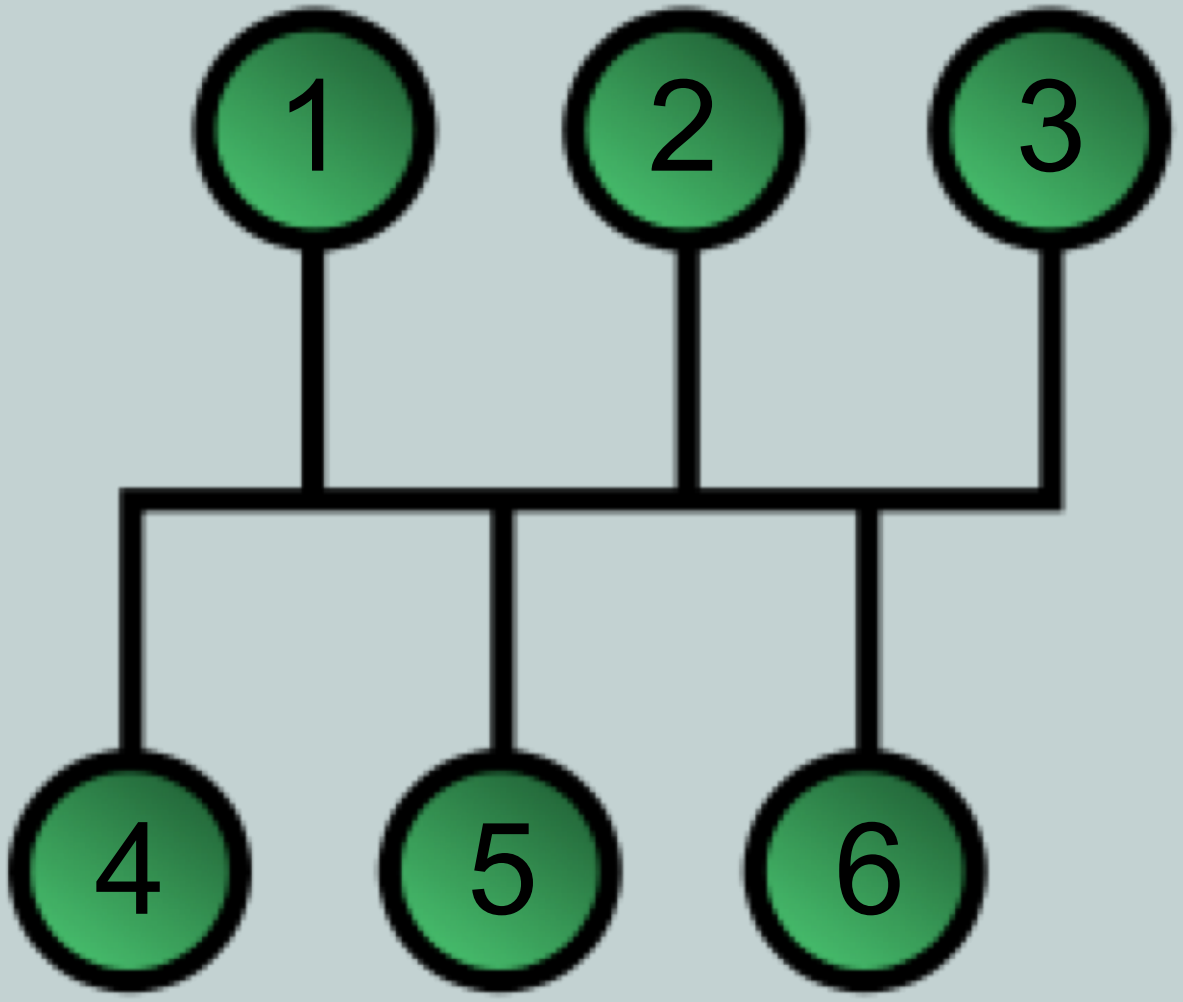
- Contention-based
  - Very chaotic
  - Transmit (almost) whenever you want
  - For example, Ethernet networks

Carrier Sense Multiple Access/ Collision Detect (CSMA/CD)

- Ethernet devices transmit based on a principle called *carrier sense multiple access/collision detect* (CSMA/CD)

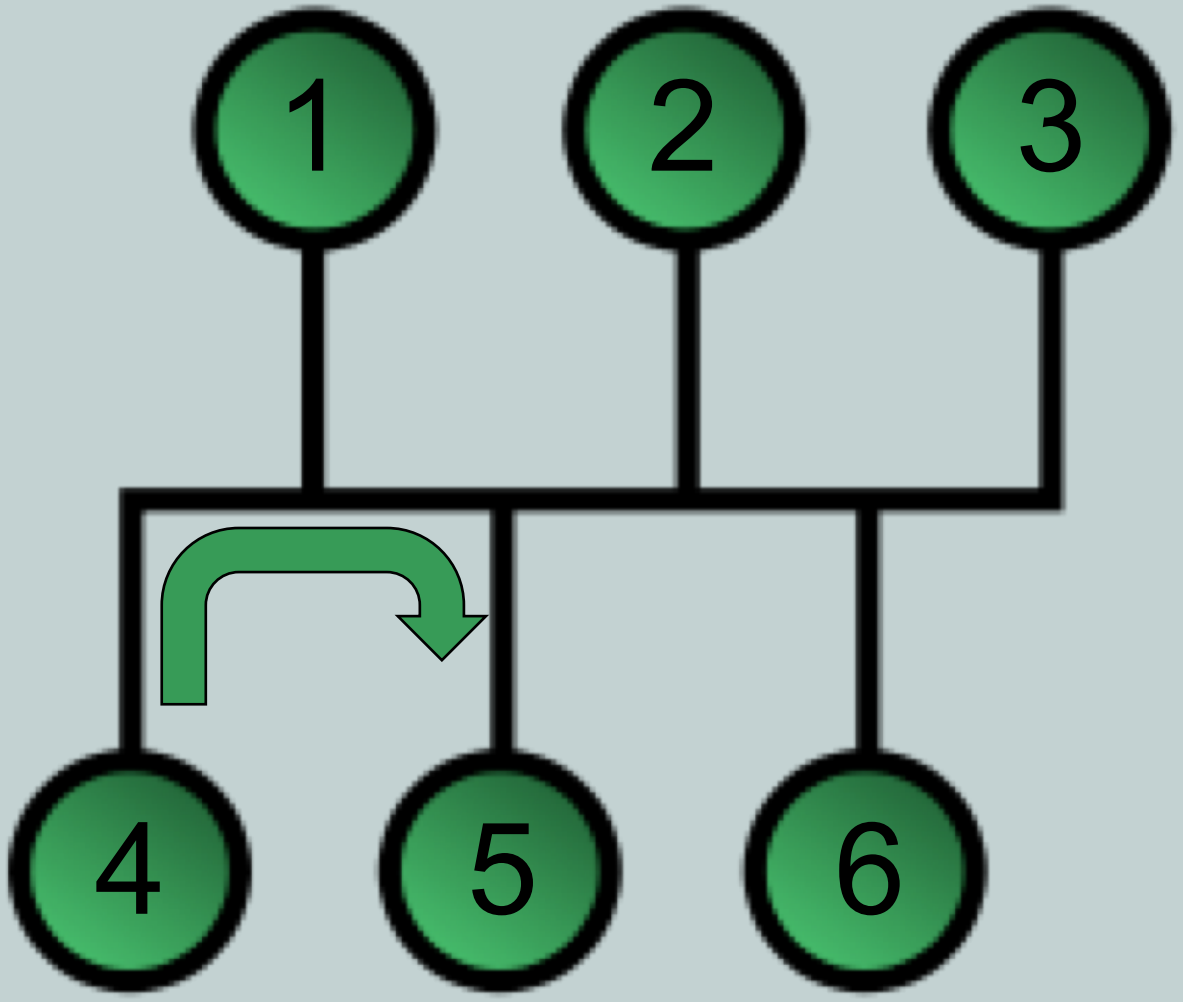
- Carrier sense
  - Listen to the wire, verify it is not busy
- Multiple access
  - All devices have access at any time
- Collision detect
  - If two devices transmit at the same time, a *collision* occurs
  - Back off, wait a random time, and try again

Example of CSMA/CD



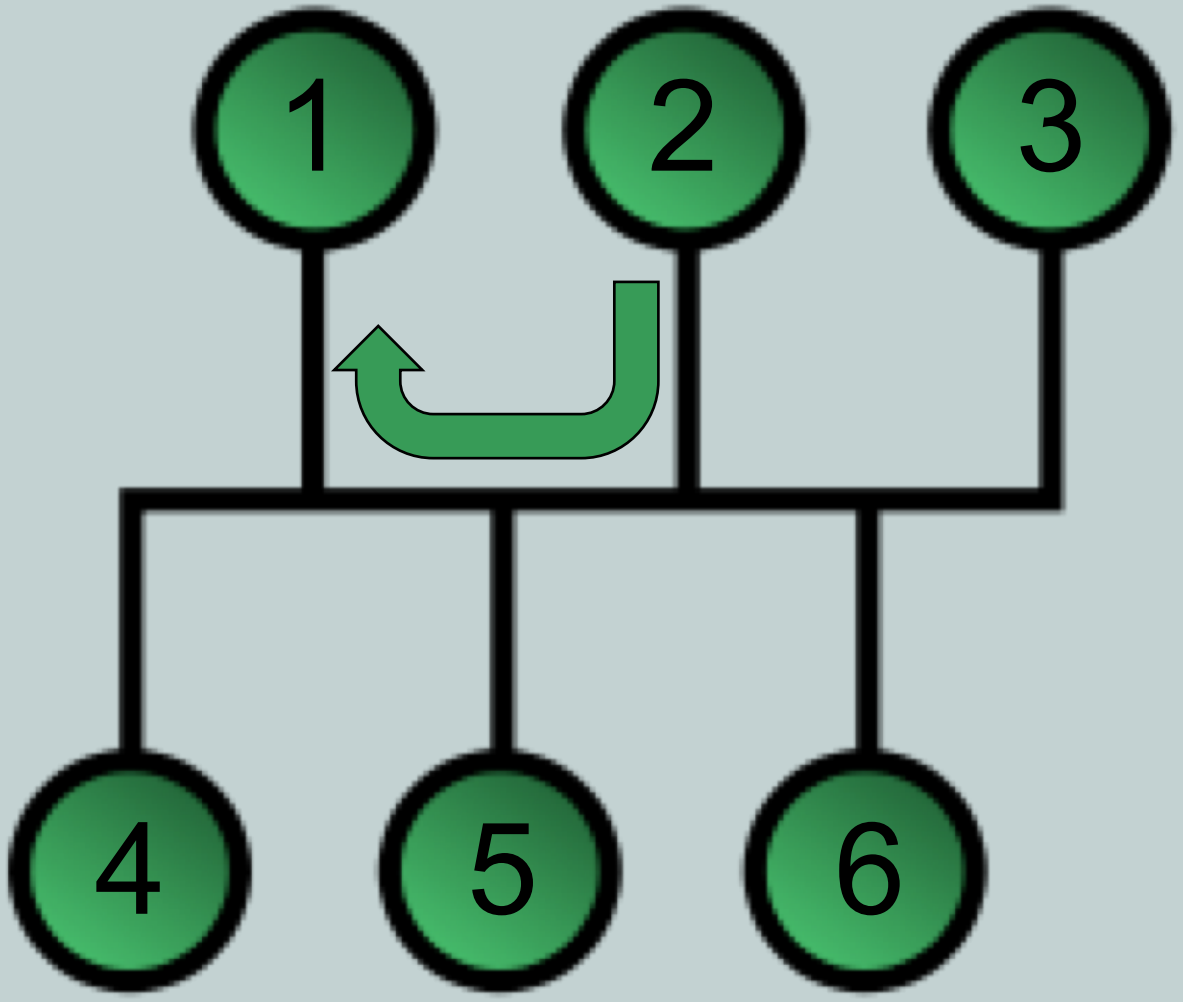
Ethernet devices on a shared network segment

