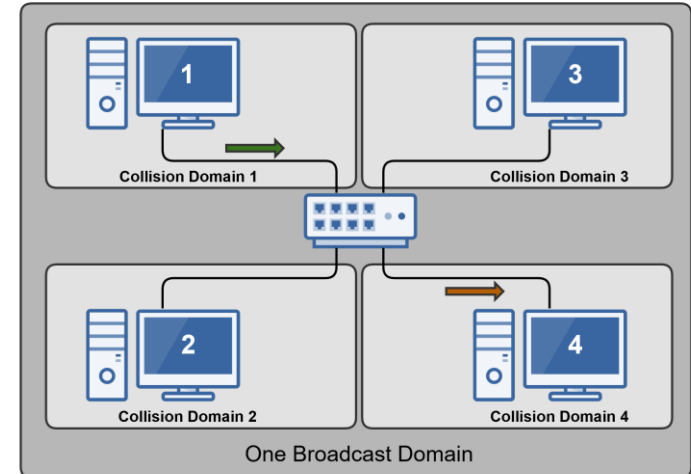


Refresher on Switches

Refresher on Switches

- Connects Devices Together Just Like a Hub
- Intelligent Network Device (OSI Layer 2)
- Memorizes the **MAC Address** of Each Device Connected to It via a **MAC Address Table**
 - Pays attention to Source and Destination MAC addresses during Communication Process
- Breaks up Collision Domains
 - Traffic Goes in One Port and Is Repeated out to Only Destination Port
 - Standard in Today's Network Infrastructure



Collision Domains

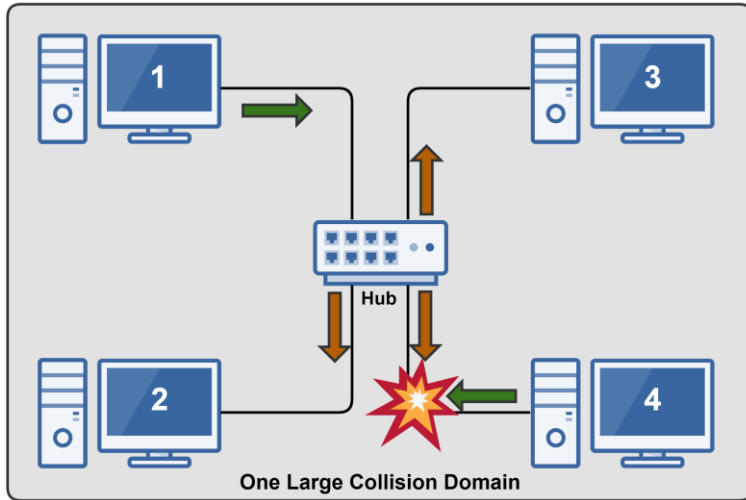
Understanding Collision Domains

- A collision domain is simply a network segment in which data collisions can occur.
- Collisions can occur on ethernet networks using:
 - Hubs
 - Switches in Half-Duplex Mode
- We utilize CSMA/CD to help minimize collisions
 - Carrier Sense Multiple Access with Collision Detection

Understanding Collision Domains

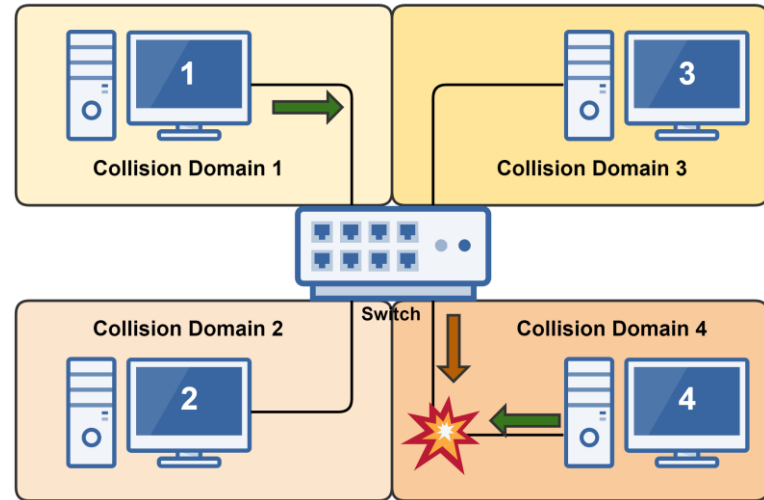
Hubs

- Create one large collision domain.



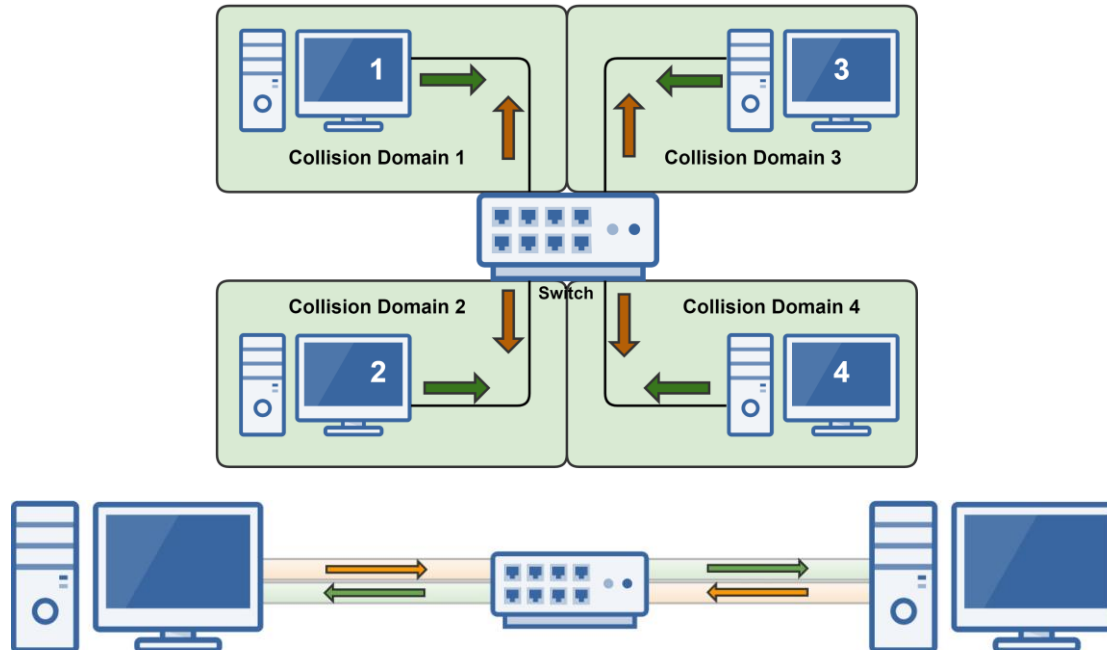
Switches (Half-Duplex)

- Break collision domains up into smaller ones.



Full Duplex Switches Eliminate Collisions

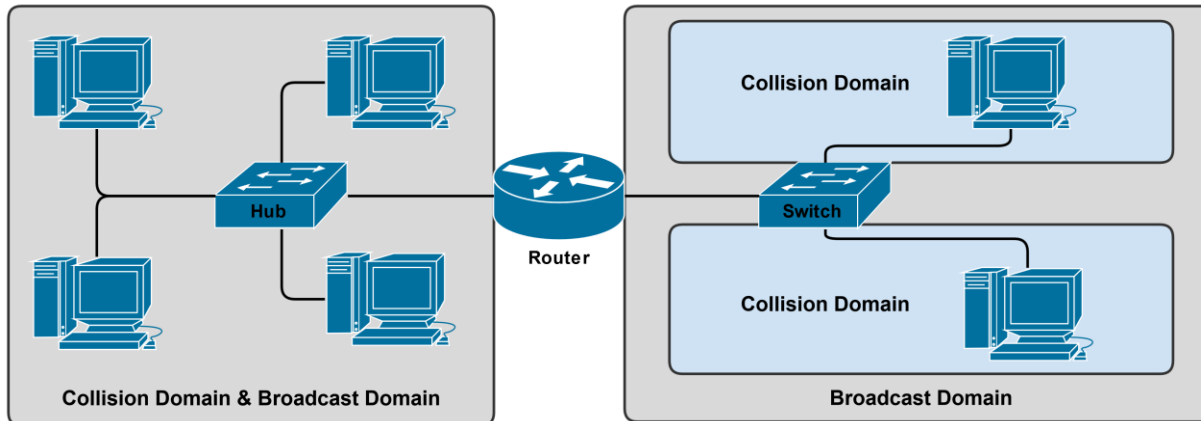
- Collisions don't occur on switches utilizing full duplex mode:
 - There's a dedicated channel for concurrent sending and receiving data.