Example of CSMA/CD



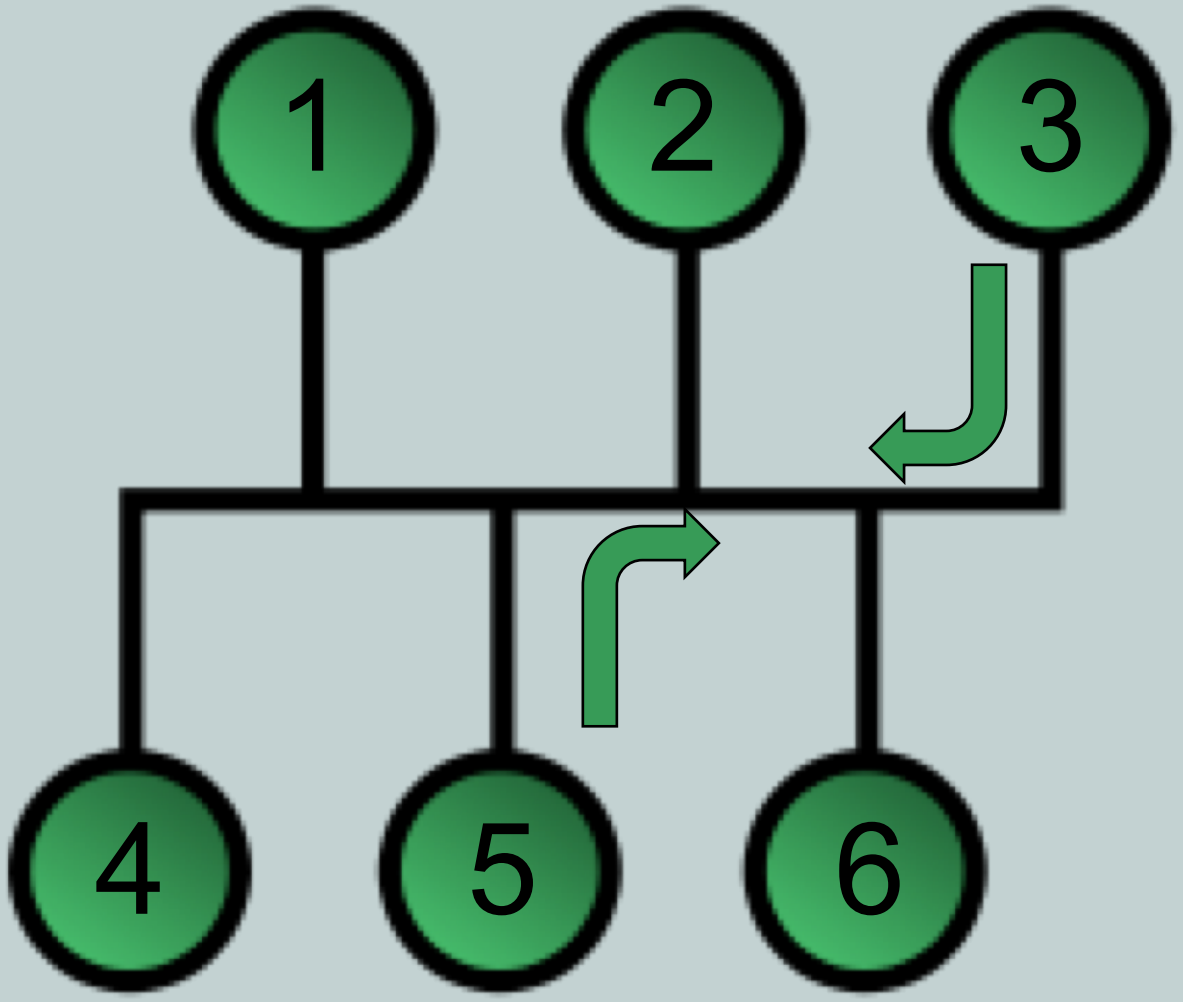
Communication on an Ethernet segment

Example of CSMA/CD



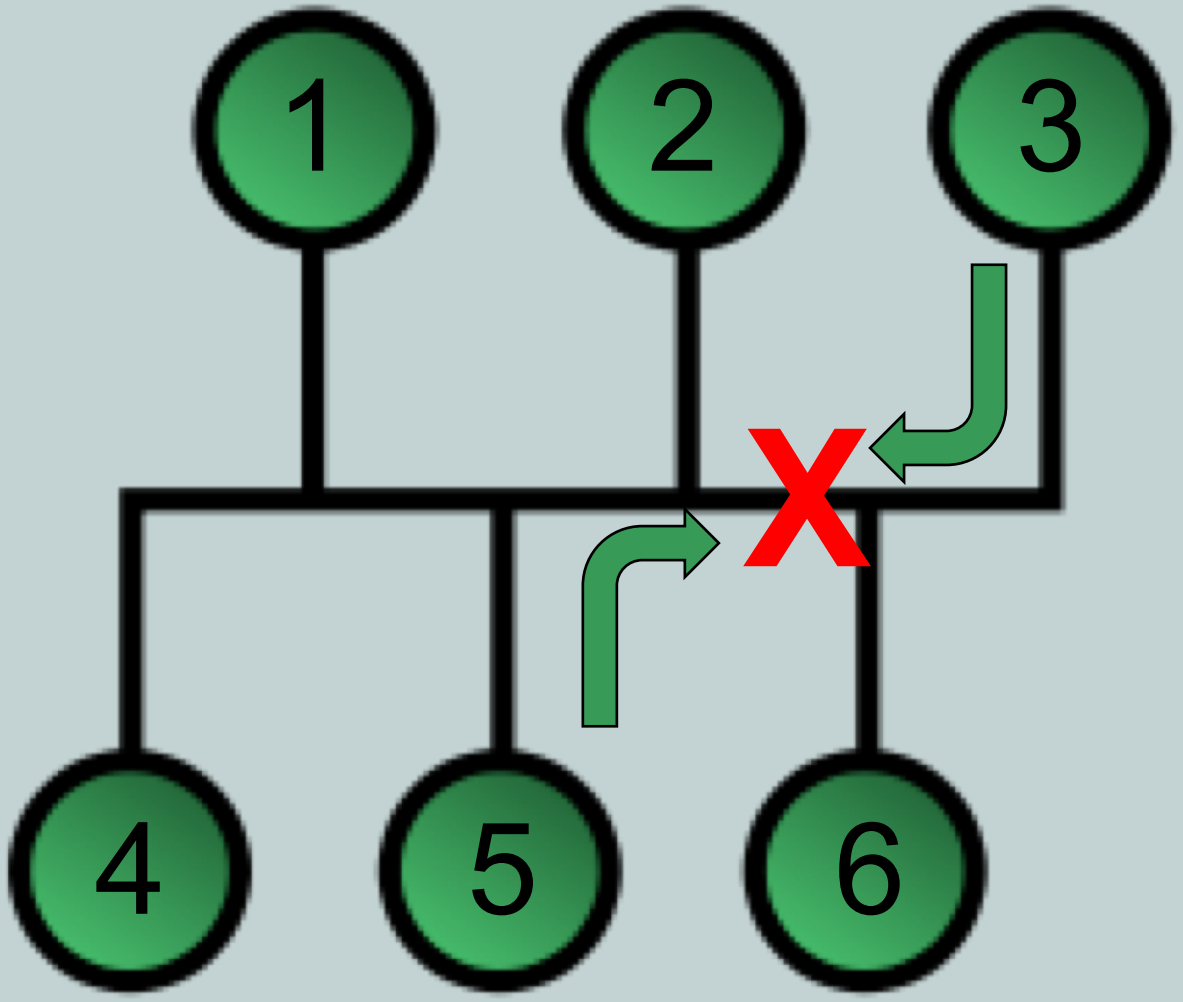
Communication on an Ethernet segment

Example of CSMA/CD



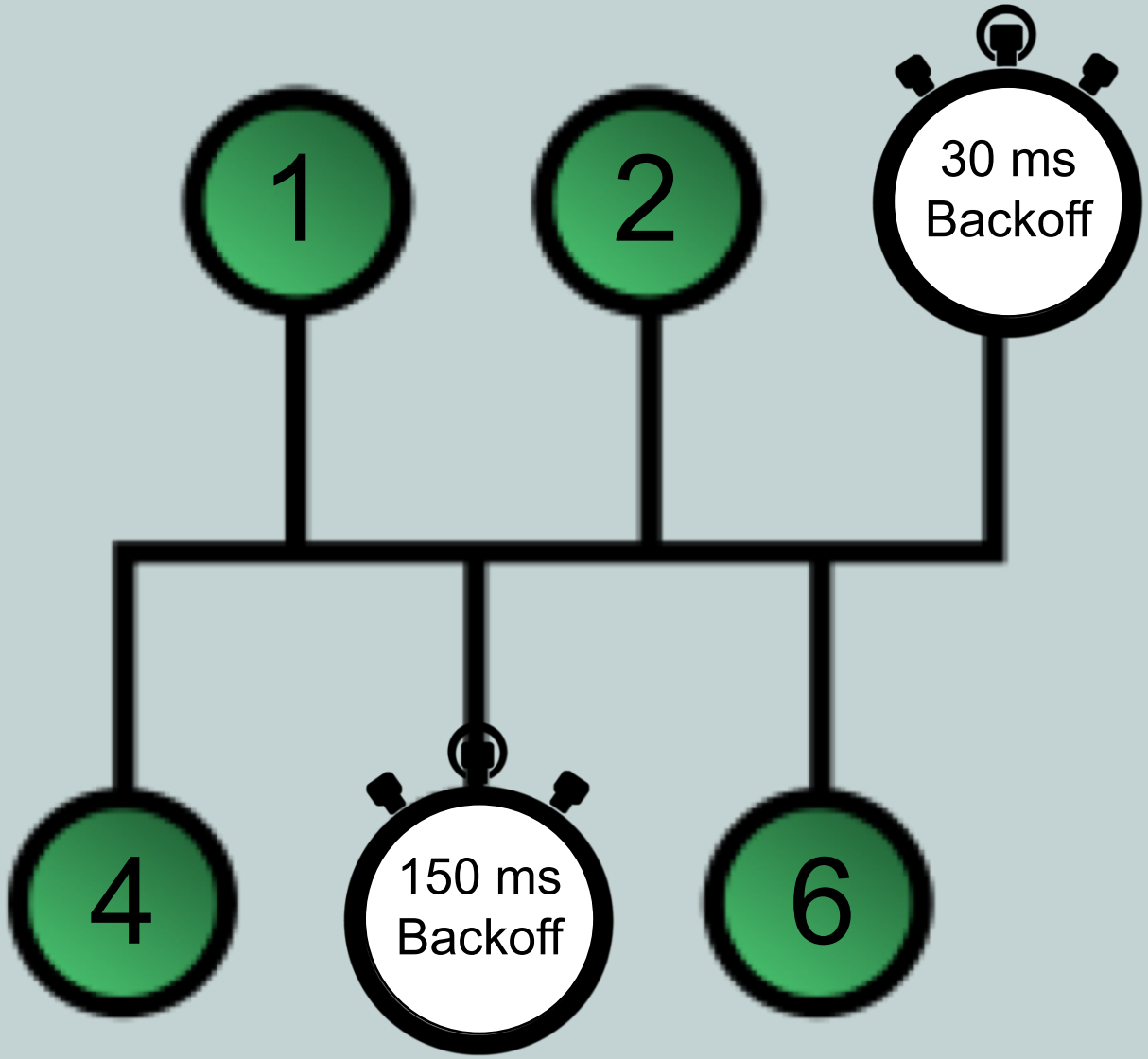
Collision on an Ethernet segment

Example of CSMA/CD



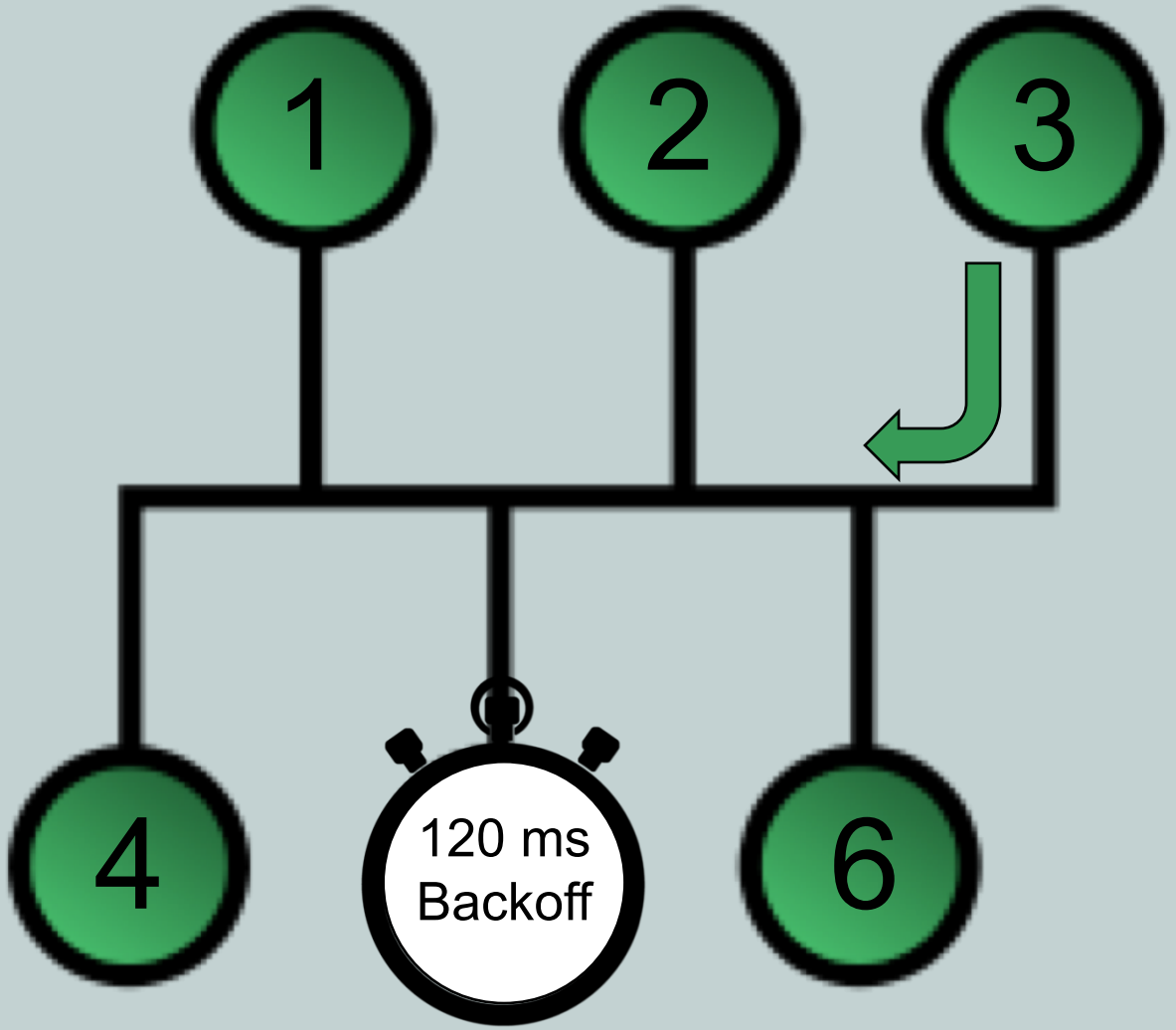
Collision on an Ethernet segment

Example of CSMA/CD



Recovering from a collision with random backoff timers

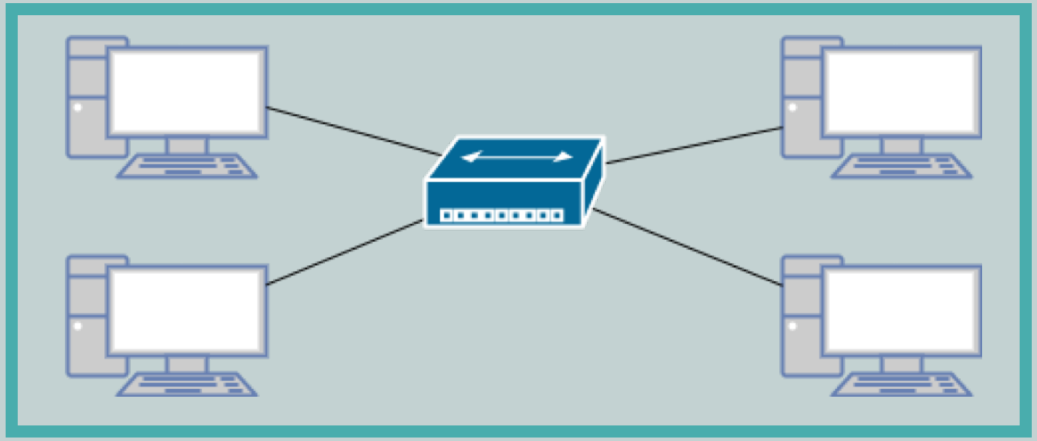
Example of CSMA/CD



Traffic flowing again while other device waits for timer

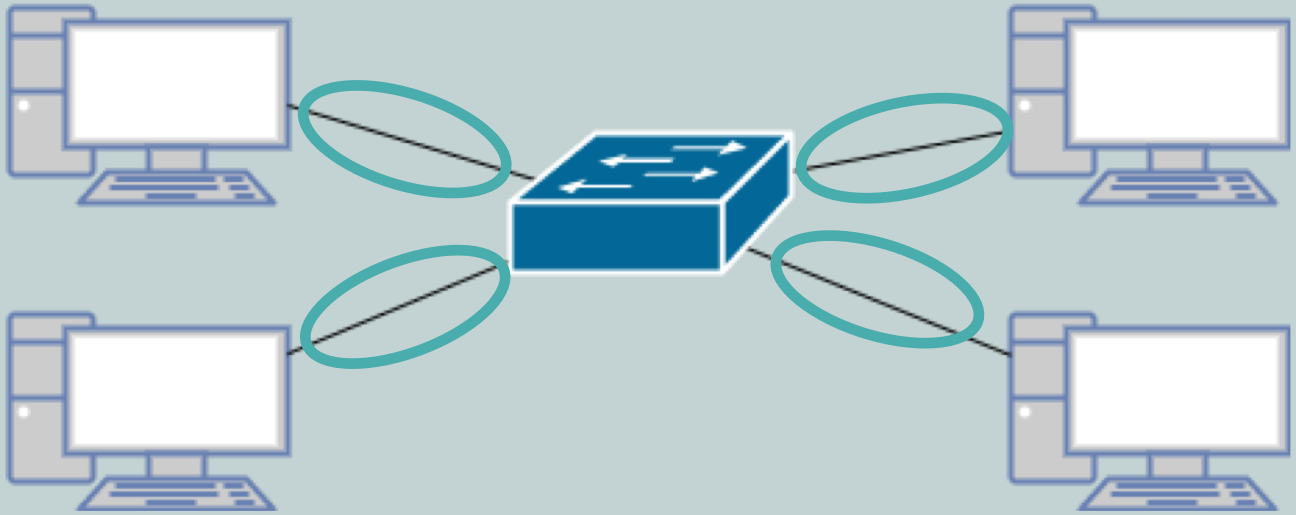
Collision Domains

- Comprised of all devices on a shared Ethernet segment (everything on same cable or hub)
- Devices operate at half-duplex when connected to a hub (Layer 1 device)
- Devices must listen before they transmit to avoid collisions when operating as CSMA/CD



Collision Domains with Switches

- Ethernet switches increase scalability of the network by creating multiple collision domains
- Each port on a switch is a collision domain, no chance of collisions, and increases speed
- Switches can operate in full-duplex mode



Speed Limitations

Ethernet Type	Bandwidth Capacity	Description
Ethernet	10 Mbps	10 million bits per second
Fast Ethernet	100 Mbps	100 million bits per second
Gigabit Ethernet	1000 Mbps (1 Gbps)	1 billion bits per second
10-Gigabit Ethernet	10 Gbps	10 billion bits per second
100-Gigabit Ethernet	100 Gbps	100 billion bits per second

- Bandwidth is the measure of how many bits the network can transmit in 1-second (bps)

- Type of cable determines the bandwidth capacity of the network

Distance Limitations

Ethernet Standard	Media Type	Bandwidth Capacity	Distance Limitation
10BASE-T	Cat 3 or higher	10 Mbps	100 m
100BASE-TX	Cat 5 or higher	100 Mbps	100 m
1000BASE-TX	Cat 6 or higher	1 Gbps	100 m
1000BASE-SX	MMF	1 Gbps	220 m
1000BASE-LX	MMF	1 Gbps	550 m
1000BASE-LX	SMF	1 Gbps	5 km
1000BASE-ZX	SMF	1 Gbps	70 km

Type of cable determines the distance limitation of the network

*** Not an exhaustive list of cable types ***

Network Infrastructure Devices

CompTIA Network+ (N10-007)

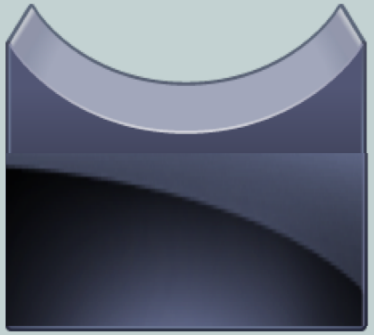
Network Infrastructure

- Primary devices used in our networks

Router

Switch

- Devices they evolved from



Bridge

Hub

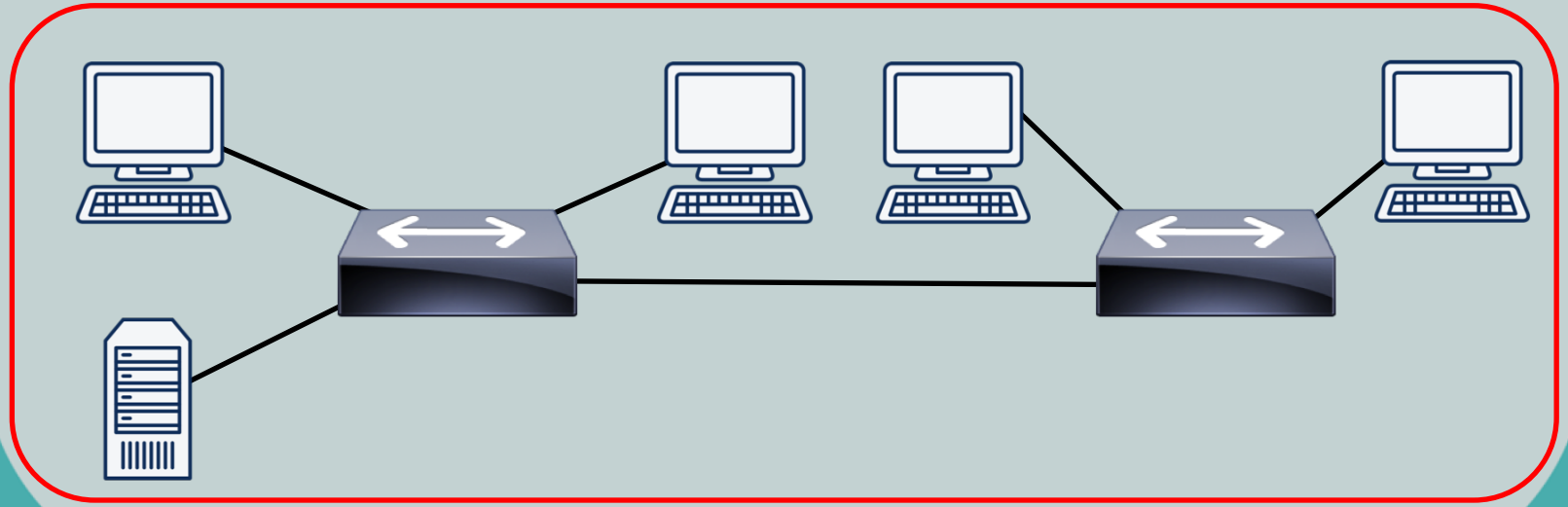
Hub

- Layer 1 device used to connect multiple network devices/workstations

- Known as *multiport repeaters*
- Three basic types of Ethernet hubs:
  - Passive hub
    - Repeats signal with no amplification
  - Active hub
    - Repeats signal with amplification
  - Smart hub
    - Active hub with enhanced features like SNMP

Collision Domains

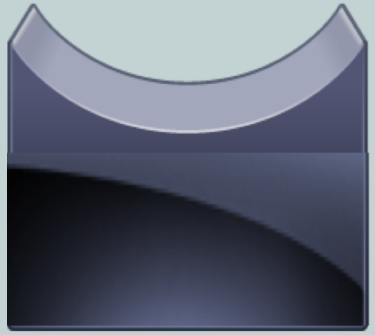
- Hubs (layer 1) were used to connect multiple network segments together
- Each LAN segment becomes a separate *collision* domain



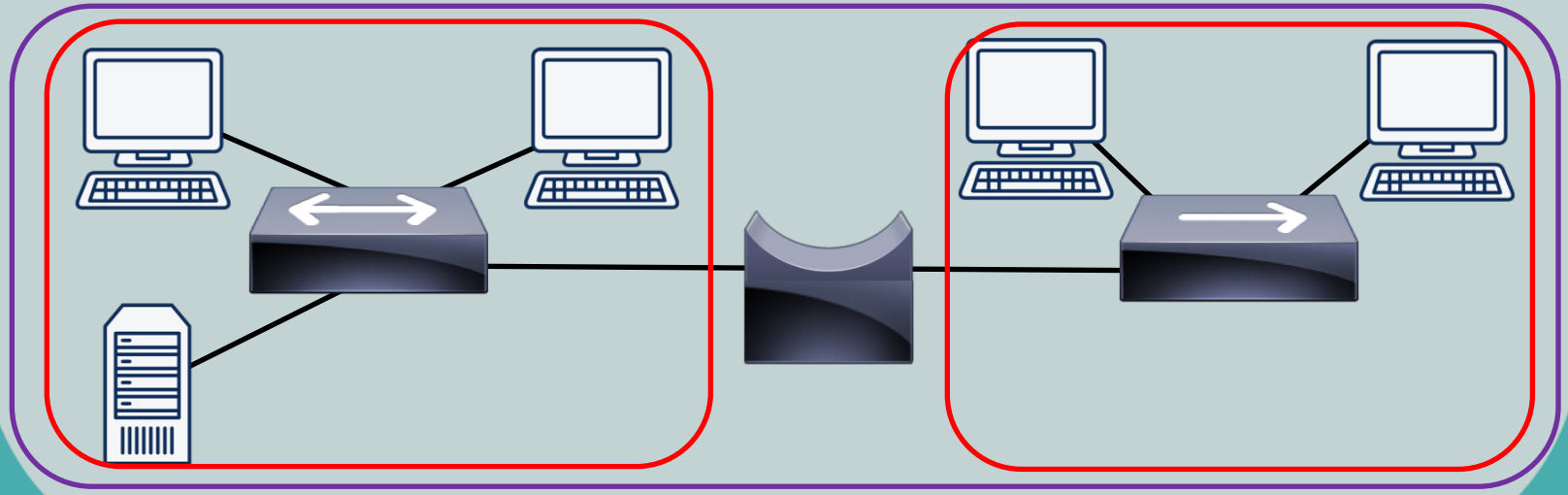
Collision Domain

Bridges

- Bridges analyze *source* MAC addresses in frames entering the bridge and populate an internal MAC address table



- Make intelligent forwarding decisions based on *destination* MAC address in the frames



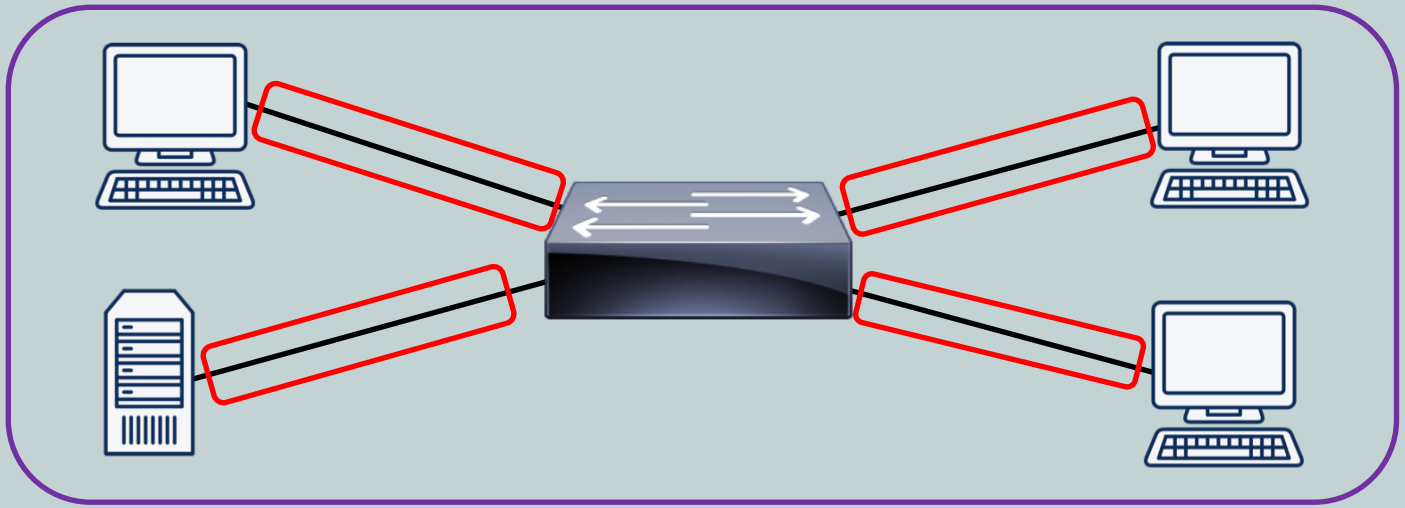
Switch

- Layer 2 device used to connect multiple network segments together

- Essentially a multiport bridge
- Switches learn MAC addresses and make forwarding decisions based on them
- Switches analyze *source* MAC addresses in frames entering the switch and populate an internal MAC address table based on them

Layer 2 Switch

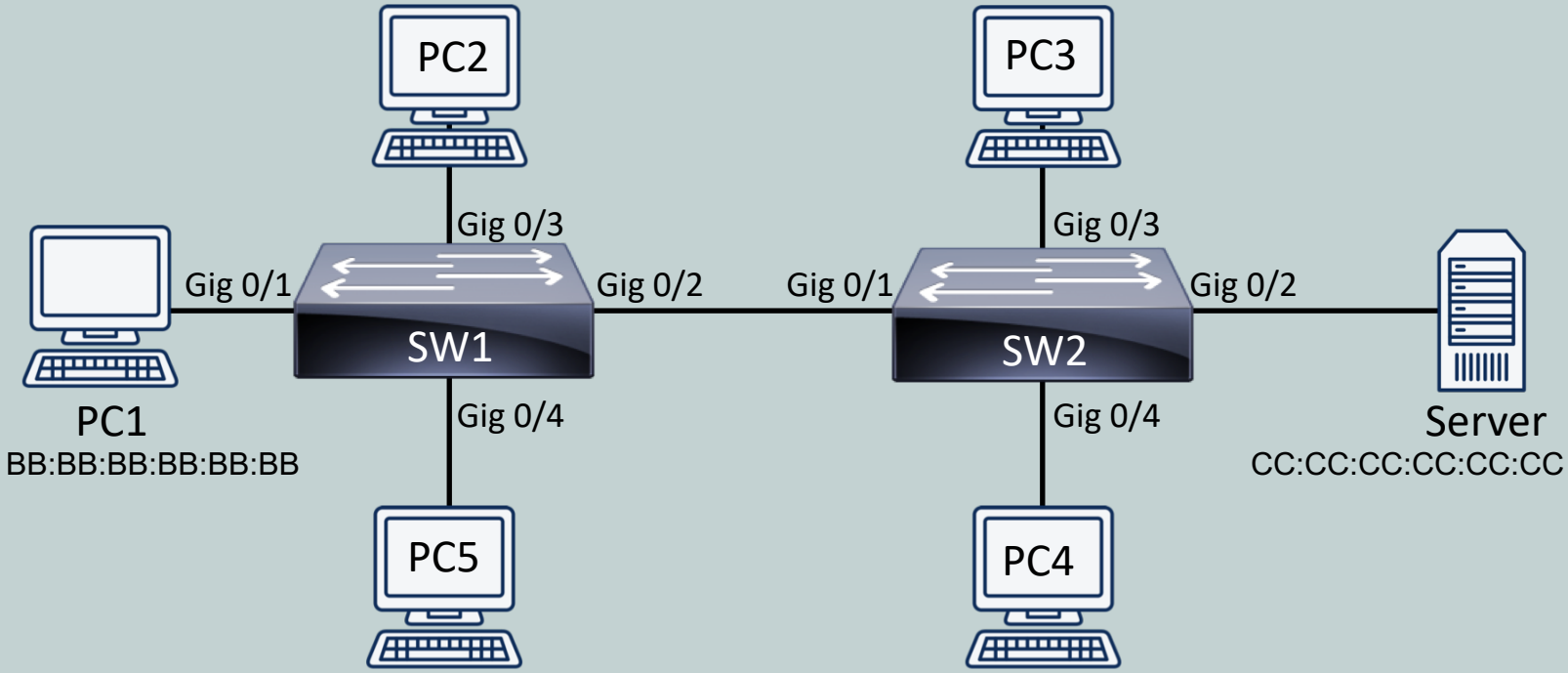
- Each port on a switch represents an individual collision domain
- All ports belong to the same broadcast domain



Collision Domain

Broadcast Domain

How Switches Improve Network Performance



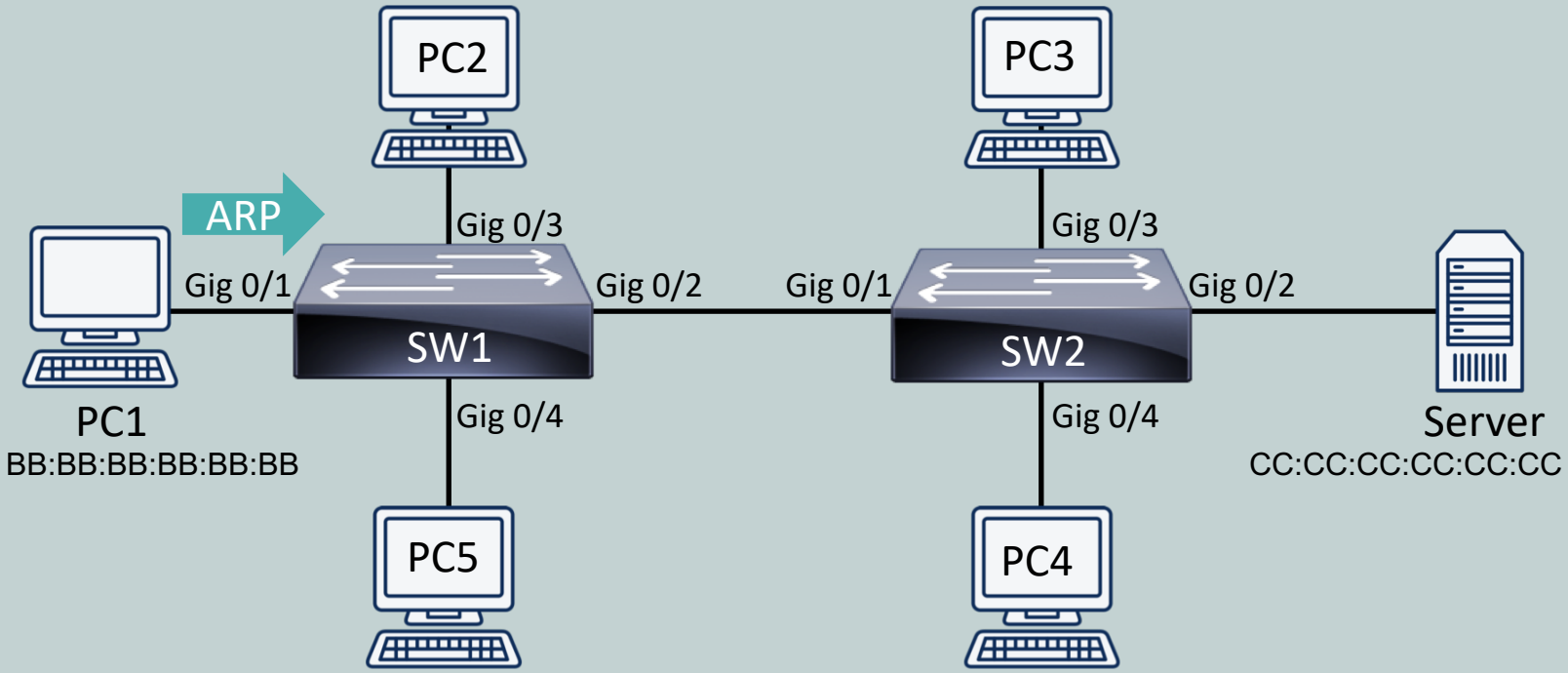
Port	MAC Address
Gig 0/1	Empty
Gig 0/2	Empty