Broadcast Domains

Understanding Broadcast Domains

- A broadcast domain is a network segment in which all devices on that network receive ethernet broadcasts messages (one-to-all) from each other.
 - **Example Broadcast Protocols:** ARP, DHCP
- Hubs and switches forward broadcast messages; routers do not.
 - Broadcast messages are very inefficient and resource-intensive.
 - If routers allowed broadcasts, WAN and Internet performance would drastically decline due to broadcast storms.

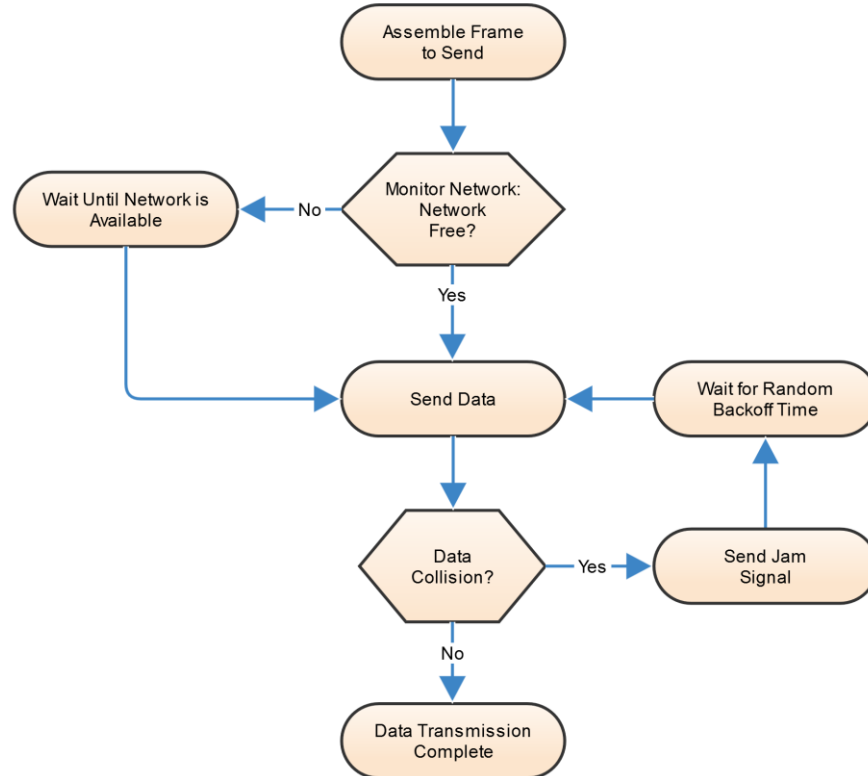


CSMA/CD

CSMA/CD

- **CSMA/CD**: Carrier Sense Multiple Access with Collision Detection
- Used on a shared network medium to help reduce data collisions.
- Helps hosts decide when to send data and also detect collisions
- Used with hubs (multi-port repeaters) where there is one large collision domain.
- Used with switches **ONLY** in half-duplex mode.

CSMA/CD Process



Managed versus Unmanaged Switches

Unmanaged vs. Managed Switches

Unmanaged

- Completely unmanaged.
- Unbox it, plug it in, and it works without any administration.

Managed

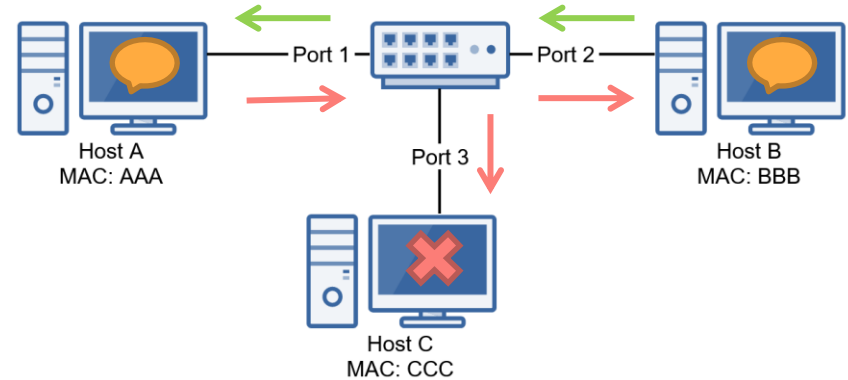
- Can be configured and managed by network administrators, typically via Telnet or SSH.
 - Configure static entries in the MAC table.
 - Configure half or full-duplex on specific ports.
 - Monitor switch performance with SNMP.
 - Create virtual LANs (VLANs)
 - Configure Port Mirroring
- Much more expensive than unmanaged switches.

How a Switch Learns MAC Addresses

How a Switch Learns MAC Addresses

The Switch Learning Process

1. Host A sends Ethernet frame to Host B
 - **Source:** AAA, **Destination:** BBB
2. Switch records that Host A's MAC address is on Port 1 in its MAC Address Table.
3. Switch doesn't know what port Host B is using, so it will flood ports 2 and 3 (broadcast).
4. Hosts B & C will examine the Ethernet frame. Host C will discard it and Host B will respond to Host A.
 - **Source:** BBB, **Destination:** AAA.
5. When Host B responds, the switch will record Host B's MAC address on Port 2.
6. The switch already knows that Host A is on Port 1, so it will forward the Ethernet frame to Port 1.

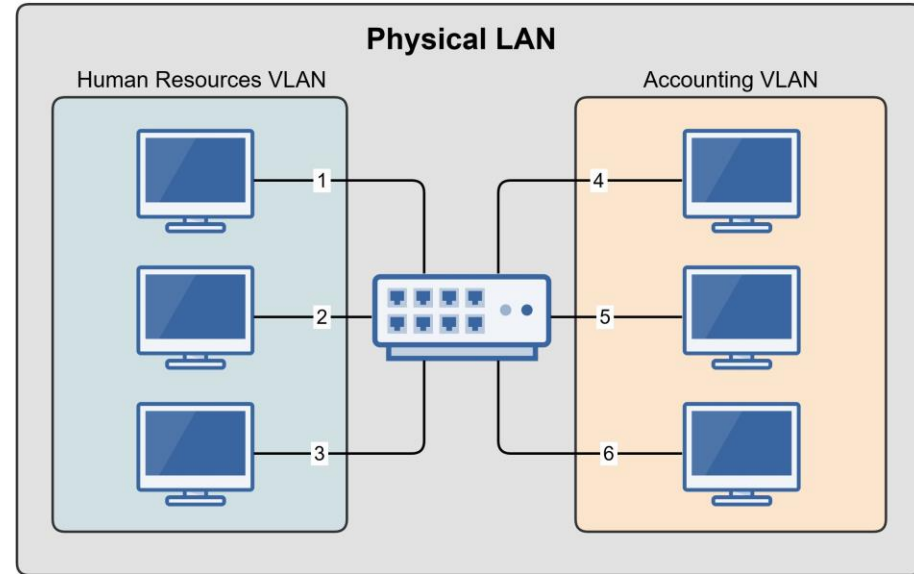


Switch's MAC Address Table	
Port Number	MAC Address
1	
2	

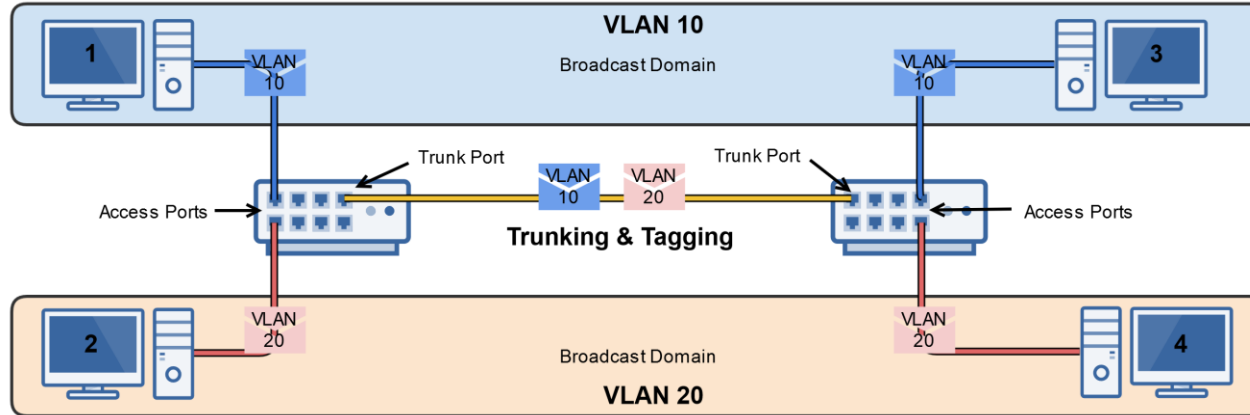
Virtual LANs (VLANs)

Virtual LANs (VLANs)