Switch 1
MAC Address Table

Port	MAC Address
Gig 0/1	Empty
Gig 0/2	Empty

Switch 2
MAC Address Table

How Switches Improve Network Performance



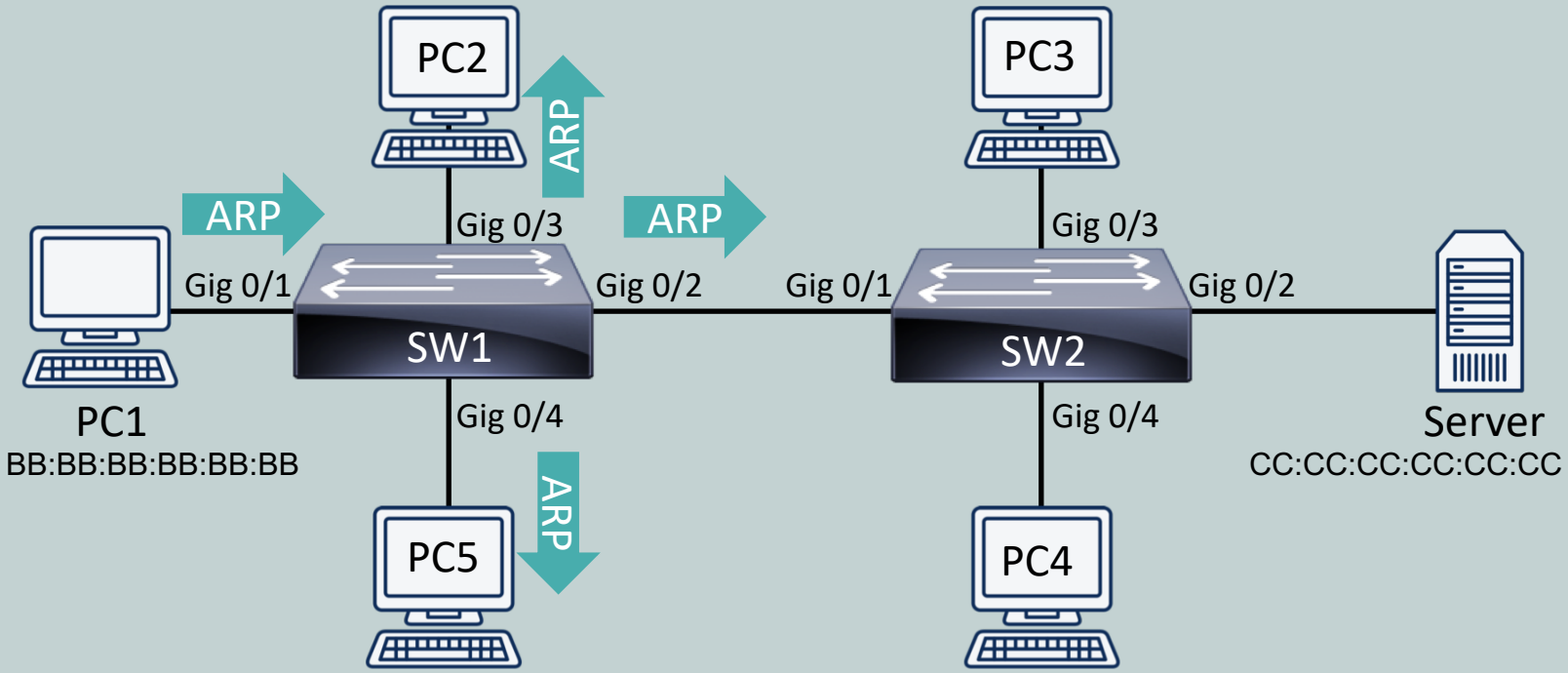
Port	MAC Address
Gig 0/1	Empty
Gig 0/2	Empty

Switch 1
MAC Address Table

Port	MAC Address
Gig 0/1	Empty
Gig 0/2	Empty

Switch 2
MAC Address Table

How Switches Improve Network Performance



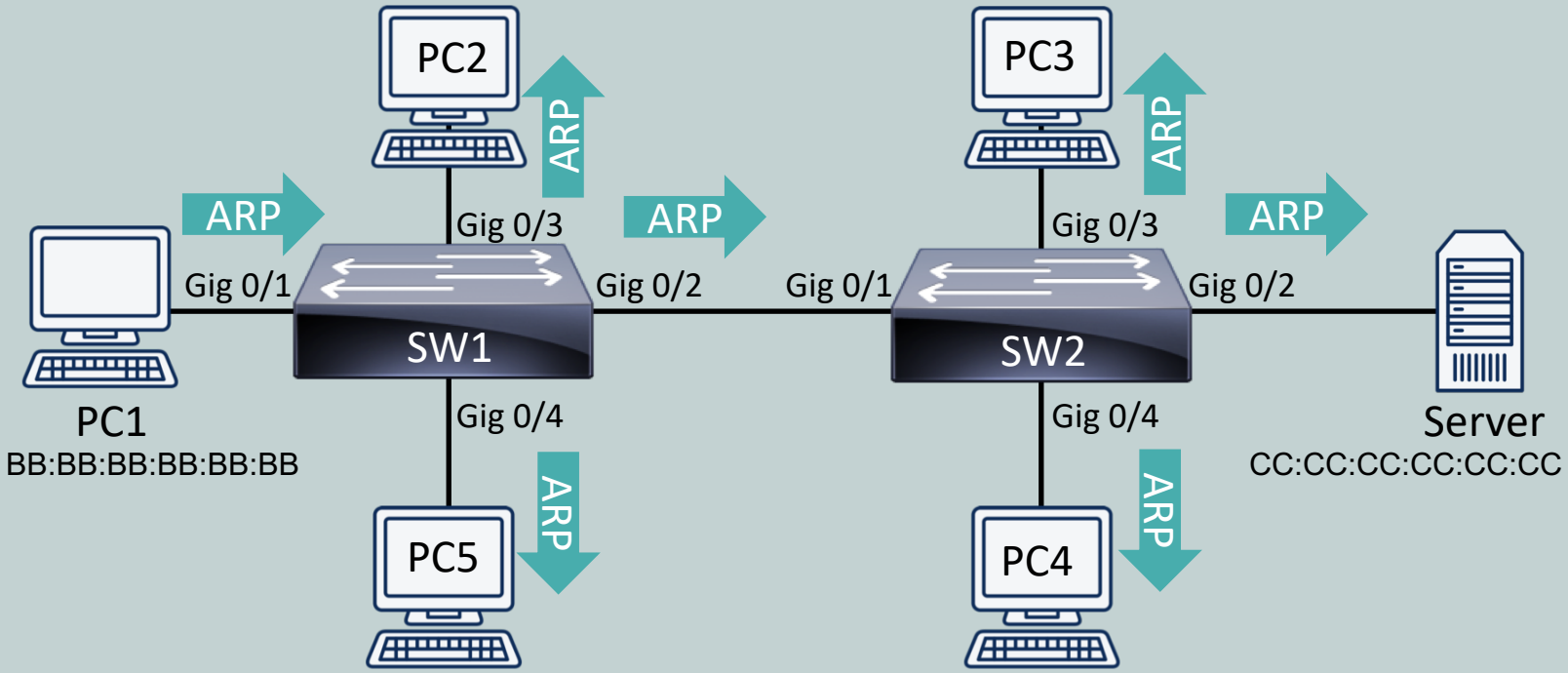
Port	MAC Address
Gig 0/1	BB:BB:BB:BB:BB:BB
Gig 0/2	Empty

Switch 1
MAC Address Table

Port	MAC Address
Gig 0/1	Empty
Gig 0/2	Empty

Switch 2
MAC Address Table

How Switches Improve Network Performance



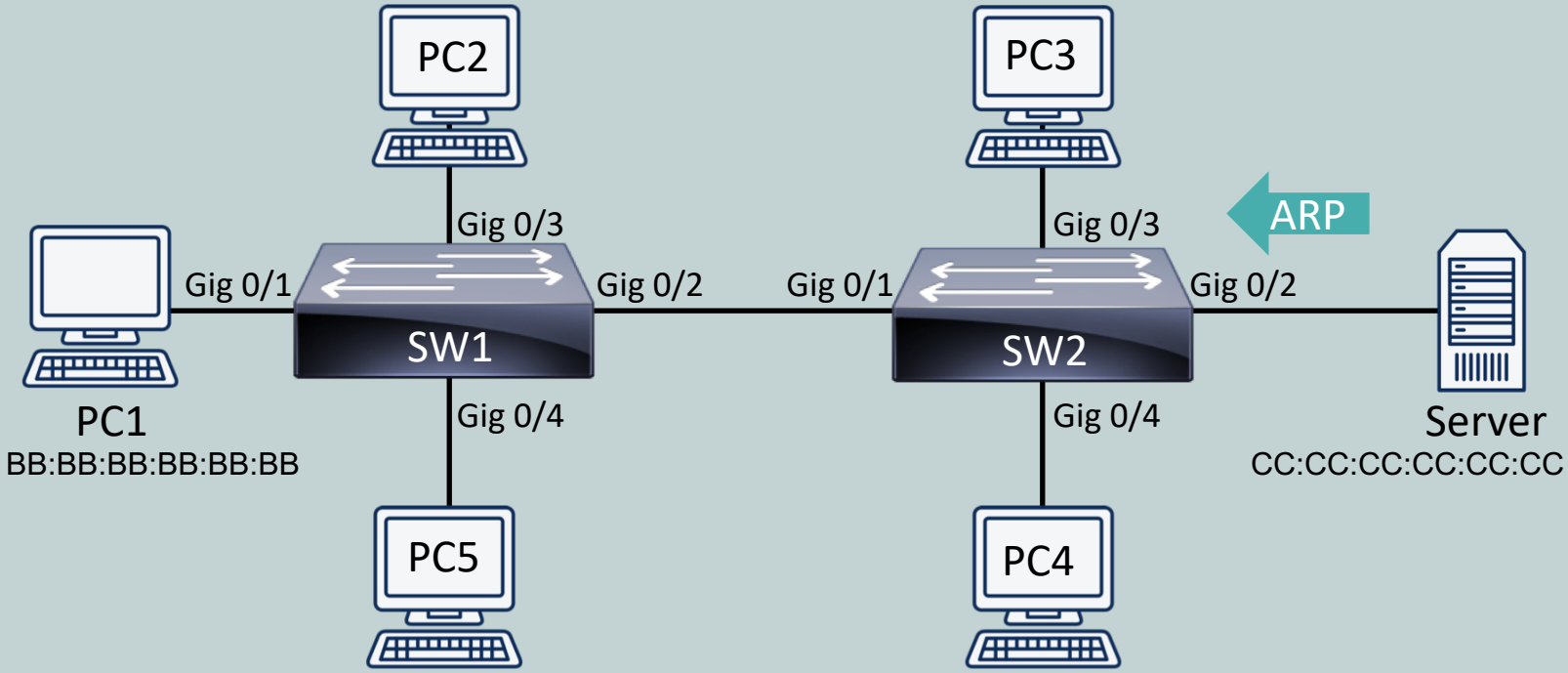
Port	MAC Address
Gig 0/1	BB:BB:BB:BB:BB:BB
Gig 0/2	Empty

Switch 1
MAC Address Table

Port	MAC Address
Gig 0/1	BB:BB:BB:BB:BB:BB
Gig 0/2	Empty

Switch 2
MAC Address Table

How Switches Improve Network Performance



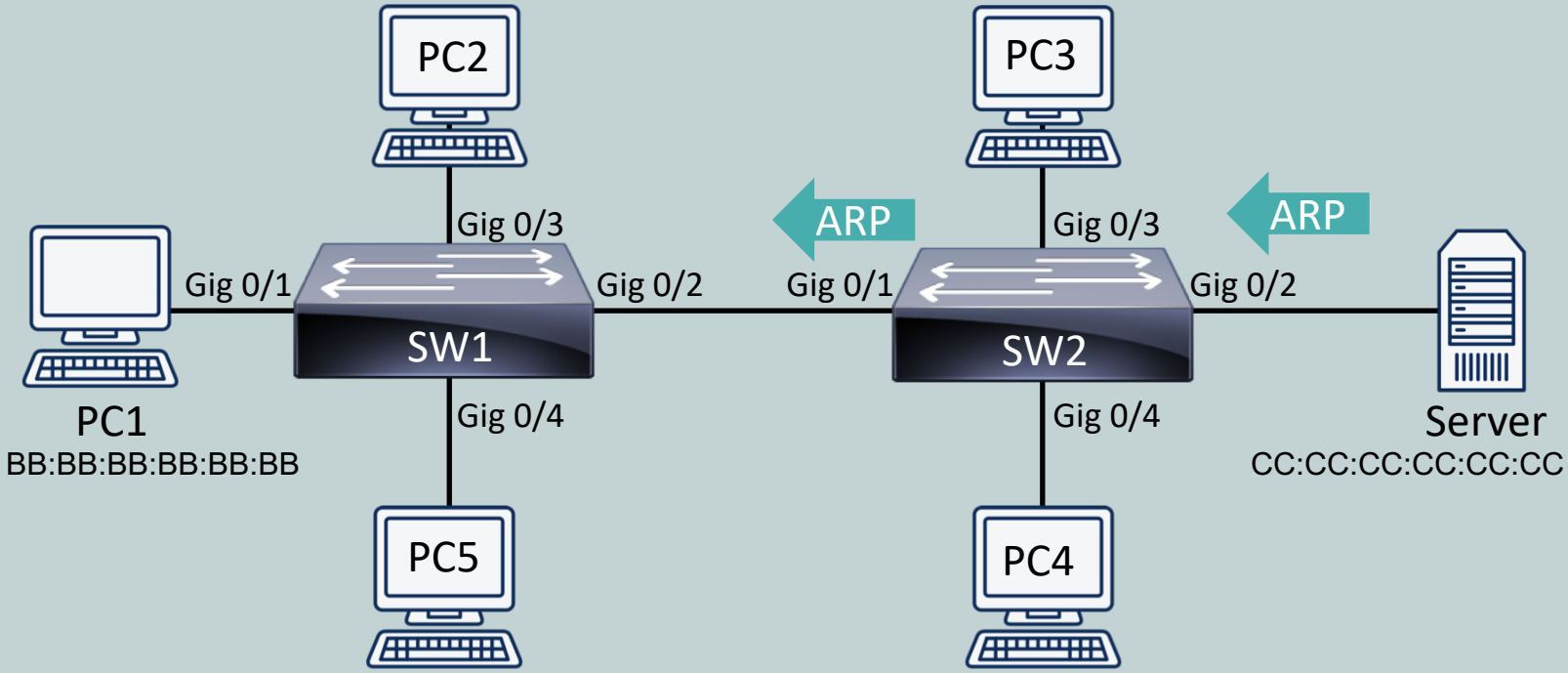
Port	MAC Address
Gig 0/1	BB:BB:BB:BB:BB:BB
Gig 0/2	Empty

Switch 1
MAC Address Table

Port	MAC Address
Gig 0/1	BB:BB:BB:BB:BB:BB
Gig 0/2	Empty

Switch 2
MAC Address Table

How Switches Improve Network Performance



Port	MAC Address
Gig 0/1	BB:BB:BB:BB:BB:BB
Gig 0/2	Empty

Switch 1
MAC Address Table

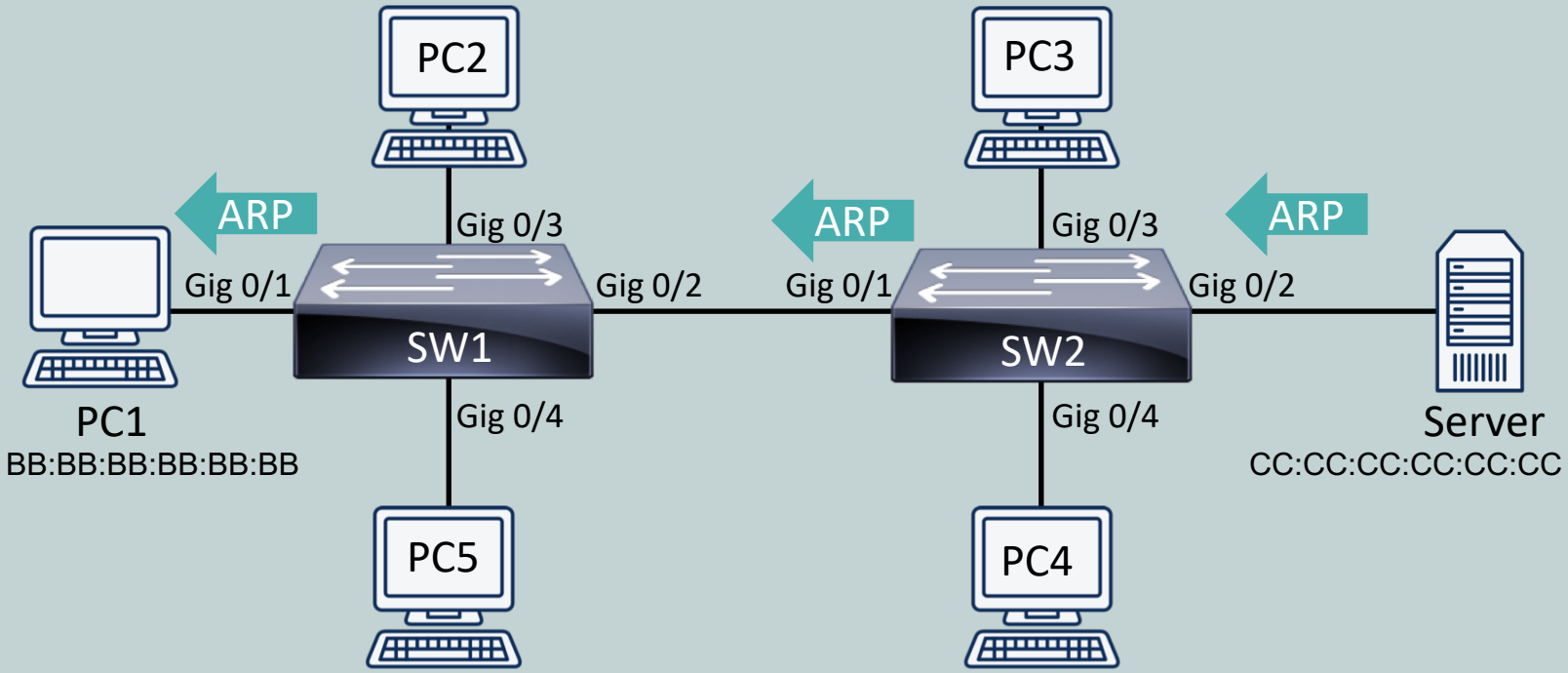
Port	MAC Address
Gig 0/1	BB:BB:BB:BB:BB:BB
Gig 0/2	CC:CC:CC:CC:CC:CC

Switch 2
MAC Address Table

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA Network+

How Switches Improve Network Performance



Port	MAC Address
Gig 0/1	BB:BB:BB:BB:BB:BB
Gig 0/2	CC:CC:CC:CC:CC:CC

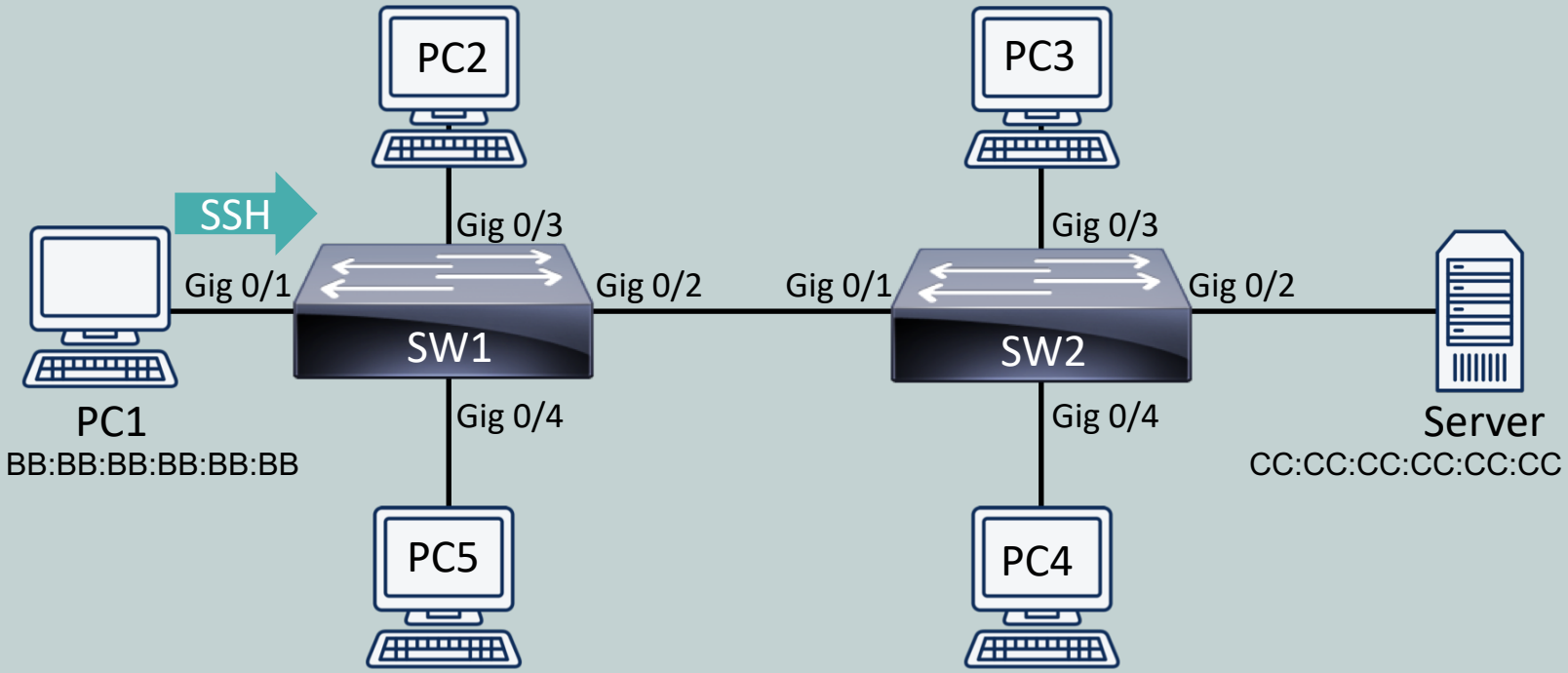
Switch 1
MAC Address Table

Port	MAC Address
Gig 0/1	BB:BB:BB:BB:BB:BB
Gig 0/2	CC:CC:CC:CC:CC:CC

Switch 2
MAC Address Table

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

How Switches Improve Network Performance



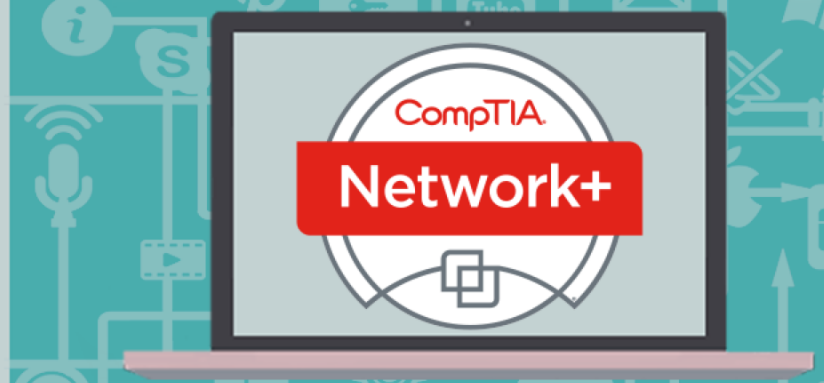
Port	MAC Address
Gig 0/1	BB:BB:BB:BB:BB:BB
Gig 0/2	CC:CC:CC:CC:CC:CC

Switch 1
MAC Address Table

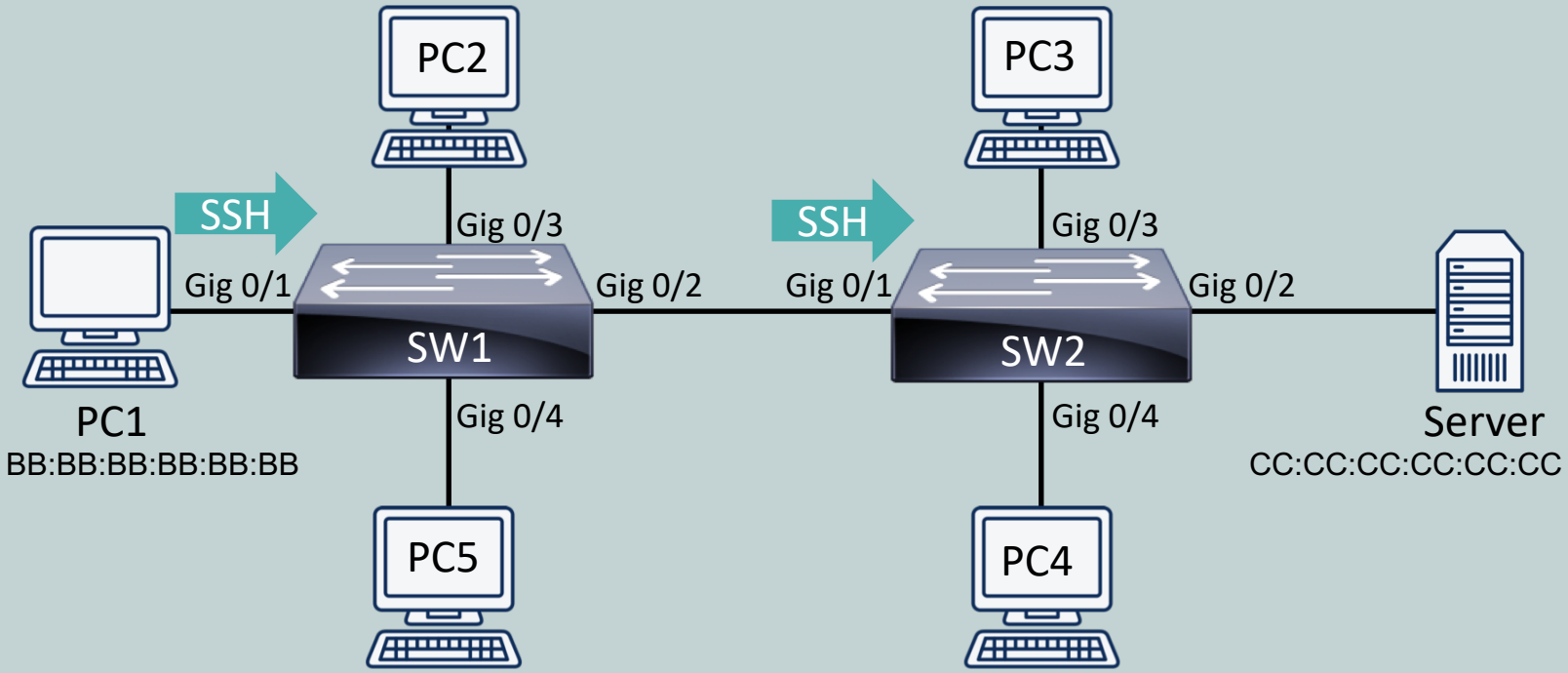
Port	MAC Address
Gig 0/1	BB:BB:BB:BB:BB:BB
Gig 0/2	CC:CC:CC:CC:CC:CC

Switch 2
MAC Address Table

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE



How Switches Improve Network Performance



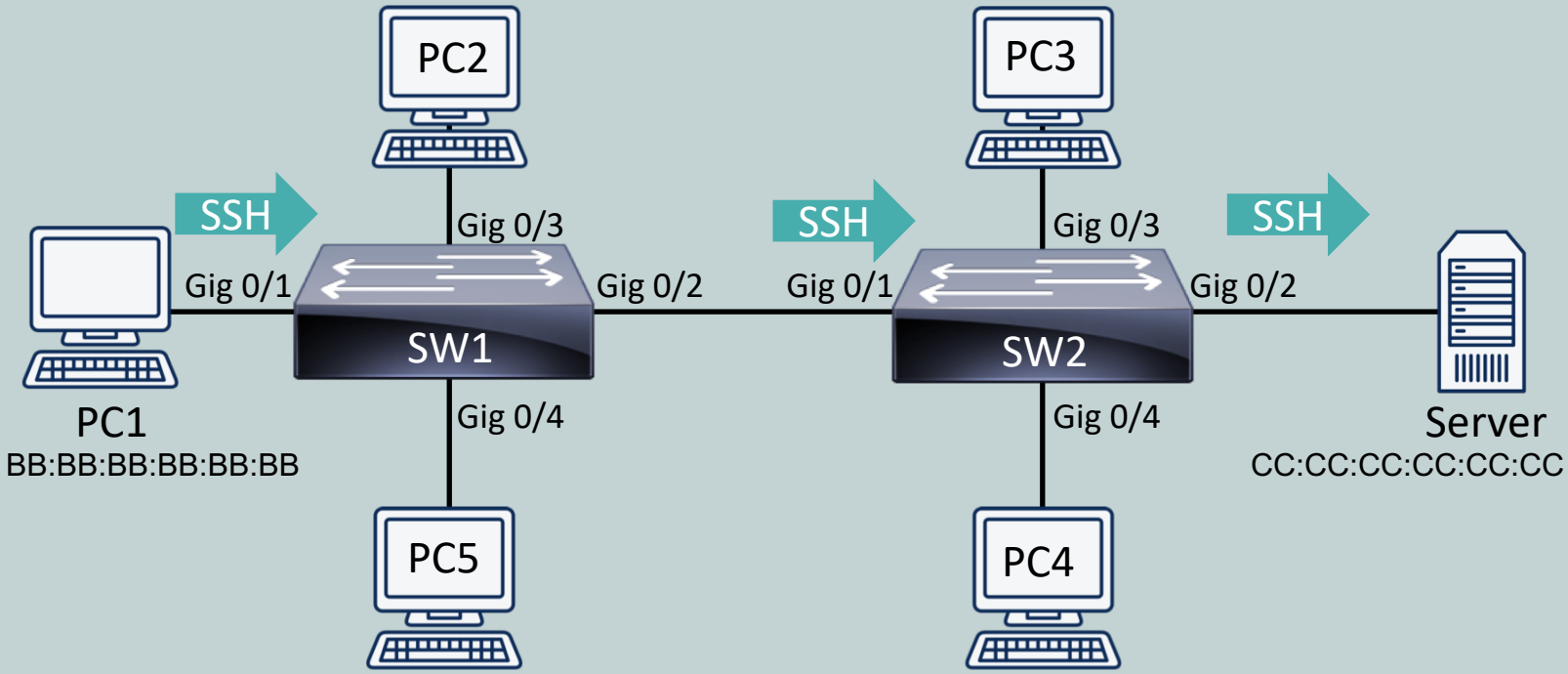
Port	MAC Address
Gig 0/1	BB:BB:BB:BB:BB:BB
Gig 0/2	CC:CC:CC:CC:CC:CC

Switch 1
MAC Address Table

Port	MAC Address
Gig 0/1	BB:BB:BB:BB:BB:BB
Gig 0/2	CC:CC:CC:CC:CC:CC

Switch 2
MAC Address Table

How Switches Improve Network Performance



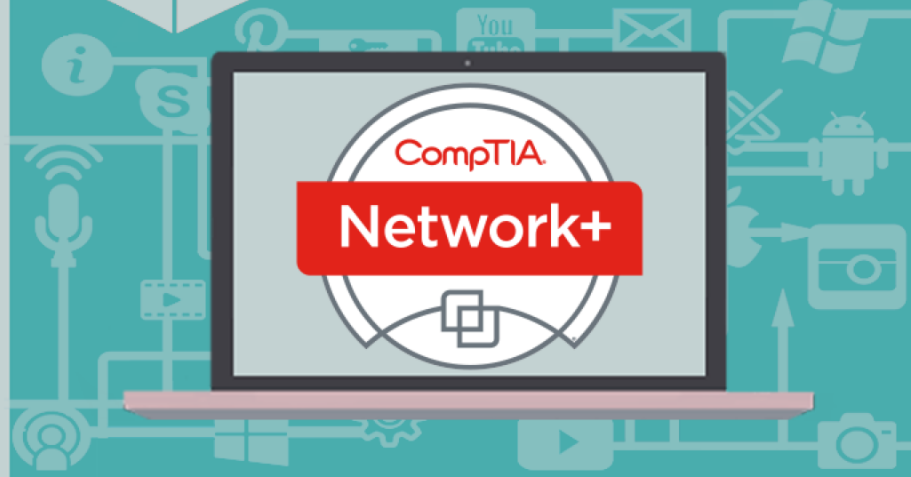
Port	MAC Address
Gig 0/1	BB:BB:BB:BB:BB:BB
Gig 0/2	CC:CC:CC:CC:CC:CC

Switch 1
MAC Address Table

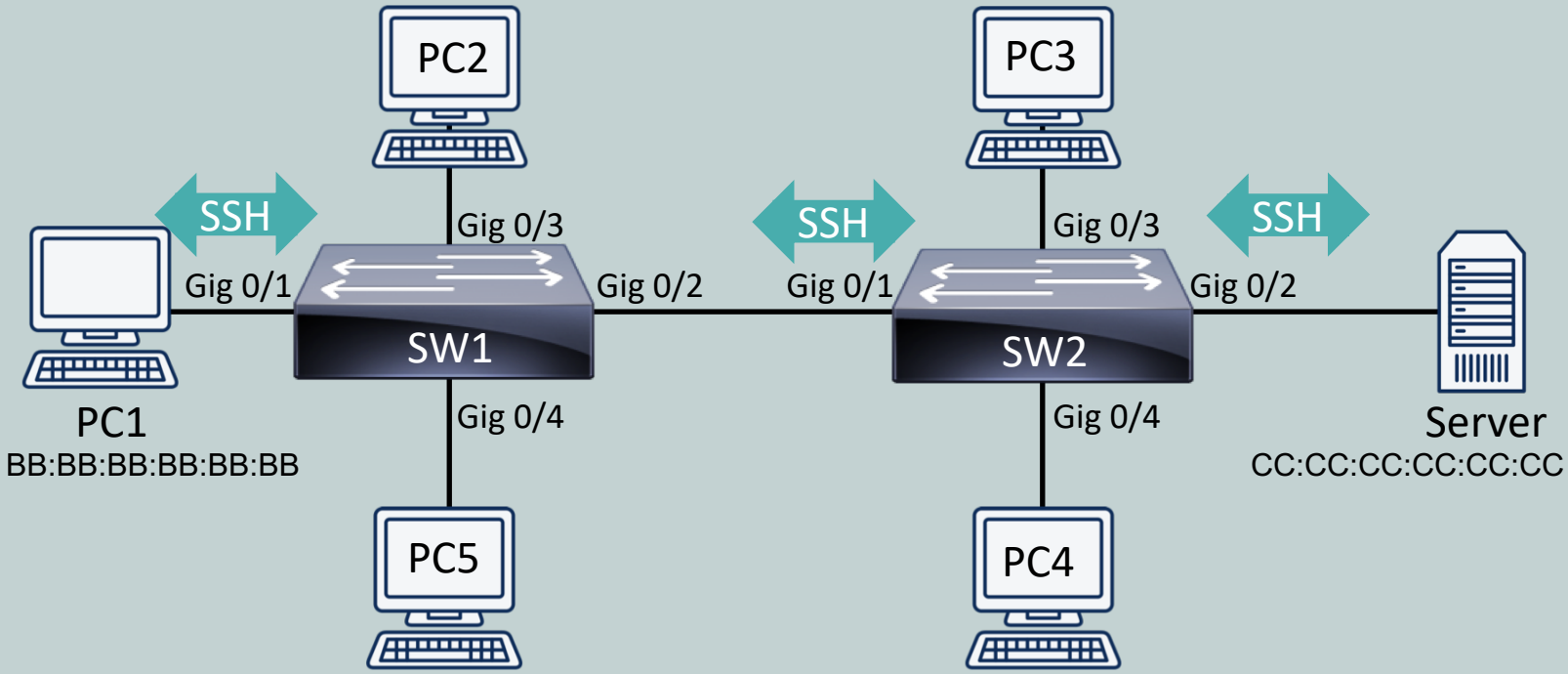
Port	MAC Address
Gig 0/1	BB:BB:BB:BB:BB:BB
Gig 0/2	CC:CC:CC:CC:CC:CC

Switch 2
MAC Address Table

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE



How Switches Improve Network Performance



Port	MAC Address
Gig 0/1	BB:BB:BB:BB:BB:BB
Gig 0/2	CC:CC:CC:CC:CC:CC

Switch 1
MAC Address Table

Port	MAC Address
Gig 0/1	BB:BB:BB:BB:BB:BB
Gig 0/2	CC:CC:CC:CC:CC:CC

Switch 2
MAC Address Table

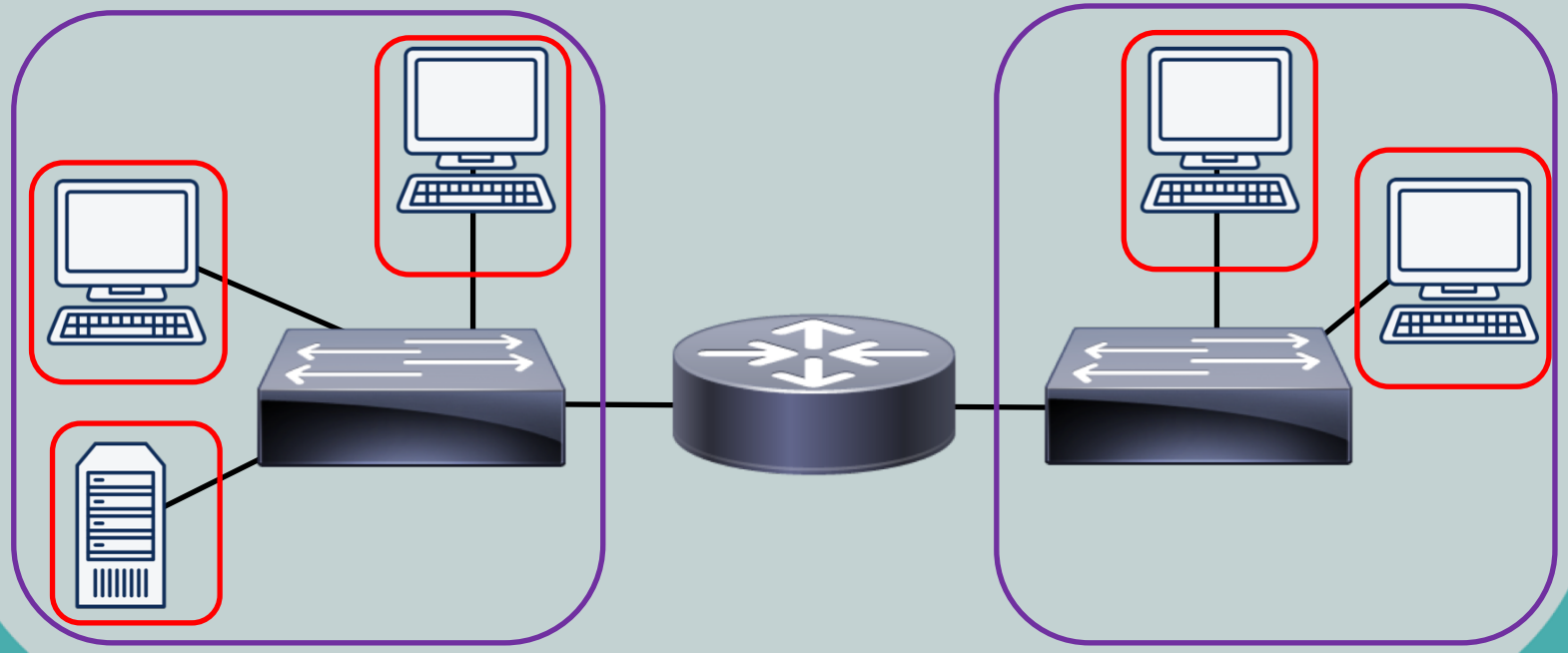
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Router

- Layer 3 device used to connect multiple networks together
- Make forwarding decisions based on logical network address information
  - Such as using IP addresses (IPv4 or IPv6)
- Routers are typically more feature rich and support a broader range of interface types than multilayer switches

Router

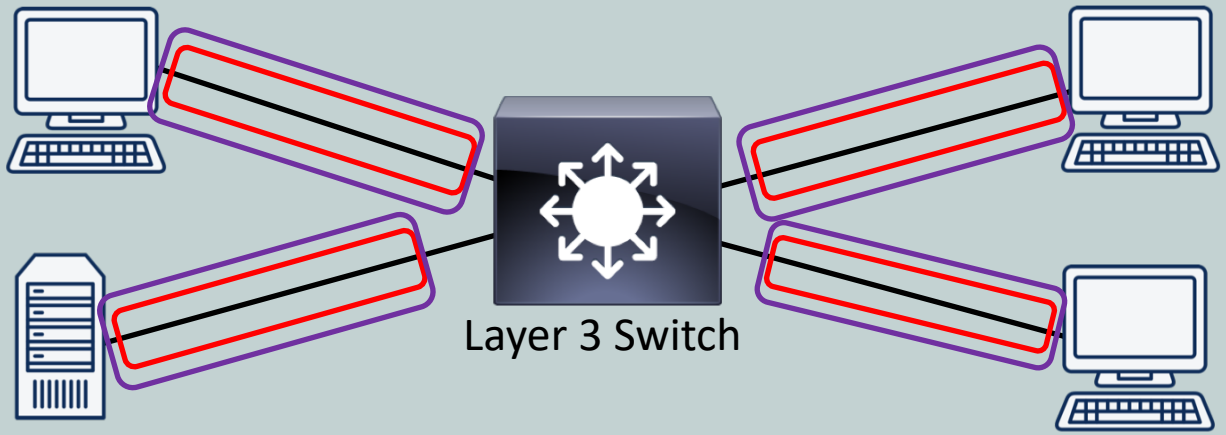
- Each port is a separate collision domain
- Each port is a separate broadcast domain



Layer 3 Switch

- Layer 3 device used to connect multiple network segments together

- Can make Layer 3 routing decisions and interconnect entire networks (like a router), not just network segments (like a switch)



Collision Domain

Broadcast Domain

Summary of Network Infrastructure

Device Type	Collision Domains Possible	Broadcast Domains Possible	OSI Layer of Operation
Hub	1	1	1
Bridge	1 per port	1	2
Switch	1 per port	1	2
Multilayer switch	1 per port	1 per port	3+
Router	1 per port	1 per port	3+

Additional Ethernet Features

CompTIA Network+ (N10-007)

Additional Ethernet Switch Features

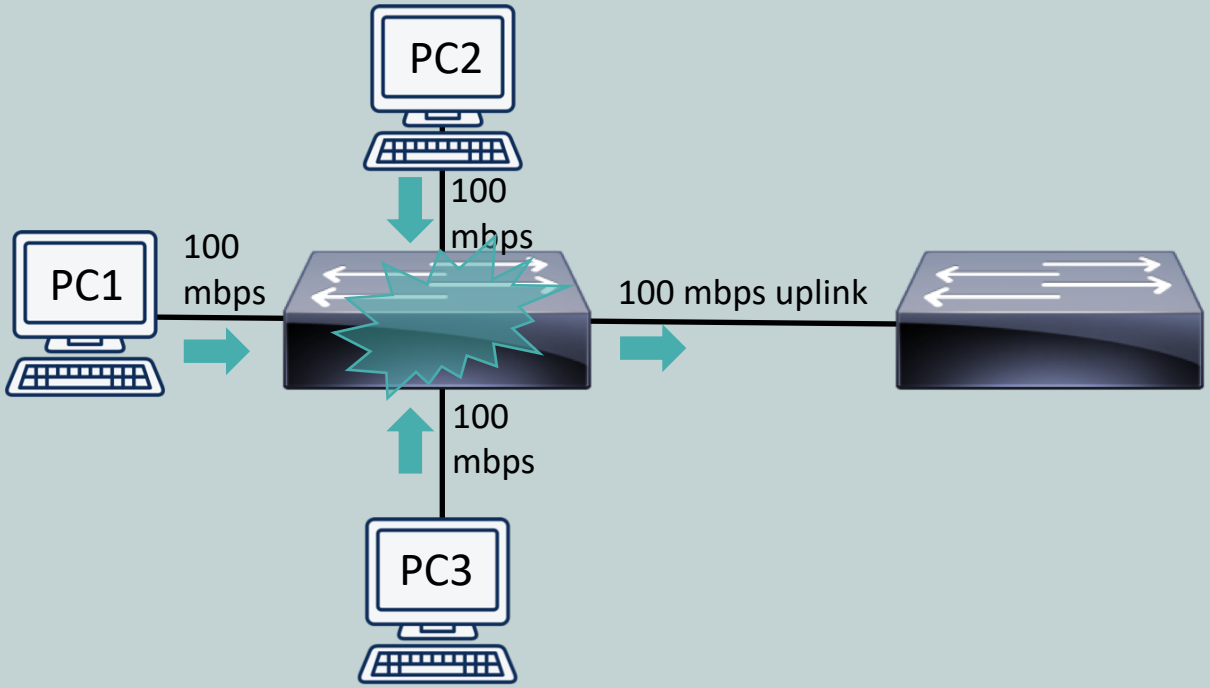
- Features to enhance network performance, redundancy, security, management, flexibility, and scalability

- Common switch features
  - *Virtual LANs (VLANs)*
  - *Trunking*
  - *Spanning Tree Protocol (STP)*
  - Link aggregation
  - Power over Ethernet
  - Port monitoring
  - User authentication

*** VLANs, Trunking, and STP are covered in other lessons ***

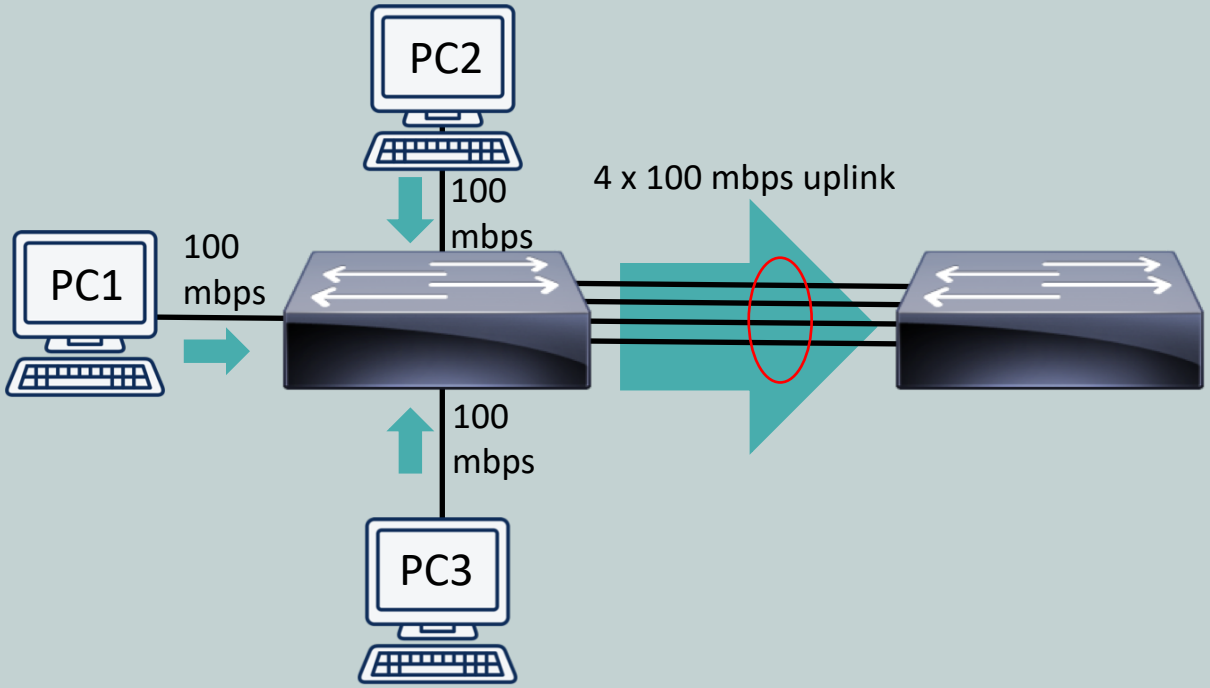
Link Aggregation (802.3ad)

- Congestion can occur when ports all operate at the same speed



Link Aggregation (802.3ad)

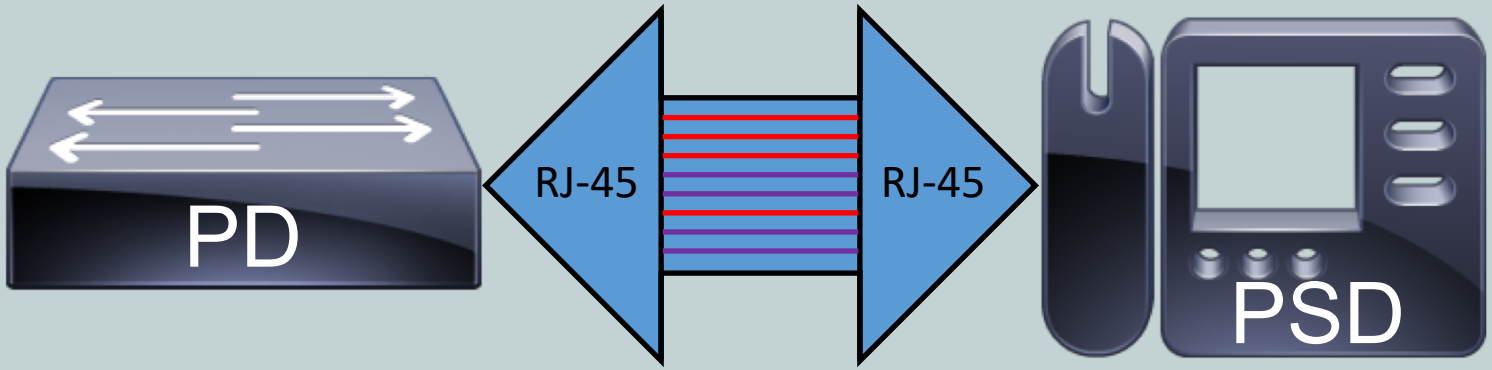
- Allows for combination of multiple physical connections into a single logical connection
- Bandwidth available is increased and the congestion is minimized or prevented



Power Over Ethernet (PoE 802.3af, PoE+ 802.3at)

- Supplies electrical power over Ethernet
  - Requires CAT 5 or higher copper cable
  - Provides up to 15.4 watts of power to device
  - PoE+ provides up to 25.5 W of power to device

- Two device types
  - Power Sourcing Equipment (PSE)
  - Powered Device (PD)

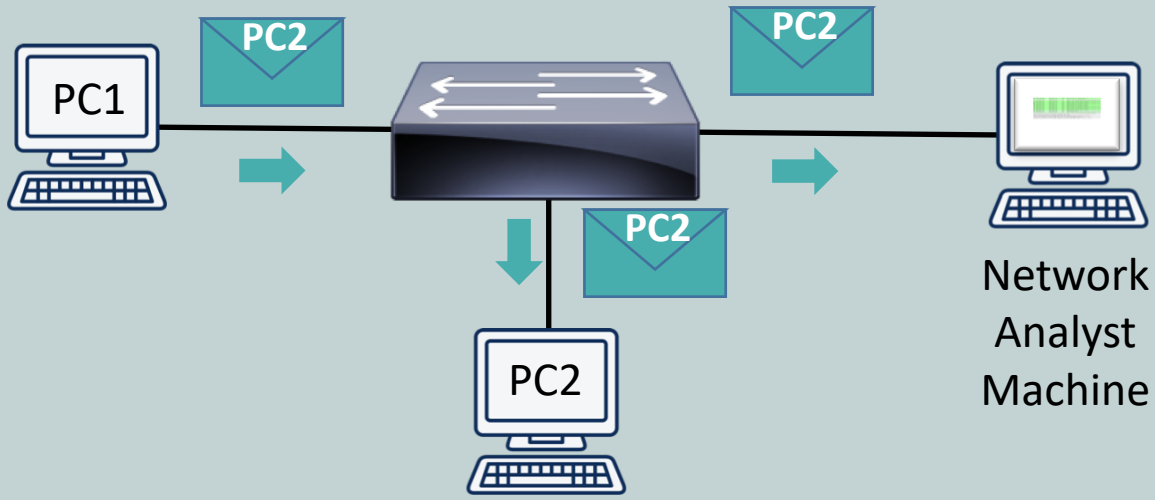


Pins 1, 2, 3, and 6
provider power

Port Monitoring or Mirroring

- Helpful to analyze packet flow over network
  - Connect a network sniffer to a hub and it sees all
  - But, switches require port monitoring for network analyzer to see all the traffic