- Essentially LANs within a LAN
 - Physical Switch → Multiple Virtual Switches
- Break up a large “physical” LAN into several smaller “logical” LANs.
- Accomplished with managed switches.
- Assign specific switch interfaces (ports) to specific virtual LANs.
 - Human Resource VLAN (Interfaces 1, 2, 3)
 - Accounting VLAN (Interfaces 4, 5, 6)
- Benefits of VLANs
 - Reduces Broadcast Domains
 - Segments Network by Role
 - Increases Security
 - Devices Cannot Communicate with Other VLANs
 - Group Devices by Need, Not Physical Location



VLANs with Multiple Switches

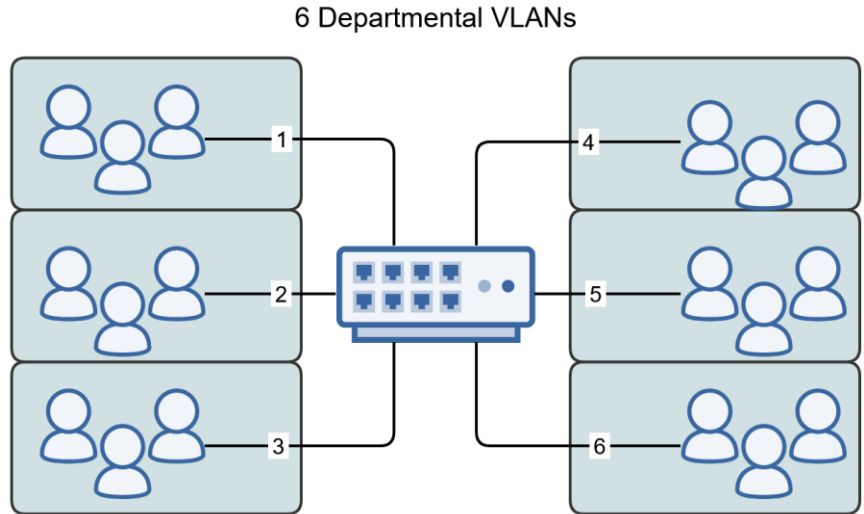


- **Trunk Ports:** Creates a connection between two switches (trunk link) for VLAN traffic to traverse for multiple VLANs.
- **Access Ports:** Ports configured for use for a single VLAN.
- **Tagging (802.1Q):** Ethernet frames are tagged with their respective VLAN ID when traversing trunk ports to ensure proper delivery.
- **Untagged Frames:** If a frame isn't tagged with a VLAN ID, switch trunk ports can be configured with a native VLAN, to which the untagged frame will be sent.

Layer 3 Switches

Layer 3 Switches

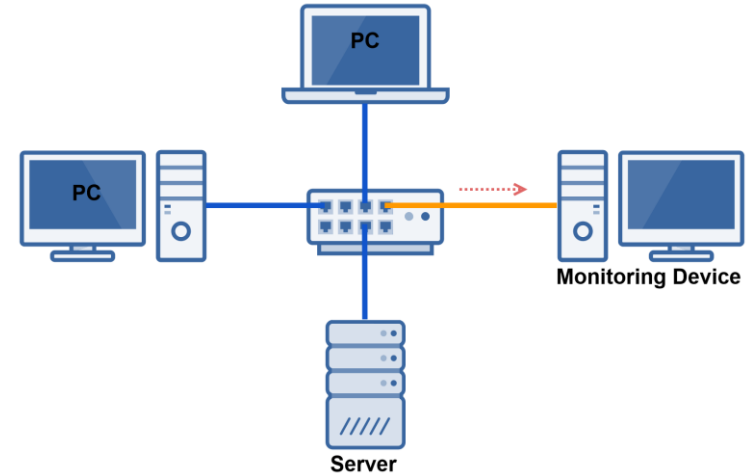
- Provide Layer 2 Switching & Layer 3 Routing.
 - **OSI Layer 2 (Data Link):** Switching
 - MAC Addresses
 - **OSI Layer 3 (Network):** Routing
 - IP Addresses
- Managed Switch Capability
- Used in Conjunction with VLANs
- Provides:
 - VLAN Switching
 - IP Routing between VLANs
- One Device Instead of Router & Switch



Port Mirroring

Port Mirroring

- When a switch is configured to have a dedicated port receive all traffic on that network for:
 - Monitoring
 - Diagnostics
 - Troubleshooting
- Also called a Switch Port Analyzer (SPAN)



Power over Ethernet (PoE)

Power over Ethernet (PoE)

- Gives us the ability to power network-connected devices with Ethernet cables:
 - VoIP Phones
 - Wireless Access Points
 - IP Security Cameras
- Provides electricity and network data in the same cable.
- Two Methods:
 - PoE Switch
 - Non-PoE Switch + PoE Injector