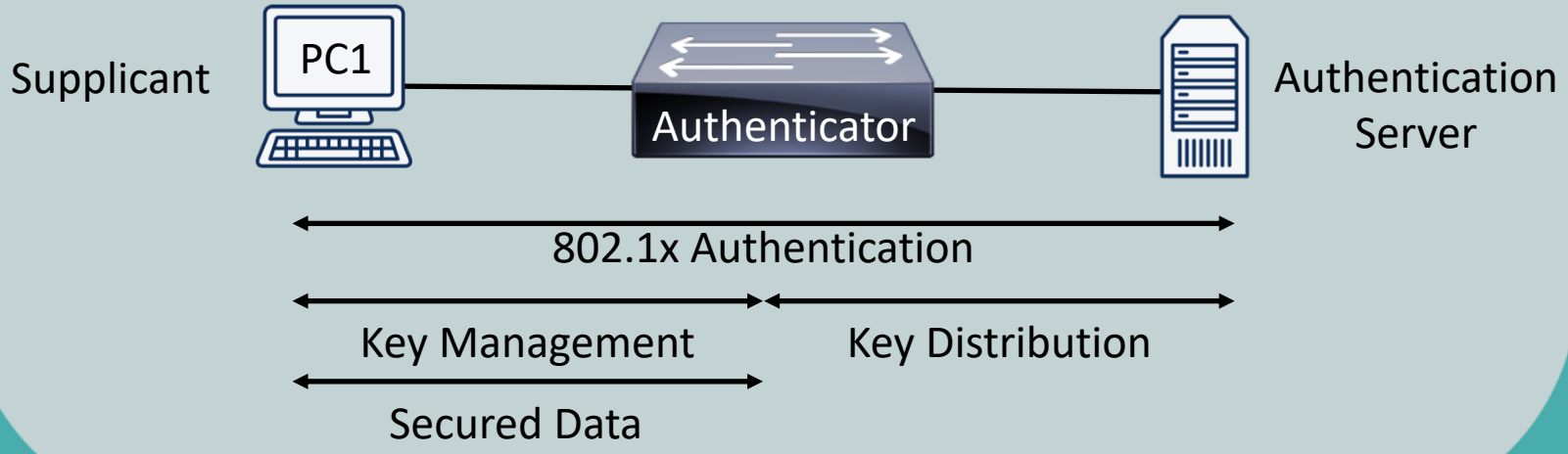
- Port mirroring makes a copy of all traffic destined for a port and sends it to another port



User Authentication (802.1x)

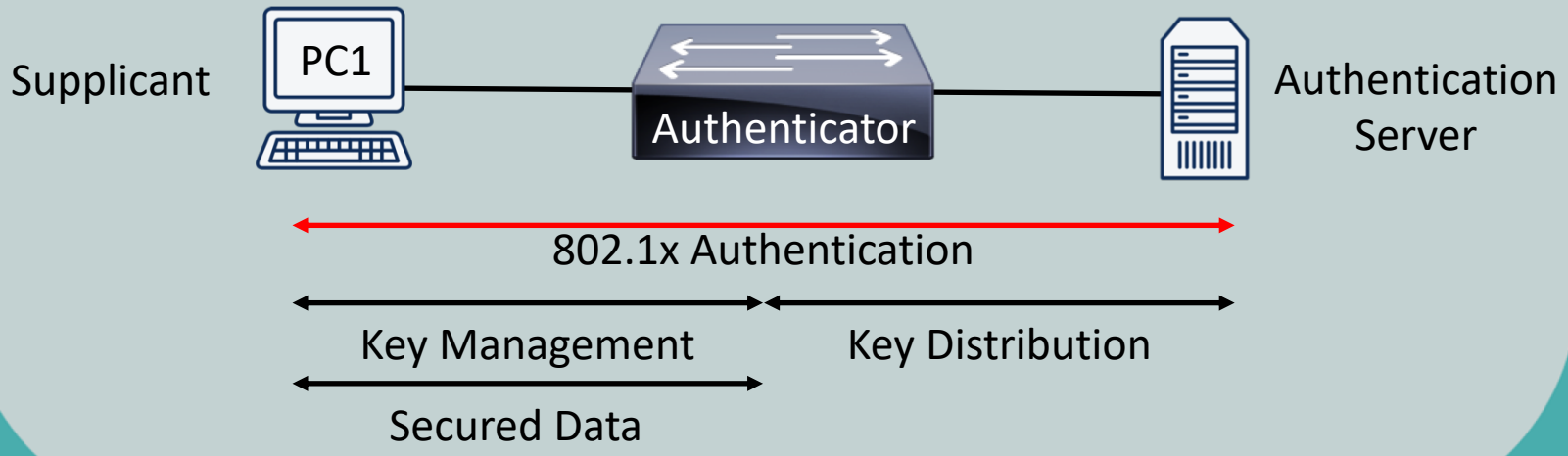
- For security purposes, switches can require users to authenticate themselves before gaining access to the network

- Once authenticated, a key is generated and shared between the supplicant (device wanting access) and the switch (authenticator)



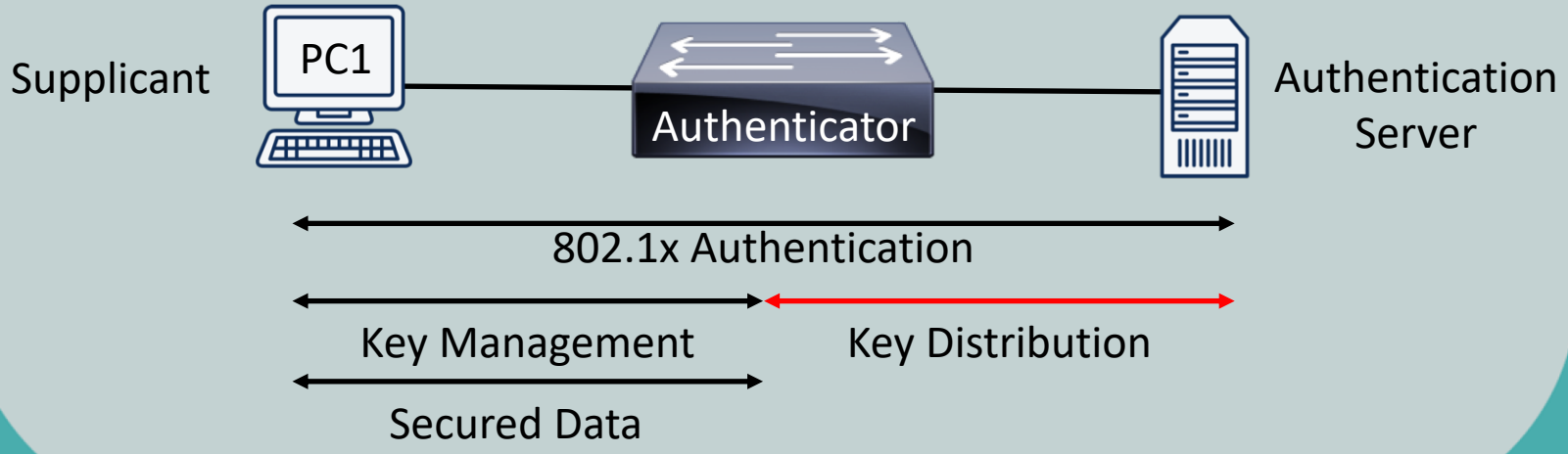
User Authentication (802.1x)

- Authentication server checks the supplicants credentials and creates the key
- Key is used to encrypt the traffic coming from and being sent to the client



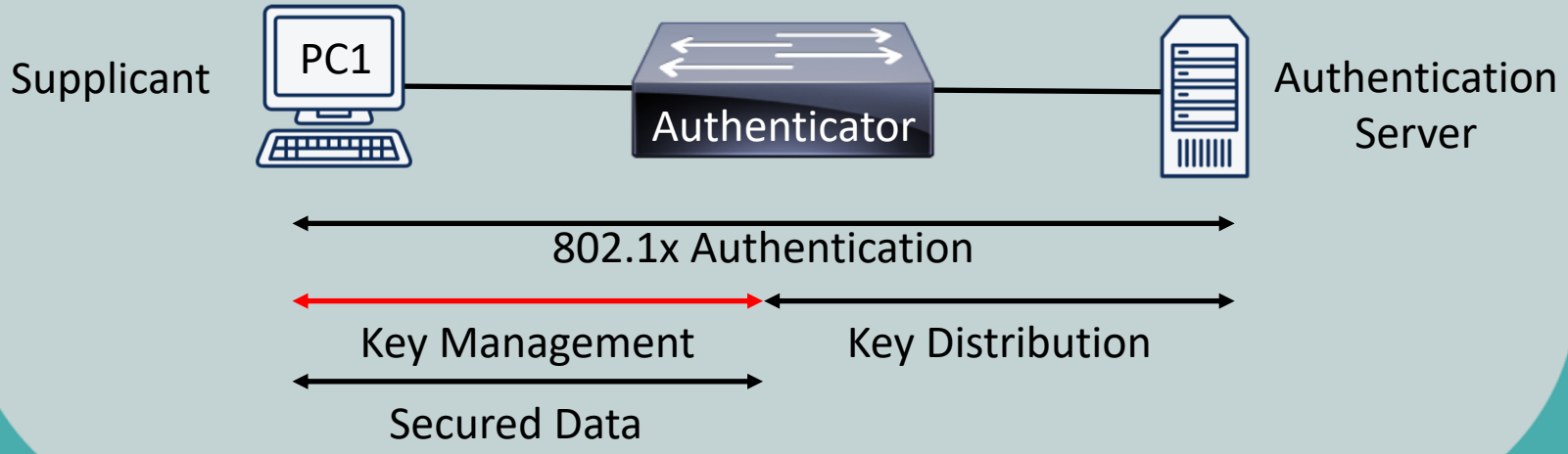
User Authentication (802.1x)

- Authentication server checks the supplicants credentials and creates the key
- Key is used to encrypt the traffic coming from and being sent to the client



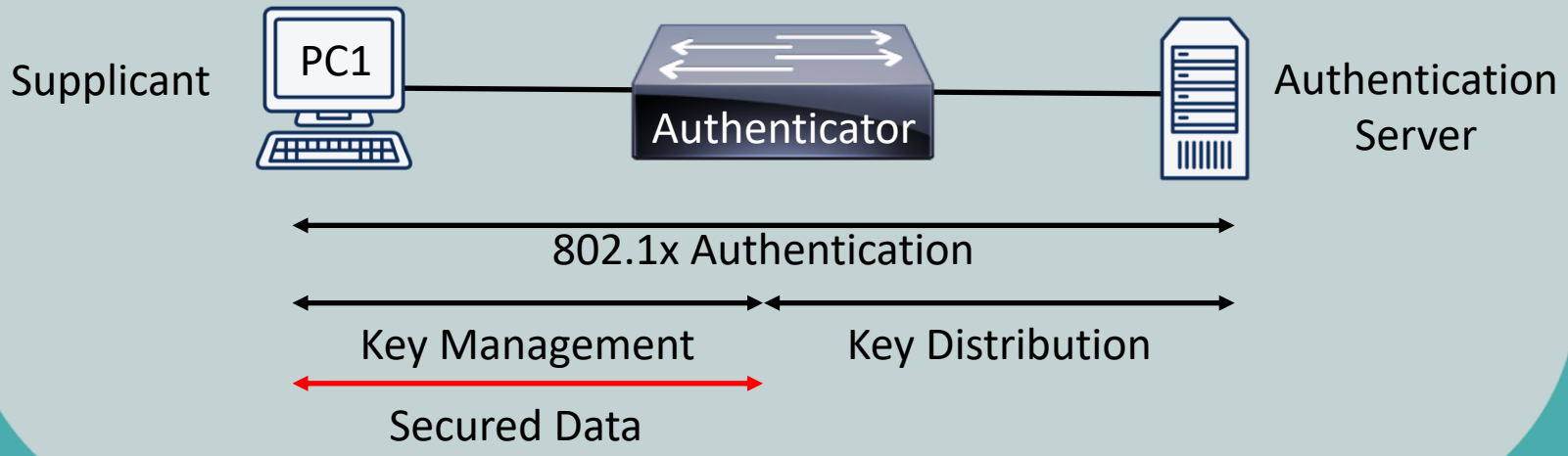
User Authentication (802.1x)

- Authentication server checks the supplicants credentials and creates the key
- Key is used to encrypt the traffic coming from and being sent to the client



User Authentication (802.1x)

- Authentication server checks the supplicants credentials and creates the key
- Key is used to encrypt the traffic coming from and being sent to the client

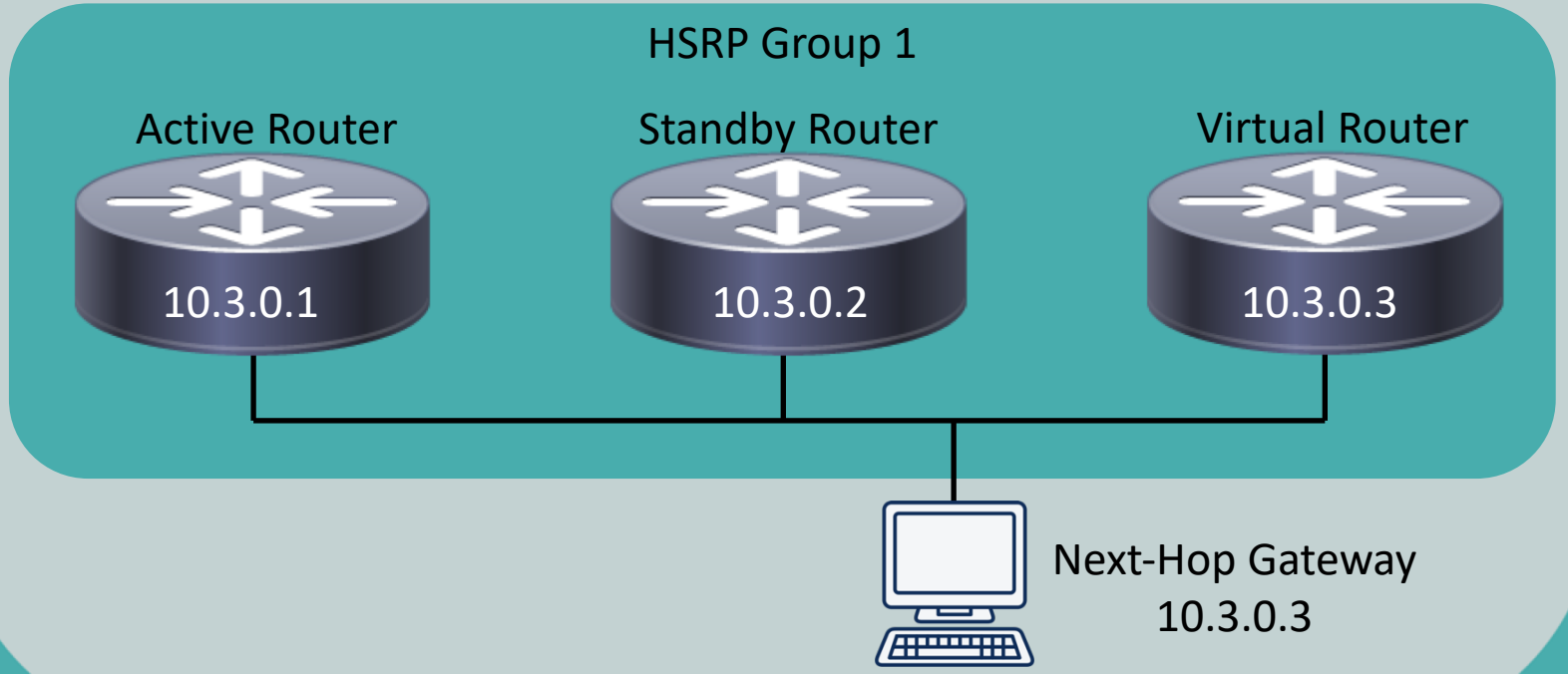


Management Access and Authentication

- To configure and manage switches, you can use two options:
  - SSH
    - Remote administration program that allows you to connect to the switch over the network
  - Console port
    - Allows for local administration of the switch using a separate laptop and a rollover cable (DB-9 to RJ-45)
- Out-of-band (OOB) management involves keeping all network configuration devices on a separate network

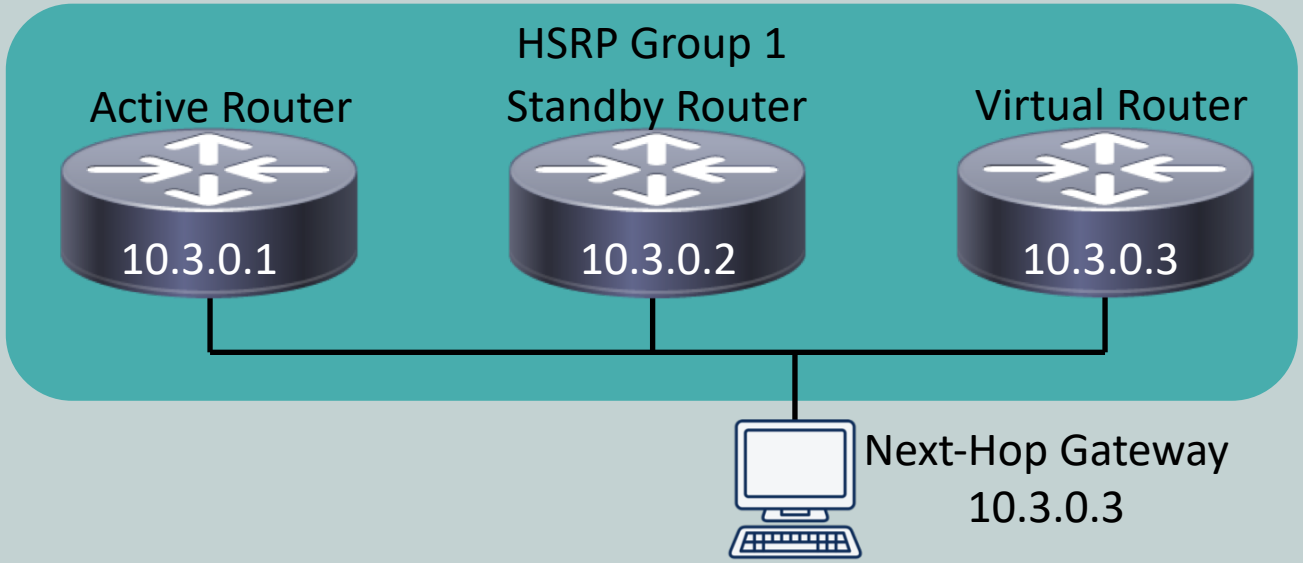
First-Hop Redundancy

- Hot Standby Router Protocol (HSRP) uses virtual IP and MAC addresses to provide a "active router" and a "standby router"
  - HSRP is a Cisco-proprietary protocol
  - If Active is offline, then standby answers



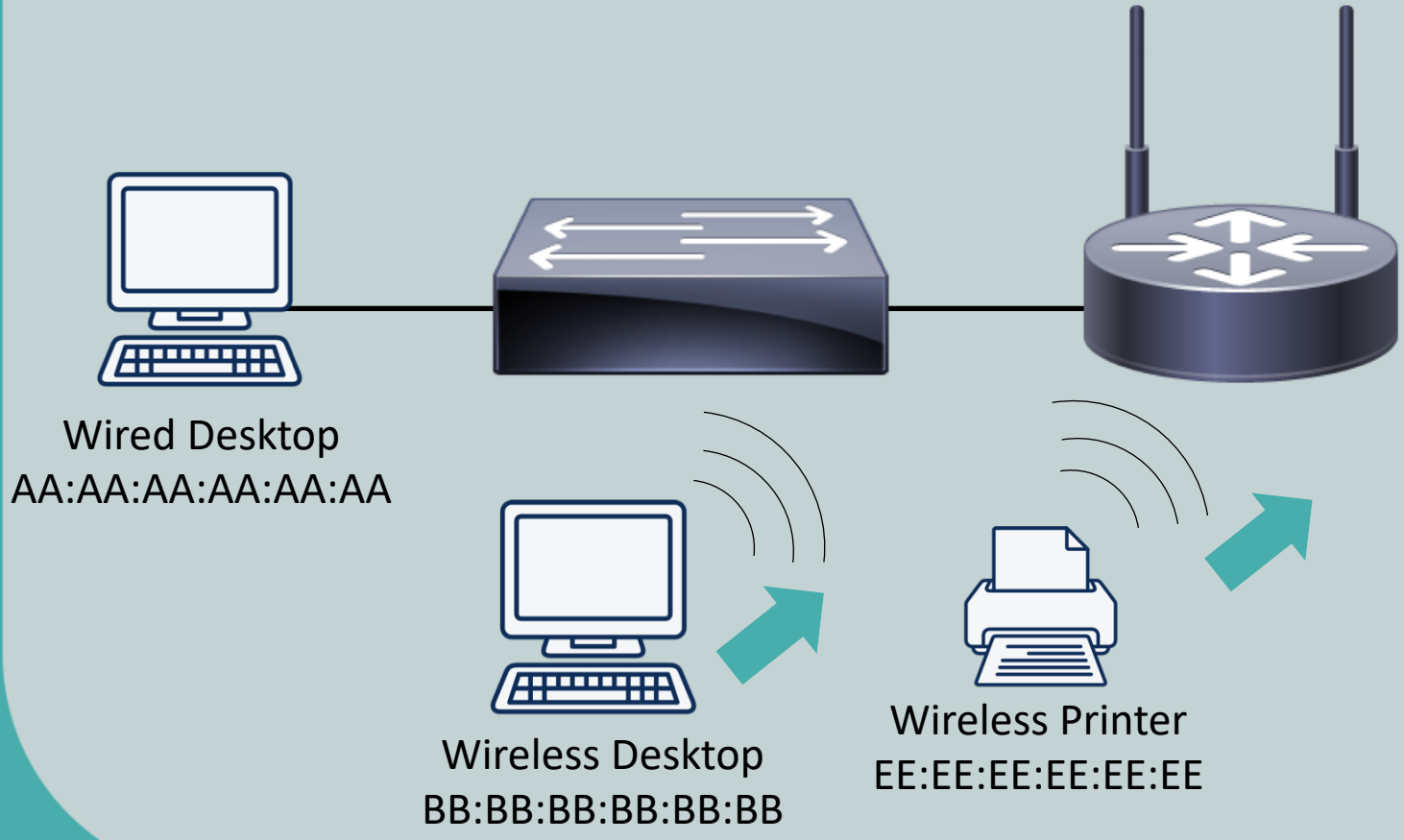
Other First-Hop Redundancy Protocols

- Gateway Load Balancing Protocol (GLBP)
  - Cisco-proprietary protocol
- Virtual Router Redundancy Protocol (VRRP)
  - Open-source protocol
- Common Address Redundancy Protocol (CARP)
  - Open-source protocol



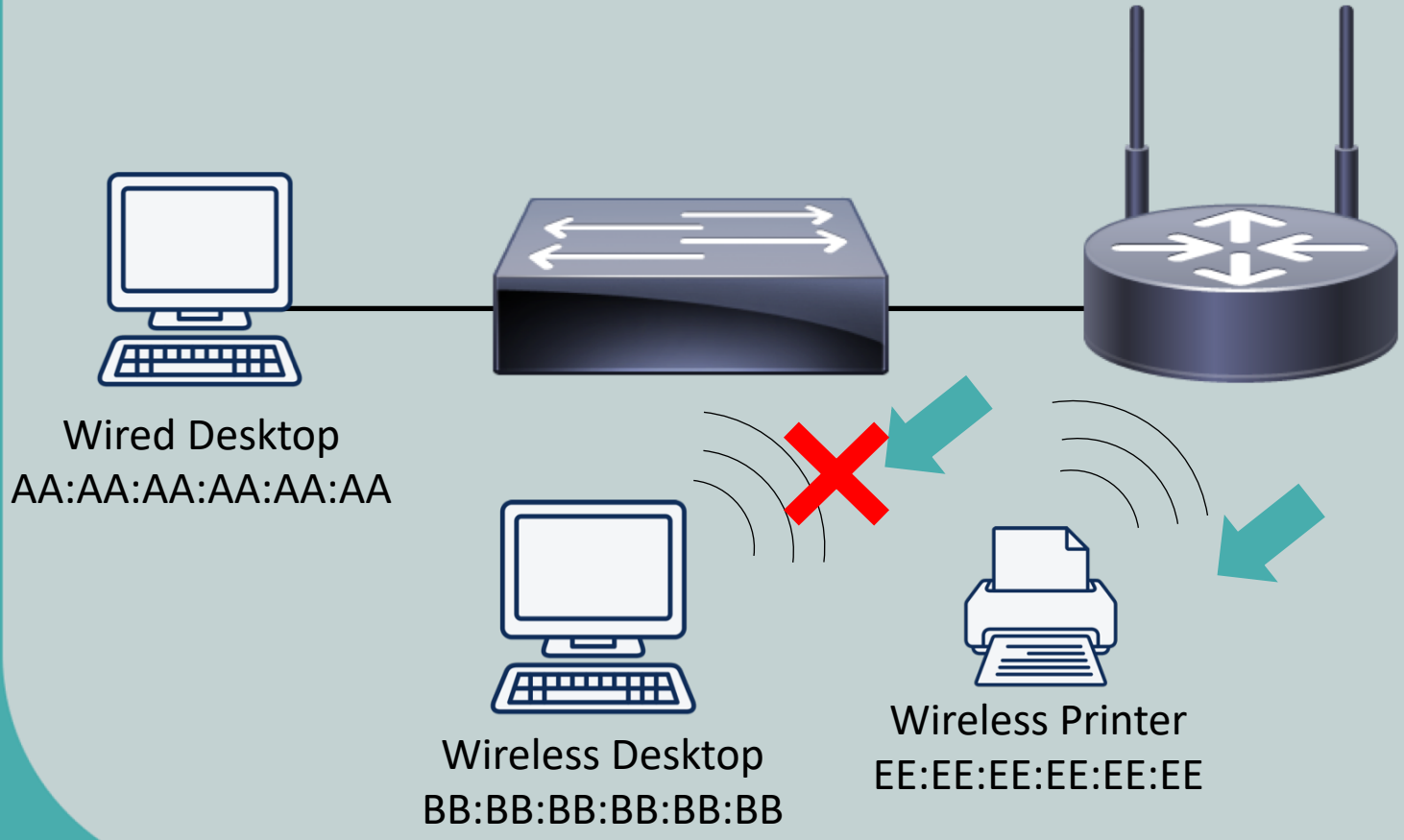
MAC Filtering

- Permits or denies traffic based on a device's MAC address to improve security



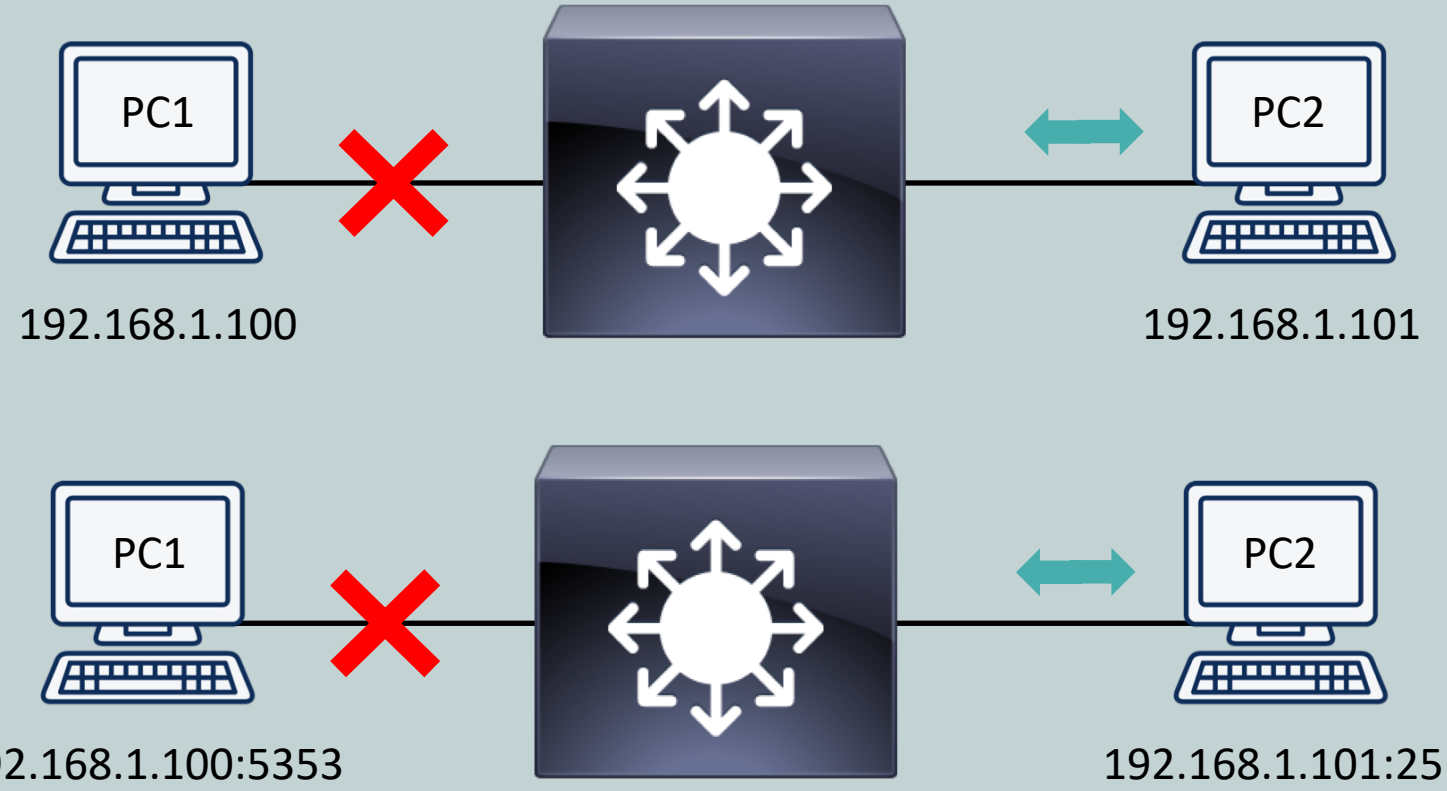
MAC Filtering

- Permits or denies traffic based on a device's MAC address to improve security



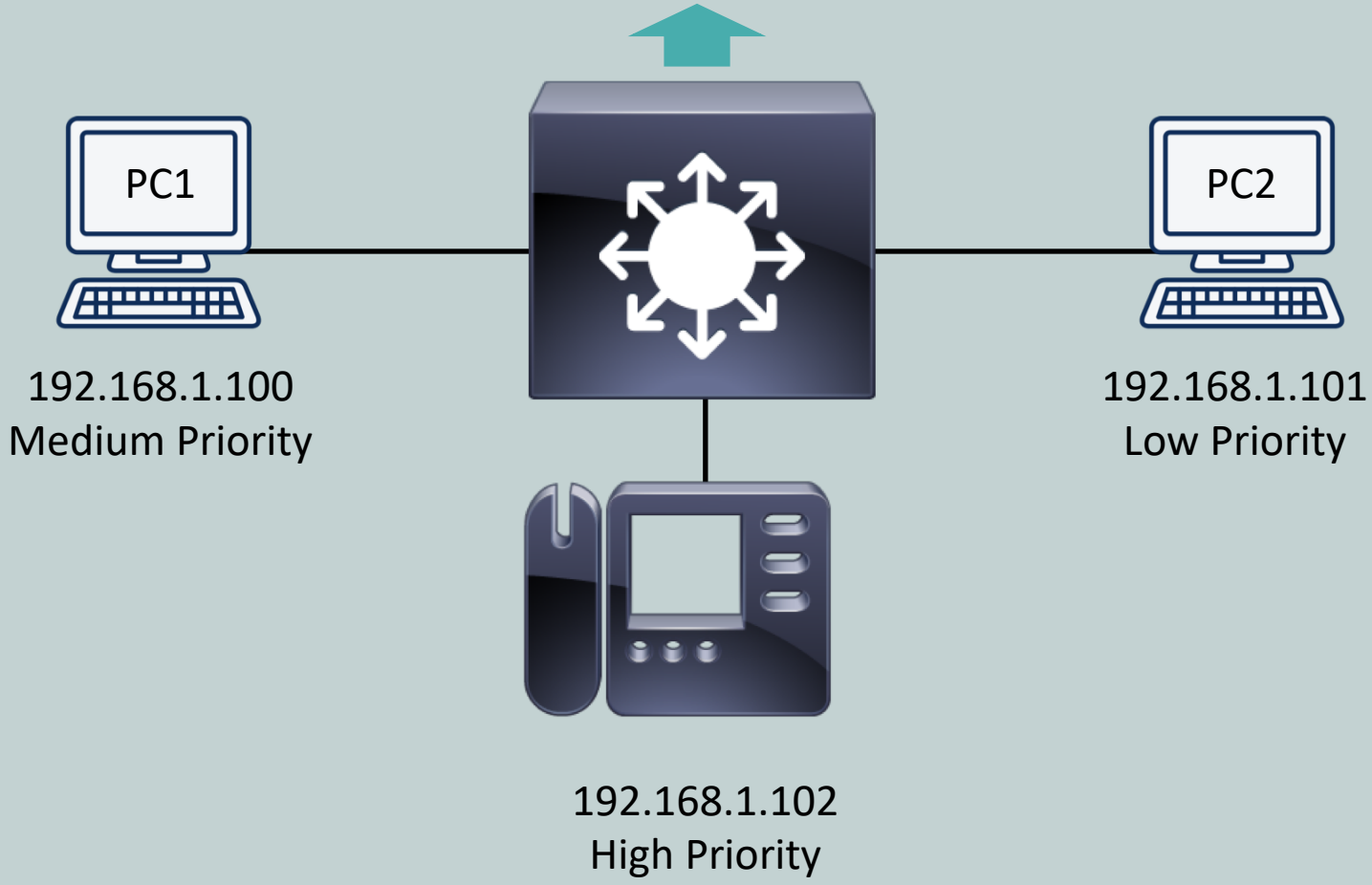
Traffic Filtering

- Multilayer switches may permit or deny traffic based on IP addresses or application ports



Quality of Service (QoS)

- Forwards traffic based on priority markings



** QoS will be covered in-depth in a future lesson **

Spanning Tree Protocol (STP)

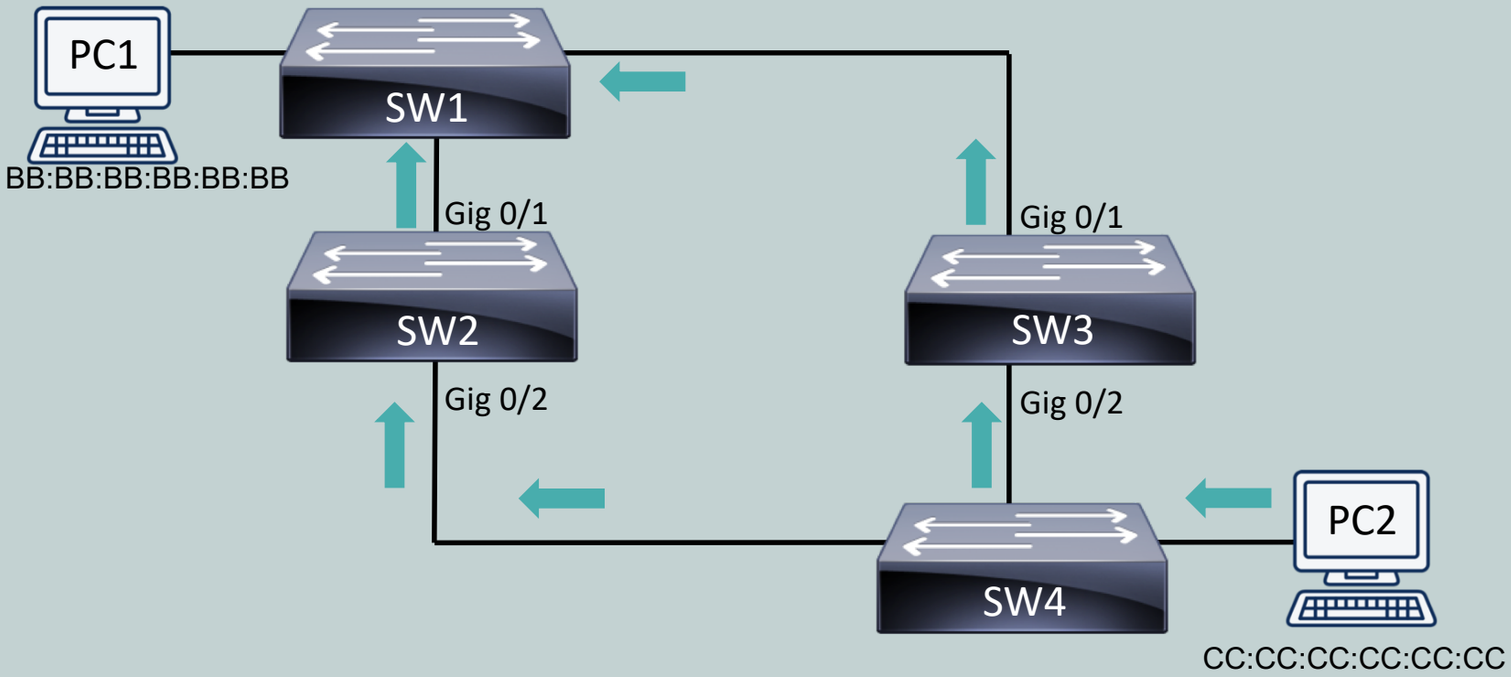
CompTIA Network+ (N10-007)

Spanning Tree Protocol (STP) (802.1D)

- Permits redundant links between switches and prevents looping of network traffic
- Availability is measured in 9's
  - Five 9's is 99.999% uptime
  - Only 5 minutes down per year allowed
- Shortest Path Bridging (SPB) is used instead of STP for larger network environments

Without STP...

- MAC Address table corruption can occur



Port	MAC Address
Gig 0/1	CC:CC:CC:CC:CC:CC
Gig 0/2	CC:CC:CC:CC:CC:CC

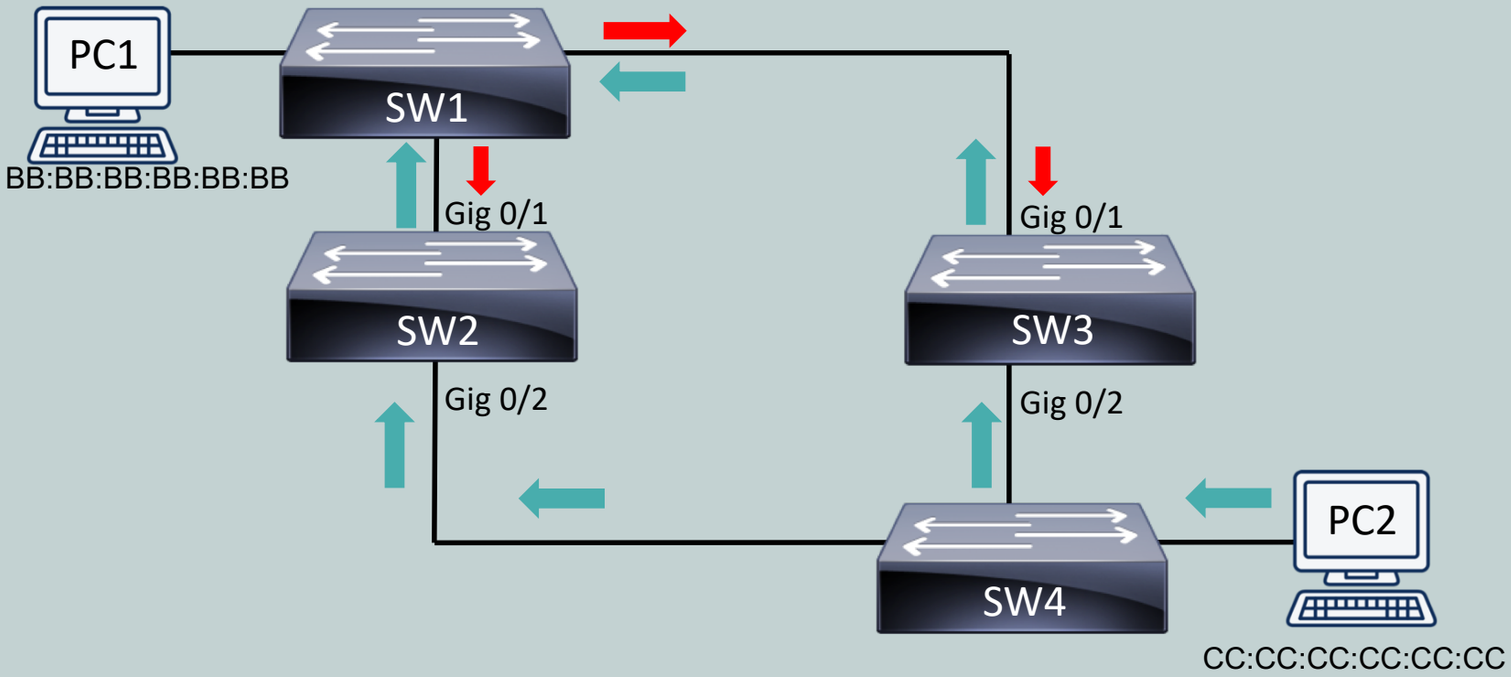
Switch 2
MAC Address Table

Port	MAC Address
Gig 0/1	
Gig 0/2	CC:CC:CC:CC:CC:CC

Switch 3
MAC Address Table

Without STP...

- MAC Address table corruption can occur



Port	MAC Address
Gig 0/1	CC:CC:CC:CC:CC:CC
Gig 0/2	CC:CC:CC:CC:CC:CC

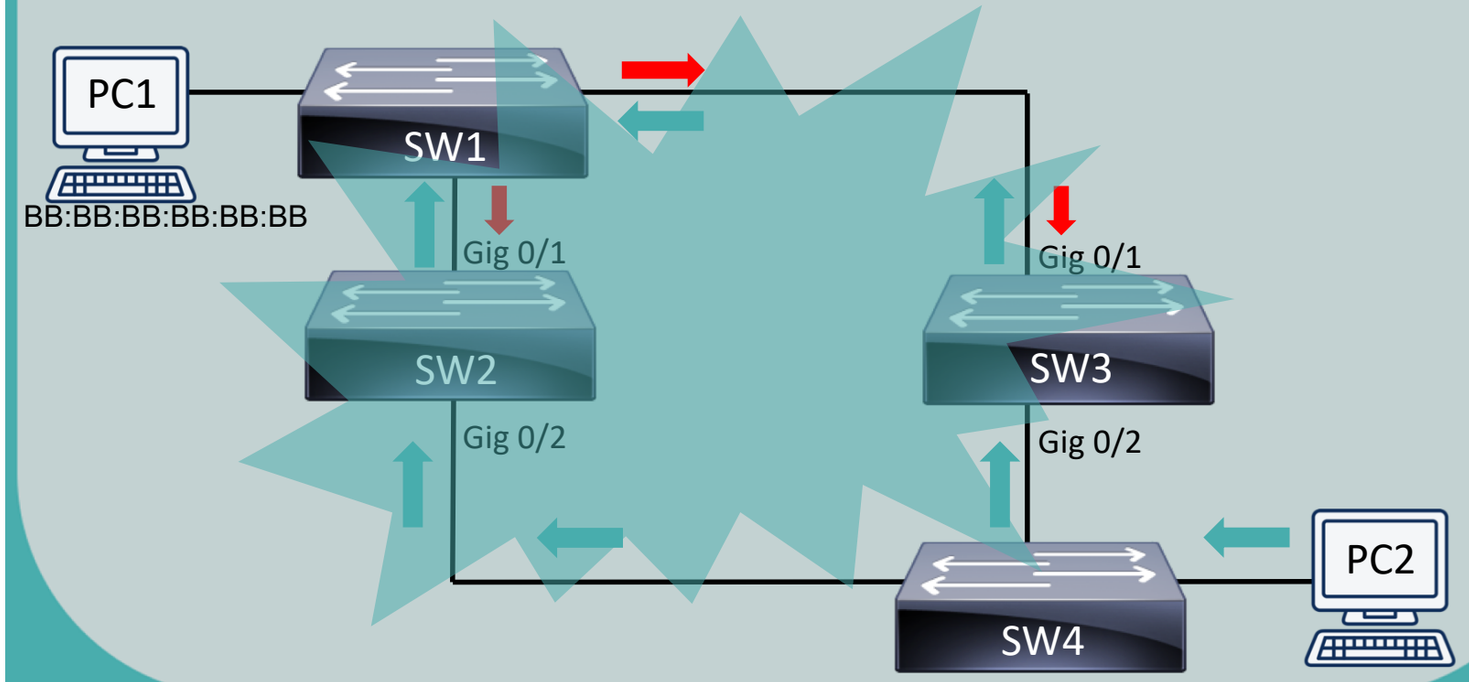
Switch 2
MAC Address Table

Port	MAC Address
Gig 0/1	CC:CC:CC:CC:CC:CC
Gig 0/2	CC:CC:CC:CC:CC:CC

Switch 3
MAC Address Table

Broadcast Storms

- If broadcast frame received by both switches, they can forward frame to each other
- Multiple copies of frame are forwarded, replicated, and forwarded again until the network is consumed with forwarding many copies of the same initial frame

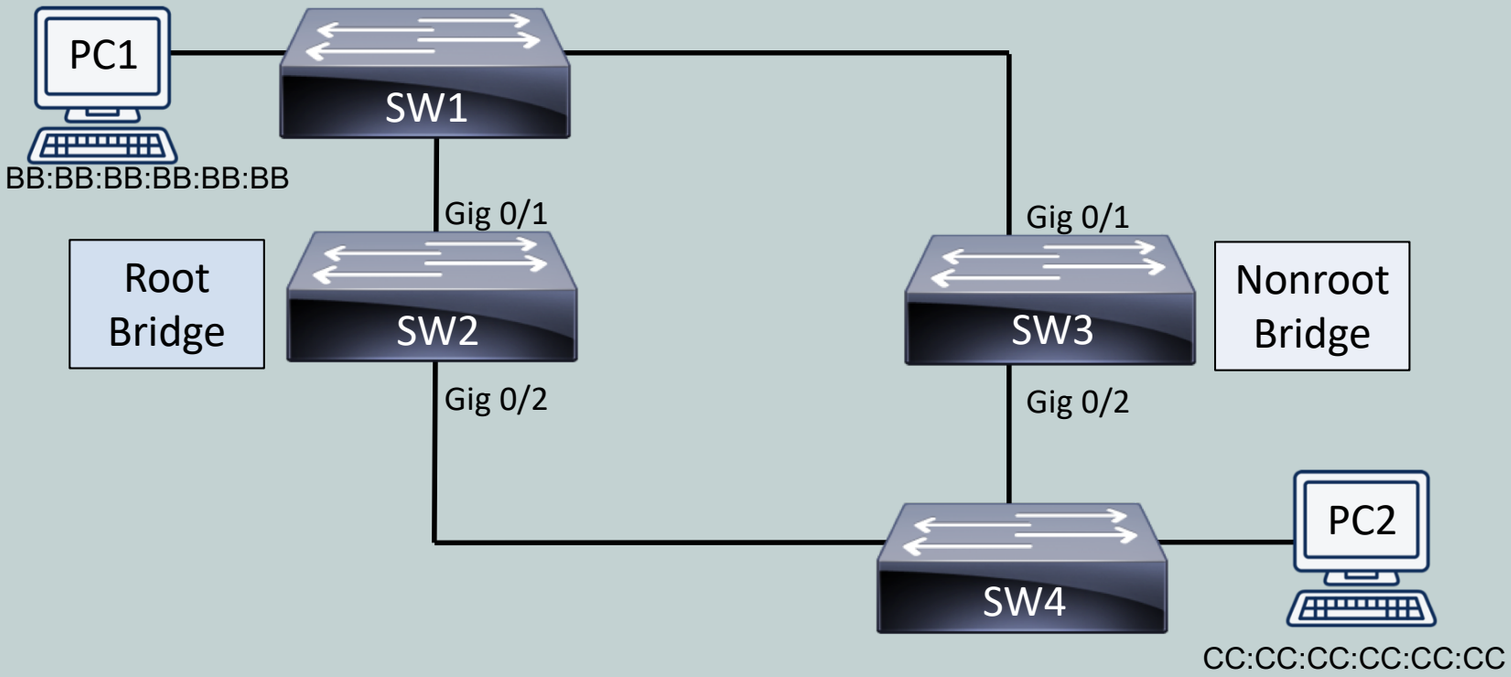


Root and Nonroot Bridges

- Root bridge
  - Switch elected to act as a reference point for a spanning tree
  - Switch with the lowest bridge ID (BID) is elected as the root bridge
  - BID is made up of a priority value and a MAC address (with the lowest value considered root)
- Nonroot bridge
  - All other switches in an STP topology

Root and Nonroot Bridges

- MAC Address table corruption can occur



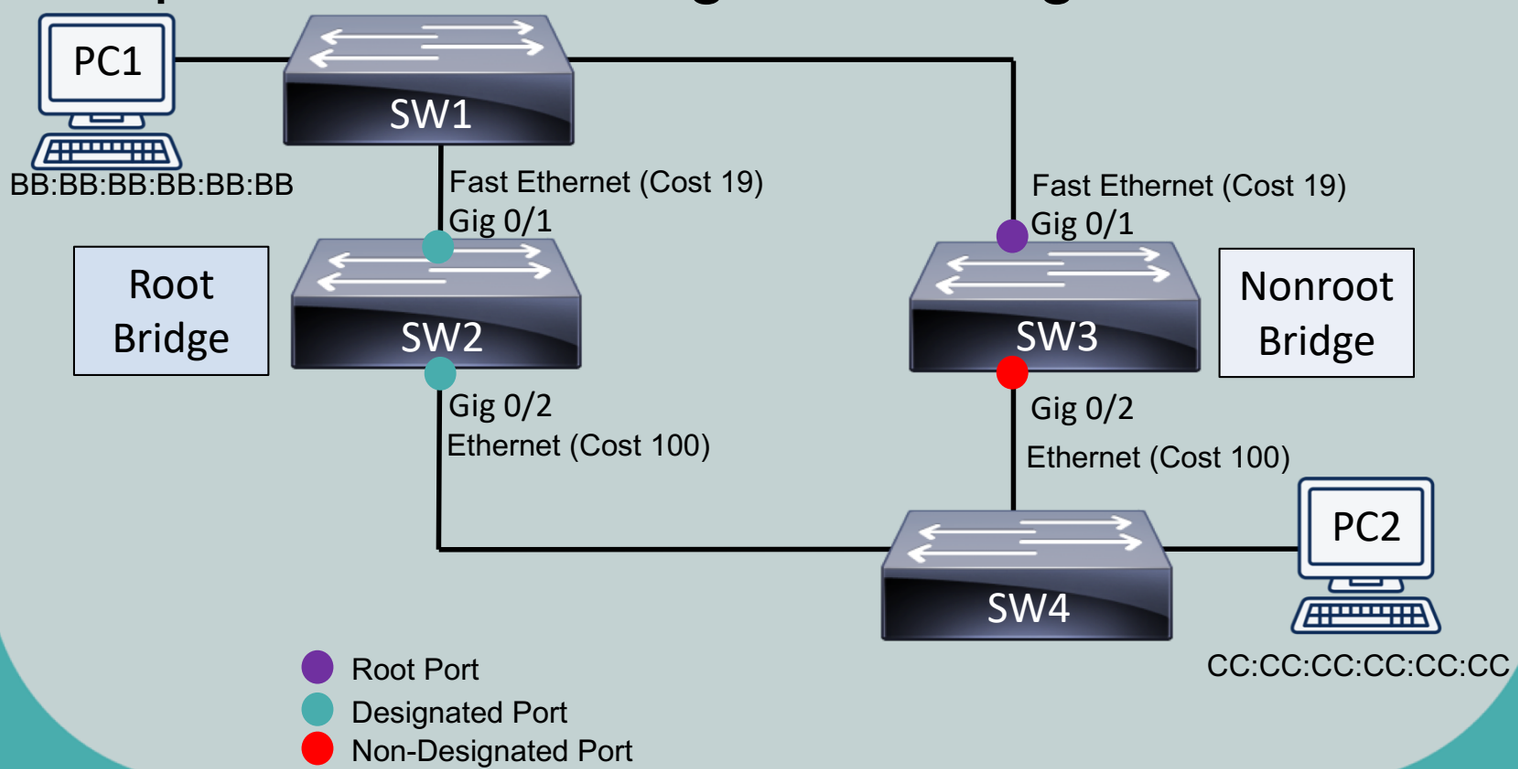
Switch	MAC Address	Priority
SW2	22:22:22:22:22:22	31423
SW3	33:33:33:33:33:33	31423

Root, Designated, and Non-Designated Ports

- Root Port
  - Every non-root bridge has a single root port
  - Port closest to the root bridge in terms of cost
  - If costs are equal, lowest port number is chosen
- Designated Port
  - Every network segment has a designated port
  - Port closest to the root bridge in terms of cost
  - All ports on root bridge are designated ports
- Non-Designated Port
  - Ports that block traffic to create loop-free topology

Root and Nonroot Bridges

- Single root port on non-root bridge
- All other ports on non-root bridge are non-designated
- All ports on root bridge are designated



Port States

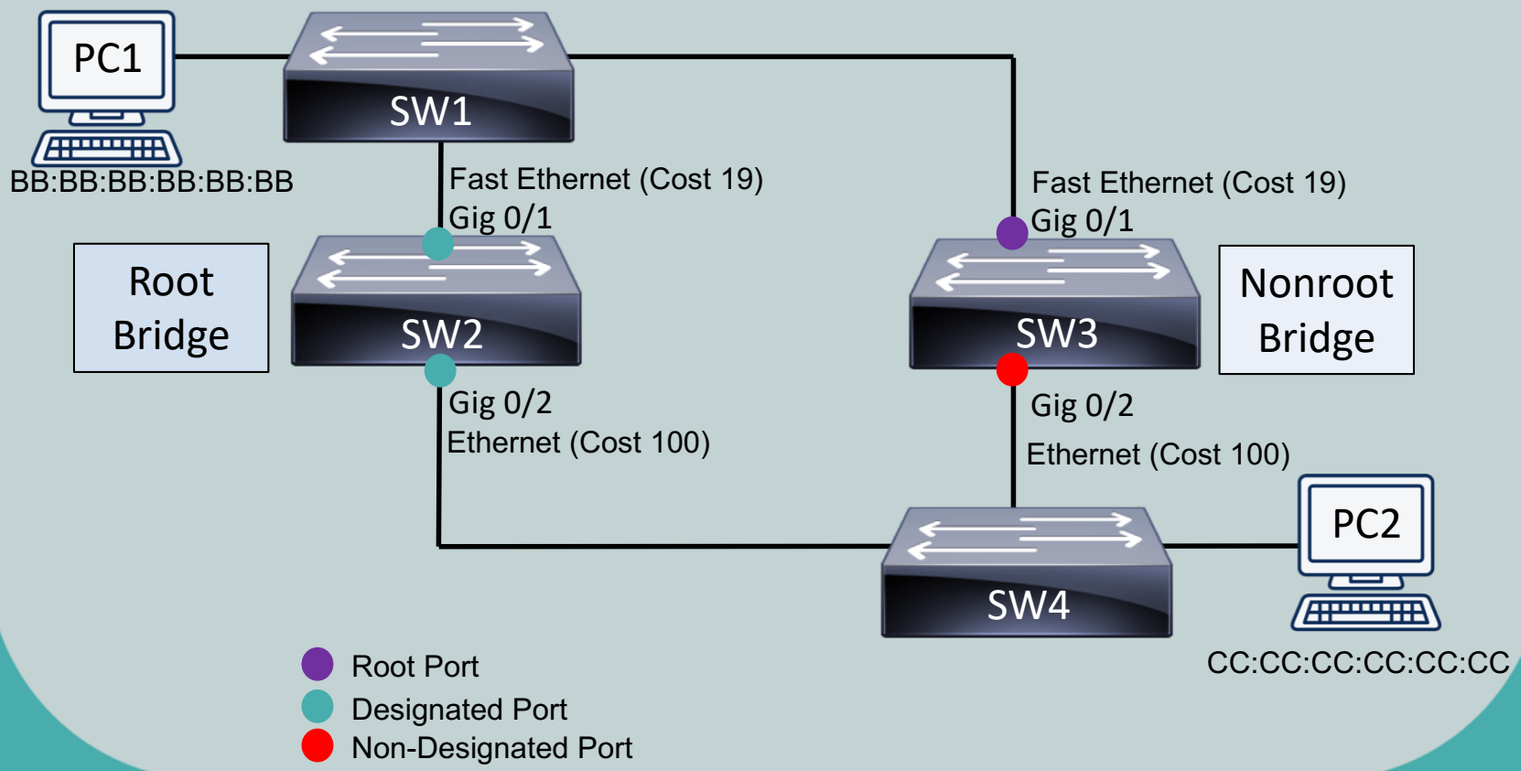
- Non-designated ports do not forward traffic during normal operation, but do receive bridge protocol data units (BPDUs)
- If a link in the topology goes down, the non-designated port detects the failure and determines whether it needs to transition to a forwarding state
- To get to the forwarding state, though, it has to transition through four states

Port States

- Blocking
  - BPDUs are received but they are not forwarded
  - Used at beginning and on redundant links
- Listening
  - Populates MAC address table
  - Does not forward frames
- Learning
  - Processes BPDUs
  - Switch determines its role in the spanning tree
- Forwarding
  - Forwards frames for operations

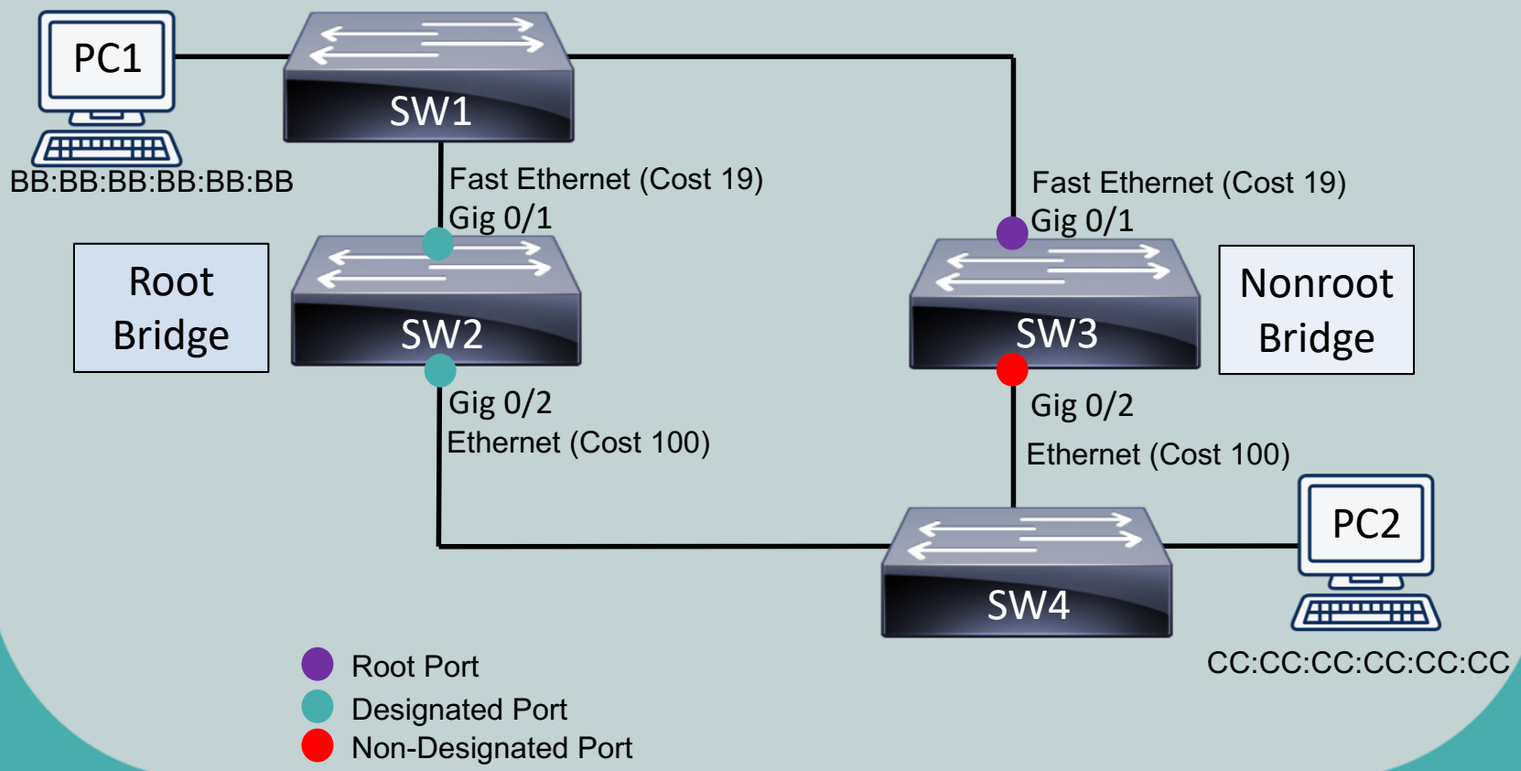
Port States

- Root and Non-designated port are blocking
- Designated ports are forwarding



Link Costs

- Associated with the speed of a link
- Lower the link's speed, the higher the cost



Link Costs

Speed	Ethernet Type	STP Port Cost
10 Mbps	Ethernet	100
100 Mbps	Fast Ethernet	19
1 Gbps	Gigabit Ethernet	4
10 Gbps	10-Gigabit Ethernet	2

- Long STP is being adopted due to higher link speeds over 10 Gbps
- Values range from 2,000,000 for 10-Mbps Ethernet to as little as 2 for 10 Tbps

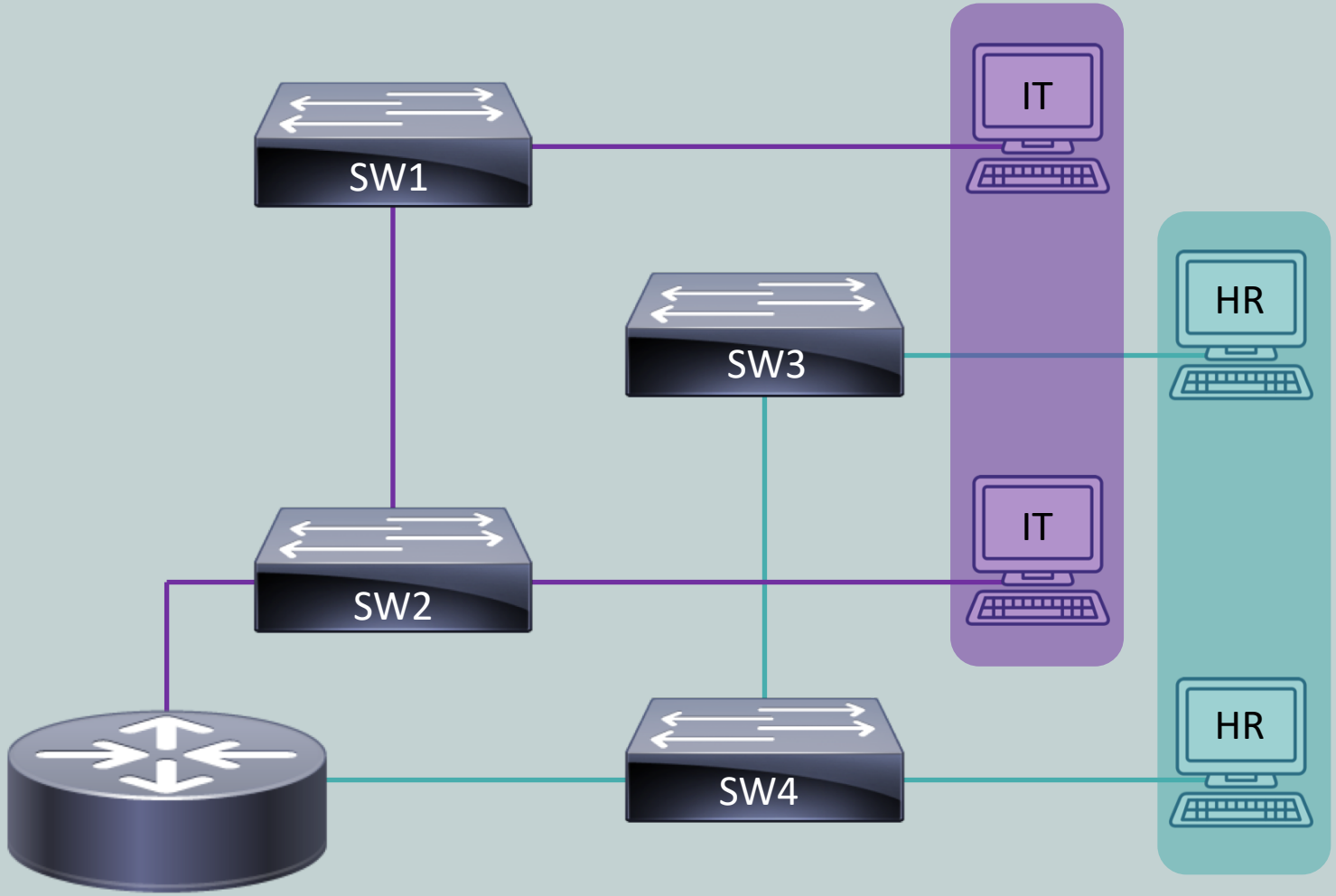
Virtual LAN (VLAN)

CompTIA Network+ (N10-007)

Virtual Local Area Network (VLAN)

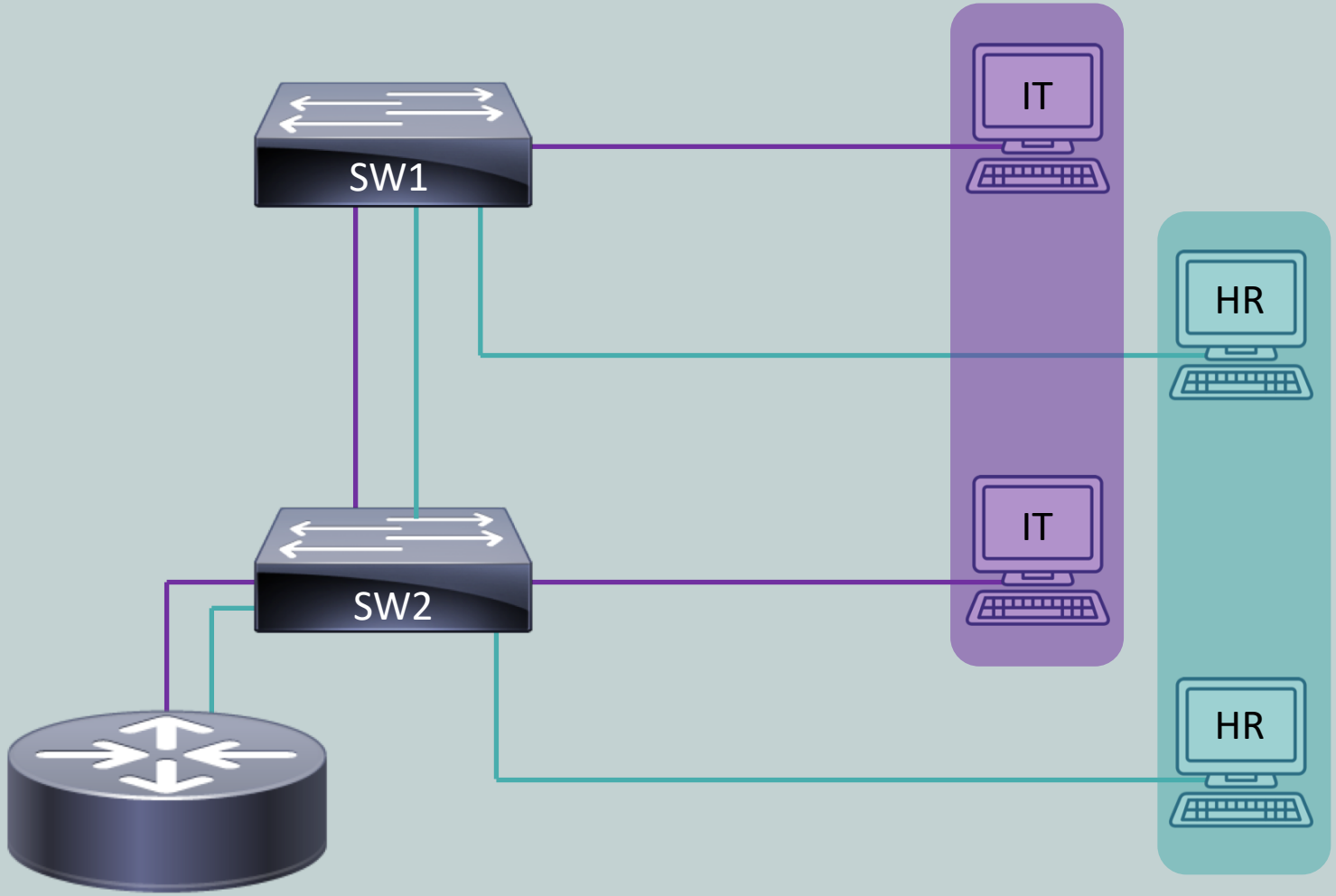
- Switch ports are in a single broadcast domain
- Allow you to break out certain ports to be in different broadcast domains
- Before VLANs, you had to use routers to separate departments, functions, or subnets
- Allow different *logical* networks to share the same *physical* hardware
- Provides added security and efficiency

Before VLANs



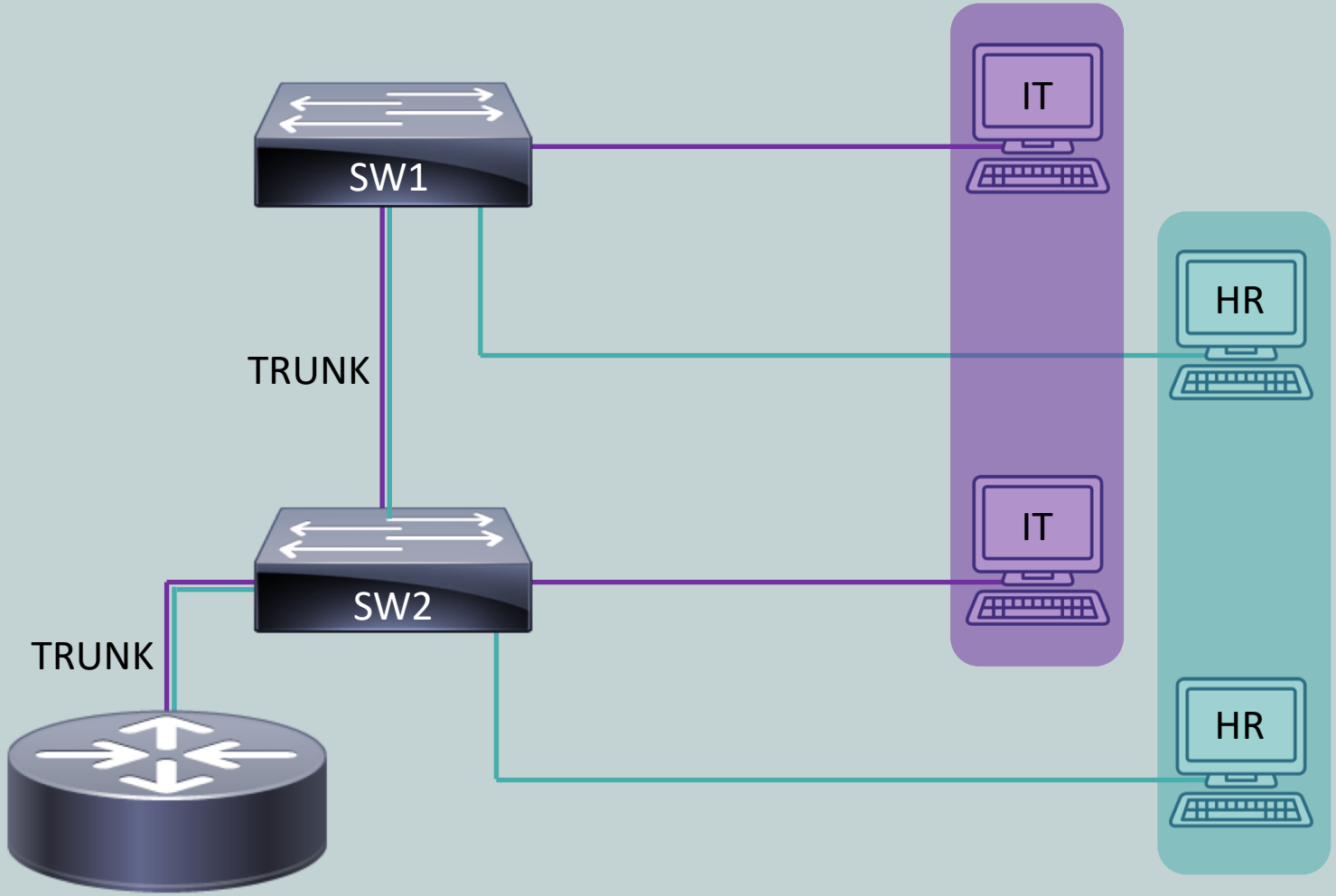
Different switches were required for each LAN for separation

Using VLANs



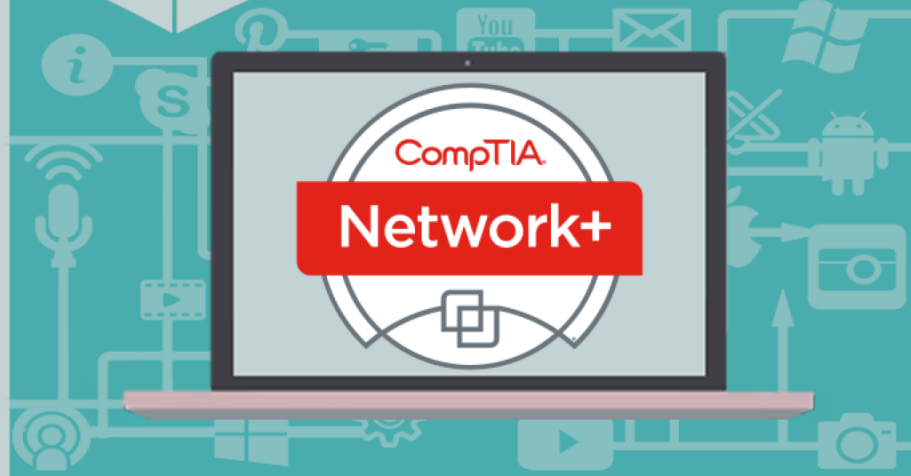
Same switches but switch ports can be in different VLANs

VLAN Trunking (802.1q)



Multiple VLANs transmitted over the same physical cable

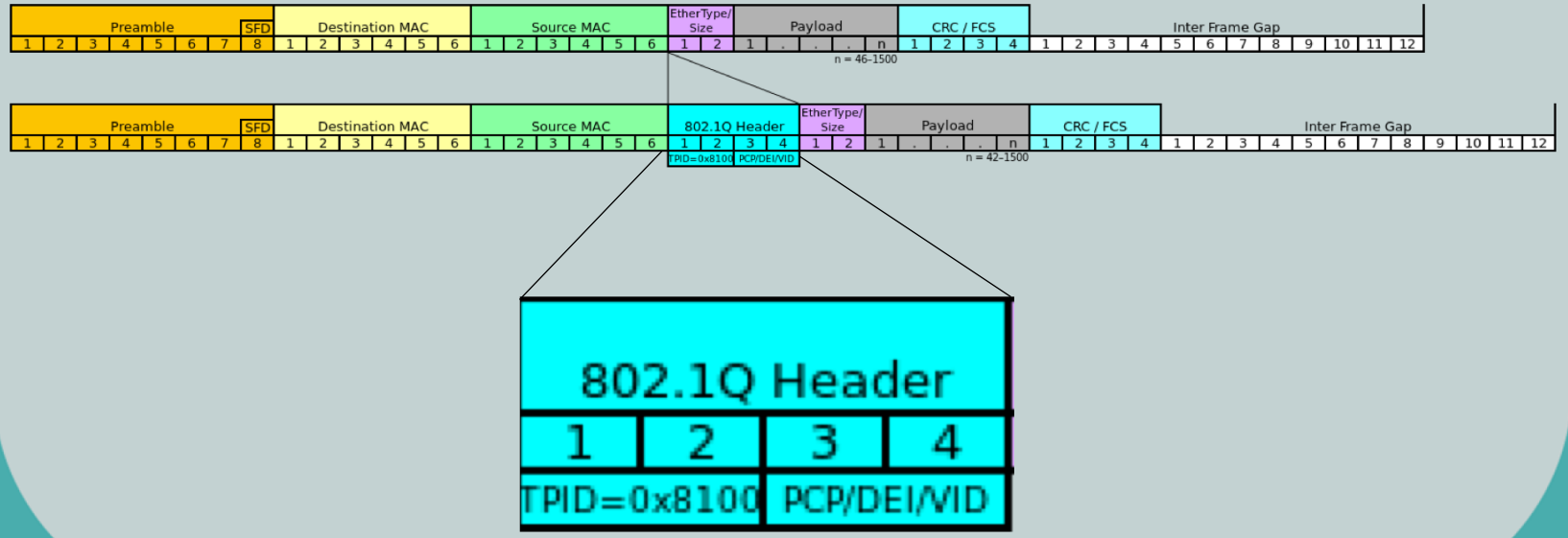
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE



VLAN Trunking (802.1q)

- VLANs are each tagged with 4 byte identifier
  - Tag Protocol Identifier (TPI)
  - Tag Control Identifier (TCI)

- One VLAN is left untagged
  - Called the Native VLAN



Specialized Network Devices

CompTIA Network+ (N10-007)

Specialized Network Devices

- Many other types of network devices besides routers, switches, servers, and workstations
- Others devices serve specific functions to improve usability, performance, and security
- Devices include
  - VPN concentrators
  - Firewalls
  - DNS servers
  - DHCP servers
  - Proxy servers
  - Content engines and switches

VPN Concentrator

- *Virtual private network* (VPN) creates a secure, virtual tunnel network over an untrusted network, like the Internet

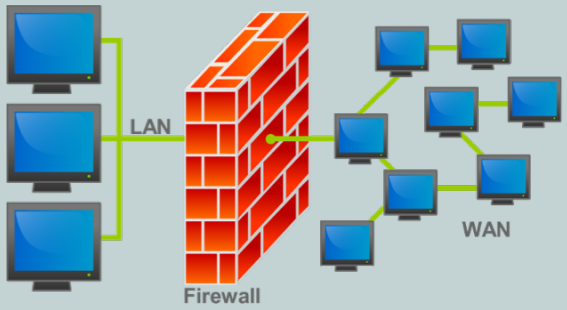
- One of the devices that can terminate VPN tunnels is a VPN concentrator, although firewalls can also perform this function

VPNs are covered in depth in another lesson

Firewalls

- Network security appliance at your boundary
- Firewalls can be software or hardware
- *Stateful firewalls*
  - Allows traffic that originates from inside the network and go out to the Internet
  - Blocks traffic originated from the Internet from getting into the network

Pix Firewall



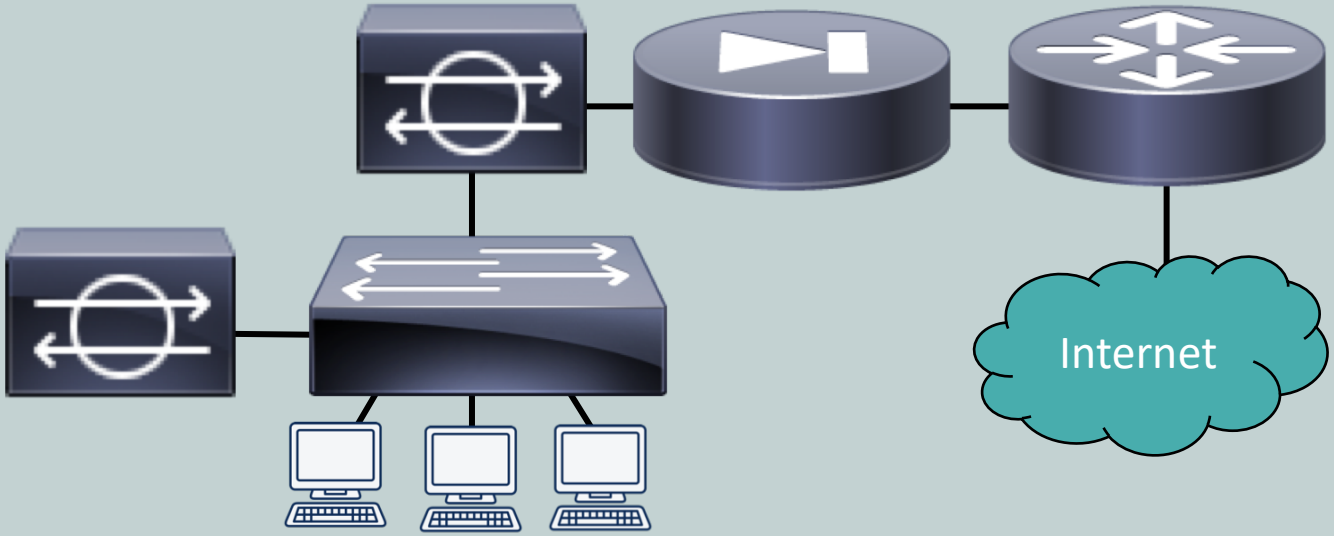
Router with Firewall

Next-Generation Firewall (NGFW)

- Conducts deep packet inspection at Layer 7
- Detects and prevents attacks
- Much more powerful than basic stateless or stateful firewalls
- Continually connects to cloud resources for latest information on threats

Intrusion Detection or Prevention System (IDS/IPS)

- IDS recognizes attacks through signatures and anomalies
- IPS recognizes and responds
- Host or network based devices



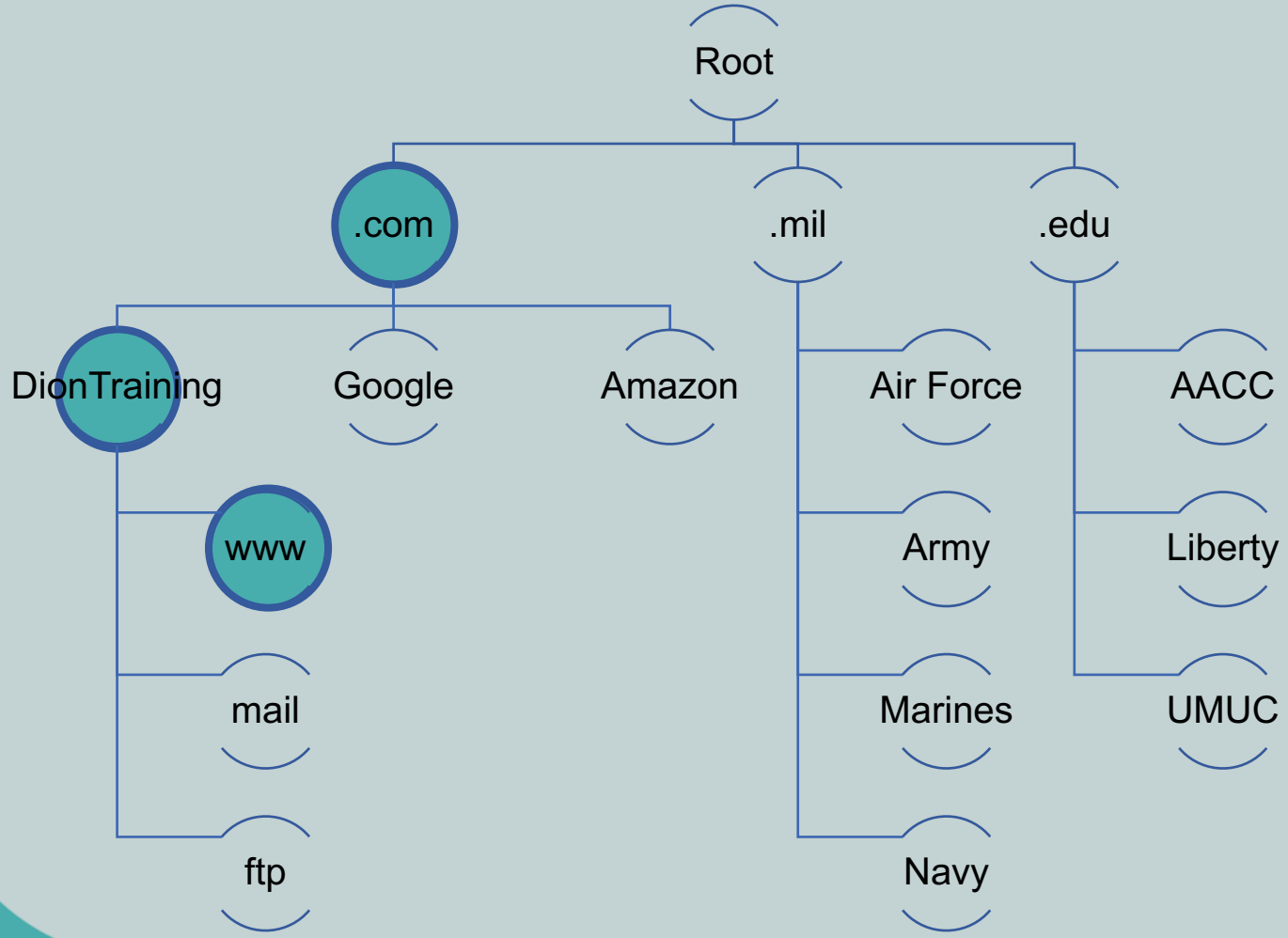
Domain Name System (DNS)

- Converts domain names to IP addresses

- Similar to the contact list on your phone
  - You rarely dial your friends' phone numbers
  - Instead you just click their name to call them

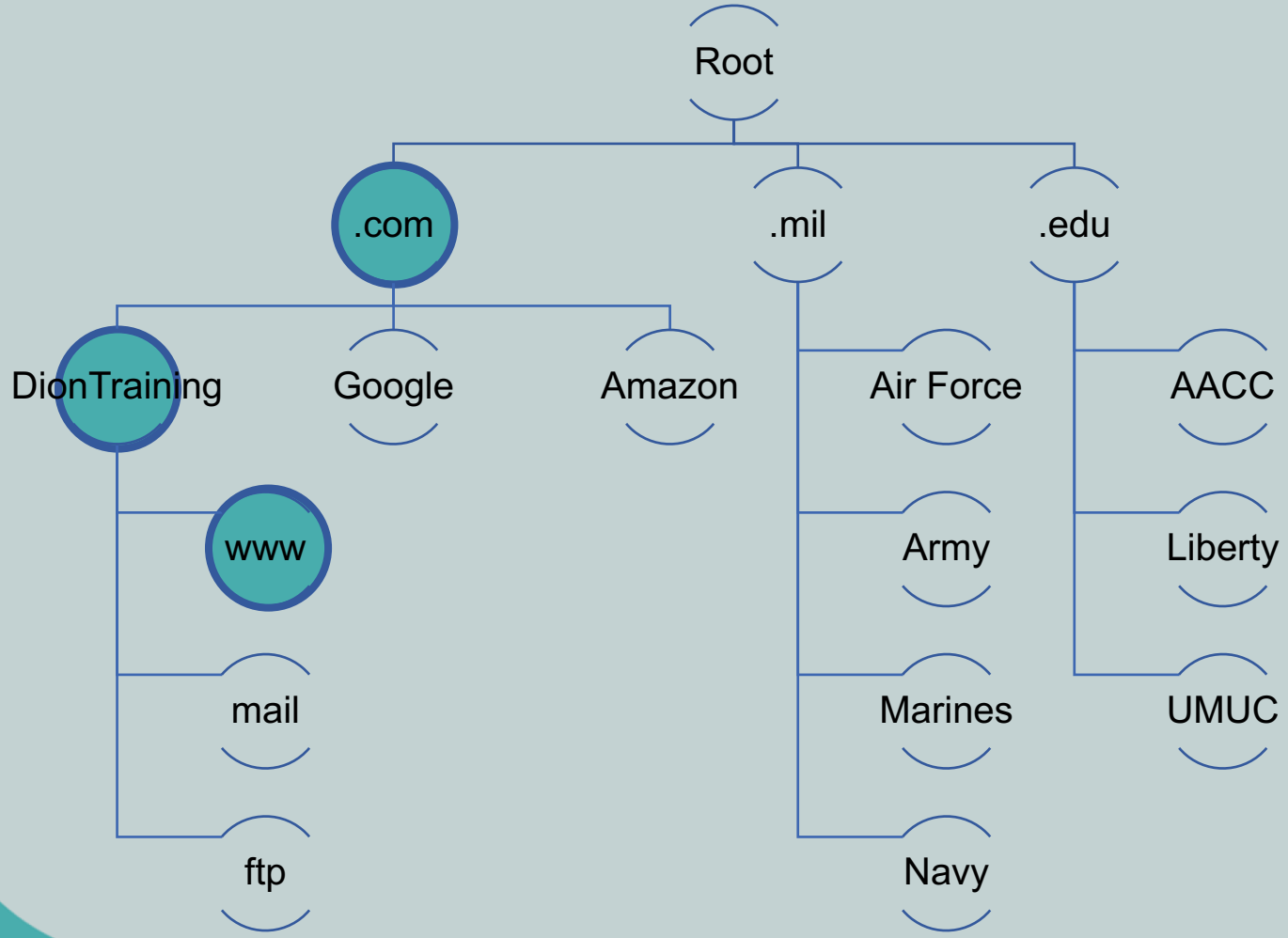
Fully-Qualified Domain Name (FQDN)

- Domain name under a Top-Level Domain and represents a web, mail, or file server



Uniform Resource Locator (URL)

- Contains the FQDN with method of accessing information (https://www.DionTraining.com)

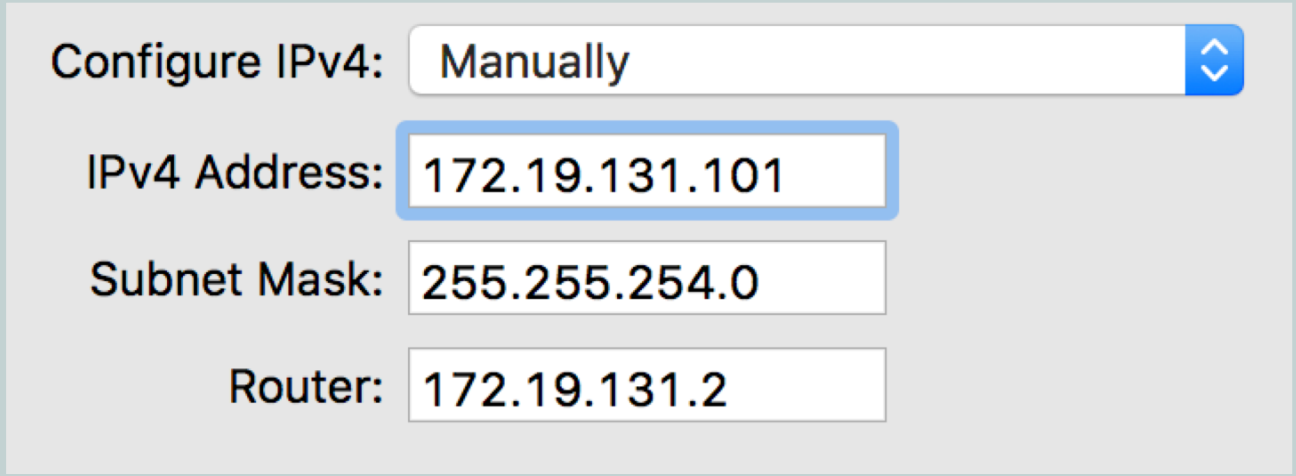


DNS Record Types

Type	Description
A	Address record maps hostname to IPv4 address
AAAA	Address record maps hostname to IPv6 address
CNAME	Canonical name is an alias for existing record; diontraining.com = www.diontraining.com
MX	Mail exchange record maps domain name to email server
NS	Denotes the authoritative name server for the domain
PTR	Pointer record refers to canonical name; used for reverse DNS lookups
SOA	Start of Authority provides authoritative info about DNS zone; contact information, primary name server, refresh times
SRV	Generalized service location record; newer protocol that doesn't require specific protocols records like MX, CNAME, etc.
TXT	Designed to hold human readable code originally; used now to hold machine readable data like DomainKeys Identified Email (DKIM), Sender Policy Framework (SPF), and opportunistic encryption

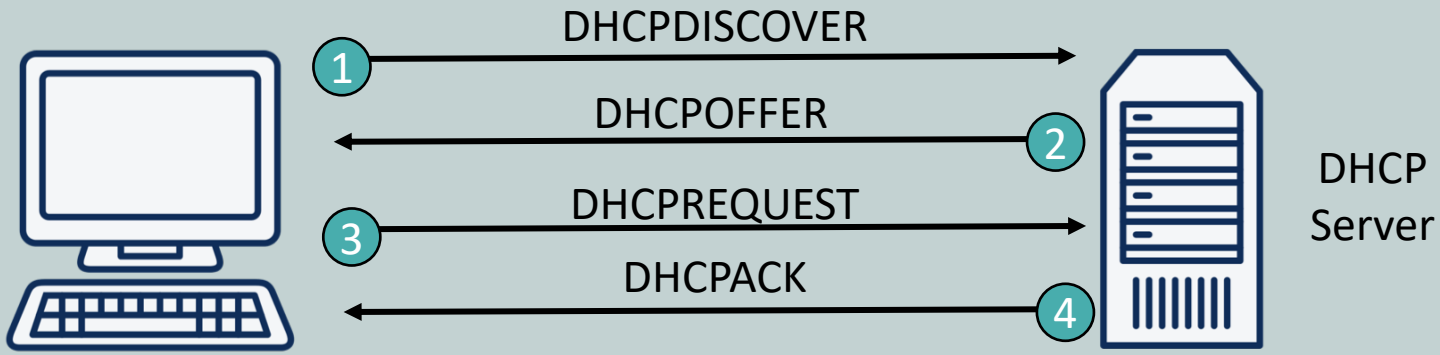
Dynamic Host Configuration Protocol (DHCP)

- Initially, clients on networks needed IP addresses manually configured (or statically assigned) to communicate
  - Can lead to configuration errors
  - Can become a hassle for large networks



Dynamic Host Configuration Protocol (DHCP)

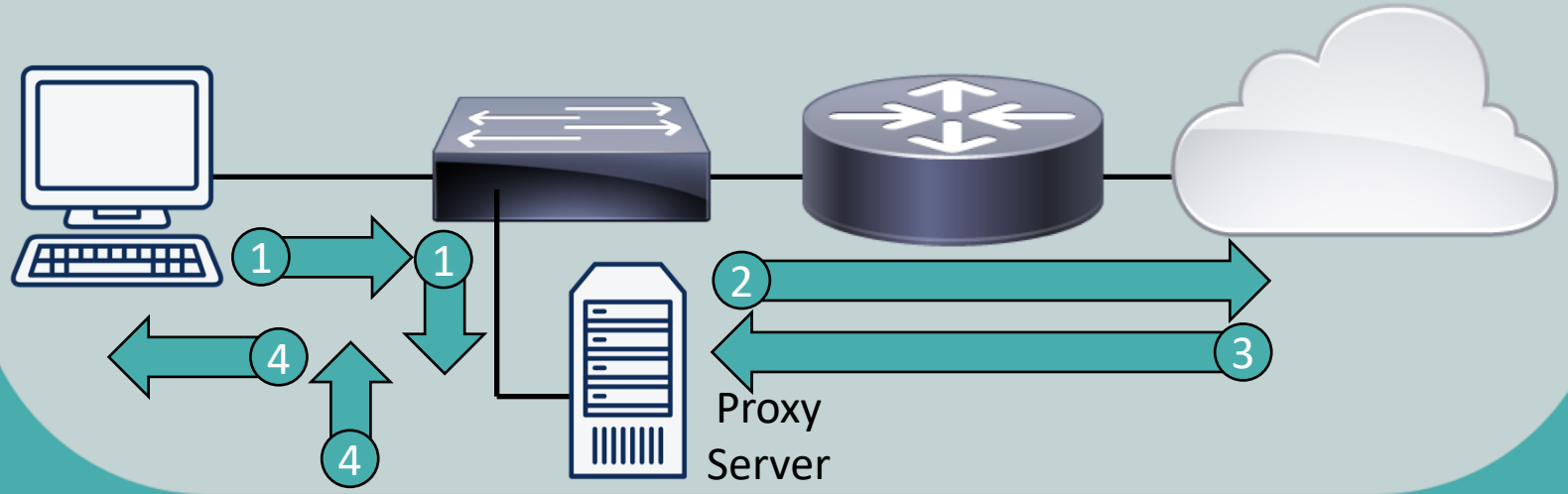
- *A*utomates process so the majority of devices on a network automatically receive
  - IP address
  - Subnet mask
  - Default gateway
  - DNS server addresses



Exam Hint → D.O.R.A.

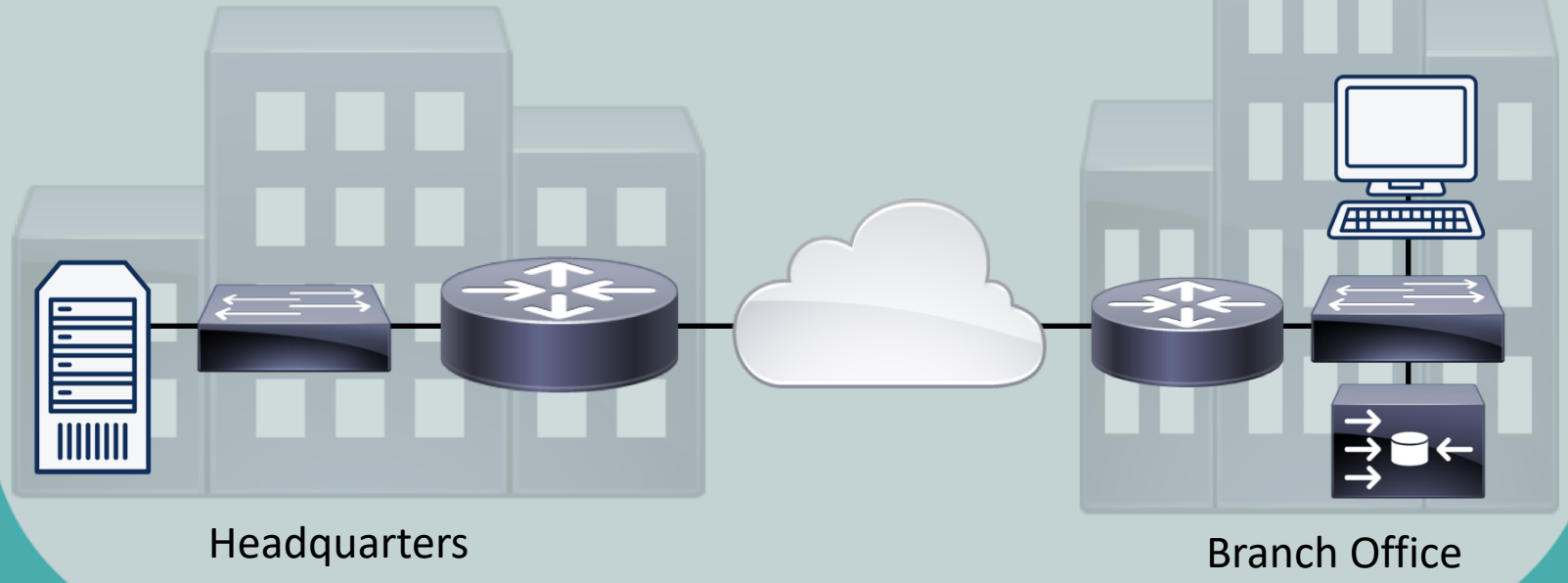
Proxy Server

- Device that makes a request to external network on behalf of a client
- Used for security to perform content filtering and logging
- Workstation clients are configured to forward their packets to a proxy server



Content Engine

- Dedicated appliances that perform the caching functions of a proxy server
- Are more efficient than a proxy server
- Also called Caching Engines



Content Switches

- Distributes incoming requests across the various servers in the server farm

- Also known as Load Balancers